กฎหมาย
ว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์
Cyber Security Law



จัดทำโดย
ฝ่ายกฎหมายและระเบียบ สำนักกฎหมาย
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

Created by
Legal and Regulatory Division, Legal Office
National Cyber Security Agency

สารบัญ
Table of content

หน้า
Page

1. **พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562** 1
   Cybersecurity Act B.E. 2562 (2019)

2. **ประกาศ กมช. เรื่อง การจัดตั้ง หน้าที่และอำนาจของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ พ.ศ. 2564** 58
   Notification of NCSC Re: Establishment, Duties, and Powers of Thailand Computer Emergency Response Team (ThaiCERT) B.E. 2564 (2021)

3. **ประกาศ กมช. เรื่อง ลักษณะ หน้าที่และความรับผิดชอบของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและภารกิจหรือให้บริการที่เกี่ยวข้อง พ.ศ. 2564** 73
   Notification of NCSC Re :Characteristics, Duties, and Responsibilities of the Computer Emergency Response Team for Critical Information Infrastructure organizations, Related Missions and Services B.E. 2564 (2021)

4. **ประกาศ กมช. เรื่อง หลักเกณฑ์ ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและการมอบหมายการควบคุมและกำกับดูแล พ.ศ. 2568** 92
   Notification of NCSC Re: Criteria and Characteristics for Designating Agencies with Missions or Services as Critical Information Infrastructure organizations and the Regulation Assignment, B.E. 2568 (2025)

5. **ประกาศ กกม. เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564** 105
   Notification of CRC Re: Codes of Practice and Standard Frameworks for Government Agencies and Critical Information Infrastructure organizations B.E. 2564 (2021)

6. **ประกาศ กมช. เรื่อง การกำหนดระดับความรู้ความชำนาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อแต่งตั้งเป็นพนักงานเจ้าหน้าที่ พ.ศ. 2564** 145
   Notification of NCSC Re: Cybersecurity Knowledge and Expertise Requirements for Competent Official Appointment B.E. 2564 (2021)

7. **ประกาศ กมช. เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. 2564** 162
   Notification of NCSC Re: Characteristics and Measures for Prevention, Response, Assessment, Eradication, and Containment of Cyber Incidents at Each Level, B.E. 2564 (2021)

สารบัญ
Table of content

หน้า
Page

8. ระเบียบ กกม. ว่าด้วยการมอบอำนาจให้ปฏิบัติการแทนคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2565 210
Regulation of CRC on the Assignment of Powers to Perform Tasks on behalf of the Cybersecurity Regulating Committee B.E. 2565 (2022)

9. ประกาศ กมช. เรื่อง นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 - 2570) 228
Notification of the NCSC Re: Policy and plan on cyber security B.E. 2565 - 2570 (2022-2027)

10. ประกาศ กกม. เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ. 2566 317
Regulation of CRC Cyber Incident Reporting Criteria and Procedure B.E.2566 (2023)

11. ประกาศ สกมช. เรื่อง หลักเกณฑ์และอัตราค่าธรรมเนียมค่าบำรุง ค่าตอบแทน และค่าบริการในการดำเนินงาน พ.ศ. 2566 347
Notification of NCSA Re: Criteria and Rates of Fees, Maintenance Fees, Compensation Fees, and Service Fees for Operations B.E. 2566 (2023)

12. ประกาศ กมช. เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. 2566 367
Notification of the NCSC Re: Standards for defining cybersecurity characteristics for data or information systems B.E. 2566 (2023)

13. ประกาศ กมช. เรื่อง มาตรฐานขั้นต่ำของข้อมูลหรือระบบสารสนเทศ พ.ศ. 2566 375
Notification of the NCSC Re: standards for data or information systems B.E. 2566 (2023)

14. ประกาศ กมช. เรื่อง มาตรฐานและแนวทางส่งเสริมพัฒนาระบบการให้บริการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2566 384
Notification of the NCSC Re: standards and guidelines for promoting the development of Cybersecurity service delivery systems B.E. 2566 (2023)

15. ประกาศ กมช. เรื่อง มาตรการและแนวทางในการยกระดับทักษะความรู้และความเชี่ยวชาญในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2567 395
Notification of the NCSC Re: measures and guidelines to enhance the knowledge and expertise in Cybersecurity B.E. 2567 (2024)

สารบัญ
Table of content

หน้า
Page

16. ประกาศ กมม. เรื่อง หน้าที่ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและหน่วยงานควบคุมหรือกำกับดูแล พ.ศ. 2567 445
Regulation of CRC on the Assignment of Powers to Perform Tasks on behalf of the Cybersecurity Regulating Committee B.E. 2565 (2022)

17. ประกาศ กมช. เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 459
Notification of the NCSC Re: Cybersecurity Standards for Cloud Systems B.E. 2567 (2024)

18. ประกาศ กมช. เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ พ.ศ. 2568 516
Notification of the NCSC Re: Website Security Standards B.E. 2568 (2025)

19. อภิธานศัพท์ 597
Glossary

20. อินโฟกราฟิกส์ 620
Infographic

1

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

มีผลใช้บังคับตั้งแต่วันที่ 28 พ.ค. 62 เป็นต้นไป

Cybersecurity Act B.E. 2562 (2019)

effective from May 28, 2019, onwards.



ฉบับภาษาไทย

Thai Version



พระราชบัญญัติ
การรักษาความมั่นคงปลอดภัยไซเบอร์
พ.ศ. ๒๕๖๒

พระบาทสมเด็จพระปรเมนทรรามาธิบดีศรีสินทรมหาวชิราลงกรณ พระวชิรเกล้าเจ้าอยู่หัว

ให้ไว้ ณ วันที่ ๒๔ พฤษภาคม พ.ศ. ๒๕๖๒
เป็นปีที่ ๔ ในรัชกาลปัจจุบัน

พระบาทสมเด็จพระปรเมนทรรามาธิบดีศรีสินทรมหาวชิราลงกรณ พระวชิรเกล้าเจ้าอยู่หัว มีพระบรมราชโองการโปรดเกล้าฯ ให้ประกาศว่า

โดยที่เป็นการสมควรมีกฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์

พระราชบัญญัตินี้มีบทบัญญัติบางประการเกี่ยวกับการจำกัดสิทธิและเสรีภาพของบุคคล ซึ่งมาตรา ๒๖ ประกอบกับมาตรา ๒๘ มาตรา ๓๒ มาตรา ๓๓ มาตรา ๓๔ มาตรา ๓๖ และมาตรา ๓๗ ของรัฐธรรมนูญแห่งราชอาณาจักรไทย บัญญัติให้กระทำได้โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมาย

เหตุผลและความจำเป็นในการจำกัดสิทธิและเสรีภาพของบุคคลตามพระราชบัญญัตินี้ เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์มีประสิทธิภาพและเพื่อให้มีมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์อันกระทบต่อความมั่นคงของรัฐและความสงบเรียบร้อยภายในประเทศ ซึ่งการตราพระราชบัญญัตินี้สอดคล้องกับเงื่อนไขที่บัญญัติไว้ในมาตรา ๒๖ ของรัฐธรรมนูญแห่งราชอาณาจักรไทยแล้ว

จึงทรงพระกรุณาโปรดเกล้าฯ ให้ตราพระราชบัญญัติขึ้นไว้โดยคำแนะนำและยินยอมของสภานิติบัญญัติแห่งชาติทำหน้าที่รัฐสภา ดังต่อไปนี้

มาตรา ๑ พระราชบัญญัตินี้เรียกว่า “พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒”

มาตรา ๒ พระราชบัญญัตินี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

มาตรา ๓ ในพระราชบัญญัตินี้

“การรักษาความมั่นคงปลอดภัยไซเบอร์” หมายความว่า มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกประเทศอันกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ

“ภัยคุกคามทางไซเบอร์” หมายความว่า การกระทำหรือการดำเนินการใด ๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

“ไซเบอร์” หมายความรวมถึง ข้อมูลและการสื่อสารที่เกิดจากการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต หรือโครงข่ายโทรคมนาคม รวมทั้งการให้บริการโดยปกติของดาวเทียมและระบบเครือข่ายที่คล้ายคลึงกัน ที่เชื่อมต่อกันเป็นการทั่วไป

“หน่วยงานของรัฐ” หมายความว่า ราชการส่วนกลาง ราชการส่วนภูมิภาค ราชการส่วนท้องถิ่น รัฐวิสาหกิจ องค์กรฝ่ายนิติบัญญัติ องค์กรฝ่ายตุลาการ องค์กรอิสระ องค์การมหาชน และหน่วยงานอื่นของรัฐ

“ประมวลแนวทางปฏิบัติ” หมายความว่า ระเบียบหรือหลักเกณฑ์ที่คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์กำหนด

“เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์” หมายความว่า เหตุการณ์ที่เกิดจากการกระทำหรือการดำเนินการใด ๆ ที่มิชอบซึ่งกระทำการผ่านทางคอมพิวเตอร์หรือระบบคอมพิวเตอร์ซึ่งอาจเกิดความเสียหายหรือผลกระทบต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือความมั่นคงปลอดภัยไซเบอร์ของคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์

“มาตรการที่ใช้แก้ปัญหาเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์” หมายความว่า การแก้ไขปัญหาความมั่นคงปลอดภัยไซเบอร์โดยใช้บุคลากร กระบวนการ และเทคโนโลยี โดยผ่านคอมพิวเตอร์ ระบบคอมพิวเตอร์ โปรแกรมคอมพิวเตอร์ หรือบริการที่เกี่ยวกับคอมพิวเตอร์ใด ๆ เพื่อสร้างความมั่นใจและเสริมสร้างความมั่นคงปลอดภัยไซเบอร์ของคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์

“โครงสร้างพื้นฐานสำคัญทางสารสนเทศ” หมายความว่า คอมพิวเตอร์หรือระบบคอมพิวเตอร์ซึ่งหน่วยงานของรัฐหรือหน่วยงานเอกชนใช้ในกิจการของตนที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของรัฐ ความปลอดภัยสาธารณะ ความมั่นคงทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ

“หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ” หมายความว่า หน่วยงานของรัฐหรือหน่วยงานเอกชน ซึ่งมีภารกิจหรือให้บริการโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

“หน่วยงานควบคุมหรือกำกับดูแล” หมายความว่า หน่วยงานของรัฐ หน่วยงานเอกชน หรือบุคคลซึ่งมีกฎหมายกำหนดให้มีหน้าที่และอำนาจในการควบคุมหรือกำกับดูแลการดำเนินกิจการของหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

“คณะกรรมการ” หมายความว่า คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

“พนักงานเจ้าหน้าที่” หมายความว่า ผู้ซึ่งรัฐมนตรีแต่งตั้งให้ปฏิบัติการตามพระราชบัญญัตินี้

“เลขาธิการ” หมายความว่า เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

“สำนักงาน” หมายความว่า สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

“รัฐมนตรี” หมายความว่า รัฐมนตรีผู้รักษาการตามพระราชบัญญัตินี้

มาตรา ๔ ให้นายกรัฐมนตรีรักษาการตามพระราชบัญญัตินี้ และให้มีอำนาจออกประกาศและแต่งตั้งพนักงานเจ้าหน้าที่ เพื่อปฏิบัติการตามพระราชบัญญัตินี้

ประกาศนั้น เมื่อได้ประกาศในราชกิจจานุเบกษาแล้วให้ใช้บังคับได้

หมวด ๑
คณะกรรมการ

ส่วนที่ ๑

คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

มาตรา ๕ ให้มีคณะกรรมการคณะหนึ่งเรียกว่า “คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ” เรียกโดยย่อว่า “กมช.” และให้ใช้ชื่อเป็นภาษาอังกฤษว่า “National Cyber Security Committee” เรียกโดยย่อว่า “NCSC” ประกอบด้วย

(๑) นายกรัฐมนตรี เป็นประธานกรรมการ

(๒) กรรมการโดยตำแหน่ง ได้แก่ รัฐมนตรีว่าการกระทรวงกลาโหม รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ปลัดกระทรวงการคลัง ปลัดกระทรวงยุติธรรม ผู้บัญชาการตำรวจแห่งชาติ และเลขาธิการสภาความมั่นคงแห่งชาติ

(๓) กรรมการผู้ทรงคุณวุฒิ จำนวนไม่เกินเจ็ดคน ซึ่งคณะรัฐมนตรีแต่งตั้งจากผู้มีความรู้ความเชี่ยวชาญ และประสบการณ์เป็นที่ประจักษ์ในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ด้านเทคโนโลยีสารสนเทศและการสื่อสาร ด้านการคุ้มครองข้อมูลส่วนบุคคล ด้านวิทยาศาสตร์ ด้านวิศวกรรมศาสตร์ ด้านกฎหมาย ด้านการเงิน หรือด้านอื่นที่เกี่ยวข้อง และเป็นประโยชน์ต่อการรักษาความมั่นคงปลอดภัยไซเบอร์

ให้เลขาธิการเป็นกรรมการและเลขานุการ และให้เลขาธิการแต่งตั้งพนักงานของสำนักงานเป็นผู้ช่วยเลขานุการได้ไม่เกินสองคน

หลักเกณฑ์และวิธีการสรรหาบุคคลเพื่อเสนอคณะรัฐมนตรีแต่งตั้งเป็นกรรมการผู้ทรงคุณวุฒิ รวมทั้งการสรรหากรรมการผู้ทรงคุณวุฒิเพื่อดำรงตำแหน่งแทนผู้ที่พ้นจากตำแหน่งก่อนวาระตามมาตรา ๗ วรรคสอง ให้เป็นไปตามระเบียบที่คณะรัฐมนตรีกำหนดโดยการเสนอแนะของคณะกรรมการ

มาตรา ๖ กรรมการผู้ทรงคุณวุฒิในคณะกรรมการต้องมีสัญชาติไทยและไม่มีลักษณะต้องห้าม ดังต่อไปนี้

(๑) เป็นบุคคลล้มละลายหรือเคยเป็นบุคคลล้มละลายทุจริต

(๒) เป็นคนไร้ความสามารถหรือคนเสมือนไร้ความสามารถ

(๓) เคยต้องคำพิพากษาถึงที่สุดให้จำคุกไม่ว่าจะได้รับโทษจำคุกจริงหรือไม่ เว้นแต่เป็นโทษสำหรับความผิดที่ได้กระทำโดยประมาทหรือความผิดลหุโทษ

(๔) เคยถูกไล่ออก ปลดออก หรือให้ออกจากราชการ หรือออกจากงานจากหน่วยงานที่เคยปฏิบัติหน้าที่ เพราะทุจริตต่อหน้าที่หรือประพฤติชั่วอย่างร้ายแรง

(๕) เคยถูกถอดถอนออกจากตำแหน่งตามกฎหมาย

(๖) เป็นผู้ดำรงตำแหน่งทางการเมือง สมาชิกสภาท้องถิ่นหรือผู้บริหารท้องถิ่น กรรมการหรือผู้ดำรงตำแหน่งซึ่งรับผิดชอบการบริหารพรรคการเมือง ที่ปรึกษาพรรคการเมือง หรือเจ้าหน้าที่ของพรรคการเมือง

มาตรา ๗ กรรมการผู้ทรงคุณวุฒิในคณะกรรมการมีวาระการดำรงตำแหน่งคราวละสี่ปี และอาจได้รับแต่งตั้งอีกได้ แต่จะดำรงตำแหน่งเกินสองวาระไม่ได้

ในกรณีที่มีการแต่งตั้งกรรมการผู้ทรงคุณวุฒิเพิ่มเติมหรือแทนกรรมการผู้ทรงคุณวุฒิซึ่งพ้นจากตำแหน่งก่อนวาระ ให้ผู้ได้รับแต่งตั้งเป็นกรรมการผู้ทรงคุณวุฒิเพิ่มเติมหรือแทนตำแหน่งที่ว่างนั้นดำรงตำแหน่งได้เท่ากับวาระที่เหลืออยู่ของกรรมการผู้ทรงคุณวุฒิซึ่งได้แต่งตั้งไว้แล้ว เว้นแต่วาระที่เหลืออยู่ไม่ถึงเก้าสิบวันจะไม่แต่งตั้งกรรมการผู้ทรงคุณวุฒิแทนก็ได้

เมื่อครบกำหนดวาระตามวรรคหนึ่ง หากยังมิได้แต่งตั้งกรรมการผู้ทรงคุณวุฒิขึ้นใหม่ ให้กรรมการผู้ทรงคุณวุฒิซึ่งพ้นจากตำแหน่งตามวาระนั้นอยู่ในตำแหน่งเพื่อดำเนินงานต่อไปจนกว่าจะได้มีการแต่งตั้งกรรมการผู้ทรงคุณวุฒิขึ้นใหม่

มาตรา ๘ นอกจากการพ้นจากตำแหน่งตามวาระตามมาตรา ๗ กรรมการผู้ทรงคุณวุฒิพ้นจากตำแหน่ง เมื่อ

(๑) ตาย

(๒) ลาออก

(๓) คณะรัฐมนตรีให้ออก

(๔) ขาดคุณสมบัติหรือมีลักษณะต้องห้ามตามมาตรา ๖

มาตรา ๙ คณะกรรมการมีหน้าที่และอำนาจ ดังต่อไปนี้

(๑) เสนอนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ ส่งเสริมและสนับสนุนการดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ตามมาตรา ๔๒ และมาตรา ๔๓ ต่อคณะรัฐมนตรีเพื่อให้ความเห็นชอบ ซึ่งต้องเป็นไปตามแนวทางที่กำหนดไว้ในมาตรา ๔๒

(๒) กำหนดนโยบายการบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(๓) จัดทำแผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์เสนอต่อคณะรัฐมนตรี สำหรับเป็นแผนแม่บทในการรักษาความมั่นคงปลอดภัยไซเบอร์ในสถานการณ์ปกติและในสถานการณ์ที่อาจจะเกิดหรือเกิดภัยคุกคามทางไซเบอร์ โดยแผนดังกล่าวจะต้องสอดคล้องกับนโยบาย ยุทธศาสตร์และแผนระดับชาติและกรอบนโยบายและแผนแม่บทที่เกี่ยวกับการรักษาความมั่นคงของสภาความมั่นคงแห่งชาติ

(๔) กำหนดมาตรฐานและแนวทางส่งเสริมพัฒนาระบบการให้บริการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ สร้างมาตรฐานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ และกำหนดมาตรฐานขั้นต่ำที่เกี่ยวข้องกับคอมพิวเตอร์ ระบบคอมพิวเตอร์ โปรแกรมคอมพิวเตอร์ รวมถึงส่งเสริมการรับรองมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานเอกชน

(๕) กำหนดมาตรการและแนวทางในการยกระดับทักษะความรู้และความเชี่ยวชาญในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของพนักงานเจ้าหน้าที่ เจ้าหน้าที่ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานเอกชนที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์

(๖) กำหนดกรอบการประสานความร่วมมือกับหน่วยงานอื่นทั้งในประเทศและต่างประเทศที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์

(๗) แต่งตั้งและถอดถอนเลขาธิการ

(๘) มอบหมายการควบคุมและกำกับดูแล รวมถึงการออกข้อกำหนด วัตถุประสงค์ หน้าที่และอำนาจ และกรอบการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานของรัฐ หรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(๙) ติดตามและประเมินผลการปฏิบัติตามนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ แผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์และการรักษาความมั่นคงปลอดภัยไซเบอร์ตามที่บัญญัติไว้ในพระราชบัญญัตินี้

(๑๐) เสนอแนะและให้ความเห็นต่อคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติหรือคณะรัฐมนตรี เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์

(๑๑) เสนอแนะต่อคณะรัฐมนตรีในการจัดให้มีหรือปรับปรุงกฎหมายที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์

(๑๒) จัดทำรายงานสรุปผลการดำเนินงานของการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีผลกระทบอย่างมีนัยสำคัญหรือแนวทางการพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ให้คณะรัฐมนตรีทราบ

(๑๓) ปฏิบัติการอื่นใดตามที่บัญญัติไว้ในพระราชบัญญัตินี้ หรือคณะรัฐมนตรีมอบหมาย

มาตรา ๑๐ การประชุมของคณะกรรมการ ให้เป็นไปตามระเบียบที่คณะกรรมการกำหนด โดยอาจประชุมด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นก็ได้

มาตรา ๑๑ ให้ประธานกรรมการ และกรรมการได้รับเบี้ยประชุมหรือค่าตอบแทนอื่นตามหลักเกณฑ์ที่คณะรัฐมนตรีกำหนด

ส่วนที่ ๒

คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์

มาตรา ๑๒ ในการดำเนินการตามหน้าที่และอำนาจของคณะกรรมการตามมาตรา ๙ ให้มีคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรียกโดยย่อว่า “กกม.” ประกอบด้วย

(๑) รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เป็นประธานกรรมการ

(๒) กรรมการโดยตำแหน่ง ได้แก่ ปลัดกระทรวงการต่างประเทศ ปลัดกระทรวงคมนาคม ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ปลัดกระทรวงพลังงาน ปลัดกระทรวงมหาดไทย ปลัดกระทรวงสาธารณสุข ผู้บัญชาการตำรวจแห่งชาติ ผู้บัญชาการทหารสูงสุด เลขาธิการสภาความมั่นคงแห่งชาติ ผู้อำนวยการสำนักข่าวกรองแห่งชาติ ผู้ว่าการธนาคารแห่งประเทศไทย เลขาธิการสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ และเลขาธิการคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ

(๓) กรรมการผู้ทรงคุณวุฒิ จำนวนไม่เกินสี่คน ซึ่งคณะกรรมการแต่งตั้งจากผู้มีความรู้ความเชี่ยวชาญ และประสบการณ์เป็นที่ประจักษ์และเป็นประโยชน์ต่อการรักษาความมั่นคงปลอดภัยไซเบอร์

ให้เลขาธิการเป็นกรรมการและเลขานุการ และให้เลขาธิการแต่งตั้งพนักงานของสำนักงานเป็นผู้ช่วยเลขานุการได้ไม่เกินสองคน

หลักเกณฑ์และวิธีการสรรหาบุคคลที่เห็นสมควรเพื่อพิจารณาแต่งตั้งเป็นกรรมการผู้ทรงคุณวุฒิให้เป็นไปตามระเบียบที่คณะกรรมการกำหนด

มาตรา ๑๓ กกม. มีหน้าที่และอำนาจ ดังต่อไปนี้

(๑) ติดตามการดำเนินการตามนโยบายและแผนตามมาตรา ๙ (๑) และมาตรา ๔๒

(๒) ดูแลและดำเนินการเพื่อรับมือกับภัยคุกคามทางไซเบอร์ในระดับร้ายแรง ตามมาตรา ๖๑ มาตรา ๖๒ มาตรา ๖๓ มาตรา ๖๔ มาตรา ๖๕ และมาตรา ๖๖

(๓) กำกับดูแลการดำเนินงานของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ และการเผชิญเหตุและนิติวิทยาศาสตร์ทางคอมพิวเตอร์

(๔) กำหนดประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อันเป็นข้อกำหนดขั้นต่ำในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมทั้งกำหนดมาตรการในการประเมินความเสี่ยง การตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ เมื่อมีภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่ส่งผลกระทบหรืออาจก่อให้เกิดผลกระทบหรือความเสียหายอย่างมีนัยสำคัญหรืออย่างร้ายแรงต่อระบบสารสนเทศของประเทศ เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ปฏิบัติได้อย่างรวดเร็ว มีประสิทธิภาพ และเป็นไปในทิศทางเดียวกัน

(๕) กำหนดหน้าที่ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน้าที่ของหน่วยงานควบคุมหรือกำกับดูแล โดยอย่างน้อยต้องกำหนดหน้าที่ให้หน่วยงานควบคุมหรือกำกับดูแลต้องกำหนดมาตรฐานที่เหมาะสมเพื่อรับมือกับภัยคุกคามทางไซเบอร์ของแต่ละหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน่วยงานของรัฐ

(๖) กำหนดระดับของภัยคุกคามทางไซเบอร์ พร้อมทั้งรายละเอียดของมาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์ในแต่ละระดับเสนอต่อคณะกรรมการ

(๗) วิเคราะห์สถานการณ์ และประเมินผลกระทบจากภัยคุกคามทางไซเบอร์ เพื่อเสนอต่อคณะกรรมการพิจารณาสั่งการ เมื่อมีหรือคาดว่าจะมีภัยคุกคามทางไซเบอร์ในระดับร้ายแรงขึ้น

ในการกำหนดกรอบมาตรฐานตามวรรคหนึ่ง (๔) ให้คำนึงถึงหลักการบริหารความเสี่ยงโดยอย่างน้อยต้องประกอบด้วยวิธีการและมาตรการ ดังต่อไปนี้

(๑) การระบุความเสี่ยงที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล

(๒) มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น

(๓) มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์

(๔) มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์

(๕) มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์

มาตรา ๑๔ ในการดำเนินการตามมาตรา ๑๓ วรรคหนึ่ง (๒) เพื่อรับมือกับภัยคุกคามทางไซเบอร์ได้ทันท่วงที กกม. อาจมอบอำนาจให้รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ผู้บัญชาการทหารสูงสุด และกรรมการอื่นซึ่ง กกม. กำหนด ร่วมกันปฏิบัติการในเรื่องดังกล่าวได้ และจะกำหนดให้หน่วยงานควบคุมหรือกำกับดูแลและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่ถูกคุกคามเข้าร่วมดำเนินการ ประสานงาน และให้การสนับสนุนด้วยก็ได้

การปฏิบัติตามวรรคหนึ่ง ให้เป็นไปตามระเบียบที่ กกม. กำหนด

มาตรา ๑๕ ให้นำความในมาตรา ๖ มาตรา ๗ และมาตรา ๘ มาใช้บังคับกับกรรมการผู้ทรงคุณวุฒิใน กกม. โดยอนุโลม

มาตรา ๑๖ ให้ กกม. มีอำนาจแต่งตั้งคณะอนุกรรมการเพื่อปฏิบัติการอย่างใดอย่างหนึ่งตามที่ กกม. มอบหมาย

มาตรา ๑๗ การประชุมของ กกม. และคณะอนุกรรมการ ให้เป็นไปตามระเบียบที่ กกม. กำหนด โดยอาจประชุมด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นก็ได้

มาตรา ๑๘ ให้ประธานกรรมการและกรรมการ ประธานอนุกรรมการและอนุกรรมการที่ กกม. แต่งตั้ง ได้รับเบี้ยประชุมหรือค่าตอบแทนอื่นตามหลักเกณฑ์ที่คณะรัฐมนตรีกำหนด

มาตรา ๑๙ ในการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ พนักงานเจ้าหน้าที่ต้องแสดงบัตรประจำตัวต่อบุคคลที่เกี่ยวข้อง

ในการแต่งตั้งพนักงานเจ้าหน้าที่ ให้รัฐมนตรีพิจารณาแต่งตั้งจากผู้มีความรู้ความชำนาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เป็นพนักงานเจ้าหน้าที่เพื่อปฏิบัติการอย่างหนึ่งอย่างใดตามพระราชบัญญัตินี้ ทั้งนี้ ระดับความรู้ความชำนาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของพนักงานเจ้าหน้าที่ ให้เป็นไปตามที่คณะกรรมการประกาศกำหนด

บัตรประจำตัวพนักงานเจ้าหน้าที่ให้เป็นไปตามแบบที่ กกม. ประกาศกำหนด

หมวด ๒
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

มาตรา ๒๐ ให้มีสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เป็นหน่วยงานของรัฐ มีฐานะเป็นนิติบุคคล และไม่เป็นส่วนราชการตามกฎหมายว่าด้วยระเบียบบริหารราชการแผ่นดิน หรือรัฐวิสาหกิจตามกฎหมายว่าด้วยวิธีการงบประมาณหรือกฎหมายอื่น

มาตรา ๒๑ กิจการของสำนักงานไม่อยู่ภายใต้บังคับแห่งกฎหมายว่าด้วยการคุ้มครองแรงงาน กฎหมายว่าด้วยแรงงานสัมพันธ์ กฎหมายว่าด้วยประกันสังคม และกฎหมายว่าด้วยเงินทดแทน แต่พนักงานและลูกจ้างของสำนักงานต้องได้รับประโยชน์ตอบแทนไม่น้อยกว่าที่กำหนดไว้ในกฎหมายว่าด้วยการคุ้มครองแรงงาน กฎหมายว่าด้วยประกันสังคม และกฎหมายว่าด้วยเงินทดแทน

มาตรา ๒๒ ให้สำนักงานรับผิดชอบงานธุรการ งานวิชาการ งานการประชุม และงานเลขานุการของคณะกรรมการ และ กกม. และให้มีหน้าที่และอำนาจดังต่อไปนี้ด้วย

(๑) เสนอแนะและสนับสนุนในการจัดทำนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ และแผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ตามมาตรา ๙ ต่อคณะกรรมการ

(๒) จัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามมาตรา ๑๓ วรรคหนึ่ง (๔) เสนอต่อ กกม. เพื่อให้ความเห็นชอบ

(๓) ประสานงานการดำเนินการเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามมาตรา ๕๓ และมาตรา ๕๔

(๔) ประสานงานและให้ความร่วมมือในการตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ในประเทศและต่างประเทศในส่วนที่เกี่ยวข้องกับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์และกำหนดมาตรการที่ใช้แก้ปัญหาเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์

(๕) ดำเนินการและประสานงานกับหน่วยงานของรัฐและเอกชนในการตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ตามที่ได้รับมอบหมายจากคณะกรรมการ

(๖) เฝ้าระวังความเสี่ยงในการเกิดภัยคุกคามทางไซเบอร์ ติดตาม วิเคราะห์และประมวลผลข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ และการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์

(๗) ปฏิบัติการ ประสานงาน สนับสนุน และให้ความช่วยเหลือ หน่วยงานที่เกี่ยวข้องในการปฏิบัติตามนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ แผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ และมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์หรือตามคำสั่งของคณะกรรมการ

(๘) ดำเนินการและให้ความร่วมมือหรือช่วยเหลือในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ โดยเฉพาะภัยคุกคามทางไซเบอร์ที่กระทบหรือเกิดแก่โครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(๙) เสริมสร้างความรู้ความเข้าใจเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมถึงการสร้างความตระหนักด้านสถานการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ร่วมกันเพื่อให้มีการดำเนินการเชิงปฏิบัติการที่มีลักษณะบูรณาการและเป็นปัจจุบัน

(๑๐) เป็นศูนย์กลางในการรวบรวมและวิเคราะห์ข้อมูลด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ รวมทั้งเผยแพร่ข้อมูลที่เกี่ยวข้องกับความเสี่ยงและเหตุการณ์ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้แก่หน่วยงานของรัฐและหน่วยงานเอกชน

(๑๑) เป็นศูนย์กลางในการประสานความร่วมมือระหว่างหน่วยงานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานของรัฐและหน่วยงานเอกชน ทั้งในประเทศและต่างประเทศ

(๑๒) ทำความตกลงและร่วมมือกับองค์การหรือหน่วยงานทั้งในประเทศและต่างประเทศในกิจการที่เกี่ยวกับการดำเนินการตามหน้าที่และอำนาจของสำนักงาน เมื่อได้รับความเห็นชอบจากคณะกรรมการ

(๑๓) ศึกษาและวิจัยข้อมูลที่จำเป็นสำหรับการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อจัดทำข้อเสนอแนะเกี่ยวกับมาตรการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมทั้งดำเนินการอบรมและฝึกซ้อมการรับมือกับภัยคุกคามทางไซเบอร์ให้แก่หน่วยงานที่เกี่ยวข้องเป็นประจำ

(๑๔) ส่งเสริม สนับสนุน และดำเนินการในการเผยแพร่ความรู้เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ ตลอดจนดำเนินการฝึกอบรมเพื่อยกระดับทักษะความเชี่ยวชาญในการปฏิบัติหน้าที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์

(๑๕) รายงานความคืบหน้าและสถานการณ์เกี่ยวกับการปฏิบัติตามพระราชบัญญัตินี้ รวมทั้งปัญหาและอุปสรรค เสนอต่อคณะกรรมการเพื่อพิจารณาดำเนินการ ทั้งนี้ ตามระยะเวลาที่คณะกรรมการกำหนด

(๑๖) ปฏิบัติงานอื่นใดอันเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศตามที่คณะกรรมการหรือคณะรัฐมนตรีมอบหมาย

เพื่อประโยชน์ในการดำเนินการตามหน้าที่และอำนาจตาม (๖) ให้สำนักงานจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติขึ้นเป็นหน่วยงานภายในสำนักงาน และให้มีหน้าที่และอำนาจตามที่คณะกรรมการกำหนด

มาตรา ๒๓ ในการดำเนินการของสำนักงาน นอกจากหน้าที่และอำนาจตามที่บัญญัติในมาตรา ๒๒ แล้ว ให้สำนักงานมีหน้าที่และอำนาจทั่วไปดังต่อไปนี้ด้วย

(๑) ถือกรรมสิทธิ์ มีสิทธิครอบครอง และมีทรัพยสิทธิต่าง ๆ

(๒) ก่อตั้งสิทธิ หรือทำนิติกรรมทุกประเภทผูกพันทรัพย์สิน ตลอดจนทำนิติกรรมอื่นใดเพื่อประโยชน์ในการดำเนินกิจการของสำนักงาน

(๓) จัดให้มีและให้ทุนเพื่อสนับสนุนการดำเนินกิจการของสำนักงาน

(๔) เรียกเก็บค่าธรรมเนียม ค่าบำรุง ค่าตอบแทน หรือค่าบริการในการดำเนินงาน ทั้งนี้ตามหลักเกณฑ์และอัตราที่สำนักงานกำหนดโดยความเห็นชอบของ กบส.

(๕) ปฏิบัติการอื่นใดที่กฎหมายกำหนดให้เป็นหน้าที่และอำนาจของสำนักงาน หรือตามที่คณะกรรมการ หรือ กบส. มอบหมาย

มาตรา ๒๔ ทุนและทรัพย์สินในการดำเนินงานของสำนักงาน ประกอบด้วย

(๑) ทุนประเดิมที่รัฐบาลจัดสรรให้ตามมาตรา ๘๑ วรรคหนึ่ง และเงินและทรัพย์สินที่ได้รับโอนมาตามมาตรา ๘๒

(๒) เงินอุดหนุนทั่วไปที่รัฐบาลจัดสรรให้ตามความเหมาะสมเป็นรายปี

(๓) เงินอุดหนุนจากหน่วยงานของรัฐทั้งในประเทศและต่างประเทศ หรือองค์การระหว่างประเทศระดับรัฐบาล

(๔) ค่าธรรมเนียม ค่าบำรุง ค่าตอบแทน ค่าบริการ หรือรายได้อันเกิดจากการดำเนินการตามหน้าที่และอำนาจของสำนักงาน

(๕) ดอกผลของเงินหรือรายได้จากทรัพย์สินของสำนักงาน

เงินและทรัพย์สินของสำนักงานตามวรรคหนึ่ง ต้องนำส่งคลังเป็นรายได้แผ่นดิน

มาตรา ๒๕ ให้มีคณะกรรมการบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ เรียกโดยย่อว่า “กบส.” เพื่อดูแลงานด้านกิจการบริหารงานทั่วไปของสำนักงาน ประกอบด้วย รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เป็นประธานกรรมการ ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม อธิบดีกรมบัญชีกลาง เลขาธิการ ก.พ. เลขาธิการ ก.พ.ร. และกรรมการผู้ทรงคุณวุฒิจำนวนไม่เกินหกคน เป็นกรรมการ

ให้เลขาธิการเป็นกรรมการและเลขานุการ และให้เลขาธิการแต่งตั้งพนักงานของสำนักงานเป็นผู้ช่วยเลขานุการได้ไม่เกินสองคน

กรรมการผู้ทรงคุณวุฒิตามวรรคหนึ่ง ให้รัฐมนตรีแต่งตั้งจากบุคคลซึ่งมีความรู้ ความเชี่ยวชาญและความสามารถเป็นที่ประจักษ์ในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ด้านเทคโนโลยีสารสนเทศและการสื่อสาร ด้านเศรษฐศาสตร์ ด้านสังคมศาสตร์ ด้านกฎหมาย ด้านบริหารธุรกิจ หรือด้านอื่นที่เกี่ยวข้อง และเป็นประโยชน์ต่อการดำเนินงานของ กบส. ตามหลักเกณฑ์และวิธีการที่คณะกรรมการกำหนด

ให้นำความในมาตรา ๖ และมาตรา ๘ มาใช้บังคับกับกรรมการผู้ทรงคุณวุฒิโดยอนุโลม

มาตรา ๒๖ ให้กรรมการผู้ทรงคุณวุฒิใน กบส. มีวาระการดำรงตำแหน่งคราวละสี่ปี

ในกรณีที่มีการแต่งตั้งกรรมการผู้ทรงคุณวุฒิเพิ่มเติมหรือแทนกรรมการผู้ทรงคุณวุฒิซึ่งพ้นจากตำแหน่งก่อนวาระ รัฐมนตรีอาจแต่งตั้งกรรมการผู้ทรงคุณวุฒิเพิ่มเติมหรือแทนตำแหน่งที่ว่างได้ และให้ผู้ได้รับแต่งตั้งเป็นกรรมการผู้ทรงคุณวุฒิเพิ่มเติมหรือแทนตำแหน่งที่ว่างนั้นดำรงตำแหน่งได้เท่ากับวาระที่เหลืออยู่ของกรรมการผู้ทรงคุณวุฒิซึ่งได้แต่งตั้งไว้แล้ว

เมื่อครบกำหนดวาระตามวรรคหนึ่ง หากยังมิได้แต่งตั้งกรรมการผู้ทรงคุณวุฒิขึ้นใหม่ ให้กรรมการผู้ทรงคุณวุฒิซึ่งพ้นจากตำแหน่งตามวาระนั้นอยู่ในตำแหน่งเพื่อดำเนินงานต่อไปจนกว่าจะได้มีการแต่งตั้งกรรมการผู้ทรงคุณวุฒิขึ้นใหม่

มาตรา ๒๗ ให้ กบส. มีหน้าที่และอำนาจ ดังต่อไปนี้

(๑) กำหนดนโยบายการบริหารงาน และให้ความเห็นชอบแผนการดำเนินงานของสำนักงาน

(๒) ออกข้อบังคับว่าด้วยการจัดองค์กร การเงิน การบริหารงานบุคคล การบริหารงานทั่วไป การพัสดุ การตรวจสอบภายใน รวมตลอดทั้งการสงเคราะห์และสวัสดิการต่าง ๆ ของสำนักงาน

(๓) อนุมัติแผนการใช้จ่ายเงินและงบประมาณรายจ่ายประจำปีของสำนักงาน

(๔) ควบคุมการบริหารงานและการดำเนินการของสำนักงานและเลขาธิการ ให้เป็นไปตามพระราชบัญญัตินี้และกฎหมายอื่นที่เกี่ยวข้อง

(๕) วินิจฉัยคำสั่งทางปกครองของเลขาธิการในส่วนที่เกี่ยวกับการบริหารงานของสำนักงาน

(๖) ประเมินผลการดำเนินงานของสำนักงานและการปฏิบัติงานของเลขาธิการ

(๗) ปฏิบัติหน้าที่อื่นตามที่พระราชบัญญัตินี้หรือกฎหมายอื่นกำหนดให้เป็นหน้าที่และอำนาจของ กบส. หรือตามที่คณะกรรมการหรือคณะรัฐมนตรีมอบหมาย

ในการปฏิบัติงานตามวรรคหนึ่ง กบส. อาจแต่งตั้งคณะอนุกรรมการเพื่อพิจารณา เสนอแนะ หรือกระทำการอย่างหนึ่งอย่างใดตามที่ กบส. มอบหมายได้ ทั้งนี้ การปฏิบัติงานและการประชุมให้เป็นไปตามหลักเกณฑ์และวิธีการที่ กบส. กำหนด

กบส. อาจแต่งตั้งผู้ทรงคุณวุฒิซึ่งมีความเชี่ยวชาญในด้านที่เป็นประโยชน์ต่อการดำเนินงานของสำนักงานเป็นที่ปรึกษา กบส. ทั้งนี้ ตามหลักเกณฑ์และวิธีการที่คณะกรรมการกำหนด

มาตรา ๒๘ ให้ประธานกรรมการและกรรมการ ประธานอนุกรรมการและอนุกรรมการที่ กบส. แต่งตั้ง ได้รับเบี้ยประชุมและค่าตอบแทนอื่นตามหลักเกณฑ์ที่คณะกรรมการกำหนด

มาตรา ๒๙ ให้สำนักงานมีเลขาธิการคนหนึ่ง รับผิดชอบการปฏิบัติงานของสำนักงาน และเป็นผู้บังคับบัญชาพนักงานและลูกจ้างของสำนักงาน

มาตรา ๓๐ เลขาธิการต้องมีคุณสมบัติ ดังต่อไปนี้

(๑) มีสัญชาติไทย

(๒) มีอายุไม่ต่ำกว่าสามสิบห้าปี แต่ไม่เกินหกสิบปี

(๓) เป็นผู้มีความรู้ ความสามารถ และประสบการณ์ในด้านที่เกี่ยวกับภารกิจของสำนักงานและการบริหารจัดการ

มาตรา ๓๑ ผู้มีลักษณะอย่างใดอย่างหนึ่งดังต่อไปนี้ ต้องห้ามมิให้เป็นเลขาธิการ

(๑) เป็นบุคคลล้มละลายหรือเคยเป็นบุคคลล้มละลายทุจริต

(๒) เป็นคนไร้ความสามารถหรือคนเสมือนไร้ความสามารถ

(๓) เคยต้องคำพิพากษาถึงที่สุดให้จำคุกไม่ว่าจะได้รับโทษจำคุกจริงหรือไม่ เว้นแต่เป็นโทษสำหรับความผิดที่ได้กระทำโดยประมาทหรือความผิดลหุโทษ

(๔) เป็นข้าราชการ พนักงาน หรือลูกจ้าง ของส่วนราชการหรือรัฐวิสาหกิจหรือหน่วยงานอื่นของรัฐหรือของราชการส่วนท้องถิ่น

(๕) เป็นหรือเคยเป็นข้าราชการการเมือง ผู้ดำรงตำแหน่งทางการเมือง สมาชิกสภาท้องถิ่นหรือผู้บริหารท้องถิ่น เว้นแต่จะได้พ้นจากตำแหน่งมาแล้วไม่น้อยกว่าหนึ่งปี

(๖) เป็นหรือเคยเป็นกรรมการหรือผู้ดำรงตำแหน่งอื่นในพรรคการเมืองหรือเจ้าหน้าที่ของพรรคการเมือง เว้นแต่จะได้พ้นจากตำแหน่งมาแล้วไม่น้อยกว่าหนึ่งปี

(๗) เคยถูกไล่ออก ปลดออก หรือให้ออกจากราชการ หรือออกจากงานจากหน่วยงานที่เคยปฏิบัติหน้าที่ เพราะทุจริตต่อหน้าที่หรือประพฤติชั่วอย่างร้ายแรง หรือเคยถูกถอดถอนจากตำแหน่ง

(๘) เคยถูกให้ออกเพราะไม่ผ่านการประเมินผลการปฏิบัติงานตามมาตรา ๓๕ (๕)

มาตรา ๓๒ ให้คณะกรรมการเป็นผู้กำหนดอัตราเงินเดือนและค่าตอบแทนอื่นของเลขาธิการตามหลักเกณฑ์ที่คณะรัฐมนตรีกำหนด

มาตรา ๓๓ เลขาธิการมีวาระอยู่ในตำแหน่งคราวละสี่ปี

เลขาธิการซึ่งพ้นจากตำแหน่งตามวาระอาจได้รับแต่งตั้งอีกได้ แต่ต้องไม่เกินสองวาระ

มาตรา ๓๔ ในแต่ละปี ให้มีการประเมินผลการปฏิบัติงานของเลขาธิการ ทั้งนี้ ให้เป็นไปตามระยะเวลาและวิธีการที่คณะกรรมการกำหนด

มาตรา ๓๕ นอกจากการพ้นจากตำแหน่งตามวาระ เลขาธิการพ้นจากตำแหน่ง เมื่อ

(๑) ตาย

(๒) ลาออก

(๓) ขาดคุณสมบัติตามมาตรา ๓๐ หรือมีลักษณะต้องห้ามตามมาตรา ๓๑

(๔) คณะกรรมการมีมติให้ออก เพราะบกพร่องหรือทุจริตต่อหน้าที่ มีความประพฤติเสื่อมเสียหรือหย่อนความสามารถ

(๕) คณะกรรมการให้ออก เพราะไม่ผ่านการประเมินผลการปฏิบัติงาน

(๖) ออกตามกรณีที่กำหนดไว้ในสัญญาจ้างหรือข้อตกลงระหว่างคณะกรรมการกับเลขาธิการ

มาตรา ๓๖ ให้เลขาธิการภายใต้การควบคุมดูแลของคณะกรรมการ กกม. และ กบส. ต้องดำเนินการตามคำสั่งของคณะกรรมการ กกม. และ กบส. ภายใต้หน้าที่และอำนาจ ดังต่อไปนี้

(๑) บริหารงานของสำนักงานให้เกิดผลสัมฤทธิ์ตามภารกิจของสำนักงาน และตามนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ แผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ นโยบายของคณะรัฐมนตรีและคณะกรรมการ และข้อบังคับ นโยบาย มติ และประกาศของ กบส.

(๒) วางระเบียบภายใต้นโยบายของคณะกรรมการและ กกม. โดยไม่ขัดหรือแย้งกับกฎหมาย มติของคณะรัฐมนตรี และข้อบังคับ นโยบาย มติ และประกาศที่คณะกรรมการและ กกม. กำหนด

(๓) เป็นผู้บังคับบัญชาพนักงานและลูกจ้างของสำนักงาน และประเมินผลการปฏิบัติงานของพนักงานและลูกจ้างของสำนักงานตามข้อบังคับของ กบส. และระเบียบของสำนักงาน

(๔) แต่งตั้งรองเลขาธิการหรือผู้ช่วยเลขาธิการโดยความเห็นชอบของคณะกรรมการ เพื่อเป็นผู้ช่วยปฏิบัติงานของเลขาธิการตามที่เลขาธิการมอบหมาย

(๕) บรรจุ แต่งตั้ง เลื่อน ลด ตัดเงินเดือนหรือค่าจ้าง ลงโทษทางวินัยพนักงานและลูกจ้างของสำนักงาน ตลอดจนให้พนักงานและลูกจ้างของสำนักงานออกจากตำแหน่ง ทั้งนี้ ตามข้อบังคับของ กบส. และระเบียบของสำนักงาน

(๖) ปฏิบัติการอื่นใดตามข้อบังคับ นโยบาย มติ หรือประกาศของ กบส. หรือ กกม.

ในกิจการของสำนักงานที่เกี่ยวกับบุคคลภายนอก ให้เลขาธิการเป็นผู้แทนของสำนักงาน ภายใต้ขอบเขตที่ได้รับการแต่งตั้งโดยคณะกรรมการ

เลขาธิการอาจมอบอำนาจให้บุคคลใดในสังกัดของสำนักงาน ปฏิบัติงานเฉพาะอย่างแทนก็ได้ ทั้งนี้ ตามข้อบังคับที่ กบส. กำหนด

ในกรณีที่ไม่มีเลขาธิการหรือเลขาธิการไม่อาจปฏิบัติหน้าที่ได้ ให้รองเลขาธิการที่มีอาวุโสตามลำดับรักษาการแทน ถ้าไม่มีรองเลขาธิการหรือรองเลขาธิการไม่อาจปฏิบัติหน้าที่ได้ ให้คณะกรรมการแต่งตั้งบุคคลที่เหมาะสมมารักษาการแทน

มาตรา ๓๗ การบัญชีของสำนักงานให้จัดทำตามแบบและหลักเกณฑ์ที่ กบส. กำหนด โดยให้คำนึงถึงหลักสากลและมาตรฐานการบัญชี

มาตรา ๓๘ ให้สำนักงานจัดทำงบการเงินและบัญชี แล้วส่งผู้สอบบัญชีภายในเก้าสิบวันนับแต่วันสิ้นปีบัญชี

ให้สำนักงานการตรวจเงินแผ่นดินหรือผู้สอบบัญชีรับอนุญาตที่สำนักงานการตรวจเงินแผ่นดินให้ความเห็นชอบเป็นผู้สอบบัญชีของสำนักงาน และประเมินผลการใช้จ่ายเงินและทรัพย์สินของสำนักงานทุกรอบปีแล้วทำรายงานผลการสอบบัญชีเสนอต่อ กบส. เพื่อรับรอง

มาตรา ๓๙ ให้สำนักงานจัดทำรายงานผลการดำเนินงานประจำปีเสนอคณะกรรมการและรัฐมนตรีภายในหนึ่งร้อยแปดสิบวันนับแต่วันสิ้นปีบัญชี และเผยแพร่รายงานนี้ต่อสาธารณชน

รายงานผลการดำเนินงานประจำปีตามวรรคหนึ่ง ให้แสดงรายละเอียดของงบการเงินที่ผู้สอบบัญชีให้ความเห็นแล้ว พร้อมทั้งผลงานของสำนักงานและรายงานการประเมินผลการดำเนินงานของสำนักงานในปีที่ล่วงมาแล้ว

การประเมินผลการดำเนินงานของสำนักงานตามวรรคสอง จะต้องดำเนินการโดยบุคคลภายนอกที่ กบส. ให้ความเห็นชอบ

มาตรา ๔๐ ให้รัฐมนตรีมีอำนาจกำกับดูแลโดยทั่วไปซึ่งกิจการของสำนักงานให้เป็นไปตามหน้าที่และอำนาจของสำนักงาน กฎหมาย แผนยุทธศาสตร์ชาติ นโยบายและแผนของรัฐบาล และมติคณะรัฐมนตรีที่เกี่ยวข้อง เพื่อการนี้ให้รัฐมนตรีมีอำนาจสั่งให้เลขาธิการชี้แจงข้อเท็จจริง แสดงความคิดเห็น หรือทำรายงานเสนอ และมีอำนาจสั่งยับยั้งการกระทำของสำนักงานที่ขัดต่อหน้าที่และอำนาจของสำนักงาน กฎหมาย แผนยุทธศาสตร์ชาติ นโยบายและแผนของรัฐบาล หรือมติคณะรัฐมนตรีที่เกี่ยวข้อง ตลอดจนสั่งสอบสวนข้อเท็จจริงเกี่ยวกับการดำเนินการของสำนักงานได้

หมวด ๓
การรักษาความมั่นคงปลอดภัยไซเบอร์

ส่วนที่ ๑
นโยบายและแผน

มาตรา ๔๑ การรักษาความมั่นคงปลอดภัยไซเบอร์ต้องคำนึงถึงความเป็นเอกภาพและการบูรณาการในการดำเนินงานของหน่วยงานของรัฐและหน่วยงานเอกชน และต้องสอดคล้องกับนโยบายและแผนระดับชาติว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมตามกฎหมายว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม และนโยบายและแผนแม่บทที่เกี่ยวกับการรักษาความมั่นคงของสภาความมั่นคงแห่งชาติ

การดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ต้องมุ่งหมายเพื่อสร้างศักยภาพในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ โดยเฉพาะอย่างยิ่งในการปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ

มาตรา ๔๒ นโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ ต้องมีเป้าหมายและแนวทางอย่างน้อย ดังต่อไปนี้

(๑) การบูรณาการการจัดการในการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ

(๒) การสร้างมาตรการและกลไกเพื่อพัฒนาศักยภาพในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

(๓) การสร้างมาตรการในการปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ

(๔) การประสานความร่วมมือระหว่างภาครัฐ เอกชน และประสานความร่วมมือระหว่างประเทศเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์

(๕) การวิจัยและพัฒนาเทคโนโลยีและองค์ความรู้ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์

(๖) การพัฒนาบุคลากรและผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ทั้งภาครัฐและเอกชน

(๗) การสร้างความตระหนักและความรู้ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

(๘) การพัฒนาระเบียบและกฎหมายเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์

มาตรา ๔๓ ให้คณะกรรมการจัดทำนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ขึ้นตามแนวทางในมาตรา ๔๒ เพื่อเสนอคณะรัฐมนตรีให้ความเห็นชอบ โดยให้ประกาศในราชกิจจานุเบกษา และเมื่อได้ประกาศแล้ว ให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามที่กำหนดไว้ในแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ ดำเนินการให้เป็นไปตามนโยบายและแผนดังกล่าว

ในการจัดทำนโยบายและแผนตามวรรคหนึ่ง ให้สำนักงานจัดให้มีการรับฟังความเห็นหรือประชุมร่วมกับหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

มาตรา ๔๔ ให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเร็ว

ประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามวรรคหนึ่ง อย่างน้อยต้องประกอบด้วยเรื่อง ดังต่อไปนี้

(๑) แผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจประเมิน ผู้ตรวจสอบภายใน หรือผู้ตรวจสอบอิสระจากภายนอก อย่างน้อยปีละหนึ่งครั้ง

(๒) แผนการรับมือภัยคุกคามทางไซเบอร์

เพื่อประโยชน์ในการจัดทำประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามวรรคหนึ่ง ให้สำนักงานโดยความเห็นชอบของคณะกรรมการจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานสำหรับให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนำไปใช้เป็นแนวทางในการจัดทำหรือนำไปใช้เป็นประมวลแนวทางปฏิบัติของหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศของตน และในกรณีที่หน่วยงานดังกล่าวยังไม่มีหรือมีแต่ไม่ครบถ้วนหรือไม่สอดคล้องกับประมวลแนวทางปฏิบัติและกรอบมาตรฐาน ให้นำประมวลแนวทางปฏิบัติและกรอบมาตรฐานดังกล่าวไปใช้บังคับ

ส่วนที่ ๒
การบริหารจัดการ

มาตรา ๔๕ หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ มีหน้าที่ป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงาน และจะต้องดำเนินการให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามมาตรา ๑๓ วรรคหนึ่ง (๔) ด้วย

ในกรณีที่หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศไม่อาจดำเนินการหรือปฏิบัติตามวรรคหนึ่งได้ สำนักงานอาจให้ความช่วยเหลือด้านบุคลากรหรือเทคโนโลยีแก่หน่วยงานนั้นตามที่ร้องขอได้

มาตรา ๔๖ เพื่อประโยชน์ในการรักษาความมั่นคงปลอดภัยไซเบอร์ ให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ แจ้งรายชื่อเจ้าหน้าที่ระดับบริหารและระดับปฏิบัติการ เพื่อประสานงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ไปยังสำนักงาน

ในกรณีที่มีการเปลี่ยนแปลงเจ้าหน้าที่ตามวรรคหนึ่ง ให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ แจ้งให้สำนักงานทราบโดยเร็ว

มาตรา ๔๗ ในกรณีที่การปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ต้องอาศัยความรู้ ความเชี่ยวชาญ คณะกรรมการหรือ กกม. อาจมอบหมายให้เลขาธิการว่าจ้างผู้เชี่ยวชาญตามความเหมาะสมเฉพาะงานได้

ผู้เชี่ยวชาญตามวรรคหนึ่งต้องมีคุณสมบัติหรือประสบการณ์ที่เหมาะสมตามที่คณะกรรมการประกาศกำหนด

เลขาธิการต้องออกบัตรประจำตัวผู้เชี่ยวชาญให้แก่บุคคลที่ได้รับการแต่งตั้ง และในการปฏิบัติหน้าที่บุคคลดังกล่าวต้องแสดงบัตรประจำตัวในฐานะผู้เชี่ยวชาญ และเมื่อพ้นจากหน้าที่แล้วจะต้องคืนบัตรประจำตัวแก่สำนักงานโดยเร็ว

ส่วนที่ ๓
โครงสร้างพื้นฐานสำคัญทางสารสนเทศ

มาตรา ๔๘ โครงสร้างพื้นฐานสำคัญทางสารสนเทศเป็นกิจการที่มีความสำคัญต่อความมั่นคงของรัฐ ความมั่นคงทางทหาร ความมั่นคงทางเศรษฐกิจ และความสงบเรียบร้อยภายในประเทศ และเป็นหน้าที่ของสำนักงานในการสนับสนุนและให้ความช่วยเหลือในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ โดยเฉพาะภัยคุกคามทางไซเบอร์ที่กระทบหรือเกิดแก่โครงสร้างพื้นฐานสำคัญทางสารสนเทศ

มาตรา ๔๙ ให้คณะกรรมการมีอำนาจประกาศกำหนดลักษณะหน่วยงานที่มีภารกิจหรือให้บริการในด้านดังต่อไปนี้ เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(๑) ด้านความมั่นคงของรัฐ

(๒) ด้านบริการภาครัฐที่สำคัญ

(๓) ด้านการเงินการธนาคาร

(๔) ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม

(๕) ด้านการขนส่งและโลจิสติกส์

(๖) ด้านพลังงานและสาธารณูปโภค

(๗) ด้านสาธารณสุข

(๘) ด้านอื่นตามที่คณะกรรมการประกาศกำหนดเพิ่มเติม

การพิจารณาประกาศกำหนดภารกิจหรือบริการตามวรรคหนึ่ง ให้เป็นไปตามหลักเกณฑ์ที่คณะกรรมการกำหนด โดยประกาศในราชกิจจานุเบกษา ทั้งนี้ คณะกรรมการจะต้องพิจารณาทบทวนการประกาศกำหนดภารกิจหรือบริการดังกล่าวเป็นคราว ๆ ไปตามความเหมาะสม

มาตรา ๕๐ ให้คณะกรรมการมีอำนาจประกาศกำหนดลักษณะ หน้าที่และความรับผิดชอบของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามมาตรา ๔๙ เพื่อประสานงาน เฝ้าระวัง รับมือ และแก้ไขภัยคุกคามทางไซเบอร์ โดยจะกำหนดให้หน่วยงานของรัฐที่มีความพร้อมหรือหน่วยงานควบคุมหรือกำกับดูแลหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนั้น ๆ ทำหน้าที่ดังกล่าวให้แก่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามมาตรา ๔๙ ทั้งหมดหรือบางส่วนก็ได้

การพิจารณาประกาศกำหนดภารกิจหรือบริการของหน่วยงานตามวรรคหนึ่ง ให้เป็นไปตามหลักเกณฑ์ที่คณะกรรมการกำหนด โดยประกาศในราชกิจจานุเบกษา ทั้งนี้ คณะกรรมการจะต้องพิจารณาทบทวนการประกาศกำหนดภารกิจหรือบริการดังกล่าวเป็นคราว ๆ ไปตามความเหมาะสม

มาตรา ๕๑ กรณีมีข้อสงสัยหรือข้อโต้แย้งเกี่ยวกับลักษณะหน่วยงานที่มีภารกิจหรือให้บริการในด้านที่มีการประกาศกำหนดตามมาตรา ๔๙ หรือมาตรา ๕๐ ให้คณะกรรมการเป็นผู้วินิจฉัยชี้ขาด

มาตรา ๕๒ เพื่อประโยชน์ในการติดต่อประสานงาน ให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศแจ้งรายชื่อและข้อมูลการติดต่อของเจ้าของกรรมสิทธิ์ ผู้ครอบครองคอมพิวเตอร์ และผู้ดูแลระบบคอมพิวเตอร์ไปยังสำนักงาน หน่วยงานควบคุมหรือกำกับดูแลของตน และหน่วยงานตามมาตรา ๕๐ ภายในสามสิบวันนับแต่วันที่คณะกรรมการประกาศตามมาตรา ๔๙ วรรคสอง และมาตรา ๕๐ วรรคสอง หรือนับแต่วันที่คณะกรรมการมีคำวินิจฉัยตามมาตรา ๕๑ แล้วแต่กรณี โดยอย่างน้อยเจ้าของกรรมสิทธิ์ ผู้ครอบครองคอมพิวเตอร์ และผู้ดูแลระบบคอมพิวเตอร์ต้องเป็นบุคคลซึ่งรับผิดชอบในการบริหารงานของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนั้น

ในกรณีที่มีการเปลี่ยนแปลงเจ้าของกรรมสิทธิ์ ผู้ครอบครองคอมพิวเตอร์ และผู้ดูแลระบบคอมพิวเตอร์ตามวรรคหนึ่ง ให้แจ้งการเปลี่ยนแปลงไปยังหน่วยงานที่เกี่ยวข้องตามวรรคหนึ่งก่อนการเปลี่ยนแปลงล่วงหน้าไม่น้อยกว่าเจ็ดวัน เว้นแต่มีเหตุจำเป็นอันไม่อาจก้าวล่วงได้ให้แจ้งโดยเร็ว

มาตรา ๕๓ ในการดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ให้หน่วยงานควบคุมหรือกำกับดูแลตรวจสอบมาตรฐานขั้นต่ำเรื่องความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ภายใต้การกำกับควบคุมดูแลของตน หากพบว่าหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศใดไม่ได้มาตรฐาน ให้หน่วยงานควบคุม

หรือกำกับดูแลนั้นรีบแจ้งให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่ต่ำกว่ามาตรฐานแก้ไขให้ได้มาตรฐานโดยเร็ว หากหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนั้นยังคงเพิกเฉยไม่ดำเนินการหรือไม่ดำเนินการให้แล้วเสร็จภายในระยะเวลาที่หน่วยงานควบคุมหรือกำกับดูแลกำหนด ให้หน่วยงานควบคุมหรือกำกับดูแลส่งเรื่องให้ กกม. พิจารณาโดยไม่ชักช้า

เมื่อได้รับคำร้องเรียนตามวรรคหนึ่ง หาก กกม. พิจารณาแล้วเห็นว่า มีเหตุดังกล่าวและอาจทำให้เกิดภัยคุกคามทางไซเบอร์ ให้ กกม. ดำเนินการ ดังต่อไปนี้

(๑) กรณีเป็นหน่วยงานของรัฐ ให้แจ้งต่อผู้บริหารระดับสูงสุดของหน่วยงานเพื่อใช้อำนาจในทางบริหาร สั่งการไปยังหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนั้นเพื่อให้ดำเนินการแก้ไขจนได้มาตรฐานโดยเร็ว

(๒) กรณีเป็นหน่วยงานเอกชน ให้แจ้งไปยังผู้บริหารระดับสูงสุดของหน่วยงาน ผู้ครอบครองคอมพิวเตอร์ และผู้ดูแลระบบคอมพิวเตอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนั้นเพื่อให้ดำเนินการแก้ไขจนได้มาตรฐานโดยเร็ว

ให้เลขาธิการดำเนินการติดตามเพื่อให้เป็นไปตามความในวรรคสองด้วย

มาตรา ๕๔ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ต้องจัดให้มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยมีผู้ตรวจประเมิน รวมทั้งต้องจัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ ทั้งโดยผู้ตรวจสอบภายในหรือโดยผู้ตรวจสอบอิสระภายนอก อย่างน้อยปีละหนึ่งครั้ง

ให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดส่งผลสรุปรายงานการดำเนินการต่อสำนักงานภายในสามสิบวันนับแต่วันที่ดำเนินการแล้วเสร็จ

มาตรา ๕๕ ในกรณีที่ กกม. เห็นว่า การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ ตามมาตรา ๕๔ ไม่เป็นไปตามมาตรฐานตามรายงานของหน่วยงานควบคุมหรือกำกับดูแล ให้ กกม. มีคำสั่งให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนั้นดำเนินการประเมินความเสี่ยงใหม่เพื่อให้เป็นไปตามมาตรฐานหรือดำเนินการตรวจสอบในด้านอื่น ๆ ที่มีผลต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศได้

ในกรณีที่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนั้น ได้จัดให้มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์หรือการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ตามวรรคหนึ่งแล้ว แต่ กกม. เห็นว่ายังไม่เป็นไปตามมาตรฐาน ให้ กกม. ดำเนินการ ดังต่อไปนี้

(๑) กรณีเป็นหน่วยงานของรัฐ ให้แจ้งต่อผู้บริหารระดับสูงสุดของหน่วยงานเพื่อใช้อำนาจในทางบริหาร สั่งการไปยังหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนั้น เพื่อให้ดำเนินการแก้ไขจนได้มาตรฐานโดยเร็ว

(๒) กรณีเป็นหน่วยงานเอกชน ให้แจ้งไปยังผู้บริหารระดับสูงสุดของหน่วยงาน ผู้ครอบครองคอมพิวเตอร์ และผู้ดูแลระบบคอมพิวเตอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนั้น เพื่อให้ดำเนินการแก้ไขจนได้มาตรฐานโดยเร็ว

ให้เลขาธิการดำเนินการติดตามเพื่อให้เป็นไปตามความในวรรคสองด้วย

มาตรา ๕๖ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ต้องกำหนดให้มีกลไกหรือขั้นตอนเพื่อการเฝ้าระวังภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศของตน ตามมาตรฐานซึ่งกำหนดโดยหน่วยงานควบคุมหรือกำกับดูแล และตามประมวลแนวทางปฏิบัติ รวมถึงระบบมาตรการที่ใช้แก้ปัญหาเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ที่คณะกรรมการหรือ กกม. กำหนด และต้องเข้าร่วมการทดสอบสถานะความพร้อมในการรับมือกับภัยคุกคามทางไซเบอร์ที่สำนักงานจัดขึ้น

มาตรา ๕๗ เมื่อมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญต่อระบบของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รายงานต่อสำนักงานและหน่วยงานควบคุมหรือกำกับดูแล และปฏิบัติการรับมือกับภัยคุกคามทางไซเบอร์ตามที่กำหนดในส่วนที่ ๔ ทั้งนี้ กกม. อาจกำหนดหลักเกณฑ์และวิธีการการรายงานด้วยก็ได้

ส่วนที่ ๔
การรับมือกับภัยคุกคามทางไซเบอร์

มาตรา ๕๘ ในกรณีที่เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ต่อระบบสารสนเทศซึ่งอยู่ในความดูแลรับผิดชอบของหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศใด ให้หน่วยงานนั้นดำเนินการตรวจสอบข้อมูลที่เกี่ยวข้อง ข้อมูลคอมพิวเตอร์ และระบบคอมพิวเตอร์ของหน่วยงานนั้น รวมถึงพฤติการณ์แวดล้อมของตน เพื่อประเมินว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้นหรือไม่ หากผลการตรวจสอบปรากฏว่าเกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ขึ้น ให้ดำเนินการป้องกันรับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานนั้น และแจ้งไปยังสำนักงานและหน่วยงานควบคุมหรือกำกับดูแลของตนโดยเร็ว

ในกรณีที่หน่วยงานหรือบุคคลใดพบอุปสรรคหรือปัญหาในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ของตน หน่วยงานหรือบุคคลนั้นอาจร้องขอความช่วยเหลือไปยังสำนักงาน

มาตรา ๕๙ เมื่อปรากฏแก่หน่วยงานควบคุมหรือกำกับดูแล หรือเมื่อหน่วยงานควบคุมหรือกำกับดูแลได้รับแจ้งเหตุตามมาตรา ๕๘ ให้หน่วยงานควบคุมหรือกำกับดูแล ร่วมกับหน่วยงานตามมาตรา ๕๐ รวบรวมข้อมูล ตรวจสอบ วิเคราะห์สถานการณ์ และประเมินผลกระทบเกี่ยวกับภัยคุกคามทางไซเบอร์ และดำเนินการ ดังต่อไปนี้

(๑) สนับสนุนและให้ความช่วยเหลือแก่หน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ในการควบคุมหรือกำกับดูแลของตน และให้ความร่วมมือและประสานงานกับสำนักงาน ในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

(๒) แจ้งเตือนหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ในการควบคุมหรือกำกับดูแลของตน รวมทั้งหน่วยงานควบคุมหรือกำกับดูแลหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศอื่นที่เกี่ยวข้องโดยเร็ว

มาตรา ๖๐ การพิจารณาเพื่อใช้อำนาจในการป้องกันภัยคุกคามทางไซเบอร์ คณะกรรมการจะกำหนดลักษณะของภัยคุกคามทางไซเบอร์ โดยแบ่งออกเป็นสามระดับ ดังต่อไปนี้

(๑) ภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง หมายถึง ภัยคุกคามทางไซเบอร์ที่มีความเสี่ยงอย่างมีนัยสำคัญถึงระดับที่ทำให้ระบบคอมพิวเตอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศหรือการให้บริการของรัฐด้อยประสิทธิภาพลง

(๒) ภัยคุกคามทางไซเบอร์ในระดับร้ายแรง หมายถึง ภัยคุกคามที่มีลักษณะการเพิ่มขึ้นอย่างมีนัยสำคัญของการโจมตีระบบคอมพิวเตอร์ คอมพิวเตอร์ หรือข้อมูลคอมพิวเตอร์ โดยมุ่งหมายเพื่อโจมตีโครงสร้างพื้นฐานสำคัญของประเทศและการโจมตีดังกล่าวมีผลทำให้ระบบคอมพิวเตอร์หรือโครงสร้างสำคัญทางสารสนเทศที่เกี่ยวข้องกับการให้บริการของโครงสร้างพื้นฐานสำคัญของประเทศความมั่นคงของรัฐ ความสัมพันธ์ระหว่างประเทศ การป้องกันประเทศ เศรษฐกิจ การสาธารณสุข ความปลอดภัยสาธารณะ หรือความสงบเรียบร้อยของประชาชนเสียหาย จนไม่สามารถทำงานหรือให้บริการได้

(๓) ภัยคุกคามทางไซเบอร์ในระดับวิกฤติ หมายถึง ภัยคุกคามทางไซเบอร์ในระดับวิกฤติที่มีลักษณะ ดังต่อไปนี้

(ก) เป็นภัยคุกคามทางไซเบอร์ที่เกิดจากการโจมตีระบบคอมพิวเตอร์ คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ในระดับที่สูงขึ้นกว่าภัยคุกคามทางไซเบอร์ในระดับร้ายแรง โดยส่งผลกระทบรุนแรง

ต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศในลักษณะที่เป็นวงกว้าง จนทำให้การทำงานของหน่วยงานรัฐหรือการให้บริการของโครงสร้างพื้นฐานสำคัญของประเทศที่ให้กับประชาชนล้มเหลวทั้งระบบ จนรัฐไม่สามารถควบคุมการทำงานส่วนกลางของระบบคอมพิวเตอร์ของรัฐได้ หรือการใช้มาตรการเยียวยาตามปกติในการแก้ไขปัญหาภัยคุกคามไม่สามารถแก้ไขปัญหาได้และมีความเสี่ยงที่จะลุกลามไปยังโครงสร้างพื้นฐานสำคัญอื่น ๆ ของประเทศ ซึ่งอาจมีผลทำให้บุคคลจำนวนมากเสียชีวิตหรือระบบคอมพิวเตอร์ คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์จำนวนมากถูกทำลายเป็นวงกว้างในระดับประเทศ

(ข) เป็นภัยคุกคามทางไซเบอร์อันกระทบหรืออาจกระทบต่อความสงบเรียบร้อยของประชาชนหรือเป็นภัยต่อความมั่นคงของรัฐหรืออาจทำให้ประเทศหรือส่วนใดส่วนหนึ่งของประเทศตกอยู่ในภาวะคับขันหรือมีการกระทำความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา การรบหรือการสงคราม ซึ่งจำเป็นต้องมีมาตรการเร่งด่วนเพื่อรักษาไว้ซึ่งการปกครองระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุขตามรัฐธรรมนูญแห่งราชอาณาจักรไทย เอกราชและบูรณภาพแห่งอาณาเขต ผลประโยชน์ของชาติ การปฏิบัติตามกฎหมาย ความปลอดภัยของประชาชน การดำรงชีวิตโดยปกติสุขของประชาชน การคุ้มครองสิทธิเสรีภาพ ความสงบเรียบร้อยหรือประโยชน์ส่วนรวม หรือการป้องปัดหรือแก้ไขเยียวยาความเสียหายจากภัยพิบัติสาธารณะอันมีมาอย่างฉุกเฉินและร้ายแรง

ทั้งนี้ รายละเอียดของลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ ให้คณะกรรมการเป็นผู้ประกาศกำหนด

มาตรา ๖๑ เมื่อปรากฏแก่ กกม. ว่าเกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ในระดับร้ายแรงให้ กกม. ออกคำสั่งให้สำนักงานดำเนินการ ดังต่อไปนี้

(๑) รวบรวมข้อมูล หรือพยานเอกสาร พยานบุคคล พยานวัตถุที่เกี่ยวข้องเพื่อวิเคราะห์สถานการณ์ และประเมินผลกระทบจากภัยคุกคามทางไซเบอร์

(๒) สนับสนุน ให้ความช่วยเหลือ และเข้าร่วมในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้น

(๓) ดำเนินการป้องกันเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เกิดจากภัยคุกคามทางไซเบอร์ เสนอแนะหรือสั่งการให้ใช้ระบบที่ใช้แก้ปัญหาเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ รวมถึงการหาแนวทางตอบโต้หรือการแก้ไขปัญหาเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

(๔) สนับสนุน ให้สำนักงาน และหน่วยงานที่เกี่ยวข้องทั้งภาครัฐและเอกชน ให้ความช่วยเหลือและเข้าร่วมในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้น

(๕) แจ้งเตือนภัยคุกคามทางไซเบอร์ให้ทราบโดยทั่วกัน ทั้งนี้ ตามความจำเป็นและเหมาะสม โดยคำนึงถึงสถานการณ์ ความร้ายแรงและผลกระทบจากภัยคุกคามทางไซเบอร์นั้น

(๖) ให้ความสะดวกในการประสานงานระหว่างหน่วยงานของรัฐที่เกี่ยวข้องและหน่วยงานเอกชน เพื่อจัดการความเสี่ยงและเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

มาตรา ๖๒ ในการดำเนินการตามมาตรา ๖๑ เพื่อประโยชน์ในการวิเคราะห์สถานการณ์และประเมินผลกระทบจากภัยคุกคามทางไซเบอร์ ให้เลขาธิการสั่งให้พนักงานเจ้าหน้าที่ดำเนินการดังต่อไปนี้

(๑) มีหนังสือขอความร่วมมือจากบุคคลที่เกี่ยวข้องเพื่อมาให้ข้อมูลภายในระยะเวลาที่เหมาะสมและตามสถานที่ที่กำหนด หรือให้ข้อมูลเป็นหนังสือเกี่ยวกับภัยคุกคามทางไซเบอร์

(๒) มีหนังสือขอข้อมูล เอกสาร หรือสำเนาข้อมูลหรือเอกสารซึ่งอยู่ในความครอบครองของผู้อื่นอันเป็นประโยชน์แก่การดำเนินการ

(๓) สอบถามบุคคลผู้มีความรู้ความเข้าใจเกี่ยวกับข้อเท็จจริงและสถานการณ์ที่มีความเกี่ยวพันกับภัยคุกคามทางไซเบอร์

(๔) เข้าไปในอสังหาริมทรัพย์หรือสถานประกอบการที่เกี่ยวข้องหรือคาดว่ามีส่วนเกี่ยวข้องกับภัยคุกคามทางไซเบอร์ของบุคคลหรือหน่วยงานที่เกี่ยวข้อง โดยได้รับความยินยอมจากผู้ครอบครองสถานที่นั้น

ผู้ให้ข้อมูลตามวรรคหนึ่ง ซึ่งกระทำโดยสุจริตย่อมได้รับการคุ้มครองและไม่ถือว่าเป็นการละเมิดหรือผิดสัญญา

มาตรา ๖๓ ในกรณีที่มีความจำเป็นเพื่อการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ให้ กกม. มีคำสั่งให้หน่วยงานของรัฐให้ข้อมูล สนับสนุนบุคลากรในสังกัด หรือใช้เครื่องมือทางอิเล็กทรอนิกส์ที่อยู่ในความครอบครองที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์

กกม. ต้องดูแลมิให้มีการใช้ข้อมูลที่ได้มาตามวรรคหนึ่งในลักษณะที่อาจก่อให้เกิดความเสียหาย และให้ กกม. รับผิดชอบในค่าตอบแทนบุคลากร ค่าใช้จ่ายหรือความเสียหายที่เกิดขึ้นจากการใช้เครื่องมือทางอิเล็กทรอนิกส์ดังกล่าว

ให้นำความในวรรคหนึ่งและวรรคสองมาใช้บังคับในการร้องขอต่อเอกชนโดยความยินยอมของเอกชนนั้นด้วย

มาตรา ๖๔ ในกรณีที่เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ซึ่งอยู่ในระดับร้ายแรง ให้ กกม. ดำเนินการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์และดำเนินมาตรการที่จำเป็น

ในการดำเนินการตามวรรคหนึ่ง ให้ กกม. มีหนังสือถึงหน่วยงานของรัฐที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ให้กระทำการหรือระงับการดำเนินการใด ๆ เพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ได้อย่างเหมาะสมและมีประสิทธิภาพตามแนวทางที่ กกม. กำหนด รวมทั้งร่วมกันบูรณาการในการดำเนินการเพื่อควบคุม ระงับ หรือบรรเทาผลที่เกิดจากภัยคุกคามทางไซเบอร์นั้นได้อย่างทันท่วงที

ให้เลขาธิการรายงานการดำเนินการตามมาตรานี้ต่อ กกม. อย่างต่อเนื่อง และเมื่อภัยคุกคามทางไซเบอร์ดังกล่าวสิ้นสุดลง ให้รายงานผลการดำเนินการต่อ กกม. โดยเร็ว

มาตรา ๖๕ ในการรับมือและบรรเทาความเสียหายจากภัยคุกคามทางไซเบอร์ในระดับร้ายแรง กกม. มีอำนาจออกคำสั่งเฉพาะเท่าที่จำเป็นเพื่อป้องกันภัยคุกคามทางไซเบอร์ให้บุคคลผู้เป็นเจ้าของกรรมสิทธิ์ ผู้ครอบครอง ผู้ใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรือผู้ดูแลระบบคอมพิวเตอร์ซึ่งมีเหตุอันเชื่อได้ว่าเป็นผู้เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ หรือได้รับผลกระทบจากภัยคุกคามทางไซเบอร์ดำเนินการ ดังต่อไปนี้

(๑) เฝ้าระวังคอมพิวเตอร์หรือระบบคอมพิวเตอร์ในช่วงระยะเวลาใดระยะเวลาหนึ่ง

(๒) ตรวจสอบคอมพิวเตอร์หรือระบบคอมพิวเตอร์เพื่อหาข้อบกพร่องที่กระทบต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ วิเคราะห์สถานการณ์ และประเมินผลกระทบจากภัยคุกคามทางไซเบอร์

(๓) ดำเนินมาตรการแก้ไขภัยคุกคามทางไซเบอร์เพื่อจัดการข้อบกพร่องหรือกำจัดชุดคำสั่งไม่พึงประสงค์ หรือระงับบรรเทาภัยคุกคามทางไซเบอร์ที่ดำเนินการอยู่

(๔) รักษาสถานะของข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ด้วยวิธีการใด ๆ เพื่อดำเนินการทางนิติวิทยาศาสตร์ทางคอมพิวเตอร์

(๕) เข้าถึงข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ที่เกี่ยวข้องเฉพาะเท่าที่จำเป็น เพื่อป้องกันภัยคุกคามทางไซเบอร์

ในกรณีมีเหตุจำเป็นที่ต้องเข้าถึงข้อมูลตาม (๕) ให้ กกม. มอบหมายให้เลขาธิการยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งให้เจ้าของกรรมสิทธิ์ ผู้ครอบครอง ผู้ใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือผู้ดูแลระบบคอมพิวเตอร์ตามวรรคหนึ่งดำเนินการตามคำร้อง ทั้งนี้ คำร้องที่ยื่นต่อศาลต้องระบุเหตุอันควรเชื่อได้ว่าบุคคลใดบุคคลหนึ่งกำลังกระทำหรือจะกระทำการอย่างใดอย่างหนึ่งที่ก่อให้เกิดภัยคุกคามทางไซเบอร์ในระดับร้ายแรง ในการพิจารณาคำร้องให้ยื่นเป็นคำร้องไต่สวนคำร้องฉุกเฉินและให้ศาลพิจารณาไต่สวนโดยเร็ว

มาตรา ๖๖ ในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ในระดับร้ายแรง กกม. มีอำนาจปฏิบัติการหรือสั่งให้พนักงานเจ้าหน้าที่ปฏิบัติการเฉพาะเท่าที่จำเป็นเพื่อป้องกันภัยคุกคามทางไซเบอร์ในเรื่อง ดังต่อไปนี้

(๑) เข้าตรวจสอบสถานที่ โดยมีหนังสือแจ้งถึงเหตุอันสมควรไปยังเจ้าของหรือผู้ครอบครองสถานที่เพื่อเข้าตรวจสอบสถานที่นั้น หากมีเหตุอันควรเชื่อได้ว่ามีคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ หรือได้รับผลกระทบจากภัยคุกคามทางไซเบอร์

(๒) เข้าถึงข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ทำสำเนา หรือสกัดคัดกรองข้อมูลสารสนเทศหรือโปรแกรมคอมพิวเตอร์ ซึ่งมีเหตุอันควรเชื่อได้ว่าเกี่ยวข้องหรือได้รับผลกระทบจากภัยคุกคามทางไซเบอร์

(๓) ทดสอบการทำงานของคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีเหตุอันควรเชื่อได้ว่าเกี่ยวข้องหรือได้รับผลกระทบจากภัยคุกคามทางไซเบอร์ หรือถูกใช้เพื่อค้นหาข้อมูลใด ๆ ที่อยู่ภายในหรือใช้ประโยชน์จากคอมพิวเตอร์หรือระบบคอมพิวเตอร์นั้น

(๔) ยึดหรืออายัดคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรืออุปกรณ์ใด ๆ เฉพาะเท่าที่จำเป็น ซึ่งมีเหตุอันควรเชื่อได้ว่าเกี่ยวข้องกับภัยคุกคามทางไซเบอร์ เพื่อการตรวจสอบหรือวิเคราะห์ ทั้งนี้ ไม่เกินสามสิบวัน เมื่อครบกำหนดเวลาดังกล่าวให้ส่งคืนคอมพิวเตอร์หรืออุปกรณ์ใด ๆ แก่เจ้าของกรรมสิทธิ์หรือผู้ครอบครองโดยทันทีหลังจากเสร็จสิ้นการตรวจสอบหรือวิเคราะห์

ในการดำเนินการตาม (๒) (๓) และ (๔) ให้ กกม. ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งให้พนักงานเจ้าหน้าที่ดำเนินการตามคำร้อง ทั้งนี้ คำร้องต้องระบุเหตุอันควรเชื่อได้ว่าบุคคลใดบุคคลหนึ่งกำลังกระทำหรือจะกระทำการอย่างใดอย่างหนึ่งที่ก่อให้เกิดภัยคุกคามทางไซเบอร์ในระดับร้ายแรง ในการพิจารณาคำร้องให้ยื่นเป็นคำร้องไต่สวนคำร้องฉุกเฉินและให้ศาลพิจารณาไต่สวนโดยเร็ว

มาตรา ๖๗ ในกรณีที่เกิดภัยคุกคามทางไซเบอร์ในระดับวิกฤติ ให้เป็นหน้าที่และอำนาจของสภาความมั่นคงแห่งชาติ ในการดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ตามกฎหมายว่าด้วยสภาความมั่นคงแห่งชาติและกฎหมายอื่นที่เกี่ยวข้อง

มาตรา ๖๘ ในกรณีที่เป็นเหตุจำเป็นเร่งด่วน และเป็นภัยคุกคามทางไซเบอร์ในระดับวิกฤติ คณะกรรมการอาจมอบหมายให้เลขาธิการมีอำนาจดำเนินการได้ทันทีเท่าที่จำเป็นเพื่อป้องกันและเยียวยาความเสียหายก่อนล่วงหน้าได้โดยไม่ต้องยื่นคำร้องต่อศาล แต่หลังจากการดำเนินการดังกล่าว ให้แจ้งรายละเอียดการดำเนินการดังกล่าวต่อศาลที่มีเขตอำนาจทราบโดยเร็ว

ในกรณีร้ายแรงหรือวิกฤติเพื่อประโยชน์ในการป้องกัน ประเมินผล รับมือ ปราบปราม ระงับ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ให้เลขาธิการโดยความเห็นชอบของคณะกรรมการหรือ กกม. มีอำนาจขอข้อมูลที่เป็นปัจจุบันและต่อเนื่องจากผู้ที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ โดยผู้นั้นต้องให้ความร่วมมือและให้ความสะดวกแก่คณะกรรมการหรือ กกม. โดยเร็ว

มาตรา ๖๙ ผู้ที่ได้รับคำสั่งอันเกี่ยวกับการรับมือกับภัยคุกคามทางไซเบอร์อาจอุทธรณ์คำสั่งได้เฉพาะที่เป็นภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรงเท่านั้น

หมวด ๔
บทกำหนดโทษ

มาตรา ๗๐ ห้ามมิให้พนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้เปิดเผยหรือส่งมอบข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการ ที่ได้มาตามพระราชบัญญัตินี้ให้แก่บุคคลใด ผู้ใดฝ่าฝืนต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

ความในวรรคหนึ่งมิให้ใช้บังคับกับการกระทำเพื่อประโยชน์ในการดำเนินคดีกับผู้กระทำความผิดตามพระราชบัญญัตินี้หรือผู้กระทำความผิดตามกฎหมายอื่นหรือเพื่อประโยชน์ในการดำเนินคดีกับพนักงานเจ้าหน้าที่เกี่ยวกับการใช้อำนาจหน้าที่โดยมิชอบ

มาตรา ๗๑ พนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้ผู้ใดกระทำโดยประมาทเป็นเหตุให้ผู้อื่นล่วงรู้ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ ข้อมูลของผู้ใช้บริการหรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ที่ได้มาตามพระราชบัญญัตินี้ ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๗๒ ผู้ใดล่วงรู้ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ ข้อมูลของผู้ใช้บริการหรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ที่พนักงานเจ้าหน้าที่ได้มาตามพระราชบัญญัตินี้ และเปิดเผยข้อมูลนั้นต่อผู้หนึ่งผู้ใดโดยมิชอบ ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๗๓ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศใดไม่รายงานเหตุภัยคุกคามทางไซเบอร์ตามมาตรา ๕๗ โดยไม่มีเหตุอันสมควร ต้องระวางโทษปรับไม่เกินสองแสนบาท

มาตรา ๗๔ ผู้ใดไม่ปฏิบัติตามหนังสือเรียกของพนักงานเจ้าหน้าที่หรือไม่ส่งข้อมูลให้แก่พนักงานเจ้าหน้าที่ตามมาตรา ๖๒ (๑) หรือ (๒) โดยไม่มีเหตุอันสมควรแล้วแต่กรณี ต้องระวางโทษปรับไม่เกินหนึ่งแสนบาท

มาตรา ๗๕ ผู้ใดฝ่าฝืนหรือไม่ปฏิบัติตามคำสั่งของ กกม. ตามมาตรา ๖๕ (๑) และ (๒) โดยไม่มีเหตุอันสมควร ต้องระวางโทษปรับไม่เกินสามแสนบาท และปรับอีกไม่เกินวันละหนึ่งหมื่นบาทนับแต่วันที่ครบกำหนดระยะเวลาที่ กกม. ออกคำสั่งให้ปฏิบัติจนกว่าจะปฏิบัติให้ถูกต้อง

ผู้ใดฝ่าฝืนหรือไม่ปฏิบัติตามคำสั่งของ กกม. ตามมาตรา ๖๕ (๓) และ (๔) หรือไม่ปฏิบัติตามคำสั่งศาลตามมาตรา ๖๕ (๕) ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๗๖ ผู้ใดขัดขวาง หรือไม่ปฏิบัติตามคำสั่งของ กกม. หรือพนักงานเจ้าหน้าที่ซึ่งปฏิบัติการตามคำสั่งของ กกม. ตามมาตรา ๖๖ (๑) หรือไม่ปฏิบัติตามคำสั่งศาลตามมาตรา ๖๖ (๒) (๓) หรือ (๔) โดยไม่มีเหตุอันสมควร ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๗๗ ในกรณีที่ผู้กระทำความผิดตามพระราชบัญญัตินี้เป็นนิติบุคคล ถ้าการกระทำความผิดของนิติบุคคลนั้นเกิดจากการสั่งการหรือการกระทำของกรรมการหรือผู้จัดการ หรือบุคคลใดซึ่งรับผิดชอบในการดำเนินงานของนิติบุคคลนั้น หรือในกรณีที่บุคคลดังกล่าวมีหน้าที่ต้องสั่งการหรือกระทำการและละเว้นไม่สั่งการหรือไม่กระทำการจนเป็นเหตุให้นิติบุคคลนั้นกระทำความผิด ผู้นั้นต้องรับโทษตามที่บัญญัติไว้สำหรับความผิดนั้น ๆ ด้วย

บทเฉพาะกาล

มาตรา ๗๘ ในวาระเริ่มแรก ให้คณะกรรมการประกอบด้วยประธานกรรมการและกรรมการตามมาตรา ๕ (๑) (๒) และให้เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเป็นกรรมการและเลขานุการ เพื่อปฏิบัติหน้าที่เท่าที่จำเป็นไปพลางก่อน และให้ดำเนินการแต่งตั้งกรรมการผู้ทรงคุณวุฒิของคณะกรรมการตามมาตรา ๕ (๓) ให้แล้วเสร็จภายในเก้าสิบวันนับแต่วันที่พระราชบัญญัตินี้ใช้บังคับ

ในการแต่งตั้งกรรมการผู้ทรงคุณวุฒิตามวรรคหนึ่ง รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมอาจเสนอรายชื่อบุคคลต่อคณะรัฐมนตรีเพื่อพิจารณาแต่งตั้งเป็นกรรมการผู้ทรงคุณวุฒิดังกล่าวด้วยได้

มาตรา ๗๙ ให้ดำเนินการเพื่อให้มี กกม. และ กบส. ภายในเก้าสิบวันนับแต่วันที่ได้มีการแต่งตั้งกรรมการผู้ทรงคุณวุฒิของคณะกรรมการตามมาตรา ๗๘

ให้ดำเนินการแต่งตั้งเลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติตามพระราชบัญญัตินี้ให้แล้วเสร็จภายในเก้าสิบวันนับแต่วันที่จัดตั้งสำนักงานแล้วเสร็จตามมาตรา ๘๐

มาตรา ๘๐ ให้ดำเนินการจัดตั้งสำนักงานให้แล้วเสร็จเพื่อปฏิบัติงานตามพระราชบัญญัตินี้ภายในหนึ่งปีนับแต่วันที่พระราชบัญญัตินี้ใช้บังคับ

ในระหว่างที่การดำเนินการจัดตั้งสำนักงานยังไม่แล้วเสร็จ ให้สำนักงานปลัดกระทรวงกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมทำหน้าที่สำนักงานตามพระราชบัญญัตินี้ และให้ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมทำหน้าที่เลขาธิการจนกว่าจะมีการแต่งตั้งเลขาธิการตามมาตรา ๗๙ วรรคสอง

มาตรา ๘๑ ในวาระเริ่มแรก ให้คณะรัฐมนตรีจัดสรรทุนประเดิมให้แก่สำนักงานตามความจำเป็น

ให้รัฐมนตรีเสนอต่อคณะรัฐมนตรีเพื่อพิจารณาให้ข้าราชการ พนักงาน เจ้าหน้าที่ หรือผู้ปฏิบัติงานอื่นใดในหน่วยงานของรัฐ มาปฏิบัติงานที่สำนักงานเป็นการชั่วคราวภายในระยะเวลาที่คณะรัฐมนตรีกำหนด

ให้ถือว่าข้าราชการ พนักงาน เจ้าหน้าที่ หรือผู้ปฏิบัติงานอื่นใดในหน่วยงานของรัฐที่มาปฏิบัติงานในสำนักงานเป็นการชั่วคราวตามวรรคสองไม่ขาดจากสถานภาพเดิมและคงได้รับเงินเดือนหรือค่าจ้างแล้วแต่กรณี จากสังกัดเดิม ทั้งนี้ คณะกรรมการอาจกำหนดค่าตอบแทนพิเศษให้แก่ข้าราชการ พนักงาน เจ้าหน้าที่ หรือผู้ปฏิบัติงานอื่นใดในหน่วยงานของรัฐตามวรรคสอง ในระหว่างปฏิบัติงานในสำนักงานด้วยก็ได้

ภายในหนึ่งร้อยแปดสิบวันนับแต่วันที่จัดตั้งสำนักงานแล้วเสร็จ ให้สำนักงานดำเนินการคัดเลือกข้าราชการ พนักงาน เจ้าหน้าที่ หรือผู้ปฏิบัติงานอื่นใดในหน่วยงานของรัฐตามวรรคสองเพื่อบรรจุเป็นพนักงานของสำนักงานต่อไป

ข้าราชการ พนักงาน เจ้าหน้าที่ หรือผู้ปฏิบัติงานอื่นใดในหน่วยงานของรัฐผู้ใดได้รับการคัดเลือกและบรรจุตามวรรคสี่ ให้มีสิทธินับระยะเวลาทำงานที่เคยทำงานอยู่ในสังกัดเดิมต่อเนื่องรวมกับระยะเวลาทำงานในสำนักงานตามพระราชบัญญัตินี้

มาตรา ๘๒ เมื่อพระราชบัญญัตินี้ใช้บังคับ ให้รัฐมนตรีเสนอคณะรัฐมนตรีดำเนินการเพื่ออนุมัติให้มีการโอนบรรดาอำนาจหน้าที่ กิจการ ทรัพย์สิน สิทธิ หนี้ และงบประมาณของบรรดาภารกิจที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ของสำนักงานปลัดกระทรวง กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม และสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ ที่มีอยู่ในวันก่อนวันที่พระราชบัญญัตินี้ใช้บังคับ ไปเป็นของสำนักงานตามพระราชบัญญัตินี้

มาตรา ๘๓ การดำเนินการออกกฎกระทรวง ระเบียบ และประกาศ ตามพระราชบัญญัตินี้ให้ดำเนินการให้แล้วเสร็จภายในหนึ่งปีนับแต่วันที่พระราชบัญญัตินี้ใช้บังคับ หากไม่สามารถดำเนินการได้ให้รัฐมนตรีรายงานเหตุผลที่ไม่อาจดำเนินการได้ต่อคณะรัฐมนตรีเพื่อทราบ

ผู้รับสนองพระบรมราชโองการ
พลเอก ประยุทธ์ จันทร์โอชา
นายกรัฐมนตรี

หมายเหตุ :- เหตุผลในการประกาศใช้พระราชบัญญัติฉบับนี้ คือ โดยที่ในปัจจุบันการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ อินเทอร์เน็ต โครงข่ายโทรคมนาคม หรือการให้บริการโดยปกติของดาวเทียมมีความเสี่ยงจากภัยคุกคามทางไซเบอร์อันอาจกระทบต่อความมั่นคงของรัฐ และความสงบเรียบร้อยภายในประเทศ ดังนั้น เพื่อให้สามารถป้องกัน หรือรับมือกับภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงที สมควรกำหนดลักษณะของภารกิจหรือบริการที่มีความสำคัญเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศทั้งหน่วยงานของรัฐและหน่วยงานเอกชน ที่จะต้องมีการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ มิให้เกิดผลกระทบต่อความมั่นคงในด้านต่าง ๆ รวมทั้งให้มีหน่วยงานเพื่อรับผิดชอบในการดำเนินการประสานการปฏิบัติงานร่วมกันทั้งภาครัฐและเอกชน ไม่ว่าในสถานการณ์ทั่วไปหรือสถานการณ์อันเป็นภัยต่อความมั่นคงอย่างร้ายแรง ตลอดจนกำหนดให้มีแผนปฏิบัติการและมาตรการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างมีเอกภาพและต่อเนื่อง อันจะทำให้การป้องกันและการรับมือกับภัยคุกคามทางไซเบอร์เป็นไปอย่างมีประสิทธิภาพ จึงจำเป็นต้องตราพระราชบัญญัตินี้



ฉบับภาษาอังกฤษ
English Version

[Official Emblem of Royal Command]

Cybersecurity Act,
B.E. 2562 (2019)

His Majesty King Phra Poramenthra Ramathibodi Sisin Maha Vajiralongkorn Phra Vajira Klao Chao Yu Hua

Given on the 24th Day of May B.E. 2562;
Being the 4th Year of the Present Reign.

His Majesty King Phra Poramenthra Ramathibodi Sisin Maha Vajiralongkorn Phra Vajira Klao Chao Yu Hua is graciously pleased to proclaim that:

Whereas it is expedient to have an enabling act on the law concerning cybersecurity.

This Act contains certain provisions in relation to the restriction of rights and freedom of a person, which section 26 in conjunction with section 28, section 32, section 33, section 34, section 36, and section 37 of the Constitution of the Kingdom of Thailand so permit by virtue of the law.

The rationale and necessity to restrict the rights and freedom of a person in accordance with this Act are to efficiently protect cybersecurity and to establish preventive measures to protect, handle, and mitigate the risk of cyber incidents which affect the national security and public order. The enactment of this Act complies with the criteria prescribed under section 26 of the Constitution of the Kingdom of Thailand.

Be it, therefore, enacted by the King, by and with the advice and consent of the National Legislative Assembly acting as the parliament, as follows:

Section 1 This Act is called the " Cybersecurity Act, B.E. 2562 (2019)"

Section 2 This Act shall come into force on the day following the date of its publication in the *Government Gazette*.

Section 3 Under this Act,

"Cybersecurity" shall mean any established measures, procedures, or actions to prevent, response, and mitigate the risk of cyber incidents from both inside and outside the country which affect national security, economic security, martial security, and public order in the country;

"Cyber Threat" shall mean any action or unlawful undertaking by using the computer, computer system, or undesirable program with an intention to cause any harm to the computer system, computer data, or other relevant data, and be an imminent threat to damage or affect operation of the computer, computer system, or other relevant data;

“Cyber” shall include data and communication from the service providing or application of the computer networks, internet system, or telecommunication networks including the usual service provision of satellite and other similar network systems which are connected;

"Government Agency" shall mean the central government, regional governments, local governments, state enterprises, the legislative institution, the judicial institutions, independent institutions, public organizations, and other government agencies;

"Code of Practice" shall mean any regulations or rules determined by the Cybersecurity Regulating Committee;

"Cyber Incident" shall mean an incident caused by any action or unlawful undertaking committed through a computer or computer system which may damage or affect Cybersecurity or Cybersecurity of a computer, computer data, computer system, or other data related to the computer system;

"Cybersecurity Solution" shall mean the act of solving a Cybersecurity issue by using personnel, process, and technology through a computer, computer system, computer program, or any service related to a computer, to create confidence and enhance Cybersecurity of the computer, computer data, computer system, or other data related to the computer system;

"Critical Information Infrastructure" shall mean the computer or computer system that the Government Agency or private organization uses in their operations which relate to maintaining national security, public safety, national economic security, or infrastructures in the public interest;

"Organization of Critical Information Infrastructure" shall mean a Government Agency or private organization who has a mission of or provides a Critical Information Infrastructure service;

“Regulator” shall mean a Government Agency or private organization or a person that is appointed by law to have the duty and power to supervise or regulate the operations of a Government Agency or Organization of Critical Information Infrastructure;

"Committee" shall mean the National Cyber Security Committee;

"Competent Official" shall mean a person appointed by the Minister for the execution of this Act;

"Secretary-General" shall mean the secretary-general of the National Cyber Security Committee;

"Agency" shall mean the National Cyber Security Agency, which is the office of the National Cyber Security Committee;

“Minister” shall mean the Minister who is in charge and control of this Act.

Section 4 The Prime Minister shall be in charge and control of this Act and shall be authorized to issue notifications related hereto and appoint the Competent Official for execution of this Act.

Notifications, shall come into force upon its publication in the *Royal Thai Government Gazette.*

Chapter 1
Committee

Part 1
National Cyber Security Committee

Section 5 There shall be a committee named the "National Cyber Security Committee". The English name shall be "National Cyber Security Committee" abbreviated as "NCSC." The NCSC shall be comprised of:

(1) the Prime Minister as a chairperson;

(2) directors by position, comprising the Minister of Defence, Minister of Digital Economy and Society, Permanent Secretary of the Ministry of Finance, Permanent Secretary of the Ministry of Justice, Commissioner-General of the National Police Bureau, and Secretary-General of the National Security Council;

(3) honorary directors not exceeding seven persons, appointed by the Cabinet, who have knowledge, expertise, and remarkable experience in Cybersecurity, information

technology and communications, personal data protection, science, engineering, law, finance, or other relevant aspects which are beneficial to Cybersecurity.

The Secretary-General shall be a director and secretary, and the Secretary-General shall appoint assistant secretaries from the officials of the Agency not exceeding two persons.

The criteria and procedure for selecting the persons to be proposed to the Cabinet as honorary directors, including the selection of honorary directors to stay in the office in replacement of a person who vacated the office prior to the expiry of the term in accordance with section 7 paragraph two shall be in accordance with the rules as determined by the Cabinet as suggested by the Committee.

Section 6 Honorary directors in the Committee must have Thai nationality and shall not possess the following prohibited characteristics:

(1) being bankrupt or having been previously dishonestly bankrupt;
(2) be an incompetent or quasi-incompetent person;
(3) having been previously imprisoned by final court judgement, regardless of whether there was actual punishment of imprisonment, except for offenses committed by negligence or misdemeanors;
(4) having been previously dismissed, fired, or removed from an official position or from any other previous organization on grounds of malpractice or severe gross misconduct;
(5) having been previously removed from an official position by way of the law;
(6) be a person holding a political position or serving as a local councilor, a local administer, a director or a person responsible for managing a political party, a counsel of a political party, or an officer of a political party.

Section 7 An honorary director in the Committee shall have a four-year term for each office, and may be reappointed, but shall not be in the office for more than two consecutive terms.

In case of the additional appointment of the honorary director or the replacement of the honorary director who has vacated the office prior to the expired term, the honorary director who has been additionally appointed or appointed in replacement of the vacant office shall stay in the office for the remaining period of the term of the appointed honorary director, unless the remaining term is less than ninety days, the honorary director may not be appointed.

When the term expires in accordance with paragraph one, if the new honorary director has yet to be appointed, the honorary director whose term has expired shall remain in the office to further perform the duties until a new honorary director is appointed.

Section 8 Apart from the expiration of term under section 7, an honorary director vacates office upon:

(1) death;
(2) resignation;
(3) being dismissed by an order of the Cabinet;
(4) lacking qualifications or possessing the prohibited characteristics as specified in section 6.

Section 9 The Committee shall have the following duties and powers to:

(1) propose the Policy and Plan on Cybersecurity, promote, and support the Cybersecurity Act in accordance with section 42 and section 43 for the Cabinet's approval, which shall be in accordance with the guideline specified under section 42;
(2) determine management policy for Cybersecurity for the Government Agencies and

Organizations of Critical Information Infrastructure;

(3) prepare the operational plan for Cybersecurity to propose to the Cabinet as a master plan for Cybersecurity under general situations and situations where the Cyber Incidents may occur or have occurred; such plan shall be in accordance with the policy, strategy, and national plan as well as the policy framework and master plan which are related to maintaining the security of the National Security Council;

(4) establish standards and guidelines for promoting the development of Cybersecurity service delivery systems, establish the Cybersecurity standards, and determine the Cybersecurity baselines pertaining to a computer, computer system, computer program, as well as promote the certification and accreditation of Cybersecurity standards for Organizations of Critical Information Infrastructure, Government Agencies, Regulators, and private organizations;

(5) prescribe measures and guidelines to enhance the knowledge and expertise in Cybersecurity of the Competent Officials, officers of Organizations of Critical Information Infrastructure, Government Agencies, Regulators, and private organizations which are related to Cybersecurity;

(6) set out a framework on coordinating with other Cybersecurity-related agencies, both in and outside the country;

(7) appoint and remove the Secretary-General;

(8) assign the supervision and regulation, including the issuing of regulations, objectives, duties and power, and the operational Cybersecurity framework to the Regulators, Government Agencies, or the Organizations of Critical Information Infrastructure.

(9) monitor and evaluate the results of operations in accordance with the Cybersecurity Policy and Plan, operational Cybersecurity plans, and Cybersecurity maintenance as specified under this Act;

(10) suggest and provide opinions to the Digital Economy and Society Committee or to the Cabinet on Cybersecurity;

(11) suggest to the Cabinet the legislation or amendment of laws related to Cybersecurity;

(12) prepare a summary report of Cybersecurity actions that have significant effect, or the approach for developing Cybersecurity standards for the Cabinet to be informed;

(13) perform any other task as specified under this Act or as assigned by the Cabinet.

Section 10 The meeting of the Committee shall be in accordance with the rules as determined by the Committee, possibly via electronic meeting or by other means.

Section 11 The chairperson and the directors shall receive a meeting allowance or other compensation in accordance with the rules determined by the Cabinet.

Part 2
Cybersecurity Regulating Committee

Section 12 In undertaking the duty and power of the Committee in accordance with section 9, there shall be a Cybersecurity Regulating Committee abbreviated as "CRC," comprising:

(1) the Minister of the Digital Economy and Society as a chairperson;

(2) directors by position, comprising the Permanent Secretary of the Ministry of Foreign Affairs, Permanent Secretary of the Ministry of Transport, Permanent Secretary of the Ministry of Digital Economy and Society, Permanent Secretary of the Ministry of Energy, Permanent Secretary of the Ministry of Interior, Permanent Secretary of

the Ministry of Public Health, Commissioner-General of the Royal Thai Police, Supreme Commander, Secretary-General of the National Security Council, Director of the National Intelligence Agency, Governor of the Bank of Thailand, Secretary-General of the Securities and Exchange Commission, and the Secretary-General of the National Broadcasting and Telecommunications Commission;

(3) honorary directors not exceeding four persons, who are appointed by the Committee among the persons who have knowledge, expertise, and experience which is remarkable and beneficial to maintain Cybersecurity.

The Secretary-General shall be a director and secretary, and the Secretary-General shall appoint assistant secretaries from the officials of the Agency not exceeding two persons.

The criteria and procedure for appointing the appropriate persons as honorary directors shall comply with the rules as determined by the Committee.

Section 13 The CRC shall have the following duties and powers:

(1) monitor the undertaking in accordance with the Policy and Plan according to section 9 (1) and section 42;

(2) supervise and take actions in order to response to Cyber Incidents at a critical level in accordance with section 61, section 62, section 63, section 64, section 65, and section 66;

(3) regulate the undertaking of Thailand Computer Emergency Response Team (ThaiCERT)and the incident responses and computer forensic science;

(4) determine the Codes of Practice and standard Cybersecurity frameworks which are the minimum requirements for Government Agencies and the Organizations of Critical Information Infrastructure, including determining the measure for risk assessment of, responding to, and coping with the occurring Cyber Incidents or any other incidents that affect or may significantly or severely affect or damage the information system of the country, for the quick, efficient, and united Cybersecurity operations;

(5) determine the duties of Organizations of Critical Information Infrastructure and duties of Regulators which should at least determine the duties for the Regulators to determine the appropriate standards for each Organization of Critical Information Infrastructure and Government Agency in handling Cyber Incidents;

(6) prescribe the level of Cyber Incidents including the detailed measures to prevent, respond, assess, eradicate, and contain Cyber Incidents at each level to present to the Committee;

(7) analyze the situation and evaluate the effect from Cyber Incidents, in order to propose course of actions to the Committee to consider issuing an order, in the case there exist or may exist Cyber Incidents in a more critical level.

In determining the standard framework according to paragraph one (4), the risk management principals shall be considered, which shall contain at least the approaches and measures as follows;

(1) identification of risks that may occur to the computer, computer data, computer system, other information related to computer system, asset, and a person’s life and body;

(2) measures for preventing potential risks;

(3) measures for monitoring and detecting Cyber Incidents;

(4) measures for responding to detected Cyber Incidents;

(5) measures for remedying and restoring the damage impacted by Cyber Incidents.

Section 14 In order to act in accordance with section 13 paragraph one (2) to handle Cyber Incidents in a timely manner, the CRC may assign the Minister of the Digital Economy and Society, Supreme Commander, and other directors as determined by the CRC to jointly perform such duty, and may determine that the Regulator(s) and the affected Organization(s) of Critical Information Infrastructure shall cooperate, coordinate, and provide support.

The performance under paragraph one shall be in accordance with the rules prescribed by the CRC.

Section 15 The provision of section 6, section 7, and section 8 shall be applied to the honorary directors in the CRC *mutatis mutandis*.

Section 16 The CRC shall have the power to appoint the sub-committee to perform any tasks as assigned by the CRC.

Section 17 The meeting of the CRC and the sub-committee shall be in accordance with the rules as determined by the CRC, via electronic meeting or by other means.

Section 18 The chairperson, the chairman of the sub-committee, and the sub-committee which the CRC appointed shall receive a meeting allowance or other compensation in accordance with the criteria determined by the Cabinet.

Section 19 In order to perform the duties in accordance with this Act, the Competent Official shall present his/her identification card to the relevant person.

In the appointment of the Competent Official, the Minister shall consider appointing a person with the knowledge and expertise in Cybersecurity to be the Competent Official to perform any tasks under this Act. The level of such knowledge and expertise of the Competent Official shall be in accordance with the notification(s) prescribed by the CRC.

The identification card issued to the Competent Official shall be in accordance with the notification(s) prescribed by the CRC.

Chapter 2
National Cyber Security Agency

Section 20 There shall be the National Cyber Security Agency (NCSA) as the Government Agency who is a juristic person and not a government sector entity under the Organization of State Administration Act nor a state enterprise under the Budgetary Procedures Act, or other laws.

Section 21 The operation of the Agency is not regulated by the labor protection law, labor relation law, social security law, and compensation fund law. However, officers and employees of the Agency shall receive compensation not less than that specified under the labor protection law, social security law, and compensation fund law.

Section 22 The Agency shall be responsible for administrative, academic, meeting, and secretarial tasks of the Committee and the CRC, and shall also have the duties and powers to:

(1) suggest and support preparation of the Policy and Plan on Cybersecurity and the operational plan for Cybersecurity in accordance with section 9 to the Committee;

(2) prepare the Codes of Practice and standard Cybersecurity frameworks in accordance with section 13 paragraph one (4) and submit the documents to the CRC for the

approval;

(3) coordinate Cybersecurity tasks to secure Organizations of Critical Information Infrastructure in accordance with section 53 and section 54;

(4) coordinate and cooperate in the establishment of Thailand Computer Emergency Response Team (ThaiCERT) in and outside the country with respect to Cybersecurity related events, and determine Cybersecurity corrective measures;

(5) act and coordinate with the Government Agencies and private organizations in order to respond and handle Cyber Incidents as assigned by the Committee;

(6) monitor the risk of occurrence of Cyber Incidents, follow, analyze, and process information in relation to the Cyber Incidents and alerts on the Cyber Incidents;

(7) perform, coordinate, support, and assist relevant agencies in complying with the Policy and Plan on Cybersecurity, the operational plan for Cybersecurity, and the Cybersecurity measures to prevent, response and mitigate the risks of Cyber Incidents or as ordered by the Committee;

(8) act and cooperate or assist in preventing, handling, and mitigating the risks of Cyber Incidents, especially those that affect or occur in relation to the Critical Information Infrastructure;

(9) strengthen the knowledge and understanding in Cybersecurity, including to raising collective awareness of Cybersecurity threat landscapes in order to have a practical operation in a manner that is integrated and up-to-date;

(10) act as central point of collection and analysis of data regarding Cybersecurity of the country, and disseminating the information related to Cybersecurity risks and Cyber Incidents to Government Agencies and private organizations;

(11) act as the central inter-agency coordinator regarding Cybersecurity among Government Agencies and private organizations, both in and outside the country;

(12) make agreements and cooperate with organizations or agencies both in and outside the country for the operations that fall within the duty and power of the Agency, upon receiving approval from the Committee;

(13) study and research necessary information required for Cybersecurity, in order to prepare recommendations on Cybersecurity measures, as well as regularly provide relevant agencies with training and practice for Cyber Incident handling;

(14) enhance, support, and act in order to disseminate Cybersecurity knowledge, and provide trainings to enhance the skills and expertise in performing Cybersecurity duties;

(15) report the progress and situation for the execution of this Act including the problems, obstacles, and propose to the Committee to consider actions to proceed within the period as prescribed by the Committee;

(16) perform any other Cybersecurity related tasks of the country as assigned by the Committee or the Cabinet.

For the benefit of acting according to the duties and powers in accordance with (6), the Agency shall establish the Thailand Computer Emergency Response Team (ThaiCERT) as an internal department of the Agency, which shall have duties and powers as determined by the Committee.

Section 23 In the operation of the Agency, aside from the duties and powers under section 22, the Agency shall have the following general duties and powers to:

(1) have the ownership, possession, and property rights;

(2) establish any rights or enter into any juristic acts that shall bind the properties as well as enter into any other juristic acts for the benefit of the operation of the Agency;

(3) prepare and provide funding in support of the operation of the Agency;
(4) collect fees, maintenance fees, compensation, or service fees for its operation, in accordance with the criteria and rate as determined by the Agency under the approval of the CMSA;
(5) perform any other tasks determined under law to be the duties and powers of the Agency, or as assigned by the Committee or the CMSA.

Section 24 The capital and assets for the operation of the Agency shall consist of:
(1) the initial funding assigned by the government under section 81 paragraph one and the money and assets transferred under section 82;
(2) general subsidiaries appropriately allocated by the government on an annual basis;
(3) general subsidiaries from Government Agencies both in and outside the country, or international government-level organizations;
(4) fees, maintenance fees, compensation, service fees, or income from performing duties and powers of the Agency;
(5) fruit from money or income from the assets of the Agency.

Money and assets of the Agency under paragraph one must be provided to the treasury as national revenue.

Section 25 There shall be the Committee Managing the National Cyber Security Agency, abbreviated as "CMSA", to supervise the general administration of the Agency, consisting of the Minister of the Digital Economy and Society as the chairperson, Permanent Secretary of the Ministry of Digital Economy and Society, Director General of the Controller General's Department, the Secretary-General of the Civil Service Commission, the Secretary-General of the Office of the Public Sector Development, and honorary directors not exceeding six persons to be directors.

The Secretary-General shall be a director and secretary, and the Secretary-General shall appoint assistant secretaries from the officials of the Agency not exceeding two persons.

The honorary directors under paragraph one shall be appointed by the Cabinet among the persons who have knowledge, expertise, and remarkable competency in Cybersecurity, information technology and communications, economics, social science, law, business management, or other relevant aspects which are beneficial to the operation of the CMSA in accordance with the criteria and procedures as determined by the Committee.

Section 6 and section 8 shall be applied *mutatis mutandis* to the honorary committees.

Section 26 The honorary directors of the CMSA shall have a four-year term for each office.

In case of the additional appointment of the honorary directors or the replacement of the honorary directors who has vacated the office prior to the expired term, the Minister may appoint the additional honorary directors or in replacement of the vacant office. An honorary director who has been additionally appointed or appointed in replacement of the vacant office shall stay in the office for the remaining period of the term of the appointed honorary director.

When a term expires in accordance with paragraph one, if the new honorary director has yet to be appointed, the honorary director whose term has expired shall remain in the office to further perform the duties until a new honorary director is appointed.

Section 27 The CMSA shall have the following duties and powers to:
(1) determine the management policy and approve the operational plan of the Agency;
(2) issue regulations regarding organizing, finance, human resources, general management, stock, internal audit, and other support and welfare of the Agency;

(3) approve the payment plan and annual expense budget of the Agency;
(4) control the management and operation of the Agency and Secretary-General in accordance with this Act and other relevant laws;
(5) analyze the administrative order of the Secretary-General in relation to the management of the Agency;
(6) evaluate the result of the operation of the Agency and the execution of the Secretary-General;
(7) perform any other task as specified under this Act or other relevant laws as duties and powers of the CMSA or as assigned by the Committee or the Cabinet.

In performing the duties under paragraph one, the CMSA may appoint a sub-committee to consider, suggest, or perform any act as assigned by the CMSA, with performance of such duties and meetings to be in accordance with the criteria and procedures determined by the CMSA.

The CMSA may appoint the honorary committee who has expertise in aspects beneficial to the operation of the Agency as a consultant of the CMSA under the criteria and procedures determined by the Committee.

Section 28 The chairperson and the director, the chairman of the sub-committee, and the sub-committee appointed by the CMSA shall receive a meeting allowance and other compensation in accordance with the rules determined by the Committee.

Section 29 The Agency shall have a Secretary-General responsible for the operation of the Agency and being a supervisor of the officers and employees of the Agency.

Section 30 A Secretary-General shall have the following qualifications:
(1) have Thai nationality;
(2) not be under 35 years of age but not over 60 years of age;
(3) have knowledge, competencies, and experience in fields related to the mission of the Agency and management skills.

Section 31 A person having any of the following characteristics shall be prohibited from being a Secretary-General:
(1) be a bankrupted person or used to be a dishonestly bankrupted person;
(2) be an incompetent or quasi-incompetent person;
(3) having been previously imprisoned by the final court judgement regardless the actual imprisonment unless the offences committed by negligence or misdemeanors;
(4) be a civil servant, officer, or employee of a government authority, state enterprise, or other Government Agencies or local governments;
(5) be or having been previously a political official, public office holder, local councilor, or local administer unless having vacated from the office for not less than one year;
(6) be or having been previously a director or a person in other positions in the political party, or an officer of the political party unless having vacated from the office for not less than one year;
(7) having been previously dismissed, fired, or removed from a government agency or an organization on grounds of dishonest performance of duties or gross misconduct, or removed from a position;
(8) having been previously removed on grounds of not passing a performance evaluation under section 35 (5).

Section 32 The Committee shall determine the salary and other compensation of a

Secretary-General in accordance with the method determined by the Cabinet.

Section 33 A Secretary-General shall have a four-year term for each office.

A Secretary-General who has vacated the office due to expiration of the term may be reappointed, but not exceeding two terms.

Section 34 Each year, there shall be a performance evaluation of a Secretary-General in accordance with the period and method determined by the Committee.

Section 35 Apart from the expiration of term, a Secretary-General vacates office upon:

(1) death;
(2) resignation;
(3) lacking qualifications as specified in section 30 or possessing prohibited characteristics as specified in section 31;
(4) resolution for removal passed by the Committee on grounds of deficiency or dishonest performance of duties, disgraceful behaviors, or incapacity;
(5) removal from the Committee due to failure to pass the performance evaluation;
(6) vacating in accordance with the terms specified under the employment agreement or agreement between the Committee and the Secretary-General.

Section 36 A Secretary-General under the supervision of the Committee, CRC, and CMSA shall comply with the orders of the Committee, CRC, and CMSA under the duties and powers as follows:

(1) manage the operation of the Agency to accomplish in accordance with the mission of the Agency, and with the Policy and Plan on Cybersecurity, the operational plan for Cybersecurity, the policies of the Cabinet and the Committee, and regulations, policies, resolutions and notifications of the CMSA;
(2) issue regulations under the policy of the Committee and CRC that are not contrary to the law, Cabinet resolutions, and the regulations, policies, resolutions, and notifications determined by the Committee and CRC;
(3) be a supervisor of the officers and employees of the Agency and evaluate the performances of officers and employees of the Agency in accordance with the regulations of the CMSA and the rules of the Agency;
(4) appoint the deputy Secretary-General or assistant of the Secretary-General as approved by the Committee to be an assistant in the operation of the Secretary-General as assigned by the Secretary-General;
(5) assign, appoint, promote, demote, deduct the salaries or wages of, execute disciplinary action against officers and employees of the Agency, and remove officers and employees of the Agency in accordance with the regulations determined by the CMSA and the rules of the Agency;
(6) perform any other task as specified under the regulations, policies, resolutions, or notifications of the CMSA or the CRC.

For the operation of the Agency in relation to outsourcing, the Secretary-General shall be the representative of the Agency, under the scope set forth by the Committee.

The Secretary-General may assign its power to any person under the Agency to perform a specific task under the regulations determined by the CMSA.

In case that there is no Secretary-General or the Secretary-General cannot perform his or her duties, the deputy Secretary-General in order of the seniority shall be in charge. If there is no

deputy Secretary-General or the deputy Secretary-General cannot execute the duties, the Committee shall appoint an appropriate person to do so.

Section 37 The accounts of the Agency shall be prepared in accordance with the forms and criteria determined by the CMSA, taking into account international principles and accounting standards.

Section 38 The Agency shall prepare and submit a financial statement and accounting report to an auditor within ninety days from end of the fiscal year.

The State Audit Office of the Kingdom of Thailand or certified public accountant(s) approved by the State Audit Office of the Kingdom of Thailand shall be the auditor of the Agency and appraise the results of expenses and assets of the Agency in each fiscal year, and shall prepare the result of the audit to be submitted to the CMSA for approval.

Section 39 The Agency shall prepare an annual report to be submitted to the Committee within one hundred and eighty days from the end of the fiscal year, and shall disclose the annual report to the public.

The annual report under paragraph one shall describe the details of balance sheets as approved by an auditor, the performance of the Agency, and the outcome of the performance evaluation of the Agency during the previous fiscal year.

The evaluation of the Agency under paragraph two shall be done by a third party who has been approved by the CMSA.

Section 40 The Minister shall to generally supervise the operation of the Agency in accordance with the duties and powers of the Agency, the laws, national strategies, policies and plans of the government, and relevant Cabinet resolutions. In the light of this, the Minister shall have the power to order the Secretary-General to clarify facts, comment, or prepare the report, and cease operations of the Agency that are against the duties and powers of the Agency, the laws, national strategies, policies and plans of the government, or the relevant Cabinet resolutions, including to order an investigation of the facts regarding operations of the Agency.

Chapter 3
Maintaining Cybersecurity

Part 1
The Policy and Plan

Section 41 Maintaining Cybersecurity shall take into consideration the unity and integration of the operation of Government Agencies and private organizations, and shall align with the national Policy and Plan regarding the digital development for economy and society in accordance with the laws regarding the digital development for economy and society, and the policy and master plan which are related to maintaining the security of the National Security Council.

The operation on Cybersecurity shall aim to create the capability to protect, cope with, and mitigate risks of Cyber Incidents, especially in protecting the Critical Information Infrastructure of the country.

Section 42 The Cybersecurity Policy and Plan shall at least contain the following objectives and approaches:

(1) integration of management in Cybersecurity of the country;
(2) establishment of measures and mechanisms to develop capability to protect, cope with, and mitigate the risks of Cyber Incidents;
(3) establishment of measures to protect the Critical Information Infrastructure of the country;
(4) national and international cooperation between the public and private sectors on Cybersecurity;
(5) research and development of technology and knowledge related to Cybersecurity;
(6) development of Cybersecurity personnel and experts, both in the public and the private sectors;
(7) creation of awareness and knowledge in Cybersecurity;
(8) development of rules and laws for Cybersecurity.

Section 43 The Committee shall prepare the Cybersecurity Policy and Plan in accordance with section 42 to propose to the Cabinet for approval, which shall be published in the *Royal Thai Government Gazette*. Once published, the Government Agencies, Regulators, and Organizations of Critical Information Infrastructure as prescribed in the Cybersecurity Policy and Plan shall act in accordance with the Cybersecurity Policy and Plan.

In preparing the Policy and Plan under paragraph one, the Agency shall hold a hearing or meeting with the Government Agencies, Regulators, and Organizations of Critical Information Infrastructure.

Section 44 Each of the Government Agencies, Regulators, and Organizations of Critical Information Infrastructure shall prepare its Code of Practice and a standard Cybersecurity framework in accordance with the Cybersecurity Policy and Plan without delay.

The Code of Practice under paragraph one, at least, shall consist of the following:
(1) Cybersecurity audit and risk assessment plans conducted by an assessor, an internal auditor, or an independent external auditor, at least once per year;
(2) a Cyber Incident response plan.

For the benefit of preparing the Code of Practice for Cybersecurity in paragraph one, the Agency, upon the approval of the Committee, shall develop a Code of Practice and standard framework for the Government Agencies, Regulators, or Organizations of Critical Information Infrastructure to be used as a guideline to prepare or exercise as their own Code of Practice. In case such agencies and organizations do not yet have or have but incomplete or incompliant with the Agency's Code of Practice and standard framework, such the Agency's Code of Practice and standard framework shall be enforced.

Part 2
Management

Section 45 Each of the Government Agencies, Regulators, and Organizations of Critical Information Infrastructure have a duty to protect, cope with, and mitigate risks of Cyber Incidents in accordance with its Code of Practice and standard Cybersecurity framework and shall act in compliance with the Code of Practice and standard Cybersecurity framework in accordance with section 13 paragraph one (4).

In case the Government Agencies, Regulators, or Organization of Critical Information Infrastructure could not act or comply in accordance with paragraph one, the Agency may grant assistance in the personnel or technological aspects to such agencies and organizations as requested.

Section 46 For the benefit of maintaining Cybersecurity, the Government Agencies, Regulators, and Organization of Critical Information Infrastructure shall provide the name of executive officials and operational officials for the Cybersecurity-related coordination with the Agency.

In the event there is a change to the officials under paragraph one, the Government Agencies, Regulators, and Organization of Critical Information Infrastructure shall notify the Agency without delay.

Section 47 In case the performance of the duties in accordance with this Act requires knowledge and expertise, the Committee or the CRC may assign the Secretary-General to hire an expert as appropriate for each specific task.

The expert in paragraph one shall have appropriate qualifications or experience in accordance with the notification of requirements prescribed by the Committee.

The Secretary-General shall issue an expert identification card to the appointed person. When performing duties, such person shall display the identification card as an expert and, once duties are completed, shall return the identification card to the Agency without delay.

Part 3
Critical Information Infrastructures

Section 48 Critical Information Infrastructures provide services that are important to national security, military security, economic security, and public order in the country, and it shall be the duty of the Agency to support and provide assistance to protect, cope with, and mitigate risks of Cyber Incidents, especially, those that affect or occur in the Critical Information Infrastructures.

Section 49 The Committee shall have the power to prescribe in a notification the characteristics of agencies and organizations that have missions or provide services in the following aspects, as the Organizations of Critical Information Infrastructure:

(1) national security sector;
(2) critical government service sector;
(3) banking and financial sector;
(4) information technology and telecommunication sector;
(5) transportation and logistics sector;
(6) energy and public utility sector;
(7) public health sector;
(8) others as prescribed by the Committee.

The consideration for the prescription of such mission or services under paragraph one shall be in accordance with the rules prescribed by the Committee, which shall be in the *Royal Thai Government Gazette*. The Committee shall consider and review such prescription of the mission or services on a case-by-case basis as appropriate.

Section 50 The Committee shall have the power to prescribe the characteristics, duties, and responsibilities of Computer Emergency Response Teams (CERTs) for the Organizations of Critical Information Infrastructure of section 49 to coordinate, monitor, response, and resolve Cyber Incidents by prescribing Government Agencies that are ready or the Regulators to perform such duties for their Organizations of Critical Information Infrastructure in accordance with section 49, in whole or in part.

Consideration for the prescription of such mission or services under paragraph one shall be in accordance with the rules prescribed by the Committee, which shall be published in the *Royal Thai Government Gazette*. The Committee shall consider and review such prescription of the mission or services on a case-by-case basis as appropriate.

Section 51 In the event of any inquiries or claims related to the characteristics of the agencies and organizations having the mission or providing the services as prescribed in accordance with section 49 or section 50, the Committee shall make the final decision.

Section 52 For the benefit of communication and coordination, the Organizations of Critical Information Infrastructure shall notify the name and contact information of the owner, the person possessing the computer, and the person administering the computer system to the Agency, their Regulator, and the entity under section 50, within thirty days from the date the Committee prescribes the notification in accordance with section 49 paragraph two and section 50 paragraph two, or from the date the Committee issues adjudication in accordance with section 51, as the case may be; the owner, the person possessing the computer, and the person administering the computer system shall at least be a person responsible for the management of such Organization of Critical Information Infrastructure.

In case there is any change to the owner, the person possessing the computer and the person administering monitoring the computer system in accordance with paragraph one, notice of change to the relevant entities under paragraph one shall be given not less than seven days in advance, unless there is reasonable cause which is inevitable, it shall be notified without delay.

Section 53 In respect to Cybersecurity of the Organizations of Critical Information Infrastructure, the Regulator shall audit the Cybersecurity baseline of the Organization of Critical Information Infrastructure under its supervision. If found that any Organizations of Critical Information Infrastructure do not comply with the baseline, the Regulator shall notify such Organizations of Critical Information Infrastructure to make corrections in order to meet the baseline without delay. If such Organizations of Critical Information Infrastructure neglect or fail to comply within the period prescribed by the Regulator, the Regulator shall file a motion to the CRC for consideration without delay.

Upon receipt of the motion under paragraph one, if the CRC considers and views that there is such reason and which may cause a cyber incident, the CRC may perform the following:

(1) in case of a Government Agency, the CRC shall notify the chief executive of the agency to exercise executive power to issue an order to the Government Agency or the Organization of Critical Information Infrastructure to take correction actions in order to comply with the baselines without delay;

(2) in case of a private organization, the CRC shall notify the chief executive of the organization, the person possessing the computer, and the person administering the computer system of the Organization of Critical Information Infrastructure to take correction actions to until it complies with the baselines without delay.

The Secretary-General shall monitor to ensure compliance of paragraph two.

Section 54 The Organization of Critical Information Infrastructure shall conduct Cybersecurity risk assessment by an assessor, and shall conduct Cybersecurity audit including the Cybersecurity aspect by the information security auditor, either internal auditor or external independent auditor, at least once per year.

The Organizations of Critical Information Infrastructure shall submit a summary report of

the to the Agency within thirty days after the assessment and the audit have been finished.

Section 55 In case the CRC views that the Cybersecurity risk assessment or the audit result in the Cybersecurity aspect in accordance with section 54 is incompliant with the baselines according to the report of the Regulator, the CRC shall order the Organization of Critical Information Infrastructure to conduct the Cybersecurity risk assessment again to be compliant with the baseline, or proceed with the examination in other aspects that may affect the Critical Information Infrastructure.

In case the Organization of Critical Information Infrastructure has already reconducted the Cybersecurity risk assessment or the audit in the Cybersecurity aspect of paragraph one but the CRC still views that it is not in compliance with the standards, the CRC shall perform the following:

(1) in case of a Government Agency, the CRC shall notify the chief executive of the agency to exercise executive power to issue an order to the Government Agency or the Organization of Critical Information Infrastructure to take corrective actions in order to comply with the standards without delay;

(2) in case of a private organization, the CRC shall notify the chief executive of the organization, the person possessing the computer, and the person administering the computer system of the Organization of Critical Information Infrastructure to take corrective actions in order to comply with the standards without delay.

The Secretary-General shall monitor to ensure compliance of paragraph two.

Section 56 The Organizations of Critical Information Infrastructure shall establish a mechanism or process to monitor Cyber Threats or Cyber Incidents which relate to its Critical Information Infrastructure in accordance with the standards as determined by the Regulator and in accordance with the Code of Practice, including Cybersecurity corrective measures and systems as determined by the Committee or the CRC, and shall participate in the assessment on the readiness in responding Cyber Incidents as held by the Agency.

Section 57 In the event of a Cyber Incident significantly occurring to the system of the Organization of Critical Information Infrastructure, the Organization of Critical Information Infrastructure shall report to the Agency and the Regulator and response Cyber Incidents as prescribed in Part 4, the CRC may prescribe criteria and procedures of the reporting.

Part 4
Cybersecurity Incident Response

Section 58 In the case there exists or may exist a Cyber Incident to an information system that is under the responsibility of a Government Agency or an Organization of Critical Information Infrastructure, such agency or organization shall investigate its related information, computer data, and the computer system, including the surrounding circumstances to assess whether a Cyber Incident has occurred. If the investigation results show that there exists or may exist a Cyber Incident, the agency or the organization shall protect, cope with, and mitigate the risks from such Cyber Incident in accordance with the Code of Practice and standard Cybersecurity frameworks and shall notify the Agency and its Regulator without delay.

In case the agency or organization, or any person, finds an obstacle or issues in protecting, coping with, or mitigating the risks from a Cyber Incident, such entity may request assistance from the Agency.

Section 59 When it appears to the Regulator, or when the Regulator is notified of a Cyber Incident in accordance with section 58, the Regulator in cooperation with the entities under section 50 shall gather information, investigate, analyze the situation, and evaluate the impacts of the Cyber Incident and shall perform the following:

(1) support and grant assistance to the Government Agency or Organization of Critical Information Infrastructure under its supervision or regulation and cooperate and coordinate with the Agency to protect, cope with, and mitigate the risks from the Cyber Incident;

(2) notify the Government Agencies or Organizations of Critical Information Infrastructure under its supervision or regulation, as well as other relevant Government Agencies or Organizations of Critical Information Infrastructure without delay.

Section 60 In consideration to exercise its power to prevent Cyber Incidents, the Committee will determine the characteristic of Cyber Incidents into three levels, as follows:

(1) a Cyber Incident at a non-critical level means a Cyber Incident with a significant risk level which causes the computer system of the country's Organization(s) of Critical Information Infrastructure or public service(s) to have degraded performance;

(2) a Cyber Incident at a critical level means a Cyber Incident with the nature of having significant increase in attacks on computer systems, computers, or computer data, targeting the Organization of Critical Information Infrastructure of the country, and such attack has the effect of causing damage to the computer systems or the information technology infrastructures related to the services provided by Critical Information Infrastructure of the country, public stability, international relations, national defense, economy, public health, public safety, or the public order of the people to the point that they could not operate or provide service;

(3) a Cyber Incident at a crisis level means a Cyber Incident of the following nature;

(a) is a Cyber Incident resulting from attacks on computer systems, computers, computer data at a level higher than the critical level, which cause severe effect to Critical Information Infrastructures of the country in a large-scale to the point where the whole operation of Government Agency or the service(s) provided by Organizations of Critical Information Infrastructure fail and the state consequently could not control the operating center of the state's computer system from the central, or the normal Cyber Incident mitigation measures could not resolve the issue and there is risk of spreading to other critical infrastructures of the country, which may cause death to many people or cause a large number of computer systems, computers, and computer data to be destroyed in a large scale at a national level;

(b) is a Cyber Incident that affects or may affect the public order or is a threat to national security or may cause the country or part of the country to be in a crisis situation, or an offense regarding terrorism under the Penal Code, armed conflict or war, in which an urgent measure is required to maintain the democratic regime of government with the King as the Head of the State in accordance with the Constitution of the Kingdom of Thailand, sovereignty and the integrity of the territory, national interests, lawfulness, public safety, peaceful living of the public, protection of freedom and rights, public order or interests, or the protection of or remedy for damages caused by an acute and catastrophic public disaster.

The details of the characteristics of Cyber Incident and measure for prevention, response, assessment, eradication, and containment of incidents at each level shall be in accordance with the notification prescribed by the Committee.

Section 61 When it appears to the CRC that there exists or may exist a Cyber Incident at the critical level, the CRC shall issue an order to the Agency to perform the following:

(1) gather information, or relevant documentary evidence, witness, material evidence to analyze the situation, and evaluate the effects from Cyber Incidents;
(2) support, assist, and participate in the protection, coping with, and mitigation of risks from the Cyber Incident;
(3) prevent the Cyber Incident resulting from Cyber Threats, recommend or issue an order to use the solution system to maintain Cybersecurity, as well as find the countermeasure approach or corrective actions to solve the Cybersecurity related problems;
(4) support the Agency and the relevant public and private agencies and organizations to assist and participate in protection, coping with, and mitigation of risks from the occurring Cyber Incident;
(5) notify of the Cyber Incident to related parties, as necessary and appropriate, taking into consideration the situation, severity, and impact from such Cyber Incident;
(6) facilitate in coordinating between relevant Government Agencies and private organizations to manage the risks and events related to the Cybersecurity.

Section 62 When acting under section 61, for the benefit of analyzing the situation and evaluating the effects from the Cyber Incident, the Secretary-General shall order the Competent Officials to:

(1) issue a letter requesting cooperation from the relevant persons to provide information within an appropriate period and at the prescribed place, or provide information in writing related to the Cyber Incident;
(2) issue a letter requesting for information, documents, or copy of the information or documents in the possession of other entities which is beneficial to the operation;
(3) inquire the persons who has knowledge and understanding of the facts and situations which are related to the Cyber Incident;
(4) enter into a property or a business premise which involves or may involves in the Cyber Incident and belongs to the relevant person or entity, with the consent from the person in possession of such property or premise.

Any person providing information in accordance with paragraph one, which acts in good faith, shall receive protection and shall not be deemed a wrongful act or a breach of a contract.

Section 63 In case of necessity to protect, cope with, and mitigate risks from a Cyber Incident, the CRC shall order the Government Agency to provide information, its personnel, or electronic devices under its possession in relation to maintain Cybersecurity.

The CRC shall ensure that there shall be no use of information under paragraph one that may cause damages and the CRC is responsible for the compensation for the personnel, expenses, and damages occurred from the use of such electronic devices.

Paragraph one and two shall also be applied to the requests to private organization, upon the consent of such private organization.

Section 64 In case there exists or may exist a Cyber Incident at the critical level, the CRC shall protect, cope with, and mitigate risks from the Cyber Incident and conduct necessary

measures.

When acting under paragraph one, the CRC shall issue a letter to the Government Agency which relates to maintain Cybersecurity to act or to stop any actions to protect, cope with, or mitigate risks from the Cyber Incident properly and efficiently, in accordance with the guideline prescribed by the CRC, as well as integrating the actions in order to control, contain, or mitigate the effect caused by the Cyber Incident in a timely manner.

The Secretary-General shall report the ongoing operation in accordance with this Section to the CRC constantly and when such Cyber Incident ends, the Secretary-General shall report the result to the CRC without delay.

Section 65 In handling and mitigating the damages from a Cyber Incident at the critical level, the CRC has the power to order, only as necessary to prevent the Cyber Incident, for the owner, the person possessing the computers, or the user of the computers or the computer systems, or a person administering the computer systems, which the CRC has a reasonable cause to believe that he/she involves in the Cyber Incident or is affected by the Cyber Incident to conduct the following acts:

(1) monitor the computer or computer system during a certain period of time;

(2) assess the computer or computer system to find a vulnerability that affects Cybersecurity, analyze the situation, and evaluate the effects from the Cyber Incident;

(3) take a corrective measure to handle vulnerabilities or remove unwanted programs or contain and mitigate the Cyber Incident that are running;

(4) maintain the status of the computer data or computer system via any possible methods to facilitate the computer forensic science;

(5) access relevant computer data or computer system or other information related to the computer system only to the extent it is necessary to prevent Cyber Incidents.

In case of necessity to access information under (5), the CRC shall assign the Secretary-General to file the motion to the Competent Court to order the owner, the person possessing the computer, the user of the computer or computer system, or a person administering the computer system in accordance with paragraph one to comply with the motion. The motion submitted to the Court shall specify the cause to believe that there exists a person who is acting or is going to act in one way or another that cause Cyber Incident at the critical level. The motion shall be submitted as emergency hearing motion and shall be considered by the Court without delay.

Section 66 In protecting, coping with, or mitigating the risks from a Cyber Incident at the critical level, the CRC has the power to order a Competent Official, only to the extent that it is necessary to prevent the Cyber Incident, to do the following:

(1) enter into a place to investigate, with a letter informing the appropriate reason to the owner or the occupier to investigate such place. If there is a cause to believe that there is a computer or computer system related to the Cyber Incident or is affected from the Cyber Incident;

(2) access the computer data, computer systems, or other data related to the computer systems, and copy or filter information data or computer programs which the CRC has a reason to believe that they are related to or are affected by the Cyber Incident;

(3) test the operation of the computers or computer systems which the CRC has a reason to believe that they are related to or are affected by the Cyber Incident or have been used to search any information from the inside or has been exploited from such computers or computer systems;

(4) seize or freeze computers, computer systems, or any equipment, only to the extent it

is necessary, which the CRC has a reason to suspect that is related to the Cyber Incident for the investigation or analysis, for not more than thirty days. Once such period is over, the computer or any equipment shall be returned to the owner or the possessor immediately after the investigation or analysis is finished.

When acting under (2), (3), and (4), the CRC may submit a motion to the Competent Court to order the officers to comply with the motion. The motion submitted to the Court shall specify the cause to believe that a person is acting or is going to act in one way or another that will cause a Cyber Incident at the critical level. The motion shall be submitted as emergency hearing motion and shall be considered by the Court without delay.

Section 67 In case there is a Cyber Incident at the crisis level, it shall be in the duty and power of the National Security Council in maintaining Cybersecurity under the laws on National Security Council and other relevant laws.

Section 68 In case it is urgent and necessary and the Cyber Incident at the crisis level, the Committee may assign to the Secretary-General the power to act, only to the extent it is necessary to prevent and remedy the damages in advance without requiring to submit the motion to the Court. However, after completing such actions, the details of the actions shall be notified to the Competent Court without delay.

In a critical or crisis case, for the benefit of preventing, assessing, coping with, containing, and mitigating the risks from the Cyber Incident, the Secretary-General, upon the approval of the Committee or CRC, shall have the power to request real-time information from the individual(s) who involves in the Cyber Incident. Such person shall cooperate with and facilitate the Committee or the CRC without delay.

Section 69 A person receiving an order related to Cyber Incident handling may appeal such order only for the case where the level of the Cyber Incident is non-critical.

Chapter 4
Penalty Provisions

Section 70 The Competent Officials under this Act is prohibited from disclosing or sending computer data, network data, other computer system related data, or user data from this Act to any person. Any officer violating shall be subject to imprisonment not exceeding three years, a fine not exceeding Baht sixty thousand, or both.

Paragraph one shall not apply to act for the benefit of litigation against an offender under this Act or an offender under other laws or for the benefit of the prosecution against the officer related to the exercising of unlawful authority.

Section 71 Any Competent Officials under this Act negligently causing other persons to know computer data, network data, user data, or other computer system related data obtained from this Act, shall be subject to imprisonment not exceeding one year, a fine not exceeding Baht twenty thousand, or both.

Section 72 Any person who knows computer data, network data, user data, or computer system related data that the Competent Officials has obtained from this Act and unlawfully discloses such data to any person shall be subject to imprisonment not exceeding two years, a fine not exceeding Baht forty thousand, or both.

Section 73 Any Organizations of Critical Information Infrastructure not reporting Cyber Incidents under section 57 without a reasonable cause shall be subject to Baht two hundred thousand.

Section 74 Any person not complying with the summoning letter of the Competent Officials, or not sending information to the Competent Official in accordance with section 62 (1) or (2) without a reasonable cause, as the case may be, shall be subject to a fine not exceeding Baht one hundred thousand.

Section 75 Any person violating or not complying with an order of the CRC in accordance with section 65 (1) and (2) without a reasonable cause shall be subject to a fine not exceeding Baht three hundred thousand and a daily fine not exceeding Baht ten thousand from the date on which the CRC issues the orders until compliance.

Any person violating or not complying with the order of the CRC in accordance with section 65 (3) and (4) or not complying with the court order in accordance with section 65 (5) shall be subject to imprisonment not exceeding one year, a fine not exceeding Baht twenty thousand, or both.

Section 76 Any person impeding or not complying with an order of the CRC or the Competent Official performing its duty in accordance with the CRC's order in accordance with section 66 (1), or not complying with the Court order in accordance with section 66 (2), (3), or (4), without a reasonable cause shall be subject to imprisonment not exceeding three years, a fine not exceeding Baht sixty thousand, or both.

Section 77 In case the person committing an offense under this Act is a juristic person, if such offense is a result of the order or the act of a director or a manager, or any person responsible for the acts of such juristic person, or in case such person has the duty to order or act but neglect to order or act, causing the juristic person to commit such an offense, such person shall be liable for the penalties prescribed for such offense.

Transitory Provisions

Section 78 At the beginning, the Committee shall consist of the chairperson and the committees under section 5 (1) and (2) and the Secretary-General of the National Cybersecurity Committee shall be a committee and secretary in order to temporarily conduct the duty only to the extent necessary and shall appoint the honorary committees of the Committee under section 5 (3) within ninety days from the date this Act enters into force.

In appointing the honorary director under paragraph one, the Minister of Digital Economy and Society may nominate list of individuals to the Cabinet for considering on appointing as honorary director.

Section 79 The CRC and the CMSA shall be established within ninety days from the date of appointment of the honorary director of the Committee under section 78.

The Secretary-General under this Act shall be appointed within ninety days from the date the establishment of the Agency has been complete under section 80.

Section 80 Establishment of the Agency shall be completed in order to perform its duty in accordance with this Act within one year from the date this Act enters into force.

While the establishment of the Agency has not been completed, the Office of the Permanent Secretary, Ministry of Digital Economy and Society, shall perform the duty of the Agency under this Act, and the Permanent Secretary of the Ministry of Digital Economy and Society shall perform the duty as the Secretary-General until there is an appointment of the Secretary-General in accordance with section 79 paragraph two.

Section 81 At the beginning, the Cabinet shall assign an initial funding to the Agency as necessary.

The Minister shall propose to the Cabinet for consideration the public servant, official, personnel, officer, or the person performing any other task in a Government Agency to work in the Agency temporarily within the period prescribed by the Cabinet.

The public servant, official, personnel, officer, or the person performing any other task in a Government Agency operating in the Agency temporarily in accordance to paragraph two shall not be rid of their current status and shall receive salary or wage, as the case may be, from the same organization. The CRC may prescribe special compensation for the public servant, officials, personnel, officer, or the person performing any other task in a Government Agency in accordance with paragraph two during the operation in the Agency.

Within one hundred and eighty days from the date the establishment of the Agency has been completed, the Agency shall select the public servant, official, personnel, officer, or the person performing any other task in a Government Agency to be employed as its personnel.

The public servant, official, personnel, officer, or the person performing any other task in a Government Agency who has been selected and placed in accordance with paragraph four shall be entitled to count the duration of employment at the previous agency in continuation to the duration of employment in the Agency under this Act.

Section 82 When this Act enters into effect, the Minister shall present to the Cabinet to approve the transfer of all the duties, power, business, assets, rights, debts, and all Cybersecurity related budgets of the Permanent Secretary, Ministry of Digital Economy and Society and the Electronic Transactions Development Agency, which exist prior to the day this Act enters into force, to the Agency, in accordance with this Act.

Section 83 Issuance of the regulations, rules, and notifications in accordance with this Act shall be completed within one year from the day this Act enters into force. If such cannot be carried out, the Minister shall report the reasons that is could not be carried out to the Cabinet.

Countersigned by

General Prayut Chan-o-cha

Prime Minister

Remarks: - The reason for the enactment of this Act is that nowadays the provision of services or application of the computer networks, the internet, telecommunication networks, or general satellite services are currently under the risk of Cyber Threats which may threaten national security and public order in the country. In order to be able to simultaneously prevent or handle Cyber Incidents, it is deemed appropriate to determine the characteristics of the essential missions or services as critical information infrastructure, for both the government agencies and private organizations, which are necessary to have the capabilities to protect, cope with, and mitigate the risk from Cyber Incidents, such that there are no adverse effects on Cybersecurity in varying aspects. It also deems necessary to have the competent authorities responsible for coordinating between the government and private sectors regardless of the situations, whether they are normal or pose severe threats to national security, and to establish operational plans and Cybersecurity measures in united and continuous manner. This will make the prevention and Cyber Incident handling efficient and thus the Act is necessary to be enacted.

2

ประกาศ กมช.

เรื่อง การจัดตั้ง หน้าที่และอำนาจของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ พ.ศ. 2564

มีผลใช้บังคับตั้งแต่วันที่ 24 ส.ค. 64 เป็นต้นไป

Notification of NCSC

Re: Establishment, Duties, and Powers of Thailand Computer Emergency Response Team (ThaiCERT) B.E. 2564 (2021)

effective from August 24, 2021, onwards.



ฉบับภาษาไทย
Thai Version

ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

เรื่อง การจัดตั้ง หน้าที่และอำนาจของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ พ.ศ. ๒๕๖๔

โดยที่พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดให้มีการจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติขึ้นเป็นหน่วยงานภายในสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เพื่อเฝ้าระวังความเสี่ยงในการเกิดภัยคุกคามทางไซเบอร์ ติดตาม วิเคราะห์และประมวลผลข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์และการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์

อาศัยอำนาจตามความในมาตรา ๒๒ วรรคสอง แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ประกอบกับมติที่ประชุมคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ในคราวการประชุมครั้งที่ ๑/๒๕๖๔ เมื่อวันที่ ๒๕ มิถุนายน ๒๕๖๔ คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ จึงออกประกาศฉบับนี้ เพื่อกำหนดหน้าที่และอำนาจของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง การจัดตั้ง หน้าที่และอำนาจของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ พ.ศ. ๒๕๖๔”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ข้อ ๓ ในประกาศนี้

“คณะกรรมการ” หมายความว่า คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

“หน่วยงานภายใต้การดูแล” หมายความว่า หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแลหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานที่ทำหน้าที่เป็นศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและหน่วยงานเอกชนอื่นตามที่ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติได้รับมอบหมายจากคณะกรรมการให้ดำเนินการ

ข้อ ๔ ในการดำเนินการใด ๆ ของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ รวมถึงการติดต่อ ประสานงาน หรือการแจ้งเตือนที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ ให้ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติจัดให้มีหลักเกณฑ์ เงื่อนไข และวิธีการในการจัดชั้นความลับของข้อมูลต่าง ๆ การกำหนดสิทธิในการเข้าถึงข้อมูลและการดำเนินการอื่นใดที่เกี่ยวข้อง เพื่อรักษาความลับ (confidentiality) ความถูกต้อง (integrity) ตลอดจนความพร้อมในการใช้งาน (availability) ของข้อมูลที่เกี่ยวข้อง

ข้อ ๕ ให้ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติมีหน้าที่และอำนาจ รวมทั้งให้มีการดำเนินมาตรการในด้านต่าง ๆ ดังต่อไปนี้

๕.๑ การดำเนินมาตรการเชิงรุกเพื่อป้องกันและเฝ้าระวังความเสี่ยงในการเกิดภัยคุกคามทางไซเบอร์ ให้เป็นไปตามหลักเกณฑ์ ดังนี้

๕.๑.๑ ปฏิบัติงานร่วมกับหรือสนับสนุนการปฏิบัติงานของหน่วยงานภายใต้การดูแล เพื่อเฝ้าระวัง ติดตาม และเตรียมความพร้อมในการรับมือเมื่อได้รับการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์

๕.๑.๒ เป็นศูนย์กลางเครือข่ายข้อมูลและส่งเสริมความร่วมมือด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ โดยอาจประสานงานหรือร่วมมือกับเครือข่ายหรือภาคีทั้งในและต่างประเทศ เพื่อรับ ส่งต่อ หรือแลกเปลี่ยนข้อมูลที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ และเตรียมความพร้อมในการรับมือเมื่อได้รับการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์

๕.๑.๓ จัดทำข้อมูลทางสถิติด้านการตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ ตลอดจนข้อมูลการแจ้งเตือนที่สำคัญ และข้อมูลอื่น ๆ ที่เกี่ยวข้องเพื่อเผยแพร่ต่อสาธารณะ

๕.๑.๔ วิเคราะห์และตรวจสอบข่าวกรองเกี่ยวกับภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้น ดำเนินการเพื่อป้องกันปัญหาที่อาจเกิดขึ้น รวมถึงการเผยแพร่ข้อมูลที่มีความจำเป็นเพื่อให้หน่วยงานภายใต้การดูแลสามารถดำเนินมาตรการป้องกันหรือจัดการกับสถานการณ์ด้านภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้น เช่น การให้คำแนะนำแก่หน่วยงานดังกล่าวในการตรวจจับการบุกรุก และการวิเคราะห์ข้อมูล เป็นต้น

๕.๑.๕ ให้การแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้น หรือให้คำเตือนเกี่ยวกับช่องโหว่ที่อาจถูกใช้เป็นช่องทางในการก่อภัยคุกคามทางไซเบอร์ เพื่อให้หน่วยงานภายใต้การดูแลดำเนินการเพื่อให้มีการป้องกันโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หรือระบบงานที่มีความสำคัญอื่น ๆ ได้อย่างทันท่วงที

๕.๑.๖ ติดตามความก้าวหน้าด้านเทคโนโลยีต่าง ๆ เพื่อจัดทำข้อเสนอแนะเกี่ยวกับการป้องกันภัยคุกคามทางไซเบอร์หรือแนวปฏิบัติพื้นฐาน (baseline) ในการป้องกันหรือเตรียมความพร้อมในการรับมือเมื่อได้รับการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์

๕.๑.๗ เมื่อได้รับการร้องขอจากหน่วยงานภายใต้การดูแล หรือเมื่อได้รับการประสานงานในกรณีที่คาดว่าจะเกิดภัยคุกคามทางไซเบอร์ขึ้นกับหน่วยงานดังกล่าว ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติอาจพิจารณาดำเนินการ ดังนี้

(๑) รวบรวมข้อมูล ติดตาม วิเคราะห์ และประมวลผลข้อมูลเพื่อทำวิจัยเชิงรุกเกี่ยวกับรูปแบบของการเกิดภัยคุกคามทางไซเบอร์ เพื่อประเมินผลกระทบและแนวโน้มของการเกิดภัยคุกคามทางไซเบอร์ในรูปแบบต่าง ๆ

(๒) ให้การช่วยเหลือ แนะนำ และสนับสนุนในการดำเนินมาตรการป้องกันตามแนวทางปฏิบัติที่ดี (best practice) เพื่อเตรียมความพร้อมในการรับมือเมื่อได้รับการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์

(๓) ประเมินความเสี่ยงและช่องโหว่ที่อาจถูกใช้ในการก่อภัยคุกคามทางไซเบอร์เพื่อนำไปสู่การจัดการช่องโหว่ การดำเนินมาตรการป้องกัน หรือกระทำการอื่นใดเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์

(๔) ตรวจจับเหตุการณ์ที่อาจนำมาสู่การบุกรุก วิเคราะห์สิ่งบอกเหตุการณ์ หรือดำเนินการอื่นใดที่เกี่ยวข้องเพื่อตรวจสอบโปรแกรม หรือค้นหาสิ่งที่ไม่พึงประสงค์ (malicious code) ซึ่งอาจเป็นอันตรายต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หรือระบบงานที่มีความสำคัญอื่น ๆ

ทั้งนี้ เพื่อประโยชน์ในการประสานงานและการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์ให้ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติดำเนินการเพื่อให้มีการรับลงทะเบียนข้อมูลและจัดทำบัญชีช่องทางการติดต่อ (point of contact) ของหน่วยงานภายใต้การดูแล เพื่อใช้เป็นช่องทางหลักในการติดต่อสื่อสารระหว่างศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติกับหน่วยงานดังกล่าว

๕.๒ การดำเนินมาตรการเชิงรับเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น ให้เป็นไปตามหลักเกณฑ์ ดังนี้

๕.๒.๑ เป็นศูนย์กลางในการรับและแจ้งเหตุเกี่ยวกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นทั้งในประเทศและต่างประเทศ และประสานงานกับหน่วยงานภายใต้การดูแล เพื่อตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์อย่างเหมาะสมและทันท่วงที ตลอดจนให้การสนับสนุนข้อมูลต่าง ๆ ที่จำเป็นแก่หน่วยงานดังกล่าว เพื่อดำเนินการแก้ไขเหตุภัยคุกคามทางไซเบอร์ โดยจัดให้มีช่องทางในการรับและแจ้งเหตุผ่านระบบอิเล็กทรอนิกส์ที่กำหนดขึ้นโดยเฉพาะหรือช่องทางอื่นใดตามที่ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติกำหนด

๕.๒.๒ พิจารณาความเหมาะสมในการกำหนดระดับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นตามที่ได้รับแจ้งจากหน่วยงานภายใต้การดูแล โดยอาจพิจารณากำหนดความเร่งด่วนตามที่ได้รับแจ้งหรือกำหนดความเร่งด่วนขึ้นใหม่จากลักษณะหรือผลกระทบจากภัยคุกคามทางไซเบอร์ และให้คำแนะนำในการกำหนดแผนการรับมือและแก้ไขภัยคุกคามทางไซเบอร์ที่เหมาะสมเพื่อจำกัดขอบเขตความเสียหาย

๕.๒.๓ ติดตามการตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ ผลกระทบเกี่ยวกับภัยคุกคามทางไซเบอร์ และผลการตอบสนองและรับมือเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น

๕.๒.๔ เมื่อได้รับการร้องขอจากหน่วยงานภายใต้การดูแล หรือเมื่อได้รับการประสานงานในกรณีที่คาดว่าจะเกิดภัยคุกคามทางไซเบอร์ขึ้นกับหน่วยงานดังกล่าว ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติอาจพิจารณาดำเนินการ ดังนี้

(๑) ให้การช่วยเหลือ แนะนำ และสนับสนุนในการตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้น เช่น การช่วยวิเคราะห์ต้นเหตุของภัยคุกคาม โปรไฟล์ของผู้โจมตี วิธีการระงับเหตุการณ์ตอบโต้ผู้บุกรุกและการกำจัดช่องโหว่ โดยอาจเข้าไปในสถานที่ที่เกิดเหตุการณ์ หรือดำเนินการผ่านวิธีการทางอิเล็กทรอนิกส์ที่ใช้ในการติดต่อสื่อสารจากสถานที่ปฏิบัติงานของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ

(๒) ให้การช่วยเหลือ แนะนำ และสนับสนุนในการฟื้นฟูเพื่อให้สามารถกลับมาดำเนินภารกิจหรือให้บริการได้ต่อไปภายหลังการระงับเหตุภัยคุกคามทางไซเบอร์เสร็จสิ้น

(๓) ให้การช่วยเหลือ แนะนำ และสนับสนุนในการดำเนินกระบวนการทางนิติวิทยาศาสตร์ การตรวจพิสูจน์พยานหลักฐานทางดิจิทัล การเชื่อมโยงข้อมูลภัยคุกคามทางไซเบอร์จากแหล่งข้อมูลต่าง ๆ ตลอดจนการสืบสวนหรือสอบสวนเกี่ยวกับการกระทำความผิดที่เกี่ยวข้องกับการก่อภัยคุกคามทางไซเบอร์

๕.๒.๕ จัดทำรายงานข้อมูลผลการรับมือกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นทั้งในกรณีที่ได้รับทราบจากการแจ้งเหตุของผู้เกี่ยวข้อง รวมถึงกรณีที่พบเห็นเหตุการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ เพื่อรายงานต่อสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

ทั้งนี้ เพื่อประโยชน์ในการรับมือกับเหตุภัยคุกคามทางไซเบอร์ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติอาจดำเนินการรวบรวมข้อมูลการโจมตีทางไซเบอร์ที่เกิดขึ้น เพื่อใช้เป็นข้อมูลในการศึกษา วิเคราะห์และประมวลผลข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ เพื่อนำไปสู่การดำเนินมาตรการเชิงรุกในการป้องกันและเฝ้าระวังความเสี่ยงในการเกิดภัยคุกคามทางไซเบอร์ในอนาคต

๕.๓ การดำเนินมาตรการด้านการบริหารจัดการคุณภาพเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ ให้เป็นไปตามหลักเกณฑ์ ดังนี้

๕.๓.๑ ผลักดันและสนับสนุนให้เกิดการสร้างความตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ เพื่อนำไปสู่การดำเนินมาตรการในการป้องกันและการรักษาความมั่นคงปลอดภัยไซเบอร์

๕.๓.๒ ยกระดับความรู้ความสามารถของหน่วยงานภายใต้การดูแลเพื่อเตรียมความพร้อมในการปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และสามารถยกระดับการป้องกันโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และระบบงานที่มีความสำคัญอื่น ๆ

๕.๓.๓ เมื่อได้รับการร้องขอจากหน่วยงานภายใต้การดูแล ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติอาจพิจารณาดำเนินการ ดังนี้

(๑) ให้การช่วยเหลือ แนะนำ และสนับสนุนในการประเมินความเสี่ยงของการเกิดภัยคุกคามทางไซเบอร์ โดยใช้กระบวนการเรียนรู้ที่ได้รับจากการดำเนินมาตรการเชิงรุกเพื่อป้องกันและเฝ้าระวังความเสี่ยงในการเกิดภัยคุกคามทางไซเบอร์ และการดำเนินมาตรการเชิงรับเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น เพื่อช่วยให้หน่วยงานดังกล่าวสามารถวางแผนการรับมือในกรณีที่ต้องเผชิญเหตุภัยคุกคามทางไซเบอร์

(๒) ให้การช่วยเหลือ แนะนำและสนับสนุนในการจัดทำแผนความต่อเนื่องของการดำเนินงาน (business continuity plan) เพื่อรับมือในกรณีที่เกิดเหตุภัยคุกคามทางไซเบอร์ แผนการป้องกันโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (critical information infrastructure protection plan) และแผนฟื้นฟู (disaster recovery plan) ภายหลังเกิดภัยคุกคามทางไซเบอร์

๕.๓.๔ เพื่อให้การบริหารจัดการคุณภาพเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ ดำเนินการได้อย่างมีประสิทธิภาพและมีประสิทธิผล ให้ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติดำเนินการ ดังนี้

(๑) ระบุตัวชี้วัดและติดตามผลการดำเนินงาน เพื่อประเมินคุณภาพของการดำเนินการ เช่น ระยะเวลาที่ใช้ตอบสนองต่อการร้องขอ ระยะเวลาที่ใช้ต่อการดำเนินงานในสถานการณ์ต่าง ๆ และจำนวนรายงานหรือคู่มือที่เกี่ยวข้องกับพันธกิจ เป็นต้น

(๒) กำหนดแนวทางการดำเนินงานด้านนโยบายและการปฏิบัติเป็นระดับ (phase) โดยอาจใช้โมเดลการวัดระดับขีดความสามารถขององค์กร (Capability Maturity Model หรือ “CMM”) เป็นเครื่องมือในการกำหนด

(๓) จัดให้มีระบบบริหารจัดการคุณภาพ (service management quality system) เพื่อติดตามผลการดำเนินงานและปรับปรุงการดำเนินงานอย่างต่อเนื่อง เพื่อให้เป็นไปตามผลการดำเนินงานที่ตั้งเป้าหมาย

(๔) กำหนดกระบวนการและขั้นตอน รวมถึงเครื่องมือที่จำเป็นเพื่อใช้สนับสนุนการให้บริการแก่หน่วยงานภายใต้การดูแล เช่น ระบบบันทึกภัยคุกคามและการติดตามการดำเนินงาน (ticketing system) และระบบบริหารจัดการงานต่าง ๆ (workflow management system) เป็นต้น

๕.๓.๕ ดำเนินกิจกรรมร่วมกับหน่วยงานของรัฐ หน่วยงานเอกชน องค์การหรือหน่วยงานทั้งในประเทศและต่างประเทศ อันเป็นประโยชน์ต่อการบริหารจัดการคุณภาพเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์และการรับมือกับภัยคุกคามทางไซเบอร์ตามที่สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติมอบหมายเพิ่มเติม

ข้อ ๖ เพื่อประโยชน์ในการเฝ้าระวังความเสี่ยงในการเกิดภัยคุกคามทางไซเบอร์ ติดตาม วิเคราะห์และประมวลผลข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ และการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์ ให้ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติให้การช่วยเหลือสนับสนุน หรือปฏิบัติงานร่วมกับพนักงานเจ้าหน้าที่ หรือสนับสนุนการดำเนินการของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติในกิจการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์และการรับมือกับภัยคุกคามทางไซเบอร์ หรือปฏิบัติหน้าที่อื่นใดเพิ่มเติมได้ตามที่คณะกรรมการกำหนด

ประกาศ ณ วันที่ ๑๑ สิงหาคม พ.ศ. ๒๕๖๔
พลเอก ประวิตร วงษ์สุวรรณ
รองนายกรัฐมนตรี ปฏิบัติหน้าที่
ประธานกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ



ฉบับภาษาอังกฤษ
English Version

Notification of the National Cyber Security Committee

Re: Establishment, Duties, and Powers of

Thailand Computer Emergency Response Team (ThaiCERT)

B.E. 2564 (2021)

Whereas the Cybersecurity Act B.E. 2562 (2019) stipulates that there shall be an establishment of Thailand Computer Emergency Response Team (ThaiCERT) as a unit of the National Cyber Security Agency to monitor cybersecurity risks, to track, analyze and process information related to cyber incidents, and to issue incident warnings.

By Virtue of Section 22 paragraph two of the Cybersecurity Act B.E. 2562 (2019), together with the resolution of the National Cyber Security Committee meeting no. 1/2564 on 25 June B.E. 2564 (2021), the National Cyber Security Committee hereby issues this notification to prescribe the duties and powers of Thailand Computer Emergency Response Team (ThaiCERT) as follows:

Clause 1 This notification shall be called the "Notification of the National Cyber Security Committee Re: Establishment, Duties, and Powers of Thailand Computer Emergency Response Team (ThaiCERT) B.E. 2564 (2021)".

Clause 2 This notification shall come into force on the date after its publication in the Royal Thai Government Gazette.

Clause 3 In this notification

"Committee" means the National Cyber Security Committee.

"Constituents" mean government agencies, regulators, organizations of critical Information Infrastructure, organizations that act as computer emergency response teams for organizations of critical information infrastructure, and other private organizations as assigned to the Thailand Computer Emergency Response Team by the Committee.

Clause 4 Thailand Computer Emergency Response Team (ThaiCERT) must prescribe a set of rules, conditions, and procedures for data classification and access control when carrying out any of their operations, which include contacting, coordinating, or issuing alerts on cyber incidents, so that confidentiality, integrity, and availability of relevant information can be maintained.

Clause 5 Thailand Computer Emergency Response Team (ThaiCERT) shall have the duties and powers, including the implementation of measures in various areas, as set out in the following.

5.1 The implementation of proactive measures to prevent and monitor cybersecurity risks shall be in accordance with the following:

5.1.1 collaborating with or supporting operations of the Constituents to monitor, track, and prepare for incident handling in responding to an incident alert;

5.1.2 acting as an information sharing hub and promoting national cybersecurity collaboration by coordinating or collaborating with both domestic and international networks or alliances to receive, forward, or share information related to cyber threats and prepare for incident handling in responding to an incident alert;

5.1.3 preparing statistical information about responding and handling of cyber incidents, as well as other important alerts and related information, to disseminate to the public;

5.1.4 analyzing and verifying cyber threat intelligence that may occur and taking an action to prevent the possible occurrence, which include disseminating necessary information so that the Constituents is able to implement any preventive measure or handle cyber incidents that may occur. Such information may include advice on the detection of intrusion and information analysis;

5.1.5 issuing an alert on a possible occurrence of an incident, or a warning about the vulnerability that may be exploited in a cyberattack, so that the Constituents can take an action to protect their critical information infrastructure or other critical systems in a timely manner;

5.1.6 tracking technological advancements to make recommendations regarding incident prevention or suggest a baseline for prevention and preparation in responding to an incident alert;

5.1.7 when receiving a request from the Constituents, or being informed of an incident that may occur to the Constituents, Thailand Computer Emergency Response Team (ThaiCERT) may consider taking the following actions:

(1) gathering, tracking, analyzing, and processing information to conduct proactive research on characteristics of the occurrence of the incident to assess the impact and the occurrence trends of various forms of cyber incident;

(2) providing assistance, advice, and support in implementing a preventive measure based on the best practice to prepare for the incident handling in responding to an incident alert;

(3) assessing risks and vulnerabilities that may be exploited in a cyberattack, leading to vulnerability management, any preventive measures, or any cybersecurity maintenance activities;

(4) detecting events that may lead to an intrusion, analyzing incident indicators, or taking any related actions to scan applications for malicious codes or vulnerabilities that may be harmful to the critical information infrastructure or other critical systems.

To facilitate the coordination and warning of cyber threats, Thailand Computer Emergency Response Team (ThaiCERT) shall set up an information registration service and compile points of contact of the Constituents to be used as a main communication channel between the Thailand Computer Emergency Response Team (ThaiCERT) and the Constituents.

5.2 The Implementation of reactive measures following an occurrence of a cyber incident shall be in accordance with the following:

5.2.1 acting as a center of incident reporting and notification both domestically and internationally and coordinating with the Constituents in responding and handling cyber incidents in an appropriate and timely manner, and to additionally supply necessary information to the Constituents to remedy the incident. Thailand Computer Emergency Response Team (ThaiCERT) shall establish a channel for incident reporting and notification through specifically dedicated electronic systems or through other communication means;

5.2.2 reviewing the appropriateness of the reported criticality level of the incident that has occurred. The level of urgency may remain as originally reported or revised after considering the characteristics and impact of the incident. Some advice on handling and mitigating plan shall be provided to contain the damage;

5.2.3 tracking the incident response and handling, the incident impact, and the result of the response and handling of the incident that has occurred;

5.2.4 when receiving a request from the Constituents, or being informed of an incident that may occur to the Constituents, Thailand Computer Emergency Response Team (ThaiCERT) shall consider taking the following actions:

(1) providing assistance, advice, support in responding to and handling incident that has occurred, e.g., assisting in analyzing the root cause of the incident, attacker's profile, how to contain the incident, how to countermeasure intruder and eliminate vulnerabilities. These actions may be done by visiting the site where the incident occurred or by electronic communication from operating location of Thailand Computer Emergency Response Team (ThaiCERT);

(2) providing assistance, advice, and support in recovery to resume missions or services after the incident has been contained;

(3) providing assistance, advice, and support in operations related to forensic science, digital forensics, correlation of information related to the incidents from various sources, and the investigation of any delinquency related to cybers incidents;

5.2.5 preparing a report on the result of the incident handlings that are either reported by a related party, or directly witnessed, so that the report may be submitted to the National Cyber Security Agency.

In addition, to facilitate incident handling, Thailand Computer Emergency Response Team (ThaiCERT) may gather information on occurred cyber incidents to be utilized for studies, analyses, and processes to set up proactive measures in preventing and monitoring potential cybersecurity risks.

5.3 The implementation of quality management measure to ensure cybersecurity shall be in accordance with the following:

5.3.1 driving and supporting efforts to raise awareness regarding cyber threats that will lead to the implementation of cybersecurity measures;

5.3.2 elevating knowledge and capabilities of the Constituents to be ready for cybersecurity operations and for further enhancing the protection capability for the critical information infrastructures and other critical systems;

5.3.3 upon receiving a request from the Constituents, Thailand Computer Emergency Response Team (ThaiCERT) may consider taking the following actions:

(1) providing assistance, advice, and support in the assessment of cybersecurity risks based on the knowledge from the implementation of proactive measures in preventing and monitoring cybersecurity risks, and from that of reactive measures after incidents occurred, to ensure that the Constituents are able to devise a handling plan when facing an incident;

(2) providing assistance, advice, and support in devising a business continuity plan for responding to ongoing cyber incidents, and devising a critical information infrastructure protection plan, and disaster recovery plan after the incident has occurred;

5.3.4 In order to provide an efficient and effective cybersecurity quality management, the Thailand Computer Emergency Response Team (ThaiCERT) shall take the following actions:

(1) identifying indicators and tracking performance to evaluate the service quality, e.g., response time to service request, duration of operations in various situations, and the number of reports and manuals related to the mission;

(2) outlining directions for developing policies and for implementations in phases. The Capability Maturity Model or CMM may be used as a tool to define directions;

(3) establishing a service management quality system for continuously tracking and improving performance to achieve performance goals;

(4) prescribing processes and steps, including tools needed to provide services to the Constituents, e.g., a ticketing system, a workflow management system.

5.3.5 Engaging in activities with government agencies, private organizations, corporations and agencies, both domestically and internationally, which are beneficial to quality management for ensuring cybersecurity and incident handling, as additionally assigned by the National Cyber Security Agency.

Clause 6 To facilitate the monitoring of cybersecurity risks, tracking, analyzing and processing of information related to cyber incidents, and issuing incident alerts, Thailand Computer Emergency Response Team (ThaiCERT) shall provide assistance, support, and collaboration with Competent Officials, support operations of the National Cyber Security

Agency in matters related to cybersecurity and cyber incident handling, or any other duties that may be additionally prescribed by the Committee.

Given on the 11th of August B.E. 2564 (2021)

General Pravit Wongsuwan

(Pravit Wongsuwan)

Deputy Prime Minister as

Chairman of the National Cyber Security Committee

3

ประกาศ กมช.

เรื่อง ลักษณะ หน้าที่และความรับผิดชอบของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและภารกิจหรือให้บริการที่เกี่ยวข้อง พ.ศ. 2564

มีผลใช้บังคับตั้งแต่วันที่ 23 ส.ค. 65 เป็นต้นไป

Notification of NCSC

Re: Characteristics, Duties, and Responsibilities of the Computer Emergency Response Team for Critical Information Infrastructure organizations, Related Missions and Services B.E. 2564 (2021)

effective from August 23, 2022, onwards.



ฉบับภาษาไทย

Thai Version

ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

เรื่อง ลักษณะ หน้าที่และความรับผิดชอบของศูนย์ประสานการรักษาความมั่นคงปลอดภัย
ระบบคอมพิวเตอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
และภารกิจหรือให้บริการที่เกี่ยวข้อง
พ.ศ. ๒๕๖๔

โดยที่พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดให้คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติประกาศกำหนดลักษณะ หน้าที่และความรับผิดชอบของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เพื่อประสานงาน เฝ้าระวัง รับมือ และแก้ไขภัยคุกคามทางไซเบอร์ โดยจะกำหนดให้หน่วยงานของรัฐที่มีความพร้อมหรือหน่วยงานควบคุมหรือกำกับดูแลหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนั้น ๆ ทำหน้าที่ดังกล่าว ให้แก่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศทั้งหมดหรือบางส่วนก็ได้ รวมถึงให้คณะกรรมการพิจารณากำหนดภารกิจหรือให้บริการของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศดังกล่าว

อาศัยอำนาจตามความในมาตรา ๕๐ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ประกอบกับมติที่ประชุมคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ในคราวการประชุมครั้งที่ ๑/๒๕๖๔ เมื่อวันที่ ๒๕ มิถุนายน ๒๕๖๔ คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ จึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะ หน้าที่และความรับผิดชอบของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และภารกิจหรือให้บริการที่เกี่ยวข้อง พ.ศ. ๒๕๖๔

ข้อ ๒ ประกาศนี้ให้ใช้บังคับเมื่อพ้นกำหนดหนึ่งปีนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ข้อ ๓ ให้หน่วยงานของรัฐที่มีความพร้อมหรือหน่วยงานควบคุมหรือกำกับดูแลหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศในแต่ละด้านจัดตั้งหรือดำเนินการเพื่อให้มีศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยหน่วยงานควบคุมหรือกำกับดูแลอาจจัดให้มีหลักเกณฑ์ เงื่อนไขและแนวทางในการพิจารณาคุณสมบัติ และความเหมาะสมของการเป็นศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

ให้ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามวรรคหนึ่ง มีลักษณะ หน้าที่และความรับผิดชอบ รวมถึงจัดให้มีการดำเนินภารกิจหรือให้บริการไม่น้อยกว่าหลักเกณฑ์ที่กำหนดแนบท้ายประกาศฉบับนี้

ข้อ ๔ เมื่อมีการจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศในด้านใดแล้ว ให้หน่วยงานควบคุมหรือกำกับดูแลแจ้งการจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศในด้านดังกล่าว พร้อมกับรายชื่อหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ภายใต้การดูแลและข้อมูลอื่น ๆ ที่เกี่ยวข้อง ให้สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติทราบภายในสามสิบวันนับแต่วันที่ประกาศนี้มีผลใช้บังคับ

ในกรณีที่มีการจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศเพิ่มเติม หรือมีการเปลี่ยนแปลงใด ๆ เกี่ยวกับศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่ให้หน่วยงานควบคุมหรือกำกับดูแลแจ้งการจัดตั้งเพิ่มเติมหรือการเปลี่ยนแปลงดังกล่าว พร้อมข้อมูลที่เกี่ยวข้อง ต่อสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติทราบภายในสามสิบวันนับแต่วันที่จัดตั้งเพิ่มเติมหรือเปลี่ยนแปลงแล้วเสร็จ

ให้สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติรายงานการจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามวรรคหนึ่งให้คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติทราบ โดยคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ อาจให้ข้อเสนอแนะหรือให้ความเห็นเพิ่มเติมได้

ข้อ ๕ ในระหว่างที่หน่วยงานของรัฐหน่วยงานใดยังไม่มีความพร้อมในการทำหน้าที่เป็นศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ให้หน่วยงานดังกล่าวแจ้งเหตุขัดข้อง หรือสาเหตุที่ทำให้ยังไม่มีความพร้อมให้หน่วยงานควบคุมหรือกำกับดูแลทราบ เพื่อให้หน่วยงานควบคุมหรือกำกับดูแลประสานงานร่วมกับสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เพื่อพิจารณาดำเนินการตามแนวทางที่เหมาะสม เพื่อให้การช่วยเหลือในด้านการประสานงาน เฝ้าระวัง รับมือ และแก้ไขภัยคุกคามทางไซเบอร์แก่หน่วยงานดังกล่าว ต่อไป

ประกาศ ณ วันที่ ๑๑ สิงหาคม พ.ศ. ๒๕๖๔
พลเอก ประวิตร วงษ์สุวรรณ
รองนายกรัฐมนตรี ปฏิบัติหน้าที่
ประธานกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

ลักษณะ หน้าที่และความรับผิดชอบของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และภารกิจหรือให้บริการที่เกี่ยวข้อง พ.ศ. ๒๕๖๔

คำนิยาม

๑.	ศูนย์ประสานการรักษาความมั่นคงปลอดภัย	หมายถึง	ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
๒.	หน่วยงาน CII	หมายถึง	หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure) ที่อยู่ภายใต้การดูแลของศูนย์ประสานการรักษาความมั่นคงปลอดภัย
๓.	สำนักงาน	หมายถึง	สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

ลักษณะ หน้าที่และความรับผิดชอบของศูนย์ประสานการรักษาความมั่นคงปลอดภัย

๔. ศูนย์ประสานการรักษาความมั่นคงปลอดภัยอาจจัดตั้งขึ้นในลักษณะที่เป็นหน่วยงานอิสระที่มีการบริหารงานเป็นของตนเอง หรือกำหนดให้เป็นส่วนงานหนึ่งภายในองค์กรที่จัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยหรือกำหนดให้เป็นหน่วยงานที่อยู่ภายใต้การดูแลของหน่วยงานของรัฐหรือหน่วยงานควบคุมหรือกำกับดูแลซึ่งทำหน้าที่กำกับดูแลหน่วยงาน CII ในแต่ละด้าน หรืออาจจัดตั้งขึ้นในรูปแบบของการรวมกลุ่มระหว่างหน่วยงาน หรือผู้ประกอบธุรกิจที่มีภารกิจ หรือให้บริการในลักษณะเดียวกันหรือคล้ายคลึงกันก็ได้ ทั้งนี้ ให้หน่วยงานควบคุมหรือกำกับดูแลเป็นผู้แจ้งการจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยตามแนวทางที่กำหนดในประกาศฉบับนี้

ให้ศูนย์ประสานการรักษาความมั่นคงปลอดภัยที่จัดตั้งขึ้นนั้นมีหน้าที่และความรับผิดชอบในด้านการประสานงาน เฝ้าระวัง รับมือ และแก้ไขภัยคุกคามทางไซเบอร์ให้แก่หน่วยงาน CII ตลอดจนมีหน้าที่ในการช่วยเหลือ สนับสนุน หรือปฏิบัติงานร่วมกับสำนักงาน หน่วยงานควบคุมหรือกำกับดูแล พนักงานเจ้าหน้าที่ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

นอกจากนี้ ในการดำเนินการจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยนั้น ควรมีการกำหนดภารกิจหรือให้บริการของศูนย์ประสานการรักษาความมั่นคงปลอดภัยและบันทึกไว้เป็นลายลักษณ์อักษรในพันธกิจ (mission statement) ของศูนย์ประสานการรักษาความมั่นคงปลอดภัยดังกล่าว โดยพันธกิจนั้นจะต้องกำหนดวัตถุประสงค์และขอบเขตภารกิจหรือให้บริการของศูนย์ประสานการรักษาความมั่นคงปลอดภัยให้ชัดเจนและต้องมีสาระสำคัญอย่างน้อย ดังต่อไปนี้

ภารกิจหรือให้บริการของศูนย์ประสานการรักษาความมั่นคงปลอดภัย

๕. ให้ศูนย์ประสานการรักษาความมั่นคงปลอดภัยมีภารกิจหรือให้บริการที่เกี่ยวข้องกับการประสานงาน เฝ้าระวัง รับมือ และแก้ไขภัยคุกคามทางไซเบอร์ให้แก่หน่วยงาน CII เพื่อปกป้องหน่วยงานดังกล่าว ตลอดจนโครงสร้างพื้นฐานสำคัญทางสารสนเทศและระบบงานที่มีความสำคัญอื่น ๆ จากภัยคุกคามทางไซเบอร์ที่อาจกระทบต่อภารกิจหรือการให้บริการของหน่วยงาน CII โดยภารกิจหรือให้บริการของศูนย์ประสานการรักษาความมั่นคงปลอดภัยนั้น สามารถแบ่งออกเป็น ๔ ด้าน ดังนี้

- ภารกิจหรือให้บริการในด้านการประสานงาน
- ภารกิจหรือให้บริการในด้านการเฝ้าระวังภัยคุกคามทางไซเบอร์
- ภารกิจหรือให้บริการในด้านการรับมือและแก้ไขภัยคุกคามทางไซเบอร์
- ภารกิจหรือให้บริการในด้านการดำเนินมาตรการด้านการบริหารจัดการคุณภาพ

ทั้งนี้ ให้ภารกิจหรือให้บริการในแต่ละด้านของศูนย์ประสานการรักษาความมั่นคงปลอดภัย มีรายละเอียดอย่างน้อยดังต่อไปนี้ และในกรณีที่ศูนย์ประสานการรักษาความมั่นคงปลอดภัยใดมีความพร้อม อาจพิจารณาดำเนินภารกิจหรือจัดให้มีบริการเพิ่มเติมแก่หน่วยงาน CII โดยมีรายละเอียดปรากฏตามที่ระบุไว้ในภาคผนวก แนบท้ายนี้ทั้งหมดหรือบางส่วนก็ได้

ภารกิจหรือให้บริการในด้านการประสานงาน

๕.๑ ให้ศูนย์ประสานการรักษาความมั่นคงปลอดภัยประสานความร่วมมือกับศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติในการปฏิบัติหน้าที่ด้านการเฝ้าระวัง รับมือ และแก้ไขภัยคุกคามทางไซเบอร์ให้แก่หน่วยงาน CII ตลอดจนให้การช่วยเหลือ สนับสนุน หรือปฏิบัติงานร่วมกับศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติในการดำเนินภารกิจหรือให้บริการ ซึ่งรวมถึงแต่ไม่จำกัดเฉพาะการดำเนินมาตรการเชิงรุกเพื่อป้องกันและเฝ้าระวังความเสี่ยงในการเกิดภัยคุกคามทางไซเบอร์ การดำเนินมาตรการเชิงรับเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น และการดำเนินมาตรการด้านการบริหารจัดการคุณภาพเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ เป็นต้น และควรให้ความสำคัญกับการแบ่งปันข้อมูลที่เกี่ยวข้องเพื่อประโยชน์ในการเฝ้าระวัง รับมือ และแก้ไขภัยคุกคามทางไซเบอร์

นอกจากนี้ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยอาจร่วมมือกับหน่วยงานอื่น ๆ ที่ดำเนินภารกิจหรือให้บริการเกี่ยวกับการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ให้แก่หน่วยงานที่มีภารกิจหรือให้บริการในลักษณะเดียวกันหรือมีความเกี่ยวข้องกันกับหน่วยงาน CII เพื่อช่วยยกระดับความสามารถในการดำเนินภารกิจหรือให้บริการด้านต่าง ๆ ของศูนย์ประสานการรักษาความมั่นคงปลอดภัย ตลอดจนการปฏิบัติหน้าที่ในการเฝ้าระวัง รับมือ และแก้ไขภัยคุกคามทางไซเบอร์

ภารกิจหรือให้บริการในด้านการเฝ้าระวังภัยคุกคามทางไซเบอร์

๕.๒ ให้ศูนย์ประสานการรักษาความมั่นคงปลอดภัยดำเนินการเฝ้าระวังความเสี่ยงในการเกิดภัยคุกคามทางไซเบอร์ให้แก่หน่วยงาน CII ดังต่อไปนี้

๕.๒.๑ เฝ้าระวังความเสี่ยงและติดตามแนวโน้มของการเกิดภัยคุกคามทางไซเบอร์ในรูปแบบต่าง ๆ รวมถึงดำเนินการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้น หรือให้คำเตือนเกี่ยวกับช่องโหว่ที่อาจถูกใช้เป็นช่องทางในการก่อภัยคุกคามทางไซเบอร์ เพื่อให้หน่วยงาน CII ดำเนินการป้องกันโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และระบบงานที่มีความสำคัญอื่น ๆ ได้อย่างทันท่วงที

๕.๒.๒ วิเคราะห์และตรวจสอบข่าวกรองเกี่ยวกับภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้น รวมถึงการเผยแพร่ข้อมูลที่มีความจำเป็นเพื่อให้หน่วยงาน CII สามารถดำเนินมาตรการป้องกันหรือจัดการกับสถานการณ์ด้านภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้น เช่น การให้คำแนะนำแก่หน่วยงาน CII ในการตรวจจับเหตุการณ์ที่อาจนำมาสู่การบุกรุก และการวิเคราะห์ข้อมูล เป็นต้น

เพื่อประโยชน์ในการเฝ้าระวังและแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์ ให้ศูนย์ประสานการรักษาความมั่นคงปลอดภัยดำเนินการเพื่อให้มีการรับลงทะเบียนข้อมูลและจัดทำบัญชีช่องทางการติดต่อ (point of contact) ของหน่วยงาน CII เพื่อใช้เป็นช่องทางหลักในการติดต่อสื่อสารระหว่างศูนย์ประสานการรักษาความมั่นคง

ปลอดภัยกับหน่วยงานดังกล่าว และจัดทำรายชื่อของหน่วยงาน CII รวมถึงโครงสร้างพื้นฐานสำคัญทางสารสนเทศและระบบงานที่มีความสำคัญอื่น ๆ ที่หน่วยงาน CII ใช้ในการดำเนินภารกิจหรือให้บริการในกิจการของตน ซึ่งจำเป็นต้องมีการเฝ้าระวัง หรือดำเนินการป้องกัน รับมือ และแก้ไขภัยคุกคามทางไซเบอร์ และปรับปรุงข้อมูลดังกล่าว ให้เป็นปัจจุบันอยู่เสมอ

ภารกิจหรือให้บริการในด้านการรับมือและแก้ไขภัยคุกคามทางไซเบอร์

๕.๓ ให้ศูนย์ประสานการรักษาความมั่นคงปลอดภัยดำเนินการรับมือและแก้ไขภัยคุกคามทางไซเบอร์ที่เกิดขึ้นแก่หน่วยงาน CII ดังต่อไปนี้

๕.๓.๑ เป็นศูนย์กลางในการรับและแจ้งเหตุเกี่ยวกับภัยคุกคามทางไซเบอร์เพื่อตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ ตลอดจนให้การสนับสนุนข้อมูลต่าง ๆ ที่จำเป็นต่อหน่วยงาน CII เพื่อดำเนินการแก้ไขเหตุภัยคุกคามทางไซเบอร์ โดยจัดให้มีช่องทางในการรับและแจ้งเหตุผ่านระบบอิเล็กทรอนิกส์ที่กำหนดขึ้นโดยเฉพาะหรือช่องทางอื่นใดตามที่ศูนย์ประสานการรักษาความมั่นคงปลอดภัยกำหนด

๕.๓.๒ ให้การช่วยเหลือ แนะนำ หรือสนับสนุนหน่วยงาน CII ในการตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้น และปฏิบัติงานร่วมกับหน่วยงานควบคุมหรือกำกับดูแลในการตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ดังกล่าว

๕.๓.๓ เมื่อศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติแจ้งการเปลี่ยนแปลงระดับ หรือยกระดับการแจ้งเตือน หรือเมื่อศูนย์ประสานการรักษาความมั่นคงปลอดภัยพบการเปลี่ยนแปลงลักษณะของภัยคุกคามทางไซเบอร์หรือผลกระทบต่อภารกิจ หรือการให้บริการของหน่วยงาน CII ให้ศูนย์ประสานการรักษาความมั่นคงปลอดภัยแจ้งการเปลี่ยนแปลง หรือดำเนินการแจ้งเตือนไปยังหน่วยงาน CII เพื่อให้หน่วยงานดังกล่าวเตรียมความพร้อมในการตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์

ในการดำเนินการรับมือและแก้ไขภัยคุกคามทางไซเบอร์ที่เกิดขึ้น ให้ศูนย์ประสานการรักษาความมั่นคงปลอดภัยให้การช่วยเหลือ สนับสนุน หรือปฏิบัติงานร่วมกับสำนักงาน หน่วยงานควบคุมหรือกำกับดูแลพนักงานเจ้าหน้าที่ ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

ภารกิจหรือให้บริการในด้านการดำเนินมาตรการด้านการบริหารจัดการคุณภาพเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์

๕.๔ ให้ศูนย์ประสานการรักษาความมั่นคงปลอดภัยดำเนินมาตรการด้านการบริหารจัดการคุณภาพเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ให้แก่หน่วยงาน CII ที่อยู่ภายใต้การดูแล โดยมีหน้าที่และความรับผิดชอบดังต่อไปนี้

๕.๔.๑ ผลักดันและสนับสนุนการสร้างความตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ เพื่อนำไปสู่การดำเนินมาตรการในการป้องกันและการรักษาความมั่นคงปลอดภัยไซเบอร์

๕.๔.๒ ผลักดันและสนับสนุนการเพิ่มความรู้ความสามารถของหน่วยงาน CII เพื่อเตรียมความพร้อมในการปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และสามารถยกระดับการป้องกันโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และระบบงานที่มีความสำคัญอื่น ๆ

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยอาจดำเนินการจัดให้มีการฝึกอบรมและให้ความรู้แก่หน่วยงาน CII เพื่อสร้างความตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Education Training and Awareness หรือ “ETA”) เช่น การวางแผนรับมือในสถานการณ์ที่ต้องเผชิญเหตุภัยคุกคามทางไซเบอร์หรือการยกระดับการรักษาความมั่นคงปลอดภัยไซเบอร์ เป็นต้น

การขอผ่อนผันภารกิจหรือให้บริการของศูนย์ประสานการรักษาความมั่นคงปลอดภัย

๖. ในระยะเริ่มต้นของการจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัย หากศูนย์ประสานการรักษาความมั่นคงปลอดภัยในด้านใดยังไม่สามารถดำเนินภารกิจหรือให้บริการได้ครบถ้วนตามที่กำหนดแนบท้ายประกาศนี้ ให้หน่วยงานดังกล่าวหารือร่วมกับหน่วยงานควบคุมหรือกำกับดูแล เพื่อพิจารณากำหนดแนวทางการเริ่มต้นภารกิจหรือให้บริการของศูนย์ประสานการรักษาความมั่นคงปลอดภัย โดยอาจจัดทำแผนการปฏิบัติงานโดยแบ่งเป็นระยะต่าง ๆ ตามระดับความสำคัญและความพร้อมของหน่วยงาน และนำเสนอต่อสำนักงานเพื่อให้สำนักงานรายงานแผนการปฏิบัติงานดังกล่าวต่อคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเพื่อพิจารณาต่อไป

ภาคผนวก
ภารกิจหรือให้บริการที่ศูนย์ประสานการรักษาความมั่นคงปลอดภัย
อาจจัดให้มีเพิ่มเติมเพื่อให้บริการแก่หน่วยงาน CII ที่อยู่ภายใต้การดูแล

เมื่อมีความพร้อม ศูนย์ประสานการรักษาความมั่นคงปลอดภัยอาจพิจารณาดำเนินภารกิจหรือให้บริการเพิ่มเติมแก่หน่วยงาน CII ปรากฏตามรายละเอียดที่ระบุในภาคผนวกนี้ โดยอาจพิจารณาดำเนินการทั้งหมดหรือบางส่วนก็ได้

๑. จัดให้มีภารกิจหรือให้บริการเพิ่มเติมเพื่อป้องกันและเฝ้าระวังความเสี่ยงในการเกิดภัยคุกคามทางไซเบอร์ เช่น

(ก) การจัดให้มีกลไกหรือกระบวนการทำงานที่เหมาะสมในการตรวจจับการเกิดภัยคุกคามทางไซเบอร์ หรืออาจใช้การวิเคราะห์ข้อมูลที่ได้รับจากศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ เพื่อเฝ้าระวังความเสี่ยงและประเมินแนวโน้มของการเกิดภัยคุกคามทางไซเบอร์ในรูปแบบต่าง ๆ

(ข) การติดตามความก้าวหน้าด้านเทคโนโลยีเพื่อจัดทำข้อเสนอแนะเกี่ยวกับการป้องกันภัยคุกคามทางไซเบอร์หรือแนวปฏิบัติพื้นฐาน (baseline) ที่เกี่ยวข้องให้แก่หน่วยงาน CII เพื่อใช้เป็นแนวทางในการป้องกันหรือเตรียมความพร้อมในการรับมือเมื่อได้รับการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์

(ค) การให้ความช่วยเหลือ แนะนำ และสนับสนุนในการดำเนินมาตรการป้องกันตามแนวทางปฏิบัติที่ดี (best practice) เพื่อให้หน่วยงาน CII สามารถเตรียมความพร้อมในการรับมือเมื่อได้รับการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์

(ง) การประเมินความเสี่ยงและช่องโหว่ที่อาจถูกใช้ในการก่อภัยคุกคามทางไซเบอร์เพื่อนำไปสู่การจัดการช่องโหว่ การดำเนินมาตรการป้องกัน หรือกระทำการอื่นใดเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์เมื่อได้รับการร้องขอจากหน่วยงาน CII

(จ) การดำเนินการอื่นใดที่เกี่ยวข้องเพื่อตรวจสอบโปรแกรม หรือค้นหาสิ่งที่ไม่พึงประสงค์ (malicious code) ซึ่งอาจเป็นอันตรายต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หรือระบบงานที่มีความสำคัญอื่น ๆ หรืออาจให้ความช่วยเหลือแก่หน่วยงาน CII ในการดำเนินการดังกล่าว เป็นต้น

๒. จัดให้มีภารกิจหรือให้บริการเพิ่มเติมเพื่อรับมือและแก้ไขภัยคุกคามทางไซเบอร์ เช่น

(ก) การให้ความช่วยเหลือ แนะนำ และสนับสนุนหน่วยงาน CII เกี่ยวกับวิธีการในการบรรเทาผลกระทบและแผนการฟื้นฟูเพื่อให้หน่วยงาน CII สามารถกลับมาดำเนินภารกิจหรือให้บริการได้ต่อไปภายหลังการระงับเหตุภัยคุกคามทางไซเบอร์เสร็จสิ้น

(ข) การให้ความช่วยเหลือ แนะนำ และสนับสนุนหน่วยงาน CII ในการดำเนินกระบวนการทางนิติวิทยาศาสตร์ การตรวจพิสูจน์พยานหลักฐานทางดิจิทัล การเชื่อมโยงข้อมูลภัยคุกคามทางไซเบอร์จากแหล่งข้อมูลต่าง ๆ ตลอดจนการสืบสวนหรือสอบสวนเกี่ยวกับการกระทำความผิดที่เกี่ยวข้องกับการก่อภัยคุกคามทางไซเบอร์ เป็นต้น

๓. จัดให้มีภารกิจหรือให้บริการเพิ่มเติมเพื่อดำเนินมาตรการด้านการบริหารจัดการคุณภาพเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ เช่น

(ก) ผลักดันและสนับสนุนหน่วยงาน CII ในการจัดทำแผนความต่อเนื่องของการดำเนินงาน (business continuity plan) เพื่อรับมือในกรณีที่เกิดเหตุภัยคุกคามทางไซเบอร์ แผนการป้องกันโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (critical information infrastructure protection plan) และแผนฟื้นฟู (disaster recovery plan) ภายหลังเกิดภัยคุกคามทางไซเบอร์

(ข) ผลักดันและสนับสนุนหน่วยงาน CII ในการประเมินความเสี่ยงของการเกิดภัยคุกคามทางไซเบอร์ โดยอาจดำเนินการตรวจสอบความมั่นคงปลอดภัย (security assessments) ของโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หรือระบบงานที่มีความสำคัญอื่น ๆ ด้วยวิธีการต่าง ๆ และให้คำแนะนำเพื่อยกระดับคุณภาพของการดำเนินมาตรการป้องกันและการรักษาความมั่นคงปลอดภัยไซเบอร์ให้มีความแข็งแกร่งมากขึ้น เป็นต้น



ฉบับภาษาอังกฤษ
English Version

Notification of the National Cyber Security Committee

Re: Characteristics, Duties, and Responsibilities of the Computer Emergency Response Team for Organizations of Critical Information Infrastructure and Related Missions and Services

B.E. 2564 (2021)

Whereas the Cybersecurity Act B.E. 2562 (2019) stipulates that the National Cyber Security Committee prescribes the characteristics, duties, and responsibilities of the Computer Emergency Response Team for Organizations of Critical Information Infrastructure to coordinate, monitor, handle, and mitigate cyber incidents. The Committee may prescribe Government Agencies that are ready or the Regulator of Organizations of Critical Information Infrastructure to perform such duties for the Organizations of Critical Information Infrastructure, either in full or in part. In addition, the Committee shall prescribe the Computer Emergency Response Team's missions and services for Organizations of Critical Information Infrastructure.

By Virtue of Section 50 of the Cybersecurity Act B.E. 2562 (2019), together with the resolution of the National Cyber Security Committee meeting no. 1/2564 on 25 June B.E. 2564 (2021), the National Cyber Security Committee hereby issues the following notification:

Clause 1 This notification shall be called the "Notification of the National Cyber Security Committee Re: Characteristics, Duties, and Responsibilities of the Computer Emergency Response Team for Organizations of Critical Information Infrastructure and Related Missions and Services B.E. 2564 (2021)".

Clause 2 This notification shall come into force one year after the date of its publication in the Royal Thai Government Gazette.

Clause 3 Government Agencies that are ready or the Regulators of Organizations of Critical Information Infrastructure in each sector shall establish or take action to ensure the existence of the Computer Emergency Response Team for the Organizations of Critical Information Infrastructure. The Regulator may prescribe rules, criteria, and guidelines in considering the characteristics and suitability of the Computer Emergency Response Team for Organizations of Critical Information Infrastructure.

The Computer Emergency Response Team for Organizations of Critical Information Infrastructure in paragraph one shall have characteristics, duties, and

responsibilities, including missions and services, no less than the prescription in the attached enclosure of this notification.

Clause 4 When a Computer Emergency Response Team for Organizations of Critical Information Infrastructure is established, the Regulator shall notify the establishment, together with the list of its constituents and other related information, to the National Cyber Security Agency within thirty days from the effective date of this notification.

If there is an establishment of an additional Computer Emergency Response Team for Organizations of Critical Information Infrastructure, or there is any change related to the Computer Emergency Response Team for Organizations of Critical Information Infrastructure, the Regulator shall notify the additional establishment or the change, together with any related information, to the National Cyber Security Agency within thirty days after the completion of such establishment or change.

The National Cyber Security Agency shall report the establishment of the Computer Emergency Response Team for Organizations of Critical Information Infrastructure in paragraph one to the National Cyber Security Committee. The Committee may provide additional suggestions or comments.

Clause 5 In the absence of Government Agencies ready to perform the duties of the Computer Emergency Response Team for Organizations of Critical Information Infrastructure, the Government Agencies shall notify the cause of or the reason for their unreadiness to their Regulator so that the Regulator can coordinate with the National Cyber Security Agency in determining an appropriate solution for an effort to coordinate, monitor, handle, and mitigate cyber incidents for the Organizations of Critical Information Infrastructure.

Given on the 11th of August B.E. 2564 (2021)

General Pravit Wongsuwan

(Pravit Wongsuwan)

Deputy Prime Minister as

Chairman of the National Cyber Security Committee

Characteristics, Duties, and Responsibilities of the Computer Emergency Response Team for Organizations of Critical Information Infrastructure and Related Missions and Services

B.E. 2564 (2021)

1.	Sectoral CERT	means	the Computer Emergency Response Team for Organizations of Critical Information Infrastructure
2.	CII	means	the Organization of Critical Information Infrastructure under the supervision of Sectoral CERT
3.	Agency	means	the National Cyber Security Agency

Characteristics, Duties, and Responsibilities of Sectoral CERT

4. A Sectoral CERT may be established as an independent unit with its own management system. Alternatively, it may be part of the Organization that is responsible for the Sectoral CERT establishment, or under the supervision of the Government Agency or the Regulator of the CIIs in each sector. Alternatively, a Sectoral CERT may be established as a consortium of agencies or businesses that share similar missions or services. Nonetheless, the Regulator shall be responsible for notifying the establishment of the Sectoral CERT according to the direction prescribed in this notification.

Established Sectoral CERTs shall have duties and responsibilities in coordinating, monitoring, handling, and mitigating cyber incidents for their CIIs. The Sectoral CERTs shall be responsible for providing aid, support, and collaboration for the Agency, the Regulators, and the Competent Officials in accordance with the Cybersecurity Act B.E. 2562 (2019).

In addition, in the establishment process, the missions and services of the Sectoral CERT should be prescribed in a written mission statement. The statement shall clearly state the objectives and the scope of missions and services of the Sectoral CERT, which shall cover at least the following key elements:

Missions and Services of Sectoral CERTs

5. Sectoral CERTs' missions or services shall involve coordinating, monitoring, handling, and mitigating cyber incidents for the CIIs with the aim to protect the CIIs, other critical information infrastructures, and critical systems from cyber incidents that may affect the CII's missions and services. The missions and services of the Sectoral CERTs may be categorized into 4 areas:

- coordination missions or services;
- threat monitoring missions or services;
- incident handling and mitigation missions or services;
- quality management missions or services.

Each area of missions or services of Sectoral CERTs shall contain the following details. If any Sectoral CERTs are ready, they may consider fulfilling further missions or services for the CII as set out in the appendix of the attached enclosure, either in full or in part.

Coordination Missions or Services

5.1 Sectoral CERTs shall coordinate with Thailand Computer Emergency Response Team in monitoring, handling, and mitigating cyber incidents for the CII. They shall also aid, support and collaborate with Thailand Computer Emergency Response Team in carrying out missions or delivering services that may include but are not limited to implementing proactive measures for preventing and monitoring cybersecurity risks, reactive measures for handling cyber incidents, and quality management measures for ensuring cybersecurity. Moreover, Sectoral CERTs should emphasize sharing relevant information to facilitate monitoring, handling and mitigating cyber incidents.

In addition, Sectoral CERTs may coordinate with other agencies that share similar missions or provide cybersecurity services to agencies with the same or similar missions or services, or to those that are related to the CII. This coordination aims at improving capabilities of Sectoral CERTs to fulfil its missions or services and perform duties in monitoring, handling, and mitigating cyber incidents.

Threat Monitoring Missions or Services

5.2 Sectoral CERTs shall monitor cybersecurity risks for the CIIs, as detailed in the following:

5.2.1 Sectoral CERTs shall monitor cybersecurity risks, track trends of various cyber threats, and issue a warning regarding potential threats or vulnerabilities that may be exploited in a cyberattack, with the aim of enabling the CIIs to protect their critical information infrastructures and other critical systems in a timely manner;

5.2.2 Sectoral CERTs shall verify threat intelligence related to potential incidents. Sectoral CERTs shall also share necessary information with the CIIs so they can implement proactive measures or handle cyber incidents. For example, Sectoral CERTs may advise the CIIs about how to detect incidents that may lead to an intrusion or about information analysis.

To assist in monitoring and warning of cyber threats, Sectoral CERTs shall set up an information registration service and collect points of contact of the CIIs to be used as a main communication channel between each Sectoral CERT and its CIIs. Sectoral CERTs shall also compile a list of CIIs, as well as other critical information infrastructures and critical systems utilized by the CIIs to carry out their missions or services, which require an effort to monitor, prevent, handle, and mitigate cyber incidents. Sectoral CERTs shall ensure that the information in this paragraph shall be updated regularly.

Incident Handling and Mitigation Missions or Services

5.3 Sectoral CERTs shall handle and mitigate a cyber incident that has occurred to the CII in the following manner:

5.3.1 Sectoral CERTs shall be the centers of incident reporting and notification to respond to and handle the incident and provide necessary information to the CII to mitigate the incident. Sectoral CERTs shall establish channels for incidents to be reported and notified through specifically dedicated electronic systems or through other communication means;

5.3.2 Sectoral CERTs shall aid, advise or support the CII in responding to and handling the incident that has occurred. Sectoral CERTs shall also collaborate with the Regulator in responding to and handling the incident;

5.3.3 when Thailand Computer Emergency Response Team notifies the change in or the escalation of the criticality level of the incident, or when Sectoral CERTs discover a change in the characteristics of the cyber incident or its impact on the missions or services of the CII, the Sectoral CERTs shall notify the changes or issue the CII a warning so it could make a preparation for responding to and handling the cyber incident.

In handling and mitigating the incident that has occurred, the Sectoral CERTs shall aid, support, or collaborate with the Agency, the Regulator, and the Competent Officials under the Cybersecurity Act B.E. 2562 (2019).

Quality Management Missions or Services

5.4 Sectoral CERTs shall implement cybersecurity quality management measures for the CIIs under their supervision. Sectoral CERTs shall have the following duties and responsibilities:

5.4.1 Sectoral CERTs shall drive and support efforts to raise awareness regarding cyber threats, which will lead to the implementation of cybersecurity measures;

5.4.2 Sectoral CERTs shall drive and support efforts to elevate the knowledge and capability of the CIIs for cybersecurity operations and for further enhancing the protection capability for their critical information infrastructures and other critical systems.

To raise cybersecurity awareness, Sectoral CERTs may organize an Education Training and Awareness (ETA) for the CIIs. The ETA may include incident response planning or elevation of cybersecurity measures.

Request of Deference of Missions or Services of Sectoral CERTs

6. During the initial phase of its establishment, the Sectoral CERT in any sector shall consult with the Regulator if it is not prepared to carry out any missions or services in full as prescribed in the attached enclosure of this notification. The discussion shall entail the effort to determine the direction for its missions or services' initial launch. The Sectoral CERT may prepare an action plan containing phases of actions according to the priority and its readiness and present the action plan to the Agency who will report the action plan to the National Cyber Security Committee for further consideration.

Appendix

Further Missions or Additional Services that Sectoral CERTs may provide for the CIIs under their supervision

---

When ready, Sectoral CERTs may consider carrying out further missions or providing additional services for the CII as indicated in this appendix in part or in whole.

1. Sectoral CERTs may carry out further missions or providing additional services in preventing and monitoring the cybersecurity risks such as the following:

(a) Sectoral CERTs may provide mechanisms or processes appropriate for detecting cyber incidents. Sectoral CERTs may analyze information from Thailand Computer Emergency Response Team to monitor the risks and determine the occurrence trends of various forms of cyber incidents;

(b) Sectoral CERTs may follow news of technological advancements and provide cybersecurity recommendations or related baselines to the CIIs who may use them as guidelines for incident prevention and response preparation when notified of an incident;

(c) Sectoral CERTs may aid, advise, and support in implementing a preventive measure based on best practices so that the CIIs can prepare for response when notified of an incident;

(d) Sectoral CERTs may assess the risks and vulnerabilities that may be exploited in a cyberattack so that those vulnerabilities may be managed and that any preventive measure or any cybersecurity activities requested by the CIIs may be carried out;

(e) Sectoral CERTs may conduct any other activities related to application testing or scanning for malicious codes or vulnerabilities that may harm the critical information infrastructures or other critical systems or may aid the CIIs in carrying out such actions.

2. Sectoral CERTs may carry out further missions or provide additional services to handle and mitigate cyber incidents. For example,

(a) Sectoral CERTs may provide assistance, advice, and support to the CIIs regarding the impact mitigation methods and the recovery plan so that the CIIs can resume their normal mission or service after the incident is contained;

(b) Sectoral CERTs may provide assistance, advice, and support to the CIIs in areas such as forensic science, digital forensics, correlation of incident information obtained from various sources, and investigation of any delinquency related to cyber incidents.

3. Sectoral CERTs may provide further missions or additional services to implement cybersecurity quality management measures. For example,

(a) Sectoral CERTs may drive and support the CIIs in developing a business continuity plan for handling cyber incidents, a critical information infrastructure protection plan, and a post-incident disaster recovery plan;

(b) Sectoral CERTs may drive and support the CIIs in assessing cybersecurity risks and conducting a cybersecurity assessment of their critical information infrastructures or other critical systems and provide advice to raise the quality of cybersecurity measures.

4

ประกาศ กมช.

เรื่อง หลักเกณฑ์ ลักษณะหน่วยงานที่มีภารกิจ
หรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญ
ทางสารสนเทศและการมอบหมายการควบคุมและกำกับดูแล
พ.ศ. 2568

มีผลใช้บังคับตั้งแต่วันที่ 17 ก.ย. 68 เป็นต้นไป

Notification of NCSC

Re: Criteria and Characteristics for Designating Agencies with Missions or Services as Critical Information Infrastructure organizations and the Regulation Assignment, B.E. 2568 (2025)

effective from September 17, 2025, onwards.



ฉบับภาษาไทย
Thai Version

ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

เรื่อง หลักเกณฑ์ ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการ
เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการมอบหมายการควบคุมและกำกับดูแล
พ.ศ. ๒๕๖๘

ตามที่มีการเปลี่ยนแปลงหน่วยงานควบคุมหรือกำกับดูแลและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้มีความทันสมัย จึงเห็นสมควรมีการปรับปรุงประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง การกำหนดหลักเกณฑ์ ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการมอบหมายการควบคุมและกำกับดูแล พ.ศ. ๒๕๖๔ ให้สอดคล้องกับลักษณะหน่วยงานที่มีภารกิจหรือให้บริการในปัจจุบัน

อาศัยอำนาจตามความในมาตรา ๙ (๘) มาตรา ๔๙ และมาตรา ๕๑ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ประกอบมติที่ประชุมคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ครั้งที่ ๓/๒๕๖๘ เมื่อวันที่ ๒๙ สิงหาคม ๒๕๖๘ คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ จึงออกประกาศไว้ ดังนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง การกำหนดหลักเกณฑ์ ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการมอบหมายการควบคุมและกำกับดูแล พ.ศ. ๒๕๖๘”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ข้อ ๓ ให้ยกเลิกประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง การกำหนดหลักเกณฑ์ ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการมอบหมายการควบคุมและกำกับดูแล พ.ศ. ๒๕๖๔

ข้อ ๔ ในประกาศนี้

“ประธาน กมช.” หมายความว่า ประธานกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

“กมช.” หมายความว่า คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

“สำนักงาน” หมายความว่า สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

“หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ” หมายความว่า หน่วยงานของรัฐหรือหน่วยงานเอกชน ซึ่งมีภารกิจหรือให้บริการโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

“หน่วยงานควบคุมหรือกำกับดูแล” หมายความว่า หน่วยงานของรัฐ หน่วยงานเอกชน หรือบุคคลซึ่งมีกฎหมายกำหนดให้มีหน้าที่และอำนาจในการควบคุมหรือกำกับดูแลการดำเนินกิจการของหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

ข้อ ๕ ให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง การกำหนดหลักเกณฑ์ ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการมอบหมายการควบคุมและกำกับดูแล พ.ศ. ๒๕๖๔ ยังคงมีสถานะเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศอยู่ จนกว่า กมช. จักดำเนินการกำหนดหน่วยงานที่มีภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามประกาศฉบับนี้แล้วเสร็จ

ข้อ ๖ ในกรณีที่หน่วยงานมีภารกิจหรือการให้บริการในด้านต่าง ๆ ตามที่กำหนดไว้ในแนบท้ายประกาศนี้ อาจถือได้ว่าหน่วยงานนั้น เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หากมีลักษณะอย่างหนึ่งอย่างใด ดังต่อไปนี้

(๑) กรณีที่มีภัยคุกคามทางไซเบอร์เกิดขึ้นกับภารกิจหรือบริการของหน่วยงานแล้วจะก่อให้เกิดผลกระทบต่อการให้บริการของโครงสร้างพื้นฐานสำคัญของประเทศ ความมั่นคงของรัฐ ความสัมพันธ์ระหว่างประเทศ การป้องกันประเทศ เศรษฐกิจ การสาธารณสุข ความปลอดภัยสาธารณะ หรือความสงบเรียบร้อยของประชาชน หรืออาจนำมาซึ่งผลกระทบด้านสิ่งแวดล้อม

(๒) กรณีที่มีภัยคุกคามทางไซเบอร์เกิดขึ้นกับภารกิจหรือบริการของหน่วยงานแล้วจะส่งผลกระทบต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศของหน่วยงานอื่น

(๓) กรณีที่หน่วยงานมีภารกิจหรือบริการเฉพาะด้านที่ถือเป็นบริการสำคัญของชาติหรือเกิดขึ้นตามนโยบายของรัฐและเป็นภารกิจหรือบริการหลักของหน่วยงานนั้น ๆ ซึ่งหากไม่สามารถแก้ไขหรือหาช่องทางอื่นมาดำเนินการทดแทนได้ทันการณ์อาจก่อให้เกิดผลกระทบต่อร่างกาย อนามัยความปลอดภัยในชีวิตและทรัพย์สินหรือกระทบต่อการปฏิบัติงานหรือการดำรงชีวิตของประชาชน หรือกระทบต่อความมั่นคงทางเศรษฐกิจของประเทศ เป็นต้น

ข้อ ๗ ให้หน่วยงานควบคุมหรือกำกับดูแลที่กำหนดไว้ตามแนบท้ายประกาศนี้เป็นหน่วยงานที่ได้รับมอบหมายให้ควบคุมและกำกับดูแลด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แก่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

ข้อ ๘ หน่วยงานควบคุมหรือกำกับดูแลที่กำหนดไว้ในแต่ละด้าน ตามแนบท้ายประกาศนี้ต้องพิจารณาจัดทำบัญชีรายชื่อหน่วยงานที่อยู่ภายใต้การดูแลของตนที่เข้าข่ายเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยพิจารณาจากรายละเอียดของลักษณะหน่วยงานที่มีภารกิจหรือให้บริการตามแนบท้ายประกาศนี้ และมีหนังสือแจ้งไปยังสำนักงาน

ให้สำนักงาน เสนอบัญชีรายชื่อหน่วยงานในแต่ละด้านตามวรรคหนึ่ง ต่อ กมช. เพื่อพิจารณากำหนดเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

เมื่อ กมช. กำหนดหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ตามวรรคสองแล้ว ให้สำนักงาน แจ้งไปยังหน่วยงานควบคุมหรือกำกับดูแลเพื่อดำเนินการแจ้งหน่วยงานนั้น ๆ ให้ทราบถึงสถานะการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

การดำเนินการตามวรรคหนึ่ง ให้หน่วยงานควบคุมหรือกำกับดูแลดำเนินการให้แล้วเสร็จภายในเก้าสิบวันนับแต่วันที่ประกาศนี้ใช้บังคับ

ข้อ ๙ ให้นำความในข้อ ๘ มาใช้บังคับกับกรณีมีการเปลี่ยนแปลงบัญชีรายชื่อหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยอนุโลม

ข้อ ๑๐ กรณีที่หน่วยงานมีข้อสงสัยหรือข้อโต้แย้งเกี่ยวกับลักษณะหน่วยงานที่มีภารกิจหรือให้บริการในด้านที่กำหนดไว้แนบท้ายประกาศนี้ ให้มีหนังสือแจ้งข้อสงสัยหรือข้อโต้แย้งไปยังสำนักงาน

ภายหลังสำนักงานได้รับหนังสือตามวรรคหนึ่ง ให้เสนอข้อสงสัยหรือข้อโต้แย้งของหน่วยงานแล้วแต่กรณี ไปยัง กมช. เพื่อวินิจฉัยชี้ขาด

เมื่อ กมช. วินิจฉัยชี้ขาด ตามวรรคสองแล้วผลเป็นประการใดให้สำนักงานมีหนังสือแจ้งผลการวินิจฉัยชี้ขาดไปยังหน่วยงานโดยเร็ว

ข้อ ๑๑ การใดที่ได้ดำเนินการไปก่อนวันที่ประกาศนี้ ใช้บังคับและยังดำเนินการไม่แล้วเสร็จให้ดำเนินการต่อไปตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง การกำหนดหลักเกณฑ์ ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการมอบหมายการควบคุมและกำกับดูแล พ.ศ. ๒๕๖๔ จนกว่าจะแล้วเสร็จ

ข้อ ๑๒ ให้ประธาน กมช. รักษาการตามประกาศนี้ และให้มีอำนาจออกประกาศ คำสั่ง หลักเกณฑ์และวิธีการเพื่อปฏิบัติตามประกาศนี้

ในกรณีมีปัญหาเกี่ยวกับการปฏิบัติตามประกาศนี้ หรือประกาศนี้ไม่ได้กำหนดเรื่องใดไว้ ให้ประธาน กมช. เป็นผู้มีอำนาจตีความและวินิจฉัยชี้ขาด ทั้งนี้ การตีความและคำวินิจฉัยชี้ขาดของประธาน กมช. ให้ถือเป็นที่สุด

ประกาศ ณ วันที่ ๙ กันยายน พ.ศ. ๒๕๖๘
ประเสริฐ จันทรรวงทอง
รองนายกรัฐมนตรี
ประธานกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการ
เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการมอบหมายการควบคุมและกำกับดูแล

หมวด ๑
ด้านความมั่นคงของรัฐ

ลักษณะหน่วยงาน	ภารกิจหรือให้บริการ (Critical Services)	หน่วยงานควบคุมหรือกำกับดูแล (Regulator)
ข้อ ๑ ที่มีภารกิจเกี่ยวข้องกับการป้องกันประเทศ	ภารกิจด้านการพัฒนาศักยภาพการป้องกันประเทศ	สำนักงานปลัดกระทรวงกลาโหม
ข้อ ๒ ที่มีภารกิจเกี่ยวข้องกับการบังคับใช้กฎหมาย	ภารกิจด้านการบังคับใช้กฎหมายและอำนวยความยุติธรรมทางอาญา	สำนักงานตำรวจแห่งชาติ
ข้อ ๓ ที่มีภารกิจเกี่ยวข้องกับความมั่นคงอื่น ๆ	(๑) ภารกิจด้านการเฝ้าระวังและการแจ้งเตือนภัยคุกคามที่กระทบต่อความมั่นคง (๒) ภารกิจด้านการป้องกันและแก้ไขปัญหาที่กระทบต่อความมั่นคง	สำนักข่าวกรองแห่งชาติ
	(๓) ภารกิจด้านการป้องกัน ปราบปรามและแก้ไขปัญหายาเสพติด	สำนักงานคณะกรรมการป้องกันและปราบปรามยาเสพติด

หมวด ๒
ด้านบริการภาครัฐที่สำคัญ

ลักษณะหน่วยงาน	ภารกิจหรือให้บริการ (Critical Services)	หน่วยงานควบคุมหรือกำกับดูแล (Regulator)
ข้อ ๑ ที่มีบริการด้านการเงิน	(๑) บริการที่เกี่ยวข้องกับการบริหารการเงินการคลังภาครัฐ (GFMIS)	กระทรวงการคลัง
	(๒) บริการที่เกี่ยวข้องกับการเชื่อมโยงข้อมูลหน่วยงานภาครัฐและภาคธุรกิจสำหรับการนำเข้า - ส่งออกและโลจิสติกส์	กรมศุลกากร
ข้อ ๒ ที่มีการให้บริการโดยตรงแก่ประชาชน	(๑) บริการที่เกี่ยวข้องกับการทะเบียนราษฎร (๒) บริการที่เกี่ยวข้องกับบัตรประจำตัวประชาชน (๓) บริการที่เกี่ยวข้องกับทะเบียนครอบครัว (๔) บริการ Linkage Center	กรมการปกครอง

ลักษณะหน่วยงาน	ภารกิจหรือให้บริการ (Critical Services)	หน่วยงานควบคุมหรือกำกับดูแล (Regulator)
	(๕) บริการที่เกี่ยวข้องกับการพิสูจน์และยืนยันตัวตนทางดิจิทัล	
	(๖) บริการที่เกี่ยวข้องกับการตรวจสอบคนเข้าเมือง (๗) บริการที่เกี่ยวข้องกับการรับแจ้งเหตุฉุกเฉิน (๘) บริการที่เกี่ยวข้องกับการพิสูจน์และยืนยันตัวตนทางดิจิทัล (๙) บริการที่เกี่ยวข้องกับการแลกเปลี่ยนข้อมูลกลางภาครัฐ	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ข้อ ๓ ที่มีการให้บริการที่เกี่ยวข้องกับการแจ้งเตือน	(๑) บริการที่เกี่ยวข้องกับการคาดการณ์คุณภาพน้ำและการเตือนภัย (๒) บริการที่เกี่ยวข้องกับการชลประทาน	กรมชลประทาน

หมวด ๓
ด้านการเงินการธนาคาร

ลักษณะหน่วยงาน	ภารกิจหรือให้บริการ (Critical Services)	หน่วยงานควบคุมหรือกำกับดูแล (Regulator)
ข้อ ๑ ที่มีการให้บริการทางการเงิน	(๑) บริการฝาก - ถอนเงินรายย่อย (๒) บริการระบบชำระเงินรายใหญ่ระหว่างสถาบันการเงินผ่านระบบบาทเนต (BAHTNET) (๓) บริการระบบการหักบัญชีเช็คด้วยภาพเช็ค (ICS) (๔) บริการระบบชำระเงินรายย่อยผ่านระบบพร้อมเพย์ (PromptPay) (๕) บริการระบบชำระเงินรายย่อยผ่านระบบการโอนเงินทีละรายการ (Single Payment System)	ธนาคารแห่งประเทศไทย

ลักษณะหน่วยงาน	ภารกิจหรือให้บริการ (Critical Services)	หน่วยงานควบคุมหรือกำกับดูแล (Regulator)
ข้อ ๒ ที่มีการให้บริการที่เกี่ยวข้องกับตลาดทุน	(๑) บริการศูนย์กลางจับคู่คำสั่งซื้อขาย (๒) บริการศูนย์กลางชำระราคาและส่งมอบหลักทรัพย์ (๓) บริการศูนย์กลางรับฝากหลักทรัพย์	สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์

หมวด ๔
ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม

ลักษณะหน่วยงาน	ภารกิจหรือให้บริการ (Critical Services)	หน่วยงานควบคุมหรือกำกับดูแล (Regulator)
ข้อ ๑ ที่มีการให้บริการโทรคมนาคม	(๑) บริการโทรศัพท์ประจำที่ภายในประเทศ (Fixed - line) (๒) บริการโทรศัพท์เคลื่อนที่ภายในประเทศ (Mobile) (๓) บริการอินเทอร์เน็ตบรอดแบนด์ประจำที่ (Internet) (๔) บริการโทรคมนาคมระหว่างประเทศผ่านโครงข่ายภาคพื้นดินและภาคพื้นน้ำ	สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ
	(๕) บริการระบบชื่อโดเมน (DNS - Domain Name System)	มูลนิธิศูนย์สารสนเทศเครือข่ายไทย

หมวด ๕
ด้านการขนส่งและโลจิสติกส์

ลักษณะหน่วยงาน	ภารกิจหรือให้บริการ (Critical Services)	หน่วยงานควบคุมหรือกำกับดูแล (Regulator)
ข้อ ๑ ที่มีการให้บริการขนส่งทางบก	(๑) บริการที่เกี่ยวข้องกับการควบคุมการจราจรในพื้นที่กรุงเทพมหานคร	สำนักงานตำรวจแห่งชาติ
ข้อ ๒ ที่มีการให้บริการขนส่งทางราง	(๑) บริการที่เกี่ยวข้องกับการควบคุมการเดินรถจากศูนย์กลาง (๒) บริการที่เกี่ยวข้องกับการส่งสัญญาณ การสื่อสารและการส่งข้อมูล (๓) บริการขายตั๋วและสำรองที่นั่ง	กรมการขนส่งทางราง

ลักษณะหน่วยงาน	ภารกิจหรือให้บริการ (Critical Services)	หน่วยงานควบคุมหรือกำกับดูแล (Regulator)
	(๔) บริการที่เกี่ยวข้องกับการควบคุม กำกับดูแล และเก็บข้อมูล	
ข้อ ๓ ที่มีการให้บริการขนส่งทางน้ำ	(๑) บริการที่เกี่ยวข้องกับการบริหารจัดการท่าเรือ (๒) บริการด้านเรือ สินค้า คลังสินค้า เครื่องมือทุ่นแรง และใบแจ้งหนี้ค่าภาระต่าง ๆ (๓) บริการที่เกี่ยวข้องกับการจัดการท่าเทียบเรือตู้สินค้า (๔) บริการควบคุมจราจรทางน้ำ	กรมเจ้าท่า
ข้อ ๔ ที่มีการให้บริการขนส่งทางอากาศ	(๑) บริการจราจรทางอากาศ (๒) บริการข่าวสารการบิน (๓) บริการที่เกี่ยวข้องกับการปฏิบัติการท่าอากาศยาน (๔) บริการเครื่องอำนวยความสะดวกการเดินอากาศ (๕) บริการที่เกี่ยวข้องกับบริการสิ่งอำนวยความสะดวกและรักษาความปลอดภัยกิจการการบิน (๖) บริการที่เกี่ยวข้องกับอุตุนิยมวิทยาการบิน (๗) บริการสายการบิน (๘) บริการที่เกี่ยวข้องกับการป้องกันคลื่นวิทยุ (สนามบิน) (๙) บริการที่เกี่ยวข้องกับการขนถ่ายสินค้า (๑๐) บริการครัวการบินและสิ่งอำนวยความสะดวกสำหรับผู้โดยสารบนอากาศยาน (๑๑) บริการลานจอด ตรวจสอบและบำรุงรักษาอากาศยาน	สำนักงานการบินพลเรือนแห่งประเทศไทย

หมวด ๖
ด้านพลังงานและสาธารณูปโภค

ลักษณะหน่วยงาน	ภารกิจหรือให้บริการ (Critical Services)	หน่วยงานควบคุมหรือกำกับดูแล (Regulator)
ข้อ ๑ ที่มีการให้บริการด้านไฟฟ้า	(๑) บริการผลิตไฟฟ้า (๒) บริการสายส่งไฟฟ้า (๓) บริการจำหน่ายไฟฟ้า (๔) บริการควบคุมไฟฟ้า (๕) บริการที่เกี่ยวข้องกับการบริหารจัดการพลังงานไฟฟ้า	กระทรวงพลังงาน
ข้อ ๒ ที่มีการให้บริการด้านปิโตรเลียมและก๊าซ	(๑) บริการผลิตปิโตรเลียม (๒) บริการขนส่งก๊าซ และน้ำมัน (๓) บริการจำหน่ายก๊าซ และน้ำมัน (๔) บริการเก็บรักษาและแปรสภาพก๊าซ	กระทรวงพลังงาน
ข้อ ๓ ที่มีการให้บริการด้านประปา	(๑) บริการที่เกี่ยวข้องกับงานควบคุมคุณภาพน้ำประปา (๒) บริการที่เกี่ยวข้องกับการผลิตน้ำ (๓) บริการจำหน่ายน้ำ	กระทรวงมหาดไทย

หมวด ๗
ด้านสาธารณสุข

ลักษณะหน่วยงาน	ภารกิจหรือให้บริการ (Critical Services)	หน่วยงานควบคุมหรือกำกับดูแล (Regulator)
ข้อ ๑ ที่มีการให้บริการสุขภาพในโรงพยาบาล	(๑) บริการทางการแพทย์ในสถานพยาบาล และบริการที่เกี่ยวข้องกับงานสนับสนุน (๒) บริการที่เกี่ยวข้องกับการตรวจวิเคราะห์ทางการแพทย์ (๓) บริการทางรังสีวิทยา	กรมสนับสนุนบริการสุขภาพ
ข้อ ๒ ที่มีการให้บริการด้านยา เวชภัณฑ์และเครื่องมือแพทย์	(๑) บริการที่เกี่ยวข้องกับการผลิตยา ยาเสพติด (๒) บริการที่เกี่ยวข้องกับการผลิตเครื่องมือแพทย์ (๓) บริการนำเข้า กระจาย และจำหน่ายยา ยาเสพติด (๔) บริการนำเข้า กระจาย และจำหน่ายเครื่องมือแพทย์	สำนักงานคณะกรรมการอาหารและยา

ลักษณะหน่วยงาน	ภารกิจหรือให้บริการ (Critical Services)	หน่วยงานควบคุมหรือกำกับดูแล (Regulator)
ข้อ ๓ ที่มีการให้บริการทางรังสีวิทยา	(๑) บริการทางรังสีวิทยา (๒) บริการทางกัมมันตรังสี	สำนักงานปรมาณูเพื่อสันติ
ข้อ ๔ ที่มีการให้บริการข้อมูลสุขภาพดิจิทัล	(๑) บริการข้อมูลสุขภาพและบริการแอปพลิเคชันหรือโปรแกรมที่เกี่ยวข้องกับข้อมูลสุขภาพ (๒) บริการแลกเปลี่ยนข้อมูลสุขภาพ (๓) บริการที่เกี่ยวข้องกับคลังข้อมูลสุขภาพ	สำนักงานปลัดกระทรวงสาธารณสุข



ฉบับภาษาอังกฤษ
English Version

อยู่ระหว่างดำเนินการแปลเอกสารเป็นฉบับภาษาอังกฤษ

The translation of the document into English is underway.

5

ประกาศ กกม.

เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐาน
ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงาน
ของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
พ.ศ. 2564

มีผลใช้บังคับตั้งแต่วันที่ 6 ก.ย. 65 เป็นต้นไป

Notification of CRC

Re: Codes of Practice and Standard Frameworks for Government Agencies and Critical Information Infrastructure organizations B.E. 2564 (2021)

effective from September 6, 2022, onwards.



ฉบับภาษาไทย
Thai Version

ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์

เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
พ.ศ. ๒๕๖๔

เพื่อจัดให้มีประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อันเป็นข้อกำหนดขั้นต่ำในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมทั้งกำหนดมาตรการในการประเมินความเสี่ยงการตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ เมื่อมีภัยคุกคามทางไซเบอร์ หรือเหตุการณ์ที่ส่งผลกระทบหรืออาจก่อให้เกิดผลกระทบหรือความเสียหายอย่างมีนัยสำคัญหรืออย่างร้ายแรงต่อระบบสารสนเทศของประเทศ เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ปฏิบัติได้อย่างรวดเร็ว มีประสิทธิภาพและเป็นไปในทิศทางเดียวกัน สอดคล้องกับมาตรฐานสากล

อาศัยอำนาจตามความในมาตรา ๑๓ วรรคหนึ่ง (๔) และวรรคสอง และมาตรา ๕๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ประกอบมติที่ประชุมคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ครั้งที่ ๑/๒๕๖๔ เมื่อวันที่ ๒๕ มิถุนายน ๒๕๖๔ และมติที่ประชุมคณะกรรมการกำกับดูแลด้านความปลอดภัยไซเบอร์ ครั้งที่ ๑/๒๕๖๔ เมื่อวันที่ ๘ มิถุนายน ๒๕๖๔ คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ จึงออกประกาศไว้ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับเมื่อพ้นกำหนดหนึ่งปีนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ข้อ ๓ ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ให้เป็นไปตามแนบท้ายประกาศนี้

ข้อ ๔ ให้ประธานกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ มีอำนาจตีความและวินิจฉัยปัญหาเกี่ยวกับการปฏิบัติตามประกาศนี้

ข้อ ๕ ให้เลขาธิการคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ รักษาการตามประกาศนี้ และให้มีอำนาจออกประกาศ คำสั่ง หลักเกณฑ์และวิธีการเพื่อประโยชน์ในการปฏิบัติตามประกาศนี้

บรรดาระเบียบ ข้อบังคับ ประกาศ หรือคำสั่ง ซึ่งขัดหรือแย้งกับประกาศนี้ ให้ใช้ประกาศนี้แทน

ประกาศ ณ วันที่ ๒ สิงหาคม พ.ศ. ๒๕๖๔
ชัยวุฒิ ธนาคมานุสรณ์
รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
ประธานกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์

ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
พ.ศ. ๒๕๖๔

บทนำ

๑. พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ได้กำหนดให้มีการจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อันเป็นข้อกำหนดขั้นต่ำในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมทั้งกำหนดมาตรการในการประเมินความเสี่ยง การตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ เมื่อมีภัยคุกคามทางไซเบอร์ หรือเหตุการณ์ที่ส่งผลกระทบหรืออาจก่อให้เกิดผลกระทบหรือความเสียหายอย่างมีนัยสำคัญ หรืออย่างร้ายแรงต่อระบบสารสนเทศของประเทศ เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ปฏิบัติได้อย่างรวดเร็ว มีประสิทธิภาพ และเป็นไปในทิศทางเดียวกัน สอดคล้องกับมาตรฐานสากล เพื่อสนับสนุนการดำเนินงานของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

วัตถุประสงค์

๒. เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ปฏิบัติได้อย่างรวดเร็ว มีประสิทธิภาพ และเป็นไปในทิศทางเดียวกัน สอดคล้องกับมาตรฐานสากล

ขอบเขตการใช้

๓. ใช้กับของหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

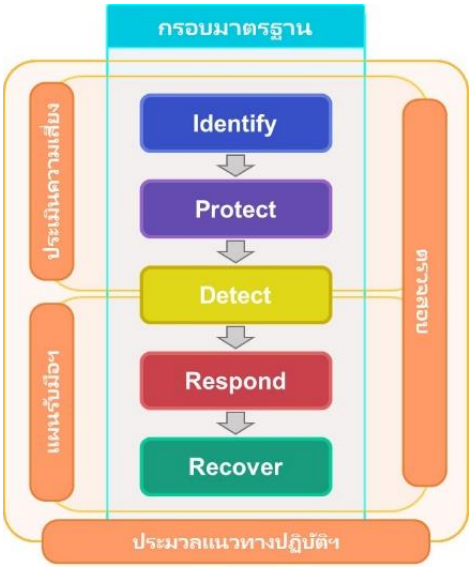
คำนิยาม

๔. คณะกรรมการ	หมายถึง	คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
๕. กกม.	หมายถึง	คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์
๖. หน่วยงานของรัฐ	หมายถึง	หน่วยงานของรัฐที่ถูกประกาศเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
๗. บริการที่สำคัญ	หมายถึง	ภารกิจหรือบริการของหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามมาตรา ๔๙
๘. สำนักงาน	หมายถึง	สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
๙. ดัชนีชี้วัดความเสี่ยงที่สำคัญ	หมายถึง	เครื่องมือที่ใช้วัดกิจกรรมที่อาจจะทำให้องค์กรมีความเสี่ยงที่เพิ่มขึ้น ช่วยติดตามความเสี่ยงพร้อมทั้งเป็นสัญญาณเตือนเพื่อให้หน่วยงานสามารถคาดการณ์เหตุการณ์และความเสี่ยงในอนาคตและเตรียมมาตรการป้องกันก่อนเกิดเหตุการณ์ความเสียหาย

๑๐. ผู้ให้บริการภายนอก	หมายถึง	บุคคลหรือนิติบุคคลผู้ให้บริการภายนอก ซึ่งเป็นผู้ให้บริการด้านเทคโนโลยีสารสนเทศ หรือเป็นผู้ที่มีการเชื่อมต่อกับระบบเทคโนโลยีสารสนเทศของหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หรือเป็นผู้ที่สามารถเข้าถึงข้อมูลสำคัญของหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญ ทางสารสนเทศ หรือข้อมูลของผู้ใช้บริการที่ควบคุมดูแลโดยหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญ ทางสารสนเทศได้ ทั้งนี้ ผู้ให้บริการภายนอกไม่ครอบคลุมถึงผู้ใช้บริการที่ใช้ผลิตภัณฑ์และบริการของหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
๑๑. คอมไพเลอร์	หมายถึง	โปรแกรมแปลโปรแกรม ตัวแปลโปรแกรม เป็นโปรแกรมคอมพิวเตอร์ที่ทำหน้าที่แปลงชุดคำสั่งภาษาคอมพิวเตอร์หนึ่งไปเป็นชุดคำสั่งที่มีความหมายเดียวกันในภาษาคอมพิวเตอร์อื่น
๑๒. แพตช์	หมายถึง	โปรแกรมที่ใช้ในการปรับปรุงแก้ไขซอฟต์แวร์ โดยส่วนใหญ่จะอยู่ในลักษณะของไฟล์ และใช้เพื่อแก้ไขช่องโหว่เรื่องความมั่นคงปลอดภัย หรือเพื่อเพิ่มความสามารถของซอฟต์แวร์ ผู้พัฒนาซอฟต์แวร์หลายรายได้เผยแพร่แพตช์ออกมาเป็นระยะ เช่น บริษัท Microsoft จะเผยแพร่แพตช์ที่แก้ไขช่องโหว่ของซอฟต์แวร์ผ่านระบบ Windows Update
๑๓. Recovery Time Objective (RTO)	หมายถึง	ระยะเวลาในการกู้คืนระบบ
๑๔. Recovery Point Objective (RPO)	หมายถึง	ระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย
๑๕. Maximum Tolerance Period of Disruption (MTPD)	หมายถึง	ระยะเวลาสูงสุดที่ยอมให้ธุรกิจหยุดชะงัก เพื่อรองรับการดำเนินธุรกิจอย่างต่อเนื่องของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและรองรับการเกิดเหตุการณ์ผิดปกติต่าง ๆ ที่อาจส่งผลให้เกิดการหยุดชะงักหรือเกิดความเสียหายต่อระบบ เช่น ภัยคุกคามการทำงานได้ตามปกติให้เร็วที่สุด

๑๖. การจัดทำประมวลแนวทางปฏิบัติ มีองค์ประกอบ ดังนี้

- แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
- การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
- แผนการรับมือภัยคุกคามทางไซเบอร์



รูปที่ ๑ ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๑๗. องค์ประกอบที่ ๑ แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

แนวปฏิบัติ

๑๗.๑ ต้องจัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ ทั้งโดยผู้ตรวจสอบภายใน หรือโดยผู้ตรวจสอบอิสระภายนอก อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง โดยมีขอบเขตของการตรวจสอบ ดังนี้

(ก) กระบวนการจัดทำและผลการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA)

(ข) บริการที่สำคัญที่หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศเป็นเจ้าของและใช้บริการ ตามผลการวิเคราะห์ในข้อ (ก)

(ค) การปฏิบัติตามพระราชบัญญัตินี้ และประมวลแนวทางปฏิบัตินี้และหลักปฏิบัติใด ๆ ที่เกี่ยวข้องกับประมวลแนวทางปฏิบัติ มาตรฐานการปฏิบัติงาน และที่คณะกรรมการประกาศกำหนด

๑๗.๒ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดส่งผลสรุปรายงานการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ต่อสำนักงานภายในกำหนด ๓๐ (สามสิบ) วันนับแต่วันที่ดำเนินการแล้วเสร็จตามที่กำหนดไว้ในมาตรา ๕๔ พร้อมทั้งส่งสำเนาให้หน่วยงานควบคุมหรือกำกับดูแลด้วย

ทั้งนี้ รูปแบบและรายละเอียดผลสรุปรายงานการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ให้สำนักงานประกาศกำหนด

๑๗.๓ ในกรณีที่การตรวจสอบดำเนินการภายใต้มาตรา ๕๔ ระบุการไม่ปฏิบัติตามข้อ ๑๗.๑ เว้นแต่ กกม. จะระบุเป็นลายลักษณ์อักษรเป็นอย่างอื่น ให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศส่งแผนการดำเนินการแก้ไขไปยังสำนักงานภายในกำหนด ๓๐ (สามสิบ) วันนับแต่จากวันที่ได้รับรายงานการตรวจสอบโดยแผนการดำเนินการแก้ไขต้องมีรายละเอียดอย่างน้อย ดังนี้

(ก) ให้รายละเอียดการดำเนินการแก้ไขที่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจะดำเนินการเพื่อจัดการกับการไม่ปฏิบัติตาม และ

(ข) กำหนดระยะเวลาสำหรับการดำเนินการตามที่ระบุไว้ในข้อ ๑๗.๓ (ก)

๑๗.๔ ในกรณีที่ กกม. เห็นสมควรให้ปรับปรุงแผนการดำเนินการแก้ไข ให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศดำเนินการและส่งแผนการดำเนินการแก้ไขที่ได้รับการปรับปรุงแล้วไปยังสำนักงานภายในระยะเวลาที่ กกม. กำหนด พร้อมส่งทั้งสำเนาให้หน่วยงานควบคุมหรือกำกับดูแลด้วย

๑๗.๕ เมื่อแผนการดำเนินการแก้ไขได้รับความเห็นชอบจาก กกม. หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจะดำเนินการตามแผนการดำเนินการแก้ไขดังกล่าว และดำเนินการแก้ไขทั้งหมดให้แล้วเสร็จภายในกำหนดระยะเวลาตามที่ระบุไว้ เพื่อให้ผ่านเกณฑ์การพิจารณาของ กกม.

๑๘. องค์ประกอบที่ ๒ การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

แนวปฏิบัติ

เพื่อให้หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศสามารถประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ได้อย่างมีประสิทธิภาพและต่อเนื่อง หน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องกำหนดนโยบายการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ตามที่ระบุไว้ในนโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้ครอบคลุมเรื่องโครงสร้างองค์กรและบทบาทหน้าที่ของผู้ที่เกี่ยวข้องในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และต้องนำนโยบายดังกล่าวมาจัดทำระเบียบวิธีปฏิบัติและกระบวนการในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยต้องจัดให้มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง ต้องประกอบด้วยรายละเอียดอย่างน้อย ดังต่อไปนี้

๑๘.๑ การประเมินความเสี่ยง (Risk Assessment)

(ก) การระบุความเสี่ยง (Risk Identification)

ต้องระบุถึงความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งรวมถึงความเสี่ยงจากภัยคุกคามทางไซเบอร์ และช่องโหว่ต่าง ๆ โดยความเสี่ยงดังกล่าวอาจมีสาเหตุ มาจากกระบวนการปฏิบัติงาน ระบบงาน บุคลากร หรือปัจจัยภายนอก

(ข) การวิเคราะห์ความเสี่ยง (Risk Analysis)

ต้องเข้าใจและวิเคราะห์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อหาแนวทางในการจัดการความเสี่ยงที่เหมาะสม

(ค) การประเมินค่าความเสี่ยง (Risk Evaluation)

ต้องประเมินถึงโอกาสที่ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์จะเกิดขึ้นและผลกระทบต่อการปฏิบัติงานและการดำเนินธุรกิจ รวมถึงกำหนดระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ (Risk Appetite)

๑๘.๒ การจัดการความเสี่ยง (Risk Treatment)

ต้องมีแนวทางจัดการ ควบคุม และป้องกันความเสี่ยงที่เหมาะสมสอดคล้องกับผลการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้ความเสี่ยงที่เหลืออยู่ (Residual Risk) อยู่ในระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ โดยต้องคำนึงถึงความสมดุลระหว่างต้นทุนในการป้องกันความเสี่ยงและผลประโยชน์ที่คาดว่าจะได้รับ

นอกจากนี้ต้องกำหนดดัชนีชี้วัดความเสี่ยงที่สำคัญ (Key Risk Indicator: KRI) ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับการดำเนินธุรกิจ ให้สอดคล้องกับความสำคัญของความมั่นคงปลอดภัยไซเบอร์แต่ละงาน เพื่อใช้ติดตามและทบทวนความเสี่ยง

๑๘.๓ การติดตามและทบทวนความเสี่ยง (Risk Monitoring and Review)

ต้องมีกระบวนการที่มีประสิทธิภาพในการติดตาม และทบทวนความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้อยู่ภายใต้ระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ที่กำหนดไว้

๑๘.๔ การรายงานความเสี่ยง (Risk Reporting)

ต้องรายงานระดับความเสี่ยงและผลการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ต่อคณะกรรมการของหน่วยงานที่ได้รับมอบหมายเป็นประจำ เช่น ตามรอบการประชุมของคณะกรรมการของหน่วยงานที่ได้รับมอบหมาย

ทั้งนี้ ต้องทบทวนระเบียบวิธีปฏิบัติและกระบวนการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เช่น กรณีที่มีการเปลี่ยนแปลงของระบบความมั่นคงปลอดภัยไซเบอร์ ความเสี่ยง มาตรฐานสากล อย่างมีนัยสำคัญ เป็นต้น

๑๙. องค์ประกอบที่ ๓ แผนการรับมือภัยคุกคามทางไซเบอร์

แนวปฏิบัติ

๑๙.๑ ต้องจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan) ที่กำหนดว่าควรตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์อย่างไร โดยแผนการรับมือภัยคุกคามทางไซเบอร์ต้องมีรายละเอียดอย่างน้อย ดังต่อไปนี้

(ก) โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT) รวมถึงบทบาทและความรับผิดชอบที่กำหนดไว้อย่างชัดเจนของสมาชิกในทีมแต่ละคนและรายละเอียดการติดต่อ

(ข) โครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure) ซึ่งกำหนดว่าหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจะปฏิบัติตามภาระหน้าที่ในการรายงานภายใต้พระราชบัญญัติ และกฎหมายย่อยใด ๆ ที่ทำขึ้นภายใต้กฎหมายดังกล่าว ตลอดจนภาระหน้าที่ในการรายงานภายใต้กฎหมาย และข้อกำหนดด้านกฎระเบียบที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(ค) เกณฑ์และขั้นตอนในการเรียกใช้งาน (Activate) การตอบสนองต่อเหตุการณ์และ CIRT

(ง) ขั้นตอนจำกัดขอบเขต (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

(จ) การเรียกใช้งานกระบวนการกู้คืน (Recovery Process)

(ฉ) ขั้นตอนในการสอบสวน (Investigate) สาเหตุและผลกระทบของเหตุการณ์

(ช) ขั้นตอนการเก็บรักษาหลักฐาน (Preservation of Evidence) ก่อนเริ่มกระบวนการกู้คืน ซึ่งรวมถึงการได้มาของบันทึกการยึดหลักฐานคอมพิวเตอร์ที่ได้มา หรืออุปกรณ์อื่น ๆ เพื่อสนับสนุนการสอบสวน

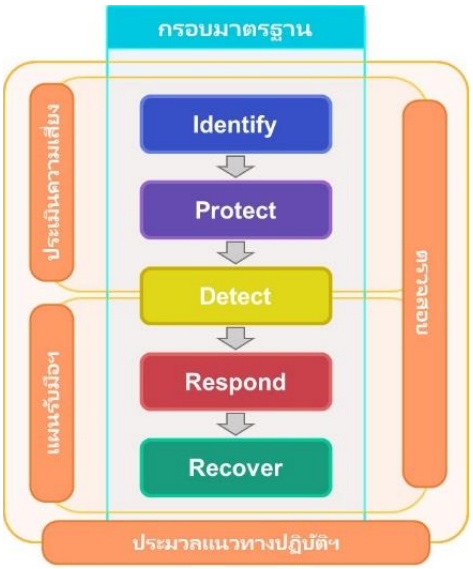
(ซ) ระเบียบวิธีการมีส่วนร่วม (Engagement Protocols) กับบุคคลภายนอก หรือแนวปฏิบัติการบริหารจัดการบุคคลภายนอก ซึ่งรวมถึงรายละเอียดการติดต่อ ตัวอย่างเช่น ผู้ขายสำหรับบริการด้านนิติวิทยาศาสตร์/การกู้คืนและการบังคับใช้กฎหมายเพื่อดำเนินคดี และ

(ฌ) กระบวนการทบทวนหลังการดำเนินการ (After-Action Review Process) เพื่อระบุและแนะนำให้ปรับปรุงการดำเนินการเพื่อป้องกันการเกิดซ้ำ

๑๙.๒ ต้องตรวจสอบให้แน่ใจว่าแผนการรับมือภัยคุกคามทางไซเบอร์ได้รับการสื่อสารอย่างมีประสิทธิผลไปยังบุคลากรที่เกี่ยวข้องทั้งหมดที่สนับสนุนบริการสำคัญของหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๑๙.๓ ต้องทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง โดยนับแต่วันที่แผนได้รับการอนุมัติ

๑๙.๔ ต้องทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ เมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญในสภาพแวดล้อมการปฏิบัติการทางไซเบอร์ของบริการที่สำคัญของหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หรือข้อกำหนดในการตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์



รูปที่ ๒ ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๒๐. กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

ประกอบไปด้วย ๕ หัวข้อหลัก (ดังรูปที่ ๒) ดังนี้

๒๐.๑ การระบุความเสี่ยงที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล (Identify)

๒๐.๑.๑ การจัดการทรัพย์สิน (Asset Management)

๒๐.๑.๒ การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy)

๒๐.๑.๓ การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing)

๒๐.๑.๔ การจัดการผู้ให้บริการภายนอก (Third Party Management)

๒๐.๒ มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect)

๒๐.๒.๑ การควบคุมการเข้าถึง (Access Control)

๒๐.๒.๒ การทำให้ระบบมีความแข็งแกร่ง (System Hardening)

๒๐.๒.๓ การเชื่อมต่อระยะไกล (Remote Connection)

๒๐.๒.๔ สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media)

๒๐.๒.๕ การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)

๒๐.๒.๖ การแบ่งปันข้อมูล (Information Sharing)

๒๐.๓ มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)

๒๐.๓.๑ การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring)

๒๐.๔ มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)

๒๐.๔.๑ แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)

๒๐.๔.๒ แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)

๒๐.๔.๓ การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise)

๒๐.๕ มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)

๒๐.๕.๑ การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery)

๒๑. หัวข้อหลักที่ ๑ การระบุความเสี่ยงที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล (Identify)

กรอบมาตรฐาน

๒๑.๑ การจัดการทรัพย์สิน (Asset Management)

๒๑.๑.๑ ต้องมีทะเบียนทรัพย์สิน (Inventory) ที่ระบุทรัพย์สินของบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และดูแลรักษาทะเบียนทรัพย์สินให้เป็นปัจจุบัน โดยทะเบียนทรัพย์สินต้องมีข้อมูลอย่างน้อย ดังนี้

(ก) ชื่อ/คำอธิบายของทรัพย์สิน ของบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(ข) ฟังก์ชันที่สำคัญของทรัพย์สิน ของบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(ค) การระบุและการจัดลำดับความสำคัญของทรัพย์สิน บริการที่สำคัญของหน่วยงานของรัฐ และโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(ง) เจ้าของและ/หรือผู้ดำเนินการของทรัพย์สินของบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(จ) ตำแหน่งทางกายภาพของทรัพย์สินของบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศแต่ละรายการ และ

(ฉ) การขึ้นต่อกันของทรัพย์สินของบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศบนระบบ/เครือข่ายภายใน และ/หรือภายนอก

๒๑.๑.๒ ต้องระบุขอบเขตเครือข่ายของบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และระบบคอมพิวเตอร์ที่เชื่อมต่อโดยตรงและมีนัยสำคัญ (Direct and Significant Interface)

๒๑.๑.๓ ต้องมีการตรวจสอบทะเบียนทรัพย์สินอย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง หากมีการเปลี่ยนแปลงใด ๆ กับทรัพย์สินของบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ให้ปรับปรุงทะเบียนทรัพย์สินดังกล่าวด้วย

๒๑.๑.๔ ตามมาตรา ๕๔ ต้องดำเนินการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศซึ่งรวมถึงรายการทั้งหมดที่ระบุไว้ในทะเบียนทรัพย์ในข้อ ๒๑.๑.๑ อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง

๒๑.๒ การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy)

๒๑.๒.๑ ต้องประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญที่กระทบต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศของหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ตามเกณฑ์ประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่กำหนดไว้ในการบริหารความเสี่ยง (Risk Management) ตามนโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ที่คณะกรรมการประกาศกำหนด

๒๑.๒.๒ ต้องปรับปรุงทะเบียนความเสี่ยงทุกครั้งหลังการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ทะเบียนความเสี่ยงต้องจัดทำเอกสารโดยมีรายละเอียดอย่างน้อย ดังต่อไปนี้

(ก) วันที่ระบุความเสี่ยง (Date the Risk is Identified)

(ข) คำอธิบายของความเสี่ยง (Description of the Risk)

(ค) โอกาสที่จะเกิดขึ้น (Likelihood of Occurrence)

(ง) ความรุนแรงของเหตุการณ์ (Severity of the Occurrence)

(ฉ) การจัดการความเสี่ยง (Risk Treatment)

(ง) เจ้าของความเสี่ยง (Risk Owner)

(ฉ) สถานะของการจัดการความเสี่ยง (Status of Risk Treatment) และ

(ช) ความเสี่ยงที่เหลือ (Residual Risk)

๒๑.๓ การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing)

๒๑.๓.๑ ต้องดำเนินการประเมินช่องโหว่ของบริการที่สำคัญของหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศอ้างอิงตามหลักการบริหารความเสี่ยงของหน่วยงานเพื่อระบุจุดอ่อนด้านความมั่นคงปลอดภัยและการควบคุมโดยครอบคลุมบริการที่สำคัญของหน่วยงานของ รัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศซึ่งเป็น

(ก) ระบบเทคโนโลยีสารสนเทศ (Information Technology (IT) system)

(ข) ระบบที่ใช้ควบคุมเครื่องจักรในอุตสาหกรรม (Industrial Control System: ICS)

๒๑.๓.๒ ต้องตรวจสอบให้แน่ใจว่าขอบเขตของการประเมินช่องโหว่แต่ละรายการ ประกอบด้วย

(ก) การประเมินความมั่นคงปลอดภัยของโฮสต์ (Host Security Assessment)

(ข) การประเมินความมั่นคงปลอดภัยของเครือข่าย (Network Security Assessment) และ

(ค) การตรวจสอบความมั่นคงปลอดภัยของสถาปัตยกรรม (Architecture Security Review)

๒๑.๓.๓ ต้องทำการประเมินช่องโหว่ของบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เพื่อระบุจุดอ่อนด้านความมั่นคงปลอดภัยและควบคุมก่อนที่จะทำการทดสอบระบบใหม่ใด ๆ ที่เชื่อมต่อ หรือดำเนินการเปลี่ยนแปลงระบบที่สำคัญใด ๆ กับบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ การเปลี่ยนแปลงระบบที่สำคัญ ได้แก่ การเพิ่มโมดูลแอปพลิเคชัน (Adding New Application Module) การปรับปรุงระบบ และการปรับเปลี่ยนเทคโนโลยี

๒๑.๓.๔ ควรพิจารณาดำเนินการทดสอบเจาะระบบ (Penetration Testing) บริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยเฉพาะอย่างยิ่ง ระบบเทคโนโลยีสารสนเทศ (Information Technology: IT) ที่เชื่อมต่อกับอินเทอร์เน็ต (Internet Facing) ให้สอดคล้องกับระดับของความเสี่ยง และพิจารณาผลกระทบหรือความเสี่ยงจากการทดสอบเจาะระบบด้วย

๒๑.๓.๕ ต้องตรวจสอบให้แน่ใจว่าขอบเขตของการทดสอบเจาะระบบ (Scope of a Penetration Test) รวมถึงการทดสอบเจาะระบบของโฮสต์ เครือข่าย และแอปพลิเคชันของบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยเฉพาะอย่างยิ่ง ทุกระบบที่เป็นมีการเชื่อมต่ออินเทอร์เน็ตโดยตรง (Internet Facing)

๒๑.๓.๖ ควรพิจารณาดำเนินการทดสอบเจาะระบบอย่างน้อยปีละ ๑ (หนึ่ง) ตามความจำเป็นเพื่อตรวจสอบความถูกต้องของระบบรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ก่อนที่จะทำการทดสอบระบบใหม่ หรือการเปลี่ยนแปลงระบบที่สำคัญ เช่น โมดูลเสริม การปรับปรุงระบบ และการปรับเปลี่ยนเทคโนโลยี เป็นต้น

๒๑.๓.๗ ต้องตรวจสอบให้แน่ใจว่าการทดสอบเจาะระบบและผู้ทดสอบเจาะระบบ (Penetration Testers) ที่ทำการทดสอบเจาะระบบบนโครงสร้างพื้นฐานสำคัญสารสนเทศ มีการรับรองและได้รับประกาศนียบัตร (Accreditations and Certifications) ที่เป็นที่ยอมรับในอุตสาหกรรม และเป็นอิสระจากระบบที่ทำการทดสอบเจาะระบบ ทั้งนี้ คุณสมบัติของผู้ทดสอบเจาะระบบ ให้เป็นไปตามหลักเกณฑ์และวิธีการที่หน่วยงานควบคุมหรือกำกับดูแลกำหนด

๒๑.๓.๘ ต้องตรวจสอบให้แน่ใจว่าการทดสอบเจาะระบบทั้งหมดโดยผู้ให้บริการทดสอบเจาะระบบดำเนินการภายใต้การดูแลของหน่วยงาน

๒๑.๓.๙ ต้องสร้างกระบวนการเพื่อติดตามและจัดการกับช่องโหว่ที่ระบุในผลการประเมินช่องโหว่และในผลการทดสอบเจาะระบบและตรวจสอบว่าช่องโหว่ที่ระบุทั้งหมดได้รับการแก้ไขอย่างเพียงพอ

๒๑.๓.๑๐ หากได้รับการร้องขอจาก กกม. หรือสำนักงาน หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องส่งสำเนารายงานสรุปผลการทดสอบเจาะระบบ เพื่อประโยชน์ในการประเมินระดับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานดังกล่าว ไปยังสำนักงานภายในกำหนด ๓๐ (สามสิบ) วัน นับแต่วันที่ได้รับหนังสือด้วย

ทั้งนี้ รูปแบบรายงานสรุปผลการทดสอบเจาะระบบ ให้เป็นไปตามหลักเกณฑ์และวิธีการที่สำนักงานประกาศกำหนด

๒๑.๔ การจัดการผู้ให้บริการภายนอก (Third Party Management)

๒๑.๔.๑ ต้องรับผิดชอบ (Responsible) และมีภาระรับผิดชอบ (Accountable) ต่อการดูแลรักษาความมั่นคงปลอดภัยไซเบอร์ของโครงสร้างพื้นฐานสำคัญทางสารสนเทศ แม้ว่าผู้ให้บริการภายนอกจะดำเนินงานใด ๆ ก็ตามในส่วนของบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๒๑.๔.๒ ต้องกำหนดข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์เพื่อลดความเสี่ยงที่เกี่ยวข้องกับการเข้าถึงกระบวนการจัดเก็บ การสื่อสาร และการดำเนินการของโครงสร้างพื้นฐานสำคัญทางสารสนเทศของผู้ให้บริการภายนอกในข้อตกลงระดับการให้บริการ (Service Level Agreement) หรือเงื่อนไขของสัญญากับผู้ให้บริการภายนอก ข้อกำหนดต้องคำนึงถึงรายละเอียดอย่างน้อย ดังต่อไปนี้

(ก) ประเภทของผู้ให้บริการภายนอกที่เข้าถึงทรัพย์สินของบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามความต้องการทางธุรกิจขององค์กรและโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

(ข) ภาระหน้าที่ของผู้ให้บริการภายนอกในการปกป้องบริการที่สำคัญหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจากภัยคุกคามทางไซเบอร์

(ค) ความเสี่ยงที่เกี่ยวข้องกับบริการและห่วงโซ่อุปทานผลิตภัณฑ์ และ

(ง) สิทธิ์ของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศในการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการภายนอก

๒๑.๔.๓ ควรพิจารณาสร้างกระบวนการตรวจสอบความถูกต้องของผู้ให้บริการภายนอกว่าสอดคล้องกับข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ในเงื่อนไขของสัญญา ตัวอย่างเช่น การตรวจสอบโดยบุคคลที่สาม และการตรวจสอบผลิตภัณฑ์

๒๑.๔.๔ ควรพิจารณาดำเนินการเจรจาต่อรองเงื่อนไขของสัญญาจ้างให้สอดคล้องกับกรณีที่มีข้อกำหนดทางกฎหมายหรือข้อบังคับใหม่

๒๒. หัวข้อหลักที่ ๒ มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect)

กรอบมาตรฐาน

๒๒.๑ การควบคุมการเข้าถึง (Access Control)

๒๒.๑.๑ ต้องตรวจสอบให้แน่ใจว่าการเข้าถึงบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศถูกจำกัดไว้ที่

(ก) บุคลากร และกิจกรรมที่ได้รับอนุญาต และ

(ข) อุปกรณ์ และอินเทอร์เฟซ (Interface) ที่ได้รับอนุญาต

๒๒.๑.๒ ในส่วนที่เกี่ยวกับภาระหน้าที่ภายใต้ข้อ ๒๒.๑.๑ หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องกำหนดให้แต่ละบุคลากร กิจกรรมและกระบวนการที่ได้รับอนุญาตมีการใช้เทคนิคการตรวจสอบสิทธิ์ที่สอดคล้องกับโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Profile) สำหรับแต่ละโหมดการเข้าถึงบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๒๒.๑.๓ ต้องเก็บรักษาบันทึกของการเข้าถึงทั้งหมด (Logs of All Access) และความพยายามทั้งหมดในการเข้าถึงบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และตรวจสอบบันทึกเหล่านี้เพื่อหากิจกรรมที่ผิดปกติเป็นประจำ ความสม่ำเสมอในการตรวจสอบบันทึกเหล่านี้ควรสอดคล้องกับความถี่ หรือความสม่ำเสมอของกิจกรรมการเข้าถึงดังกล่าว

๒๒.๑.๔ ต้องตรวจสอบให้แน่ใจว่าการเข้าถึงอินเทอร์เฟซ (Interface) ของบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (เช่น USB, พอร์ตอนุกรม) และการเข้าถึงทางลอจิคอล (Logical) มีการกำกับดูแลโดย

(ก) ทำภายใต้การดูแลของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศเท่านั้น และ

(ข) ดำเนินการในสถานที่ หากเป็นไปได้

๒๒.๒ การทำให้ระบบมีความแข็งแกร่ง (System Hardening)

๒๒.๒.๑ ต้องสร้างมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) สำหรับระบบปฏิบัติการ แอปพลิเคชัน และอุปกรณ์เครือข่ายทั้งหมดของบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่สอดคล้องกับโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Profile) ของบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๒๒.๒.๒ มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ต้องมีหลักการรักษาความมั่นคงปลอดภัยอย่างน้อย ดังต่อไปนี้

(ก) สิทธิพิเศษในการเข้าถึงน้อยที่สุด (Least Access Privilege)

(ข) การแบ่งแยกหน้าที่ (Separation of Duties)

(ค) การบังคับใช้นโยบายความซับซ้อนของรหัสผ่าน

(ง) การลบบัญชีที่ไม่ได้ใช้

(จ) การลบบริการและแอปพลิเคชันที่ไม่จำเป็น เช่น การลบคอมไพเลอร์ (Removal of Compiler) และแอปพลิเคชันสนับสนุนผู้ให้บริการภายนอก (Vendor Support Application)

(ฉ) การปิดพอร์ตเครือข่ายที่ไม่ได้ใช้งาน

(ช) การป้องกันมัลแวร์ (Malware) และ

(ซ) การปรับปรุงซอฟต์แวร์และแพตช์ (Patch) ความมั่นคงปลอดภัยของระบบอย่างทันการณ์และเหมาะสม

๒๒.๒.๓ ต้องตรวจสอบให้แน่ใจว่ามีการใช้มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ตามที่ระบุไว้ ก่อนที่จะมีทรัพย์สินใด ๆ เชื่อมต่อหรือเมื่อมีการเปลี่ยนแปลงหรือปรับปรุงบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๒๒.๒.๔ ต้องตรวจสอบมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standard) ของบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศอย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง เพื่อให้แน่ใจว่ามาตรฐานเหล่านี้ยังคงมีประสิทธิภาพต่อภัยคุกคามทางไซเบอร์

๒๒.๒.๕ ต้องจัดทำกระบวนการจัดการเปลี่ยนแปลง (Change Management Process) เพื่ออนุญาตและตรวจสอบความถูกต้องของการเปลี่ยนแปลงระบบทั้งหมดที่มีต่อบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๒๒.๓ การเชื่อมต่อระยะไกล (Remote Connection)

๒๒.๓.๑ ต้องตรวจสอบให้แน่ใจว่าการเชื่อมต่อระยะไกลทั้งหมดมายังบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศมีมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีประสิทธิภาพเพื่อป้องกันและตรวจจับการเข้าถึงโดยไม่ได้รับอนุญาต

๒๒.๓.๒ สำหรับการเชื่อมต่อระยะไกลกับบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ต้องปฏิบัติตามแนวทางปฏิบัติดังต่อไปนี้

(ก) ในกรณีที่เป็นไปได้ให้เปิดใช้งานการเชื่อมต่อไปยัง หรือจากไซต์ระยะไกล เมื่อจำเป็นเท่านั้น

(ข) ในกรณีที่เป็นไปได้ ใช้เทคนิคการพิสูจน์ตัวตน (Authentication Techniques) ที่มีความมั่นคงปลอดภัยในการส่ง (Transmission Security) และความสมบูรณ์ของข้อความ (Message Integrity) ที่แข็งแกร่ง

(ค) ใช้การเข้ารหัสสำหรับการเชื่อมต่อเครือข่ายทั้งหมด เช่น https, ssh, scp เป็นต้น

(ง) ไม่อนุญาตให้เชื่อมต่อระยะไกลจากการใช้คำสั่งระบบ (Issuing System Commands) ที่จะส่งผลกระทบต่อการดำเนินการบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เว้นแต่จะได้รับอนุญาตอย่างชัดเจนเนื่องจากความต้องการทางธุรกิจ และ

(จ) จำกัดการไหลของข้อมูลเฉพาะฟังก์ชันขั้นต่ำที่จำเป็นสำหรับการเชื่อมต่อ

๒๒.๔ สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media)

๒๒.๔.๑ ต้องตรวจสอบให้แน่ใจว่ามีการใช้การควบคุมอย่างเข้มงวดในการเชื่อมต่อสื่อบันทึกข้อมูลแบบถอดได้ และอุปกรณ์คอมพิวเตอร์แบบพกพา (เช่น แล็ปท็อป) กับบริการที่สำคัญหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยใช้มาตรการอย่างน้อย ดังนี้

(ก) ในกรณีที่มีฟังก์ชันให้ปิดใช้งานพอร์ตการเชื่อมต่อภายนอกทั้งหมด (เช่น พอร์ต USB) ที่รองรับสื่อบันทึกข้อมูลแบบถอดได้ และอุปกรณ์คอมพิวเตอร์แบบพกพา และเปิดใช้งานเมื่อจำเป็นเท่านั้น

(ข) ใช้สื่อบันทึกข้อมูลที่ได้รับอนุญาตตามข้อ ๒๒.๑.๑ (ข) เท่านั้น และ

(ค) ตรวจสอบว่าสื่อบันทึกข้อมูลแบบถอดได้และอุปกรณ์คอมพิวเตอร์พกพาทั้งหมดไม่มีมัลแวร์ก่อนที่จะเชื่อมต่อกับบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๒๒.๔.๒ ต้องเข้ารหัสข้อมูลที่ละเอียดอ่อนทั้งหมดของบริการที่สำคัญของหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศบนสื่อบันทึกข้อมูลแบบถอดได้

๒๒.๕ การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)

๒๒.๕.๑ ต้องให้ความสำคัญกับแผนงานในการสร้างตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness) สำหรับพนักงาน ผู้รับเหมา และผู้ให้บริการภายนอกบุคคลที่สามที่สามารถเข้าถึงโครงสร้างพื้นฐานสำคัญทางสารสนเทศได้ ต้องมีรายละเอียดอย่างน้อย ดังต่อไปนี้

(ก) กิจกรรมให้ความรู้แก่บุคลากรทุกประเภท ได้แก่

- พนักงานใหม่ (New Employees)
- ผู้ใช้และระดับบริหาร (Users and Management)
- เจ้าหน้าที่สนับสนุนโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เช่น ผู้ให้บริการ IT และ ICS และ
- ผู้ขาย ผู้รับเหมาและผู้ให้บริการ (Vendors, Contractors and Service Providers)

(ข) การเผยแพร่ความรับผิดชอบของกลุ่มและบุคคลตามลำดับสำหรับการรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(ค) การตระหนักรู้กฎหมายความมั่นคงปลอดภัยไซเบอร์ กฎ ระเบียบ นโยบาย แนวปฏิบัติ มาตรฐาน และขั้นตอนที่เกี่ยวข้องกับการใช้งาน และการเข้าถึงโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และ

(ง) การสื่อสารอย่างสม่ำเสมอและทันท่วงทีครอบคลุมเนื้อหาสำหรับการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ และภัยคุกคามทางไซเบอร์ ผลกระทบ และการบรรเทาผลกระทบ

๒๒.๕.๒ ต้องทบทวนแผนงานในการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละหนึ่ง (๑) ครั้ง เพื่อให้แน่ใจว่าเนื้อหาของแผนงานยังคงเป็นปัจจุบันและมีรายละเอียดที่เกี่ยวข้องเหมาะสม

๒๒.๖ การแบ่งปันข้อมูล (Information Sharing)

ต้องกำหนดขั้นตอนเพื่อแบ่งปันข้อมูล เกี่ยวกับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์และภัยคุกคามทางไซเบอร์ในส่วนที่เกี่ยวกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และมาตรการบรรเทาผลกระทบใด ๆ ที่ดำเนินการเพื่อตอบสนองต่อเหตุการณ์หรือภัยคุกคามดังกล่าวกับบุคคลที่ได้รับผลกระทบหรืออาจเกิดขึ้นได้ ได้รับผลกระทบจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์หรือภัยคุกคามด้านความมั่นคงปลอดภัยไซเบอร์ (เช่น ผู้ใช้ ผู้รับเหมาที่ให้บริการแก่บริการที่สำคัญหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และเจ้าของคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ที่จำเป็นต้องเชื่อมต่อกับบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ) เพื่อให้สามารถใช้มาตรการป้องกันที่จำเป็นได้

รายละเอียด แนวทางและรูปแบบในการแบ่งปันข้อมูล เพื่อความเป็นมาตรฐานในการปฏิบัติงานและสามารถใช้ข้อมูลได้อย่างมีประสิทธิภาพ ให้เป็นไปตามหลักเกณฑ์และวิธีการที่สำนักงานประกาศกำหนด

๒๓. หัวข้อหลักที่ ๓ มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)

กรอบมาตรฐาน

๒๓.๑ การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring)

๒๓.๑.๑ ต้องสร้างกลไกและกระบวนการเพื่อ

(ก) ตรวจจับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ทั้งหมดที่เกี่ยวข้องกับบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(ข) การจัดประเภทและวิเคราะห์เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่ตรวจพบ และ

(ค) การระบุว่ามีภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศหรือไม่

๒๓.๑.๒ ต้องดำเนินการทบทวนกลไกและกระบวนการภายในข้อ ๒๓.๑.๑ อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง เพื่อให้แน่ใจว่ากลไกและกระบวนการต่าง ๆ ยังคงมีประสิทธิภาพ

๒๔. หัวข้อหลักที่ ๔ มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)

กรอบมาตรฐาน

๒๔.๑ แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)

๒๔.๑.๑ ต้องมีการจัดทำ สื่อสาร ฝึกซ้อม ทบทวน และปรับปรุง แผนการรับมือภัยคุกคามทางไซเบอร์ ตามที่ระบุไว้ในประมวลแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง เพื่อให้แน่ใจว่าแผนการรับมือภัยคุกคามทางไซเบอร์สามารถดำเนินการได้อย่างมีประสิทธิภาพและประสิทธิผล

๒๔.๒ แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)

๒๔.๒.๑ ต้องจัดทำแผนการสื่อสารในภาวะวิกฤตเพื่อตอบสนองต่อวิกฤตที่เกิดจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

๒๔.๒.๒ ต้องตรวจสอบให้แน่ใจว่าแผนการสื่อสารในภาวะวิกฤต

(ก) จัดตั้งทีมสื่อสารในภาวะวิกฤตเพื่อเปิดใช้งานในช่วงวิกฤต

(ข) ระบุสถานการณ์จำลองเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เป็นไปได้และแผนการดำเนินการที่เกี่ยวข้อง

(ค) ระบุกลุ่มเป้าหมาย และผู้มีส่วนได้ส่วนเสียสำหรับสถานการณ์จำลองเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์แต่ละประเภท

(ง) ระบุโฆษกหลักและผู้เชี่ยวชาญด้านเทคนิคที่จะเป็นตัวแทนขององค์กรเมื่อกล่าวแถลงกับสื่อมวลชน และ

(จ) ระบุแพลตฟอร์ม/ช่องทางการเผยแพร่ที่เหมาะสม (เช่น สื่อดั้งเดิม และโซเชียลมีเดีย) สำหรับการเผยแพร่ข้อมูล

๒๔.๒.๓ ต้องตรวจสอบให้แน่ใจว่าแผนการสื่อสารในภาวะวิกฤตรวมถึงการประสานงานระหว่างทุกฝ่ายที่ได้รับผลกระทบเพื่อให้แน่ใจว่ามีการตอบสนองที่ประสานกันและสอดคล้องกันในช่วงวิกฤต

๒๔.๒.๔ ต้องดำเนินการฝึกซ้อมแผนการสื่อสารในภาวะวิกฤตอย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง เพื่อให้แน่ใจว่าสามารถสื่อสารและเผยแพร่ข้อมูลได้อย่างทันท่วงทีและมีประสิทธิผลในช่วงวิกฤตอันเนื่องมาจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

๒๔.๓ การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise)

๒๔.๓.๑ ตามมาตรา ๒๒ วรรคหนึ่ง (๑๓) หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องมีส่วนร่วมในการฝึกซ้อมรับมือกับภัยคุกคามทางไซเบอร์ หากได้รับคำสั่งเป็นลายลักษณ์อักษรให้ทำโดยคณะกรรมการ การฝึกซ้อมการรักษาความมั่นคงปลอดภัยไซเบอร์ดังกล่าวอาจดำเนินการได้ ทั้งในระดับชาติหรือระดับภาคส่วน หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องตรวจสอบให้แน่ใจว่าบุคลากรที่เกี่ยวข้องที่ระบุไว้ในแผนการรับมือภัยคุกคามทางไซเบอร์มีส่วนร่วมในการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ดังกล่าว

๒๔.๓.๒ ต้องปฏิบัติตามคำขอใด ๆ ของคณะกรรมการเพื่อให้ข้อมูลที่เกี่ยวข้องกับบริการที่สำคัญหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เพื่อวัตถุประสงค์ในการวางแผนและดำเนินการฝึกซ้อมรับมือกับภัยคุกคามทางไซเบอร์ ข้อมูลที่คณะกรรมการอาจร้องขอภายใต้ข้อนี้รวมถึงแผนการรับมือภัยคุกคามทางไซเบอร์และแผนการสื่อสารในภาวะวิกฤตที่กำหนดขึ้นตามข้อ ๒๔.๑ และข้อ ๒๔.๒ ขั้นตอนการปฏิบัติงานมาตรฐานที่เกี่ยวข้องกับการดำเนินงานของบริการที่สำคัญของหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๒๕. หัวข้อหลักที่ ๕ มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)

กรอบมาตรฐาน

๒๕.๑ การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery)

๒๕.๑.๑ ต้องจัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan : BCP) เพื่อให้แน่ใจว่าบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศสามารถให้บริการที่จำเป็นต่อไปได้ในกรณีที่เกิดการหยุดชะงักเนื่องจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ เพื่อให้สามารถใช้ปฏิบัติงานได้จริง รวมถึงสอบทานแผนของผู้ให้บริการภายนอกเพื่อพิจารณาความสอดคล้องกับแผนของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เช่น ความสอดคล้องกันของขอบเขตคำนิยามและการกำหนดระยะเวลาที่สำคัญ : Maximum Tolerable Period of Disruption (MTPD), Recovery Time Objective (RTO) และ Recovery Point Objective (RPO) เป็นต้น

การจัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan : BCP) ให้เป็นไปตามหลักเกณฑ์และวิธีการที่สำนักงานประกาศกำหนด

๒๕.๑.๒ ต้องตรวจสอบให้แน่ใจว่ามีการฝึกซ้อม BCP อย่างน้อยปีละ ๑ (หนึ่ง) ครั้งเพื่อประเมินประสิทธิภาพของ BCP ต่อภัยคุกคามทางไซเบอร์และเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์



ฉบับภาษาอังกฤษ
English Version

Notification of the Cybersecurity Regulating Committee

Re: Codes of Practice and Standard Frameworks

for Government Agencies and Organizations of Critical Information Infrastructure

B.E. 2564 (2021)

Whereas it is deemed appropriate to establish Codes of Practice and Cybersecurity Standard Frameworks as minimum cybersecurity requirements for Government Agencies and Organizations of Critical Information Infrastructure. The Codes of Practice and the Cybersecurity Standard Frameworks outline risk assessment together with measures for responding and handling cybersecurity incidents or any events that may significantly cause severe impacts or damage to nation's information systems, with the aims to facilitate swift, efficient, and coherent operations that are in line with international standards.

By virtue of Section 13 paragraph one (4) and paragraph two and Section 54 of the Cybersecurity Act B.E. 2562 (2019), and in accordance with the resolution of the National Cyber Security Committee meeting No. 1/2564 on 25 June B.E. 2564 (2021), and the resolution of the Cybersecurity Regulating Committee meeting No. 1/2564 on 8 June B.E. 2564 (2021), the Cybersecurity Regulating Committee hereby issues the following notification:

Clause 1 This notification shall be called the "Notification of the Cybersecurity Regulating Committee Re: Codes of Practice and Standard Frameworks for Government Agencies and Organizations of Critical Information Infrastructure B.E. 2564 (2021)".

Clause 2 This notification shall come into force one year following its publication date in the Royal Thai Government Gazette.

Clause 3 The Codes of Practice and the Cybersecurity Standard Frameworks for Government Agencies and Organizations of Critical Information Infrastructure shall be carried out in accordance with the provisions set forth in the attached enclosure.

Clause 4 The Chairperson of the Cybersecurity Regulating Committee is hereby vested with the authority to provide interpretations and render decisions on matters related to the enforcement of compliance with this notification.

Clause 5 The Secretary-General of the National Cyber Security Committee shall have charge and control of this notification and shall be authorized to issue notifications, directives, criteria, and procedures that are conducive to the effective execution of tasks in accordance with the provisions outlined in this notification.

Any rules, regulations, notifications, or directives that contradict or conflict with the provisions contained within this notification shall be replaced by this notification.

Given on the 2nd of August B.E. 2564 (2021)

Chaiwut Thanakamanusorn

(Mr .Chaiwut Thanakamanusorn)
Minister of Digital Economy and Society
Chairperson of the Cybersecurity Regulating Committee

Codes of Practice and Standard Frameworks
for Government Agencies and Organizations of Critical Information Infrastructure
B.E. 2564 (2021)

Introduction

1. The Cybersecurity Act B.E. 2562 (2019) prescribes that there shall be codes of practices and standard frameworks as minimum cybersecurity requirements for Government Agencies and Organizations of Critical Information Infrastructure, and there shall be measures for assessing risks, responding to and handling cybersecurity incidents or events that affect or potentially cause significant or severe impacts or damage to the nation's information systems, with the aim to facilitate swift, efficient, and coherent operations in line with international standards, and to support the operations of the National Cyber Security Agency.

Objective

2. To ensure swift, efficient, and coherent operations that are in line with international standards.

Scope of Application

3. For Government Agencies and Organizations of Critical Information Infrastructure

Interpretation

4. Committee	means	the National Cyber Security Committee.
5. CRC	means	the Cybersecurity Regulating Committee.
6. Government Agency	means	the government agency designated as an Organization of Critical Information Infrastructure.
7. Critical Service	means	missions or services of Government Agencies and Organizations of Critical Information Infrastructure according to Section 49.
8. Agency	means	the National Cyber Security Agency.
9. Key Risk Indicator	means	all metrics used to assess activities that may potentially increase organizational risks, facilitate

		risk monitoring, and serve as a warning so that agencies could predict future incidents and risks, and prepare preventive measures prior to the occurrence of any potential damaging incident.
10. External Service Provider	means	an individual or juristic person who provides information technology services, or has connections to information technology systems of Government Agencies and Organizations of Critical Information Infrastructure, or could access important information of Government Agencies and Organizations of Critical Information Infrastructure or information of service recipients controlled by Government Agencies and Organizations of Critical Information Infrastructure. The External Service Provider does not encompass users of products and services offered by Government Agencies and Organizations of Critical Information Infrastructure.
11. Compiler	means	a computer program that translates a specific instruction set written in one programming language into another set of instructions in another programming language.
12. Patch	means	a computer program used to update computer software. Most of them are in a computer file format and are used to fix security vulnerabilities or upgrade the computer software's features. Many software developers have occasionally issued a Patch. For example, Microsoft may periodically release patches through its Windows Updates to fix software vulnerabilities.
13. Recovery Time Objective (RTO)	means	a period of time spent restoring a system.
14. Recovery Point Objective (RPO)	means	the maximum duration for data allowed to be lost or corrupted.

15. Maximum Tolerance Period of Disruption (MTPD) means the maximum duration during which business is allowed to be disrupted to accommodate the ongoing business operations of Government Agencies and Organizations of Critical Information Infrastructure, and to respond to various abnormal events (such as cybersecurity incidents) that may disrupt or damage the system. This aims to allow the organization to resume its normal operations as quickly as possible.

16. Codes of Practice consist of three elements:

- Cybersecurity Audit Plan
- Cybersecurity Risk Assessment
- Cybersecurity Incident Response Plan

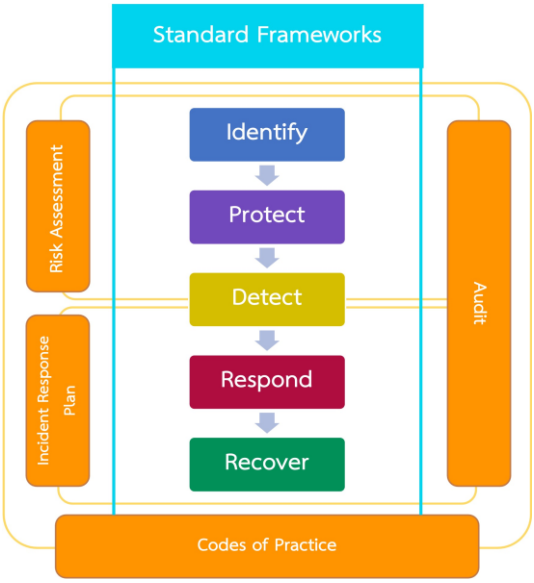


Figure 1 Cybersecurity Codes of Practice and Standard Frameworks

17. Element 1 Cybersecurity Audit Plan

Practice

17.1 A cybersecurity audit shall be conducted by internal or external information security auditors at least once a year. The scope of the audit is as follows:

(a) processes and results of Business Impact Analysis (BIA);

(b) critical services owned or utilized by Government Agencies and Organizations of Critical Information Infrastructure, which are in accordance with the analysis from Clause 17.1 (a);

(c) actions in compliance with the Cybersecurity Act, these Codes of Practice and any practices related to any codes of practice, operational standards and any notifications issued by the Committee.

17.2 Organizations of Critical Information Infrastructure shall submit the cybersecurity audit summary report to the Agency within 30 (thirty) days following the date of completion as prescribed in Section 54 along with a copy of the said report to their regulator.

The Agency shall issue a notification regarding the formats and details of the cybersecurity audit summary report.

17.3 In the event that the audit conducted pursuant to Section 54 identifies non-compliances with Clause 17.1, unless otherwise specified by the CRC in writing, the Organization of Critical Information Infrastructure shall be obliged to furnish the Agency with a corrective action plan within a period of 30 (thirty) days after the receipt of the audit report. The corrective action plan shall encompass, at a minimum, the following particulars:

(a) details of corrective actions that the Organization of Critical Information Infrastructure shall proceed to address the non-compliance matters and;

(b) a timeframe in accordance with the actions outlined in Clause 17.3 (a).

17.4 In the event that the CRC deems it necessary to revise the corrective action plan, the Organization of Critical Information Infrastructure shall promptly undertake the necessary actions and furnish the duly amended corrective action plan to the Agency within the timeframe stipulated by the CRC, and concurrently provide a copy to its regulator.

17.5 Upon the approval of the corrective action plan by the CRC, the Organization of Critical Information Infrastructure shall execute the prescribed actions as per the approved plan, within the stipulated timeframe to satisfy the criteria, set forth by the CRC.

18. Element 2 Cybersecurity Risk Assessment

Practice

To ensure that Government Agencies and Organizations of Critical Information Infrastructure can efficiently and continuously assess cybersecurity risks, they shall establish a cybersecurity risk management policy as stipulated in the Cybersecurity Management Policies for Government Agencies and Organizations of Critical Information Infrastructure. The

cybersecurity risk management policy shall include an organizational structure and designate the roles and responsibilities of all stakeholders involved in managing cybersecurity risks. Furthermore, the policy shall serve as the foundation for setting up regulations and procedures pertaining to cybersecurity risk management for Government Agencies and Organizations of Critical Information Infrastructure, which shall conduct a risk assessment at least once annually. The details of the assessment are as follows:

18.1 Risk Assessment

(a) Risk Identification

Cybersecurity risks, including those associated with cybersecurity incidents and vulnerabilities, shall be clearly identified. These risks may be resulted from operational processes, work systems, personnel, or external factors.

(b) Risk Analysis

Cybersecurity risks shall be comprehensively analyzed and clearly understood to identify appropriate risk treatments.

(c) Risk Evaluation

The likelihood of cybersecurity risk and potential impacts on performance and business operation shall be evaluated, and cybersecurity risk appetite shall also be determined.

18.2 Risk Treatment

In accordance with the findings from the risk assessment, proper guidelines shall be developed to manage, control, and prevent the risks, with consideration to cost of risk mitigation and expected benefits. This is to ensure that the residual risk remains within the Cybersecurity Risk Appetite.

In addition, to monitor and review risks, cybersecurity Key Risk Indicators (KRI), pertaining to business operations, must be designated with consideration of the significance of each cybersecurity function.

18.3 Risk Monitoring and Review

Effective cybersecurity risk monitoring and review processes shall be instituted to ensure that the risk level stays within the prescribed cybersecurity risk appetite.

18.4 Risk Reporting

Cybersecurity risk levels and outcomes of the cybersecurity risk management shall be regularly reported to the Committee designated by the agencies, for instance, during the scheduled Committee meeting.

A periodic review of the regulations and procedures pertaining cybersecurity risk management shall be conducted once a year at minimum and whenever there is a significant change in cybersecurity systems, risks, or international standards.

19. Element 3 Cybersecurity Incident Response Plan

Practice

19.1 A Cybersecurity Incident Response Plan, determining the approach for handling cybersecurity incidents, shall be formulated. The plan shall encompass, at a minimum, the subsequent particulars:

(a) structure of the Cyber Incident Response Team (CIRT), as well as the unambiguous description of roles and responsibilities, and contact details for each team member;

(b) Incident Reporting Structure, which requires Government Agencies and Organizations of Critical Information Infrastructure to perform their duties as stipulated in the Act or any subordinate legislation made thereunder, and adhere to any reporting obligations under the laws and regulations pertaining to critical information technology infrastructure;

(c) criteria and process to activate the Incident Response Plan and CIRT;

(d) containment process to minimize effects of cybersecurity incidents;

(e) activation of recovery process;

(f) investigation process to determine root causes and impacts of cybersecurity incidents;

(g) evidence preservation process (prior to the recovery process), and evidence collection process to support lawful investigation;

(h) third-party engagement protocol or third-party management guideline, which include contact details, such as those pertaining to digital forensics and data recovery service providers, as well as law enforcement; and

(i) after-action review process which identifies areas of improvement for operations in order to prevent any incidents from reoccurring.

19.2 Cybersecurity Incident Response Plan shall be communicated to all personnel that support Critical Services of Government Agencies and Organizations of Critical Information Infrastructure.

19.3 Cybersecurity Incident Response Plan shall undergo mandatory annual reviews at least once per year from the date of its approval.

19.4 Cybersecurity Incident Response Plan shall undergo a review if there are significant changes to operational environment of Critical Services provided by Government Agencies and Organizations of Critical Information Infrastructure or significant changes to regulations that affect cybersecurity incident response.

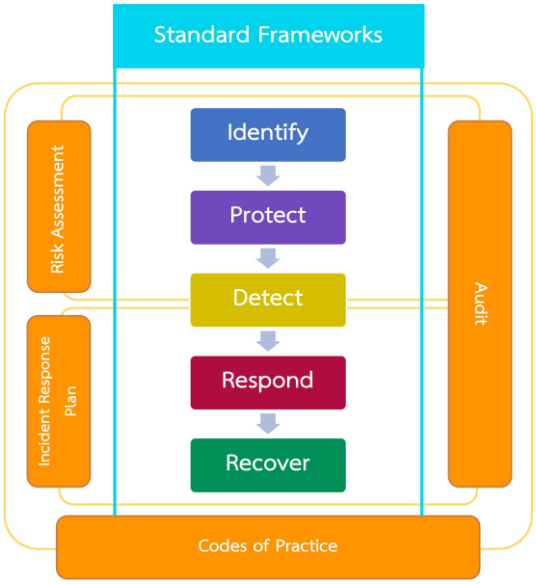


Figure. 2 Codes of Practice and Standard Framework

20. Standard Framework

Shown in Figure 2, the framework comprises 5 core functions as follows:

20.1 Identification of potential risks to computers, computer data, computer systems, other data related to computer systems, assets, and human safety (Identify)

20.1.1 Asset Management

20.1.2 Risk Assessment and Risk Management Strategy

20.1.3 Vulnerability Assessment and Penetration Testing

20.1.4 Third Party Management

20.2 Potential Risks Prevention Measure (Protect)

20.2.1 Access Control

20.2.2 System Hardening

20.2.3 Remote Connection

20.2.4 Removable Media

20.2.5 Cybersecurity Awareness Raising

20.2.6 Information Sharing

20.3 Cyber threat Monitoring and Detection Measures (Detect)

20.3.1 Incident Detection and Monitoring

20.4 Incident Response Measures (Respond)

20.4.1 Cybersecurity Incident Response Plan

20.4.2 Crisis Communication Plan

20.4.3 Cybersecurity Exercise

20.5 Incident Resilience and Recovery Measure (Recover)

20.5.1 Cybersecurity Incident Resilience and Recovery.

21. Core Function 1 Identification of potential risks to computers, computer data, computer systems, and other data related to computer systems, assets, and human safety (Identify)

Standard Framework

21.1 Asset Management

21.1.1 There shall exist an asset inventory prescribing assets of Critical Services of Government Agencies and Organizations of Critical Information Infrastructure, and the asset inventory shall be regularly maintained and updated. The said asset inventory shall at least encompass the following particulars:

(a) names/description of assets pertaining to Critical Services of Government Agencies and Organizations of Critical Information Infrastructure;

(b) critical functions of assets pertaining to Critical Services of Government Agencies and Organizations of Critical Information Infrastructure;

(c) identification and prioritization of assets pertaining to Critical Services of Government Agencies and Organizations of Critical Information Infrastructure;

(d) owners and/or operators of assets pertaining to Critical Services of Government Agencies and Organizations of Critical Information Infrastructure;

(e) physical location of assets pertaining to Critical Services of Government Agencies and Organizations of Critical Information Infrastructure; and

(f) dependencies of assets, involving Critical Services of Government Agencies and the Organizations of Critical Information Infrastructures, on internal systems and networks and/or external systems and networks.

21.1.2 Identification of network perimeter of Critical Services of Government Agencies and Organizations of Critical Information Infrastructure, and computer systems interconnected via Direct and Significant Interface.

21.1.3 The asset inventory shall undergo an annual update. In the event of any alterations to assets associated with Critical Services of Government Agencies and Organizations of Critical Information Infrastructure, the asset inventory shall be updated accordingly.

21.1.4 Pursuant to Section 54, a cybersecurity risk assessment shall be conducted for Critical Services of Government Agencies and Organizations of Critical Information Infrastructure. This risk assessment shall include all components outlined within the asset inventory, as specified in Clause 21.1.1, and shall be conducted at least once a year.

21.2 Risk Assessment and Risk Management Strategy

21.2.1 As stipulated by the cybersecurity risk-assessment criteria established in the Risk Management section of the Management Policies concerning Cybersecurity for Government Agencies and Organizations of Critical Information Infrastructure issued by the Committee, cybersecurity risk assessment shall be conducted at least once a year, or whenever there are significant changes that affect critical information infrastructures of Government Agencies and Organizations of Critical Information Infrastructure.

21.2.2 The risk register shall be expeditiously updated subsequent to the completion of the cybersecurity risk assessment. The risk register shall, at a minimum, encompass the following particulars:

(a) Date the Risk is Identified;

(b) Description of the Risk;

(c) Likelihood of Occurrence;

(e) Severity of the Occurrence;

(f) Risk Treatment;

(g) Risk Owner;

(h) Status of Risk Treatment; and,

(i) Residual Risk.

21.3 Vulnerability Assessment and Penetration Testing

21.3.1 Vulnerability assessment for Critical Services of Government Agencies and Organizations of Critical Information Infrastructure shall be undertaken in accordance with their risk management principles. The assessment aims to identify vulnerabilities in cybersecurity

and control of all Critical Services of Government Agencies and Organizations of Critical Information Infrastructure which includes:

(a) Information Technology (IT) system;

(b) Industrial Control System (ICS).

21.3.2 Supervision is mandated to verify that scope of vulnerability assessment shall encompass the subsequent particulars:

(a) Host Security Assessment;

(b) Network Security Assessment; and,

(c) Architecture Security Review.

21.3.3 Vulnerability assessment for Critical Services of Government Agencies and Organizations of Critical Information Infrastructure shall be conducted to identify and control vulnerabilities in cybersecurity before testing any new systems that will be connected to the Critical Services, or before implementing any changes of systems that are vital to the Critical Services. The changes include the addition of new application modules, system updates, and technological modifications.

21.3.4 Penetration testing should be undertaken for Critical Services of Government Agencies and Organizations of Critical Information Infrastructure, specifically Information Technologies (IT) with internet-facing components, to ensure the conformity with the predetermined risk levels. Impacts and potential risks arising from the penetration testing shall also be evaluated.

21.3.5 It is imperative to ensure that the penetration testing includes hosts, networks, and applications of Critical Services of Government Agencies and Organizations of Critical Information Infrastructure, especially all Internet-facing ones.

21.3.6 The penetration testing shall be carried out at least once a year, or as many times as required, to validate cybersecurity systems of Critical Services of Government Agencies and Organizations of Critical Information Infrastructure. This validation shall be conducted prior to the testing of any new systems or significant system changes, such as introduction of add-on modules, system updates, or technological modifications.

21.3.7 It is mandatory to ascertain that both penetration testing activities and penetration testers who perform such activities on critical information infrastructure shall possess necessary accreditations and certifications with industry recognition. Furthermore, these individuals shall maintain independence from the systems under the test. The

qualifications of the penetration testers shall comply with criteria and procedures established by the regulator.

21.3.8 It is mandatory to ascertain that all the penetration testing activities conducted by service providers shall be under supervision of Government Agencies and Organizations of Critical Information Infrastructure.

21.3.9 Vulnerability tracking and management process shall be established to address vulnerabilities discovered during vulnerability assessments and penetration testing, and to ensure that all discovered vulnerabilities are adequately mitigated.

21.3.10 Upon request by the CRC or the Agency, the Organization of Critical Information Infrastructure shall furnish a copy of summary report of penetration testing to the Agency within 30 (thirty) days of receipt of the request letter. The summary report will be used to evaluate cybersecurity risk level of the Organization of Critical Information Infrastructure.

The structure and content of the penetration testing summary report must adhere to the criteria and procedures delineated in the notification prescribed by the Agency.

21.4 Third Party Management

21.4.1 Government Agencies and Organizations of Critical Information Infrastructure shall be responsible and accountable for cybersecurity of critical information infrastructure although third-party service providers are the ones engaging in any operations of Critical Services of the Government Agencies and Organizations of Critical Information Infrastructure.

21.4.2 There shall be a formulation of cybersecurity requirements to mitigate risks inherent to third-party service providers' accesses to storages, communications, and operations of Critical Information Infrastructure. Such requirements shall be stated particularly in Service Level Agreements or contractual provisions with the said third-party service providers. These requirements shall be set forth in no less detail than the following:

(a) types of third-party service providers eligible to access Assets of Critical Services of Government Agencies and Organizations of Critical Information Infrastructure according to business needs and cybersecurity risk profile;

(b) obligations of third-party service providers to protect Critical Services of Government Agencies and Organizations of Critical Information Infrastructure from cybersecurity incidents;

(c) risks related to services, supply chain, products; and

(d) rights of Government Agencies and Organizations of Critical Information Infrastructure to audit cybersecurity third party service providers.

21.4.3 Auditing and monitoring processes shall be established to ensure that third-party service providers are in adherence to cybersecurity requirements specified within the contract. Such processes may encompass third-party audits and product validation.

21.4.4 Contract negotiations shall be undertaken to ensure their alignment with laws and regulations or newly enacted provisions.

22. Core Function 2 Preventive Measures for Potential Risks (Protect)

Standard Framework

22.1 Access Control

22.1.1 It is mandatory to ascertain that accesses to Critical Services of Government Agencies and Organizations of Critical Information Infrastructure are restricted to:

(a) authorized personnel and activities; and,

(b) authorized devices and Interface.

22.1.2 In accordance with the obligations outlined in Clause 22.1.1, Government Agencies and Organizations of Critical Information Infrastructure shall require authorized personnel, activities, and processes to have authorization checking techniques consistent with Cybersecurity Risk Profile for each mode of accesses to Critical Services of Government Agencies and Organizations of Critical Information Infrastructure.

22.1.3 Logs of all accesses and any attempts to access Critical Services of Government Agencies and Organizations of Critical Information Infrastructure shall be meticulously maintained and be subject to regular analysis to detect abnormal activities. The frequency of such analysis shall be aligned with the frequency and regularity of the accesses.

22.1.4 It is mandatory to ascertain that accesses to interfaces of Critical Services of Government Agencies and Organizations of Critical Information Infrastructure via physical, for example, USBs, serial ports, and logical accesses, are regulated:

(a) under supervision of the Government Agencies and the Organizations of Critical Information Infrastructure; and,

(b) within the premises and grounds, if feasible.

22.2 System Hardening

22.2.1 Security Baseline Configuration Standards shall be established for the operating systems, applications, and network devices of Critical Services of Government Agencies and Organizations of Critical Information Infrastructure. These standards shall be aligned with Cybersecurity Risk Profile associated with the Critical Services.

22.2.2 Security Baseline Configuration Standards shall at least encompass the following principles:

(a) Least access privilege;

(b) Separation of duties;

(c) Enforcement of password complexities policies;

(d) Removal of unused accounts;

(e) Removal of unnecessary services and applications, such as compilers, and vendor support applications;

(f) Disabling unused network ports;

(g) Malware protection; and,

(h) Updating software and installing security patches in a timely and appropriate manner.

22.2.3 It is mandatory to ascertain that Security Baseline Configuration Standards are met at a minimum prior to having new assets connected to or when there are changes or updates in Critical Services of Government Agencies and Organizations of Critical Information Infrastructure.

22.2.4 Security Baseline Configuration Standards of Critical Services of Government Agencies and Organizations of Critical Information Infrastructure shall be subject to a review at a minimum frequency of once per annum to ascertain the efficacy of these standards in safeguarding against cybersecurity incidents.

22.2.5 A Change Management Process shall be instituted to authorize and validate all system changes in Critical Services of Government Agencies and Organizations of Critical Information Infrastructure.

22.3 Remote Connection

22.3.1 It is mandatory to ascertain that all remote connections to Critical Services of Government Agencies and Organizations of Critical Information Infrastructure are

equipped with robust cybersecurity measures designed to prevent and detect any unauthorized access.

22.3.2 Remote Connection to Critical Services of Government Agencies and Organizations of Critical Information Infrastructure shall be performed according to the following practices:

(a) where functionally possible, enable connections to or from remote sites only when they are necessary;

(b) wherever available, implement strong authentication techniques that utilize transmission security, and message integrity;

(c) all connections to networks must be encrypted using protocols such as https, ssh, and scp;

(d) strictly prohibit remote connections from issuing system commands that would impact operations of Critical Services of Government Agencies and Organizations of Critical Information Infrastructure, unless otherwise explicitly permitted according to business needs; and

(e) restrict data flows only to the minimum functions required for establishing connections.

22.4 Removable media

22.4.1 It is mandatory to ascertain that strict controls are exercised when connecting removable media and portable computing devices (e.g., laptop computers) to Critical Services of Government Agencies and Organizations of Critical Information Infrastructure. At a minimum, the following prescribed measures must be employed:

(a) where the “enable/disable” function is available, disable all external interfaces (e.g., USB ports) supporting removable media and portable computing devices, and enable only when deemed necessary;

(b) use solely storage media that have been duly authorized under Clause 22.1.1 (b); and,

(c) thoroughly verify absence of malware on all removable media and portable computing devices prior to connecting to Critical Services of Government Agencies and Organizations of Critical Information Infrastructure.

22.4.2 All sensitive information of Critical Services of Government Agencies and Organizations of Critical Information Infrastructure on removable media shall be encrypted.

22.5 Cybersecurity Awareness Promotion

22.5.1 A focus shall be directed toward a cybersecurity awareness program to promote cybersecurity awareness among personnel, contractors, and the third-party service providers, who are granted accesses to critical information infrastructures. The program shall, at a minimum, encompass subsequent particulars:

(a) activities designed to impart knowledge for all categories of personnel, including:

- new employees;
- users and management;
- staff supporting critical information infrastructures, for example, IT and ICS operators; and,
- vendors, contractors, and service providers;

(b) dissemination of stipulated responsibilities of groups and individuals, based on the importance of their roles in safeguarding Critical Services of Government Agencies and Organizations of Critical Information Infrastructure;

(c) awareness of cybersecurity laws, rules, regulations, policies, codes of practices, standards, and procedures governing usage of and accesses to Critical Information Infrastructures; and

(d) regular and timely communications, covering content relevant to cultivating awareness in cybersecurity and cyber threats, impacts, and mitigations.

22.5.2 The cybersecurity awareness program shall be subject to an annual review to ensure that its contents remain up to date and relevant.

22.6 Information Sharing

Information sharing procedures and threat mitigation measures shall be formally established, with individuals affected or potentially affected by cybersecurity incidents or threats, pertaining to the incidents or threats involving Critical Information Infrastructures. These individuals include users of Critical Information Infrastructures, contractors providing services to Critical Services of Government Agencies and Organizations of Critical Information Infrastructure, computer owners, or computer systems necessarily connected to Critical Services of Government Agencies and Organizations of Critical Information Infrastructure. The establishment of these procedures is imperative to apply necessary preventive measures.

To standardize operational practices and facilitate efficient information usage, the particulars, guidelines, and formats of information sharing shall be established in accordance with the criteria and procedures prescribed by the Agency.

23. Core Function 3 Cyber Threat Monitoring and Detection Measures (Detect)

Standard Framework

23.1 Cyber Threat Detection and Monitoring

23.1.1 Mechanisms and processes shall be established to

(a) detect all cybersecurity events in respect of Critical Services of Government Agencies and Organizations of Critical Information Infrastructure;

(b) classify and analyze the identified cybersecurity events; and,

(c) determine whether there are or have been any cybersecurity incidents involving Critical Services of Government Agencies and Organizations of Critical Information Infrastructure.

23.1.2 The mechanisms and processes described in Clause 23.1.1 shall be reviewed at least once a year to ensure their continuing effectiveness.

24. Core Function 4 Incident Response Measures (Respond)

Standard Framework

24.1 Cybersecurity Incident Response Plan

24.1.1 A Cybersecurity Incident Response Plan shall be formulated, disseminated, exercised, reviewed, and improved at least once per year, in accordance with the Cybersecurity Codes of Practice, to ensure that it can be utilized efficiently and effectively.

24.2 Crisis Communication Plan

24.2.1 Crisis Communication Plan designed to respond to crises stemming from cybersecurity incidents shall be formulated.

24.2.2 It is mandatory to ascertain that the Crisis Communication Plan shall:

(a) establish a crisis communication team to be activated during a crisis;

(b)identify probable cyber incident scenarios and their corresponding operational plans;

(c) identify the target group and stakeholders for each type of cyber incident scenarios;

(d) identify primary spokespersons and technical experts designated to represent the organization in engagement with the media; and

(e) identify appropriate platforms/ channels (such as traditional media and social media) for dissemination of information related to cybersecurity incidents.

24.2.3 It is imperative to ensure the Crisis Communication Plan includes the coordination among all impacted parties to guarantee consistent and coordinated responses throughout crisis.

24.2.4 Exercises of Crisis Communication Plans shall be conducted at least once a year to facilitate prompt and efficient communication and dissemination of information during cybersecurity-related crises.

24.3 Cybersecurity Exercise

24.3.1 Pursuant to Section 22 paragraph one (13), Government Agencies and Organizations of Critical Information Infrastructure are obligated to participate in Cybersecurity Exercises addressing cybersecurity incident handling. The specific requirements of participation shall be set forth in written directives issued by the Committee. The exercises shall be undertaken at a national level or sectoral level. Government Agencies and Organizations of Critical Information Infrastructure shall ascertain the participation of all personnel assigned in the Cybersecurity Incident Response plan in these Cybersecurity Exercises.

24.3.2 Government agencies and Organizations of Critical Information Infrastructure shall comply with the Committee's requests for information pertaining to Critical Services of Government Agencies and Organizations of Critical Information Infrastructure. This information is intended for planning and executing cybersecurity incident response exercises. Information that the Committee may request under this clause may encompass the Cybersecurity Incident Response Plan in Clause 24.1, the Crisis Communication Plans in Clause 24.2, and standard operating procedures pertaining to Critical Services of Government Agencies and Organizations of Critical Information Infrastructure.

25. Core Function 5 Incident Resilience and Recovery Measures (Recover)

Standard Framework

25.1 Cybersecurity Resilience and Recovery

25.1.1 Business Continuity Plan (BCP) shall be formulated to ensure uninterrupted provision of Critical Services of Government Agencies and Organizations of Critical Information Infrastructure in the event of service disruption due to a cybersecurity incident. Government Agencies and Organizations of Critical Information Infrastructure shall validate practical applicability of the plan, and review plans provided by third-party service providers to assess alignment of their plans with the BCP in various areas, such as definitions

and critical timelines, which include Maximum Tolerable Period of Disruption (MTPD), Recovery Time Objective (RTO), and Recovery Point Objective (RPO).

The formulation of Business Continuity Plan (BCP) shall comply with the criteria and procedures stipulated in the Agency's official notification of requirements.

25.1.2 It is mandatory to ascertain that exercises for the Business Continuity Plan (BCP) are conducted at least once a year to assess its effectiveness in addressing cybersecurity incidents and cybersecurity events.

6

ประกาศ กมช.

เรื่อง การกำหนดระดับความรู้ความชำนาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อแต่งตั้งเป็นพนักงานเจ้าหน้าที่ พ.ศ. 2564

มีผลใช้บังคับตั้งแต่วันที่ 8 ธ.ค. 64 เป็นต้นไป

Notification of NCSC

Re: Cybersecurity Knowledge and Expertise Requirements for Competent Official Appointment B.E. 2564 (2021)

effective from December 8, 2021, onwards.



ฉบับภาษาไทย
Thai Version

ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

เรื่อง การกำหนดระดับความรู้ความชำนาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
เพื่อแต่งตั้งเป็นพนักงานเจ้าหน้าที่

พ.ศ. ๒๕๖๔

เพื่อให้การแต่งตั้งพนักงานเจ้าหน้าที่ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มีความชัดเจนและเป็นไปอย่างมีประสิทธิภาพ

อาศัยอำนาจตามความในมาตรา ๑๙ วรรคสอง แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ประกอบมติคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ครั้งที่ ๒/๒๕๖๔ เมื่อวันที่ ๔ ตุลาคม ๒๕๖๔ คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติจึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง การกำหนดระดับความรู้ความชำนาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อแต่งตั้งเป็นพนักงานเจ้าหน้าที่ พ.ศ. ๒๕๖๔”

ข้อ ๒ ประกาศนี้มีผลใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ข้อ ๓ ในประกาศนี้

“พนักงานเจ้าหน้าที่” หมายความว่า ผู้ซึ่งรัฐมนตรีแต่งตั้งให้ปฏิบัติการตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

“รัฐมนตรี” หมายความว่า นายกรัฐมนตรี

ข้อ ๔ พนักงานเจ้าหน้าที่ต้องมีคุณสมบัติ ดังต่อไปนี้

(๑) มีคุณสมบัติอย่างหนึ่งอย่างใด ดังต่อไปนี้

(๑.๑) รับราชการ หรือเคยรับราชการ หรือเป็นบุคคลที่ทำงานเกี่ยวกับการสืบสวนสอบสวนหรือวิเคราะห์ข้อมูล (Data Analyst) ไม่น้อยกว่า ๒ (สอง) ปี ในตำแหน่งที่เกี่ยวข้องกับด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security) ด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) ด้านการบริหารจัดการเหตุภัยคุกคามไซเบอร์ (Incident Handling) หรือด้านการพิสูจน์หลักฐานทางดิจิทัล (Digital Forensics) หรือ

(๑.๒) สำเร็จการศึกษาไม่น้อยกว่าระดับปริญญาตรี หรือเทียบเท่าทางวิศวกรรมศาสตร์ วิทยาศาสตร์ วิทยาการคอมพิวเตอร์ เทคโนโลยีสารสนเทศ สถิติศาสตร์ นิติศาสตร์ รัฐศาสตร์ รัฐประศาสนศาสตร์ หรือด้านอื่นที่เกี่ยวข้อง และเป็นประโยชน์ต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ ดังต่อไปนี้

ก. สำเร็จการศึกษาตาม (๑.๒) ในระดับปริญญาตรี หรือเทียบเท่าและมีประสบการณ์ที่เป็นประโยชน์ต่อการปฏิบัติงานตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ นับแต่สำเร็จการศึกษาดังกล่าวไม่น้อยกว่า ๔ (สี่) ปี

ข. สำเร็จการศึกษาตาม (๑.๒) ในระดับปริญญาโทและมีประสบการณ์ที่เป็นประโยชน์ต่อการปฏิบัติงานตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ นับแต่สำเร็จการศึกษาดังกล่าวไม่น้อยกว่า ๓ (สาม) ปี

ค. สำเร็จการศึกษาตาม (๑.๒) ในระดับปริญญาเอกและมีประสบการณ์ที่เป็นประโยชน์ต่อการปฏิบัติงานตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ นับแต่สำเร็จการศึกษาดังกล่าวไม่น้อยกว่า ๒ (สอง) ปี

(๒) มีความรู้ความชำนาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

(๓) ผ่านการอบรมด้านจริยธรรม สืบสวน สอบสวน ความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security) การบริหารจัดการเหตุภัยคุกคามไซเบอร์ (Incident Handling) หรือการพิสูจน์หลักฐานทางดิจิทัล (Digital Forensics) ตามภาคผนวกท้ายประกาศนี้

ข้อ ๕ ในกรณีที่มีเหตุผลความจำเป็น รัฐมนตรีอาจยกเว้นคุณสมบัติตามข้อ ๔ ไม่ว่าทั้งหมดหรือบางส่วนก็ได้ ทั้งนี้ ในการยกเว้นคุณสมบัติดังกล่าว ให้สำนักงานแสดงเหตุผลความจำเป็นเสนอรัฐมนตรีเพื่อใช้ประกอบการพิจารณาแต่งตั้งบุคคลใดเป็นพนักงานเจ้าหน้าที่เป็นการเฉพาะก็ได้

ทั้งนี้ บุคคลที่ได้รับการยกเว้นคุณสมบัติตามวรรคหนึ่ง ต้องผ่านการอบรมหลักสูตรเร่งรัด (Intensive Courses) ตามภาคผนวกท้ายประกาศนี้ด้วย

ข้อ ๖ พนักงานเจ้าหน้าที่ต้องมีสัญชาติไทยและไม่มีลักษณะต้องห้าม ดังต่อไปนี้

(๑) เป็นบุคคลล้มละลาย หรือเคยเป็นบุคคลล้มละลายทุจริต

(๒) เป็นคนไร้ความสามารถ หรือคนเสมือนไร้ความสามารถ

(๓) เคยต้องคำพิพากษาถึงที่สุดให้จำคุกไม่ว่าจะได้รับโทษจำคุกจริงหรือไม่ เว้นแต่เป็นโทษสำหรับความผิดที่ได้กระทำโดยประมาทหรือความผิดลหุโทษ

(๔) เคยถูกไล่ออก ปลดออก หรือให้ออกจากราชการ หรือออกจากงานจากหน่วยงานที่เคยปฏิบัติหน้าที่เพราะทุจริตต่อหน้าที่หรือประพฤติชั่วอย่างร้ายแรง

(๕) เคยถูกถอดถอนออกจากตำแหน่งตามกฎหมาย

(๖) เป็นผู้ดำรงตำแหน่งทางการเมือง สมาชิกสภาท้องถิ่นหรือผู้บริหารท้องถิ่น กรรมการหรือผู้ดำรงตำแหน่งซึ่งรับผิดชอบการบริหารพรรคการเมือง ที่ปรึกษาพรรคการเมือง หรือเจ้าหน้าที่ของพรรคการเมือง

ข้อ ๗ การแต่งตั้งบุคคลหนึ่งบุคคลใดเป็นพนักงานเจ้าหน้าที่ ให้แต่งตั้งจากบุคคลซึ่งมีคุณสมบัติตามข้อ ๔ หรือข้อ ๕ และไม่มีลักษณะต้องห้ามตามข้อ ๖

การแต่งตั้งบุคคลใดเป็นพนักงานเจ้าหน้าที่ตามวรรคหนึ่ง ให้พนักงานเจ้าหน้าที่ดำรงตำแหน่งคราวละ ๔ (สี่) ปี

การแต่งตั้งและการพ้นจากตำแหน่งของพนักงานเจ้าหน้าที่ ให้ประกาศในราชกิจจานุเบกษา

ข้อ ๘ พนักงานเจ้าหน้าที่พ้นจากตำแหน่ง เมื่อ

(๑) ตาย

(๒) ลาออก

(๓) มีลักษณะต้องห้ามตามข้อ ๖

(๔) คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติมีมติให้ออกเพราะบกพร่องหรือทุจริตต่อหน้าที่ มีความประพฤติเสื่อมเสีย

(๕) ครบวาระการดำรงตำแหน่ง

ประกาศ ณ วันที่ ๑๙ พฤศจิกายน พ.ศ. ๒๕๖๔
พลเอก ประวิตร วงษ์สุวรรณ
รองนายกรัฐมนตรี ปฏิบัติหน้าที่
ประธานกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

ภาคผนวก

ท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
เรื่อง การกำหนดระดับความรู้ความชำนาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
เพื่อแต่งตั้งเป็นพนักงานเจ้าหน้าที่

พ.ศ. ๒๕๖๔

ผู้ที่จะได้รับการแต่งตั้งให้เป็นพนักงานเจ้าหน้าที่ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ จะต้องผ่านการอบรมด้านจริยธรรม สืบสวน สอบสวน ที่เกี่ยวข้องกับด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security) ด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) ด้านการบริหารจัดการเหตุภัยคุกคามไซเบอร์ (Incident Handling) หรือด้านการพิสูจน์หลักฐานทางดิจิทัล (Digital Forensics) แล้วแต่กรณี ดังต่อไปนี้

๑. หลักสูตรมาตรฐานสากล (International Standard Courses)

วัตถุประสงค์ : เพื่อใช้เป็นแนวทางในการจัดอบรมให้กับบุคคลซึ่งจะได้รับการแต่งตั้งเป็นพนักงานเจ้าหน้าที่ในกรณีทั่วไป (หลักสูตรเต็มเวลาประมาณ ๑ เดือน) ทั้งภาคทฤษฎีและปฏิบัติ

เนื้อหาหลักสูตรที่อบรม :

ด้านแรก การอบรมด้านจริยธรรม/จรรยาบรรณที่พึงมีในบทบาทและอำนาจหน้าที่เป็นพนักงานเจ้าหน้าที่

ด้านที่สอง ความรู้พื้นฐานด้านการสืบสวนและสอบสวน เพื่อการบังคับใช้กฎหมาย (Law Enforcement)

ลำดับ	เนื้อหาหลักสูตร
๑	กฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์
๒	กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
๓	กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล
๔	กฎหมายอาญาและวิธีพิจารณาความอาญาที่เกี่ยวข้องกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
๕	รูปแบบการกระทำความผิดและกรณีศึกษา (Case Studies)
๖	แนวทางปฏิบัติในการดำเนินคดี/การทำสำนวนคดี เช่น การร้องทุกข์กล่าวโทษ (การแจ้งความ) การประสานความร่วมมือกับหน่วยงานที่เกี่ยวข้อง การรวบรวมพยานหลักฐาน และแสวงหาข้อเท็จจริง การตรวจสถานที่เกิดเหตุ การยื่นคำร้องต่อศาล การยึดอายัดและคืนพยานหลักฐาน การเก็บรักษา พยานหลักฐานให้คงความน่าเชื่อถือในกระบวนการเปรียบเทียบปรับและการดำเนินคดี เป็นต้น
๗	การบริหารจัดการคดีให้เป็นไปอย่างมีประสิทธิภาพ

ด้านที่สาม ความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security)

ลำดับ	เนื้อหาหลักสูตร
๑	General security concepts and Management
๒	Treats, Attacks and Vulnerabilities
๓	Network Components and Protocol
๔	System Architecture and topology
๕	Secure System Design and Secure Application Development
๖	Identity and Access Management
๗	Risk Management
๘	Cryptography

ด้านที่สี่ การบริหารจัดการเหตุภัยคุกคามไซเบอร์ (Incident Handling)

ลำดับ	เนื้อหาหลักสูตร
๑	Fundamentals of Incident Management
๒	Incident Handling and Response Program Planning
๓	Anti-forensics Techniques
๔	Malware Incident Handling and Response
๕	Email Security Incident Handling and Response
๖	Network Security Incident Handling and Response
๗	Web Security Incident Handling and
๘	Response Cloud Security Incident Handling and Response
๙	Insider Threat-related Incident Handling and Response

ด้านที่ห้า การพิสูจน์หลักฐานทางดิจิทัล (Digital Forensics)

ลำดับ	เนื้อหาหลักสูตร
๑	Fundamentals of Computer Forensics and Forensic Readiness
๒	Computer Forensics Investigation Process - Obtain Search Warrant - Evaluate and Secure the Scene - Collect the Evidence - Secure the Evidence and Chain of Custody - Acquire Data and Analyze Data - Assess Evidence and Case - Testify as Expert Witness
๓	Defeating Anti-Forensics Techniques
๔	Operating System Forensics
๕	Network Forensics
๖	Web Attack Forensics
๗	Database Forensics
๘	Cloud Forensics
๙	Wireless Forensics
๑๐	Malware Forensics
๑๑	Email-Crime Forensics
๑๒	Mobile Forensics
๑๓	Application Password Cracker
๑๔	Investigative Reports

๒. หลักสูตรเร่งรัด (Intensive Courses) (๕ วัน)

วัตถุประสงค์ : เพื่อใช้เป็นแนวทางในการจัดอบรมให้กับบุคคลซึ่งจะได้รับการแต่งตั้งเป็นพนักงานเจ้าหน้าที่ในกรณีพิเศษ ซึ่งได้รับการยกเว้นตามหลักเกณฑ์ในการกำหนดคุณสมบัติเป็นพนักงานทั่วไป ให้สามารถบริหารจัดการภัยคุกคามไซเบอร์เบื้องต้นได้

เนื้อหาหลักสูตรที่อบรม :

ด้านแรก การอบรมด้านจริยธรรม/จรรยาบรรณที่พึงมีในบทบาทและอำนาจหน้าที่เป็นพนักงานเจ้าหน้าที่

ด้านที่สอง ความรู้พื้นฐานด้านการสืบสวนและสอบสวนเพื่อการบังคับใช้กฎหมาย (Law Enforcement)

ลำดับ	เนื้อหาหลักสูตร
๑	กฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์
๒	กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
๓	กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล
๔	กฎหมายอาญาและวิธีพิจารณาความอาญาที่เกี่ยวข้องกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
๕	รูปแบบการกระทำความผิดและกรณีศึกษา (Case Studies)
๖	แนวทางปฏิบัติในการดำเนินคดี/การทำสำนวนคดี เช่น การร้องทุกข์กล่าวโทษ (การแจ้งความ) การประสานความร่วมมือกับหน่วยงานที่เกี่ยวข้อง การรวบรวมพยานหลักฐาน และแสวงหาข้อเท็จจริง การตรวจสถานที่เกิดเหตุ การยื่นคำร้องต่อศาล การยึดอายัดและคืนพยานหลักฐาน การเก็บรักษา พยานหลักฐานให้คงความน่าเชื่อถือในกระบวนการเปรียบเทียบปรับและการดำเนินคดี เป็นต้น
๗	การบริหารจัดการคดีให้เป็นไปอย่างมีประสิทธิภาพ

ด้านที่สาม การบริหารจัดการเหตุภัยคุกคามไซเบอร์ (Incident Handling) และการพิสูจน์หลักฐานทางดิจิทัล (Digital Forensics)

ลำดับ	เนื้อหาหลักสูตร
๑	Fundamentals of Incident Management
๒	Incident Handling and Response Program Planning
๓	Anti-forensics Techniques
๔	Malware Incident Handling and Response
๕	Email Security Incident Handling and Response
๖	Network Security Incident Handling and Response
๗	Web Security Incident Handling and Response
๘	Cloud Security Incident Handling and Response
๙	Insider Threat-related Incident Handling and Response
๑๐	Fundamentals of Computer Forensics
๑๑	Computer Forensics Investigation Process
๑๒	Investigative Reports



ฉบับภาษาอังกฤษ
English Version

Notification of the National Cyber Security Committee

Re: Cybersecurity Knowledge and Expertise Requirements

for Competent Official Appointment

B.E. 2564 (2021)

Whereas it is appropriate to have a transparent and efficient appointment of Competent Officials in accordance with the Cybersecurity Act B.E. 2562 (2019).

By virtue of section 19, paragraph two of the Cybersecurity Act B.E. 2562 (2019) and the resolution adopted by the National Cyber Security Committee meeting no. 2/2564 on 4 October B.E. 2564 (2019), the National Cyber Security Committee hereby issues the following notification:

Clause 1 This notification shall be called the "Notification of the National Cyber Security Committee Re: Cybersecurity Knowledge and Expertise Requirements for Competent Official Appointment B.E. 2564 (2021)".

Clause 2 This notification shall come into force on the date following its publication date in the Royal Thai Government Gazette.

Clause 3 In this notification

"Competent Official" shall mean a person appointed by the Minister for the execution of the Cybersecurity Act B.E.2562 (2019);

"Minister" shall mean the Prime Minister;

Clause 4 A Competent Official must have the following qualifications:

(1) having one of the following qualifications:

(1.1) be a current or former civil servant or an individual with a minimum of 2 (two) years of professional experience as an investigator or a data analyst in the branch of information security, cybersecurity, incident handling or digital forensics or;

(1.2) have at least a Bachelor's degree or its equivalent in Engineering, Science, Information Technology, Statistics, Law, Political Science, Political and Administrative Science, or any other field related to and beneficial for cybersecurity, with the following details:

a. graduate with a bachelor's degree or its equivalent in accordance with (1.2) and have a minimum of 4 (four) years of experience that are beneficial for the tasks specified in the Cyber Security Act B.E. 2562 (2019);

b. graduate with a master's degree in accordance with (1.2) and have a minimum of 3 (three) years of experience that are beneficial for the tasks specified in the Cybersecurity Act B.E. 2562 (2019);

c. graduate with a Ph.D. in accordance with (1.2) and have a minimum of 2 (two) years of experience that are beneficial for the tasks specified in the Cybersecurity Act B.E. 2562 (2019);

(2) have the knowledge and expertise in cybersecurity;

(3) undertake trainings in ethical practice, investigation, and interrogation related to information security, cybersecurity incident handling or digital forensics as specified in the appendix of this notification.

Clause 5 If deemed necessary, the Minister may grant a partial or full exemption from the qualification requirements in Clause 4. The Agency shall provide justifications to the Minister during the Competent Official appointment process of an individual in a specific case.

Nonetheless, any person granted an exemption from the qualification requirements in paragraph one must complete the intensive courses as specified in the appendix of this notification.

Clause 6 A Competent Official must have Thai nationality and not have any prohibited characteristics as specified in the following:

(1) be a bankrupted person or used to be a dishonestly bankrupted person;

(2) be an incompetent or quasi-incompetent person;

(3) having been previously imprisoned by final court judgement, regardless of whether there was actual punishment of imprisonment, except for offenses committed by negligence or misdemeanors;

(4) having been previously dismissed, fired, or removed from an official position or any other previous organization on grounds of dishonest performance of duties or severe wrongful conduct;

(5) having been previously removed from an official position by way of the law;

(6) be a person holding a political position or serving as a local councilor, local administer, or director of, or a person responsible for managing a political party, counsel of a political party, or an officer of a political party.

Clause 7 Any person to be appointed a Competent Official must possess the qualifications specified in Clause 4 or Clause 5 and must not have any prohibited characteristics as specified in Clause 6.

Any person to be appointed a Competent Official according to paragraph one shall have a 4 (four) year term.

The appointment and vacation of office of a Competent Official shall be announced in the Royal Thai Government Gazette.

Clause 8 A Competent Official shall vacate the office upon:

(1) death;

(2) resignation;

(3) possessing prohibited characteristics as specified in Clause 6;

(4) resolution for removal passed by the National Cyber Security Committee on grounds of unsatisfactory or dishonest performance of duties, disgraceful behavior;

(5) expiration of term.

Given on the of November B.E. 2564 (2021)

General Pravit Wongsuwan

(Pravit Wongsuwan)

Deputy Prime Minister as

Chairman of the National Cyber Security Committee

Appendix

Annex to the Notification of the National Cyber Security Committee

Re: Cybersecurity Knowledge and Expertise Requirements

for Competent Official Appointment

B.E. 2564 (2021)

A Competent Official appointed under the Cybersecurity Act B.E. 2562 (2019) must undergo trainings on ethics and the procedures for conducting investigations and inquiries related to information security, cyber incident handling, or digital forensics, depending on the needs of each individual, as outlined below:

1. International Standard Curriculum

Objective: To implement as a guideline in providing both theoretical and practical trainings to individuals that will be appointed a Competent Official in a general circumstance (The full course length is about 1 month).

Contents:

Part I **Ethical and professional conduct trainings to perform the role and execute duties as a Competent Official**

Part II **Basic knowledge in investigation for law enforcement**

No.	Course Content
1	Laws regarding maintaining cybersecurity
2	Laws regarding the commission of computer-related offenses
3	Laws regarding the protection of private information
4	The Penal Code and criminal procedure regarding the commission of computer-related offenses
5	Offense pattern and case studies
6	Guidelines in case proceeding and preparation such as complaint and allegation (filing a police report), coordination with relevant agencies, evidence compilation and fact inquiry, scene inspection, submitting motion to the competent court, evidence seizure and release, evidence preservation to maintain credibility in the prosecution and fine imposition processes
7	Effective case management

Part III Information Security

No.	Course Content
1	General Security Concepts and Management
2	Treats, Attacks and Vulnerabilities
3	Network Components and Protocol
4	System Architecture and Topology
5	Secure System Design and Secure Application Development
6	Identity and Access Management
7	Risk Management
8	Cryptography

Part IV Incident Handling

No.	Course Content
1	Fundamentals of Incident Management
2	Incident Handling and Response Program Planning
3	Anti-Forensics Techniques
4	Malware Incident Handling and Response
5	Email Security Incident Handling and Response
6	Network Security Incident Handling and Response
7	Web Security Incident Handling and Response
8	Response Cloud Security Incident Handling and Response
9	Insider Threat-related Incident Handling and Response

Part V Digital Forensics

No.	Course Content
1	Fundamentals of Computer Forensics and Forensic Readiness
2	Computer Forensics Investigation Process - Obtain Search Warrant - Evaluate and Secure the Scene - Collect the Evidence - Secure the Evidence and Chain of Custody - Acquire Data and Analyze Data - Assess Evidence and Case - Testify as Expert Witness
3	Defeating Anti-Forensics Techniques
4	Operating System Forensics
5	Network Forensics
6	Web Attack Forensics
7	Database Forensics
8	Cloud Forensics
9	Wireless Forensics
10	Malware Forensics
11	Email-Crime Forensics
12	Mobile Forensics
13	Application Password Cracker
14	Investigative Reports

2. Intensive Curriculum (5 days)

Objective: To use as a guideline in providing both theoretical and practical trainings to individuals that will be appointed a Competent Official in a special circumstance in which an exemption to the appointment rules is granted so that the Competent Official can perform initial tasks in incident handling.

Course Content:

Part I **Ethical and professional conduct trainings to perform the role and execute duties as a Competent Official**

Part II **Basic knowledge in investigation for law enforcement**

No.	Course Content
1	Laws regarding maintaining cybersecurity
2	Laws regarding the commission of computer-related offenses
3	Laws regarding the protection of private data
4	The Penal Code and criminal procedure regarding the commission of computer-related offenses
5	Offense pattern and case studies
6	Guidelines in case proceeding and preparation such as complaint and allegation (filing a police report), coordination with relevant agencies, evidence compilation and fact inquiry, scene inspection, submitting motion to the competent court, evidence seizure and release, evidence preservation to maintain credibility in the prosecution and fine imposition processes.
7	Effective case management

Part III **Incident Handling and Digital Forensics**

No.	Course Content
1	Fundamentals of Incident Management
2	Incident Handling and Response Program Planning
3	Anti-forensics Techniques
4	Malware Incident Handling and Response
5	Email Security Incident Handling and Response
6	Network Security Incident Handling and Response
7	Web Security Incident Handling and Response
8	Cloud Security Incident Handling and Response
9	Insider Threat-related Incident Handling and Response
10	Fundamentals of Computer Forensics
11	Computer Forensics Investigation Process
12	Investigative Reports

7

ประกาศ กมช.

เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์ แต่ละระดับ พ.ศ. 2564

มีผลใช้บังคับตั้งแต่วันที่ 12 ธ.ค. 64 เป็นต้นไป

Notification of NCSC

Re: Characteristics and Measures for Prevention, Response, Assessment, Eradication, and Containment of Cyber Incidents at Each Level, B.E. 2564 (2021)

effective from December 12, 2021, onwards.



ฉบับภาษาไทย
Thai Version

ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔

โดยที่พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดให้คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ประกาศกำหนดรายละเอียดของลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ

อาศัยอำนาจตามความในมาตรา ๖๐ วรรคสอง แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ประกอบกับมติที่ประชุมคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ครั้งที่ ๒/๒๕๖๔ ลงวันที่ ๔ ตุลาคม ๒๕๖๔ คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ จึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ข้อ ๓ เพื่อประโยชน์ในการจำแนกลักษณะของภัยคุกคามทางไซเบอร์แต่ละระดับ ให้กำหนดรายละเอียดของลักษณะภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง ภัยคุกคามทางไซเบอร์ในระดับร้ายแรง และภัยคุกคามทางไซเบอร์ในระดับวิกฤต โดยพิจารณาและประเมินจากระดับผลกระทบที่อาจเกิดขึ้นหากระบบคอมพิวเตอร์ คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือโครงสร้างพื้นฐานสำคัญทางสารสนเทศหรือระบบงานที่มีความสำคัญอื่น ๆ ถูกโจมตีจากภัยคุกคามทางไซเบอร์ ตามลักษณะและการประเมินภัยคุกคามทางไซเบอร์แต่ละระดับที่กำหนดในเอกสารแนบ ๑ ท้ายประกาศนี้

ข้อ ๔ เพื่อให้การดำเนินการรับมือ ปราบปราม และระงับภัยคุกคามทางไซเบอร์เป็นไปอย่างเหมาะสมและสอดคล้องกับลักษณะของภัยคุกคามทางไซเบอร์แต่ละระดับ ให้กำหนดแนวทางที่เกี่ยวข้อง เพื่อเป็นข้อเสนอแนะสำหรับการจัดการกับภัยคุกคามทางไซเบอร์ ตามหลักเกณฑ์ เงื่อนไข และวิธีการที่กำหนดในเอกสารแนบ ๒ ท้ายประกาศนี้

ข้อ ๕ ให้ประธานกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ รักษาการตามประกาศนี้

ในกรณีที่มีปัญหาเกี่ยวกับการปฏิบัติตามประกาศนี้ หรือประกาศนี้ไม่ได้กำหนดเรื่องใดไว้ ให้ประธานกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เป็นผู้มีอำนาจตีความและวินิจฉัยชี้ขาด การตีความและคำวินิจฉัยของประธานกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ให้ถือเป็นที่สุด

ประกาศ ณ วันที่ ๒๕ พฤศจิกายน พ.ศ. ๒๕๖๔
พลเอก ประวิตร วงษ์สุวรรณ
รองนายกรัฐมนตรี ปฏิบัติหน้าที่
ประธานกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

เอกสารแนบ ๑ ท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม
และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔
ว่าด้วยลักษณะและการประเมินภัยคุกคามทางไซเบอร์แต่ละระดับ

บทนำ

ตามที่พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ได้กำหนดลักษณะของภัยคุกคามทางไซเบอร์ โดยแบ่งออกเป็น ๓ ระดับ ได้แก่ ภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง ภัยคุกคามทางไซเบอร์ในระดับร้ายแรง และภัยคุกคามทางไซเบอร์ในระดับวิกฤติ โดยได้มีการให้ความหมายของภัยคุกคามทางไซเบอร์ในแต่ละระดับไว้แล้วนั้น เพื่อให้เกิดความสะดวกแก่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศในการประเมินและระบุระดับของภัยคุกคามทางไซเบอร์ คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ จึงได้กำหนดลักษณะและการประเมินภัยคุกคามทางไซเบอร์แต่ละระดับโดยพิจารณาจากปัจจัยต่าง ๆ เพื่อเป็นแนวทางให้แก่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ สำหรับการพิจารณาระบุระดับของภัยคุกคามทางไซเบอร์ ดังมีรายละเอียดปรากฏตามแนบท้ายนี้

นิยาม

๑.	คณะกรรมการ	หมายถึง	คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
๒.	บริการหลัก	หมายถึง	ภารกิจหรือบริการอันถือเป็นหน้าที่โดยตรงของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศซึ่งมีการดำเนินภารกิจหรือให้บริการโดยใช้ระบบคอมพิวเตอร์ คอมพิวเตอร์ หรือข้อมูลคอมพิวเตอร์ ในการดำเนินการ
๓.	โครงสร้างสำคัญทางสารสนเทศ	หมายถึง	โครงสร้างสำคัญทางสารสนเทศที่เกี่ยวข้องกับการให้บริการของโครงสร้างพื้นฐานสำคัญของประเทศที่เกี่ยวข้องกับความมั่นคงปลอดภัยของรัฐ ความปลอดภัยสาธารณะ ความสงบเรียบร้อยของประชาชน ความสัมพันธ์ระหว่างประเทศ การป้องกันประเทศ เศรษฐกิจ การสาธารณสุข หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ
๔.	การประทุษร้ายต่อคอมพิวเตอร์หรือระบบคอมพิวเตอร์	หมายถึง	การกระทำโดยมิชอบที่มีผลต่อคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ โดยทำให้คอมพิวเตอร์หรือระบบคอมพิวเตอร์แล้วแต่กรณี เสียหาย ถูกทำลาย ด้อยประสิทธิภาพหรือไม่สามารถนำมาใช้งานได้ และให้หมายความรวมถึงการกระทำอื่นใดที่มีผลในทำนองเดียวกัน
๕.	ข้อมูล	หมายถึง	ข้อความ ข้อเท็จจริง หรือโปรแกรมที่มีการสร้าง จัดเก็บหรือมีการใช้งาน โดยสามารถรับย-ส่งด้วยซอฟต์แวร์คอมพิวเตอร์ รวมถึงซอฟต์แวร์ระบบ โปรแกรมประยุกต์ หรือสื่ออื่นใดที่ใช้คู่กับอุปกรณ์คอมพิวเตอร์ ระบบคอมพิวเตอร์ หรืออุปกรณ์ที่ถูกควบคุมด้วยอิเล็กทรอนิกส์ ไม่ว่าจะปรากฏในรูปแบบของตัวอักษร ตัวเลข เสียง ภาพ หรือรูปแบบอื่นใดที่สื่อความหมายได้โดยสภาพของสิ่งนั้นเองหรือโดยผ่านวิธีการใด ๆ

๖. การประทุษร้ายต่อข้อมูล	หมายถึง	การกระทำโดยมิชอบที่มีผลเป็นการเปลี่ยนแปลงข้อมูล ทำลายข้อมูล ขโมยข้อมูล นำข้อมูลไปใช้โดยไม่ได้รับอนุญาต หรือจำกัดมิให้ผู้เป็นเจ้าของหรือผู้ครอบครองข้อมูลเข้าถึงข้อมูลของตนได้ และให้หมายความรวมถึงการกระทำอื่นใดที่มีผลในทำนองเดียวกัน
๗. แผนการกู้คืน	หมายถึง	แผนปฏิบัติงานหรือรายละเอียดความตกลงที่เกี่ยวข้องกับการกู้คืนระบบหรือการกู้คืนการให้บริการ (service level agreement) หรือ แผนการบริหารความต่อเนื่องของหน่วยงาน แล้วแต่กรณี
๘. มาตรการเร่งด่วน	หมายถึง	มาตรการเร่งด่วนเพื่อรักษาไว้ซึ่งการปกครองระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุขตามรัฐธรรมนูญแห่งราชอาณาจักรไทย เอกราชและบูรณภาพแห่งอาณาเขต ผลประโยชน์ของชาติ การปฏิบัติตามกฎหมาย ความปลอดภัยของประชาชน การดำรงชีวิตโดยปกติสุขของประชาชน การคุ้มครองสิทธิเสรีภาพ ความสงบเรียบร้อยหรือประโยชน์ส่วนรวม หรือการป้องปัดหรือแก้ไขเยียวยาความเสียหายจากภัยพิบัติสาธารณะอันมีมาอย่างฉุกเฉินและร้ายแรง

ลักษณะของภัยคุกคามทางไซเบอร์ และปัจจัยที่ใช้ในการประเมินภัยคุกคามทางไซเบอร์แต่ละระดับ

ในการพิจารณาระบุระดับของภัยคุกคามทางไซเบอร์ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศควรพิจารณาจากเหตุการณ์ต่าง ๆ ที่เป็นพฤติการณ์แวดล้อม ผลกระทบที่เกิดขึ้น ความเสี่ยงหรือแนวโน้มที่อาจเกิดขึ้นจากภัยคุกคามทางไซเบอร์ในกรณีต่าง ๆ เพื่อพิจารณาว่าลักษณะของภัยคุกคามทางไซเบอร์นั้นอยู่ในระดับใด โดยให้พิจารณาจากปัจจัยที่ใช้ในการประเมินทั้ง ๔ ปัจจัย ดังนี้

(๑) ลักษณะผลกระทบที่เกิดขึ้นต่ออุปกรณ์หรือระบบงาน

(๒) ลักษณะผลกระทบต่อข้อมูลในระบบ

(๓) แนวโน้มในการกู้คืนระบบ

(๔) ลักษณะผลกระทบต่อลูกค้าหรือผู้ใช้บริการ

การพิจารณาเพื่อระบุระดับของภัยคุกคามทางไซเบอร์แต่ละระดับนั้น หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศควรพิจารณาให้ครบทั้ง ๔ ปัจจัย ตามที่ได้ระบุไว้ข้างต้น โดยหากปรากฏข้อเท็จจริงว่าลักษณะภัยคุกคามทางไซเบอร์ที่เกิดขึ้นนั้นเข้าลักษณะหรือมีแนวโน้มเป็นภัยคุกคามทางไซเบอร์ในระดับใด ให้ถือเอาระดับสูงสุดที่ประเมินได้เป็นเกณฑ์ในการระบุระดับของภัยคุกคามทางไซเบอร์ในครั้งนั้น ๆ นอกจากนี้ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศอาจพิจารณากำหนดปัจจัยที่ใช้ในการประเมินและลักษณะภัยคุกคามทางไซเบอร์เพิ่มเติมร่วมกับหน่วยงานควบคุมหรือกำกับดูแลเพื่อให้มีแนวทางในการจำแนกระดับของภัยคุกคามทางไซเบอร์ที่เหมาะสม โดยจะต้องมีรายละเอียดไม่น้อยกว่าหรือเทียบเท่ากับแนวทางการพิจารณาที่กำหนดไว้ในตารางที่ ๑

อย่างไรก็ดี เพื่อให้การดำเนินการรับมือ ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับมีความเหมาะสมและสอดคล้องกับสถานการณ์โดยรวมที่เกิดขึ้น คณะกรรมการอาจพิจารณาปรับเปลี่ยนหรือยกระดับของภัยคุกคามทางไซเบอร์ที่ได้รับรายงานเป็นอย่างอื่นได้ หากปรากฏข้อเท็จจริงเพิ่มเติมหรือพบว่าภัยคุกคามทางไซเบอร์ที่เกิดขึ้นนั้นมีแนวโน้มที่จะลุกลามหรือก่อให้เกิดความเสียหายมากขึ้น

อนึ่ง เพื่อให้สอดคล้องกับสภาวการณ์ที่เปลี่ยนแปลงไป คณะกรรมการหรือผู้ที่ได้รับมอบหมายจากคณะกรรมการอาจพิจารณาทบทวนลักษณะภัยคุกคามทางไซเบอร์ ปรับปรุงปัจจัยที่ใช้ในการประเมินหรือนำเงื่อนไขอื่น ๆ มาประกอบการพิจารณาเพิ่มเติมได้ตามที่เห็นสมควร

ตารางที่ ๑ ลักษณะภัยคุกคามทางไซเบอร์แต่ละระดับและแนวทางการพิจารณาผลกระทบ

ปัจจัยที่ใช้ในการประเมิน	ลักษณะภัยคุกคามทางไซเบอร์			
	ระดับไม่ร้ายแรง	ระดับร้ายแรง	ระดับวิกฤติ	
			กรณี (ก)	กรณี (ข)
๑. ลักษณะผลกระทบที่เกิดขึ้นต่ออุปกรณ์หรือระบบงาน	การประทุษร้ายต่อคอมพิวเตอร์หรือระบบคอมพิวเตอร์ ดังนี้ (๑) ระบบคอมพิวเตอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศ หรือ (๒) อุปกรณ์หรือระบบงานอื่นใดที่ใช้สำหรับการให้บริการของรัฐ ทั้งนี้ ผลกระทบที่เกิดกับอุปกรณ์หรือระบบงานดังกล่าว ทำให้ระบบคอมพิวเตอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศ หรือการให้บริการของรัฐด้อยประสิทธิภาพลงไปบ้าง แต่ไม่ถึงขนาดที่จะทำให้ระบบหรือบริการต้องหยุดชะงักหรือไม่สามารถใช้งานได้	การประทุษร้ายต่อคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่ถูกใช้สำหรับให้บริการหลัก ดังนี้ (๑) ระบบคอมพิวเตอร์ (๒) โครงสร้างสำคัญทางสารสนเทศ ทั้งนี้ ผลกระทบที่เกิดกับอุปกรณ์หรือระบบงานดังกล่าว แสดงให้เห็นได้ว่าผู้โจมตีมีความมุ่งหมายที่จะทำให้โครงสร้างพื้นฐานสำคัญของประเทศเสียหายจนไม่สามารถทำงานหรือให้บริการได้	การประทุษร้ายต่อคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่รุนแรงในลักษณะที่เป็นวงกว้างต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ ทั้งนี้ ผลกระทบที่เกิดกับอุปกรณ์หรือระบบงานดังกล่าว ทำให้ (๑) การทำงานของหน่วยงานรัฐหรือการให้บริการของโครงสร้างพื้นฐานสำคัญของประเทศที่ให้กับประชาชนล้มเหลวทั้งระบบจนรัฐไม่สามารถควบคุมการทำงานส่วนกลางของระบบคอมพิวเตอร์ของรัฐได้ หรือ (๒) การใช้มาตรการเยียวยาตามปกติในการแก้ไขปัญหาภัยคุกคามไม่สามารถแก้ไขปัญหาได้และมีความเสี่ยงที่จะลุกลามไปยังโครงสร้างพื้นฐานสำคัญอื่น ๆ ของประเทศ หรือระบบคอมพิวเตอร์ คอมพิวเตอร์ข้อมูลคอมพิวเตอร์จำนวนมากถูกทำลายเป็นวงกว้างในระดับประเทศ	ไม่เจาะจงอุปกรณ์หรือระบบงานที่ได้รับผลกระทบ แต่เมื่อพิจารณาจากพฤติกรรมของผู้โจมตีหรือพฤติการณ์แวดล้อมแล้วมีเหตุอันควรเชื่อได้ว่าการก่อภัยคุกคามทางไซเบอร์นั้นกระทบหรืออาจกระทบต่อความสงบเรียบร้อยของประชาชน หรือเป็นภัยต่อความมั่นคงของรัฐ หรืออาจทำให้ประเทศหรือส่วนใดส่วนหนึ่งของประเทศตกอยู่ในภาวะคับขัน หรือมีการกระทำความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา การรบหรือการสงคราม

ปัจจัยที่ใช้ในการประเมิน	ลักษณะภัยคุกคามทางไซเบอร์			
	ระดับไม่ร้ายแรง	ระดับร้ายแรง	ระดับวิกฤติ	
			กรณี (ก)	กรณี (ข)
๒. ลักษณะผลกระทบต่อข้อมูลในระบบ	มีเหตุอันควรเชื่อได้ว่าผู้โจมตีมีความมุ่งหมายให้เกิดการประทุษร้ายต่อข้อมูล ซึ่งส่งผลกระทบทำให้ระบบคอมพิวเตอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศ หรือการให้บริการของรัฐด้อยประสิทธิภาพลงไปบ้าง แต่ไม่ถึงขนาดที่จะทำให้ระบบหรือบริการต้องหยุดชะงักหรือไม่สามารถใช้งานได้	มีเหตุอันควรเชื่อได้ว่าผู้โจมตีมีความมุ่งหมายให้เกิดการประทุษร้ายต่อข้อมูลที่ใช้สำหรับระบบคอมพิวเตอร์หรือโครงสร้างสำคัญทางสารสนเทศ ซึ่งส่งผลให้บริการหลักไม่สามารถทำงานหรือให้บริการได้	มีเหตุอันควรเชื่อได้ว่าผู้โจมตีมีความมุ่งหมายให้เกิดการประทุษร้ายต่อข้อมูลอันมีลักษณะดังนี้ (๑) เป็นข้อมูลที่เกี่ยวข้องกับการทำงานของหน่วยงานรัฐหรือการให้บริการของโครงสร้างพื้นฐานสำคัญของประเทศที่ให้กับประชาชน หรือ (๒) เป็นข้อมูลที่เกี่ยวข้องกับชีวิตของบุคคลจำนวนมาก หรือเป็นข้อมูลคอมพิวเตอร์จำนวนมากในระดับประเทศ	มีเหตุอันควรเชื่อได้ว่าผู้โจมตีมีความมุ่งหมายให้เกิดการประทุษร้ายต่อข้อมูลใด ๆ อันกระทบหรืออาจกระทบต่อความสงบเรียบร้อยของประชาชน หรือเป็นภัยต่อความมั่นคงของรัฐ หรืออาจทำให้ประเทศหรือส่วนใดส่วนหนึ่งของประเทศตกอยู่ในภาวะคับขัน หรือมีการกระทำความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา การรบหรือการสงคราม
๓. แนวโน้มในการกู้คืนระบบ	สามารถกู้คืนระบบคอมพิวเตอร์ หรือทำให้บริการของรัฐกลับมาได้บางส่วน โดยสามารถดำเนินการได้ตามแผนการกู้คืน	ไม่สามารถกู้คืนระบบคอมพิวเตอร์หรือโครงสร้างสำคัญทางสารสนเทศที่ใช้สำหรับให้บริการหลักได้ ตามแผนการกู้คืน	ไม่สามารถกู้คืนการทำงานของโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศได้ตามแผนการกู้คืน ทำให้ (๑) รัฐไม่สามารถควบคุมการทำงานส่วนกลางของระบบคอมพิวเตอร์ของรัฐได้ หรือ (๒) มีความเสี่ยงที่จะลุกลามไปยังโครงสร้างพื้นฐานสำคัญอื่น ๆ ของประเทศ ซึ่งอาจมีผลทำให้บุคคลจำนวนมากเสียชีวิต หรือระบบคอมพิวเตอร์ คอมพิวเตอร์	ไม่สามารถกู้คืนอุปกรณ์หรือระบบงานที่ได้รับผลกระทบได้ และจำเป็นต้องมีมาตรการเร่งด่วนในการกู้คืนอุปกรณ์หรือระบบงานที่เกี่ยวข้อง

ปัจจัยที่ใช้ในการประเมิน	ลักษณะภัยคุกคามทางไซเบอร์			
	ระดับไม่ร้ายแรง	ระดับร้ายแรง	ระดับวิกฤติ	
			กรณี (ก)	กรณี (ข)
			ข้อมูลคอมพิวเตอร์จำนวนมากถูกทำลายเป็นวงกว้างในระดับประเทศ	
๔. ลักษณะผลกระทบต่อลูกค้าหรือผู้ใช้บริการ	ส่งผลหรืออาจส่งผลกระทบต่อผู้ใช้บริการในวงจำกัด	อาจส่งผลกระทบต่อผู้ใช้บริการทั้งหมด	ส่งผลกระทบต่อผู้ใช้บริการทั้งหมด หรืออาจมีผลทำให้บุคคลจำนวนมากเสียชีวิต	ส่งผลหรืออาจส่งผลกระทบต่อความสงบเรียบร้อยของประชาชน หรือเป็นภัยต่อความมั่นคงของรัฐ หรืออาจทำให้ประเทศหรือส่วนใดส่วนหนึ่งของประเทศตกอยู่ในภาวะคับขัน หรือมีการกระทำความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา การรบหรือการสงคราม

เอกสารแนบ ๒ ท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม
และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔
ว่าด้วยมาตรการป้องกัน รับมือ ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ

บทนำ

ตามที่พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ได้กำหนดลักษณะของภัยคุกคามทางไซเบอร์ โดยแบ่งออกเป็น ๓ ระดับ ได้แก่ ภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง ภัยคุกคามทางไซเบอร์ในระดับร้ายแรง และภัยคุกคามทางไซเบอร์ในระดับวิกฤติ นั้น

เพื่อให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หรือหน่วยงานที่ถือเป็นโครงสร้างพื้นฐานสำคัญของประเทศ มีแนวทางปฏิบัติที่ชัดเจนในการดำเนินมาตรการป้องกัน รับมือ ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ จึงกำหนดรายละเอียดที่เกี่ยวข้องเพื่อเป็นแนวทางดำเนินการไว้ในแนบท้ายนี้

นิยาม

๑. ทรัพย์สินสำคัญทางสารสนเทศ	หมายถึง	ระบบคอมพิวเตอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศ หรือโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หรือระบบงานที่มีความสำคัญอื่น ๆ ตามที่หน่วยงานพิจารณาแล้วเห็นว่ามีความจำเป็นต้องเฝ้าระวัง หรือดำเนินมาตรการป้องกัน รับมือ และแก้ไขภัยคุกคามทางไซเบอร์
๒. หน่วยงาน	หมายถึง	หน่วยงานหรือองค์กรที่มีการครอบครองหรือเป็นเจ้าของทรัพย์สินสำคัญทางสารสนเทศ ซึ่งอาจได้รับผลกระทบหากมีภัยคุกคามทางไซเบอร์เกิดขึ้น
๓. แนวปฏิบัติพื้นฐาน (Security Control Baselines)	หมายถึง	แนวปฏิบัติพื้นฐานที่กำหนดไว้สำหรับการดำเนินมาตรการป้องกัน รับมือ ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ

มาตรการป้องกัน รับมือ ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ

การดำเนินมาตรการที่เกี่ยวข้องเพื่อจัดการภัยคุกคามทางไซเบอร์ (incident handling) นั้น สามารถแบ่งขั้นตอนการดำเนินการออกได้เป็น ๔ ขั้นตอนหลัก เพื่อให้สอดคล้องกับมาตรฐานหรือแนวทางปฏิบัติสากลที่เกี่ยวข้องกับการจัดการภัยคุกคามทางไซเบอร์ โดยมีรายละเอียดดังนี้



ภาพแสดงขั้นตอนการดำเนินมาตรการที่เกี่ยวข้องเพื่อจัดการภัยคุกคามทางไซเบอร์
(Incident Handling Cycle)

ขั้นตอนที่ ๑: การเตรียมการและป้องกันการเกิดภัยคุกคามทางไซเบอร์

การดำเนินมาตรการเพื่อเตรียมการและป้องกันการเกิดภัยคุกคามทางไซเบอร์ (preparation) เป็นสิ่งที่จะต้องทำในระยะเริ่มต้น เพื่อเตรียมความพร้อมเมื่อต้องเผชิญเหตุ ได้แก่ การจัดเตรียมข้อมูลให้พร้อม การจัดตั้งและฝึกอบรมบุคลากรหรือทีมงาน การจัดหาเครื่องมือและทรัพยากรต่าง ๆ ที่จำเป็น การตั้งค่าระบบต่าง ๆ ให้ปลอดภัย การจัดทำนโยบาย แผนงาน และกระบวนการที่เกี่ยวข้อง รวมถึงการสร้างเครือข่ายความร่วมมือ โดยพิจารณาดำเนินมาตรการตามรายละเอียดที่ระบุในตารางที่ ๒.๑

ขั้นตอนที่ ๒: การตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์

แม้ว่าหน่วยงานจะจัดให้มีมาตรการต่าง ๆ เพื่อป้องกันหรือควบคุมมิให้เกิดภัยคุกคามทางไซเบอร์ขึ้นแล้วก็ตาม แต่หน่วยงานก็ยังคงต้องเตรียมความพร้อมอยู่เสมอเพื่อรับมือกับสถานการณ์ภัยคุกคามทางไซเบอร์ที่ไม่อาจหลีกเลี่ยงได้ การดำเนินมาตรการในการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (detection and analysis) จึงเป็นสิ่งจำเป็นที่จะช่วยให้หน่วยงานสามารถบรรเทาความเสี่ยงที่ยังคงเหลืออยู่และสามารถแจ้งเตือนได้อย่างทันท่วงทีเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น โดยพิจารณาดำเนินมาตรการตามรายละเอียดที่ระบุในตารางที่ ๒.๒

ขั้นตอนที่ ๓: การระงับภัยคุกคามทางไซเบอร์[๑] ปราบปรามภัยคุกคามทางไซเบอร์[๒] และการฟื้นฟูระบบงานที่ได้รับผลกระทบ[๓]

เมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้นหรือเมื่อหน่วยงานได้รับแจ้งเตือนการเกิดภัยคุกคามทางไซเบอร์ หน่วยงานควรกำหนดแนวทางการดำเนินมาตรการเพื่อระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ (containment, eradication, and recovery) โดยการดำเนินการดังกล่าว ควรกำหนดให้สอดคล้องกับความรุนแรงและระดับของภัยคุกคามทางไซเบอร์แต่ละระดับ จนกระทั่งสามารถกู้คืนทรัพย์สินสำคัญทางสารสนเทศให้กลับมาดำเนินงานหรือให้บริการได้ตามปกติ โดยพิจารณาดำเนินมาตรการตามรายละเอียดที่ระบุในตารางที่ ๒.๓ ซึ่งการดำเนินการในขั้นตอนนี้อาจจะต้องกระทำควบคู่ไปกับการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ที่อาจมีการลุกลามหรือทวีความรุนแรงมากขึ้นเพื่อให้การระงับและการปราบปรามภัยคุกคามทางไซเบอร์ ตลอดจนการฟื้นฟูระบบงานที่ได้รับผลกระทบจากการเกิดภัยคุกคามทางไซเบอร์ สอดคล้องกับสถานการณ์ที่เปลี่ยนแปลงไป

ขั้นตอนที่ ๔: การดำเนินการภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์

การดำเนินกิจกรรมที่เกี่ยวข้องภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ (post-incident activity) นั้น หน่วยงานควรกำหนดขั้นตอน วิธีปฏิบัติ หรือกำหนดนโยบายภายในที่เกี่ยวข้องเพื่อให้มีแนวทางที่ชัดเจน โดยพิจารณาดำเนินมาตรการตามรายละเอียดที่ระบุในตารางที่ ๒.๔ ซึ่งการปฏิบัติตามมาตรการดังกล่าว จะช่วยให้หน่วยงานสามารถเรียนรู้จากเหตุภัยคุกคามทางไซเบอร์ที่ผ่านมา และสามารถหาแนวทางเพื่อแก้ไขจุดบกพร่องและพัฒนาแนวทางรับมือกับภัยคุกคามทางไซเบอร์ต่อไปในอนาคต นอกจากนี้หน่วยงานต้องเก็บรักษาข้อมูลและพยานหลักฐานที่จำเป็น เพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์ หรือใช้ในกรณีที่ต้องการร้องทุกข์หรือดำเนินคดี เนื่องจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้นนั้น อาจเข้าลักษณะเป็นความผิดตามประมวลกฎหมายอาญา หรือพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐ และที่แก้ไขเพิ่มเติม (ถ้ามี) หรือกฎหมายอื่น ๆ ที่เกี่ยวข้อง (โดยการเก็บข้อมูลบางประเภทนั้นอาจจำเป็นต้องดำเนินการตั้งแต่เมื่อมีการตรวจพบว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้น เนื่องจากข้อมูลดังกล่าวอาจสูญหายไปในระหว่างที่ต้องระงับเหตุภัยคุกคามทางไซเบอร์นั้น หรืออาจถูกลบหรือทำลายโดยผู้โจมตี)

เมื่อมีการเก็บรวบรวมข้อมูลและหลักฐานที่จำเป็นตามวรรคหนึ่งแล้ว หน่วยงานควรนำข้อมูลและหลักฐานที่รวบรวมได้มาใช้ในการจัดทำบันทึกข้อมูลสถิติภัยคุกคามทางไซเบอร์ โดยอาจจัดทำเป็นรายสัปดาห์หรือรายเดือน เพื่อเสนอต่อผู้ที่มีหน้าที่ดูแลและรับผิดชอบภายในหน่วยงาน และกำหนดขั้นตอนที่หน่วยงานควรดำเนินการ เพื่อป้องกันไม่ให้เกิดภัยคุกคามทางไซเบอร์ในลักษณะดังกล่าวขึ้นอีกในอนาคต

[๑] การระงับภัยคุกคามทางไซเบอร์ คือ การดำเนินการเพื่อจำกัดความเสียหายจากภัยคุกคามทางไซเบอร์ที่กำลังเกิดขึ้น กักกันภัยคุกคามไม่ให้แพร่กระจาย และป้องกันไม่ให้มีความเสียหายเพิ่มมากขึ้น โดยผู้เผชิญเหตุภัยคุกคามทางไซเบอร์ต้องระมัดระวังไม่ให้หลักฐานทางนิติวิทยาศาสตร์ถูกทำลายในการดำเนินการดังกล่าว

[๒] การปราบปรามภัยคุกคามทางไซเบอร์ คือ การดำเนินการกำจัดภัยคุกคาม ผู้เผชิญเหตุภัยคุกคามทางไซเบอร์จะต้องลบโปรแกรมหรือสิ่งที่ไม่พึงประสงค์ (malicious object) ออกให้หมด และตรวจสอบระบบที่ได้รับผลกระทบทั้งระบบเพื่อให้มั่นใจถึงความปลอดภัยด้านไซเบอร์ โดยพยายามให้เกิดความเสียหายต่อข้อมูลน้อยที่สุด

[๓] การฟื้นฟูระบบงานที่ได้รับผลกระทบ คือ การดำเนินการเพื่อนำระบบให้กลับมาอยู่ในสถานะปกติที่มั่นใจว่าปราศจากการโจมตีที่เป็นภัยคุกคามทางไซเบอร์ โดยรวมถึงการเฝ้าระวังและตรวจสอบระบบที่ถูกกู้คืนในระยะแรกของการนำกลับมาใช้งาน เพื่อป้องกันการโจมตีซ้ำ

อนึ่ง ในการป้องกัน รับมือ ปราบปราม และระงับภัยคุกคามทางไซเบอร์ ตามรายละเอียดที่ระบุไว้ข้างต้นนั้น หน่วยงานควรจัดให้มีมาตรการที่สอดคล้องกับระดับของภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นกับหน่วยงานนั้น ๆ โดยให้ใช้แนวทางการประเมินความเสี่ยงของหน่วยงานเป็นเกณฑ์ในการพิจารณา ประกอบกับความสำคัญของภารกิจหรือบริการที่อยู่ภายใต้ความรับผิดชอบของหน่วยงาน ความสำคัญของทรัพย์สินสำคัญทางสารสนเทศ และอาจนำปัจจัยที่ใช้ในการประเมินระดับภัยคุกคามทางไซเบอร์ ตามตารางที่ ๑ ของเอกสารแนบ ๑ มาประกอบการพิจารณาด้วยก็ได้ นอกจากนี้ หน่วยงานอาจพิจารณากำหนดแนวทางการดำเนินมาตรการต่าง ๆ เพิ่มเติมหรือแตกต่างจากที่กำหนดไว้ เพื่อป้องกัน รับมือ ปราบปราม และระงับภัยคุกคามทางไซเบอร์ หรือจัดทำนโยบายที่เกี่ยวข้องร่วมกับหน่วยงานควบคุมหรือกำกับดูแลเพื่อให้มีแนวทางการดำเนินมาตรการที่เหมาะสม โดยจะต้องมีรายละเอียดไม่น้อยกว่าหรือเทียบเท่ากับมาตรการต่าง ๆ ที่กำหนดไว้ในแนบท้ายนี้

รายละเอียดที่เกี่ยวข้องเพื่อเป็นแนวทางในการดำเนินมาตรการเตรียมการและป้องกัน รับมือ ปราบปราม และระงับภัยคุกคามทางไซเบอร์

คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ได้กำหนดรายละเอียดที่เกี่ยวข้องเพื่อเป็นแนวทางในการดำเนินมาตรการเตรียมการและป้องกัน รับมือ ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับไว้ ดังนี้

๑. กรณีหน่วยงานมีการครอบครองทรัพย์สินสำคัญทางสารสนเทศที่อาจมีแนวโน้มนำไปสู่ภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง

ให้หน่วยงานพิจารณาดำเนินมาตรการเตรียมการและป้องกัน รับมือ ปราบปราม และระงับภัยคุกคามทางไซเบอร์ ตามแนวทางที่ระบุในประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานซึ่งได้จัดทำขึ้นตามมาตรา ๔๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และที่แก้ไขเพิ่มเติม (ถ้ามี) และดำเนินการตามแนวปฏิบัติพื้นฐาน (Security Control Baselines) ที่กำหนดไว้ในตารางที่ ๒.๑ – ตารางที่ ๒.๔ (สำหรับกรณีภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง)

๒ กรณีหน่วยงานมีการครอบครองทรัพย์สินสำคัญทางสารสนเทศที่อาจมีแนวโน้มนำไปสู่ภัยคุกคามทางไซเบอร์ในระดับร้ายแรง

ให้หน่วยงานพิจารณาดำเนินมาตรการเตรียมการและป้องกัน รับมือ ปราบปราม และระงับภัยคุกคามทางไซเบอร์ ตามแนวทางที่ระบุในข้อ ๑ และดำเนินการตามแนวปฏิบัติพื้นฐาน (Security Control Baselines) ที่กำหนดไว้เพิ่มเติมในตารางที่ ๒.๑ – ๒.๔ (สำหรับกรณีภัยคุกคามทางไซเบอร์ในระดับร้ายแรง)

๓ กรณีหน่วยงานมีการครอบครองทรัพย์สินสำคัญทางสารสนเทศที่อาจมีแนวโน้มนำไปสู่ภัยคุกคามทางไซเบอร์ในระดับวิกฤติ

ให้หน่วยงานพิจารณาดำเนินมาตรการเตรียมการและป้องกัน รับมือ ปราบปราม และระงับภัยคุกคามทางไซเบอร์ ตามแนวทางที่ระบุในข้อ ๒ และดำเนินการตามแนวปฏิบัติพื้นฐาน (Security Control Baselines) ที่กำหนดไว้เพิ่มเติมในตารางที่ ๒.๑ – ๒.๔ (สำหรับกรณีภัยคุกคามทางไซเบอร์ในระดับวิกฤติ)

ตารางที่ ๒.๑ การดำเนินมาตรการเพื่อเตรียมการและป้องกันการเกิดภัยคุกคามทางไซเบอร์ (preparation)

ระดับ	แนวปฏิบัติพื้นฐาน (Security Control Baselines)
กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับร้ายแรง กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับวิกฤติ	(๑) จัดเตรียมข้อมูลและอุปกรณ์การติดต่อสื่อสารที่จำเป็น เช่น ข้อมูลการติดต่อของบุคคลหรือองค์กรต่าง ๆ คู่มือการปฏิบัติงานเพื่อรับมือกับภัยคุกคามทางไซเบอร์ และกลไกอื่นใด ที่ช่วยสนับสนุนการรายงานเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น เป็นต้น (๒) จัดเตรียมอุปกรณ์หรือทรัพยากรสนับสนุนที่จำเป็นสำหรับการรับมือกับภัยคุกคามทางไซเบอร์ (๓) ดำเนินการให้มีการจัดหมวดหมู่ข้อมูลและระบบสารสนเทศให้สอดคล้องกับแนวทางของกฎหมาย กฎเกณฑ์ หรือนโยบายต่าง ๆ ที่เกี่ยวข้อง เพื่อธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) ตลอดจนสภาพพร้อมใช้งาน (availability) ของข้อมูลและระบบสารสนเทศดังกล่าว (๔) จัดเตรียมข้อมูลสนับสนุนที่จำเป็นสำหรับการวิเคราะห์เหตุภัยคุกคามทางไซเบอร์ เช่น รายการทรัพย์สินสำคัญทางสารสนเทศ และแผนผังโครงสร้างเครือข่าย (Network diagrams) เป็นต้น (๕) พิจารณาซ่อนบริการหรือระบบที่ผู้โจมตีสามารถค้นพบในเครือข่ายได้ง่าย โดยไม่ต้องใช้ความพยายามเจาะระบบ เช่น การค้นหาผ่านกลไกการสืบค้น (discovery protocol) เป็นต้น (๖) ดำเนินการควบคุมการเปลี่ยนแปลงการตั้งค่าของอุปกรณ์ต่าง ๆ (configuration change control) และจัดทำแผนการบริหารจัดการการตั้งค่าหรือการเปลี่ยนแปลงค่าของอุปกรณ์ (configuration management plan) (๗) กำหนดตัวบุคคลหรือมอบหมายให้เจ้าหน้าที่ที่มีความชำนาญเป็นผู้ดำเนินการที่เกี่ยวข้องกับการเปลี่ยนแปลงการตั้งค่าของอุปกรณ์ต่าง ๆ รวมถึงการทำหน้าที่ในการประสานงานหรือหารือกับผู้ที่เกี่ยวข้อง (๘) จัดให้มีกระบวนการในการพิสูจน์ตัวตนผู้ใช้งานก่อนทำการเปลี่ยนแปลงการตั้งค่าของอุปกรณ์ใด ๆ เช่น การเข้ารหัสข้อมูลและการบริหารจัดการคีย์สำหรับการเข้าถึงระบบต่าง ๆ (cryptography / key managements) เป็นต้น (๙) ตรวจสอบแอปพลิเคชันที่ให้บริการโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้มีความปลอดภัยเพียงพอ โดยมีการคัดกรองนักพัฒนา (developer screening) ที่ได้รับมอบหมายให้ดำเนินการใด ๆ กับเครือข่าย แอปพลิเคชัน หรือระบบงานต่าง ๆ (๑๐) ดำเนินการให้มีการทดสอบความสามารถในการตอบสนองต่อภัยคุกคามทางไซเบอร์ (incident respond capability testing) (๑๑) รวบรวมข่าวกรองเกี่ยวกับภัยคุกคามทางไซเบอร์ (threat Intelligence) (๑๒) พิจารณาจัดให้มีกลไกที่สามารถทำงานได้โดยอัตโนมัติ เพื่อดำเนินการทดสอบการเจาะระบบเป็นประจำ และสามารถแจ้งเตือนได้อย่างทันท่วงทีเมื่อพบช่องโหว่หรือจุดอ่อนต่าง ๆ (ถ้าหน่วยงานมีความพร้อม) (๑๓) กำหนดแนวทางและระยะเวลาการเก็บรักษาหลักฐานเกี่ยวกับการก่อภัยคุกคามทางไซเบอร์

ระดับ	แนวปฏิบัติพื้นฐาน (Security Control Baselines)
	(๑๔) ดำเนินการควบคุมการเปลี่ยนแปลงการตั้งค่าของอุปกรณ์ต่าง ๆ (configuration change control) และจัดทำแผนการบริหารจัดการการตั้งค่าหรือการเปลี่ยนแปลงค่าของอุปกรณ์ (configuration management plan) โดยจะต้องจัดให้มีกลไกที่สามารถบันทึกประวัติการเปลี่ยนแปลงการตั้งค่าของอุปกรณ์ที่เป็นลายลักษณ์อักษร การแจ้งเตือนเมื่อมีการเปลี่ยนแปลงค่าของอุปกรณ์ที่ตั้งไว้ และให้พิจารณาจัดให้มีกลไกที่สามารถป้องกันการเปลี่ยนแปลงค่าของอุปกรณ์ต่าง ๆ โดยอัตโนมัติ (ถ้าหน่วยงานมีความพร้อม) (๑๕) จัดให้มีการฝึกอบรมเพื่อเตรียมพร้อมรับมือกับสถานการณ์ฉุกเฉินเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น (simulated events) เพื่อให้ผู้ปฏิบัติรับทราบบทบาทและความรับผิดชอบของตนเมื่อต้องรับมือกับสถานการณ์ดังกล่าว (๑๖) สร้างเครือข่ายความร่วมมือเพื่อแบ่งปันข้อมูลและประสานงานเกี่ยวกับการจัดการภัยคุกคามทางไซเบอร์

ตารางที่ ๒.๒ การดำเนินมาตรการในการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (detection and analysis)

ระดับ	แนวปฏิบัติพื้นฐาน (Security Control Baselines)
กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับร้ายแรง	(๑) จัดให้มีกลไกที่สามารถตรวจจับสิ่งบ่งชี้หรือลักษณะเบื้องต้นของการเกิดภัยคุกคามทางไซเบอร์ได้ในเวลาอันเหมาะสม โดยอาจอาศัยข้อมูลจากแหล่งข้อมูลต่าง ๆ เช่น ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เป็นต้น (๒) จัดให้มีกลไกที่สามารถรับการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์ (๓) จัดให้มีข้อพึงปฏิบัติพื้นฐานเกี่ยวกับการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (logs) ข้อความการแจ้งข้อผิดพลาด หรือข้อความเตือนภัยจากเครื่องมือรักษาความปลอดภัยด้านไซเบอร์ และการตรวจสอบระบบงานที่มีความสำคัญ (critical systems) โดยจะต้องจัดให้มีข้อพึงปฏิบัติที่สูงขึ้นสำหรับทุกระบบงานที่มีความสำคัญมากขึ้น (๔) วิเคราะห์ข้อมูลและประวัติการใช้งานต่าง ๆ เช่น ลักษณะการใช้งานเครือข่ายและระบบงาน (profile networks and systems) เป็นต้น เพื่อทำความเข้าใจพฤติกรรมการใช้งานในช่วงเวลาปกติ (normal behaviors) ทำการศึกษาวิจัยและค้นหาความสัมพันธ์ของข้อมูลในระบบกับสถานการณ์ต่าง ๆ (event correlation) (๕) ทันทีที่พบว่ามี หรืออาจมีภัยคุกคามทางไซเบอร์เกิดขึ้น ให้ดำเนินการสืบหาและรวบรวมข้อมูลทั้งหมด เช่น ลักษณะภัยคุกคามทางไซเบอร์, ช่องโหว่ที่อาจถูกใช้ในการโจมตี, สถานการณ์ของการโจมตี (อาทิ กำลังเกิดเหตุหรือสถานการณ์ได้สิ้นสุดแล้ว การโจมตีเป็นผลสำเร็จหรือไม่สำเร็จ ฯลฯ) จำนวนระบบหรือบริการที่ได้รับผลกระทบ, โฮสต์เนม ตำแหน่งหรือสถานที่ของระบบหรือบริการที่ได้รับผลกระทบ ข้อมูลผู้ใช้ เวลาประทับ ข้อมูล payload ข้อมูลแจ้งเตือนจาก IDS (ถ้ามี) และ ข้อมูลจราจรทางคอมพิวเตอร์ (log) เป็นต้น โดยหน่วยงานจะต้องเก็บรักษาข้อมูลดังกล่าว (safeguard incident data) ให้มีความปลอดภัย เพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์และใช้

ระดับ	แนวปฏิบัติพื้นฐาน (Security Control Baselines)
	เป็นพยานหลักฐานในการดำเนินคดี รวมถึงการจัดทำรายงานที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ (๖) ระบุหมวดหมู่ของภัยคุกคามทางไซเบอร์ตามสถานการณ์ที่เกิดขึ้น และติดตามเพื่อระบุหมวดหมู่ของภัยคุกคามทางไซเบอร์ที่เปลี่ยนแปลงไปจนกว่าสถานการณ์ดังกล่าวจะสิ้นสุด โดยอาจพิจารณาจากข้อมูลตามที่ระบุในข้อ ๒ ของภาคผนวกแนบท้ายนี้ (๗) จัดลำดับความสำคัญของการดำเนินการเพื่อรับมือกับภัยคุกคามทางไซเบอร์ให้ทันท่วงที โดยพิจารณาปัจจัยต่าง ๆ ที่เกี่ยวข้อง เช่น ผลกระทบต่อการทำงานของระบบ (functional impact) ผลกระทบต่อข้อมูล (information impact) และความสามารถในการกู้คืน (recoverability effort) เป็นต้น (๘) ศึกษาวิธีและลักษณะการโจมตี พร้อมทั้งระบุสาเหตุที่แท้จริงของภัยคุกคามทางไซเบอร์ รวมถึงจุดอ่อนของระบบที่ถูกโจมตี (๙) ดำเนินการแจ้งไปยังผู้ที่รับผิดชอบในการเผชิญเหตุหรือผู้ที่เกี่ยวข้องผ่านช่องทางที่มีความปลอดภัย โดยคำนึงถึงระดับชั้นความลับและความสำคัญของข้อมูล เพื่อให้บุคคลดังกล่าวสามารถปฏิบัติหน้าที่ในการรับมือกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้น (๑๐) รายงานภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับบริการของโครงสร้างพื้นฐานสำคัญทางสารสนเทศอย่างมีนัยสำคัญให้ผู้ที่เกี่ยวข้องทราบ ภายในระยะเวลาที่หน่วยงานควบคุมหรือกำกับดูแลกำหนด (โดยหน่วยงานควบคุมหรือกำกับดูแลอาจกำหนดให้นำข้อปฏิบัติตามแผนการกู้คืนของหน่วยงานมาประกอบการพิจารณาด้วยก็ได้) หรืออาจเทียบเคียงจากตัวอย่างตามที่ระบุในข้อ ๓ ของภาคผนวกแนบท้ายนี้ แล้วแต่กรณี
กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับวิกฤติ	ให้หน่วยงานดำเนินการตามข้อ ๑ ถึงข้อ ๒ และดำเนินมาตรการเพิ่มเติม ดังนี้ (๑) จัดให้มีกลไกที่สามารถแจ้งเตือนได้ทันที (real-time alerts) เมื่อพบว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้น (๒) จัดให้มีกลไกหรือระบบงานที่สามารถติดตามเหตุการณ์ และสามารถจัดเก็บและวิเคราะห์ข้อมูลต่าง ๆ เพื่อตรวจจับการเกิดภัยคุกคามทางไซเบอร์ได้โดยอัตโนมัติ (ถ้าหน่วยงานมีความพร้อม) (๓) จัดให้มีการแจ้งเตือนเกี่ยวกับความผิดปกติของการใช้ทรัพยากรของระบบงาน เช่น แจ้งเตือนเมื่อหน่วยความจำที่ใช้ในการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์เหลือน้อย (storage capacity warning) เมื่อมีการใช้หน่วยประมวลผลกลาง (CPU) หรือมีการใช้หน่วยความจำหลัก (RAM) ของอุปกรณ์เครือข่ายหรือระบบงานหลักที่สูงผิดปกติ หรือเมื่อมีการส่งข้อมูลออกนอกเครือข่ายมากผิดปกติ เป็นต้น (๔) วิเคราะห์ข้อมูลและค้นหาความสัมพันธ์ของข้อมูลกับเหตุการณ์ต่าง ๆ (information correlation) โดยอาจรับข้อมูลจากแหล่งข้อมูลอื่น ๆ นอกเหนือจากข้อมูลในระบบเพื่อเพิ่มความสามารถในการรับรู้และดำเนินการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ

ตารางที่ ๒.๓ การดำเนินมาตรการเพื่อระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ (containment, eradication, and recovery)

ระดับ	แนวปฏิบัติพื้นฐาน (Security Control Baselines)
กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง	(๑) ดำเนินการตามแนวทางหรือวิธีการในการจำกัดขอบเขตและระงับภัยคุกคามทางไซเบอร์ โดยที่แนวทางหรือวิธีการดังกล่าวจะต้องมีหลักเกณฑ์ที่ชัดเจนเพื่อใช้ประกอบการตัดสินใจในการดำเนินการ ทั้งนี้ แนวทางดังกล่าวรวมถึง (๑.๑) การดำเนินการเชิงเทคนิค เช่น การลบมัลแวร์ การปิดการใช้งานบัญชีของผู้ใช้งานที่ถูกละเมิด การปิดระบบหรือตัดการเชื่อมต่อของระบบจากเครือข่าย ภายหลังการเก็บหลักฐานหรือข้อมูลที่จำเป็นเพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์และใช้เป็นพยานหลักฐานในการดำเนินคดีแล้ว เป็นต้น (๑.๒) การดำเนินการเชิงบริหาร เช่น กำหนดแนวทางดำเนินการหรือการตัดสินใจของฝ่ายบริหารของหน่วยงาน การสื่อสารทั้งภายในและภายนอกหน่วยงาน เป็นต้น (๑.๓) การเตรียมการเพื่อดำเนินการทางกฎหมายกับผู้กระทำความผิด (๒) ดำเนินการตามแนวปฏิบัติที่เกี่ยวข้องเพื่อเก็บรวบรวมและจัดการหลักฐานต่าง ๆ ที่เกี่ยวข้องกับการก่อภัยคุกคามทางไซเบอร์โดยทันทีหลังจากที่ตรวจพบ เช่น การจัดการกับข้อมูลที่บันทึกอยู่ในหน่วยความจำประเภทที่สามารถสูญหายได้เมื่อปิดอุปกรณ์ (volatile data) การเก็บข้อมูลจราจรทางคอมพิวเตอร์ (logs) ข้อมูลเกี่ยวกับมัลแวร์ ข้อมูลสถานะของระบบ (system snapshot) หรือข้อมูลอื่น ๆ ที่จำเป็นให้เพียงพอสำหรับใช้วิเคราะห์ในเชิงเทคนิค และเพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์และใช้เป็นพยานหลักฐานในการดำเนินคดี (๓) ดำเนินการเพื่อให้มีการระบุแหล่งที่มาของการโจมตี (attacking host) เช่น การระบุหมายเลขประจำเครื่อง (IP address) การระบุช่องทางที่ผู้โจมตีใช้ การค้นหาและวิจัยที่มาของการโจมตีจากแหล่งข้อมูลต่าง ๆ เช่น ฐานข้อมูลภัยคุกคามทางไซเบอร์ที่รวบรวมข้อมูลจากหลายแหล่ง เป็นต้น (๔) ประสานงานเพื่อแจ้งหรือรายงานสถานการณ์การรับมือภัยคุกคามทางไซเบอร์และความคืบหน้าในการตอบสนองไปยังบุคคลหรือหน่วยงานที่เกี่ยวข้อง ตลอดจนผู้ที่อาจได้รับผลกระทบ อย่างทันท่วงที โดยอาจขอความช่วยเหลือไปยังบุคคลหรือหน่วยงานต่าง ๆ โดยเฉพาะการเกิดภัยคุกคามทางไซเบอร์ที่จัดอยู่ในหมวดหมู่ที่ ๑, ๒, ๔, ๕ และ ๗ ตามที่ระบุในข้อ ๑ ของภาคผนวกแนบท้ายนี้ ทั้งนี้ ในการแจ้งหรือรายงานสถานการณ์นั้น หน่วยงานควรเลือกใช้ช่องทางที่มีความเหมาะสมและปลอดภัย และดำเนินการแจ้งหรือรายงานเหตุภายในระยะเวลาที่หน่วยงานควบคุมหรือกำกับดูแลกำหนด หรืออาจเทียบเคียงจากตัวอย่างตามที่ระบุในข้อ ๓ ของภาคผนวกแนบท้ายนี้ แล้วแต่กรณี (๕) ดำเนินการจัดการกับช่องโหว่ทั้งหมดที่ได้รับผลกระทบจากภัยคุกคามทางไซเบอร์ และดำเนินการตามวิธีการป้องกันระบบจากความเสียหายที่อาจเกิดขึ้นเพิ่มเติม เช่น การปรับเปลี่ยนการควบคุมการเข้าถึงเครือข่าย (อาทิ ไฟร์วอลล์) การติดตั้งลายเซ็นของ Anti-Virus หรือ IDS / IPS ใหม่ หรือการเปลี่ยนแปลงทางกายภาพในโครงสร้างพื้นฐาน

ระดับ	แนวปฏิบัติพื้นฐาน (Security Control Baselines)
	และดำเนินการระงับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นโดยทันทีหลังจากที่ตรวจพบ เป็นต้น (๖) ดำเนินการที่เกี่ยวข้องเพื่อให้มั่นใจว่าระบบงานต่าง ๆ ยังคงสามารถใช้งานได้ตามปกติภายในกรอบระยะเวลาที่กำหนด (restore within time period) เช่น การกู้คืนระบบให้กลับมาดำเนินการได้ตามปกติ (integrity restoration) การสร้างระบบงานขึ้นใหม่ (rebuild) การแทนที่ไฟล์ที่ได้รับผลกระทบ (replace) การติดตั้งโปรแกรมคอมพิวเตอร์ (install) การเปลี่ยนแปลงรหัสผ่าน และการรักษาความปลอดภัยทางเครือข่าย (securing network) เป็นต้น (๗) สร้างมาตรการป้องกันทั้งเชิงรุกและเชิงรับเพื่อป้องกันไม่ให้เกิดภัยคุกคามทางไซเบอร์ที่มีลักษณะคล้ายคลึงกันเกิดขึ้นอีกในอนาคต เช่น การเพิ่มมาตรการเฝ้าระวังสัญญาณเตือนและเหตุการณ์ต่าง ๆ ที่มีความเกี่ยวข้องกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นแล้ว เป็นต้น
กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับร้ายแรง	ให้หน่วยงานดำเนินการตามข้อ ๑ และดำเนินมาตรการเพิ่มเติม ดังนี้ (๑) หากมีความจำเป็น ให้หน่วยงานดำเนินการใช้ระบบงานสำรองสำหรับการประมวลผล (alternate processing) การจัดเก็บข้อมูล (storage site) และกู้คืนข้อมูลที่เกี่ยวข้องกับการทำรายการหรือการดำเนินธุรกรรมต่าง ๆ (transaction recovery) (๒) ส่งคำแจ้งเตือนเพื่อขอรับการสนับสนุน ความช่วยเหลือ หรือประสานความร่วมมือไปยังหน่วยงานที่เกี่ยวข้อง (supply chain coordination) รวมถึงแจ้งไปยังศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (๓) ดำเนินการตามนโยบายการรายงานเกี่ยวกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นภายในหน่วยงานซึ่งครอบคลุมถึงรูปแบบ ระดับความลับ และเนื้อหาที่ต้องรายงาน ลำดับชั้นการรายงาน กำหนดเวลา เครื่องมือที่ใช้รายงาน (โดยอาจพิจารณาใช้เครื่องมือที่สามารถช่วยรายงานภัยคุกคามโดยอัตโนมัติ (ถ้าหน่วยงานมีความพร้อม)) (๔) ให้การช่วยเหลือ สนับสนุน หรือปฏิบัติงานร่วมกับสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ หน่วยงานควบคุมหรือกำกับดูแล พนักงานเจ้าหน้าที่ หรือบุคคลอื่นใดที่ปฏิบัติหน้าที่หรือได้รับมอบหมายให้ปฏิบัติหน้าที่ตามกฎหมาย (๕) พิจารณาจัดให้มีกลไกที่สามารถทำงานได้โดยอัตโนมัติ ในการรับมือหรือสนับสนุนการรับมือเมื่อเกิดภัยคุกคามทางไซเบอร์ (automated incident handling processes) (ถ้าหน่วยงานมีความพร้อม)
กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับวิกฤติ	ให้หน่วยงานดำเนินการตามข้อ ๑ ถึงข้อ ๒ และดำเนินมาตรการเพิ่มเติม ดังนี้ (๑) ดำเนินการตามแผนการทำงานในการกู้คืนระบบงานต่าง ๆ เพื่อให้ระบบสามารถให้บริการได้ภายในกรอบระยะเวลาที่กำหนด (restore within time period) โดยอาศัยความรู้จากทีมผู้เชี่ยวชาญด้านต่าง ๆ เพื่อให้การกู้คืนระบบและเครือข่ายของหน่วยงานทำได้อย่างรวดเร็ว

หมายเหตุ: ในกรณีที่มีภัยคุกคามทางไซเบอร์เกิดขึ้นแล้ว แต่หน่วยงานยังไม่สามารถระบุระดับของภัยคุกคามทางไซเบอร์โดยใช้ปัจจัยที่ใช้ในการประเมินตามที่ระบุในตามตารางที่ ๑ ของเอกสารแนบ ๑ ได้ ซึ่งอาจเกิดจากการที่หน่วยงานยังไม่สามารถรวบรวมรายละเอียดหรือ

ข้อมูลที่จำเป็นเพื่อใช้ในการวิเคราะห์ได้ในช่วงแรก หรือไม่ว่าด้วยเหตุอื่นใดก็ตาม ให้หน่วยงานดำเนินการประเมินผลกระทบเบื้องต้น โดยพิจารณาจากตัวอย่างตามที่ระบุในข้อ ๑ ของภาคผนวกแนบท้ายนี้ จนกว่าจะมีข้อมูลหรือปรากฏหลักฐานที่เพียงพอต่อการวิเคราะห์เพื่อระบุระดับของภัยคุกคามทางไซเบอร์

ตารางที่ ๒.๔ การดำเนินกิจกรรมที่เกี่ยวข้องภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ (post-incident activity)

ระดับ	แนวปฏิบัติพื้นฐาน (Security Control Baselines)
กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับร้ายแรง กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับวิกฤติ	ภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ ให้หน่วยงานพิจารณาดำเนินการดังนี้ (๑) นำเหตุการณ์ที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นและมีลักษณะเป็นภัยคุกคามทางไซเบอร์ที่มีนัยสำคัญมาเป็นกรณีศึกษา เช่น การพิจารณาถึงจุดอ่อนของโครงสร้างพื้นฐานของบริการ นโยบายและกระบวนการ การฝึกบุคลากร การระบุผู้มีอำนาจดำเนินงาน และเครื่องมือที่ใช้ เป็นต้น และหาแนวทางเพื่อเตรียมการรับมือและป้องกันการเกิดภัยคุกคามทางไซเบอร์ที่มีลักษณะดังกล่าวร่วมกับบุคคลหรือหน่วยงานที่เกี่ยวข้อง (๒) รวบรวมข้อมูลการดำเนินงานที่เกี่ยวข้องกับการรับมือภัยคุกคามทางไซเบอร์ (โดยอาจดำเนินการเป็นรายสัปดาห์หรือรายเดือน) เช่น จำนวนของภัยคุกคามทางไซเบอร์ที่เกิดขึ้น เวลาที่ใช้ในการจัดการกับภัยคุกคามทางไซเบอร์ประเภทต่าง ๆ และวัตถุประสงค์ของการโจมตี เป็นต้น เพื่อเสนอต่อผู้ที่มีหน้าที่ดูแลและรับผิดชอบภายในหน่วยงาน (๓) ปรับปรุงมาตรการเตรียมการและป้องกัน รับมือ ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับให้มีความเหมาะสม และเป็นปัจจุบัน (๔) เก็บรักษาข้อมูลและหลักฐานที่จำเป็น เพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์ หรือใช้ในกรณีที่ต้องการร้องทุกข์หรือดำเนินคดี ตามแนวทางและระยะเวลาการเก็บรักษาหลักฐานเกี่ยวกับการก่อภัยคุกคามทางไซเบอร์ที่หน่วยงานได้กำหนด

อนึ่ง แนวปฏิบัติพื้นฐาน (Security Control Baselines) ตามรายละเอียดที่กำหนดไว้ในตารางที่ ๒.๑ – ตารางที่ ๒.๔ นี้ เป็นเพียงแนวทางที่คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเห็นว่ามีความเหมาะสมที่จะช่วยให้หน่วยงานสามารถดำเนินมาตรการเตรียมการและป้องกัน รับมือ ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับได้อย่างมีประสิทธิภาพ และสามารถบรรลุวัตถุประสงค์ตามหลักการของพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และที่แก้ไขเพิ่มเติม (ถ้ามี) ได้ อย่างไรก็ดี หน่วยงานสามารถหารือร่วมกับหน่วยงานควบคุมหรือกำกับดูแลเพื่อให้มีแนวทางการดำเนินมาตรการที่เหมาะสมและสอดคล้องกับลักษณะการดำเนินภารกิจ การให้บริการหรือทรัพยากรที่มีอยู่ภายใต้ความรับผิดชอบของหน่วยงานได้

ภาคผนวก
ท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม
และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔

ข้อ ๑ การจำแนกหมวดหมู่ของภัยคุกคามทางไซเบอร์

หมวดหมู่	คำอธิบาย
๐	เหตุการณ์จำลอง และ การฝึกจู่โจม ของหน่วยงานเอง (Training and Exercises)
๑	การพยายามเข้าถึงระบบที่ไม่สำเร็จ (Unsuccessful Activity Attempt)
๒	การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance)
๓	การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยที่หน่วยงานกำหนด (Non-Compliance Activity)
๔	การบุกรุกโดยการใช้มัลแวร์ (Malicious Logic)
๕	การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion)
๖	การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion)
๗	การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)
๘	เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating)[๔]
๙	เหตุการณ์ผิดปกติที่ได้รับการวิเคราะห์แล้วว่าไม่ใช่เหตุการณ์ที่เป็นภัยคุกคาม (Explained Anomaly)

ข้อ ๒ ตัวอย่างลักษณะภัยคุกคามทางไซเบอร์แยกตามระดับต่าง ๆ

	หมวดหมู่ภัยคุกคาม						
ประเภทอุปกรณ์เครือข่าย	**๑**	**๒**	**๓**	**๔**	**๕**	**๖**	**๗**
Backbone	ไม่ร้ายแรง	ไม่ร้ายแรง	ไม่ร้ายแรง	ไม่ร้ายแรง	วิกฤต	วิกฤต	วิกฤต
เราเตอร์	ไม่ร้ายแรง	ไม่ร้ายแรง	ร้ายแรง	ไม่ร้ายแรง	วิกฤต	วิกฤต	วิกฤต
เครื่องแม่ข่ายสำหรับการจัดการเครือข่าย หรือ ดูแลความปลอดภัย	ไม่ร้ายแรง	ไม่ร้ายแรง	ร้ายแรง	ร้ายแรง	วิกฤต	วิกฤต	วิกฤต
เครื่องแม่ข่ายที่ไม่ได้ให้บริการกับสาธารณะ	ไม่ร้ายแรง	ไม่ร้ายแรง	ร้ายแรง	ร้ายแรง	ร้ายแรง	ร้ายแรง	ร้ายแรง
เครื่องแม่ข่ายที่เปิดให้บริการกับสาธารณะ	ไม่ร้ายแรง	ไม่ร้ายแรง	ไม่ร้ายแรง	ร้ายแรง	ไม่ร้ายแรง	ไม่ร้ายแรง	ร้ายแรง
เครื่องเวิร์กสเตชัน	ไม่ร้ายแรง	ไม่ร้ายแรง	ไม่ร้ายแรง	ร้ายแรง	ไม่ร้ายแรง	ไม่ร้ายแรง	ร้ายแรง

[๔] การแจ้งหรือรายงานภัยคุกคามตามหมวดนี้เกิดขึ้นเมื่อผู้เผชิญเหตุยังไม่ทราบรายละเอียดภัยคุกคาม และ กำลังดำเนินการวิเคราะห์เหตุการณ์ (เช่น อาจอยู่ในช่วงแรก ๆ ที่พบการกระทำผิด) โดยหากทราบผลของการสอบสวนแล้ว ผู้รายงานควรเปลี่ยนเป็นหมวดอื่นให้ถูกต้อง และ ในรายงานสรุปปิดเหตุการณ์ ไม่ควรมีภัยคุกคามที่อยู่ในหมวดนี้ เนื่องจากการวิเคราะห์สอบสวนเสร็จสิ้นแล้ว)

ข้อ ๓ ตัวอย่างกำหนดระยะเวลาในการแจ้งและรายงานภัยคุกคามทางไซเบอร์

หมวดหมู่ภัยคุกคามทางไซเบอร์	ระดับภัยคุกคามทางไซเบอร์	การแจ้งเบื้องต้นตามช่องทางที่กำหนด (ภายในเวลา)	การส่งรายงานให้หน่วยงานควบคุมหรือกำกับดูแล (ภายในเวลา)	การส่งรายงานให้สำนักงาน (ภายในเวลา)
๑	**ทุกเหตุการณ์**	**๓๐ นาที**	**๒ ชั่วโมง**	**๔ ชั่วโมง**
๒	ทุกเหตุการณ์	ตามหน่วยงานกำหนด	ตามหน่วยงานกำหนด	ตามหน่วยงานกำหนด
๓	ทุกเหตุการณ์	**๓๐ นาที**	**๒ ชั่วโมง**	**๘ ชั่วโมง**
๔	วิกฤต	**๑๐ นาที**	**๓๐ นาที**	**๑ ชั่วโมง**
	ร้ายแรง	**๒๐ นาที**	**๑ ชั่วโมง**	**๒ ชั่วโมง**
	ไม่ร้ายแรง	ตามหน่วยงานกำหนด	ตามหน่วยงานกำหนด	ตามหน่วยงานกำหนด
๕	วิกฤต	**๑๐ นาที**	**๓๐ นาที**	**๑ ชั่วโมง**
	ร้ายแรง	**๒๐ นาที**	**๑ ชั่วโมง**	**๒ ชั่วโมง**
	ไม่ร้ายแรง	**๓๐ นาที**	**๒ ชั่วโมง**	**๔ ชั่วโมง**
๖	วิกฤต	**๑๐ นาที**	**๓๐ นาที**	**๑ ชั่วโมง**
	ร้ายแรง	**๒๐ นาที**	**๑ ชั่วโมง**	**๒ ชั่วโมง**
	ไม่ร้ายแรง	**๓๐ นาที**	**๒ ชั่วโมง**	**๔ ชั่วโมง**
๗	วิกฤต	**๑๐ นาที**	**๓๐ นาที**	**๑ ชั่วโมง**
	ร้ายแรง	**๑๐ นาที**	**๑ ชั่วโมง**	**๑ ชั่วโมง**
	ไม่ร้ายแรง	ตามหน่วยงานกำหนด	ตามหน่วยงานกำหนด	ตามหน่วยงานกำหนด
๘	-	**๒๐ นาที**	ตามเวลาที่ต้องใช้ในการสืบสวน	**๔ ชั่วโมง**
๙	-	-	**๔ ชั่วโมง**	**๑๒ ชั่วโมง**



ฉบับภาษาอังกฤษ
English Version

Notification of the National Cyber Security Committee
Re: Characteristics and Measures for Prevention, Response, Assessment, Eradication, and Containment of Cyber Incidents at Each Level
B.E. 2564 (2021)

In accordance with the provisions stipulated in the Cybersecurity Act B.E. 2562, it is mandated that the National Cyber Security Committee issues the details of cyber incident characteristics and measures for prevention, response, assessment, eradication, and containment of cyber incidents at each level.

By virtue of Section 60 paragraph two of the Cybersecurity Act B.E. 2562 (2019), and the resolution of the National Cyber Security Committee Meeting no. 2/2564 on 4 October 2019, the National Cyber Security Committee has issued a notification, as follows:

Clause 1 This notification shall be called "Characteristics and Measures for Prevention, Response, Assessment, Eradication, and Containment of Cyber Incidents at Each Level B.E. 2564 (2021)".

Clause 2 This notification shall come into force on the date following its publication date in the Royal Thai Government Gazette.

Clause 3 For the purpose of cyber incident characterization at each level, it is mandated that the National Cyber Security Committee issues the details of the characteristics of incidents at the non-critical level, the critical level, and the crisis level. This is to enable Government Agencies and Organizations of Critical Information Infrastructure to determine and assess incidents based upon their level of potential impacts if computer systems, computers, computer data, critical information infrastructures, or other critical systems face attacks from cyber threats. Such determination and assessment should be conducted in accordance with characteristics and assessment of cyber incidents at each level, outlined in attached Enclosure 1 of this notification.

Clause 4 To ensure that the incident response, eradication, and containment are appropriate and consistent with the characteristics of each cyber incident level, it is mandated that the National Cyber Security Committee establishes related guidelines as recommendations for handling cyber incidents in accordance with the rules, conditions, and methods specified in the attached Enclosure 2 of this notification.

Clause 5 The Chairperson of the Cybersecurity Regulating Committee shall be vested with the authority to oversee and enforce the provisions outlined in this notification.

When issues arise concerning the compliance of this notification or when specific details are not expressly addressed herein, the Chairperson of the Cybersecurity Regulating Committee is empowered to interpret and make determinations. The interpretations and determinations made by the Chairperson of the Cybersecurity Regulating Committee shall be deemed final.

Given on the 25th of November B.E. 2564 (2021)

General Pravit Wongsuwan

(Pravit Wongsuwan)

Deputy Prime Minister as

Chairman of the National Cyber Security Committee

Enclosure 1 of the Notification of the National Cyber Security Committee
Re: Characteristics and Measures for Prevention, Response, Assessment, Eradication, and Containment of Cyber Incidents at Each Level
B.E. 2564 (2021)
Regarding Characteristics and Assessment of Cyber Incidents at Each Level

---

Introduction

The Cybersecurity Act B.E. 2562 (2019) has defined the characteristics of cyber incidents and classified them into three levels, i.e., non-critical, critical, and crisis. To facilitate Organizations of Critical Information Infrastructure in assessing and determining the incident level, the National Cyber Security Committee thus hereby establishes the characteristics and criteria of incidents at each level based on various factors. Cyber incidents at each level in the enclosed particulars are to serve as a guideline for Organizations of Critical Information Infrastructure to determine the level of cyber incidents.

1.	Committee	means	the National Cyber Security Committee.
2.	Core Service	means	a mission or a service directly under the purview of an Organization of Critical Information Infrastructure who utilizes computer systems, computers, or computer data in carrying out missions or providing services.
3.	Critical Information Infrastructure	means	information infrastructure that related to the country's critical infrastructure services concerning national security, public safety and order, international relations, national defense, economy, public health, or infrastructures that serve the public interest.
4.	Harm to Computers or Computer Systems	means	wrongful actions causing computers or computer systems, as the case may be, to be damaged, destroyed, degraded, or unusable, as well as any other actions imposing similar impacts.
5.	Data	mean	messages, facts, or programs that are created, stored, or utilized and can be transmitted or received by computer software. This encompasses system software, applications, or other media employed with computer devices, computer systems, or electronically controlled devices. The Data can be in the form of letters, numbers, sounds, visuals, or any formats capable of conveying meaning through inherent attributes or alternative methods.

6.	Harm to Data	means	wrongful actions causing alterations of data, destruction of data, data theft, unauthorized data usage, or limitation or blocking the data owner or data processor from accessing the data, as well as any other actions imposing similar impacts.
7.	Recovery Plan	means	an execution plan or detail of the agreement (service level agreement) related to system recovery or service recovery or, as the case maybe, business continuity plans.
8.	Urgent Measure	means	a measure to safeguard the Democratic regime of government with the King as Head of State under the Constitution of the Kingdom of Thailand as well as the country's independence, territorial integrity, national interests, lawfulness, public safety, peaceful daily lives of the public, rights and liberties, public peace and order or the public interest, or to avert, mitigate or remedy losses from urgent and catastrophic public disasters.

Cyber incident characteristics and factors used to assess the cyber incident level

To identify the level of a cyber incident, Organizations of Critical Information Infrastructure shall take surrounding circumstances, impacts, risks, or trends arising from diverse cyber incidents into consideration in order to determine the level of the cyber incident. The assessment relies on four factors, outlined as follows:

(1) Impacts on devices or operational systems;

(2) Impacts on system data;

(3) System recovery ability;

(4) Impacts on customers or users.

In determining the cyber incident level, Organizations of Critical Information Infrastructure shall duly consider the four factors. If it is established as a fact that the characteristics of the cyber incident in question align with or exhibit tendencies of being a cyber incident at a certain level, the highest level indicated by the assessment shall be deemed the level of that cyber incident. Furthermore, Organizations of Critical Information Infrastructure may, in collaboration with their regulator, formally designate supplementary factors as well as additional characteristic of cyber incidents to be considered in the assessment to establish guidelines for classifying incident levels. The details of the supplementary factors and characteristics must be equal to or greater than those stipulated in the guideline outlined in Table 1.

To ensure that operations in responding, eradicating, and containing cyber incidents at each level are aligned with overall situation, the Committee may adjust or escalate the reported

cyber incident level if additional facts emerge, or if the incident exhibits tendencies to spread and inflict additional or heightened damages.

To ensure an alignment with evolving situations, the Committee or its duly designated representatives retain the authority to amend cyber incident characteristics, update the factors used in the assessment, or employ other criteria for further considerations as deemed necessary.

Table 1 Cyber Incident Characteristics and Guideline for Impact Assessment

Assessment Factors	Cyber Incident Characteristics			
	Non-Critical	Critical	Crisis	
			Case (a)	Case (b)
1. Impacts on devices or systems	Harm to computers or computer systems, as detailed below: (1) computer systems of Organizations of Critical Information Infrastructure; or (2) devices or other systems employed in providing public services. Impacts on such devices or systems result in deterioration of the computer systems of Organizations of Critical Information Infrastructure, or a decline in the effectiveness of public services; however, such	Harm to computers or computer systems used for providing core services, as detailed below: (1) computer systems; (2) critical information infrastructures. Impacts on such devices or systems exhibit the attacker's aim to impair the national critical information infrastructures so that they are incapable of fulfilling their functions or delivering services.	Harm to computers or computer systems to a substantial degree, particularly those with widespread implications for the national critical information infrastructures. Impacts on such devices or systems lead to: (1) a complete failure of government agencies' operations or the national critical information infrastructure's services to the extent that the government	Regardless of specific devices or operational systems affected, with due consideration to the attacker's behaviors or surrounding circumstances, there exist reasonable grounds to infer that the perpetration of cyber incidents has, or may have, repercussions on public orders, pose threats to national security, may potentially precipitate crisis situations within the nation or specific regions thereof, or may give rise to offenses related to terrorism under the provisions of the Penal

Assessment Factors	Cyber Incident Characteristics			
	Non-Critical	Critical	Crisis	
			Case (a)	Case (b)
	impacts are not likely to reach a severity level that would disrupt the functionality of these systems or services or render them inoperable.		loses control over its central computer systems; or (2) an inability to mitigate incidents through customary application of incident mitigation measures, coupled with heightened risks of spreading to other national critical infrastructures, or causing nationwide-scale destruction of computer systems, computers and computer data.	Code and the laws akin to warfare or armed conflict.
2. Impacts on system data	There exist reasonable grounds to believe that the attacker intends to inflict Harm to Data, resulting in the degradation of computer systems belonging to	There exist reasonable grounds to believe that the attacker intends to inflict Harm to Data used in computer systems or critical information infrastructures,	There exist reasonable grounds to believe that the attacker intends to cause Harm to Data with the following characteristics:	There exist reasonable grounds to believe that attacker aims to cause Harm to Data that have, or may have, repercussions on public orders, pose threats to national

Assessment Factors	Cyber Incident Characteristics			
	Non-Critical	Critical	Crisis	
			Case (a)	Case (b)
	Organizations of Critical infrastructure or a decline in the effectiveness of public services; however, such impacts are not likely to reach a severity level that would disrupt the functionality of these systems or services or render them inoperable.	resulting in a disruption to their functions or services.	(1) data associated with operations of government agencies or public services of the national critical infrastructures; or (2) data related to people's lives in masses or data at an extensive national scale.	security, may potentially precipitate crisis situations within the nation or specific regions thereof, or may give rise to offenses related to terrorism under the provisions of the Penal Code and the laws akin to warfare or armed conflict.
3. System recovery ability	Computer systems can be recovered, or certain public services can be partially reinstated, in accordance with the Recovery Plan.	Computer systems or critical information infrastructures utilized in core services cannot be recovered in accordance with the Recovery Plan.	Operations of the national critical information infrastructures cannot be recovered in accordance with Recovery Plan, resulting in: (1) the government losing central control over its computer systems; or	Affected devices and systems cannot be recovered, necessitating the implementation of urgent measures to restore all related devices and systems.

Assessment Factors	Cyber Incident Characteristics			
	Non-Critical	Critical	Crisis	
			Case (a)	Case (b)
			(2) heightened risks of spreading to other national critical infrastructures, which may result in a significant loss of people's lives, or massive destruction of computers and computer data nationwide.	
4. Impacts on customers or users	Impacts can inflict a limited number of users.	Impacts have a potential to inflict the entirety of users.	Impacts inflict all users, or possibly result in numerous casualties.	Impacts affect or may affect public orders, pose threats to the national security, may potentially precipitate crisis situations within the nation or specific regions thereof, or may give rise to offenses related to terrorism under the provisions of the Penal Code and the laws akin to warfare or armed conflict.

Enclosure 2 of the Notification of the National Cyber Security Committee

Re: Characteristics and Measures for Prevention, Response, Assessment, Eradication, and Containment of Cyber Incidents at Each Level

B.E. 2564 (2021)

Regarding Measures for Prevention, Response, Assessment, Eradication, and Containment of Cyber Incidents at Each Level

---

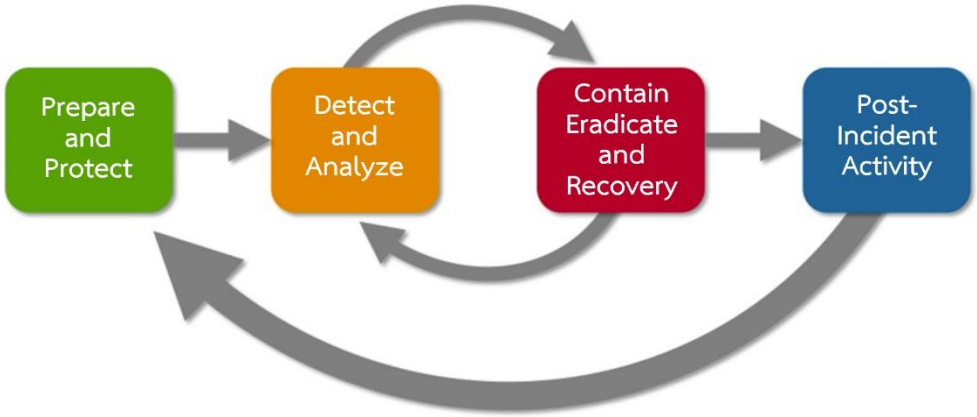
Introduction

The Cybersecurity Act B.E. 2562 (2019) has defined the characteristics of cyber incidents and classified them into three levels, i.e., non-critical, critical, and crisis. In order for Organizations of Critical Information Infrastructure, or agencies that serve as a national critical infrastructure, to have a clear guideline for implementing measures to prevent, respond to, eradicate, and contain cyber incidents at each level, the National Cyber Security Committee has therefore specified relevant details as an implementation guideline in this enclosure.

1. Critical IT Assets	mean	computer systems of Organizations of Critical Information Infrastructure, critical information infrastructures, or other essential operational systems that, after careful assessment, need to be monitored or require preventive, response, and mitigation measures against cyber incidents.
2. Agency	means	an agency or organization that possesses or owns Critical IT Assets that could be affected if a cyber incident occurs.
3. Security Control Baseline	means	a fundamental practice for implementing measures to prevent, respond, eradicate, and contain cyber incidents at each level.

Measures for Prevention, Response, Assessment, Eradication, and Containment of Cyber Incidents at Each Level

To ensure consistency with international standards or practices, cybersecurity incident handling involves 4 key steps, as follows:



Cybersecurity Incident Handling Cycle

Step 1: Preparation and Protection

Preparation and Protection against cyber incidents should be carried out in the initial phase to ensure readiness when facing incidents. The preparation and protection process involves preparing data, training personnel and workforce, acquiring necessary equipment and resources, configuring various systems securely, developing related policies, plans, and procedures, and building collaboration networks. The preparation and prevention phase should adhere to the details set forth in Table 2.1.

Step 2: Detection and Analysis

Although the Agencies may have measures in place to prevent cyber incidents from happening, they must still be ready to handle incidents that may inevitably occur. The detection and analysis procedures are crucial in helping the Agencies mitigate any residual risk and promptly issue a warning after an incident. The detection and analysis should adhere to the details set forth in Table 2.2.

Step 3: Containment[1], Eradication[2] and Recovery[3]

When a cyber incident occurs or when the Agencies receive a warning of a cyber incident, the Agencies should set up an action plan for containment, eradication, and recovery. Such a plan should align with the severity and the level of the cyber incident to enable Critical IT Assets to resume normal operations or services. Procedures to be taken in this step should adhere to the details set forth in Table 2.3 and should be implemented together with the detection and analysis step to prevent the incident from spreading further or becoming even more severe. This ensures the adaptability of the containment, eradication, and recovery steps to changing circumstances.

Step 4: Post-Incident Activity

In the Post-Incident Activity step, the Agencies should establish clear procedures, practices, or policies by following the measures detailed in Table 2.4. Adhering to these measures will enable the Agencies to learn from past incidents, determine their weakness, and discover a way to improve their incident handling procedure for future incidents. In addition, the Agencies should safeguard necessary data, witness, and evidence for digital forensics or legal proceedings because the incidents that occurred may violate the penal code or the Computer - Related Crime Act B.E. 2560 (2017) and its amendments (if any) or other related laws. (The collection of certain types of data may need to begin since the detection of the incidents because such data may be lost during containment or may be deleted or destroyed by the attacker.)

With the collection of data, witnesses, and evidence as specified in paragraph one, the Agencies should prepare a weekly or monthly statistical record of cyber incidents and present

[1] Containment is the process of limiting damage from ongoing incident, containing the incident to prevent it from spreading and causing further damages. It is critical for the incident responder to ensure that forensic evidences are not destroyed during the process.

[2] Eradication is the process of eliminating a cybersecurity threat. The incident responder must ensure that all malicious programs or objects are removed. At the same time, the incident responder needs to thoroughly inspect affected systems to ensure cybersecurity while minimizing data damage.

[3] Recovery is the process of returning the affected system to its normal and incident-free operational state, which includes monitoring and inspecting the recovered system during the initial phase of the resumed operation to prevent repeated attacks.

it to the personnel in charge. Moreover, the Agencies should establish a procedure to prevent a similar incident in the future.

In order to prevent, respond to, eradicate, and contain cyber incidents as detailed above, the Agencies should establish measures that align with the level of cyber incidents that may occur. The Agencies may use their risk assessment framework as a basis for the level determination, combined with the significance level of their missions and services, vitality of their Critical IT Assets, and the incident assessment factors in Table 1 of Enclosure 1 in establishing the measures. Furthermore, the Agencies may consider establishing additional measures that are supplementary to or deviated from recommendations in this Enclosure in the effort to prevent, respond, eradicate, and contain cyber incidents, or jointly develop related policies with their Regulator to ensure appropriate measure. However, the details of such supplementary measures must be no less comprehensive than or equal to those set forth in this Enclosure.

Details regarding the practice for implementing measures to prepare, prevent, respond, eradicate, and contain cyber incidents

The National Cyber Security Committee provides a set of details that can be used as practices for implementing measures to prepare, prevent, respond, eradicate, and contain cyber incidents at each level, as follows:

1. For the Agencies possessing Critical IT Assets that may lead to a non-critical incident

The Agencies in this category shall consider implementing measures to prepare, prevent, respond, eradicate and contain cyber incidents by following the directions set forth in the Code of Practice and Standard Framework developed in accordance with Section 44 of the Cybersecurity Act B.E. 2562 (2019) and its amendments (if any). The implementation shall also adhere to the Security Control Baseline set forth in Table 2.1 – 2.4 (for non-critical incidents).

2. For the Agencies possessing Critical IT Assets that may lead to a critical incident

The Agencies in this category shall consider implementing measures to prepare, prevent, respond, eradicate and contain cyber incidents by following the guideline specified in Clause 1 and the Security Control Baseline further furnished in Table 2.1 – 2.4 (for critical incidents).

3. For the Agencies possessing Critical IT Assets that may lead to a crisis incident

The Agencies in this category shall consider implementing measures to prepare, prevent, respond, eradicate and contain cyber incidents by following the guideline specified in Clause 2 and the Security Control Baseline further furnished in in Table 2.1 – 2.4 (for crisis incidents).

Table 2.1 Preparation and Protection Procedures for Cyber Incidents

Level	Security Control Baseline
In cases where services, systems, or devices are likely to be impacted by non-critical incidents In cases where services, systems, or devices are likely to be impacted by critical incidents In cases where services, systems, or devices are likely to be impacted by crisis incidents	(1) Prepare necessary data and communication equipment, e.g., contact information of persons or organizations, incident handling manual, and any mechanism used to facilitate incident reporting. (2) Prepare necessary equipment and resources to support incident handling. (3) Categorize data and IT systems according to the frameworks stipulated by laws, rules, or related policies to ensure confidentiality, integrity, and availability of the data and IT systems. (4) Prepare supportive data for incident analysis, e.g., a list of Critical IT Assets and network diagrams. (5) Consider hiding services or systems that the attacker can easily locate within the network without any intrusion effort, e.g., through a discovery protocol. (6) Implement controls for configuration change and develop a configuration management plan. (7) Designate appropriate individuals or personnel with relevant expertise to perform tasks concerning device configurations and collaboration or consultation with related parties. (8) Put in place an authentication process prior to any device configuration change, e.g., cryptography or access key managements. (9) Ensure that applications used in Critical Information Infrastructure services have sufficient security measures by screening developers assigned to work on networks, applications, or various systems.

Level	Security Control Baseline
	(10) Perform an incident respond capability testing. (11) Collect threat Intelligence. (12) Put in place an automatic mechanism to regularly conduct penetration tests on systems and issue prompt notifications when vulnerabilities are discovered (given that the Agencies can do so). (13) Establish guidelines and retention periods for evidence preservation. (14) Implement configuration change controls and develop a configuration management plan. The controls must include mechanisms that log any configuration changes in writing, alert when changes are made. The Agencies shall consider putting in place an automatic mechanism for automatically preventing configuration changes (given that the Agencies can do so). (15) Organize training sessions based on simulated events to prepare for emergency situations whenever an incident occurs. This is to ensure that all designated personnel understand their roles and responsibilities when handling such incidents. (16) Build collaboration networks to share information and coordinate cybersecurity incident handling efforts.

Table 2.2 Detection and Analysis Procedures for Cyber Incidents

Levels	Security Control Baselines
In cases where services, systems, or devices are likely to be impacted by a non-critical incident In cases where services, systems, or devices are likely to be impacted by critical incidents	(1) Put in place a mechanism that can detect indicators or early signs of incidents in a timely manner by employing information from various sources, e.g., Sectoral Computer Emergency Response Team (Sectoral CERT) for the Organizations of Critical Information Infrastructure. (2) Put in place a mechanism for receiving incident alerts. (3) Establish fundamental practices regarding computer logs, error messages or alert messages from cybersecurity tools as well as audits of critical systems. The numbers of the practices must be greater as the systems are more critical. (4) Analyze data and usage histories, e.g., the normal use of networks and systems (so called network and system profiles), to understand normal behaviors and to determine the correlation of events. (5) As soon as an incident is detected or may potentially occur, proceed to investigate and collect all data, e.g., incident characteristics, exploited vulnerabilities, circumstances of the attack (for example, the attack is ongoing or has ended, the attack is successful or unsuccessful), the number of affected systems or services, user data, timestamps, payload data, alerts from IDS (if any), and computer logs. The Agencies must safeguard the incident data to be used during digital forensics and as evidence in prosecution and in preparation of reports concerning the incidents. (6) Categorize the incident that has occurred and update its category following the change in circumstances until the incident has concluded. To do so, the Agencies may refer to the information in Clause 2 of the attached Appendix. (7) Prioritize the incident handling procedures to ensure a prompt response by considering related factors, e.g., functional impact, information impact, and recoverability effort.

Levels	Security Control Baselines
	(8) Analyze the methods and characteristics of the attack, identify the root cause of the incident, and identify the exploited system vulnerabilities. (9) Notify the individuals responsible for incident handling via a secure channel, selected based on the confidentiality and significance level of the data used in the notification, to ensure that such individuals can effectively handle the incident. (10) Report on the incident that significantly affected Critical Information Infrastructures to all related parties within the timeframe stipulated by the Regulator. (The Regulator may stipulate that the Agencies may consider incorporating the procedures in their Recovery Plan in deciding the report timeframe.) Alternatively, the Agencies may adapt the example timeframe in Clause 3 of the attached Appendix if applicable.
In cases where services, systems, or devices are likely to be impacted by crisis incidents	The Agencies shall follow the practices according to Clause 1 and Clause 2, and implement additional measures, as follows: (1) Put in place a mechanism issuing real-time alerts when incidents are detected. (2) Put in place a mechanism or an operational system that can track the situation and collect and analyze data automatically when the incident is detected (If the Agencies have the required resources). (3) Put in place a system that issues alerts when detecting anomalies in the utilization of operational systems' resource, such as alerts for low storage capacity for storing logs, for an unusually high CPU or RAM usage, or for abnormal outbound data transmission. (4) Analyze and determine correlation of information. This may involve data from other sources in addition to internal data sources to increase capacity to perceive, detect, and analyze cyber incidents.

Table 2.3 Containment, Eradication, and Recovery Procedures for Cyber Incidents

Level	Security Control Baseline
In cases where services, systems, or devices are likely to be impacted by non-critical incidents	(1) Follow guidelines or procedures in containing and eradicating cyber incidents. The guidelines or procedures must have clear criteria to be used in deciding a course of action. The guidelines or procedures may include: (1.1) Technical actions, e.g., removing malwares, closing violated user accounts, shutting down systems or disconnecting the system from the network after collecting the evidence and data necessary for forensic and legal processes. (1.2) Management actions, e.g., determining directions or making executive decisions, or communicating within and outside the Agencies. (1.3) Preparation to take a legal action against the perpetrator. (2) Follow relevant practices to gather and manage evidence related to incident as soon as it is detected, e.g., handling volatile data, computer logs, malware data, system snapshots or other data required to conduct a technical analysis during in forensic processes and to be used as witness evidence during prosecution. (3) Proceed to identify the attacking host, e.g., identifying the IP address, finding attack vectors, researching the origin of the attack from various data sources including cyber threat intelligence databases that collect data from numerous sources. (4) Coordinate with any related individual, agencies, or affected parties to promptly notify or report the situation of the incident handling. The Agencies may request assistance from individuals or other agencies when the incident falls in category 1, 2, 4, 5, and 7 as outlined in Clause 1 in the attached Appendix. When notifying or reporting any incident, the Agencies should use a secure and appropriate channel and make sure that the notification and report is done within the timeframe stipulated

Level	Security Control Baseline
	by the Regulator. Alternatively, they may adapt the example timeframe in Clause 3 of the attached Appendix if applicable. (5) Manage all vulnerabilities that are exploited during incident and implement a measure to prevent additional damages that may occur. For example, the Agencies may modify the network access controls (e.g., firewalls), install new Anti-Virus or IDS/IPS signatures, change the physical infrastructure, and contain the incident as soon as it is detected. (6) Ensure that systems are restored and resume normal operation within the predefined time. These actions may include restoring system integrity, rebuilding the system, replacing impacted files, installing computer system, changing password, and securing networks. (7) Develop both proactive and reactive measures to prevent similar incidents from occurring in the future, e.g., enhancing the measures for monitoring warnings and events that are related to the incidents that already occurred.
In cases where services, systems, or devices are likely to be impacted by critical incidents	The Agencies shall follow the practices according to Clause 1 and implement additional measures, as follows: (1) If necessary, the Agencies may use alternate processing systems and alternate storage sites and recover transaction data. (2) Issue notifications to request support, assistance, or supply chain coordination, and notify Thailand Computer Emergency Response Team (ThaiCERT). (3) Follow the Agencies' internal policies regarding incident reporting that covers format, confidentiality levels, required topics, reporting hierarchy, timeframe, and reporting tools. (The Agencies may consider using an automatic reporting tool (if they are capable)). (4) Provide assistance, support and coordination to the National Cyber Security Agency, the Regulators, Competent Officers, and any other individuals with legally mandated responsibilities.

Level	Security Control Baseline
	(5) Consider putting in place an automated incident handling process (if capable).
In cases where services, systems, or devices are likely to be impacted by crisis incidents	The Agencies shall follow the standard practices according to Clause 1 and Clause 2 and implement additional measures, as follows: (1) Follow the system Recovery Plan to make sure that the systems are restored and can provide services as normal within the time. The Agencies may consult experts from various fields to assist in promptly recovering its system and network.

Note: In the event that an incident has occurred but the Agencies are unable to determine the incident severity level by using the assessment factors in Table 1 of Enclosure 1 due to the incompleteness of data gathered in the beginning of the incident or any other reasons, the Agencies may assess the initial impact by consulting the examples in Clause 1 of the attached Appendix until there is sufficient data to determine the incident severity level.

Table 2.4 Post-Incident Activity Procedures

Level	Security Control Baseline
In cases where services, systems, or devices are likely to be impacted by non-critical incidents In cases where services, systems, or devices are likely to be impacted by critical incidents In cases where services, systems, or devices are likely to	After the incident is mitigated, the Agencies may consider performing the following activities: (1) Use the incident that occurred and was characterized as a critical incident as a case study. For example, study the vulnerabilities of the service's infrastructure, policies and processes, personnel training, identifying authorities to act on, and employed tools. Then, develop approaches to prepare, respond, and prevent similar incidents with related individuals or agencies. (2) Collect information of incident handling operations (either on a weekly or monthly basis), e.g., the number of incidents, the amount of time used to handle different types of incidents, and the purposes of the attack. This information can then be forwarded to the responsible individuals within the Agencies.

Level	Security Control Baseline
be impacted by crisis incidents	(3) Modify measures to prevent, respond, eradicate, and contain cyber incidents at each level so that they are applicable and up to date. (4) Preserve necessary data and evidence for forensic and legal processes by following the guideline and timeframe for preservation of incident-related evidence as stipulated by the Agencies.

These Security Control Baselines detailed in Table 2.1 – 2.4 above shall serve as a guideline that the National Cyber Security Committee deems appropriate in assisting the Agencies to effectively prepare, prevent, respond, eradicate and contain cyber incidents at each level. They are designed to meet the objectives and the principles of the Cybersecurity Act, B.E. 2562 (2019) and its amendments (if any). However, the Agencies may consult the Regulator to develop appropriate measures that suit their missions, services, or resources under their responsibility.

Appendix

Attachment of the Notification of the National Cyber Security Committee

Re: Characteristics and Measures for Prevention, Response, Assessment, Eradication, and Containment of Cyber Incidents at Each Level B.E. 2564 (2021)

1. Incident Categorization

Category	Description
0	Training and Exercises
1	Unsuccessful Activity Attempt
2	Reconnaissance
3	Non-Compliance Activity
4	Malicious Logic
5	User Level Intrusion
6	Root Level Intrusion
7	Denial of Service
8	Investigating[4]
9	Explained Anomaly

[4]The incident notifications or reports under this category occur when the incident responder is not yet aware of details and is in the analysis process (such as in the early stage of discovering wrongdoings). When the investigation yields a result, the responder should update the incident category accordingly. In the incident closure report, there should be no incident placed in this category as the analysis and investigation should already be concluded.

2. Examples of Incidents at Different Levels

	Incident Category						
Type of Network Devices	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Backbone	Non-Critical	Non-Critical	Non-Critical	Non-Critical	Crisis	Crisis	Crisis
Router	Non-Critical	Non-Critical	Critical	Non-Critical	Crisis	Crisis	Crisis
Network Management Server/ Cybersecurity Server	Non-Critical	Non-Critical	Critical	Critical	Crisis	Crisis	Crisis
Non-Public Server	Non-Critical	Non-Critical	Critical	Critical	Critical	Critical	Critical
Public Server	Non-Critical	Non-Critical	Non-Critical	Critical	Non-Critical	Non-Critical	Critical
Workstation	Non-Critical	Non-Critical	Non-Critical	Critical	Non-Critical	Non-Critical	Critical

3. Examples of Timeframes for Incident Notification and Report

Incident Category	Incident Level	Initial Notification via Established Channel (within the timeframe)	Report Submission to the Regulator (within the timeframe)	Report Submission to the National Cyber Security Agency (within the timeframe)
1	All incidents	30 minutes	2 hours	4 hours
2	All incidents	As set by the Agency	As set by the Agency	As set by the Agency
3	All incidents	30 minutes	2 hours	8 hours
4	Crisis	10 minutes	30 minutes	1 hour
	Critical	20 minutes	1 hour	2 hours
	Non-Critical	As set by the Agency	As set by the Agency	As set by the Agency
5	Crisis	10 minutes	30 minutes	1 hour
	Critical	20 minutes	1 hour	2 hours
	Non-Critical	30 minutes	2 hours	4 hours
6	Crisis	10 minutes	30 minutes	1 hour
	Critical	20 minutes	1 hour	2 hours
	Non-Critical	30 minutes	2 hours	4 hours
7	Crisis	10 minutes	30 minutes	1 hour
	Critical	10 minutes	1 hour	1 hour
	Non-Critical	As set by the Agency	As set by the Agency	As set by the Agency
8	-	20 minutes	As required for investigation	4 hours

Incident Category	Incident Level	Initial Notification via Established Channel (within the timeframe)	Report Submission to the Regulator (within the timeframe)	Report Submission to the National Cyber Security Agency (within the timeframe)
9	-	-	4 hours	12 hours

8

ระเบียบ กกม.

ว่าด้วยการมอบอำนาจให้ปฏิบัติการแทนคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2565

มีผลใช้บังคับตั้งแต่วันที่ 27 ธ.ค. 65 เป็นต้นไป

Regulation of CRC

on the Assignment of Powers to Perform Tasks on behalf of the Cybersecurity Regulating Committee B.E. 2565 (2022)

effective from December 27, 2022, onwards.



ฉบับภาษาไทย
Thai Version

ระเบียบคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์

ว่าด้วยการมอบอำนาจให้ปฏิบัติการแทนคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์

พ.ศ. ๒๕๖๕

โดยที่เป็นการสมควรกำหนดให้มีระเบียบและหลักเกณฑ์เกี่ยวกับการมอบอำนาจให้ปฏิบัติการแทนคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ ในการดูแลและดำเนินการเพื่อรับมือกับภัยคุกคามทางไซเบอร์ระดับร้ายแรงได้ทันท่วงที

อาศัยอำนาจตามความในมาตรา ๑๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ประกอบมติที่ประชุมคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ ครั้งที่ ๒/๒๕๖๕ เมื่อวันที่ ๑ สิงหาคม ๒๕๖๕ คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์จึงออกระเบียบไว้ ดังต่อไปนี้

ข้อ ๑ ระเบียบนี้เรียกว่า “ระเบียบคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ว่าด้วยการมอบอำนาจให้ปฏิบัติการแทนคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๕”

ข้อ ๒ ระเบียบนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ข้อ ๓ ในระเบียบนี้

“มอบอำนาจ” หมายความว่า การที่คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์มีหน้าที่และอำนาจที่จะพึงปฏิบัติ หรือดำเนินการตามกฎหมาย กฎ ระเบียบ ประกาศ หรือคำสั่งใด หรือมติของคณะรัฐมนตรีในเรื่องใด ได้มอบอำนาจในการสั่ง การอนุญาต การอนุมัติ การปฏิบัติการแทน หรือการดำเนินการอื่นใดตามกฎหมาย กฎ ระเบียบ ประกาศ หรือคำสั่งใด หรือมติของคณะรัฐมนตรีในเรื่องนั้น ให้แก่คณะกรรมการรับมือกับภัยคุกคามทางไซเบอร์ในระดับร้ายแรงปฏิบัติการแทน

“ผู้มอบอำนาจ” หมายความว่า คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ที่มีอำนาจที่จะพึงปฏิบัติหรือดำเนินการตามกฎหมาย กฎ ระเบียบ ประกาศ หรือคำสั่งใด หรือมติของคณะรัฐมนตรี ในการสั่งการอนุญาต การอนุมัติ การปฏิบัติการแทน หรือการดำเนินการอื่นใด

“ผู้รับมอบอำนาจ” หมายความว่า คณะกรรมการรับมือกับภัยคุกคามทางไซเบอร์ในระดับร้ายแรง หรือเลขาธิการ ที่ได้รับมอบอำนาจจากคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ที่มีอำนาจหน้าที่ดังกล่าว

“หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ” หมายความว่า หน่วยงานของรัฐหรือหน่วยงานเอกชน ซึ่งมีภารกิจหรือให้บริการโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

“หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ” หมายความว่า หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ที่ประกาศกำหนดลักษณะหน่วยงานที่มีภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ตามมาตรา ๔๙ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

“ภัยคุกคามทางไซเบอร์ในระดับร้ายแรง” หมายความว่า ภัยคุกคามที่มีลักษณะการเพิ่มขึ้นอย่างมีนัยสำคัญของการโจมตีระบบคอมพิวเตอร์ คอมพิวเตอร์ หรือข้อมูลคอมพิวเตอร์ โดยมุ่งหมายเพื่อโจมตีโครงสร้างพื้นฐานสำคัญของประเทศและการโจมตีดังกล่าวมีผลทำให้ระบบคอมพิวเตอร์หรือโครงสร้างสำคัญทางสารสนเทศที่เกี่ยวข้องกับการให้บริการของโครงสร้างพื้นฐานสำคัญของประเทศ ความมั่นคงของรัฐ ความสัมพันธ์ระหว่างประเทศ การป้องกันประเทศ เศรษฐกิจ การสาธารณสุข ความปลอดภัยสาธารณะ หรือความสงบเรียบร้อยของประชาชนเสียหาย จนไม่สามารถทำงานหรือให้บริการได้

“กกม.” หมายความว่า คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์

“คณะกรรมการรับมือกับภัยคุกคามทางไซเบอร์ในระดับร้ายแรง” หมายความว่า คณะกรรมการรับมือกับภัยคุกคามทางไซเบอร์ในระดับร้ายแรง ตามที่คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์แต่งตั้งและมอบอำนาจให้ปฏิบัติการแทนตามระเบียบนี้

“พนักงานเจ้าหน้าที่” หมายความว่า ผู้ซึ่งรัฐมนตรีแต่งตั้งให้ปฏิบัติการตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

“เลขาธิการ” หมายความว่า เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

“สำนักงาน” หมายความว่า สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

“การประชุมผ่านสื่ออิเล็กทรอนิกส์” หมายความว่า การประชุมที่กฎหมายบัญญัติให้ต้องมีการประชุมที่ได้กระทำผ่านสื่ออิเล็กทรอนิกส์ โดยผู้ร่วมประชุมมิได้อยู่ในสถานที่เดียวกันและสามารถประชุมปรึกษาหารือ และแสดงความคิดเห็นระหว่างกันได้ผ่านสื่ออิเล็กทรอนิกส์

“ผู้ร่วมประชุม” หมายความว่า ประธานกรรมการ กรรมการ หรือเลขานุการ ผู้ช่วยเลขานุการ และให้หมายความรวมถึงผู้ซึ่งต้องชี้แจงแสดงความคิดเห็นต่อคณะกรรมการรับมือกับภัยคุกคามทางไซเบอร์ในระดับร้ายแรงนั้นด้วย

ข้อ ๔ เพื่อให้การดูแลและดำเนินการเพื่อรับมือกับภัยคุกคามทางไซเบอร์ในระดับร้ายแรงได้ทันท่วงที ให้คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์สามารถมอบอำนาจให้คณะกรรมการรับมือกับภัยคุกคามทางไซเบอร์ในระดับร้ายแรง หรือเลขาธิการได้ ตามมาตรา ๖๑

มาตรา ๖๒ มาตรา ๖๓ มาตรา ๖๔ มาตรา ๖๕ และมาตรา ๖๖ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ รวมทั้งปฏิบัติการตามระเบียบนี้

ข้อ ๕ ให้มี คณะกรรมการคณะหนึ่ง เรียกว่า “คณะกรรมการรับมือกับภัยคุกคามทางไซเบอร์ในระดับร้ายแรง” เรียกโดยย่อว่า “ครร.” ประกอบด้วย

(๑) รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เป็นประธานกรรมการ
(๒) ผู้บัญชาการทหารสูงสุด เป็นกรรมการ
(๓) ผู้บัญชาการตำรวจแห่งชาติ เป็นกรรมการ
(๔) ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เป็นกรรมการ
(๕) เลขาธิการสภาความมั่นคงแห่งชาติ เป็นกรรมการ
(๖) เลขาธิการ เป็นกรรมการและเลขานุการ

ให้เลขานุการแต่งตั้งพนักงานของสำนักงาน เป็นผู้ช่วยเลขานุการได้ไม่เกินสองคน

ข้อ ๖ เมื่อปรากฏแก่ ครร. หรือโดยการเสนอแนะของสำนักงาน ว่าเกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ในระดับร้ายแรงให้ ครร. มีหน้าที่และอำนาจ ดังต่อไปนี้

(๑) ร่วมกันปฏิบัติการเพื่อรับมือกับภัยคุกคามทางไซเบอร์ในระดับร้ายแรงกับหน่วยงานควบคุมหรือกำกับดูแลและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามมาตราการป้องกันรับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกันรับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔”

(๒) ดูแลและดำเนินการเพื่อรับมือกับภัยคุกคามทางไซเบอร์ในระดับร้ายแรง ตามมาตรา ๖๑ มาตรา ๖๒ มาตรา ๖๓ มาตรา ๖๔ มาตรา ๖๕ และมาตรา ๖๖ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ดังนี้

(๒.๑) กำหนดให้หน่วยงานควบคุมหรือกำกับดูแลและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่ถูกคุกคามเข้าร่วมดำเนินการ ประสานงาน และให้การสนับสนุนต่อคณะกรรมการเพื่อรับมือกับภัยคุกคามทางไซเบอร์ในระดับร้ายแรงได้อย่างทันท่วงที

(๒.๒) มอบหมายให้สำนักงานวิเคราะห์สถานการณ์ และประเมินผลกระทบจากภัยคุกคามทางไซเบอร์ รวมทั้งการเผชิญเหตุและนิติวิทยาศาสตร์ทางคอมพิวเตอร์ เพื่อพิจารณาสั่งการ เมื่อมีหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ในระดับร้ายแรง เพื่อประโยชน์ในการติดตามและตรวจสอบผลการดำเนินการดังกล่าว ให้สำนักงานรายงานผลการดำเนินการต่อ กกม. ทราบด้วย

(๒.๓) เมื่อปรากฏแก่ ครร. ว่าเกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ในระดับร้ายแรงให้ ครร. ออกคำสั่งให้สำนักงานดำเนินการตามมาตรา ๖๑ เพื่อประโยชน์ในการวิเคราะห์สถานการณ์และประเมินผลกระทบจากภัยคุกคามทางไซเบอร์ และให้เลขาธิการสั่งให้พนักงานเจ้าหน้าที่ดำเนินการตามมาตรา ๖๒

(๒.๔) ในกรณีที่มีความจำเป็นเพื่อการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ให้ ครร. มีคำสั่งให้หน่วยงานของรัฐให้ข้อมูล สนับสนุนบุคลากรในสังกัด หรือใช้เครื่องมือทางอิเล็กทรอนิกส์ที่อยู่ในความครอบครองที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์

ครร. ต้องดูแลมิให้มีการใช้ข้อมูลที่ได้มาตาม (๒.๔) วรรคหนึ่ง ในลักษณะที่อาจก่อให้เกิดความเสียหาย และเสนอให้ กกม. รับผิดชอบในค่าตอบแทนบุคลากร ค่าใช้จ่ายหรือความเสียหายที่เกิดขึ้นจากการใช้เครื่องมือทางอิเล็กทรอนิกส์ดังกล่าว

ให้นำความใน (๒.๔) วรรคหนึ่ง และวรรคสอง มาใช้บังคับในการร้องขอต่อเอกชนโดยความยินยอมของเอกชนนั้นด้วย

(๒.๕) ในกรณีที่เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ซึ่งอยู่ในระดับร้ายแรง ให้ ครร. ดำเนินการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์และดำเนินมาตรการที่จำเป็น

ในการดำเนินการตาม (๒.๕) วรรคหนึ่ง ให้ ครร. มีหนังสือถึงหน่วยงานของรัฐที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ให้กระทำการหรือระงับการดำเนินการใด ๆ เพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ได้อย่างเหมาะสมและมีประสิทธิภาพตามแนวทางที่ กกม. กำหนด รวมทั้งร่วมกันบูรณาการในการดำเนินการเพื่อควบคุม ระงับหรือบรรเทาผลที่เกิดจากภัยคุกคามทางไซเบอร์นั้นได้อย่างทันท่วงที

ให้เลขาธิการรายงานการดำเนินการตาม (๒.๕) วรรคหนึ่ง และวรรคสองนี้ต่อ กกม. อย่างต่อเนื่อง และเมื่อภัยคุกคามทางไซเบอร์ดังกล่าวสิ้นสุดลง ให้รายงานผลการดำเนินการต่อ กกม. โดยเร็ว

(๒.๖ ในการรับมือและบรรเทาความเสียหายจากภัยคุกคามทางไซเบอร์ในระดับร้ายแรง ให้ ครร. มีอำนาจออกคำสั่งเฉพาะเท่าที่จำเป็นเพื่อป้องกันภัยคุกคามทางไซเบอร์ให้บุคคลผู้เป็นเจ้าของกรรมสิทธิ์ ผู้ครอบครอง ผู้ใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรือผู้ดูแลระบบคอมพิวเตอร์ซึ่งมีเหตุอันเชื่อได้ว่าเป็นผู้เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ หรือได้รับผลกระทบจากภัยคุกคามทางไซเบอร์ดำเนินการ ดังต่อไปนี้

(๒.๖.๑) เฝ้าระวังคอมพิวเตอร์หรือระบบคอมพิวเตอร์ในช่วงระยะเวลาใดระยะเวลาหนึ่ง

(๒.๖.๒) ตรวจสอบคอมพิวเตอร์หรือระบบคอมพิวเตอร์เพื่อหาข้อบกพร่องที่กระทบต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ วิเคราะห์สถานการณ์ และประเมินผลกระทบจากภัยคุกคามทางไซเบอร์

(๒.๖.๓) ดำเนินมาตรการแก้ไขภัยคุกคามทางไซเบอร์เพื่อจัดการข้อบกพร่องหรือกำจัดชุดคำสั่งไม่พึงประสงค์ หรือระงับบรรเทาภัยคุกคามทางไซเบอร์ที่ดำเนินการอยู่

(๒.๖.๔) รักษาสถานะของข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ด้วยวิธีการใด ๆ เพื่อดำเนินการทางนิติวิทยาศาสตร์ทางคอมพิวเตอร์

(๒.๖.๕) เข้าถึงข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ที่เกี่ยวข้องเฉพาะเท่าที่จำเป็น เพื่อป้องกันภัยคุกคามทางไซเบอร์

ในกรณีมีเหตุจำเป็นที่ต้องเข้าถึงข้อมูลตาม (๒.๖.๕) ให้ ครร. มอบหมายให้เลขาธิการ ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งให้เจ้าของกรรมสิทธิ์ ผู้ครอบครองผู้ใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรือผู้ดูแลระบบคอมพิวเตอร์ตาม (๒.๖) วรรคหนึ่งดำเนินการตามคำร้อง ทั้งนี้ คำร้องที่ยื่นต่อศาลต้องระบุเหตุอันควรเชื่อได้ว่าบุคคลใดบุคคลหนึ่งกำลังกระทำหรือจะกระทำการอย่างใดอย่างหนึ่ง ที่ก่อให้เกิดภัยคุกคามทางไซเบอร์ในระดับร้ายแรง ในการพิจารณาคำร้องให้ยื่นเป็นคำร้องไต่สวนคำร้องฉุกเฉินและให้ศาลพิจารณาไต่สวนโดยเร็ว

(๒.๗) ในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ในระดับร้ายแรง ครร. มีอำนาจปฏิบัติการหรือสั่งให้พนักงานเจ้าหน้าที่ปฏิบัติการเฉพาะเท่าที่จำเป็นเพื่อป้องกันภัยคุกคามทางไซเบอร์ในเรื่อง ดังต่อไปนี้

(๒.๗.๑) เข้าตรวจสอบสถานที่ โดยมีหนังสือแจ้งถึงเหตุอันสมควรไปยังเจ้าของหรือผู้ครอบครองสถานที่เพื่อเข้าตรวจสอบสถานที่นั้น หากมีเหตุอันควรเชื่อได้ว่ามีคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ หรือได้รับผลกระทบจากภัยคุกคามทางไซเบอร์

(๒.๗.๒) เข้าถึงข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทำสำเนา หรือสกัดคัดกรองข้อมูลสารสนเทศหรือโปรแกรมคอมพิวเตอร์ซึ่งมีเหตุอันควรเชื่อได้ว่าเกี่ยวข้องหรือได้รับผลกระทบจากภัยคุกคามทางไซเบอร์

(๒.๗.๓) ทดสอบการทำงานของคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีเหตุอันควรเชื่อได้ว่าเกี่ยวข้องหรือได้รับผลกระทบจากภัยคุกคามทางไซเบอร์ หรือถูกใช้เพื่อค้นหาข้อมูลใด ๆ ที่อยู่ภายในหรือใช้ประโยชน์จากคอมพิวเตอร์หรือระบบคอมพิวเตอร์นั้น

(๒.๗.๔) ยึดหรืออายัดคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรืออุปกรณ์ใด ๆ เฉพาะเท่าที่จำเป็นซึ่งมีเหตุอันควรเชื่อได้ว่าเกี่ยวข้องกับภัยคุกคามทางไซเบอร์ เพื่อการตรวจสอบหรือวิเคราะห์ ทั้งนี้ ไม่เกินสามสิบวัน เมื่อครบกำหนดเวลาดังกล่าวให้ส่งคืนคอมพิวเตอร์หรืออุปกรณ์ใด ๆ แก่เจ้าของกรรมสิทธิ์ หรือผู้ครอบครองโดยทันทีหลังจากเสร็จสิ้นการตรวจสอบหรือวิเคราะห์

ในการดำเนินการตาม (๒.๗.๒) (๒.๗.๓) และ (๒.๗.๔) ให้ ครร. มอบหมายให้เลขาธิการยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งให้พนักงานเจ้าหน้าที่ดำเนินการตามคำร้อง ทั้งนี้ คำร้องต้องระบุเหตุอันควรเชื่อได้ว่าบุคคลใดบุคคลหนึ่งกำลังกระทำหรือจะกระทำการอย่างใดอย่างหนึ่งที่ก่อให้เกิดภัยคุกคามทางไซเบอร์ในระดับร้ายแรง ในการพิจารณาคำร้องให้ยื่นเป็นคำร้องไต่สวนคำร้องฉุกเฉินและให้ศาลพิจารณาไต่สวนโดยเร็ว

(๓) ปฏิบัติการอื่นใดตามที่ กกม. มอบหมาย

ข้อ ๗ ในการนัดประชุมของ ครร. ให้เลขานุการแจ้งให้คณะกรรมการทุกคนทราบล่วงหน้าอย่างน้อยสามวัน โดยจะแจ้งด้วยวาจาก่อนและทำเป็นหนังสือ หรือโดยวิธีการทางอิเล็กทรอนิกส์ก็ได้ เว้นแต่จะได้มีการแจ้งกำหนดการนัดประชุมในที่ประชุมครั้งก่อนหน้าแล้ว

ในกรณีที่มีเหตุจำเป็นเร่งด่วนและไม่อาจนัดประชุมล่วงหน้าตามกำหนดเวลาในวรรคหนึ่งได้ ให้เลขานุการแจ้งให้ ครร. เพื่อนัดประชุมเป็นการเร่งด่วนได้ โดยให้นำวิธีการตามวรรคหนึ่งมาใช้โดยอนุโลม ทั้งนี้ ให้บันทึกการแจ้งนัดประชุม ครร. แต่ละคนไว้เป็นหลักฐานด้วย

ให้เลขานุการจัดส่งระเบียบวาระการประชุมและเอกสารที่เกี่ยวข้องไปพร้อมกับหนังสือนัดประชุม หรือจะส่งโดยจดหมายอิเล็กทรอนิกส์ก็ได้ แต่ต้องมีมาตรการในการรักษาความปลอดภัยต่อเอกสารอิเล็กทรอนิกส์ดังกล่าวด้วย เว้นแต่กรณีที่มีเหตุจำเป็นอาจส่งหลังจากการแจ้งนัดประชุมหรือส่งในวันที่มีการประชุมก็ได้

ข้อ ๘ การกำหนดระเบียบวาระการประชุมของ ครร. อย่างน้อยต้องมีรายละเอียด ดังต่อไปนี้

(๑) เรื่องที่ประธานแจ้งต่อที่ประชุม

(๒) เรื่องรับรองรายงานการประชุม

(๓) เรื่องเสนอเพื่อทราบ

(๔) เรื่องที่ค้างพิจารณาหรือเรื่องสืบเนื่อง

(๕) เรื่องเสนอเพื่อพิจารณา

ข้อ ๙ การประชุมของ ครร. ให้ถือปฏิบัติ ดังต่อไปนี้

(๑) ต้องมี ครร. มาประชุมไม่น้อยกว่ากึ่งหนึ่งของจำนวน ครร. ทั้งหมดที่มีอยู่จึงจะเป็นองค์ประชุม

(๒) ให้ประธาน ครร. เป็นประธานในที่ประชุม ถ้าประธาน ครร. ไม่อยู่ในที่ประชุมหรือไม่สามารถปฏิบัติหน้าที่ได้ ให้ที่ประชุมเลือก ครร. คนหนึ่ง เพื่อทำหน้าที่เป็นประธานในที่ประชุม

(๓) ครร. ผู้ใดมีส่วนได้เสียโดยตรงในเรื่องที่จะพิจารณา ครร. ผู้นั้นไม่มีสิทธิเข้าร่วมประชุมและไม่มีสิทธิออกเสียงลงคะแนนในเรื่องนั้น แต่ให้นับเป็นองค์ประชุมด้วย

(๔) การวินิจฉัยชี้ขาดของที่ประชุมให้ถือเสียงข้างมาก ครร. คนหนึ่งให้มีเสียงหนึ่งในการลงคะแนน ถ้าคะแนนเสียงเท่ากัน ให้ประธานในที่ประชุมออกเสียงเพิ่มขึ้นอีกหนึ่งเสียงเป็นเสียงชี้ขาด

(๕) เรื่องใดที่ ครร. รับรองมติการประชุมแล้ว ให้เลขานุการแจ้งมติของที่ประชุมให้ผู้เกี่ยวข้องทราบโดยมิต้องรอการรับรองรายงานการประชุม

ข้อ ๑๐ กรรมการที่แต่งตั้งโดยตำแหน่ง ถ้าผู้ดำรงตำแหน่งนั้นไม่อาจเข้าประชุมได้ ผู้เข้าประชุมแทนซึ่งเป็นผู้มีอำนาจทำหน้าที่แทนตามกฎหมายและให้นับเป็นองค์ประชุม

ข้อ ๑๑ การประชุมผ่านสื่ออิเล็กทรอนิกส์ของ ครร. ให้เป็นไปตามกฎหมายว่าด้วยการประชุมผ่านสื่ออิเล็กทรอนิกส์

ข้อ ๑๒ ให้ ครร. รีบรายงานการดำเนินการดังกล่าวตามข้อ ๖ ต่อประธาน กกม. โดยด่วนและอย่างต่อเนื่อง และเมื่อภัยคุกคามทางไซเบอร์สิ้นสุดลง ให้รายงานผลการดำเนินการต่อ กกม. เพื่อทราบด้วย

ข้อ ๑๓ กำหนดให้หน่วยงานควบคุมหรือกำกับดูแลและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่ถูกคุกคามเข้าร่วมดำเนินการ ประสานงาน และให้การสนับสนุนต่อคณะกรรมการรับมือเพื่อรับมือกับภัยคุกคามทางไซเบอร์ในระดับร้ายแรงได้อย่างทันท่วงที

ข้อ ๑๔ ให้สำนักงานหรือพนักงานเจ้าหน้าที่ ประสานงานกับผู้เกี่ยวข้อง ในการดำเนินการตามหน้าที่และอำนาจตามมาตรา ๖๑ มาตรา ๖๒ มาตรา ๖๓ มาตรา ๖๔ มาตรา ๖๕ และมาตรา ๖๖ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

ในการดำเนินการตามความวรรคหนึ่ง อาจทำเป็นหนังสือหรือวาจาหรือโดยการสื่อความหมายในรูปแบบอื่นก็ได้ แต่ต้องมีข้อความหรือความหมายที่ชัดเจนเพียงพอที่จะเข้าใจได้ ในกรณีที่สั่งการด้วยวาจา ถ้าผู้รับคำสั่งนั้นร้องขอและการร้องขอได้กระทำโดยมีเหตุอันสมควรภายในเจ็ดวันนับแต่วันที่มีคำสั่งดังกล่าว เลขาธิการต้องยืนยันคำสั่งนั้นเป็นหนังสือ

ทั้งนี้ ให้รีบรายงานต่อประธาน กกม. โดยด่วนและอย่างต่อเนื่อง และเมื่อภัยคุกคามทางไซเบอร์สิ้นสุดลง ให้รายงานผลการดำเนินการต่อ กกม. เพื่อทราบด้วย

ข้อ ๑๕ ในการปฏิบัติการแทนผู้รับมอบอำนาจอาจดำเนินการใด ๆ เพื่อให้บรรลุวัตถุประสงค์ของการมอบอำนาจนั้นตามที่เห็นสมควร แต่ต้องใช้อำนาจที่รับมอบให้เป็นไปตามกฎหมายที่เกี่ยวข้องกับเรื่องที่มีการมอบอำนาจหรือตามหลักเกณฑ์และเงื่อนไขการใช้อำนาจในเรื่องนั้น รวมทั้งต้องจัดทำรายงานผลการใช้อำนาจดังกล่าวตามหลักเกณฑ์ที่ผู้มอบอำนาจกำหนด

ข้อ ๑๖ ให้ประธานกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เป็นผู้รักษาการตามระเบียบนี้ และมีอำนาจออกประกาศ หรือคำสั่ง หลักเกณฑ์และวิธีการเพื่อประโยชน์ในการปฏิบัติตามระเบียบนี้

ในกรณีที่มีปัญหาเกี่ยวกับการบังคับใช้หรือการปฏิบัติตามระเบียบนี้ หรือระเบียบนี้ไม่ได้กำหนดเรื่องใดไว้ ให้ประธานกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ มีอำนาจตีความและวินิจฉัยชี้ขาด ทั้งนี้ การตีความและคำวินิจฉัยของประธานกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ ให้ถือเป็นที่สุด

ประกาศ ณ วันที่ ๑๓ กันยายน พ.ศ. ๒๕๖๕
ชัยวุฒิ ธนาคมานุสรณ์
รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
ประธานกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์



ฉบับภาษาอังกฤษ
English Version

Regulation of the Cybersecurity Regulating Committee
on the Assignment of Powers to Perform Tasks on behalf of the Cybersecurity Regulating Committee
B.E. 2565 (2022)

It is deemed appropriate to issue regulations and rules regarding the assignment of powers to perform tasks on behalf of the Cybersecurity Regulating Committee in supervising and undertaking actions to handle incident at a Critical Level in a timely manner.

By virtue of section 14 of the Cybersecurity Act B.E. 2562 (2019) and the resolution of the Cybersecurity Regulating Committee Meeting no. 2/2019 on 1 August 2019, the Cybersecurity Regulating Committee has issued a regulation, as follows:

Clause 1 The regulation is called the "Regulation of the Cybersecurity Regulating Committee on the Assignment of Powers to Perform Tasks on behalf of the Cybersecurity Regulating Committee B.E. 2565 (2021)"

Clause 2 The regulation shall come into force on the date following its publication date in the Royal Thai Government Gazette.

Clause 3 In this regulation

"Assignment of Powers" shall mean the Cybersecurity Regulating Committee, who has the powers and duties to act or undertake actions under the laws, rules, regulations, notifications, or any orders or resolutions of the Cabinet, assigns its powers in issuing orders, permissions, approvals, performing duties on behalf, or in undertaking any actions under any laws, rules, regulations, notifications or order or the resolution of the Cabinet in that matter to the Critical Incident Response Committee to perform such tasks for them;

"Assigner" shall mean the Cybersecurity Regulating Committee, who has the powers to act or undertake actions under the laws, rules, regulations, notifications, or any orders or resolutions of the Cabinet to issue orders, permissions, approvals, performing duties on behalf, or in undertaking any actions;

"Assignee" shall mean the Critical Incident Response Committee or the Secretary-General who is assigned the powers from the Cybersecurity Regulating Committee who has such powers;

“Organization of Critical Information Infrastructure” shall mean a Government Agency or private organization who has a mission of or provides a Critical Information Infrastructure service;

“ Regulator and Organization of Critical Information Infrastructure” shall mean the Regulator and the Organization of Critical Information Infrastructure in accordance with the notification from the National Cyber Security Committee that specifies the characteristics of the organization who has a mission of or provides a Critical Information Infrastructure service in accordance with section 49 of the Cybersecurity Act B.E. 2562 (2019);

“ Incident at a Critical Level” or “Critical Incident” shall mean an incident with the nature of having significant increase in attacks on computer systems, computers, or computer data, with the aim to attack the Organization of Critical Information Infrastructure of the country, and such attack has the effect of causing damage to the computer systems of the information technology infrastructure related to the operation of the Organization of Critical Information Infrastructure of the country, public stability, international relations, national defense, economy, public health, public safety, or the public order of the people, such that the Organization of Critical Information Infrastructure could not operate or provide service;

“CRC” shall mean the Cybersecurity Regulating Committee;

“ Critical Incident Response Committee” shall mean the Critical Incident Response Committee that the Cybersecurity Regulating Committee has appointed and assigned the powers to perform tasks in accordance with this regulation;

“ Competent Official” shall mean a person appointed by the Minister for the execution of the Cybersecurity Act B.E. 2562 (2019);

“Secretary-General” shall mean the Secretary-General of the National Cyber Security Committee;

“Agency” shall mean the National Cyber Security Agency;

“Electronic Meeting” shall mean a meeting that is required to be held by law and has been conducted through electronic means, in respect of which the attendees are not present at the same place and the consultation, discussion, and expression of opinions among them are enabled through electronic means;

“Attendees” shall mean chairpersons, directors, or secretaries, and assistant secretaries, and shall also include persons required to give explanations or opinions to the Critical Incident Response Committee.

Clause 4 In order to supervise and undertake in order to handle an Incident at a Critical Level in a timely manner, the Cybersecurity Regulating Committee may assign powers to the Critical Incident Response Committee or the Secretary-General in accordance with section 61, section 62, section

63, section 64, section 65, and section 66 of the Cybersecurity Act B.E. 2562 (2019) and in accordance with this regulation.

Clause 5 There shall be a committee named the "Critical Incident Response Committee", abbreviated as "CIRC", which shall be comprised of:

(1) Minister of Digital Economy and Society — as the chairperson;

(2) Supreme Commander — as a director;

(3) Commissioner-General of the National Police Bureau — as a director;

(4) Permanent Secretary of the Ministry of Digital Economy and Society — as a director;

(5) Secretary-General of the National Security Council — as a director;

(6) Secretary-General — as a director and secretary.

The Secretary-General shall appoint assistant secretaries from the officials of the Agency not exceeding two persons.

Clause 6 When it appears or is suggested by the Agency to the CIRC that an Incident at a Critical Level occurs or may occur, the CIRC shall have duties and powers as follows:

(1) jointly perform duties to handle the Critical Incident with the Regulator and the Organization of Critical Infrastructure in accordance with the measures to prevent, respond, assess, eradicate, and contain the incident at each level as prescribed in the "Notification of the National Cyber Security Committee regarding the Cyber Threat Impact Characteristics and Cybersecurity Measures for Prevention, Response, Assessment, Eradication, and Containment of Incidents at Each Level";

(2) supervise and undertake in order to handle an Incident at a Critical Level in a timely manner, the Cybersecurity Regulating Committee may assign powers to the Critical Incident Response Committee or the Secretary-General in accordance with section 61, section 62, section 63, section 64, section 65, and section 66 of the Cybersecurity Act B.E. 2562 (2019), as follows:

(2.1) prescribe the Regulator and the Critical Information Infrastructure that is under attack to participate, coordinate with, and provide supports for the CIRC in handling the Critical Incident in a timely manner;

(2.2) assign the Agency the task to analyze the situation, assess the incident impact, handle the incident, and perform computer forensics analysis, in order to issue an order when a Critical Incident has occurred or is expected to occur. To track and review the outcomes of such operations, the Agency shall submit an operation result report to the CRC;

(2.3) when it appears to the CIRC that a Critical Incident has occurred or is expected to occur, the CIRC shall issue an order to the Agency to act in accordance with section 61 to support the situation analysis and the incent impact assessment, and the Secretary-General shall issue an order to the Competent Officials to act in accordance with section 62;

(2.4) In case of necessity to prevent, handle, and mitigate risks from a Critical Incident, the CIRC shall order the Government Agency to provide information, support its personnel, or use electronic devices under its possession in relation to maintaining cybersecurity.

The CIRC shall ensure that there shall be no use of information under (2.4) paragraph one that may cause damages and propose that the CRC assumes responsibility for personnel compensation, expenses, or damages from the use of such electronic devices.

The contents in (2.4) paragraph one and paragraph two shall also be applied when the CIRC makes such a request to private organizations, contingent upon their consent.

(2.5) In case there is or may be an Incident at a Critical Level, the CIRC shall prevent, handle, and mitigate risks from the incident and conduct necessary measures.

In the operation under (2.5) paragraph one, the CIRC shall issue a letter to the Government Agency which relates to maintaining cybersecurity to act or omit any act to prevent, handle, or mitigate risks from the incident properly and efficiently, in accordance with the guideline prescribed by the CRC, including integrating the operation to control, contain, or mitigate the effect caused by the incident in a timely manner.

The Secretary-General shall report the operation in accordance with (2.5) paragraph one and paragraph two to the CRC constantly and when such incident ends. The Secretary-General shall report the operation result to the CRC without delay.

(2.6) To handle and remedy the damages from an Incident at a Critical Level, the CIRC has the power to issue an order, as necessary, to prevent the Incident, the owner, the person possessing the computer(s), or the user of the computer(s) or the computer system(s) or the person monitoring the computer system(s), which has a reasonable cause to believe that he/she is related to or is affected by the Incident to do the following:

(2.6.1) monitor the computer(s) or computer system(s) during a certain period of time;

(2.6.2) examine the computer(s) or computer system(s) to find vulnerabilities that affect cybersecurity, analyze the situation, and evaluate the effects from the Incident;

(2.6.3) conduct a cybersecurity measure to handle vulnerabilities or remove unwanted programs or contain and mitigate the Incidents that are active;

(2.6.4) maintain the status of the computer data or computer system(s) via any methods to perform computer forensic science analysis;

(2.6.5) access relevant computer data or computer system(s) or other information related to the computer system(s) only to the extent it is necessary to prevent the Incident.

In case of necessity to access information under (2.6.5), the CIRC shall delegate the Secretary-General to submit the motion to the Competent Court to order the owner, the possessor of the computer(s), the user of the computer(s) or computer system(s) or a person monitoring the computer system(s) in accordance with paragraph one to comply with the motion. The motion submitted to the Court shall show a probable cause that the individual is performing or is going to perform an act that causes the Incident at a Critical Level. The motion shall be submitted as emergency hearing motion and shall be considered by the Court without delay.

(2.7) In preventing, handling, or mitigating the risks from an Incident at a Critical Level, the CIRC has the power to order Competent Officials, only to the extent that it is necessary to prevent the Incident, to do the following:

(2.7.1) enter into and examine premises, with a letter stating the reason for entry to the owner or the occupier. If there is a probable cause to believe that there is a computer or computer system related to or affected by the Incident;

(2.7.2) access the computer data, computer systems, or other data related to the computer system, copy, or filter/screen information or computer programs believed to be related to or affected by the Incident;

(2.7.3) test the operation of the computer or computer system believed to be related to or affected by the Incident, or to be exploited or used to search for any internal information;

(2.7.4) for the examination or analysis, confiscate or seize a computer, a computer system, or any equipment, only to the extent that it is necessary as it is believed to be related to the incident. Such examination or analysis shall be conducted within thirty days. Once such period is over, the computer or any equipment shall be returned to the owner or the person possessing the computer immediately after the examination or analysis is finished.

In operating in accordance with (2.7.2), (2.7.3), and (2.7.4), the CIRC shall delegate the Secretary-General to submit the motion to the Competent Court to order Competent Officials to comply with the motion. The motion submitted to the Court shall show

a probable cause that the individual is performing or is going to perform an act that will cause an Incident at a Critical Level. The motion shall be submitted as emergency hearing motion and shall be considered by the Court without delay.

(3) Perform any other tasks as assigned by the CRC.

Clause 7 To schedule an appointment of a CIRC meeting, the secretary must notify all the directors of the CIRC meeting in advance at least three days. The notification can first be made verbally and followed by a written notice which can be sent electronically. An exception is when the meeting schedule is already notified in the prior meeting.

In event of urgency that prevents an advance scheduling of meetings in accordance with paragraph one, the secretary shall notify the CIRC to hold an urgent meeting by using the procedure in paragraph one *mutatis mutandis*. However, the meeting notification sent to each CIRC member shall be recorded as evidence.

The secretary shall send the meeting agenda and relevant documents along with the meeting invitation, which can be done electronically as long as there is a cybersecurity measure for such electronic documents. Only when necessary, the meeting notification may be sent on or after the meeting date.

Clause 8 The CIRC meeting agenda shall, at minimum, consist of the following items:

(1) Chairperson's Report;

(2) Approval of Minutes of the Previous Meeting;

(3) Matters of Report;

(4) Matters Pending or Arising;

(5) Matters for Consideration.

Clause 9 A CIRC meeting shall adhere to the following:

(1) a quorum of the CIRC requires at least half of the members to be present.;

(2) the CIRC chairperson is the default meeting chairperson. If the CIRC chairperson is absent or unable to perform the duties, the present members may elect a CIRC member to serve as the meeting chairperson;

(3) any CIRC member with a direct interest in a matter under consideration cannot attend the meeting or vote on the matter, but is counted as part of the quorum;

(4) the final decision of the meeting is determined by a majority vote, with each CIRC member having one vote. In the event of a tie, the chairperson casts a deciding vote;

(5) for any matter that the CIRC has approved in the meeting resolution, the secretary shall notify the meeting resolution to the stakeholders without having to wait for the approval of the meeting minutes.

Clause 10 If a director by position cannot attend the meeting, the person, who attends the meeting in the director's place and has the powers to perform such duties by law, shall be counted as part of the quorum.

Clause 11 The CIRC electronic meeting shall be in accordance with the laws regarding electronic meetings.

Clause 12 The CIRC shall report the operation in accordance with Clause 6 to the CRC chairperson constantly and without delay. When the Incident has ended, the operation outcome shall also be reported to the CRC.

Clause 13 The Regulator and the Organization of Critical Information Infrastructure that is under attack shall participate, coordinate with, and provide support to the CIRC in responding to the Critical Incident in a timely manner.

Clause 14 The Agency or the Competent Officials shall coordinate with the relevant parties in undertaking the duty and power by virtue of section 61, section 62, section 63, section 64, section 65, and section 66 of the National Cybersecurity Act B.E. 2562 (2019).

In undertaking the duty according to paragraph one, it could be done in writing, or verbally, or by conveying the message through any other means as long as the message is clear and understandable. If the order is issued verbally, the recipient may reasonably request a written order within seven days after the order date, the Secretary-General shall provide an order confirmation in a written form as requested.

Furthermore, immediate and continuous reporting to the CRC chairperson is required. When the Incident has ended, the operation outcome shall also be reported to the CRC.

Clause 15 When exercising the assigned power, the Assignee may take any actions necessary to achieve the objective of the assignment, as long as the actions comply with all relevant laws and regulations, and any other rules or conditions specified by the Assignor. The Assignee must also compile a report of the operation outcome, according to the criteria specified by the Assignor.

Clause 16 The Chairperson of the Cybersecurity Regulating Committee shall be the person in charge of this regulation, and shall have the power to issue notifications, orders, rules, and methods for the benefit of complying with this regulation.

In the case that there is a problem in enforcing or complying with this regulation, or that the regulation does not cover a particular matter, the Chairperson of the Cybersecurity Regulating Committee shall have the power to interpret and adjudicate the matter and that the interpretation and adjudication of the Chairperson of the Cybersecurity Regulating Committee is final.

Given on the of September B.E. 2565 (2022)

Chaiwut Thanakamanusorn

(Mr. Chaiwut Thanakamanusorn)
Minister of Digital Economy and Society
Chairperson of the Cybersecurity Regulating Committee

9

ประกาศ กมช.

เรื่อง นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 - 2570)

มีผลใช้บังคับตั้งแต่วันที่ 10 ธ.ค. 65 เป็นต้นไป

Notification of NCSC

Re: Policy and plan on cyber security B.E. 2565 - 2570 (2022-2027)

Effective from December 10, 2022, onwards.



ฉบับภาษาไทย
Thai Version

ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

เรื่อง นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. ๒๕๖๕ - ๒๕๗๐)

โดยที่คณะรัฐมนตรีได้มีมติเมื่อวันที่ ๒๐ กันยายน ๒๕๖๕ เห็นชอบนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. ๒๕๖๕ - ๒๕๗๐) ตามที่คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเสนอ ซึ่งเป็นการจัดทำนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. ๒๕๖๕ - ๒๕๗๐) นั้น

อาศัยอำนาจตามความในมาตรา ๙ (๑) (๒) และ (๓) และมาตรา ๔๓ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และตามคำสั่งสำนักนายกรัฐมนตรี ที่ ๒๓๙/๒๕๖๓ เรื่อง มอบหมายและมอบอำนาจให้รองนายกรัฐมนตรี และรัฐมนตรีประจำสำนักนายกรัฐมนตรีปฏิบัติหน้าที่ประธานกรรมการในคณะกรรมการต่าง ๆ ตามกฎหมาย และระเบียบสำนักนายกรัฐมนตรีและตามมติคณะรัฐมนตรีข้างต้น จึงออกประกาศแจ้งการใช้นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. ๒๕๖๕ - ๒๕๗๐) เพื่อเป็นแผนแม่บทในการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย การพัฒนาความมั่นคงปลอดภัยทางไซเบอร์ในภาพรวมที่ครอบคลุมในทุกมิติ และเพื่อใช้เป็นกรอบแนวทางการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ ซึ่งสอดคล้องกับยุทธศาสตร์ชาติด้านความมั่นคงแผนย่อย การป้องกันและแก้ไขปัญหาที่มีผลกระทบต่อความมั่นคง ซึ่งมีเป้าหมายของแนวทางพัฒนาคือปัญหาความมั่นคงที่มีอยู่ในปัจจุบัน (ความมั่นคงทางไซเบอร์) ได้รับการแก้ไขจนไม่ส่งผลกระทบต่อการบริหารและพัฒนาประเทศ ดังมีสาระสำคัญตามที่แนบท้ายประกาศนี้

ทั้งนี้ ประกาศฉบับนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ประกาศ ณ วันที่ ๑๓ พฤศจิกายน พ.ศ. ๒๕๖๕
พลเอก ประวิตร วงษ์สุวรรณ
รองนายกรัฐมนตรี ปฏิบัติหน้าที่
ประธานกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

นโยบายและแผนปฏิบัติการ ว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 – 2570)



สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

นโยบายและแผนปฏิบัติการ

ว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. ๒๕๖๕ - ๒๕๗๐)

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

ส่วนที่ ๑ บทสรุปผู้บริหาร

นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๕-๒๕๗๐ ฉบับนี้ เป็นการดำเนินการตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

มาตรา ๙ (๑) บัญญัติให้คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) มีหน้าที่และอำนาจ เสนอนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ ส่งเสริมและสนับสนุนการดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ตามมาตรา ๔๒ และมาตรา ๔๓ ต่อคณะรัฐมนตรีเพื่อให้ความเห็นชอบ

นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์นี้ใช้เป็นแผนแม่บทในการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย การพัฒนาความมั่นคงปลอดภัยทางไซเบอร์ในภาพรวมที่ครอบคลุมในทุกมิติ และเพื่อใช้เป็นกรอบแนวทางการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ

มาตรา ๙ (๓) บัญญัติให้คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) มีหน้าที่และอำนาจ จัดทำแผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์เสนอต่อคณะรัฐมนตรีสำหรับเป็นแผนแม่บทในการรักษาความมั่นคงปลอดภัยไซเบอร์ในสถานการณ์ปกติและในสถานการณ์ที่อาจจะเกิดหรือเกิดภัยคุกคามทางไซเบอร์ โดยแผนดังกล่าวจะต้องสอดคล้องกับนโยบาย ยุทธศาสตร์และแผนระดับชาติ และกรอบนโยบายและแผนแม่บทที่เกี่ยวกับการรักษาความมั่นคงของสภาความมั่นคงแห่งชาติ

ส่วนที่ ๒ ความสอดคล้องกับแผน ๓ ระดับ ตามนัยยะของมติคณะรัฐมนตรี เมื่อวันที่ ๔ ธันวาคม ๒๕๖๐

๒.๑ ยุทธศาสตร์ชาติ (แผนระดับที่ ๑)

๒.๑.๑ ยุทธศาสตร์ชาติ ด้านความมั่นคง

เป้าหมายที่ ๓ กองทัพ หน่วยงานด้านความมั่นคง ภาครัฐ ภาคเอกชนและภาคประชาชนมีความพร้อมในการป้องกันและแก้ไขปัญหาความมั่นคง

เป้าหมายที่ ๔ ประเทศไทยมีบทบาทด้านความมั่นคงเป็นที่ชื่นชมและได้รับการยอมรับโดยประชาคมระหว่างประเทศ

เป้าหมายที่ ๕ การบริหารจัดการความมั่นคงมีผลสำเร็จที่เป็นรูปธรรมอย่างมีประสิทธิภาพ

๒.๑.๒ ประเด็นยุทธศาสตร์

ข้อ ๔.๒ การป้องกันและแก้ไขปัญหาที่มีผลกระทบต่อความมั่นคง

ข้อ ๔.๒.๑ การแก้ไขปัญหาความมั่นคงในปัจจุบัน

ข้อ ๔.๒.๒ การติดตาม เฝ้าระวัง ป้องกัน และแก้ไขปัญหาที่อาจอุบัติขึ้นใหม่

๒.๒ แผนระดับที่ ๒

๒.๒.๑ แผนแม่บทภายใต้ยุทธศาสตร์ชาติ

ประเด็นยุทธศาสตร์ด้านความมั่นคง

ข้อ ๓.๒ แผนย่อยการป้องกันและแก้ไขปัญหาที่มีผลกระทบต่อความมั่นคง

๒.๒.๒ แผนปฏิรูปประเทศด้านสื่อสารมวลชน เทคโนโลยีสารสนเทศ

ประเด็นยุทธศาสตร์แผนปฏิรูปประเทศด้านสื่อสารมวลชน เทคโนโลยีสารสนเทศ

ข้อ ๕.๕ การปฏิรูปการบริหารจัดการความปลอดภัยไซเบอร์ /กิจการอวกาศและระบบและเครื่องมือด้านการสื่อสารมวลชนและโทรคมนาคมเพื่อสนับสนุนภารกิจการป้องกันบรรเทาสาธารณภัย ภายใต้กิจกรรมที่ ๑ การปกป้องคุ้มครองและรักษาความมั่นคงปลอดภัยไซเบอร์ของโครงสร้างพื้นฐานสำคัญด้านสารสนเทศของประเทศ

๒.๒.๓ แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ ๑๒

ยุทธศาสตร์ที่ ๕ การเสริมสร้างความมั่นคงแห่งชาติเพื่อการพัฒนาประเทศสู่ความมั่งคั่งและยั่งยืน

แนวทางการพัฒนาที่ ๓.๒ การพัฒนาเสริมสร้างศักยภาพการป้องกันประเทศ เพื่อเตรียมความพร้อมในการรับมือภัยคุกคาม ทั้งการทหารและภัยคุกคามอื่น ๆ

ยุทธศาสตร์ที่ ๗ การพัฒนาโครงสร้างพื้นฐานและระบบโลจิสติกส์

แนวทางการพัฒนาที่ ๓.๕ การพัฒนาเศรษฐกิจดิจิทัล

๒.๒.๔ นโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ (พ.ศ. ๒๕๖๒ – ๒๕๖๕)

นโยบายที่ ๑๐ เสริมสร้างความมั่นคงปลอดภัยไซเบอร์ รองรับวัตถุประสงค์ ๓.๔.๕ เพื่อพัฒนาศักยภาพของภาครัฐ และส่งเสริมบทบาทและความเข้มแข็งของทุกภาคส่วนในการรับมือกับภัยคุกคามทุกรูปแบบที่กระทบกับความมั่นคง

แผนที่ ๑๕ การป้องกันและแก้ไขความมั่นคงทางไซเบอร์

๒.๓ แผนระดับที่ ๓ ที่เกี่ยวข้อง

๒.๓.๑ นโยบายและแผนระดับชาติว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม (พ.ศ ๒๕๖๑ – ๒๕๘๐)

ยุทธศาสตร์ที่ ๖ สร้างความเชื่อมั่นในการใช้เทคโนโลยีดิจิทัล

แผนงาน ข้อ ๓ สร้างความเชื่อมั่นในการใช้เทคโนโลยีดิจิทัลและการทำธุรกรรมออนไลน์

๒.๓.๒ แผนปฏิบัติการด้านดิจิทัลเพื่อเศรษฐกิจและสังคมระยะ ๕ ปี (พ.ศ. ๒๕๖๒ - ๒๕๖๕)

เป้าหมายที่ ๕ สร้างความเชื่อมั่น

ประเด็นขับเคลื่อน ๕.๑ การเสริมสร้างความมั่นคงปลอดภัยไซเบอร์

ประเด็นขับเคลื่อน ๕.๒ ขับเคลื่อนการพัฒนากฎหมายและมาตรฐานดิจิทัล

เป้าหมายที่ ๖ พัฒนากำลังคนดิจิทัล

ประเด็นขับเคลื่อน ๖.๑ การพัฒนากำลังคนและประชาชนสู่ยุคดิจิทัล

๒.๓.๓ ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (พ.ศ ๒๕๖๐ - ๒๕๖๕)

ประเด็นยุทธศาสตร์ที่ ๑ เสริมสร้างความเชื่อมั่นและความไว้วางใจในทุกภาคส่วนในการดำเนินกิจกรรมทางไซเบอร์ทุกรูปแบบ

ประเด็นยุทธศาสตร์ที่ ๒ ปกป้องโครงสร้างพื้นฐานสำคัญที่บริหารจัดการด้วยระบบสารสนเทศและพัฒนาศักยภาพด้านการรับมือภัยคุกคามทางไซเบอร์

ประเด็นยุทธศาสตร์ที่ ๓ ปกป้องผลประโยชน์และความมั่นคงของชาติให้รอดพ้นจากภัยคุกคามรูปแบบเดิมและรูปแบบใหม่

ประเด็นยุทธศาสตร์ที่ ๔ เสริมสร้างระบบเศรษฐกิจดิจิทัล

ประเด็นยุทธศาสตร์ที่ ๕ สร้างความตระหนักและส่งเสริมความร่วมมือภายในประเทศด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

ประเด็นยุทธศาสตร์ที่ ๖ เพื่อส่งเสริมวัฒนธรรมการใช้ไซเบอร์สเปซในทางที่เหมาะสม

ประเด็นยุทธศาสตร์ที่ ๗ ส่งเสริมงานด้านการป้องกันและปราบปรามอาชญากรรม

ประเด็นยุทธศาสตร์ที่ ๘ ส่งเสริมบทบาทที่สร้างสรรค์ของไทยในความร่วมมือเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับภูมิภาคและระดับนานาชาติ

๒.๓.๔ แผนเตรียมพร้อมแห่งชาติ (พ.ศ. ๒๕๖๐-๒๕๖๕)

ยุทธศาสตร์ที่ ๓ การเสริมสร้างความร่วมมือ การเตรียมพร้อมรับมือภัยคุกคามกับต่างประเทศ

กลยุทธ์ ข้อ ๔ เสริมสร้างความสัมพันธ์และความร่วมมือการเตรียมพร้อมด้านวิกฤตการณ์ความมั่นคงกับต่างประเทศ อาทิ การก่อวินาศกรรม การก่อการร้าย ภัยความมั่นคงทางไซเบอร์ ภัยความมั่นคงทางอวกาศ โรคติดต่ออุบัติใหม่ ให้สอดคล้องกับนโยบายรัฐบาล นโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ และยุทธศาสตร์ความมั่นคงเฉพาะด้านที่เกี่ยวข้อง

ส่วนที่ ๓ สาระสำคัญของ นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๕-๒๕๗๐

๓.๑ การประเมินสถานการณ์ ปัญหา ความจำเป็นของนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๕-๒๕๗๐

ปัจจุบันเทคโนโลยีดิจิทัลมีบทบาทสำคัญในการเป็นเครื่องมืออำนวยความสะดวกแก่การดำรงชีวิตประจำวัน โดยรายงานของสหภาพโทรคมนาคมระหว่างประเทศ (International Telecommunication Union :ITU) พบว่า ปี พ.ศ. ๒๕๖๑ มีจำนวนผู้ใช้อินเทอร์เน็ต คิดเป็นร้อยละ ๕๑ ของประชากรทั่วโลก โดยคาดว่า ภายในปี พ.ศ. ๒๕๖๖ จะมีจำนวนผู้ใช้งานอินเทอร์เน็ต เพิ่มขึ้นถึงร้อยละ ๗๐ ของประชากรทั่วโลก

ผลสำรวจพฤติกรรมผู้ใช้งานอินเทอร์เน็ตในประเทศไทยปี พ.ศ. ๒๕๖๑ โดยสำนักงานพัฒนาธุรกรรมอิเล็กทรอนิกส์ (สพธอ.) พบว่า ประเทศไทยก้าวสู่สังคมดิจิทัลอย่างเต็มรูปแบบแล้ว ซึ่งค่าเฉลี่ยของการใช้งานอินเทอร์เน็ตของคนไทยเติบโตเพิ่มขึ้นมากกว่าปีที่ผ่านมาถึง ๓ เท่า ทั้งนี้ ความก้าวหน้าทางเทคโนโลยีดิจิทัล โดยเฉพาะอย่างยิ่งการใช้อินเทอร์เน็ตมาพร้อมกับความท้าทายและภัยคุกคามทางไซเบอร์ซึ่งมีหลากหลายรูปแบบ ไม่ว่าจะเป็นการเผยแพร่ ข้อมูลที่ไม่เป็นจริง

การพยายามบุกรุกเข้าระบบ การโจมตีสภาพการใช้งานของระบบ การพัฒนาโปรแกรมที่ไม่พึงประสงค์ และการสร้างหน้าเว็บไซต์ปลอมเพื่อหลอกลวงหาผลประโยชน์ เป็นต้น อันก่อให้เกิดความเสียหายแก่ประเทศชาติ ภาคธุรกิจ และปัจเจกบุคคล

จากข้อมูลสถิติภัยคุกคามทางไซเบอร์ของไทย ปี พ.ศ. ๒๕๖๑ รวบรวมโดยศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต) พบว่าความพยายามบุกรุกเข้าระบบสารสนเทศ (Intrusion Attempts) เป็นภัยคุกคามไซเบอร์ อันดับ ๑ ของประเทศไทย คิดเป็นสัดส่วนร้อยละ ๔๓ จากจำนวนภัยคุกคาม ทั้งหมด ๒,๕๒๐ เหตุการณ์

นอกจากนี้ ผลจากการสำรวจความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ ในปี พ.ศ. ๒๕๕๙ และ พ.ศ. ๒๕๖๑ ของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.) เพื่อวิเคราะห์ถึงสถานการณ์ ปัญหา อุปสรรค และการรับมือกับภัยคุกคามไซเบอร์ของประเทศไทย โดยมีหลักการพิจารณา ๑) การกำหนดมาตรการความมั่นคงปลอดภัยไซเบอร์ ๒) การปกป้องดูแลอุปกรณ์สารสนเทศ ๓) ความสามารถในการตรวจพบเหตุภัยคุกคาม ๔) การรับมือภัยคุกคาม และ ๕) การกู้คืนระบบหลังเกิดเหตุ พบว่า การรับมือภัยคุกคามไซเบอร์ของหน่วยงานภาครัฐและภาคเอกชนมากกว่า ๕๐๐ หน่วยงาน มีค่าเฉลี่ยในระดับต่ำ

จากสถานการณ์ภัยคุกคามไซเบอร์ข้างต้นที่เกิดขึ้นอย่างรวดเร็วและรุนแรงขึ้นทุกปี การขาดแคลนบุคลากรที่ปฏิบัติหน้าที่ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อันส่งผลต่อความสามารถในการดำเนินการ จนส่งผลให้ถูกโจมตีทางไซเบอร์และส่งผลต่อเศรษฐกิจของประเทศไทยอย่างมหาศาล ถึงแม้ว่าจะมีการลงทุนในการรักษาความมั่นคงปลอดภัยไซเบอร์ที่เพิ่มสูงขึ้น แต่ในประเทศไทยเองยังขาดแคลนบุคลากร และผลิตภัณฑ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่เป็นนวัตกรรมในประเทศ ทำให้ต้องพึ่งพาบุคลากรและผลิตภัณฑ์จากต่างประเทศ ดังนั้น จึงมีความจำเป็นต้องกำหนดนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ ในการเสริมสร้างศักยภาพในการป้องกัน รับมือและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ตลอดจนตอบสนองต่อเหตุภัยคุกคามและฟื้นฟูระบบให้กลับคืนสู่สภาวะปกติอย่างทันท่วงที

๓.๒ สาระสำคัญของ นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๕ - ๒๕๗๐

นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ฉบับสมบูรณ์นี้ ได้กำหนดวิสัยทัศน์การรักษาความมั่นคงปลอดภัยไซเบอร์ คือ **“บริการที่สำคัญของประเทศไทยมีความมั่นคงปลอดภัยไซเบอร์ เพื่อความยั่งยืนทางเศรษฐกิจและสังคม”**

นโยบายและแผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๕ – ๒๕๗๐ เป็นแผนแม่บทในการรักษาความมั่นคงปลอดภัยไซเบอร์ในสถานการณ์ปกติ และในสถานการณ์ที่อาจจะเกิดหรือเกิดภัยคุกคามทางไซเบอร์ ซึ่งสอดคล้องกับนโยบายยุทธศาสตร์และแผนระดับชาติ และกรอบนโยบายและแผนแม่บทที่เกี่ยวกับการรักษาความมั่นคงของสภาความมั่นคงแห่งชาติ

เพื่อให้บรรลุวิสัยทัศน์และเป้าหมายการขับเคลื่อนยุทธศาสตร์ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ จึงได้กำหนดยุทธศาสตร์การดำเนินงาน ๔ ยุทธศาสตร์ ดังนี้

๓.๒.๑ ยุทธศาสตร์ที่ ๑ : สร้างขีดความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ (บุคลากร องค์ความรู้ และเทคโนโลยี) (Capacity)

วัตถุประสงค์

เพื่อเสริมสร้างขีดความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ โดยบูรณาการ-บุคลากร องค์ความรู้ และเทคโนโลยี นำไปสู่การพัฒนาผลิตภัณฑ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่เป็นนวัตกรรมของประเทศ

เป้าหมาย

๑. พัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์เพื่อรองรับความต้องการของประเทศ

๒. ส่งเสริมให้บุคลากรทุกภาคส่วนมีความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์

๓. ส่งเสริมให้เกิดการมีส่วนร่วมในการสร้างความแข็งแกร่งด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศ

๔. ส่งเสริมการพัฒนาผลิตภัณฑ์ด้านความมั่นคงปลอดภัยไซเบอร์ให้เป็นนวัตกรรมของประเทศ

กลยุทธ์ที่ ๑.๑ เพิ่มบุคลากรที่มีความสามารถด้านความมั่นคงปลอดภัยไซเบอร์

๑. พัฒนาหลักสูตรการเรียนการสอนด้านความมั่นคงปลอดภัยไซเบอร์ทั้งภาคทฤษฎีและภาคปฏิบัติ เป็นสาขาเฉพาะทางในระดับอุดมศึกษา รองรับความต้องการของภาคอุตสาหกรรมที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

๒. พัฒนาทักษะและฝึกอบรมบุคลากรด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ทั้งในระดับผู้บริหารและผู้ปฏิบัติงาน

ตัวชี้วัดของกลยุทธ์

๑. มีหลักสูตรการเรียนการสอนด้านความมั่นคงปลอดภัยไซเบอร์ทั้งภาคทฤษฎีและภาคปฏิบัติ เป็นสาขาเฉพาะทางในระดับอุดมศึกษา รองรับความต้องการของภาคอุตสาหกรรมที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ ไม่น้อยกว่า ๕ สถาบัน

๒. บุคลากรด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานควบคุมหรือกำกับดูแลและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ทั้งในระดับผู้บริหารและผู้ปฏิบัติงานไม่น้อยกว่าร้อยละ ๘๐ ได้รับการพัฒนาความรู้และทักษะ

โครงการขับเคลื่อนกลยุทธ์

๑. โครงการพัฒนากรอบความสามารถและโปรแกรมการฝึกอบรมด้านความปลอดภัยทางไซเบอร์ ส่งเสริมและสนับสนุนการออกใบรับรอง (Certification) และการรับรอง (Accreditation) บุคลากรที่มีความเชี่ยวชาญในระดับชาติและนานาชาติ

๒. โครงการยกระดับวิชาชีพด้านความมั่นคงปลอดภัยไซเบอร์ ให้เป็นที่ยอมรับ

๓. โครงการพัฒนาบุคลากรทางไซเบอร์โดยส่งเสริมให้มีสถาบันการศึกษามีหลักสูตรด้านความมั่นคงปลอดภัยไซเบอร์เฉพาะทาง

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
๑. โครงการพัฒนากรอบความสามารถและโปรแกรม	๑) จัดทำกรอบความสามารถและโปรแกรมการฝึกอบรมด้านความปลอดภัยทางไซเบอร์สำหรับผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์ และสำหรับผู้ที่ไม่ใช่	**หลัก:** สกมช. **รอง:** สพร. สพธอ.

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
การฝึกอบรมด้านความปลอดภัยทางไซเบอร์ ส่งเสริมและสนับสนุนการออกใบรับรอง (Certification) และการรับรอง (Accreditation) บุคลากรที่มีความเชี่ยวชาญในระดับชาติและนานาชาติ	ไอที (non-IT) การออกใบรับรอง (Certification) และการรับรอง (Accreditation) บุคลากรที่มีความเชี่ยวชาญ ๒) จัดทำหลักสูตรและเนื้อหาสำหรับตอบสนองกรอบความสามารถและโปรแกรมการฝึกอบรม การออกใบรับรอง (Certification) และการรับรอง (Accreditation) บุคลากรที่มีความเชี่ยวชาญ ๓) กำหนดให้ใช้กรอบความสามารถและโปรแกรมการฝึกอบรมด้านความปลอดภัยทางไซเบอร์สำหรับผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์และสำหรับผู้ที่ไม่ใช่ไอที (non-IT) เป็นส่วนหนึ่งในข้อกำหนดจ้างงาน/เลื่อนตำแหน่ง ๔) เป็นพันธมิตร ให้ทุนส่งเสริมและสนับสนุนให้มีหน่วยงานที่สนับสนุนฝึกอบรมด้านความปลอดภัยทางไซเบอร์สำหรับผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์และสำหรับผู้ที่ไม่ใช่ไอที (non-IT) การออกใบรับรอง (Certification) และการรับรอง (Accreditation) บุคลากรที่มีความเชี่ยวชาญ โดยอาจพิจารณาสิทธิพิเศษทางภาษี และมาตรการส่งเสริมต่าง ๆ เพื่อเพิ่มจำนวนของหน่วยงานสนับสนุน ๕) ส่งเสริม เผยแพร่ จัดอบรม และทุนสนับสนุนอย่างต่อเนื่อง ๖) กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง	สำนักงาน ก.พ. ดศ. สคช. สดช. สอศ. อว. หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ บก.ทท. สปท. บีโอไอ
๒. โครงการยกระดับวิชาชีพด้านความมั่นคงปลอดภัยไซเบอร์ให้เป็นที่ยอมรับ	๑) กำหนดแนวทางค่าตอบแทนของวิชาชีพด้านความมั่นคงปลอดภัยไซเบอร์ให้เหมาะสมและจูงใจ ๒) จัดกิจกรรมส่งเสริม สนับสนุน รวมถึงมีกิจกรรมการแข่งขันอย่างต่อเนื่อง ๓) หารือกับหน่วยงานที่เกี่ยวข้องกำหนดกรอบอัตรากำลังและค่าตอบแทนที่เหมาะสม ๔) เผยแพร่ประชาสัมพันธ์ผู้ที่เป็นต้นแบบและแรงบันดาลใจในสายงาน ๕) ส่งเสริม สนับสนุน ผู้ที่มีความสามารถด้านความมั่นคงปลอดภัยไซเบอร์อย่างต่อเนื่อง และเป็นรูปธรรม	**หลัก:** สกมช. **รอง:** สพร. สพธอ. สำนักงาน ก.พ. สคช. อว. สดช. สอศ. สพฐ. ดศ. สำนักงบประมาณ

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
	๖) กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง	หน่วยงานควบคุมหรือกำกับดูแลและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ บก.ทท. สปท.
๓. โครงการพัฒนาบุคลากรทางไซเบอร์โดยส่งเสริมให้มีสถาบันการศึกษามีหลักสูตรด้านความมั่นคงปลอดภัยไซเบอร์เฉพาะทาง	๑) จัดทำกรอบบูรณาการทักษะการรักษาความมั่นคงปลอดภัยไซเบอร์เฉพาะทางในระบบการศึกษาอย่างเป็นทางการตั้งแต่ระดับมัธยม ประกาศนียบัตรวิชาชีพ (ปวช.) จนถึงปริญญาเอก ๒) จัดทำหลักสูตรและเนื้อหาทักษะการรักษาความมั่นคงปลอดภัยไซเบอร์เฉพาะทางในระบบการศึกษาอย่างเป็นทางการตั้งแต่ระดับมัธยม ประกาศนียบัตรวิชาชีพ (ปวช.) จนถึงปริญญาเอก ๓) จัดกิจกรรมส่งเสริม รวมถึงการแข่งขันเพื่อหาบุคลากรที่มีความสามารถในการทำงาน พัฒนาวิจัย และสร้างผลิตภัณฑ์การรักษาความมั่นคงปลอดภัยไซเบอร์ ๔) ปรับปรุงระเบียบและข้อปฏิบัติในการจ่ายค่าตอบแทนให้เหมาะสมกับผู้ปฏิบัติงานการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีทักษะขั้นสูง ๕) สร้างความร่วมมือระหว่างภาคส่วนต่าง ๆ ในการบูรณาการ ๖) กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง	**หลัก:** สกมช. **รอง:** สพร. สพธอ. สำนักงาน ก.พ. สคช. สดช. สอศ. สพฐ. อว. ดศ. สำนักงบประมาณ หน่วยงานควบคุมหรือกำกับดูแลและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ บก.ทท. สปท.

กลยุทธ์ที่ ๑.๒ สร้างความตระหนักรู้และทักษะด้านความมั่นคงปลอดภัยไซเบอร์

๑. สร้างความตระหนักและการรู้เท่าทัน ด้านความมั่นคงปลอดภัยไซเบอร์

๒. ส่งเสริมให้เกิดการบูรณาการหลักสูตรเกี่ยวกับการตระหนักรู้และทักษะด้านความมั่นคงปลอดภัยไซเบอร์ ในระบบการศึกษาทุกระดับชั้น

ตัวชี้วัดของกลยุทธ์

๑. หน่วยงานควบคุมหรือกำกับดูแลและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ จำนวนไม่น้อยกว่าร้อยละ ๘๐ มีกิจกรรมการสร้างความตระหนักและการรู้เท่าทันด้านความมั่นคงปลอดภัยไซเบอร์ในแต่ละปี

๒. มีการบูรณาการหลักสูตรเกี่ยวกับการตระหนักรู้และทักษะด้านความมั่นคงปลอดภัยไซเบอร์ ในระบบการศึกษาทุกระดับชั้น

โครงการขับเคลื่อนกลยุทธ์

๑. โครงการบูรณาการทักษะการรักษาความมั่นคงปลอดภัยไซเบอร์กับทักษะดิจิทัลในระบบการศึกษาอย่างเป็นทางการตั้งแต่ระดับประถมศึกษาจนถึงระดับหลังปริญญา

๒. โครงการสร้างความตระหนักรู้ระดับชาติสำหรับกลุ่มเป้าหมายที่แตกต่างกัน (เช่น ผู้บริโภคทั่วไป ผู้ใช้ในองค์กร เด็ก ธุรกิจ) และหลากหลายรูปแบบ

๓. โครงการพัฒนาหลักปฏิบัติ (Code of practices) เพื่อความมั่นคงปลอดภัยของอุปกรณ์และผลิตภัณฑ์ที่เชื่อมต่ออินเทอร์เน็ต

๔. โครงการให้ความรู้ประชาชนเกี่ยวกับกฎหมาย กฎระเบียบ ความเสี่ยงของอาชญากรรมไซเบอร์ และมาตรการป้องกัน

๕. โครงการฝึกซ้อมเพื่อการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามไซเบอร์ของประเทศ กิจกรรมการจัดการฝึกและทดสอบแผนเผชิญเหตุ ในกรณีเกิดเหตุภัยคุกคามทางไซเบอร์ในระดับวิกฤติในระดับประเทศ

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
๑. โครงการบูรณาการทักษะการรักษาความมั่นคงปลอดภัยไซเบอร์กับทักษะดิจิทัลในระบบการศึกษาอย่างเป็นทางการตั้งแต่ระดับประถมศึกษาจนถึงระดับหลังปริญญา	๑) จัดทำกรอบบูรณาการทักษะการรักษาความมั่นคงปลอดภัยไซเบอร์กับทักษะดิจิทัลในระบบการศึกษาอย่างเป็นทางการตั้งแต่ระดับประถมศึกษาจนถึงระดับหลังปริญญา ๒) จัดทำหลักสูตรและเนื้อหาทักษะการรักษาความมั่นคงปลอดภัยไซเบอร์กับทักษะดิจิทัลในระบบการศึกษาอย่างเป็นทางการตั้งแต่ระดับประถมศึกษาจนถึงระดับหลังปริญญา ๓) จัดกิจกรรมส่งเสริม รวมถึงการแข่งขันเพื่อหาบุคลากรที่มีความสามารถในการทำงาน พัฒนาวิจัย และสร้างผลิตภัณฑ์การรักษาความมั่นคงปลอดภัยไซเบอร์ ๔) ปรับปรุงระเบียบและข้อปฏิบัติในการพิจารณาการเลื่อนตำแหน่งหรือค่าตอบแทนต้องผ่านเกณฑ์ทักษะการรักษาความมั่นคงปลอดภัยไซเบอร์	**หลัก:** สกมช. **รอง:** สพร. สพธอ. สำนักงาน ก.พ. สคช. สดช. สอศ. สพฐ. อว. ดศ. หน่วยงานควบคุมหรือกำกับดูแลและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
	๕) สร้างความร่วมมือระหว่างภาคส่วนต่าง ๆ ในการบูรณาการ ๖) กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง	
๒. โครงการสร้างความตระหนักรู้ระดับชาติสำหรับกลุ่มเป้าหมายที่แตกต่างกัน (เช่น ผู้บริโภคทั่วไป ผู้ใช้ในองค์กร เด็ก ธุรกิจ) และหลากหลายรูปแบบ	๑) จัดทำกรอบโปรแกรมสร้างความตระหนักรู้ระดับชาติด้วยแคมเปญที่กำหนดเป้าหมายสำหรับกลุ่มเป้าหมายที่แตกต่างกัน (เช่น ผู้บริโภคทั่วไป ผู้ใช้ในองค์กร เด็ก ธุรกิจ) ๒) จัดทำหลักสูตรและเนื้อหาโปรแกรมสร้างความตระหนักรู้ที่กำหนดเป้าหมายสำหรับกลุ่มเป้าหมายที่แตกต่างกัน ๓) จัดกิจกรรมส่งเสริม เผยแพร่โปรแกรมสร้างความตระหนักรู้ระดับชาติ ผ่านช่องทางที่หลากหลายตรงกับกลุ่มเป้าหมาย เช่น ละคร โฆษณา การ์ตูน เพลง หรือสื่ออื่น ๆ รวมถึงการให้รางวัลผู้ร่วมกิจกรรม ๔) พัฒนาแพลตฟอร์มในการเผยแพร่โปรแกรมสร้างความตระหนักรู้ระดับชาติ ๕) สนับสนุนการมีส่วนร่วม โดยอาจพิจารณาสิทธิพิเศษทางภาษี และมาตรการส่งเสริมต่าง ๆ เพื่อเพิ่มจำนวนของหน่วยงานสนับสนุน ๖) กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง	**หลัก:** สกมช. **รอง:** สพร. สพธอ. สดช. สอศ. สพฐ. อว. ดศ. หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
๓. โครงการพัฒนาหลักปฏิบัติ (Code of practices) เพื่อความมั่นคงปลอดภัยของอุปกรณ์และผลิตภัณฑ์ที่เชื่อมต่ออินเทอร์เน็ต	๑) จัดทำหลักปฏิบัติ (Code of practices) เพื่อความมั่นคงปลอดภัยของอุปกรณ์และผลิตภัณฑ์ที่เชื่อมต่ออินเทอร์เน็ต ๒) สนับสนุน เผยแพร่ประชาสัมพันธ์ และให้ความรู้ความเข้าใจในการปฏิบัติ ๓) สนับสนุนการมีส่วนร่วม โดยอาจพิจารณาสิทธิพิเศษทางภาษี และมาตรการส่งเสริมต่าง ๆ เพื่อเพิ่มจำนวนของหน่วยงานสนับสนุน ๔) จัดให้เจ้าหน้าที่ของรัฐมีทักษะที่เกี่ยวข้อง ๕) กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง	**หลัก:** สกมช. **รอง:** หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ สพร. สพธอ. กพ. สคช. สดช. สอศ. สพฐ. อว. ดศ. สทป. บก.ทท. บีโอไอ

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
๔. โครงการให้ความรู้ประชาชนเกี่ยวกับกฎหมาย กฎระเบียบ ความเสี่ยงของอาชญากรรมไซเบอร์ และมาตรการป้องกัน	๑) พิจารณากฎหมาย กฎระเบียบ ความเสี่ยงของอาชญากรรมไซเบอร์ และมาตรการป้องกันแต่ละปีที่จะให้ความรู้กับประชาชน ๒) จัดทำ ปรับปรุง หรือสร้างแนวทางในการให้ความรู้ประชาชนเกี่ยวกับกฎหมาย กฎระเบียบ ความเสี่ยงของอาชญากรรมไซเบอร์ และมาตรการป้องกัน ๓) เผยแพร่ประชาสัมพันธ์ และให้ความรู้ความเข้าใจในการปฏิบัติ ๔) กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง	**หลัก:** สกมช. **รอง:** หน่วยงานควบคุมหรือกำกับดูแลและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ตร. สพร. สพธอ. สำนักงาน ก.พ. สคช. สดช. สอศ. สพฐ. อว. ดศ.
๕.โครงการฝึกซ้อมเพื่อการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามไซเบอร์ของประเทศ กิจกรรมการจัดการฝึกและทดสอบแผนเผชิญเหตุ ในกรณีเกิดเหตุภัยคุกคามทางไซเบอร์ในระดับวิกฤติในประเทศ	๑) จัดการประชุมวางแผนการฝึก (Exercise planning) ๒) จัดการประชุมเพื่อจัดทำสถานการณ์และโจทย์ฝึก (Exercise Development) ๓) จัดการฝึกเตรียมการ (Pre-exercise/Academic) ๔) จัดการฝึกเพื่อทดสอบขีดความสามารถทางไซเบอร์ในรูปแบบการฝึกฝ่ายเสนาธิการ (Staff Exercise : Staff-Ex) หรือ การฝึกปัญหาที่บังคับการ (Command Post Exercise : CPX) หรือการฝึกภาคสนาม (Field Training Exercise : FTX) ๕) จัดทำรายงานสรุปผลการฝึก	**หลัก:** สกมช. **รอง:** หน่วยงานควบคุมหรือกำกับดูแลและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

กลยุทธ์ที่ ๑.๓ ส่งเสริมการวิจัยและพัฒนาและนวัตกรรมด้านความมั่นคงปลอดภัยไซเบอร์

๑. ส่งเสริมการศึกษา วิจัย พัฒนาและสร้างนวัตกรรมด้านความมั่นคงปลอดภัยไซเบอร์

๒. ส่งเสริมความร่วมมือด้านวิจัยและพัฒนา ระหว่างหน่วยงานวิจัยในประเทศและต่างประเทศ

๓. ส่งเสริมการลงทุนด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๔. ส่งเสริมการพัฒนาผลิตภัณฑ์ด้านความมั่นคงปลอดภัยไซเบอร์ให้เป็นนวัตกรรม และสามารถต่อยอดเชิงพาณิชย์ได้

ตัวชี้วัดของกลยุทธ์

๑. มีการศึกษา วิจัย พัฒนาและสร้างนวัตกรรมด้านความมั่นคงปลอดภัยไซเบอร์ ปีละไม่น้อยกว่า ๑ ฉบับ

๒. มีความร่วมมือด้านวิจัยและพัฒนา ระหว่างหน่วยงานวิจัยในประเทศและต่างประเทศ อย่างน้อย ๑๐ หน่วยงาน

๓. มีการลงทุนด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ของจำนวนหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศไม่น้อยกว่าร้อยละ ๕๐

๔. มีผลิตภัณฑ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่เป็นนวัตกรรมสามารถต่อยอดเชิงพาณิชย์ได้

โครงการขับเคลื่อนกลยุทธ์

๑. โครงการส่งเสริมและสนับสนุน ให้ทุน และจัดทำแพลตฟอร์มการวิจัยและพัฒนา นวัตกรรม วิทยาศาสตร์และเทคโนโลยีการรักษาความมั่นคงปลอดภัยไซเบอร์

๒. โครงการส่งเสริมและสนับสนุนการพัฒนาธุรกิจ โซลูชัน และผลิตภัณฑ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่เป็นนวัตกรรมในประเทศ

๓. โครงการจัดตั้งสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ กิจกรรมการจัดตั้งห้องปฏิบัติการความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Lab)

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
๑. โครงการส่งเสริมและสนับสนุน ให้ทุน และจัดทำแพลต - ฟอร์มการวิจัยและพัฒนา นวัตกรรม วิทยาศาสตร์และเทคโนโลยีการรักษาความมั่นคงปลอดภัยไซเบอร์	๑) จัดตั้งศูนย์แห่งความเป็นเลิศ (Centers of excellence) หรือศูนย์วิจัยความมั่นคงปลอดภัยไซเบอร์ ๒) มีการเผยแพร่สมุดปกขาว บอกทิศทางและแนวทางในการวิจัยและพัฒนาด้านความมั่นคงปลอดภัยของประเทศเป็นรายปี และใช้กำหนดทิศทางในการพัฒนาและให้ทุนสนับสนุน ๓) ส่งเสริมการทำงานร่วมกัน (Collaboration) รูปแบบการระดมทุน ๔) พัฒนาฟอรัมหรือแพลตฟอร์มการวิจัยและพัฒนาสำหรับความร่วมมือระหว่างภาครัฐและเอกชน ๕) เผยแพร่กลยุทธ์วิทยาศาสตร์และเทคโนโลยีไซเบอร์ ๖) ให้ทุนและสนับสนุนการวิจัยวิทยาศาสตร์และเทคโนโลยีไซเบอร์ ๗) สนับสนุนประชาชนชาวไทย นักศึกษา นักวิจัย เพื่อเพิ่มจำนวนชาวไทยที่มีความเชี่ยวชาญด้านไซเบอร์	**หลัก:** สกมช. **รอง:** หน่วยงานควบคุมหรือกำกับดูแลและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ สพร. สพธอ. สำนักงาน ก.พ. สดช. สอศ. สพฐ. อว. ดศ. สทป. บก.ทท. บีโอไอ

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
	๘) สนับสนุนงบประมาณในการวิจัยการระบุและจัดหาโซลูชั่นที่เป็นนวัตกรรมสำหรับปัญหาเร่งด่วนที่สุดบางประการในด้านความมั่นคงปลอดภัยไซเบอร์ ๙) สนับสนุนการมีส่วนร่วม โดยอาจพิจารณาสิทธิพิเศษทางภาษี และมาตรการส่งเสริมต่าง ๆ เพื่อเพิ่มจำนวนของหน่วยงานสนับสนุน ๑๐)กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง	
๒. โครงการส่งเสริมและสนับสนุนการพัฒนาธุรกิจ โซลูชันและผลิตภัณฑ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่เป็นนวัตกรรมในประเทศ	๑) จัดทำนโยบายและแนวทางในการส่งเสริมการพัฒนาธุรกิจ โซลูชัน และผลิตภัณฑ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่เป็นนวัตกรรมในประเทศ ๒) ให้ความรู้และความร่วมมือกับสตาร์ทอัพด้านความมั่นคงปลอดภัยไซเบอร์ในประเทศไทย โดยร่วมมือกับนักวิจัย มหาวิทยาลัย บริษัทชั้นนำทั้งในและต่างประเทศ ๓) สร้างแบรนด์และความน่าเชื่อถือของโซลูชันและผลิตภัณฑ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่เป็นนวัตกรรมในประเทศ ๔) ส่งเสริมการใช้โซลูชันและผลิตภัณฑ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่เป็นนวัตกรรมในประเทศ โดยให้สิทธิพิเศษและการสนับสนุนในด้านต่าง ๆ ๕) สนับสนุนการมีส่วนร่วม โดยอาจพิจารณาสิทธิพิเศษทางภาษี และมาตรการส่งเสริมต่าง ๆ เพื่อเพิ่มจำนวนของหน่วยงานสนับสนุน ๖) กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง	**หลัก:** สกมช. **รอง:** หน่วยงานควบคุมหรือกำกับดูแลและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ สพร. สพธอ. สำนักงาน ก.พ. สคช. สดช. สอศ. สพฐ. อว. ดศ. สทป. บก.ทท. บีโอไอ
๓. โครงการจัดตั้งสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ กิจกรรมการจัดตั้งห้องปฏิบัติการความมั่นคงปลอดภัย	๑) จัดทำกรอบแนวคิดในการดำเนินงาน และแผนการดำเนินงานในโครงการฯ พร้อมทั้งอธิบายรายละเอียด ระยะเวลา และผู้รับผิดชอบในโครงการ ๒) จัดซื้อเครื่องมือเพิ่มเติม และติดตั้งประจำศูนย์ NCSA ๓) ทดสอบการใช้งานระบบ และปรับแต่งให้ตรงกับความต้องการ ๔) จัดอบรมเกี่ยวกับการใช้งานให้กับเจ้าหน้าที่ที่เกี่ยวข้องให้ใช้เครื่องมือได้อย่างมีประสิทธิภาพมากขึ้น ๕) ทดสอบวิธีการเจาะระบบ (Penetration Test)	**หลัก:** สกมช. **รอง:** หน่วยงานควบคุมหรือกำกับดูแลและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
ไซเบอร์ (Cyber Security Lab)	กลุ่มเป้าหมาย ไม่น้อยกว่า ๑๕ หน่วยงาน เพื่อรายงานช่องโหว่ให้กับหน่วยงานรับทราบและดำเนินการป้องกัน และทำการตรวจพิสูจน์หลักฐานทางดิจิทัล ให้กับหน่วยงานที่ได้รับการโจมตีทางไซเบอร์ ไม่น้อยกว่า ๑๐ หน่วยงาน	

๓.๒.๒ ยุทธศาสตร์ที่ ๒ : บูรณาการความร่วมมือเพื่อเตรียมความพร้อมในการรับมือทางไซเบอร์และฟื้นคืนสู่สภาพปกติได้ (Partnership)

วัตถุประสงค์

เพื่อบูรณาการความร่วมมือในการเตรียมความพร้อมสำหรับการรับมือภัยคุกคามทางไซเบอร์ และการฟื้นคืนบริการที่สำคัญสู่สภาพปกติได้อย่างรวดเร็วกับทุกภาคส่วนทั้งภายในประเทศและระหว่างประเทศ

เป้าหมาย

๑. มีการประสานความร่วมมือทั้งภาครัฐและภาคเอกชนภายในประเทศเพื่อเตรียมความพร้อมในการรับมือกับภัยคุกคามทางไซเบอร์และการฟื้นคืนสู่สภาพปกติ

๒. มีการประสานความร่วมมือระหว่างประเทศ เพื่อเตรียมความพร้อมในการรับมือกับภัยคุกคามทางไซเบอร์และการฟื้นคืนสู่สภาพปกติ

กลยุทธ์ที่ ๒.๑ ส่งเสริมและสนับสนุนความร่วมมือระหว่างภาครัฐและภาคเอกชน

๑. ระบุถึงการมีส่วนร่วมของผู้มีส่วนได้ส่วนเสีย เพื่อสร้างความร่วมมือระหว่างหน่วยงานภาครัฐและภาคเอกชน

๒. กำหนดโครงสร้างการกำกับดูแลที่ชัดเจน และกำหนดกลไกที่ทำหน้าที่สร้างความร่วมมือและประสานงานระหว่างหน่วยงานภาครัฐ และภาคเอกชน

๓. สร้างความร่วมมือระหว่างหน่วยงานภาครัฐ

๔. รักษาสมดุลระหว่างความมั่นคงปลอดภัยทางไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคล

๕. สนับสนุนการพัฒนาศักยภาพบุคลากรภาครัฐที่เกี่ยวข้องกับการบังคับใช้กฎหมายด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

ตัวชี้วัดของกลยุทธ์

๑. มีกิจกรรมเพื่อสร้างความร่วมมือระหว่างหน่วยงานภาครัฐ ภาคเอกชน ปีละไม่น้อยกว่า ๓ กิจกรรม

๒. มีโครงสร้างการกำกับดูแลที่ชัดเจน มีกลไกความร่วมมือและประสานงานระหว่างหน่วยงานภาครัฐ ระหว่างภาครัฐและภาคเอกชน และระหว่างภาคเอกชน

๓. มีความร่วมมือระหว่างหน่วยงานภาครัฐ ปีละไม่น้อยกว่า ๓ กิจกรรม

๔. มีแนวทางความร่วมมือระหว่างหน่วยงานความมั่นคงปลอดภัยทางไซเบอร์และหน่วยงานการคุ้มครองข้อมูลส่วนบุคคล

๕. บุคลากรภาครัฐที่เกี่ยวข้องกับการบังคับใช้กฎหมายด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ได้รับการพัฒนาศักยภาพ ปีละไม่น้อยกว่า ๑ ครั้ง

โครงการขับเคลื่อนกลยุทธ์

๑. โครงการส่งเสริมและสนับสนุนความร่วมมือระหว่างภาครัฐและเอกชนเพื่อระบุและตอบสนองต่อปัญหาที่เกี่ยวข้องกับอาชญากรรมไซเบอร์ได้อย่างรวดเร็ว

๒. โครงการประสานหน่วยงานภาคธุรกิจ มุ่งเน้นไปที่ชุมชนธุรกิจ เพื่อรวมความมั่นคงปลอดภัยไซเบอร์เข้ากับการจัดการความเสี่ยงขององค์กร

๓. โครงการสนับสนุนการสร้างขีดความสามารถด้านอาชญากรรมไซเบอร์ในระดับชาติ (เช่น กรอบการดำเนินการร่วมกันในการต่อต้านอาชญากรรมไซเบอร์เฉพาะทาง การดำเนินการร่วมกันระหว่างเจ้าหน้าที่ฝ่ายต่าง ๆ เช่น ตำรวจ และเจ้าหน้าที่ฝ่ายตุลาการ ผู้เชี่ยวชาญนิติวิทยาศาสตร์)

๔. โครงการการเป็นพันธมิตรกับหน่วยงานคุ้มครองข้อมูลส่วนบุคคล สำหรับการจัดแนวทางการปฏิบัติตามข้อกำหนดด้านความมั่นคงปลอดภัยและการปฏิบัติตามข้อกำหนดในการปกป้องข้อมูลส่วนบุคคล

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
๑. โครงการส่งเสริมและสนับสนุนความร่วมมือระหว่างภาครัฐและเอกชนเพื่อระบุและตอบสนองต่อปัญหาที่เกี่ยวข้องกับอาชญากรรมไซเบอร์ได้อย่างรวดเร็ว	๑) ส่งเสริมและสนับสนุนการกำหนดกรอบความร่วมมือระหว่างภาครัฐและเอกชนและความร่วมมือระหว่างประเทศเพื่อระบุและตอบสนองต่อปัญหาที่เกี่ยวข้องกับอาชญากรรมไซเบอร์ได้อย่างรวดเร็ว ๒) จัดทำแนวทางตามกรอบการปฏิบัติการ ๓) เผยแพร่ประชาสัมพันธ์ และให้ความรู้ความเข้าใจในการปฏิบัติ ๔) จัดให้เจ้าหน้าที่ของรัฐมีทักษะที่เกี่ยวข้อง ๕) กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง	**หลัก:** สกมช. **รอง:** สพร. สพธอ. ตร. หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
๒. โครงการประสานหน่วยงานภาคธุรกิจ มุ่งเน้นไปที่ชุมชนธุรกิจ เพื่อรวมความมั่นคงปลอดภัยไซเบอร์ เข้ากับการจัดการความเสี่ยงขององค์กร	๑) กำหนดแนวทางในการสร้างความร่วมมือกับชุมชนธุรกิจ เพื่อรวมความปลอดภัยทางไซเบอร์เข้ากับการจัดการความเสี่ยงขององค์กร ๒) จัดทำหรือปรับปรุงกฎหมาย กฎระเบียบที่เกี่ยวข้อง ๓) สนับสนุน เผยแพร่ประชาสัมพันธ์ และให้ความรู้ความเข้าใจในการปฏิบัติ ๔) จัดให้เจ้าหน้าที่ของรัฐมีทักษะที่เกี่ยวข้อง	**หลัก:** สกมช. **รอง:** สพร. สพธอ. ดศ. สดช. สศด. หน่วยงานควบคุมหรือกำกับดูแล

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
	๕) กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง	และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
๓. โครงการสนับสนุนการสร้างขีดความสามารถด้านอาชญากรรมไซเบอร์ในระดับชาติ (เช่น กรอบการดำเนินการร่วมกันในการต่อต้านอาชญากรรมไซเบอร์เฉพาะทาง พัฒนาการฝึกอบรมเฉพาะสำหรับการดำเนินการร่วมกันระหว่างเจ้าหน้าที่ฝ่ายต่าง ๆ เช่น ตำรวจและเจ้าหน้าที่ฝ่ายตุลาการ ผู้เชี่ยวชาญนิติวิทยาศาสตร์)	๑) กำหนดกรอบการดำเนินการร่วมกันในการต่อต้านอาชญากรรมไซเบอร์เฉพาะทาง พัฒนาการฝึกอบรมเฉพาะสำหรับการดำเนินการร่วมกันระหว่างเจ้าหน้าที่ฝ่ายต่าง ๆ ๒) จัดทำแนวทางตามกรอบการปฏิบัติการ ๓) เผยแพร่ประชาสัมพันธ์ และให้ความรู้ความเข้าใจในการปฏิบัติ ๔) จัดให้เจ้าหน้าที่ของรัฐมีทักษะที่เกี่ยวข้อง ๕) กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง	**หลัก:** สกมช. **รอง:** สพร. สพธอ. ตร. สำนักงานอัยการสูงสุด (อส.) หน่วยงานควบคุมหรือกำกับดูแล ยธ. กห. บก. ทท.
๔. โครงการการเป็นพันธมิตรกับหน่วยงานคุ้มครองข้อมูลส่วนบุคคล สำหรับการจัดแนวทางการปฏิบัติตามข้อกำหนดด้านความมั่นคงปลอดภัยและการปฏิบัติตามข้อกำหนดในการปกป้องข้อมูลส่วนบุคคล	๑) จัดทำกรอบในการทำงานร่วมกันกับหน่วยงานคุ้มครองข้อมูลส่วนบุคคลสำหรับการจัดแนวทางการปฏิบัติตามข้อกำหนดด้านความมั่นคงปลอดภัยและการปฏิบัติตามข้อกำหนดในการปกป้องข้อมูลส่วนบุคคล ๒) จัดทำหรือปรับปรุงกฎหมาย กฎระเบียบที่เกี่ยวข้อง ๓) สนับสนุน เผยแพร่ประชาสัมพันธ์ และให้ความรู้ความเข้าใจในการปฏิบัติ ๔) จัดให้เจ้าหน้าที่ของรัฐมีทักษะที่เกี่ยวข้อง ๕) กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง	**หลัก:** สกมช. **รอง:** สพร. สพธอ. ดศ. หน่วยงานควบคุมหรือกำกับดูแลคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

กลยุทธ์ที่ ๒.๒ ประสานความร่วมมือระหว่างประเทศเพื่อรับมือภัยคุกคาม

๑. กำหนดให้การรักษาความมั่นคงปลอดภัยไซเบอร์เป็นประเด็นสำคัญในการกำหนดนโยบายด้านการต่างประเทศ

๒. มีส่วนร่วมในเวทีการประชุมระหว่างประเทศด้านความมั่นคงปลอดภัยไซเบอร์

๓. สร้างความร่วมมือด้านความมั่นคงปลอดภัยไซเบอร์ระหว่างประเทศในทุกมิติ

๔. พัฒนายุทธศาสตร์ของประเทศให้สอดคล้องตามแนวปฏิบัติสากล

๕. สนับสนุนการพัฒนาศักยภาพบุคลากรภาครัฐที่เกี่ยวข้องกับการบังคับใช้กฎหมายระหว่างประเทศด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และกฎหมายอื่นที่เกี่ยวข้อง เพื่อให้สามารถปฏิบัติงานร่วมกับหน่วยงานที่เกี่ยวข้องในระดับนานาชาติได้อย่างมีประสิทธิภาพ

ตัวชี้วัดของกลยุทธ์

๑. มีการกำหนดให้การรักษาความมั่นคงปลอดภัยไซเบอร์เป็นนโยบายด้านการต่างประเทศ

๒. มีการเข้าร่วมประชุมระหว่างประเทศด้านความมั่นคงปลอดภัยไซเบอร์ในทุกกรอบความร่วมมือระหว่างประเทศ

๓. มีความร่วมมือด้านความมั่นคงปลอดภัยไซเบอร์ระหว่างประเทศในทุกมิติ อาทิ การบังคับใช้กฎหมาย การแลกเปลี่ยนข้อมูลภัยคุกคามไซเบอร์ เป็นต้น

๔. มีการพัฒนายุทธศาสตร์ของประเทศให้สอดคล้องตามแนวปฏิบัติสากล

๕. มีกิจกรรมเพื่อพัฒนาศักยภาพบุคลากรภาครัฐที่เกี่ยวข้องกับการบังคับใช้กฎหมายระหว่างประเทศด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และกฎหมายอื่นที่เกี่ยวข้อง ได้รับการพัฒนาศักยภาพ เพื่อให้สามารถปฏิบัติงานร่วมกับหน่วยงานที่เกี่ยวข้องในระดับนานาชาติได้อย่างมีประสิทธิภาพ ปีละไม่น้อยกว่า ๑ ครั้ง

โครงการขับเคลื่อนกลยุทธ์

๑. โครงการสนับสนุนการสร้างขีดความสามารถด้านอาชญากรรมไซเบอร์ในระดับนานาชาติ

๒. โครงการส่งเสริมและสนับสนุนการแลกเปลี่ยนด้าน Cyber Norms และกฎหมายที่เกี่ยวข้อง

๓. โครงการส่งเสริมและสนับสนุนความร่วมมือและเข้าร่วมโครงการสำคัญในระดับ ASEAN และนานาชาติ เพื่อสร้างศักยภาพด้านไซเบอร์

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
๑. โครงการสนับสนุนการสร้างขีดความสามารถด้านอาชญากรรมไซเบอร์ในระดับนานาชาติ	๑) ส่งเสริมและสนับสนุนการกำหนดกรอบการดำเนินการร่วมกันในการต่อต้านอาชญากรรมไซเบอร์เฉพาะทาง พัฒนาการฝึกอบรมเฉพาะสำหรับการดำเนินการร่วมกันระหว่างเจ้าหน้าที่ฝ่ายต่าง ๆ ในระดับนานาชาติ ๒) จัดทำแนวทางตามกรอบการปฏิบัติการ	**หลัก:** สกมช. **รอง:** สพร. สพธอ. ตร. กต.

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
	๓) เผยแพร่ประชาสัมพันธ์ และให้ความรู้ความเข้าใจในการปฏิบัติ ๔) จัดให้เจ้าหน้าที่ของรัฐมีทักษะที่เกี่ยวข้อง ๕) กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง	หน่วยงานควบคุมหรือกำกับดูแลและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
๒. โครงการส่งเสริมและสนับสนุนการแลกเปลี่ยนด้าน Cyber Norms และกฎหมายที่เกี่ยวข้อง	๑) กำหนดกรอบสนับสนุนการแลกเปลี่ยนด้าน Cyber Norms และกฎหมายที่เกี่ยวข้อง ๒) จัดทำแนวทางสนับสนุนการแลกเปลี่ยนด้าน Cyber Norms และกฎหมายที่เกี่ยวข้อง ๓) เผยแพร่ประชาสัมพันธ์ และให้ความรู้ความเข้าใจในการปฏิบัติ ๔) จัดให้เจ้าหน้าที่ของรัฐมีทักษะที่เกี่ยวข้อง ๕) กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง	**หลัก:** สกมช. **รอง:** สพร. สพธอ. กต. หน่วยงานควบคุมหรือกำกับดูแลและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
๓. โครงการส่งเสริมและสนับสนุนความร่วมมือและเข้าร่วมโครงการสำคัญในระดับ ASEAN และนานาชาติเพื่อสร้างศักยภาพด้านไซเบอร์	๑) กำหนดกรอบส่งเสริมความร่วมมือและเข้าร่วมโครงการสำคัญในระดับ ASEAN และนานาชาติเพื่อสร้างศักยภาพด้านไซเบอร์ ๒) จัดทำแนวทางส่งเสริมความร่วมมือและเข้าร่วมโครงการสำคัญในระดับ ASEAN และนานาชาติเพื่อสร้างศักยภาพด้านไซเบอร์ ๓) เผยแพร่ประชาสัมพันธ์ และให้ความรู้ความเข้าใจในการปฏิบัติ ๔) จัดให้เจ้าหน้าที่ของรัฐมีทักษะที่เกี่ยวข้อง ๕) กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง	**หลัก:** สกมช. **รอง:** สพร. สพธอ. กต. หน่วยงานควบคุมหรือกำกับดูแลและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๓.๒.๓ ยุทธศาสตร์ที่ ๓ : สร้างบริการภาครัฐ และโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้มีความมั่นคงปลอดภัยไซเบอร์และฟื้นคืนสู่สภาพปกติได้ (Resilience)

วัตถุประสงค์

เพื่อส่งเสริมบริการภาครัฐและโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้มีความมั่นคงปลอดภัยไซเบอร์ และสามารถฟื้นคืนบริการที่สำคัญสู่สภาพปกติได้

เป้าหมาย

๑. มีการกำหนดโครงสร้างการกำกับดูแลและกรอบกฎหมายสำหรับหน่วยงานภาครัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๒. มีการกำหนดมาตรการการรักษาความมั่นคงปลอดภัยขั้นต่ำสำหรับหน่วยงานภาครัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๓. มีการปกป้องระบบข้อมูลและเครือข่ายของหน่วยงานภาครัฐ

กลยุทธ์ที่ ๓.๑ กำหนดมาตรการการรักษาความมั่นคงปลอดภัยขั้นต่ำสำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure : CII)

๑. ปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยระบุถึงประเภทของโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และกำหนดมาตรการลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

๒. กำหนดหลักเกณฑ์การรักษาความมั่นคงปลอดภัยไซเบอร์ขั้นต่ำ

๓. ส่งเสริมและสนับสนุนหลักการออกแบบระบบอย่างมั่นคงปลอดภัย (Security By Design)

๔. ส่งเสริมและสนับสนุนให้บุคลากรทุกระดับมีความตระหนักรู้ในการรักษาความมั่นคงปลอดภัยไซเบอร์

ตัวชี้วัดของกลยุทธ์

๑. มีการปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และกำหนดมาตรการลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ครบทุกด้านตามประกาศของ สกมช.

๒. มีการกำหนดหลักเกณฑ์การรักษาความมั่นคงปลอดภัยไซเบอร์ขั้นต่ำสำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure : CII)

๓. มีการส่งเสริมและสนับสนุนหลักการออกแบบระบบอย่างมั่นคงปลอดภัย (Security By Design) สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure : CII)

๔. มีการส่งเสริมให้บุคลากรทุกระดับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure : CII) มีความตระหนักรู้ในการรักษาความมั่นคงปลอดภัยไซเบอร์ ไม่น้อยกว่าร้อยละ ๘๐

โครงการขับเคลื่อนกลยุทธ์

๑. โครงการพัฒนาหลักปฏิบัติ (Code of practices) และจรรยาบรรณ (Code of conduct) ที่เป็นมาตรฐานและขั้นตอนการตรวจสอบและติดตามการปฏิบัติตาม (Compliance)

๒. โครงการส่งเสริมและสนับสนุนหลักการออกแบบระบบอย่างมั่นคงปลอดภัย (Security By Design)

๓. โครงการส่งเสริมและสนับสนุนการสร้างความตระหนักรู้โดยเฉพาะที่กำหนดเป้าหมาย CII (ผู้บริหารสูงสุด และพนักงาน)

๔. โครงการขับเคลื่อนแผน ยุทธศาสตร์ นโยบายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ กิจกรรมพัฒนาขีดความสามารถ กระบวนการปฏิบัติงานด้านไซเบอร์ตามมาตรฐานสากลของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
๑. โครงการพัฒนาหลักปฏิบัติ (Code of practices) และ จรรยาบรรณ (Code of conduct) นโยบายและแนวทางที่เป็นมาตรฐานและขั้นตอนการตรวจสอบและติดตามการปฏิบัติตาม (Compliance)	๑) จัดทำพัฒนาหลักปฏิบัติ (Code of practices) และจรรยาบรรณ (Code of conduct) นโยบายและแนวทาง (Policies and Guideline) ที่เป็นมาตรฐานและขั้นตอนการตรวจสอบและติดตามการปฏิบัติตาม (Compliance) ๒) ส่วนของ Policies and Guideline ควรมีการสร้างความร่วมมือกับหน่วยงานด้านมาตรฐาน เช่น ISO หรือ NIST รวมถึงหน่วยงานภายใน เช่น ETDA เพื่อให้นโยบายและแนวปฏิบัติ มีความน่าเชื่อถือและไม่เกิดความสับสนต่อผู้ปฏิบัติ (CII) ๓) กำหนดแนวทางการใช้งานหลักปฏิบัติในแต่ละภาคส่วน ๔) ช่วยเหลือสำหรับธุรกิจในการปฏิบัติตาม ๕) กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง	**หลัก:** สกมช. **รอง:** สพร. สพธอ. หน่วยงานควบคุมหรือกำกับดูแลและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
๒. โครงการส่งเสริมและสนับสนุนหลักการออกแบบระบบอย่างมั่นคงปลอดภัย (Security By Design)	๑) จัดทำหลักการออกแบบระบบอย่างมั่นคงปลอดภัย (Security By Design) ๒) กำหนดระเบียบข้อบังคับ นโยบายและแนวทางที่เกี่ยวข้อง ๓) เผยแพร่ประชาสัมพันธ์ และให้ความรู้ความเข้าใจในการปฏิบัติ ๔) กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง	**หลัก:** สกมช. **รอง:** สพร. สพธอ. หน่วยงานควบคุมหรือกำกับดูแลและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
๓. โครงการส่งเสริมและสนับสนุนการสร้างความตระหนักรู้โดยเฉพาะที่กำหนดเป้าหมาย CII (ผู้บริหารสูงสุดและพนักงาน)	๑) จัดทำกรอบโปรแกรมการสร้างความตระหนักรู้โดยเฉพาะที่กำหนดเป้าหมาย CII (ผู้บริหารสูงสุดและพนักงาน) ๒) กำหนดระเบียบข้อบังคับ นโยบายและแนวทางที่เกี่ยวข้อง โดยกำหนดให้เป็นส่วนหนึ่งของภาระหน้าที่ในการปฏิบัติ การเลื่อนตำแหน่ง ๓) เผยแพร่ประชาสัมพันธ์ ๔) กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง	**หลัก:** สกมช. **รอง:** สพร. สพธอ. ก.พ. หน่วยงานควบคุมหรือกำกับดูแลและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
๔. โครงการขับเคลื่อนแผนยุทธศาสตร์นโยบายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์	๑) ศึกษาเพื่อทบทวนหลักสูตรเพื่อการพัฒนาขีดความสามารถกระบวนการปฏิบัติงานด้านไซเบอร์ตามมาตรฐานสากล ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ จำนวน 2 หลักสูตร ประกอบด้วย หลักสูตรผู้นำการปฏิบัติ (Lead	**หลัก:** สกมช. **รอง:** หน่วยงานควบคุมหรือกำกับดูแลและหน่วยงานโครงสร้างพื้นฐาน

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
กิจกรรมพัฒนาขีดความสามารถกระบวนการปฏิบัติงานด้านไซเบอร์ตามมาตรฐานสากลของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ	Implementor) และหลักสูตรผู้นำตรวจสอบ (Lead Auditor) ๒) จัดประชุมรับฟังความคิดเห็นจากผู้ที่มีส่วนเกี่ยวข้อง (Focus Group) เนื้อหาหลักสูตรผู้นำการปฏิบัติ (Lead Implementor) และหลักสูตรผู้นำตรวจสอบ (Lead Auditor) ๓) จัดประชุมประชาพิจารณ์ต่อ เนื้อหาหลักสูตรผู้นำการปฏิบัติ (Lead Implementor) และหลักสูตรผู้นำตรวจสอบ (Lead Auditor) ๔) จัดอบรมเชิงปฏิบัติการหลักสูตรผู้นำการปฏิบัติ (Lead Implementor) และหลักสูตรผู้นำตรวจสอบ(Lead Auditor) ๕) จัดทำเว็บไซต์สำหรับการสอนหลักสูตรผู้นำการปฏิบัติ (Lead Implementor) และหลักสูตรผู้นำตรวจสอบ (Lead Auditor)ผ่านระบบออนไลน์	สำคัญทางสารสนเทศ

กลยุทธ์ที่ ๓.๒ กำหนดโครงสร้างการกำกับดูแลและกรอบกฎหมายสำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๑. กำหนดวิธีการบริหารจัดการความเสี่ยงเพื่อปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๒. พัฒนากลไกแนวทางการกำกับดูแลของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และพิจารณากำหนดให้ ข้อมูลและบริการคลาวด์ (Data & Cloud Computing) เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่ต้องมีการกำกับดูแลในระยะต่อไป

๓. พัฒนากฎหมาย กฎระเบียบที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ให้ทันสมัย

ตัวชี้วัดของกลยุทธ์

๑. มีวิธีการบริหารจัดการความเสี่ยงเพื่อปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๒. มีกลไกและแนวทางการกำกับดูแลของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๓. มีกฎหมาย กฎระเบียบที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ทันสมัย

โครงการขับเคลื่อนกลยุทธ์

๑. โครงการกฎระเบียบและข้อบังคับที่สนับสนุนทำให้เกิดความมั่นคงปลอดภัยไซเบอร์

๒. โครงการพัฒนากรอบการทำงานที่ถูกต้องตามกฎหมายสำหรับ CII (แนวทางและการควบคุมกำกับดูแล)

๓. โครงการพัฒนากลไกในการบูรณาการเหตุการณ์ความเสี่ยงทางไซเบอร์ สถานะการดำเนินการของผู้ดำเนินการ CII และกฎหมาย/แนวโน้มระหว่างประเทศเพื่อปรับปรุงแก้ไขหรือเกิดผลทางกฎหมายเพิ่มเติมอย่างทันท่วงที

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
๑. โครงการกฎระเบียบและข้อบังคับที่สนับสนุนทำให้เกิดความมั่นคงปลอดภัยไซเบอร์	๑) การทบทวนกฎระเบียบและข้อบังคับที่สนับสนุนความมั่นคงปลอดภัยไซเบอร์ เช่น การปฏิบัติงานระหว่างหน่วยงาน ขอบเขตอำนาจหน้าที่และการประสานงาน การแบ่งปันข้อมูลข่าวสาร การรักษาความลับและข้อมูลส่วนบุคคล การคุ้มครองการปฏิบัติงานของเจ้าหน้าที่ การเก็บรวบรวม การใช้ และดูแลรักษาหลักฐานดิจิทัลที่ใช้ในชั้นศาล เป็นต้น ๒) จัดทำหรือปรับปรุงระเบียบและข้อบังคับที่สนับสนุนความมั่นคงปลอดภัยไซเบอร์ ๓) เผยแพร่ประชาสัมพันธ์ และให้ความรู้ความเข้าใจในการปฏิบัติ ๔) กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง	**หลัก:** สกมช. **รอง:** ยธ. สพร. สพธอ. หน่วยงานควบคุมหรือกำกับดูแล
๒. โครงการพัฒนากรอบการทำงานที่ถูกต้องตามกฎหมายสำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (แนวทาง และการควบคุมกำกับดูแล)	๑) กำหนดแนวทางการบริหารจัดการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหลักการควบคุมหรือกำกับดูแล (Governance) และการบริหารจัดการความเสี่ยง ๒) พัฒนารูปแบบการกำกับดูแลของภาครัฐและภาระความรับผิดชอบ (Adopt a governance model with clear responsibilities) ของหน่วยงานภาครัฐและผู้มีส่วนเกี่ยวข้องในการปกป้องคุ้มครองโครงสร้างพื้นฐานสำคัญ (Critical infrastructures: CIs) และโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CIIs) ๓) กำหนดระเบียบข้อบังคับที่เกี่ยวข้อง ๔) การสนับสนุนการร่วมลงทุนระหว่างภาครัฐและภาคเอกชน (Establish public-private partnerships) การสร้างแรงจูงใจในทุกภาคส่วน (Utilize a wide range of market levers)	**หลัก:** สกมช. **รอง:** สพร. สพธอ. หน่วยงานควบคุมหรือกำกับดูแล

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
	๕) เผยแพร่ประชาสัมพันธ์ และให้ความรู้ความเข้าใจในการปฏิบัติ ๖) กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง	
๓. โครงการพัฒนากลไกในการบูรณาการเหตุการณ์ความเสี่ยงทางไซเบอร์ สถานะการดำเนิน การของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และกฎหมาย/แนวโน้มระหว่างประเทศเพื่อปรับปรุงแก้ไขหรือเกิดผลทางกฎหมายเพิ่มเติมอย่างทันท่วงที	๑) จัดทำกลไกในการบูรณาการเหตุการณ์ความเสี่ยงทางไซเบอร์ สถานะการดำเนินการของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และกฎหมาย/แนวโน้มระหว่างประเทศเพื่อปรับปรุงแก้ไขหรือเกิดผลทางกฎหมายเพิ่มเติมอย่างทันท่วงที ๒) กำหนดระเบียบข้อบังคับที่เกี่ยวข้อง ๓) เผยแพร่ประชาสัมพันธ์ และให้ความรู้ความเข้าใจในการปฏิบัติ ๔) กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง	**หลัก:** สกมช. **รอง:** ยธ. กต. สพร. สพธอ. หน่วยงานควบคุมหรือกำกับดูแล

กลยุทธ์ที่ ๓.๓ ปกป้องระบบข้อมูลและเครือข่ายของหน่วยงานภาครัฐ

๑. กำหนดให้หน่วยงานภาครัฐปฏิบัติตามนโยบายมาตรฐานการรักษาความมั่นคงปลอดภัยขั้นต่ำ

๒. กำหนดให้มีการประเมินความเสี่ยงจากการใช้เทคโนโลยีเพื่อให้เกิดความมั่นคงปลอดภัยตั้งแต่เริ่มต้นการใช้งาน

๓. กำหนดมุมมองการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ร่วมกัน

๔. เตรียมความพร้อมด้านบุคลากร ข้อมูล เทคโนโลยี และกระบวนการเพื่อรับมือภัยคุกคามไซเบอร์สมัยใหม่

ตัวชี้วัดของกลยุทธ์

๑. มีการกำหนดให้หน่วยงานภาครัฐปฏิบัติตามนโยบาย มาตรฐานการรักษา ความมั่นคงปลอดภัยขั้นต่ำ เพิ่มขึ้นปีละไม่น้อยกว่าร้อยละ ๑๐

๒. มีการกำหนดให้มีการประเมินความเสี่ยงจากการใช้เทคโนโลยีเพื่อให้เกิดความมั่นคงปลอดภัยตั้งแต่เริ่มต้นการใช้งาน เพิ่มขึ้นปีละไม่น้อยกว่าร้อยละ ๑๐

๓. มีกิจกรรมการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ร่วมกัน อย่างน้อยปีละไม่ต่ำกว่า ๑ ครั้ง

๔. มีกิจกรรมที่เกี่ยวกับการเตรียมความพร้อมด้านบุคลากร ข้อมูล เทคโนโลยี และกระบวนการเพื่อรับมือภัยคุกคามภัยไซเบอร์สมัยใหม่ ปีละไม่น้อยกว่า ๑ กิจกรรม

โครงการขับเคลื่อนกลยุทธ์

๑. โครงการส่งเสริมและสนับสนุนการนำเทคโนโลยีมาใช้เพื่อให้เกิดความมั่นคงปลอดภัยตั้งแต่เริ่มต้นการใช้งาน (Security by default)

๒. โครงการพัฒนาและบังคับใช้มาตรฐานการรักษาความมั่นคงปลอดภัยขั้นต่ำสำหรับบริการภาครัฐ (เช่น ข้อกำหนดมาตรฐานความมั่นคงปลอดภัยไซเบอร์ที่รวมอยู่ในสัญญาด้านเทคโนโลยีสารสนเทศของรัฐบาล)

๓. โครงการสร้างการจัดการแบบบองค์รวมของเครือข่ายที่ดำเนินการโดยหน่วยงานของรัฐ

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
๑. โครงการส่งเสริมและสนับสนุนการนำเทคโนโลยีมาใช้เพื่อให้เกิดความมั่นคงปลอดภัยตั้งแต่เริ่มต้นการใช้งาน (Security by default)	๑) จัดทำแนวปฏิบัติ "ความมั่นคงปลอดภัยตั้งแต่เริ่มต้นการใช้งาน (Security by default)" ๒) จัดทำมาตรการสนับสนุนให้ผู้ให้บริการฮาร์ดแวร์และซอฟต์แวร์ให้ปฏิบัติตามแนวทางปฏิบัติ "ความมั่นคงปลอดภัยตั้งแต่เริ่มต้นการใช้งาน (Security by default)" ๓) สำรวจวิธีกระตุ้นตลาดด้วยการให้คะแนนความมั่นคงปลอดภัยสำหรับผลิตภัณฑ์ใหม่ ๔) เผยแพร่ประชาสัมพันธ์ และให้ความรู้ความเข้าใจในการปฏิบัติ ๕) กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง	**หลัก:** สกมช. **รอง:** สพร. สพธอ. หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
๒. โครงการพัฒนาและบังคับใช้มาตรฐานการรักษาความมั่นคงปลอดภัยขั้นต่ำสำหรับบริการภาครัฐ (เช่น ข้อกำหนดมาตรฐาน	๑) จัดทำมาตรฐานการรักษาความมั่นคงปลอดภัยขั้นต่ำสำหรับบริการภาครัฐ เช่น ข้อกำหนดมาตรฐานความมั่นคงปลอดภัยไซเบอร์ที่รวมอยู่ในสัญญาด้านไอทีของรัฐบาล แนวทางและเกณฑ์ในการพิจารณาความเสี่ยงในการเลือกผู้ให้บริการ	**หลัก:** สกมช. **รอง:** สพร. สพธอ. หน่วยงานควบคุมหรือกำกับดูแล

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
ความมั่นคงปลอดภัยไซเบอร์ที่รวมอยู่ในสัญญาด้านไอทีของรัฐบาล)	และผลิตภัณฑ์, Backdoor Policy, การพิจารณาความเสี่ยงจาก Vendor Lock in ๒) กำหนดระเบียบข้อบังคับที่เกี่ยวข้อง ๓) เผยแพร่ประชาสัมพันธ์ และให้ความรู้ความเข้าใจในการปฏิบัติ ๔) กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง	
๓. โครงการสร้างการจัดการแบบองค์รวมของเครือข่ายที่ดำเนินการโดยหน่วยงานของรัฐ	๑) กำหนดกรอบการจัดการแบบองค์รวมของเครือข่ายที่ดำเนินการโดยหน่วยงานของรัฐ เช่น ให้มีหน่วยงานกลางที่รับผิดชอบของแต่ละกรม มีการเชื่อมโยงขอบเขต อำนาจหน้าที่ และการประสานงานระหว่างกรมไปยังกระทรวง และการเชื่อมโยงของแต่ละกระทรวง การดำเนินการโดยหน่วยงานกลางหรือการกระจายอำนาจ และประสานการทำงานร่วมกัน ๒) จัดทำแพลตฟอร์มการจัดการแบบองค์รวมของเครือข่ายที่ดำเนินการโดยหน่วยงานของรัฐ ๓) ปรับปรุงและสนับสนุนการเข้าถึงผู้เชี่ยวชาญด้านไซเบอร์ในหน่วยงานของรัฐ ๔) เผยแพร่ประชาสัมพันธ์ และให้ความรู้ความเข้าใจในการปฏิบัติ ๕) กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง	**หลัก:** สกมช. **รอง:** สพร. สพธอ. หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๓.๒.๔ ยุทธศาสตร์ที่ ๔ : สร้างศักยภาพของหน่วยงานระดับชาติให้มีคุณภาพและมาตรฐาน (Standard)

วัตถุประสงค์

มุ่งสร้างศักยภาพของหน่วยงานระดับชาติให้มีคุณภาพและมาตรฐาน เพื่อให้การบริหารจัดการด้านความมั่นคงปลอดภัยไซเบอร์เป็นไปอย่างมีประสิทธิภาพ

เป้าหมายและตัวชี้วัด

๑. มีการบริหารจัดการการรักษาความมั่นคงปลอดภัยไซเบอร์แบบบูรณาการในระดับชาติ

๒. มีหน่วยงานหลักและหน่วยงานรองที่มีคุณภาพและมาตรฐาน สามารถทำงานร่วมกันแบบบูรณาการได้

๓. มีมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

๔. มีการแบ่งปันข้อมูลภัยคุกคามทางไซเบอร์อย่างมีประสิทธิภาพ

๕. หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศมีมาตรการการรักษาความมั่นคงปลอดภัยไซเบอร์ที่เข้มแข็ง

กลยุทธ์ที่ ๔.๑ เพิ่มขีดความสามารถในการรับมือและตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

๑. พิจารณาศึกษาและทบทวนนโยบาย กฎหมาย และขีดความสามารถด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีอยู่ในปัจจุบัน เพื่อกำหนดแนวทางการพัฒนาการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ

๒. กำหนดกลไกการขับเคลื่อนยุทธศาสตร์ กระบวนการตัดสินใจ การแบ่งหน้าที่ความรับผิดชอบ การประสานความร่วมมือกับหน่วยงานที่เกี่ยวข้อง แนวทางการดำเนินการและการติดตามประเมินผลการปฏิบัติงาน

๓. ส่งเสริมบุคลากร (People) กระบวนการ (Process) และเทคโนโลยี (Technology) ให้มีการพัฒนาศักยภาพ คุณภาพ และมาตรฐาน เพื่อสร้างความเชื่อมั่นให้กับผู้มีส่วนได้เสียและนำมาตรฐานและแนวปฏิบัติที่ดีมาใช้ในการปฏิบัติงาน โดยอาจดำเนินการเพื่อให้ได้รับใบรับรอง (Certification) และการรับรอง (Accreditation) ในส่วนของการปฏิบัติงานที่สำคัญ

๔. พัฒนาแผนรองรับสถานการณ์ฉุกเฉินด้านไซเบอร์ เพื่อใช้ในการรับมือและฟื้นฟูบริการโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยจัดตั้งทีมรับมือเหตุการณ์ด้านความมั่นคงปลอดภัยคอมพิวเตอร์ (Computer Security Incident Response Team: CSIRT) ตลอดจนการฝึกซ้อมแผนรับมือปัญหาความมั่นคงปลอดภัยไซเบอร์

ตัวชี้วัดของกลยุทธ์

๑. มีการทบทวนนโยบาย กฎหมาย และขีดความสามารถด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีอยู่ในปัจจุบัน เพื่อกำหนดแนวทางการพัฒนาการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ

๒. มีแนวทางการติดตามประเมินผลการปฏิบัติงาน

๓.ส่งเสริมให้มีการพัฒนาศักยภาพบุคลากร (People) กระบวนการ (Process) และเทคโนโลยี (Technology) ให้มีคุณภาพตามมาตรฐาน เพิ่มขึ้นปีละไม่น้อยกว่าร้อยละ ๑๐

๔. มีแผนเตรียมพร้อมด้านการรองรับสถานการณ์ฉุกเฉินด้านไซเบอร์เพื่อใช้ในการรับมือและฟื้นฟูบริการโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และมีการจัดตั้งทีมรับมือเหตุการณ์ด้านความมั่นคงปลอดภัยคอมพิวเตอร์ ตลอดจนการฝึกซ้อมแผนรับมือปัญหาความมั่นคงปลอดภัยไซเบอร์ จำนวนไม่น้อยกว่า ๑ แผน

โครงการขับเคลื่อนกลยุทธ์

๑. โครงการส่งเสริมและสนับสนุนการปฏิบัติงานของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ให้มีคุณภาพและมาตรฐาน

๒. โครงการเพิ่มขีดความสามารถสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

๓. โครงการปรับปรุงกฎหมาย ระเบียบและข้อบังคับในด้านความมั่นคงปลอดภัยไซเบอร์

๔. โครงการผสานรวมการค้นพบภัยคุกคาม การวิเคราะห์ และการตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

๕. โครงการจัดทำแผนฉุกเฉินสำหรับการจัดการวิกฤตความมั่นคงปลอดภัยไซเบอร์

๖. โครงการจัดระเบียบและดำเนินการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์

๗. โครงการการสกัดกั้นภัยคุกคามในระดับผู้ให้บริการโทรคมนาคม

๘. โครงการส่งเสริมและสนับสนุนการรวมผลิตภัณฑ์ความมั่นคงปลอดภัยไซเบอร์เข้ากับข้อเสนอบริการอื่น ๆ

๙. โครงการขับเคลื่อนแผน ยุทธศาสตร์ นโยบายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ กิจกรรมยกระดับขีดความสามารถการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Self-Assessment)

๑๐. โครงการการฝึกซ้อมเพื่อการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามไซเบอร์ของประเทศ กิจกรรมการจัดทำแผนเผชิญเหตุด้านไซเบอร์ (National Incident Response Plan)

๑๑. โครงการจัดตั้ง Sectoral CERT และพัฒนาแพลตฟอร์มรักษาความปลอดภัยทางไซเบอร์เพื่อรับมือเหตุฉุกเฉินทางคอมพิวเตอร์สำหรับ Sectoral CERT ของหน่วยงานด้านสาธารณสุข

โครงการ	**แนวทางการดำเนินการ**	**หน่วยงานรับผิดชอบ**
๑. โครงการส่งเสริมและสนับสนุนการปฏิบัติงานของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ให้มีคุณภาพและมาตรฐาน	๑) การจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (National CERT) ๒) การพัฒนาระบบสนับสนุนของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ๓) การจัดตั้งห้องปฏิบัติการวิเคราะห์ข้อมูลทางเทคนิคสำหรับการทดสอบเจาะระบบ การตรวจพิสูจน์หลักฐาน การทดสอบอุปกรณ์ CERT ของแต่ละภาคส่วนของหน่วยงาน CII (Sector CERT) ศูนย์วิเคราะห์ข่าวกรองทางไซเบอร์ (Cyber	**หลัก:** ดศ. สกมช. **รอง:** หน่วยงานควบคุมหรือกำกับดูแล บก.ทท. กห. ตร.

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
	Threat Intelligence Fusion Center), อุปกรณ์และเครื่องมือของ CPT (Cyber Protection Team) ๔) การจัดตั้งระบบแผนกช่วยเหลือ (Help Desk) ในศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ๕) การจัดตั้งศูนย์ปฏิบัติการร่วมทางไซเบอร์ของแต่ละหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ๖) นำมาตรฐานและแนวปฏิบัติที่ดีมาใช้ในการปฏิบัติงาน พร้อมทั้งได้รับใบรับรอง (Certification) และการรับรอง (Accreditation) ในส่วนของการปฏิบัติงานที่สำคัญ เช่น ISO/IEC 27001, ISO 22301, ISO/IEC 20000-1, ISO/IEC 38500 เป็นต้น ๗) จัดทำระบบในการกำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่องแบบ real-time ๘) กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง ๙) กำหนดหน่วยงานควบคุมหรือกำกับดูแลของแต่ละภาคส่วน (CII Sector) พร้อมทั้งส่งเสริมและสนับสนุนการทำงานของ CII Sector จัดให้หน่วยงานสนับสนุนในระดับภูมิภาค เช่น มหาวิทยาลัย เอกชน สถาบันการศึกษา หน่วยงานที่มีความชำนาญเฉพาะด้าน เป็นต้น เพื่อช่วยเหลือการทำงานของ CII Sector ๑๐) กำกับดูแล ติดตาม ประเมินผล ส่งเสริม และสนับสนุนอย่างต่อเนื่อง	
๒. โครงการเพิ่มขีดความสามารถสำนักงานคณะกรรมการการรักษาความมั่นคง	๑) การสร้างทีมปฏิบัติการป้องกันภัยไซเบอร์ (Cyber Protection Team : CPT) ๒) อบรมเพื่อพัฒนาทักษะทางไซเบอร์สำหรับผู้บริหารและผู้ปฏิบัติงานของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ	**หลัก:** ดศ. สกมช. **รอง:** หน่วยงานควบคุมหรือกำกับดูแลหน่วยงานโครงสร้างพื้นฐานสำคัญทาง

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
ปลอดภัยไซเบอร์แห่งชาติ (สกมช.)	๓) การจัดหาระบบฝึกซ้อมในการรับมือภัยคุกคามทางไซเบอร์ ๔) จัดตั้งศูนย์อบรม Cybersecurity Training Center ๕) จัดหาระบบ Cybersecurity Learning Platform ๖) เพิ่มศักยภาพในการกำกับดูแล (Governance) โดยกำหนดให้มีการจัดตั้ง “ประชาคมไซเบอร์แห่งชาติ” โดยมีสมาชิก เป็นผู้แทนหน่วยงานกำกับและหน่วยงานปฏิบัติ จากแต่ละ CII มีวัตถุประสงค์เพื่อให้เกิดการแลกเปลี่ยนองค์ความรู้ และแนวคิดให้เกิดการปฏิบัติตาม แผนปฏิบัติการฯ นโยบายการบริหารจัดการ ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ร่วมถึงแนวทางการปฏิบัติอื่น ๆ ที่จะมีตามมาในภายหลัง ๗) การส่งเสริมและสนับสนุนให้มีหน่วยงานพันธมิตรที่สนับสนุนด้านความมั่นคงปลอดภัยเพื่อช่วยเหลือภารกิจต่าง ๆ โดยหน่วยงานพันธมิตรควรมาจากหลากหลายภาคส่วน และหลากหลายภูมิภาค ๘) กำกับดูแล ติดตาม ประเมินผล ส่งเสริม และสนับสนุนอย่างต่อเนื่อง	สารสนเทศ บก.ทท. กห. ตร. สดช. สทป. อว. DEPA
๓. โครงการปรับปรุงกฎหมาย ระเบียบ และข้อ บังคับในด้านความมั่นคงปลอดภัยไซเบอร์	๑) การทบทวนแก้ไข หรือแนวทางในการสร้างกฎหมายในด้านมั่นคงปลอดภัยไซเบอร์ ๒) จัดทำ ปรับปรุง หรือสร้างกฎหมายในด้านมั่นคงปลอดภัยไซเบอร์ ๓) เผยแพร่ประชาสัมพันธ์ และให้ความรู้ความเข้าใจในการปฏิบัติ ๔) จัดให้เจ้าหน้าที่ของรัฐมีทักษะที่เกี่ยวข้อง ๕) กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง	**หลัก:** สกมช. **รอง:** หน่วยงานควบคุมหรือกำกับดูแล ยธ. กห. ตร. สพร. สพธอ.
๔. โครงการผสานรวมการค้นพบภัยคุกคามการวิเคราะห์ และการ	๑) จัดทำกรอบการดำเนินการการผสานรวมการค้นพบภัยคุกคาม ๒) การวิเคราะห์ และการตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์	**หลัก:** สกมช. **รอง:** หน่วยงานควบคุมหรือกำกับดูแล

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
ตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์	๓) สร้างกลไกการรายงานเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์จากทุกภาคส่วน ๔) การพัฒนาระบบการรายงานเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์และการวิเคราะห์และตอบสนองกึ่งอัตโนมัติ หรืออัตโนมัติ ๕) การพัฒนาบุคลากรในการปฏิบัติการวิเคราะห์และการตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ ๖) กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง	
๕. โครงการจัดทำแผนฉุกเฉินสำหรับการจัดการวิกฤตความมั่นคงปลอดภัยไซเบอร์	๑) กำหนดกรอบในการจัดทำแผนฉุกเฉิน (Contingency plans) สำหรับการจัดการวิกฤตความมั่นคงปลอดภัยไซเบอร์ระดับประเทศ เพื่อรองรับการจัดการในสถานการณ์ฉุกเฉินหรือภาวะวิกฤตของประเทศ โดยเฉพาะระบบโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ทั้งนี้ ควรคำนึงถึงผลการประเมินความเสี่ยงระดับประเทศและระดับภาคส่วนต่าง ๆ ซึ่งสามารถส่งผลกระทบเชื่อมโยงมายังโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศได้ ๒) ส่งเสริมและให้ความรู้ความเข้าใจแก่หน่วยงานที่เกี่ยวข้อง ๓) ทบทวน ปรับปรุงกรอบในการจัดทำแผนฉุกเฉินสำหรับการจัดการวิกฤตความมั่นคงปลอดภัยไซเบอร์ ๔) กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง	**หลัก:** สกมช. **รอง:** หน่วยงานควบคุมหรือกำกับดูแล สมช. บก.ทท.
๖. โครงการจัดระเบียบและดำเนินการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์	๑) กำหนดแนวทางในการดำเนินการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ ๒) ประชาสัมพันธ์และประกาศใช้แนวทางในดำเนินการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ ๓) ดำเนินการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ระหว่างภาคส่วนต่าง ๆ	**หลัก:** สกมช. **รอง:** สพร. สพธอ. สมช. หน่วยงานควบคุมหรือกำกับดูแล บก.ทท.

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
	๔) ขยายการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ระดับนานาชาติ ๕) กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง	
๗. โครงการการสกัดกั้นภัยคุกคามในระดับผู้ให้บริการโทรคมนาคม	๑) จัดกรอบแนวทางในการสกัดกั้นภัยคุกคามทางไซเบอร์ร่วมกับผู้ให้บริการโทรคมนาคม ๒) จัดทำแนวทางตามกรอบการปฏิบัติการ ๓) สนับสนุน เผยแพร่ประชาสัมพันธ์ และให้ความรู้ความเข้าใจในการปฏิบัติ ๔) จัดทำแนวสนับสนุนเมื่อได้รับการร้องขอความร่วมมือจากทางเจ้าหน้าที่ของรัฐเพื่อป้องกันภัยคุกคามทางไซเบอร์ ๕) กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง	**หลัก:** สกมช. **รอง:** กสทช.
๘. โครงการส่งเสริมและสนับสนุนการรวมผลิตภัณฑ์ความมั่นคงปลอดภัยไซเบอร์เข้ากับข้อเสนอบริการอื่นๆ	๑) จัดทำแนวทางในการรวมผลิตภัณฑ์ความมั่นคงปลอดภัยไซเบอร์เข้ากับข้อเสนอบริการอื่น ๆ ผลิตภัณฑ์หรือบริการอื่น ๆ ที่จะนำเข้ามาเชื่อมต่อใช้งาน หรือให้บริการกับบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical information infrastructure: CII) ต้องมีการพิจารณาด้านความมั่นคงปลอดภัยเข้าไปด้วยในแนวทางและเกณฑ์ในการพิจารณาความเสี่ยงในการเลือกผู้ให้บริการและผลิตภัณฑ์ตลอดวงจรชีวิตของการบริหารจัดการความเสี่ยงจากบุคคลภายนอก (Third Party Risk Management Life Cycle) เช่น นโยบายที่ยืนยันได้ว่าผลิตภัณฑ์หรือบริการนั้นไม่มีการแอบแฝงภัยคุกคามที่ทำงานอยู่ในฉากหลัง (Backdoor Policy) ความเสี่ยงจากการพึ่งพาบุคคลภายนอกรายใดรายหนึ่ง (Third Party/Vendor Locked-in) โดยการพึ่งพาบุคคลภายนอกรายใดรายหนึ่งเป็นหลัก อาจทำให้มีข้อจำกัดในการเปลี่ยนแปลงเทคโนโลยีผู้ให้บริการหรือพันธมิตร และข้อจำกัด	**หลัก:** สกมช. **รอง:** สพร. สพธอ. หน่วยงานควบคุมหรือกำกับดูแล

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
	ในการนำระบบหรือข้อมูลกลับมาดำเนินการเอง เป็นต้น ซึ่งต้องอาศัยกฎหมาย ระเบียบ ข้อบังคับที่จำเป็นในการบังคับใช้การรวมผลิตภัณฑ์ความมั่นคงปลอดภัยไซเบอร์เข้ากับข้อเสนอบริการอื่น ๆ ๒) ออกกฎหมาย ระเบียบ ข้อบังคับที่จำเป็นในการบังคับใช้การรวมผลิตภัณฑ์ความมั่นคงปลอดภัยไซเบอร์เข้ากับข้อเสนอบริการอื่น ๆ ๓) ให้ความรู้ความเข้าใจในการดำเนินการ ๔) กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง	
๙. โครงการขับเคลื่อนแผนยุทธศาสตร์นโยบายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ กิจกรรมยกระดับขีดความสามารถการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Self-Assessment)	๑) จัดทำขั้นตอนกิจกรรม การดำเนินงาน และแผนการดำเนินงานในแต่ละขั้นตอน (Action Plan) ๒) ศึกษากรอบแนวคิด เครื่องมือหรือตัวแบบจากข้อมูลทุติยภูมิทั้งในและต่างประเทศที่จะใช้ในการประเมินระดับการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Self-Assessment) ๓) จัดทำกรอบแนวคิด เครื่องมือหรือตัวแบบในการประเมินระดับการรักษาความมั่นคงปลอดภัยไซเบอร์ที่จะใช้กับหน่วยงานของรัฐที่ไม่ใช่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ๔) จัดประชุมกลุ่มย่อย (Focus group) ผ่านระบบอิเล็กทรอนิกส์ โดยมีผู้ทรงคุณวุฒิหรือผู้เชี่ยวชาญของหน่วยงานของรัฐที่ไม่ใช่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานควบคุมหรือกำกับดูแล หรือหน่วยงานที่เกี่ยวข้อง ๕) จัดทำแบบสอบถามอิเล็กทรอนิกส์เพื่อใช้ในการประเมินการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Self-Assessment) ๖) วิเคราะห์ข้อมูลการตรวจสอบความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและจัดทำรายงานผลการประเมินขีดความสามารถด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	**หลัก:** สกมช. **รอง:** หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
๑๐. โครงการการฝึกซ้อมเพื่อการป้องกัน รับมือและลดความเสี่ยงจากภัยคุกคามไซเบอร์ของประเทศ กิจกรรมการจัดทำแผนเผชิญเหตุด้านไซเบอร์ (National Incident Response Plan)	๑) จัดทำแผนการดำเนินงานของกิจกรรมต่าง ๆ ในโครงการฯ พร้อมทั้งอธิบายรายละเอียด ระยะเวลา และผู้รับผิดชอบในแต่ละกิจกรรม ๒) ศึกษา วิเคราะห์ ข้อมูลทั้งจากภายในประเทศและต่างประเทศเพื่อการจัดทำนโยบายและแผน นโยบายการบริหาร และแผนปฏิบัติการ ๓) นำเสนอผลแผนการดำเนินงาน ผลการศึกษาวิเคราะห์ มอบหมายงานให้หน่วยงานที่เกี่ยวข้อง ๔) ดำเนินการงานประชาสัมพันธ์โครงการสู่หน่วยงานภาครัฐ หน่วยงานที่เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หรือหน่วยงานที่เกี่ยวข้อง ๕) จัดการอบรมและประชุมเชิงปฏิบัติการเพื่อจัดทำแผนเผชิญเหตุ ในกรณีเกิดเหตุภัยคุกคามทางไซเบอร์ในระดับต่าง ๆ ๖) สรุปผลการดำเนินโครงการ	**หลัก:** สกมช. **รอง:** หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
๑๑. โครงการจัดตั้ง Sectoral CERT และพัฒนาแพลตฟอร์มรักษาความปลอดภัยทางไซเบอร์เพื่อรับมือเหตุฉุกเฉินทางคอมพิวเตอร์สำหรับ Sectoral CERT ของหน่วยงานด้านสาธารณสุข	๑) จัดทำข้อกำหนดและขอบเขตงาน ๒) เก็บรวบรวมข้อมูลและความต้องการจากหน่วยงานโครงการพื้นฐานสำคัญสารสนเทศด้านสาธารณสุขแต่ละหน่วยงาน ๓) ดำเนินการจัดซื้อจัดจ้าง ๔) ดำเนินการติดตั้งระบบรักษาความมั่นคงปลอดภัยทางไซเบอร์ให้กับสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและฝึกอบรมบุคลากร ๕) เปิดใช้งานระบบ ๖) สรุปและประเมินผลโครงการ	**หลัก:** สกมช. **รอง:** หน่วยงานโครงการพื้นฐานสำคัญสารสนเทศด้านสาธารณสุข

กลยุทธ์ที่ ๔.๒ ส่งเสริมและสนับสนุนการแบ่งปันข้อมูลภัยคุกคาม

๑.สร้างกลไกการแลกเปลี่ยนข้อมูล ข่าวกรอง และองค์ความรู้ด้านภัยคุกคามทางไซเบอร์

๒. สร้างกลไกการรายงานเหตุการณ์ภัยคุกคามทางไซเบอร์

๓.สร้างการมีส่วนร่วมของทุกภาคส่วนในการแบ่งปันข้อมูลภัยคุกคามทางไซเบอร์

ตัวชี้วัดของกลยุทธ์

๑. มีการแลกเปลี่ยนข้อมูล ข่าวกรอง และองค์ความรู้ด้านภัยคุกคามทางไซเบอร์ร่วมกัน

๒. มีการรายงานเหตุการณ์ภัยคุกคามทางไซเบอร์ โดยสามารถระบุสาเหตุและลดเหตุการณ์ภัยคุกคามทางไซเบอร์

๓. มีความร่วมมือของทุกภาคส่วนในการแบ่งปันข้อมูลภัยคุกคามทางไซเบอร์

โครงการขับเคลื่อนกลยุทธ์

๑. โครงการสร้างกลไกการแบ่งปันข้อมูลระหว่างภาครัฐและเอกชนและอำนวยความสะดวกในการแบ่งปันข้อมูลความมั่นคงปลอดภัยไซเบอร์

๒. โครงการส่งเสริมและสนับสนุนการแบ่งปันข้อมูลภัยคุกคามระหว่างประเทศ

๓. โครงการพัฒนาแพลตฟอร์มสำหรับการรับและแบ่งปันเหตุการณ์ภัยคุกคามทางไซเบอร์

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
๑. โครงการสร้างกลไกการแบ่งปันข้อมูลระหว่างภาครัฐและเอกชนและอำนวยความสะดวกในการแบ่งปันข้อมูลความมั่นคงปลอดภัยไซเบอร์	๑) สร้างกลไกการแบ่งปันข้อมูลระหว่างภาครัฐและเอกชน ระหว่าง หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ Sector CERT และหน่วยงานความมั่นคง ๒) พัฒนาแพลตฟอร์มสำหรับการรายงานและการแบ่งปันเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ข้ามภาคส่วน ๓) พัฒนาระบบแบ่งปันข้อมูลอัตโนมัติ ๔) กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง	**หลัก:** สกมช. **รอง:** สพร. สพธอ. หน่วยงานควบคุมหรือกำกับดูแล กห. ตร.
๒. โครงการส่งเสริมและสนับสนุนการแบ่งปันข้อมูลภัยคุกคามระหว่างประเทศ	๑) สร้างกลไกการแบ่งปันข้อมูลระหว่างภูมิภาคและนานาชาติ และอำนวยความสะดวกในการแบ่งปันข้อมูลความมั่นคงปลอดภัยทางไซเบอร์ การจัดตั้งกลไกการแบ่งปันข้อมูลเพื่อให้สามารถแลกเปลี่ยนข้อมูลข่าวกรองและข้อมูลภัยคุกคามที่ดำเนินการได้ ๒) จัดทำแพลตฟอร์มและระบบสำหรับการแบ่งปันข้อมูลระดับภูมิภาคและนานาชาติ ระบบแบ่งปันข้อมูลอัตโนมัติ (เช่น ระบบรักษาความมั่นคงปลอดภัยทางไซเบอร์ที่แจ้งเตือนได้โดยอัตโนมัติ	**หลัก:** สกมช. **รอง:** สพร. สพธอ. หน่วยงานควบคุมหรือกำกับดูแล กห. ตร.

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
	เมื่อเกิดเหตุการณ์หรือการโจมตีทางไซเบอร์) ควบคู่ไปกับแพลตฟอร์มแบ่งปันภัยคุกคามแบบหลายทิศทาง (multi-directional threat-sharing platform) ๓) เพิ่มขีดความสามารถในการแบ่งปันข้อมูลภัยคุกคามระดับภูมิภาคและนานาชาติอย่างต่อเนื่อง ๔) กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง	
๓. โครงการพัฒนาแพลตฟอร์มสำหรับการรับและแบ่งปันเหตุการณ์ภัยคุกคามทางไซเบอร์	๑) จัดทำกรอบแนวคิดในการดำเนินงาน และแผนการดำเนินงานในโครงการฯ พร้อมทั้งอธิบายรายละเอียดระยะเวลา และผู้รับผิดชอบในโครงการ ๒) จัดทำเอกสารเพื่อเป็นแนวทางในการใช้ระบบและเชื่อมต่อ MISP ไปยังหน่วยงานต่าง ๆ - SOP (Standard operating Procedure) for information sharing -หนังสือข้อตกลงในการใช้และเชื่อมต่อระบบ MISP ๓) สร้างความรู้ความเข้าใจถึงการแลกเปลี่ยนข้อมูลตาม SOP ๔) ดำเนินการให้สิทธิ์การเข้าใช้ MISP กลาง ๕) ดำเนินการออกแบบเตรียม Environment ของ สกมช. เพื่อการเชื่อมต่อ ๖) ดำเนินการเชื่อมต่อระบบ MISP เพื่อแลกเปลี่ยนข้อมูลแบบอัตโนมัติอย่างน้อย ๑๐ หน่วยงาน ๗) สรุปผลการดำเนินการ	**หลัก:** สกมช. **รอง:** หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

กลยุทธ์ที่ ๔.๓ ส่งเสริมและสนับสนุนความมั่นคงปลอดภัยทางไซเบอร์

๑. สร้างความเชื่อมั่นให้กับทุกภาคส่วนในการรักษาความมั่นคงปลอดภัยไซเบอร์

๒. ยกระดับการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานที่ให้บริการที่สำคัญ

๓. ส่งเสริมและสนับสนุนให้เกิดบริการด้านความมั่นคงปลอดภัยไซเบอร์

ตัวชี้วัดของกลยุทธ์

๑. ทุกภาคส่วนมีความเชื่อมั่นในการรักษาความมั่นคงปลอดภัยไซเบอร์ไม่น้อยกว่าร้อยละ ๕๐

๒. มีการออกกฎหมาย ระเบียบ ข้อบังคับที่จำเป็นในการส่งเสริมให้มีผู้ให้บริการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๓. มีจำนวนผู้ให้บริการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพิ่มขึ้นปีละไม่น้อยกว่าร้อยละ ๑๐

โครงการขับเคลื่อนกลยุทธ์

๑. โครงการขยายการสนับสนุนของ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ไปยังองค์กรที่ให้บริการที่สำคัญ

๒. โครงการส่งเสริมและสนับสนุนให้มีผู้ให้บริการด้านความมั่นคงปลอดภัยสำหรับที่ให้บริการที่สำคัญ

๓. โครงการขับเคลื่อนแผน ยุทธศาสตร์ นโยบายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์

๔. โครงการจัดตั้งสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ กิจกรรมการจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ (National CERT)

๕. โครงการจัดตั้งสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ กิจกรรมระบบช่วยเหลือ (Help Desk) ของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ

๖. โครงการจัดตั้งสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ กิจกรรมจัดตั้งปฏิบัติการร่วมทางไซเบอร์ (NCSA War room)

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
๑. โครงการขยายการสนับสนุนของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ไปยังองค์กรที่ให้บริการที่สำคัญ	๑) จัดทำแนวทางขยายการสนับสนุนของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ไปยังองค์กรที่ให้บริการที่สำคัญ ๒) สร้างกลไกขยายการสนับสนุนของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ไปยังองค์กรที่ให้บริการที่สำคัญ	**หลัก:** สกมช. **รอง:** หน่วยงานควบคุมหรือกำกับดูแล

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
	๓) พัฒนาแพลตฟอร์มสำหรับขยายการสนับสนุนของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ไปยังองค์กรที่ให้บริการที่สำคัญ ๔) พัฒนาขีดความสามารถในการสนับสนุนของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ไปยังองค์กรที่ให้บริการที่สำคัญ ๕) กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง	
๒. โครงการส่งเสริมและสนับสนุนให้มีผู้ให้บริการด้านความมั่นคงปลอดภัยสำหรับที่ให้บริการที่สำคัญ	๑) จัดทำแนวทางในการส่งเสริมให้มีผู้ให้บริการด้านความมั่นคงปลอดภัยสำหรับองค์กรที่ให้บริการที่สำคัญ ให้สิทธิพิเศษต่าง ๆ ในการดำเนินการกำหนดช่วงเกณฑ์ราคามาตรฐาน ๒) ออกกฎหมาย ระเบียบ ข้อบังคับที่จำเป็นในการส่งเสริมให้มีผู้ให้บริการด้านความมั่นคงปลอดภัยสำหรับองค์กรที่ให้บริการที่สำคัญ ๓) กำกับดูแลการส่งเสริมให้มีผู้ให้บริการด้านความมั่นคงปลอดภัยสำหรับองค์กรที่ให้บริการที่สำคัญ ๔) กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง	**หลัก:** สกมช. **รอง:** หน่วยงานควบคุมหรือกำกับดูแล อส. บีโอไอ
3. โครงการขับเคลื่อนแผน ยุทธศาสตร์ นโยบายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์	๑) วางแผนการดำเนินงาน จัดทำกรอบแนวคิดในการดำเนินงาน และแผนการดำเนินงานของกิจกรรมต่างๆในโครงการฯ พร้อมทั้งอธิบายรายละเอียด ระยะเวลาและผู้รับผิดชอบในแต่ละกิจกรรม ๒) จัดทำเนื้อหาและรูปแบบการประชาสัมพันธ์การสร้างสื่อการเรียนรู้แบบออนไลน์ ๓) ประชาสัมพันธ์กิจกรรมผ่านสื่อในรูปแบบต่าง ๆ ๔) ดำเนินการจัดประชุมสัมมนาชี้แจงทำความเข้าใจนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ฯ รวมทั้งกฎระเบียบที่เกี่ยวข้อง จำนวน ๔ ครั้ง ครั้งละ ๒ วัน โดยมีผู้เข้าร่วมงานรวม	**หลัก:** สกมช. **รอง:** หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
	ไม่น้อยกว่า ๓๐๐ คน ในสถานที่เอกชนและดำเนินการจัดสัมมนาสร้างความรู้ความเข้าใจในรูปแบบออนไลน์ ๕) ติดตามประเมินผลการดำเนินงานโครงการฯ ๖) จัดทำรายงานสรุปผลการดำเนินงานโครงการฯ	
๔. โครงการจัดตั้งสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ กิจกรรมการจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ (National CERT)	๑) ศึกษา วิเคราะห์ จัดทำกรอบแนวคิดในการดำเนินงานการออกแบบและแผนการดำเนินงานในการพัฒนาออกแบบและพัฒนาระบบงานของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ (National CERT) ๒) จัดหาครุภัณฑ์และอุปกรณ์สำหรับศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ (National CERT) ดำเนินการติดตั้ง และทดสอบระบบและอุปกรณ์ให้พร้อมใช้งานตามข้อกำหนด และจัดทำคู่มือผู้ดูแลระบบและผู้ใช้งาน ๓) ทดสอบการใช้งานระบบ และปรับแต่งให้ตรงกับความต้องการ ๔) ดำเนินการจัดทำรายงานผลการตรวจพบภัยคุกคามความปลอดภัยทางไซเบอร์ของระบบ Threat Hunting Framework (THF) เป็นรายเดือนภายหลังติดตั้งระบบแล้วเสร็จ ๕) จัดให้มีทีมที่ปรึกษาเพื่อสนับสนุนใช้งานระบบให้สามารถใช้งานได้ต่อเนื่องตลอดเวลา ๒๔ ชั่วโมง ใน ๗ วันโดยจะต้องมีผู้บุคคลที่มีความรู้ความสามารถ และมีคุณวุฒิพื้นฐานความรู้ประสบการณ์ ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ ทั้งนี้ ผู้ขาย/ผู้รับจ้าง จะต้องส่งบุคลากรประจำศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (National CERT) จำนวน ๒ คน ในระยะเวลาปฏิบัติงาน ๑๒ เดือน ในส่วนของอุปกรณ์สำนักงาน เช่น คอมพิวเตอร์ เครื่องพิมพ์ เป็นต้น ผู้ขาย/ผู้รับจ้าง จะต้องเป็นผู้จัดหาให้	**หลัก:** สกมช. **รอง:** หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน่วยงานของรัฐ

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
	๖) จัดอบรมเกี่ยวกับการใช้งานให้กับเจ้าหน้าที่ที่เกี่ยวข้อง ๗) เจ้าหน้าที่ดูแล และเฝ้าระวังภัยคุกคามทางไซเบอร์ จัดทำรายงานสรุปภัยคุกคามทางไซเบอร์ที่เกิดขึ้นในแต่ละเดือน จัดทำสรุปแนวโน้มภัยคุกคามทางไซเบอร์รายไตรมาส จัดทำรายงานสรุปผลการดำเนินงานโครงการฯ	
๕. โครงการจัดตั้งสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ กิจกรรมระบบช่วยเหลือ (Help Desk) ของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ	๑) จัดทำกรอบแนวคิดในการดำเนินงาน และแผนการดำเนินงานของกิจกรรมต่าง ๆ ในโครงการฯ พร้อมทั้งอธิบายรายละเอียดระยะเวลา และผู้รับผิดชอบในแต่ละกิจกรรม ๒) ติดตั้งและให้บริการระบบช่วยเหลืองานบริหารการรักษาความมั่นคงปลอดภัยทางไซเบอร์ External Ticketing System ระบบช่วยเหลืองานบริหารการรักษาความมั่นคงปลอดภัยทางไซเบอร์ภายในองค์กร Internal Ticketing System ระบบรักษาความปลอดภัยสารสนเทศและวิเคราะห์ข้อมูล Data Center ระบบแฟลตฟอร์มการแลกเปลี่ยนข้อมูลข่าวสารภัยคุกคามทางไซเบอร์ ๓) จัดทำรายงานสรุปผลการดำเนินงาน	**หลัก:** สกมช. **รอง:** หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและหน่วยงานของรัฐ
๖. โครงการจัดตั้งสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ กิจกรรมจัดตั้งปฏิบัติการร่วมทางไซเบอร์ (NCSA War room)	๑) จัดทำกรอบแนวคิดในการดำเนินงาน และแผนการบำรุงรักษา แก้ไข ซ่อมแซม อุปกรณ์และระบบในโครงการฯพร้อมทั้งอธิบายรายละเอียดระยะเวลาการดำเนินโครงการ ๒) ดำเนินการตรวจสอบระบบและอุปกรณ์ตามวาระปีละ ๔ ครั้ง (ทุก ๓ เดือน) ๓) จัดทำรายงานสรุปผลการบำรุงรักษาในโครงการฯ พร้อมส่งมอบ	**หลัก:** สกมช. **รอง:** หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและหน่วยงานของรัฐ

ภาคผนวก

นโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

นโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๙(๒) บัญญัติให้คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) มีหน้าที่และอำนาจ กำหนดนโยบายการบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

นโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ฉบับนี้ จัดทำเพื่อเป็นแนวทางการกำกับดูแล การบริหารความเสี่ยง และการปฏิบัติตาม (Governance, Risk and Compliance: GRC) สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ปฏิบัติได้อย่างรวดเร็ว มีประสิทธิภาพ และเป็นไปในทิศทางเดียวกัน

นโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์นี้ใช้หลักการตามแนวทางการปฏิบัติที่ดีที่ใช้กันแพร่หลายทั่วโลก รวมถึงประเทศไทย ซึ่งคือ หลักการกำกับดูแลการบริหารความเสี่ยง และการปฏิบัติตาม (Governance, Risk and Compliance: GRC) ประกอบด้วย ๓ หลักการ ดังนี้

๑. การกำกับดูแลการรักษาความมั่นคงปลอดภัยไซเบอร์ (Good Governance in Cybersecurity)

๑.๑. ต้องจัดโครงสร้างองค์กรให้มีการถ่วงดุล โดยจัดโครงสร้างองค์กร พร้อมกำหนดอำนาจ บทบาทหน้าที่ และความรับผิดชอบ (Authorities, Roles and Responsibilities) ที่ชัดเจนเกี่ยวกับการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ ให้มีการถ่วงดุลตามหลักการควบคุม กำกับ และตรวจสอบ (Three Lines of Defense) ที่มีประสิทธิภาพ โดยมีผู้ที่ทำหน้าที่ควบคุม กำกับ และตรวจสอบที่เป็นอิสระและสามารถทำหน้าที่ได้อย่างมีประสิทธิผล ซึ่งต้องมีการกำหนดหน้าที่ความรับผิดชอบอย่างชัดเจน ทั้งหน่วยงานหรือผู้ก่อให้เกิดความเสี่ยงและควบคุมความเสี่ยงในชั้นแรก (Business Unit หรือ First Line of Defense) มีหน้าที่ดูแลและปฏิบัติงานให้เป็นไปตามกฎเกณฑ์ที่กำหนดไว้ มีการควบคุมภายใน และมีการจัดการความเสี่ยงอย่างเหมาะสม หน่วยงานหรือผู้กำกับภายใน (Second Line of Defense) เช่น หน่วยงานบริหารความเสี่ยง (Risk Management) หน่วยงานกำกับการปฏิบัติตามกฎเกณฑ์ (Compliance) และหน่วยงานหรือผู้ตรวจสอบภายใน (Internal Audit หรือ Third Line of Defense) เพื่อส่งเสริมให้มีกลไกการตรวจสอบและถ่วงดุลที่เหมาะสม โดยให้หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศถือปฏิบัติตามกฎหมายหรือหลักเกณฑ์ที่เกี่ยวข้องในปัจจุบัน รวมถึงแนวปฏิบัติในเรื่องดังกล่าวที่จะออกโดยหน่วยงานควบคุมหรือกำกับดูแล และจะมีผลบังคับใช้กับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต่อไป

ทั้งนี้ กรณีที่มีโครงสร้างการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศรวมกับบริษัทในกลุ่มธุรกิจเดียวกันหรือบริษัทที่มีความเกี่ยวข้อง การพิจารณาโครงสร้างการกำกับดูแลตามหลักการแบ่งแยกหน้าที่ความรับผิดชอบตาม Three Lines of Defense ให้พิจารณาโดยดูจากภาพรวมทั้งหมดของกลุ่มธุรกิจเดียวกัน

๑.๒. การกำหนดให้มีผู้รับผิดชอบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ หน่วยงานของรัฐต้องจัดให้มีผู้บริหารที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Head of Information Security) หรือเทียบเท่าที่ปฏิบัติหน้าที่ของหน่วยงาน โดยบุคคลดังกล่างต้องเป็นผู้ที่มีความรู้หรือประสบการณ์ด้านเทคโนโลยีสารสนเทศ การบริหารความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการรับมือกับภัยคุกคามทางไซเบอร์

ทั้งนี้ผู้บริหารที่ทำหน้าที่ดังกล่าวควรมีความเป็นอิสระจากงานด้านการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT operation) และงานด้านพัฒนาระบบเทคโนโลยีสารสนเทศ (IT development) รวมทั้งควรมีบทบาทหน้าที่และความรับผิดชอบให้หน่วยงานดำเนินการเพื่อความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศอย่างน้อย ดังนี้

๑) มีนโยบาย มาตรฐาน และแนวทางการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการรับมือภัยคุกคามทางไซเบอร์ รวมทั้งดูแลให้มีการปฏิบัติตามนโยบาย มาตรฐาน และแนวทางที่กำหนด

๒) มีข้อกำหนดด้านความมั่นคงปลอดภัย (security specification) และสถาปัตยกรรมด้านความมั่นคงปลอดภัย (IT security architecture)

๓) บริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและด้านภัยคุกคามทางไซเบอร์ให้สอดรับกับความเสี่ยงที่องค์กรมี และนำเสนอความเสี่ยงดังกล่าวต่อคณะกรรมการหน่วยงานเป็นวาระประจำ

๔) ดูแลและดำเนินการให้หน่วยงานมีความพร้อมในการรับมือภัยคุกคามทางไซเบอร์

๕) ดูแลและดำเนินการให้บุคลากรในองค์กรมีความรู้และความตระหนักรู้เรื่องความเสี่ยง การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศด้านภัยคุกคามทางไซเบอร์

๑.๓ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องจัดให้มีผู้บริหารระดับสูงที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Chief Information Security Officer : CISO) หรือเทียบเท่าที่ปฏิบัติหน้าที่เสมือน CISO ของหน่วยงาน

ทั้งนี้ ผู้บริหารระดับสูงที่ทำหน้าที่ดังกล่าวควรเป็นอิสระจากงานด้านการปฏิบัติงานเทคโนโลยีสารสนเทศ (IT operation) และงานด้านพัฒนาระบบเทคโนโลยีสารสนเทศ (IT development) และมีอำนาจหน้าที่ (Authority) เพียงพอในการปฏิบัติงานในหน้าที่ CISO ได้อย่างมีประสิทธิภาพและประสิทธิผล โดยสามารถดำเนินการอย่างน้อย ดังนี้

๑) รายงานปัญหาหรือเหตุการณ์ที่มีนัยสำคัญด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและด้านภัยคุกคามทางไซเบอร์ต่อผู้บริหารในตำแหน่งสูงสุด คณะกรรมการของหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และคณะกรรมการที่เกี่ยวข้องโดยตรง

๒) ให้ความเห็นด้านภัยคุกคามไซเบอร์และการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศต่อคณะกรรมการของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ คณะกรรมการที่เกี่ยวข้องกับการบริหารจัดการและกำกับดูแลการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ เช่น IT steering committee หรือ IT risk committee และร่วมตัดสินใจดำเนินการในเรื่องความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และด้านภัยคุกคามทางไซเบอร์ที่กระทบต่อหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศอย่างมีนัยสำคัญ

๒. การบริหารความเสี่ยง (Risk Management)

๒.๑ ต้องจัดทำกรอบการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์เป็นลายลักษณ์อักษร กรอบจะรวมถึง :

(ก) ระบุเกณฑ์ประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ และระดับความเสี่ยงที่ยอมรับได้ (Risk appetite)

(ข) วิธีการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

(ค) การเฝ้าระวังและติดตามความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

๒.๒ ต้องเก็บรักษารายการความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ระบุไว้ในทะเบียนความเสี่ยง (Risk register) ที่เกี่ยวข้องกับบริการที่สำคัญของหน่วยงานของรัฐ และโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๒.๓ ต้องติดตามความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่ระบุไว้อย่างสม่ำเสมอ เพื่อให้แน่ใจว่าอยู่ภายใต้เกณฑ์ระดับความเสี่ยงที่ยอมรับได้ที่ระบุไว้ในข้อ ๒.๑ (ก)

๓. นโยบาย และแนวปฏิบัติ (Policies and Guidelines)

๓.๑ ต้องกำหนด และอนุมัตินโยบาย มาตรฐาน และแนวทางในการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ และการป้องกันบริการที่สำคัญของหน่วยงานของรัฐ และโครงสร้างพื้นฐานสำคัญทางสารสนเทศ จากภัยคุกคามทางไซเบอร์ นโยบาย มาตรฐาน และแนวปฏิบัติจะต้อง :

(ก) สอดคล้องกับหลักประมวลแนวทางปฏิบัตินี้ ข้อกำหนดการรักษาความมั่นคงปลอดภัยไซเบอร์ของภาคส่วน และนโยบาย มาตรฐาน และทิศทางการรักษาความมั่นคงปลอดภัยไซเบอร์ระดับภูมิภาค หรือระดับประเทศ

(ข) เผยแพร่และสื่อสารไปยังบุคลากรและบุคคลภายนอกทุกคนที่ทำหน้าที่หรือสามารถเข้าถึงบริการที่สำคัญของหน่วยงานของรัฐ และโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๓.๒ ต้องทบทวนนโยบาย มาตรฐาน และแนวทางปฏิบัติกับสภาพแวดล้อมการปฏิบัติการไซเบอร์ของบริการที่สำคัญของหน่วยงานของรัฐ และโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และภูมิทัศน์ภัยคุกคามทางไซเบอร์ในปัจจุบันอย่างน้อยปีละหนึ่งครั้งโดยนับถัดจากวันที่การทบทวนครั้งสุดท้าย หรือวันที่มีผลบังคับใช้ของนโยบาย มาตรฐาน หรือแนวปฏิบัติแต่ละข้อ

ทั้งนี้ นโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนี้มีผลบังคับใช้ภายในหนึ่ง (๑) ปี นับถัดจากวันที่ประกาศ

อภิธานศัพท์

คำศัพท์	ความหมาย
การรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity)	มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกประเทศ อันกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ
ภัยคุกคามทางไซเบอร์ (Cyber threat)	การกระทำหรือการดำเนินการใด ๆ โดยมิชอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์ โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง
ไซเบอร์ (Cyber)	ข้อมูลและการสื่อสารที่เกิดจากการให้บริการ หรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต หรือโครงข่ายโทรคมนาคม รวมทั้งการให้บริการโดยปกติของดาวเทียม และระบบเครือข่ายที่คล้ายคลึงกัน ที่เชื่อมต่อกันเป็นการทั่วไป
หน่วยงานของรัฐ (Government agency)	ราชการส่วนกลาง ราชการส่วนภูมิภาค ราชการส่วนท้องถิ่น รัฐวิสาหกิจ องค์กรฝ่ายนิติบัญญัติ องค์กรฝ่ายตุลาการ องค์กรอิสระ องค์การมหาชน และหน่วยงานอื่นของรัฐ
เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Incident)	เหตุการณ์ที่เกิดจากการกระทำหรือการดำเนินการใด ๆ ที่มิชอบซึ่งกระทำการผ่านทางคอมพิวเตอร์หรือระบบคอมพิวเตอร์ซึ่งอาจเกิดความเสียหายหรือผลกระทบต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือความมั่นคงปลอดภัยไซเบอร์ของคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์
โครงสร้างพื้นฐานสำคัญ (Critical Infrastructure : CI)	บรรดาหน่วยงาน หรือองค์กร หรือส่วนงานหนึ่งส่วนงานใดของหน่วยงานหรือองค์กรซึ่งธุรกรรมทางอิเล็กทรอนิกส์ของหน่วยงาน หรือองค์กร หรือส่วนงานของหน่วยงานหรือองค์กรนั้นมีผลเกี่ยวเนื่องสำคัญต่อความมั่นคงหรือความสงบเรียบร้อยของประเทศหรือต่อสาธารณชน

คำศัพท์	ความหมาย
โครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure : CII)	คอมพิวเตอร์หรือระบบคอมพิวเตอร์ซึ่งหน่วยงานของรัฐหรือหน่วยงานเอกชนใช้ในกิจการของตนที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของรัฐ ความปลอดภัยสาธารณะ ความมั่นคงทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ
หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical information infrastructure operator)	หน่วยงานของรัฐหรือหน่วยงานเอกชน ซึ่งมีภารกิจหรือให้บริการโครงสร้างพื้นฐานสำคัญทางสารสนเทศ มาตรา ๔๙ เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ มีดังนี้ (๑) ด้านความมั่นคงของรัฐ (๒) ด้านบริการภาครัฐที่สำคัญ (๓) ด้านการเงินการธนาคาร (๔) ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม (๕) ด้านการขนส่งและโลจิสติกส์ (๖) ด้านพลังงานและสาธารณูปโภค (๗) ด้านสาธารณสุข (๘) ด้านอื่นตามที่คณะกรรมการประกาศกำหนดเพิ่มเติม
หน่วยงานควบคุมหรือกำกับดูแล (Regulator)	หน่วยงานของรัฐ หน่วยงานเอกชน หรือ บุคคลซึ่งมีกฎหมายกำหนดให้มีหน้าที่และอำนาจในการควบคุมหรือกำกับดูแลการดำเนินกิจการของหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
ผลิตภัณฑ์มวลรวมของประเทศ (Gross Domestic Product: GDP)	มูลค่าตลาดของสินค้าและบริการขั้นสุดท้ายที่ผลิตในประเทศในช่วงเวลาหนึ่ง โดยไม่คำนึงว่าผลผลิตนั้นจะเป็นผลผลิตที่ได้จากทรัพยากรภายในหรือภายนอกประเทศ คิดค้นโดย Simon Kuznets นักเศรษฐศาสตร์ชาวรัสเซีย ซึ่งผลิตภัณฑ์มวลรวมในประเทศสามารถใช้เป็นตัวบ่งชี้ถึงมาตรฐานการครองชีพของประชากรในประเทศ
แพลตฟอร์ม (Platform)	ระบบโปรแกรมคอมพิวเตอร์ที่สามารถขยายขีดความสามารถอย่างไม่จำกัด มีการพัฒนาฟังก์ชั่นหรือโมดูลใหม่ๆ มาต่อยอดอยู่ตลอดเวลา เกิดนวัตกรรมใหม่ ๆ เสมอ และสามารถนำไปต่อเชื่อมกับระบบอื่นได้ แพลตฟอร์มไม่ได้จำกัดอยู่แค่ซอฟต์แวร์ แต่ยังรวมไปถึงเว็บไซต์ หรือบริการที่คนอื่นสามารถเขียนโปรแกรมมาต่อเชื่อมหรือดึงข้อมูลได้โดยอัตโนมัติ

คำศัพท์	ความหมาย
ปัญญาประดิษฐ์ (Artificial Intelligence: AI)	ศาสตร์แขนงหนึ่งของวิทยาศาสตร์คอมพิวเตอร์ ที่เกี่ยวข้องกับวิธีการทำให้คอมพิวเตอร์มีความสามารถคล้ายมนุษย์หรือเลียนแบบพฤติกรรมมนุษย์ โดยเฉพาะความสามารถในการคิดเองได้ หรือมีปัญญา ซึ่งปัญญานี้มนุษย์เป็นผู้สร้างให้คอมพิวเตอร์ จึงเรียกว่าปัญญาประดิษฐ์ มุมมองต่อ AI ที่แต่ละคนมีอาจไม่เหมือนกัน ขึ้นอยู่กับว่าเราต้องการความฉลาดโดยคำนึงถึงพฤติกรรมที่มีต่อสิ่งแวดล้อมหรือคำนึงการคิดได้ของผลผลิต AI
ดัชนีความมั่นคงปลอดภัยไซเบอร์โลก (Global Cybersecurity Index : GCI)	ดัชนีชี้วัดระดับของการพัฒนาการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละประเทศ จัดทำโดยสหภาพโทรคมนาคมระหว่างประเทศ(International Telecommunication Union: ITU) ดำเนินการร่วมกับสถาบัน ABI Research (Allied Business Intelligence) ซึ่งมีวัตถุประสงค์เพื่อสร้างแรงจูงใจให้แต่ละประเทศตระหนักถึงการรักษาความมั่นคงปลอดภัยทางไซเบอร์ โดยมีเป้าหมายสูงสุดที่ต้องการทำให้การรักษาความมั่นคงปลอดภัยทางไซเบอร์เป็นวัฒนธรรมของโลกและหลอมรวมให้อยู่ในแก่นของเทคโนโลยีสารสนเทศและการสื่อสาร
ทีมรับมือกับสถานการณ์ฉุกเฉินที่เกี่ยวกับคอมพิวเตอร์ (Computer emergency response team: CERT)	CERT หรือ Computer Emergency Response Team เป็นเครื่องหมายการค้าจดทะเบียนของ CERT Coordination Cente (CERT/CC) หมายถึงหน่วยงานรับมือเหตุภัยคุกคามที่อยู่ภายใต้สถาบันวิศวกรรมซอฟต์แวร์ (Software Engineering Institute – SEI) แห่งมหาวิทยาลัย Carnegie Mellon ในสหรัฐอเมริกา และเนื่องจาก CERT เป็นเครื่องหมายการค้าจดทะเบียน ดังนั้น ศูนย์ที่ทำหน้าที่ประสานและรับมือเหตุภัยคุกคามด้านความมั่นคงทางไซเบอร์ที่จัดตั้งขึ้นใหม่ และต้องการใช้ชื่อที่มีคำว่า CERT จะต้องยื่นขอใบอนุญาตเสียก่อน เช่น ประเทศไทย มี Thai CERT
ทีมรับมือเหตุการณ์ด้านความมั่นคงปลอดภัยคอมพิวเตอร์ (Computer Security Incident Response Team: CSIRT) หรือทีมรับมือสถานการณ์ที่เกี่ยวกับคอมพิวเตอร์ (Computer incident response teams: CIRT)	ศูนย์ประสานการรับมือภัยคุกคามด้านความมั่นคงปลอดภัยไซเบอร์ที่สามารถรับมือและแก้ไขเหตุภัยคุกคาม ซึ่งประกอบด้วยบุคลากรที่มีความรู้และทักษะในการรับมือเหตุภัยคุกคาม ให้ความช่วยเหลือผู้รับบริการในการฟื้นตัวจากการเจาะระบบ นอกจากนี้ในการดำเนินการเชิงรุก CSIRT สามารถให้บริการตรวจสอบและประเมินช่องโหว่ของระบบ

คำศัพท์	ความหมาย
	สารสนเทศและความเสี่ยงต่าง ๆ รวมทั้งสร้างความตระหนักและให้ความรู้แก่ผู้เกี่ยวข้องในการพัฒนาและปรับปรุงการบริการเพื่อให้เกิดความมั่นคงปลอดภัยไซเบอร์



ฉบับภาษาอังกฤษ
English Version

Cyber Security Policy and Action Plan 2022 - 2027



Book Cyber Security Policy and Action Plan 2022 - 2027

By National Cyber Security Agency (NCSA)
Cyber Security Strategy and Policy Office

Notification of the National Cyber Security Committee
Re: Cybersecurity Policy and Action Plan 2022 - 2027

As the Cabinet approved the Resolution on 20 September 2022 for Cybersecurity Policy and Action Plan 2022 - 2027, in accordance with the proposal from the National Cyber Security Committee to establish Cybersecurity Policy and Action Plan 2022 - 2027.

By virtue of Section 9 (1) (2) and (3) and Section 43 of Cybersecurity Act 2019 and Order of the Prime Minister No. 239/2563 Re: Designated and Authorized Deputy Prime Minister and Minister attached to the Prime Minister's Office to Officiate as the Chairman of the Committees according to Laws and Regulations of the Office of the Prime Minister and the above Cabinet's Resolution, therefore, issue the Notification to inform the implementation of Cybersecurity Policy and Action Plan 2022 - 2027 as a Master Plan for Thailand cybersecurity to develop a comprehensive cybersecurity in all dimensions, and to use as a framework guidelines for national cybersecurity conformity with the National Strategy for Security, Sub Strategy of Prevention and Solution for Problems Affecting Security. The goals of developmental guidelines are the existing security problems (cybersecurity) have been resolved to the extent that they do not affect country's administration and development according to the principles attached.

Nevertheless, this notification becomes effective following the publication date in the Royal Gazette.

Published on 13 November 2022
General Prawit Wongsuwan
Deputy Prime Minister, Acting
Chairman of the National Cyber Security Committee

CONTENT

	Page
Part 1 Executive Summary	8
Part 2 Concordance with 3-level Plan, according to the Cabinet's Resolution on 4 December 2017	9
2.1 National Strategy (Level 1 Plan)	9
2.1.1 National Strategy for Security	9
2.1.2 Strategic Issues	9
2.2 Level 2 Plan	9
2.2.1 Master Plan under the National Strategy Security Strategic Issue	9
2.2.2 Reformation Plan for Mass Communication and Information Technology	9
2.2.3 The 12th National Economic and Social Development Plan	10
2.2.4 National Security Policy and Plan (2019 - 2022)	10
2.3 Level 3 related Plan	10
2.3.1 National Digital Development for Economy and Society Policy and Plan (2018 - 2037)	10
2.3.2 5-year Digital Action Plan for Economy and Society (2019 - 2022)	10
2.3.3 National Cybersecurity Strategy (2017 - 2022)	11
2.3.4 National Preparedness Plan (2017 - 2022)	11

Cyber Security Policy and Action Plan 2022 - 2027

CONTENT

	Page
Part 3 Key Aspect of the Cybersecurity Policy and Action Plan 2022 - 2027	12
3.1 Situation Assessment, Problems, and Necessity of Cybersecurity Policy and Action Plan 2022 - 2027	12
3.2 Principle of Cybersecurity Policy and Action Plan 2022 - 2027	13
3.2.1 Strategy 1: Buildup country's ecosystem and cybersecurity capacity for all components: people, knowledge, and technology (Capacity)	13
3.2.2 Strategy 2: Build up synergy via strong partnership and integrated effort (Partnership)	26
3.2.3 Strategy 3: Build up resiliency for government services and critical information infrastructure. (Resilience)	34
3.2.4 Strategy 4: Develop capacity of national agencies to comply with quality and standards. (Standard)	45
Appendix	**65**
Cybersecurity Management Policy for Government Agency and Organization of Critical Information Infrastructure	65

Cyber Security Policy and Action Plan 2022 - 2027
National Cyber Security Agency

Part 1 Executive Summary

This Cybersecurity Policy and Action Plan 2022 - 2027 is executed according to the Cybersecurity Act 2019.

Section 9 (1) legislates the National Cyber Security Committee (NCSC) has the duties and powers to propose a Cybersecurity Policy and Plan, promote and support to maintain cybersecurity in accordance with Section 42 and Section 43 for the Cabinet's approval.

This Cybersecurity Policy and Action Plan is a Master Plan for Thailand cybersecurity to develop a comprehensive cybersecurity in all dimensions, and to use as a framework guideline for maintaining national cybersecurity.

Section 9 (3) legislates the National Cyber Security Committee (NCSC) has the duties and powers to establish a Cybersecurity Action Plan and submit to the Cabinet as a Master Plan for maintaining cybersecurity in a normal situation and in a situation where a Cyber Threats might occur or has occurred. The Plan shall be in line with national policies, strategies, and plans, as well as the security policy framework and master plans of the National Security Council.

Part 2 Concordance with 3-level Plan, according to the Cabinet's Resolution on 4 December 2017

2.1 National Strategy (Level 1 Plan)

2.1.1 National Strategy for Security

- **Objective 3** Readiness of military units, security agency(s), public, private, and civil sectors to prevent and solve security problem(s).
- **Objective 4** Thailand's security role is valued and recognized by international community.
- **Objective 5** Effective security management provides concrete outcomes.

2.1.2 Strategic Issues

4.2 Prevention and solutions to problems affecting security.

4.2.1 Solutions for current security problems

4.2.2 Monitor, observe, prevent, and solve emerging problems that might occur.

2.2 Level 2 Plan

2.2.1 Master Plan under the National Strategy

Security Strategic Issue

3.2 Sub Strategy of Prevention and Solution for Problems Affecting Security

2.2.2 Reformation Plan for Mass Communication and Information Technology

Reformation Plan for Mass Communication and Information Technology Strategic Issue

5.5 Reformation of cybersecurity management/astronautic affairs and mass communication and telecommunication systems and tools for disaster prevention and mitigation tasks under Activity 1 - protect and maintain cybersecurity of critical information infrastructure.

2.2.3 The 12th National Economic and Social Development Plan

● **Strategy 5 Reinforcing National Security for the Country's Progress towards Prosperity and Sustainability**

Development Guideline 3.2 Empower the national armed forces to respond to both traditional and non-traditional security threats.

● **Strategy 7 Advancing Infrastructure and Logistics**

Development Guideline 3.5 Growth of the digital economy

2.2.4 National Security Policy and Plan (2019 - 2022)

Policy 10 Strengthening Cybersecurity - aims to support Objective 3.4.5 to develop government's capability and role, and to empower all sectors in dealing with all kinds of threats affecting security.

Plan 15 Preventing and Resolving cybersecurity problems.

2.3 Level 3 related Plan

2.3.1 National Digital Development for Economy and Society Policy and Plan (2018 - 2037)

● **Strategy 6 Building trust in the use of digital technology**

Program 3 Building public trust in digital technology and online transactions.

2.3.2 5-year Digital Action Plan for Economy and Society (2019 - 2022)

● **Objective 5 Building Confidence**

Implementing Issue 5.1 Promoting cybersecurity

Implementing Issue 5.2 Implementing legal development and digital standards

● **Objective 6 Developing Digital Workforce**

Implementing Issue 6.1 Developing workforces and people to digital period

2.3.3 National Cybersecurity Strategy (2017 - 2022)

Strategic Issue 1 Promotes confidence and trust within all sectors in the execution of all cyber activities.

Strategic Issue 2 Protects critical infrastructure which is managed by information system and develops capability for Cyber Threats response.

Strategic Issue 3 Protects national interests and security from traditional and non-traditional threats.

Strategic Issue 4 Promotes digital economy system.

Strategic Issue 5 Raises awareness and promotes domestic cybersecurity collaboration.

Strategic Issue 6 Promote appropriate cyberspace utilization culture.

Strategic Issue 7 Promotes criminal protection and suppression.

Strategic Issue 8 Promotes Thailand's creativity roles of collaboration to maintain cybersecurity in regional and international level.

2.3.4 National Preparedness Plan (2017 - 2022)

● **Strategy 3 Promotes collaboration and preparation with foreign countries for Cyber Threats response**

Tactic 4 Building relationships and collaboration with foreign countries in preparation for security crises i.e., sabotage, terrorism, cyber security threats, space security threats, emerging infectious diseases in conform with Government policies, National Security Policy and Plan, and related specific security strategies.

Part 3 Key Aspect of the Cybersecurity Policy and Action Plan 2022 - 2027

3.1 Situation Assessment, Problems, and Necessity of Cybersecurity Policy and Action Plan 2022 - 2027

Currently, digital technology plays a vital role in facilitating everyday life. International Telecommunication Union (ITU) Report identified internet users accounted for 51 percent of world population in 2018 and predicted that the number will increase to 70 percent in 2023.

Behavior survey on Thailand's internet users in 2018 conducted by Electronic Transactions Development Agency (ETDA) revealed that Thailand is fully stride into digital society. The average duration of internet utilization is 3 times higher than last year. However, technological advancement, particularly internet usage, comes with challenges and several Cyber Threats whether dissemination of false information, system intrusion, attacking availability of a system, developing malicious software, creating a fake website for malicious intent etc. that will cause damage to the country, business sector and individuals.

According to Thailand Cyber Threats Statistic in 2018 collected by Thailand Computer Emergency Response Team (ThaiCERT) showed that intrusion attempts was the first ranked Cyber Threats which is accounted for 43 percent of total 2,520 incidents.

Additionally, cybersecurity readiness survey in 2016 undertaken by Electronic Transactions Development Agency (ETDA) to analyze situations, problems and obstacles, as well as Thailand's management of Cyber Threats in accordance with the following principles 1) establishment of cybersecurity measures 2) protection of information devices 3) ability to detect threats 4) threat management and 5) system recovery after incidents to discover that more than 500 public and private organizations have low average Cyber Threats management.

Aforementioned Cyber Threats become more frequent and dangerous, while cybersecurity workforce deficiency is affecting the ability to manage, resulting in cyber-attacks that have a significant impact on the national economy. Even though there was an increase in cybersecurity investment, there is still a lack of human resources and domestic cybersecurity innovative products remains; we are currently dependent on foreign human resources and products. Therefore, it is necessary to establish the National Cybersecurity Policy and Action Plan in order to capacity to prevent, cope with and mitigate risks posed by Cyber Threats, as well as respond to threats and restore the system to normal promptly.

3.2 Principle of Cybersecurity Policy and Action Plan 2022 - 2027

This completed Cybersecurity Policy and Action Plan has established cybersecurity visions which is **"Cybersecurity for Thailand's critical services to ensure economic and social sustainability".**

Cybersecurity Policy and Action Plan 2022 - 2027 is the master plan for maintaining cybersecurity in a normal situation and in a situation where a Cyber Threats might occur or has occurred that shall be in line with national policies, strategies, and plans, as well as the security framework policies and master plans of the National Security Council.

To achieve vision and objectives of cybersecurity strategic implementation, there are 4 operational strategies as follows.

3.2.1 Strategy 1: Buildup country's ecosystem and cybersecurity capacity for all components: people, knowledge, and technology (Capacity)

Objective To build a country's cybersecurity capacity by integrating people, knowledge, and technology leading to development of country's cybersecurity innovative products.

Goals

1. Developing cybersecurity personnel to support country requirements.
2. Promoting cybersecurity awareness to personnel in all sectors.
3. Promoting participation to strengthen a country's cybersecurity.
4. Promoting development of country's cybersecurity innovative products.

Tactics 1.1 Increase competent cybersecurity personnel.

1. Developing cybersecurity curriculum; theory and practical, in tertiary education to serve the need of cybersecurity related industry.

2.Developing cybersecurity skills and personnel training; executive and operating level.

- **Tactic's Indicators**

1. There are at least 5 institutes providing cybersecurity curriculum; theory and practical, as a major in tertiary education to serve the need of cybersecurity related industry.

2. No less than 80 percent of cybersecurity personnel; executive and operating level, in Supervising or Regulating Organization agencies and Organization of Critical Information Infrastructure obtain knowledge and skills development.

- **Tactic's Implementing Projects**

1. Project to develop cybersecurity competency framework and training program that promotes certification and accreditation for national and international expertise personnel.
2. Project to enhance cybersecurity profession to recognition.
3. Project to develop cybersecurity personnel by means of promoting cybersecurity major in academic institutes.

Project	**1. Project to develop cybersecurity competency framework and training program that promotes certification and accreditation for national and international expertise personnel**
Procedure Guidelines	1) Create cybersecurity competency framework and training program for cybersecurity experts and non-IT users. Certification, and accreditation for expertise personnel. 2) Create curriculum and subject in response to framework, competency and training program, certification, and accreditation for expertise personnel. 3) Set cybersecurity competency framework and training program for cybersecurity experts and non-IT users as one of the employment /promotion specifications. 4) Form alliance, funding and encourage those agencies who support cybersecurity experts and non-IT users training including certification and accreditation for cybersecurity experts which may consider tax privileges and other promotion measures to increase number of supporting agencies. 5) Promote, propagate, organize training, and provide funding continuously. 6) Regulate, monitor, evaluate, promote, and support continuously.
Responsible Agency	**Main:** NCSA **Supporting:** DGA, ETDA, OCSC, MDES, TPQI, ONDE, VEC, MHESI, RTARF, NDSI, BOI, Supervising or Regulating Organization, and Organization of Critical Information Infrastructure.

Project	2. Project to enhance cybersecurity profession to recognition
Procedure Guidelines	1) Set appropriate and attractive compensation guidelines for cyber security profession. 2) Arrange for promoting and supporting activities, and competition continuously. 3) Counsel with related agencies to set appropriate manpower and compensation guidelines. 4) Propagate and publish role models and inspiration in line of work. 5) Promote and support competent cybersecurity personnel continuously and tangibly. 6) Regulate, monitor, evaluate, promote, and support continuously.
Responsible Agency	**Main:** NCSA **Supporting:** DGA, ETDA, OCSC, TPQI, MHESI, ONDE, VEC, OBEC, MDES, RTARF, NDSI, Budget Bureau, Supervising or Regulating Organization, and Organization of Critical Information Infrastructure.



Project	3. Project to develop cybersecurity personnel by means of promoting cybersecurity major in academic institutes
Procedure Guidelines	1) Create specialized cybersecurity integrated framework in formal education system from secondary, vocational to doctorate level. 2) Create specialized cybersecurity skills curriculum and subjects in formal education system from secondary, vocational to doctorate level. 3) Arrange promoting activities and competition to find competent personnel with ability to research, develop and create cybersecurity products. 4) Improve regulations and procedures to appropriately compensate highly skilled cybersecurity workers. 5) Build cooperation in integration between agencies. 6) Regulate, monitor, evaluate, promote, and support continuously.
Responsible Agency	**Main:** NCSA **Supporting:** DGA, ETDA, OCSC, TPQI, ONDE, VEC, OBEC, MHESI, MDES, RTARF, NDSI, Budget Bureau, Supervising or Regulating Organization, and Organization of Critical Information Infrastructure.

Tactics 1.2 Create cybersecurity awareness and skills.

1. Raising cybersecurity awareness and knowingly.
2. Promoting integrated curriculum in cybersecurity awareness and skills in entire education level.

- **Tactic's Indicators**

1. At least 80 percent of Supervising or Regulating Organization and Organization of Critical Information Infrastructure provide activities to create cybersecurity awareness and knowingly annually.
2. There are integrated curriculums regarding cybersecurity awareness and skills in entire education level.

- **Tactic's Implementing Projects**

1. Project to integrate cybersecurity skills and digital skills in formal education from primary education to postgraduation.
2. Project to create national awareness to different target groups (i.e., general consumers, organizational users, juvenile, business) and in various forms.
3. Project to develop Code of Practices for security of internet connecting devices and products.
4. Project to educate people regarding laws, regulations, risks of cybercrime, and preventive measures.
5. Project to organize the national cyber exercise to prevent, cope with, and reduce risk from Cyber Threats, and test the incident action plan in case of national Cyber Threats crises.



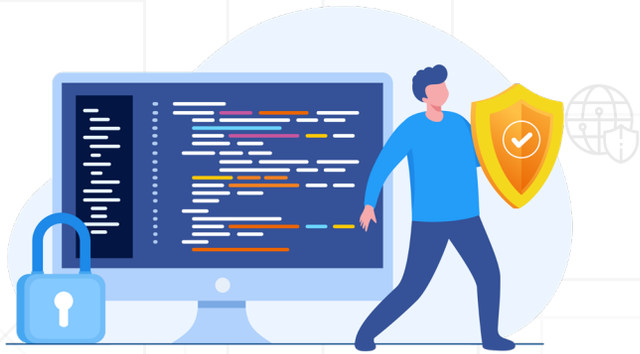
Project	**1. Project to integrate cybersecurity skills and digital skills in formal education from primary education to postgraduation**
Procedure Guidelines	1) Create an integrated framework for cybersecurity skills and digital skills in formal education from primary education to postgraduation. 2) Create curriculum and subject of cybersecurity skills and digital skills in formal education from primary education to postgraduation. 3) Arrange promoting activities and competition to find competent personnel with ability to research, develop and create cybersecurity products. 4) Improv regulations and procedures to include cybersecurity skills as one of the criteria in promoting and hiring consideration. 5) Create integrated collaboration between sectors. 6) Regulate, monitor, evaluate, promote, and support continuously.
Responsible Agency	**Main:** NCSA **Supporting:** DGA, ETDA, OCSC, TPQI, ONDE, VEC, OBEC, MHESI, MDES, Supervising or Regulating Organization, and Organization of Critical Information Infrastructure.

Project	**2. Project to create national awareness to different target groups (i.e., general consumers, organizational users, juvenile, business) and in various forms**
Procedure Guidelines	1) Create program framework to raise national awareness with campaigns targeted for various target groups (i.e., general consumers, organizational users, juvenile, business) 2) Create programs' curriculum and subjects to raise awareness for different target groups. 3) Arrange promoting activities to propagate national awareness for targeted groups through various channels such as series, advertisements, cartoons, music, or other media including rewarding activities. 4) Develop platform to propagate the national awareness raising program. 5) Support participation and may consider tax privileges and other promotional measures to increase number of supporting agencies. 6) Regulate, monitor, evaluate, promote, and support continuously.
Responsible Agency	**Main:** NCSA **Supporting:** DGA, ETDA, ONDE, VEC, OBEC, MHESI, MDES, Supervising or Regulating Organization, and Organization of Critical Information Infrastructure.



Project	**3. Project to develop Code of Practices for security of internet connecting devices and products**
Procedure Guidelines	1) Create Code of Practices for security of internet connecting devices and products. 2) Support, publicize, and educate practices. 3) Support participation and may consider tax privileges and other promotional measures to increase the number of supporting agencies. 4) Educate related skills for governmental officers. 5) Regulate, monitor, evaluate, promote, and support continuously.
Responsible Agency	**Main:** NCSA **Supporting:** DGA, ETDA, OCSC, TPQI, ONDE, VEC, OBEC, MHESI, MDES, DTI, RTARF, BOI, Supervising or Regulating Organization, and Organization of Critical Information Infrastructure.
Project	**4. Project to educate people regarding laws, regulations, risks of cybercrime, and preventive measures**
Procedure Guidelines	1) Annually consider laws, regulations, and risk of cybercrime and preventive measures to educate people. 2) Create, improve, or establish guidelines to educate people regarding laws, regulations, risk of cybercrime, and preventive measures. 3) Publicize and educate practices. 4) Regulate, monitor, evaluate, promote, and support continuously.
Responsible Agency	**Main:** NCSA **Supporting:** RTP, DGA, ETDA, OCSC, TPQI, ONDE, VEC, OBEC, MHESI, MDES, Supervising or Regulating Organization, and Organization of Critical Information Infrastructure.

Project	**5. Project to organize the national cyber exercise to prevent, cope with, and reduce risk from Cyber Threats, and test the incident action plan in case of national Cyber Threats crises**
Procedure Guidelines	1) Organize the meeting for exercise planning. 2) Organize the meeting for exercise development. 3) Organize for pre-exercise/academic. 4) Organize training for testing cyber competency in form of Staff Exercise: Staff-Ex, Command Post Exercise: CPX, or Field Training Exercise: FTX. 5) Prepare training conclusion report.
Responsible Agency	**Main:** NCSA **Supporting:** Supervising or Regulating Organization, and Organization of Critical Information Infrastructure.



Tactics 1.3 Promote Cybersecurity Research and Development and Innovation

1. Promote cybersecurity study, research, development, and innovation.

2. Promote collaboration of research and development among domestic and international agencies.

3. Promote cybersecurity investment.

4. Promote cybersecurity product development as innovation and commercialization.

- **Tactic's Indicators**

1. There is at least 1 study, research, development, and innovation annually.

2. There are at least 10 collaborations on research and development between domestic and international research institutions.

3. There are at least 50 percent of Organization of Critical Information Infrastructure invest in cybersecurity.

4. There are innovative cybersecurity products which can be commercialized.

- **Tactic's Implementing Projects**

1. Project to promote and support, funding and prepare platform for cybersecurity research and development, innovation, and science and technology.

2. Project to promote and support development of solutions business, and cybersecurity products as domestic innovation.

3. Project to establish National Cyber Security Agency Cyber Security Lab.

Project	**1. Project to promote and support, funding and prepare platform for cybersecurity research and development, innovation, and science and technology**
Procedure Guidelines	1) Establish Centers of Excellence or Cybersecurity Research Center. 2) Publish an annually White Paper to inform national cybersecurity research and development direction and guideline and to use as a development and funding guideline. 3) Promote collaboration in form of fund raising. 4) Develop forum or platform for research and development for public and private collaboration. 5) Publish cyber science and technology tactics. 6) Fund and support cyber science and technology research. 7) Promote Thai people, students, and researchers to increase quantity of Thai cyber specialists. 8) Support budget on research for identifying and supplying innovative solutions for the certain most urgent cybersecurity problems. 9) Promote participation and may consider tax privileges and other promotional measures to increase the number of supporting agencies. 10) Regulate, monitor, evaluate, promote, and support continuously.
Responsible Agency	**Main:** NCSA **Supporting:** DGA, ETDA, OCSC, ONDE, VEC, OBEC, MHESI, MDES, DTI, RTARF, BOI, Supervising or Regulating Organization, and Organization of Critical Information Infrastructure.

Project	**2. Project to promote and support development of solutions business, and cybersecurity products as domestic innovation**
Procedure Guidelines	1) Create policy and guidelines to promote development of solution business and cybersecurity products as domestic innovation. 2) Educate and collaborate with cybersecurity startup in Thailand by collaborate with researchers, university, domestic and international leading companies. 3) Create brands and credibility of cybersecurity solutions and products which are domestic innovation. 4) Promote utilization of cybersecurity solutions and products which are domestic innovation by granting privileges and sponsorships. 5) Support participation and may consider tax privileges and other promotional measures to increase number of supporting agencies. 6) Regulate, monitor, evaluate, promote, and support continuously.
Responsible Agency	**Main:** NCSA **Supporting:** DGA, ETDA, OCSC, TPQI, ONDE, VEC, OBEC, MHESI, MDES, DTI, RTARF, BOI, Supervising or Regulating Organization, and Organization of Critical Information Infrastructure.



Project	3. Project to establish National Cyber Security Agency Cyber Security Lab
Procedure Guidelines	1) Create framework for operational and action plan of the project with details, timing, and person in charge. 2) Procure additional tools and install at NCSA. 3) Perform system test and adjust according to requirements. 4) Arrange training for related officers to be able to use the tools efficiently. 5) Perform Penetration Test with at least 15 target agencies to report vulnerability to respective agencies and conduct preventive measures and perform digital forensics for at least 10 agencies that have been attacked by cyber-attacks.
Responsible Agency	**Main:** NCSA **Supporting:** Supervising or Regulating Organization, and Organization of Critical Information Infrastructure.

3.2.2 Strategy 2: Build up synergy via strong partnership and integrated effort (Partnership)

Objective To integrate domestic and international collaboration in preparation for Cyber Threats response and prompt recovery of critical services to normal operations

Goals

1. There is synchronized coordination between public and domestic private agencies to promptly prepare for Cyber Threats response and recovery to normal operations.

2. There is synchronized coordination with international agencies to promptly prepare for Cyber Threats response and recovery to normal operations.

Tactics 2.1 Promote and support public - private partnership.

1. Identify participative stakeholders to create collaboration between public and private sectors.

2. Set clear governance structure and functional mechanism to create collaboration and coordination between public and private sectors.

3. Create collaboration between government agencies.

4. Maintain balance between cybersecurity and personal data protection.

5. Support the potential development for government officers relating to cybersecurity law enforcement.

- **Tactic's Indicators**

1. There are at least 3 collaborative activities between public and private sectors annually.

2. There are clear governance structures, collaboration and coordination mechanisms between government agencies, public and private sectors, and private agencies.

3. There are at least 3 collaborative activities between government agencies annually.

4. There are collaborative guidelines between cybersecurity and personal data protection agencies.

5. Cybersecurity law enforcement officers receive at least 1 potential development annually.

- **Tactic's Implementing Projects**

1. Project to promote and support collaboration between public and private sectors to promptly identify and respond to cybercrime related problems.

2. Project to collaborate with business sectors, emphasizing on business communities to combine cybersecurity to organization risk management.

3. Project to support national cybersecurity capacity building (i.e., specific joint operational framework to counter cyber-attacks, joint operation among officers from several agencies such as policemen, and judicial officers, forensic specialists).

4. Project to enhance partnership with personal data protection agencies to create operational guidelines in accordance with security regulations and personal data protection practices.

Project	**1. Project to promote and support collaboration between public and private sectors to promptly identify and respond to cybercrime related problems**
Procedure Guidelines	1) Promote and support creation of collaboration framework between public and private sectors including international collaboration to promptly identify and respond to cybercrime related problems. 2) Create guidelines in accordance with operational framework. 3) Publish and provide knowledge of practices. 4) Provide related skills for government officers. 5) Regulate, monitor, evaluate, promote, and support continuously.
Responsible Agency	**Main:** NCSA **Supporting:** DGA, ETDA, RTP, Supervising or Regulating Organization, and Organization of Critical Information Infrastructure.
Project	**2. Project to collaborate with business sectors, emphasizing on business communities to combine cybersecurity to organization risk management**
Procedure Guidelines	1) Create guidelines to collaborate with business communities to combine cybersecurity with organization risk management. 2) Create or improve related laws and regulations. 3) Support, publish and provide knowledge of practices. 4) Provide related skills for government officers. 5) Regulate, monitor, evaluate, promote, and support continuously.
Responsible Agency	**Main:** NCSA **Supporting:** DGA, ETDA, MDES, ONDE, DEPA, Supervising or Regulating Organization, and Organization of Critical Information Infrastructure.

Project	**3. Project to support national cybersecurity capacity building (i.e., specific joint operational framework to counter cyber-attacks, joint operation among officers from several agencies such as policemen, and judicial officers, forensic specialists)**
Procedure Guidelines	1) Create specific collaborative operational framework to counter cyber-attacks and develop specific training for joint operation between officers from several agencies. 2) Create guidelines in accordance with operational framework. 3) Publish and provide knowledge of practices. 4) Provide related skills for government officers. 5) Regulate, monitor, evaluate, promote, and support continuously.
Responsible Agency	**Main:** NCSA **Supporting:** DGA, ETDA, RTP, OAG, MOJ, MOD, RTARF, Supervising or Regulating Organization.



Project	**4. Project to enhance partnership with personal data protection agencies to create operational guidelines in accordance with security regulations and personal data protection practices**
Procedure Guidelines	1) Create joint operational framework with personal data protecting agencies to establish guidelines in conform with security regulations and personal data protecting regulations. 2) Create or improve related laws and regulations. 3) Support, publish and provide knowledge of practices. 4) Provide related skills for government officers. 5) Regulate, monitor, evaluate, promote, and support continuously.
Responsible Agency	**Main: NCSA** **Supporting:** DGA, ETDA, MDES, PDPC, Supervising or Regulating Organization.



Tactics 2.2 Coordinate international collaboration to address Cyber Threats

1. Set cybersecurity as an important issue in Foreign Policy.
2. Participate in international cybersecurity conferences.
3. Create international cybersecurity collaboration in all dimensions.
4. Develop national strategy in conform with international guidelines.
5. Support potential development for cybersecurity and other law enforcement personnel to effectively operate in conjunction with related international agencies.

- **Tactic's Indicators**
  1. Set cybersecurity as a Foreign Policy.
  2. Enroll in international cybersecurity conferences in all frameworks.
  3. There are all-dimensions international cybersecurity collaborations i.e., law enforcement, Cyber Threats information exchanging etc.
  4. There are development of national strategy to be in conform with international guidelines.
  5. There is a minimum of 1 activity annually, to potentially develop cybersecurity and other law enforcement personnel to be able to jointly operate with related international agencies effectively.
- **Tactic's Implementing Projects**
  1. Project to support international cybersecurity capacity building.
  2. Project to promote and support the exchange of Cyber Norms and related laws.
  3. Project to promote and support collaboration and participation in important ASEAN and international projects to create cyber capability.

Project	**1. Project to support international cybersecurity capacity building**
Procedure Guidelines	1) Promote and support the establishment of operational framework to counter specific cybercrime, develop specific training for joint international operation among officers from respective agencies. 2) Create guidelines in conform with operational framework. 3) Publish and provide knowledge of practices. 4) Provide related skills for government officers. 5) Regulate, monitor, evaluate, promote, and support continuously.
Responsible Agency	**Main:** NCSA **Supporting:** DGA, ETDA, RTP, MFA, Supervising or Regulating Organization, and Organization of Critical Information Infrastructure.
Project	**2. Project to promote and support the exchange of Cyber Norms and related laws**
Procedure Guidelines	1) Set supporting framework for the exchange Cyber Norms and related laws. 2) Create supporting guidelines for the exchange of Cyber Norms and related laws. 3) Publish and provide knowledge of practices. 4) Provide related skills for government officers. 5) Regulate, monitor, evaluate, promote, and support continuously.
Responsible Agency	**Main:** NCSA. **Supporting:** DGA, ETDA, MFA, Supervising or Regulating Organization, and Organization of Critical Information Infrastructure.

Project	**3. Project to promote and support collaboration and participation in important ASEAN and international projects to create cyber capability**
Procedure Guidelines	1) Set supporting framework for collaboration and participation in important ASEAN and international projects to create cyber capability. 2) Create supporting guidelines for collaboration and participation in important ASEAN and international projects to create cyber potentiality. 3) Publish and provide knowledge of practices. 4) Provide related skills for government officers. 5) Regulate, monitor, evaluate, promote, and support continuously.
Responsible Agency	**Main:** NCSA **Supporting:** DGA, ETDA, MFA, Supervising or Regulating Organization, and Organization of Critical Information Infrastructure.



3.2.3 Strategy 3: Build up resiliency for government services and critical information infrastructure. (Resilience)

Objective To promote cybersecurity and resilience for government services and critical information infrastructure

Goals

1. There are sets of regulatory structures and legal framework for government agencies and Organization of Critical Information Infrastructure.
2. There are sets of minimum-security measures for government agencies and Organization of Critical Information Infrastructure.
3. There is protection for information systems and government agency networks.

Tactics 3.1 Set minimum security measure for Organization of Critical Information Infrastructure (CII).

1. Protect critical information infrastructure by identifying type of critical information infrastructure and setting measures for mitigating risk from Cyber Threats.
2. Set criteria for minimum cybersecurity.
3. Promote and support principles of Security by Design.
4. Promote and support cybersecurity awareness for all-level personnel.

- **Tactic's Indicators**

1. There are protection for Organization of Critical Information Infrastructure and creation of measures to mitigate risks from Cyber Threats in accordance with NCSA's Notification.
2. There are criteria for cybersecurity minimum standard for Organization of Critical Information Infrastructure.
3. Security by Design for Organization of Critical Information Infrastructure was promoted and supported.

4. There are promotions for at least 80 percent of all-level personnel in Organization of Critical Information Infrastructure to have cybersecurity awareness.

- **Tactic's Implementing Projects**

1. Project to develop standard Code of Practices and Code of Conduct, and Audit and Compliance Procedures.
2. Project to promote and support Security by Design.
3. Project to promote and support to raise awareness specific for targeted CII (top executives and officers).
4. Project to implement cybersecurity plan, strategy, policy, potential development activities, and cyber operating procedures in conform with international standards of Organization of Critical Information Infrastructure.

Project	**1. Project to develop standard Code of Practices and Code of Conduct, and Audit and Compliance Procedures**
Procedure Guidelines	1) Create and develop standard Code of Practices, Code of Conduct, Policies and Guideline, and Audit and Compliance Procedures. 2) Policies and Guideline shall be in collaboration with standard organization i.e., ISO or NIST as well as internal agency i.e., ETDA to acquire the credibility of Policies and Guideline and to avoid cause of confusion for officers or Organization of Critical Information Infrastructure. 3) Create Code of Practices guidelines for each sector. 4) Assistance for business in compliance with. 5) Regulate, monitor, evaluate, promote, and support continuously.
Responsible Agency	**Main:** NCSA **Supporting:** DGA, ETDA, Supervising or Regulating Organization, and Organization of Critical Information Infrastructure.

Project	**2. Project to promote and support Security by Design**
Procedure Guidelines	1) Create principles for Security by Design. 2) Create related regulations, policies, and guidelines. 3) Publish and provide knowledge of practices. 4) Regulate, monitor, evaluate, promote, and support continuously.
Responsible Agency	**Main:** NCSA **Supporting:** DGA, ETDA, OCSC, Supervising or Regulating Organization, and Organization of Critical Information Infrastructure.
Project	**3. Project to promote and support to raise awareness specific for targeted CII (top executives and officers)**
Procedure Guidelines	1) Create program framework to raise awareness specific for target CII (top executives and officers) 2) Create related regulations, policies, and guidelines, which are as part of duty and career promotion. 3) Publication. 4) Regulate, monitor, evaluate, promote, and support continuously.
Responsible Agency	**Main:** NCSA **Supporting:** DGA, ETDA, OCSC, Supervising or Regulating Organization, and Organization of Critical Information Infrastructure.

Project	**4. Project to implement cybersecurity plan, strategy, policy, potential development activities, and cyber operating procedures in conform with international standards of Organization of Critical Information Infrastructure**
Procedure Guidelines	1) Study and review the 2 curriculums; Lead Implementor and Lead Auditor, to develop cyber operational capability in conform with international standards of Organization of Critical Information Infrastructure. 2) Organize Focus Group hearing for Lead Implementor and Lead Auditor curriculums. 3) Organize public hearing for Lead Implementor and Lead Auditor curriculums. 4) Organize workshops for Lead Implementor and Lead Auditor curriculums. 5) Create website for Lead Implementor and Lead Auditor online curriculums.
Responsible Agency	**Main: NCSA** **Supporting:** Supervising or Regulating Organization, and Organization of Critical Information Infrastructure.



Tactics 3.2 Establishment of regulatory structure and legal framework for Organization of Critical Information Infrastructure.

1. Create risk management approaches to protect critical information infrastructure.

2. Develop regulatory guideline mechanisms for Organization of Critical Information Infrastructure and consider Data & Cloud Computing as a regulated critical information infrastructure subsequently.

3. Develop and modernize related cybersecurity laws and regulations.

- **Tactic's Indicators**

1. There are risk management approaches to protect critical information infrastructure.

2. There are regulated mechanisms and guidelines for Organization of Critical Information Infrastructure.

3. There are modern cybersecurity laws and regulations.

- **Tactic's Implementing Projects**

1. Project to support rules and regulations for cybersecurity.

2. Project to develop legal operational framework for critical information infrastructure (Guideline and Regulation).

3. Project to develop integration mechanisms for cyber-risk incidents, CII operational status, and international laws/tendency to rectify or create immediate legal consequences.



Project	**1. Project to support rules and regulations for cybersecurity**
Procedure Guidelines	1) Review of cybersecurity supporting rules and regulations i.e., inter-agency operations, terms of references and coordination, information exchange, confidentiality and personal data protection, operating officers' protection, digital evidence's collection, utilization, and protection which is used in Court etc. 2) Prepare or improve cybersecurity supporting rules and regulations. 3) Publish and provide knowledge of the practices. 4) Regulate, monitor, evaluate, promote, and support continuously.
Responsible Agency	**Main:** NCSA **Supporting:** MOJ, DGA, ETDA, Supervising or Regulating Organizations.



Project	**2. Project to develop legal operational framework for critical information infrastructure (Guideline and Regulation)**
Procedure Guidelines	1) Establish cybersecurity management guidelines for governance and risk management. 2) Adopt a governance model with clear responsibilities for government sector and other related in protection of critical infrastructures (Cis) and critical information infrastructures (CIIs). 3) Establish related regulations. 4) Support establishment of public-private partnerships and utilize a wide range of market levers. 5) Publish and provide knowledge of the practices. 6) Regulate, monitor, evaluate, promote, and support continuously.
Responsible Agency	**Main:** NCSA **Supporting:** DGA, ETDA, Supervising or Regulating Organizations.



Project	**3. Project to develop integration mechanisms for cyber-risk incidents, CII operational status, and international laws/tendency to rectify or create immediate legal consequences**
Procedure Guidelines	1) Establish integration mechanisms for cyber-risk incidents, CII operational status, and international laws/tendency to rectify or create immediate legal consequences. 2) Establish related regulations. 3) publish and provide knowledge of the Practices. 4) Regulate, monitor, evaluate, promote, and support continuously.
Responsible Agency	**Main:** NCSA **Supporting:** MOJ, MFA, DGA, ETDA, Supervising or Regulating Organizations.

Tactics 3.3 Protection of Government information systems and networks.

1. Regulate government agencies to follow minimum security standard policies.

2. Implement risk assessment from technology utilization to ensure security by default.

3. Establish mutual cybersecurity operational aspects.

4. Prepare personnel, information, technology, and procedures to handle modern Cyber Threats.

- **Tactic's Indicators**

1. Government agencies' minimum security standard policies operating rate must increase at least 10 percent annually.

2. Implementation of risk assessment from technology utilization to ensure security by default must increase at least 10 percent annually.

3. There must be at least 1 mutual cybersecurity operation annually.

4. There must be at least 1 activity/project to prepare personnel, information, technology, and procedures to handle modern Cyber Threats annually.

- **Tactic's Implementing Projects**

1. Project to promote and support technology utilization for security by default.

2. Project to develop and regulate minimum security standards for government services (i.e., standard cybersecurity regulations included in government information technology contracts).

3. Project to create whole management for governmental-operating networks.

Project	**1. Project to promote and support technology utilization for security by default**
Procedure Guidelines	1) Create code of practice for "security by default". 2) Create supporting measures for hardware and software services in line with code of practice for "security by default". 3) Market stimulation survey through new products security score. 4) Publish and provide knowledge of the practices. 5) Regulate, monitor, evaluate, promote, and support continuously.
Responsible Agency	**Main:** NCSA **Supporting:** DGA, ETDA, Supervising or Regulating Organization, and Organization of Critical Information Infrastructure.

Project	**2. Project to develop and regulate minimum security standards for government services (i.e., standard cybersecurity regulations included in government information technology contracts)**
Procedure Guidelines	1) Develop minimum security standards for government services i.e., standard cybersecurity regulations included in government information technology contracts, guidelines and criteria of contractors and products risk assessment, Backdoor Policy, and Vendor lock-in risk assessment. 2) Establish related regulations. 3) Publish and provide knowledge of the practices. 4) Regulate, monitor, evaluate, promote, and support continuously.
Responsible Agency	**Main:** NCSA **Supporting:** DGA, ETDA, Supervising or Regulating Organizations.



Project	**3. Project to create whole management for governmental-operating networks**
Procedure Guidelines	1) Create whole management for governmental-operated networks i.e., establish department central agency to connect, set terms of references, coordinate inter-agency from departments to ministry, inter-ministry coordination, centralize or decentralize operation, and collaborations. 2) Create platform for whole management of governmental-operated networks. 3) Improve and support access to cyber specialists in government agencies. 4) Publish and provide knowledge of the practices. 5) Regulate, monitor, evaluate, promote, and support continuously.
Responsible Agency	**Main:** NCSA **Supporting:** DGA, ETDA, Supervising or Regulating Organization, and Organization of Critical Information Infrastructure.



3.2.4 Strategy 4: Develop capacity of national agencies to comply with quality and standards. (Standard)

Objective Emphasis on developing the capacity of national agencies to comply with quality and standards for effective cybersecurity management.

Goals and Indicators

1. There is an integrated cybersecurity management at the national level.
2. The qualified and standardized primary and secondary agencies can collaborate in integrated operations.
3. There are protective, handling, and mitigating risk measures for Cyber Threats.
4. Cyber Threats information is exchanged effectively.
5. Organization of Critical Information Infrastructure have effective cybersecurity measures.

Tactics 4.1 Increase capability in handling and response to cybersecurity related incidents.

1. Study and review current cybersecurity policies, laws, and capabilities to set national cybersecurity developmental guidelines.
2. Set strategic implementing mechanisms, decision-making procedures, responsibilities division, coordinate with the related agencies, operational guidelines, and operation monitoring and evaluation.
3. Promote potential development for people, process, and technology to entrust stakeholders. Implementation of best practices and standards; perchance by certification and accreditation of important operations.
4. Develop contingency plan for cyber emergency incidents to handle and restore critical information infrastructure by establishing Computer Security Incident Response Team: CSIRT, including cybersecurity incident response exercise.

- **Tactic's Indicators**

1. There are reviews on current cybersecurity policies, laws, and capabilities to set national cybersecurity developmental guidelines.
2. There are operational monitoring guidelines.
3. Promotion of potential development for people, process, and technology to increase standardized quality by at least 10 percent annually.
4. There are preparedness plans for cybersecurity emergencies incidents to handle and restore critical information infrastructure. There is establishment of Computer Security Incident Response Team: CSIRT with at least 1 cybersecurity exercise.

- **Tactic's Implementing Projects**

1. Project to promote and support National Cyber Security Agency (NCSA) operations to attain quality and standards.
2. Project to increase capabilities of National Cyber Security Agency (NCSA).
3. Project to improve cybersecurity laws, rules, and regulations.
4. Project to integrate threats discovery, analysis, and response to related cybersecurity incidents.
5. Project to establish emergency plan to manage cybersecurity crises.
6. Project to organize and execute cybersecurity exercise.
7. Project to intercept threats in telecommunication providers' level.
8. Project to promote and support the combination of cybersecurity products and other services.
9. Project to implement cybersecurity plans, strategies, and policies through cybersecurity self-assessment.
10. Project to organize national cyber exercise for protecting, handling, and reducing risk from Cyber Threats through establishment of national incident response plan.
11. Project to establish Sectoral CERT and to develop the cybersecurity platform for Sectoral CERT to response to computer emergencies incidents in Public Health agencies.

Project	**1. Project to promote and support National Cyber Security Agency (NCSA) operations to attain quality and standards**
Procedure Guidelines	1) Establishment of National Computer Emergency Response Team (National CERT). 2) Development of supporting system of National Cyber Security Agency (NCSA) 3) Establishment of a technical data analysis laboratory for penetration testing, forensics, Sector CERT testing, Cyber Threats Intelligence Fusion Center, CPT (Cyber Protection Team) equipment and tools 4) Establishment of a Help desk in the National Computer Emergency Response Team. 5) Establishment of cybersecurity co-operational center for each critical information infrastructure organization of National Cyber Security Agency (NCSA). 6) Implementation of good practices and standards in the operations. Certification and accreditation for important operations i.e., ISO/IEC 27001, ISO 22301, ISO/IEC 20000-1, ISO/IEC 385 0 0 etc. 7) Establishment of real-time system to regulate, monitor, evaluate, promote, and support continuously. 8) Regulate, monitor, evaluate, promote, and support continuously. 9) Appoint Supervising or Regulating Organization for each Critical Information Infrastructure sector, promote and support Critical Information Infrastructure sector operations, appoint regional support agency i.e., private university, educational institutes, specialized agencies etc. to support Critical Information Infrastructure sectors. 10) Regulate, monitor, evaluate, promote, and support continuously.
Responsible Agency	**Main:** MDES, NCSA **Supporting:** RTARF, MOD, RTP, Supervising or Regulating Organization.

Project	2. Project to increase capabilities of National Cyber Security Agency (NCSA)
Procedure Guidelines	1) Establishment of Cyber Protection Team: CPT 2) Cyber skills development training for executives and operators of National Cyber Security Agency. 3) Procurement of Cyber Threats exercise system. 4) Establishment of Cybersecurity Training Center. 5) Procurement of Cybersecurity Learning Platform. 6) Increase of governance competency by establishment of "National Cyber Community" with regulators and CII operating representatives as members. The objective is the exchange of knowledge and ideas to operate according to cybersecurity action plan, policy, management, code of practices, and standard framework including other operational guidelines that might occur subsequently. 7) Promote and support alliances with security support to assist in operations. Allies should be from various agencies and regions. 8) Regulate, monitor, evaluate, promote, and support continuously.
Responsible Agency	**Main:** MDES, NCSA **Supporting:** RTARF, MOD, RTP, ONDE, DTI, MHESI, DEPA, Supervising or Regulating Organization, Organization of Critical Information Infrastructure.



Project	3. Project to improve cybersecurity laws, rules, and regulations
Procedure Guidelines	1) Revision or guidelines to create cybersecurity laws. 2) Establish, improve, or create cybersecurity laws. 3) Publish and provide knowledge of the practices. 4) Provide related skills for government officers. 5) Regulate, monitor, evaluate, promote, and support continuously.
Responsible Agency	**Main:** NCSA **Supporting:** MOJ, MOD, RTP, DGA, ETDA, Supervising or Regulating Organization

Project	4. Project to integrate threats discovery, analysis, and response to related cybersecurity incidents
Procedure Guidelines	1) Establish operational framework to collaborate threats discovery. 2) Analysis and responses to cybersecurity related incidents. 3) Create incidental cybersecurity report mechanisms from all sectors. 4) Develop incidental cybersecurity report mechanisms and the analysis and semi-automatic or automatic responses. 5) Personnel development for analysis and responses to cybersecurity related incidents. 6) Regulate, monitor, evaluate, promote, and support continuously.
Responsible Agency	**Main:** NCSA **Supporting:** Supervising or Regulating Organization.

Project	**5. Project to establish emergency plan to manage cybersecurity crises**
Procedure Guidelines	1) Establishment of framework to create contingency plans for national cybersecurity crises management to prepare for the national emergency or crises, especially critical information infrastructure, considering evaluating results, and national and sectoral risks affecting critical information infrastructure. 2) Promote and provide knowledge to related agencies. 3) Review and improve contingency plans creation framework for cybersecurity crises management. 4) Regulate, monitor, evaluate, promote, and support continuously.
Responsible Agency	**Main:** NCSA **Supporting:** NSC, RTARF, Supervising or Regulating Organization.

Project	**6. Project to organize and execute cybersecurity exercise**
Procedure Guidelines	1) Establish guidelines for cybersecurity exercise. 2) Publish and announce guidelines for cybersecurity exercise. 3) Conduct cybersecurity exercise among sectors. 4) Expand cybersecurity exercise to international level. 5) Regulate, monitor, evaluate, promote, and support continuously.
Responsible Agency	**Main:** NCSA **Supporting:** DGA, ETDA, NSC, RTARF, Supervising or Regulating Organization.

Project	**7. Project to intercept threats in telecommunication providers' level**
Procedure Guidelines	1) Establish framework to intercept Cyber Threats with telecommunication providers. 2) Establish guidelines according to operational framework. 3) Support, publish, and provide knowledge of the practices. 4) Establish supporting guidelines to prevent Cyber Threats upon government agencies request. 5) Regulate, monitor, evaluate, promote, and support continuously.
Responsible Agency	**Main:** NCSA **Supporting:** NBTC



Project	8. Project to promote and support the combination of cybersecurity products and other services
Procedure Guidelines	1) Establish guidelines to add cybersecurity products to other offers, products, or services to combine, use, or service with other government and Critical Information Infrastructure (CII) critical services. The guidelines and criteria for risks determination shall take security in consideration during providers and products procurement throughout Third Party Risk Management Life Cycle i.e., backdoor policy to confirm that there are no hidden threats in the products or services, third party/vendor locked-in to avoid monopoly that might cause change restriction i.e., technology, providers, or partnerships and restrictions to reinstate system or information to operate by the agency etc. which need necessary laws, rules and regulations to enforce combinations of cybersecurity products to other service offerings. 2) Establish necessary laws, rules, and regulations to enforce cybersecurity products and other services combination. 3) Provide operating knowledge. 4) Regulate, monitor, evaluate, promote, and support continuously.
Responsible Agency	**Main:** NCSA **Supporting:** DGA, ETDA, Supervising or Regulating Organization.

Project	9. Project to implement cybersecurity plans, strategies, and policies through cybersecurity self-assessment
Procedure Guidelines	1) Develop activity processes, practices, and an action plan. 2) Study conceptual framework, tools, or model from domestic and international secondary information for cyber security self-assessment. 3) Establish conceptual framework, tools, or model for cyber security self-assessment for government agencies, and Organization of Critical Information Infrastructure. 4) Organize electronic focus group meetings with distinguished panels or experts from government agencies who are not Organization of Critical Information Infrastructure, Supervising or Regulating Organization, or related agencies. 5) Provide electronic questionnaires for Cyber Security Self-Assessment. 6) Analyze information technology security examination and prepare cybersecurity proficiency evaluation report.
Responsible Agency	**Main:** NCSA **Supporting:** Government Agency, Supervising or Regulating Organization, and Organization of Critical Information Infrastructure.

Project	**10. Project to organize national cyber exercise for protecting, handling, and reducing risk from Cyber Threats through establishment of national incident response plan**
Procedure Guidelines	1) Establish projects' activities action plans with details, duration, and person in charge. 2) Study and analyze domestic and international information to establish policies, plans, administrative policies, and action plans. 3) Presentation of action plan, analysis conclusion, delegation of duties to related agencies. 4) Publicize the projects to government sectors, Organization of Critical Information Infrastructure, or related agencies. 5) Organize meetings and workshops to prepare incident response plans for each Cyber Threats level. 6) Conclusion of the project.
Responsible Agency	**Main:** NCSA **Supporting:** Government Agency, Supervising or Regulating Organization, and Organization of Critical Information Infrastructure.



Project	**11. Project to establish Sectoral CERT and to develop the cybersecurity platform for Sectoral CERT to response to computer emergencies incidents in Public Health agencies**
Procedure Guidelines	1) Establish terms of references and scope of work. 2) Collect information and requirements from each Public Health critical information infrastructure organization. 3) Conduct procurement. 4) Conduct cybersecurity system installation for National Cyber Security Agency and Organization of Critical Information Infrastructure. Conduct personnel training. 5) Enable the system. 6) Conclude and evaluate the project.
Responsible Agency	**Main:** NCSA **Supporting:** Public Health Organization of Critical Information Infrastructure.



Tactics 4.2 Promote and Support threats information sharing.

1. Establish exchanging mechanisms for Cyber Threats information, intelligence, and knowledge.
2. Establish reporting mechanisms for Cyber Threats incident.
3. Establish stakeholders' involvement in Cyber Threats information sharing.

- **Tactic's Indicators**

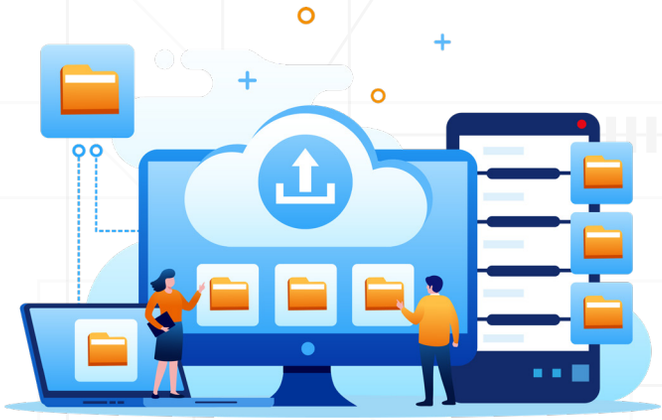
1. There is exchange of Cyber Threats information, intelligence, and knowledge.
2. There are Cyber Threats incident reports which can identify causes and reduce Cyber Threats incidents.
3. There are Cyber Threats information sharing among stakeholders.

- **Tactic's Implementing Projects**

1. Project to establish information sharing between government and private sectors and to facilitate cybersecurity information sharing.
2. Project to promote and support international Cyber Threats information sharing.
3. Project to develop Cyber Threats incidents receive and sharing platform.

Project	**1. Project to establish information sharing between government and private sectors and to facilitate cybersecurity information sharing**
Procedure Guidelines	1) Create information sharing mechanisms between government and private sectors, and between Organization of Critical Information Infrastructure, sector CERT and security agency. 2) Develop cybersecurity incidents report and sharing platform across sector CERT. 3) Develop automatic information sharing system. 4) Regulate, monitor, evaluate, promote, and support continuously.
Responsible Agency	**Main:** NCSA **Supporting:** DGA, ETDA, MOD, RTP, Supervising or Regulating Organization

Projectt	**2. Project to promote and support international Cyber Threats information sharing**
Procedure Guidelines	1) Create regional and international information sharing mechanisms, facilitate cybersecurity information sharing. Establish information sharing mechanisms to exchange operational intelligence and Cyber Threats information. 2) Create regional and international automatic information sharing platform and system (i.e., automatic cybersecurity alert upon cyber-attacks or cyber-attacks) with multi-directional threat-sharing platform. 3) Increase regional and international threats information sharing capacity continuously. 4) Regulate, monitor, evaluate, promote, and support continuously.
Responsible Agency	**Main:** NCSA **Supporting:** DGA, ETDA, MOD, RTP, Supervising or Regulating Organizations.



Project	**3. Project to develop Cyber Threats incidents receive and sharing platform**
Procedure Guidelines	1) Establish conceptual framework for the operation and action plan with details, duration, and person in charge. 2) Create system guidelines documents and connect MISP to agencies. - SOP (Standard Operating Procedure) for information sharing - MISP Utilization and Connection Agreement 3) Provide knowledge for SOP information sharing. 4) Provide central MISP access permissions. 5) Design NCSA environment to connect. 6) Connect MISP system to exchange information automatically with at least 10 agencies. 7) Conclude the operation.
Responsible Agency	**Main:** NCSA **Supporting:** Government Agency, Supervising or Regulating Organization, and Organization of Critical Information Infrastructure.



Tactics 4.3 Promote and support cybersecurity.

1. Create cybersecurity confidence for stakeholders.
2. Enhance cybersecurity in critical service-providing agencies.
3. Promote and support cybersecurity services.

- **Tactic's Indicators**

1. Stakeholders have at least 50 percent confidence in cybersecurity.
2. There are establishment of necessary laws, rules, and regulations to promote growth of cybersecurity service providers.
3. Number of cybersecurity service provider increase by 10 percent annually.

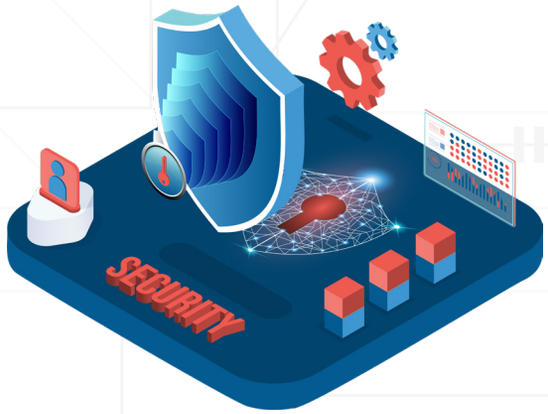
- **Tactic's Implementing Projects**

1. Project to expand National Cyber Security Agency (NCSA) support for critical service provider organizations.
2. Project to promote and support security service providers for critical services.
3. Project to implement cybersecurity plans, strategies, and policy.
4. Project to establish National Cyber Security Agency (National Computer Emergency Response Team (National CERT)).
5. Project to establish National Cyber Security Agency (Help Desk for National Computer Emergency Response Team (National CERT)).
6. Project to establish National Cyber Security Agency (NCSA War room).

Project	**1. Project to expand National Cyber Security Agency (NCSA) support for critical service provider organizations**
Procedure Guidelines	1) Establish guidelines to expand National Cyber Security Agency (NCSA) support for critical service provider organizations. 2) Establish National Cyber Security Agency (NCSA) support expansion mechanisms for critical service provider organizations. 3) Develop National Cyber Security Agency (NCSA) platform to expand support for critical service provider organizations. 4) Develop National Cyber Security Agency (NCSA) capability to support critical service provider organizations. 5) Regulate, monitor, evaluate, promote, and support continuously.
Responsible Agency	**Main:** NCSA **Supporting:** Supervising or Regulating Organization.

Project	**2. Project to promote and support security service providers for critical services**
Procedure Guidelines	1) Establish guidelines to promote security service providers for critical services by providing operational privileges and set standard price range. 2) Issue necessary laws, rules, and regulations to encourage service providers for critical services organizations. 3) Regulate the promotion of service providers for critical services organizations. 4) Regulate, monitor, evaluate, promote, and support continuously.
Responsible Agency	**Main:** NCSA **Supporting:** OAG, BOI, Supervising or Regulating Organization.

Project	**3. Project to implement cybersecurity plans, strategies, and policy**
Procedure Guidelines	1) Plan the operation, establish conceptual framework, and activities' action plans with details, duration, and person in charge. 2) Prepare public relations content and format, create online instructional media. 3) Public relations using various forms of media. 4) Organize 4 two-days meetings/seminars to clarify cybersecurity policy and plan including related rules and regulations with at least 300 participants, in private venue and via online. 5) Monitor and evaluate projects performance. 6) Prepare project conclusion reports.
Responsible Agency	**Main:** NCSA **Supporting:** Government Agency, Supervising or Regulating Organization, and Organization of Critical Information Infrastructure.



Project	4. Project to establish National Cyber Security Agency (National Computer Emergency Response Team (National CERT))
Procedure Guidelines	1) Study, analyze, establish conceptual framework to operate and design. Action plan to develop the design and develop National Computer Emergency Response Team (National CERT) system. 2) Procure durable articles and tools for National Computer Emergency Response Team (National CERT). Install and test tools and system to ensure operational readiness as per requirements. Prepare manuals for system administrators and users. 3) Test the system usability and adjust according to requirements. 4) Prepare monthly Cyber Threats discovery of Threat Hunting Framework (THF) reports after complete installation. 5) Provide advising team to support system utilization to ensure continuously run 24 hours in 7 days. Advising team members must be profoundly intellectual and qualified with basic cybersecurity knowledge and experience. Therefore, supplier/contractor must have 2 operators' station at National CERT for a 12-month operational period. Supplier/contractor also provides office supplies i.e., computer and printer etc. for the operators. 6) Organize training sessions for related personnel. 7) The officers in charge of attending and monitoring Cyber Threats prepare the monthly conclusion of occurred Cyber Threats report, quarterly Cyber Threats tendency report, and operational conclusion report.
Responsible Agency	**Main:** NCSA **Supporting:** Supervising or Regulating Organization, Organization of Critical Information Infrastructure, and Government Agency.

Project	5. Project to establish National Cyber Security Agency (Help Desk for National Computer Emergency Response Team (National CERT))
Procedure Guidelines	1) Establish conceptual framework, and activities' action plans with details, duration, and person in charge. 2) Install and provide cybersecurity administrative assistant service (External Ticketing System), internal cybersecurity administrative assistant service (Internal Ticketing System), information security and analysis system (Data center), Cyber Threats information exchange platform system. 3) Prepare project conclusion reports.
Responsible Agency	**Main:** NCSA **Supporting:** Supervising or Regulating Organization, Organization of Critical Information Infrastructure, and Government Agency.

Project	6. Project to establish National Cyber Security Agency (NCSA War room)
Procedure Guidelines	1) Establish operational conceptual framework and tools and system maintenance, fix, repair plan with details and duration. 2) Run system and tools test 4 times per year (quarterly). 3) Prepare maintenance conclusion reports and prepare to deliver.
Responsible Agency	**Main:** NCSA **Supporting:** Supervising or Regulating Organization, Organization of Critical Information Infrastructure, and Government Agency.

Appendix

Cybersecurity Management Policy for Government Agency and Organization of Critical Information Infrastructure

Cybersecurity Management Policy for Government Agency and Critical Information Infrastructure Organization.

Cybersecurity Act 2019 Section 9 (2) instructs that National Cyber Security Committee (NCSC) has responsibility and power to propose cybersecurity policy and management for Government Agency and Organization of Critical Information Infrastructure.

This Cybersecurity Management Policy is established as a guideline for governance, risk management, and compliance (Governance, Risk and Compliance: GRC) for Government Agency and Organization of Critical Information Infrastructure to operate cybersecurity duty effectively and unidirectional.

This Cybersecurity Management Policy equipped with extensively international good principles and practices including Thailand which is Governance, Risk and Compliance: GRC that consisted of:

1. Good Governance in Cybersecurity

1.1 Organizational structure of the cybersecurity management should have checked and balanced with clear authorities, roles, and responsibilities in line with effective Three Lines of Defense (control, regulate, and audit) with independent regulator and auditor who can perform effectively. Therefore, roles and responsibilities must be clearly identified, both agencies, or those who create risks and control risks at the first level (Business Unit or First Line of Defense). They shall tend and operate according to guidelines with appropriate internal control and risk management. Internal agency or regulator (Second Line of Defense) i.e., risk management, compliance, and internal audit (Third Line of Defense) to promote appropriate audit and check and balance mechanisms. The Government Agency and Organization of Critical Information Infrastructure shall practice and be in line with current related laws and regulations including related guidelines issued by Supervising and Regulating Organization subsequently and will become effective for Government Agency and Organization of Critical Information Infrastructure.

Nonetheless, if the information technology risk regulatory structure is combined with companies in the same business group or related companies, roles and responsibilities of the regulatory structure in accordance with the Three Lines of Defense shall be considered in the context of the same business group.

1.2 In establishment of information technology security management, government agencies must assign Head of Information Security or equivalency to manage the agency. The aforementioned person must be qualified with knowledge and experiences on information technology, information technology security management and Cyber Threats handling.

Thus, the aforementioned executive must be independent from IT operation and IT development and shall have the minimum roles and responsibility in IT security agency as followed.

1) There are information technology security policy, standards, and guidelines, Cyber Threats handling as well as monitoring to ensure the practice accordingly.

2) There are security specifications and IT security architecture.

3) Risk management for information technology security and Cyber Threats according to the organizational risks and submit to the committee as regular agenda.

4) Manage the agency to be prepared for handling Cyber Threats.

5) Manage to provide knowledge and awareness of information technology security and Cyber Threats to organizational personnel.

1.3 Organization of Critical Information Infrastructure must assign a Chief Information Security Officer: CISO or equivalency to act as agency's CISO.

Nevertheless, the aforementioned executive must operate independently from IT operation and IT development and have sufficient authority to effectively operate as CISO as followed.

1) Report significant information technology security issues and Cyber Threats to top executive, governmental committee, Organization of Critical Information Infrastructure and related committee.

2) Suggest comments on Cyber Threats and information technology security risk management to governmental committee, Organization of Critical Information Infrastructure, and information technology management and supervision related committee i.e., IT Steering Committee or IT Risk Committee. Involved in determination of information technology security and Cyber Threats that affect government and Organization of Critical Information Infrastructure significantly.



2. Risk Management

2.1 Establishment of written cybersecurity risk management which include.

(a) Cybersecurity risk assessment criteria and risk appetite.

(b) Cybersecurity risk assessment procedures.

(c) Cybersecurity risks observation and monitoring.

2.2 Keep records of cybersecurity risks identified in risk register relating to government critical services and Organization of Critical Information Infrastructure.

2.3 Regularly monitor identified cybersecurity risks to ensure they are under acceptable risk appetite stated in 2.1 (a).

3. Policies and Guidelines

3.1 Establish and approve policy, standards, and guidelines for cybersecurity risk management and protect government critical services and critical information infrastructure from Cyber Threats. Policy, standards, and guidelines must

(a) in accordance with this Code of Practices, sectoral cybersecurity regulations, and regional or national cybersecurity policy, standards, and direction.

(b) publish and communicate to personnel and third parties involved and able to access government critical services and critical information infrastructure organization.

3.2 Revision of policy, standards, and guidelines with cyber operational environments for government critical services and critical information infrastructure and Cyber Threats landscape at least annually after last revision or each policy, standards, and guidelines effective implementation date.

Therefore, cybersecurity management policy for government agencies and Organization of Critical Information Infrastructure are in effective for 1 year after publication.

Glossary

Term	Definition
Cybersecurity	Measures and operations established to prevent, handle, and reduce risks from domestic and international Cyber Threats which affect national security, economic security, military security, and internal peace and order.
Cyber Threats	Any unlawful act or operation performed by the use of a computer, or a computer system, or malicious program with intention to violate a computer system, computer data, or other related data and which is an imminent danger causing damage to or affect computer functionality, computer system, or other related data.
Cyber	Data and communications from service providing or computer networks application, internet or telecommunication networks and common satellite services, and similar network system of general connectivity.
Government agency	Central administration, regional administration, local administration, state enterprises, legislative body, judiciary body, independent organization, public organizations, and other government agency.



Term	Definition
Cybersecurity incident	Incident caused by unlawful action or operation performed by computer or computer system and is likely to cause damages to or affects cybersecurity, cybersecurity of a computer, computer data, computer system, or other data related computer system.
Critical Infrastructure: CI	Agencies, organizations or part of agency or organization which their electronic transactions have consequences to the national or public security, peace and order.
Critical Information Infrastructure: CII	Computers or computer systems used by government or private agencies to maintain national security, public security, national economic security, or public interest infrastructure.
Organization of Critical Information Infrastructure	Government or private agencies who have tasks or provide critical information infrastructure service. According to Section 49, Organization of Critical Information Infrastructure as followed: (1) National security (2) Substantive public services (3) Finance and banking (4) Information technology and telecommunications (5) Transportation and logistics (6) Energy and public utilities (7) Public Health (8) Others as specified by the Committee

Term	Definition
Supervising or Regulating Organization	Government or private agencies or person legally authorizes to have responsibility and power to regulate the operation of government agency or critical information infrastructure organization.
Gross Domestic Product: GDP	Market value of finishing products and services produced within the country during a given period regardless of its origin. GDP is defined by Simon Kuznets, Russian economist. GDP is the indicator of the population's standard of living in the nation.
Platform	Computer program system that can expand the capability infinitely. There are functional development and new module creation of innovation continually that can connect to other system. Platform is not limited to software but also inclusive of websites and other programs created to automatically connect or retrieve information.
Artificial Intelligence: AI	A field of computer science relating to the creation of human-like computer or computer that imitates human behavior especially intelligence ability. This intelligence was created by human thus it was called artificial intelligence. The aspects of AI may vary from intelligence needed based on environmental concerning behavior or the intelligence of AI products.

Term	Definition
Global Cybersecurity Index: GCI	Indicating index of each nation cybersecurity development, prepared by International Telecommunication Union: ITU with ABI Research (Allied Business Intelligence). The objective is to motivate cybersecurity awareness of each nation with the ultimate goal to create cybersecurity as global culture and unite in information technology and communication core.
Computer emergency response team: CERT	CERT or Computer Emergency Response Team is a registered trademark of CERT Coordination Center (CERT/CC). CERT is the team response to threats under Software Engineering Institute: SEI of Carnegie Mellon University, the United States of America. As CERT is a registered trademark, therefore, the newly established center to coordinate and handle cybersecurity threats who intend to use CERT in the name must apply for permission i.e., ThaiCERT in Thailand.



Term	Definition
Computer Security Incident Response Team: CSIRT or Computer incident response teams: CIRT	Cybersecurity Incident Response Center who handles and resolves threats which consisted of knowledgeable and skillful personnel to handle threats, assist clients to restore from system hacking. Furthermore, with proactive operation, CSIRT can provide vulnerability verification and assessment and other risks of the information system including raise awareness and provide knowledge to related personnel to develop and improve cybersecurity services.



Cyber Security Policy and Action Plan 2022 - 2027

Note : .....

10

ประกาศ กกม.

เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ. 2566

มีผลใช้บังคับตั้งแต่วันที่ 10 พ.ค. 66 เป็นต้นไป

Notification of CRC

Re: Cyber Incident Reporting Criteria and Procedure B.E. 2566 (2023)

effective from May 10, 2023, onwards.



ฉบับภาษาไทย
Thai Version

ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์

เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์

พ.ศ. ๒๕๖๖

โดยที่พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดให้คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์กำหนดหลักเกณฑ์และวิธีการรายงานเมื่อมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญต่อระบบของหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

อาศัยอำนาจตามความในมาตรา ๑๓ (๕) และมาตรา ๕๗ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์จึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ. ๒๕๖๖”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ข้อ ๓ ในประกาศนี้

“เหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญ” หมายความว่า เหตุภัยคุกคามทางไซเบอร์ที่ปรากฏต่อระบบสารสนเทศ และเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามมาตรา ๔๙ ซึ่งคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติได้กำหนดลักษณะของภัยคุกคามทางไซเบอร์ไว้ตามมาตรา ๖๐ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

ข้อ ๔ กรณีที่เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ต่อระบบสารสนเทศของหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศใด ให้หน่วยงานนั้นดำเนินการตรวจสอบข้อมูลที่เกี่ยวข้องของข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ รวมถึงพฤติการณ์แวดล้อม เพื่อประเมินว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้นหรือไม่ และเป็นภัยคุกคามระดับใด หากตรวจพบต้องดำเนินการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของตน พร้อมทั้งแจ้งข้อมูลดังกล่าวไปยังสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติโดยเร็ว หลังจากการตรวจพบหรือเกิดภัยคุกคามทางไซเบอร์ดังกล่าว และในส่วนของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้แจ้งภัยคุกคามนั้นไปยังหน่วยงานควบคุมหรือกำกับดูแลของตนภายในเวลาที่หน่วยงานควบคุมหรือกำกับดูแลกำหนดไว้ด้วย ทั้งนี้ ให้แจ้งข้อมูลตามที่กำหนดในเอกสาร ก๑ ข้อมูลที่ต้องแจ้ง ท้ายประกาศนี้

ทั้งนี้ การแจ้งข้อมูลตามวรรคหนึ่งให้เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ มีหน้าที่และอำนาจในการกำหนดแนวทาง วิธีปฏิบัติและอื่น ๆ เพื่อประโยชน์ในการปฏิบัติตามประกาศนี้

ข้อ ๕ กรณีที่มีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญต่อระบบของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ให้หน่วยงานดังกล่าวจัดทำและส่งรายงานเหตุภัยคุกคามทางไซเบอร์นั้น ตามแบบที่กำหนดในเอกสาร ก๒ แบบรายงานภัยคุกคามทางไซเบอร์ ท้ายประกาศนี้ไปยังสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติภายในระยะเวลา ๒๔ ชั่วโมง หลังจากการตรวจพบหรือเกิดภัยคุกคามทางไซเบอร์ดังกล่าวแล้ว พร้อมทั้งให้จัดส่งรายงานดังกล่าวไปยังหน่วยงานควบคุมหรือกำกับดูแลของตนภายในเวลาที่หน่วยงานควบคุมหรือกำกับดูแลกำหนดด้วย

ให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พิจารณาส่งข้อมูลสำคัญที่จำเป็นต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ให้สอดคล้องกับนโยบายการรักษาความลับของหน่วยงานด้วยและต้องปรับปรุงข้อมูลในรายงานเหตุภัยคุกคามทางไซเบอร์และสถานะการตอบสนองภัยคุกคามทางไซเบอร์ให้สอดคล้องกับข้อมูลอันเป็นปัจจุบันที่หน่วยงานได้สืบทราบเพิ่มมากขึ้นในระหว่างการดำเนินการรับมือเหตุภัยคุกคาม รวมทั้งจัดส่งรายงานปิดเหตุการณ์ภัยคุกคามดังกล่าวด้วย

ให้นำความในวรรคหนึ่งและวรรคสอง มาใช้บังคับแก่หน่วยงานของรัฐ กรณีมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญต่อระบบสารสนเทศของหน่วยงานของรัฐ โดยอนุโลม

ข้อ ๖ ให้หน่วยงานของรัฐหรือหน่วยงานควบคุมหรือกำกับดูแล จัดทำและส่งรายงานสรุปจำนวนเหตุภัยคุกคามทางไซเบอร์ทั้งหมดที่ได้เกิดขึ้นกับข้อมูลหรือระบบสารสนเทศของหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ภายใต้การควบคุมหรือกำกับดูแลของตนในแต่ละปี ภายในวันที่ ๓๑ มกราคม ของปีถัดไป ให้แก่สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ โดยให้แยกสถิติหมวดหมู่ตามแบบที่กำหนดในเอกสาร ก๓ แบบรายงานสรุปภัยคุกคามทางไซเบอร์ในหนึ่งรอบปี ท้ายประกาศนี้

ข้อ ๗ การแจ้ง การรายงาน และการรายงานสรุปตามประกาศนี้ จะทำเป็นหนังสือหรือโดยวิธีการทางอิเล็กทรอนิกส์ก็ได้

ข้อ ๘ ให้ประธานกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เป็นผู้รักษาการตามประกาศนี้

ในกรณีที่มีปัญหาเกี่ยวกับการปฏิบัติตามประกาศนี้ หรือประกาศนี้ไม่ได้กำหนดเรื่องใดไว้ ให้ประธานกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์เป็นผู้มีอำนาจตีความและวินิจฉัยชี้ขาด และคำวินิจฉัยของประธานกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ให้ถือเป็นที่สุด

ประกาศ ณ วันที่ ๒๐ มีนาคม พ.ศ. ๒๕๖๖
ชัยวุฒิ ธนาคมานุสรณ์
รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
ประธานกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์

เอกสารแนบท้ายประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์
เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ. ๒๕๖๖
ว่าด้วยข้อมูลที่ต้องแจ้งและแบบการรายงานภัยคุกคามทางไซเบอร์

บทนำ

ตามที่พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ได้กำหนดลักษณะของภัยคุกคามทางไซเบอร์ โดยแบ่งออกเป็น ๓ ระดับ ได้แก่ ภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง ภัยคุกคามทางไซเบอร์ในระดับร้ายแรง และภัยคุกคามทางไซเบอร์ในระดับวิกฤติ และให้หน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศแจ้งในกรณีที่เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ต่อระบบสารสนเทศซึ่งอยู่ในความดูแลรับผิดชอบของหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำรายงานเมื่อมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญต่อระบบของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ นั้น

เพื่อให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ มีแนวทางปฏิบัติที่ชัดเจนในการรายงานการดำเนินมาตรการตามที่กำหนดในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ว่าด้วยลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ จึงกำหนดให้หน่วยงานดังกล่าวจัดทำรายงานเหตุภัยคุกคามทางไซเบอร์ที่เกิดขึ้นอย่างมีนัยสำคัญต่อระบบของหน่วยงานตามรายการที่กำหนดไว้ในแนบท้ายนี้ ผ่านการส่งทางอีเมล โทรสาร หรือด้วยวิธีการทางอิเล็กทรอนิกส์อื่นใดที่มีความปลอดภัย เช่น การส่งรายงานที่เข้ารหัสด้วย PGP มาทางอีเมล (เป็นอย่างน้อย)

เนื่องด้วยการส่งรายงานของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้ทันการณ์เป็นเรื่องที่สำคัญ[๑,๒] ในกรณีหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศยังไม่สามารถแจ้งข้อมูลตามแบบรายงานได้อย่างครบถ้วนภายในระยะเวลา ๒๔ ชั่วโมง ให้หน่วยงานดังกล่าวจัดส่งรายงานด้วยข้อมูลเท่าที่มีและเมื่อมีความคืบหน้าหรือมีข้อมูลเพิ่มเติมในการดำเนินการรับมือ ให้แจ้งต่อสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเป็นระยะ และรีบจัดทำและส่งรายงานที่สมบูรณ์ให้แก่สำนักงานโดยเร็ว ทั้งนี้ ให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศพิจารณาส่งข้อมูลสำคัญที่จำเป็นต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ และสอดคล้องกับนโยบายการรักษาความลับของหน่วยงาน

ในกรณีที่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศไม่สามารถดำเนินการจัดเตรียมข้อมูลในรายงานได้ด้วยเหตุผลบางประการ ให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศแจ้งหน่วยงานควบคุมหรือกำกับดูแลของตนและสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติให้ทราบโดยเร็ว

ทั้งนี้ เพื่อให้หน่วยงานของรัฐ มีแนวทางปฏิบัติที่ชัดเจนในการรายงานเหตุภัยคุกคามทางไซเบอร์กรณีมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญต่อระบบสารสนเทศของหน่วยงานของรัฐ จึงให้นำหลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศดังกล่าวข้างต้น มาบังคับใช้แก่หน่วยงานของรัฐโดยอนุโลม

---

[๑] การรายงานภัยคุกคามทางไซเบอร์ที่เกิดขึ้นอย่างมีนัยสำคัญต้องรายงานภายในระยะเวลาที่หน่วยงานควบคุมหรือกำกับดูแลกำหนด (โดยหน่วยงานควบคุมหรือกำกับดูแลอาจกำหนดให้นำข้อปฏิบัติตามแผนการกู้คืนของหน่วยงานมาประกอบการพิจารณาด้วยก็ได้) หรืออาจเทียบเคียงจากตัวอย่างตามที่ระบุในข้อ ๓ ของภาคผนวกแนบท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔

[๒] มาตรา ๗๓ กำหนดให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่ไม่รายงานเหตุภัยคุกคามทางไซเบอร์ โดยไม่มีเหตุอันสมควร ต้องระวางโทษปรับไม่เกิน ๒๐๐,๐๐๐ บาท

เอกสาร ก๑ ข้อมูลที่ต้องแจ้ง

ข้อมูลการประสานงานและผลการตรวจสอบภัยคุกคามเบื้องต้น

๑. ข้อมูลการประสานงาน

ชื่อหน่วยงานที่รับผิดชอบติดตามเหตุภัยคุกคาม

วันที่และเวลาที่แจ้ง

๒. ด้านภารกิจหรือบริการของหน่วยงาน และ ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม

ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม

ที่อยู่ของหน่วยงานหรือหน่วยงานย่อยที่เกิดเหตุภัยคุกคาม

๓. ข้อมูลการติดต่อสำหรับการประสานงานเหตุภัยคุกคาม

ชื่อ-นามสกุล ตำแหน่งงาน

ชื่อหน่วยงาน อีเมล

โทรศัพท์ (ที่ทำงาน / มือถือ)

๔. ความต่อเนื่องของเหตุภัยคุกคาม

☐ เหตุภัยคุกคามใหม่ ☐ การรายงานข้อมูลต่อเนื่องจากเหตุภัยคุกคามเดิม

๕. ลักษณะภัยคุกคามทางไซเบอร์

ระบบที่ได้รับผลกระทบมีความสำคัญต่อพันธกิจหลักของหน่วยงานหรือไม่

เหตุการณ์ที่เกิดขึ้นเกิดจากภัยคุกคามทางไซเบอร์[๓] ในระดับใด (มาตรา ๖๐)

☐ ไม่ร้ายแรง ☐ ร้ายแรง ☐ วิกฤต (ก) ☐ วิกฤต (ข)

☐ ยังไม่สามารถระบุได้

๖. หมวดหมู่ของภัยคุกคาม (แจ้งได้มากกว่า ๑ รายการ)

หมวดหมู่*	คำอธิบาย
หมวดหมู่ที่ ๒	การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance)
หมวดหมู่ที่ ๓	การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยของหน่วยงาน (Non-Compliance Activity)
หมวดหมู่ที่ ๔	การบุกรุกโดยการใช้มัลแวร์ (Malicious Logic)
หมวดหมู่ที่ ๕	การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion)
หมวดหมู่ที่ ๖	การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion)
หมวดหมู่ที่ ๗	การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)
หมวดหมู่ที่ ๘	เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating)

* อ้างอิงหมวดหมู่ตามภาคผนวกท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ (ทั้งนี้ ภัยคุกคามทางไซเบอร์หมวดหมู่ที่ ๐ หมวดหมู่ที่ ๑ และหมวดหมู่ที่ ๙ ไม่เข้าข่ายเป็นภัยคุกคามทางไซเบอร์ที่ต้องรายงาน)

[๓] พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดความหมายของ “ภัยคุกคามทางไซเบอร์” ดังนี้ การกระทำหรือการดำเนินการใด ๆ โดยมิชอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

เอกสาร ก๒ แบบรายงานภัยคุกคามทางไซเบอร์

ส่วนที่ ๑

หมวด ก. ข้อมูลการประสานงานและผลการตรวจสอบภัยคุกคามเบื้องต้น

หมายเลขอ้างอิง (สำหรับเจ้าหน้าที่ สกมช.): โปรดระบุ
หน่วยงานที่รับผิดชอบติดตามเหตุภัยคุกคาม (ถ้ามี): โปรดระบุ
วันที่: เลือกวันที่ **เวลา:** โปรดระบุ

ก๑. ด้านภารกิจหรือบริการของหน่วยงาน และ ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม

ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม: โปรดระบุ
ที่อยู่ของหน่วยงานหรือหน่วยงานย่อยที่เกิดเหตุภัยคุกคาม: โปรดระบุ

ก๒. ข้อมูลการติดต่อสำหรับการประสานงานเหตุภัยคุกคาม

ชื่อ-นามสกุล: โปรดระบุ ตำแหน่งงาน: โปรดระบุ
ชื่อหน่วยงาน: โปรดระบุ อีเมล: โปรดระบุ
โทรศัพท์ (ที่ทำงาน / มือถือ): โปรดระบุ

ก๓. ความต่อเนื่องของเหตุภัยคุกคาม

☐ เหตุภัยคุกคามใหม่ ☐ การรายงานข้อมูลต่อเนื่องจากเหตุภัยคุกคามเดิม

ก๔. ลักษณะภัยคุกคามทางไซเบอร์

ระบบที่ได้รับผลกระทบมีความสำคัญต่อพันธกิจหลักของหน่วยงาน

☐ ใช่ ☐ ไม่ใช่

เหตุการณ์ที่เกิดขึ้นเกิดจากภัยคุกคามทางไซเบอร์[๔] ในระดับใด (มาตรา ๖๐)

☐ ไม่ร้ายแรง ☐ ร้ายแรง ☐ วิกฤต (ก) ☐ วิกฤต (ข)

☐ ยังไม่สามารถระบุได้

[๔] พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดความหมายของ “ภัยคุกคามทางไซเบอร์” ดังนี้ การกระทำหรือการดำเนินการใด ๆ โดยมิชอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

หมวด ข. ข้อมูลการตรวจพบภัยคุกคามไซเบอร์

ข๑. วัน เวลา ที่เกิดเหตุภัยคุกคาม

วันที่ : เลือกวันที่ เวลา : โปรดระบุ

วัน เวลา ที่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศทราบเหตุภัยคุกคาม

วันที่ : เลือกวันที่ เวลา : โปรดระบุ

ข๒. วัน เวลา ที่แจ้งเหตุภัยคุกคามให้หน่วยงานควบคุมหรือกำกับดูแลทราบ

☐ ยังไม่ได้แจ้ง ☐ แจ้งแล้ว _____

ข๓. หมวดหมู่ของภัยคุกคาม (เลือกได้มากกว่า ๑ รายการ)

หมวดหมู่*	คำอธิบาย
☐ หมวดหมู่ที่ ๒	การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance)
☐ หมวดหมู่ที่ ๓	การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยของหน่วยงาน (Non-Compliance Activity)
☐ หมวดหมู่ที่ ๔	การบุกรุกโดยการใช้มัลแวร์ (Malicious Logic)
☐ หมวดหมู่ที่ ๕	การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion)
☐ หมวดหมู่ที่ ๖	การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion)
☐ หมวดหมู่ที่ ๗	การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)
☐ หมวดหมู่ที่ ๘	เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating)
☐ อื่น ๆ	โปรดระบุ

* อ้างอิงหมวดหมู่ตามภาคผนวกท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ (ทั้งนี้ภัยคุกคามหมวดหมู่ที่ ๐ ๑ และ ๙ ไม่เข้าข่ายเป็นภัยคุกคามที่ต้องรายงาน)

ข๔. ข้อมูลเบื้องต้นเกี่ยวกับระบบคอมพิวเตอร์ คอมพิวเตอร์ บริการ หรือข้อมูลที่ได้รับผลกระทบ:

สถานที่ตั้งของเครื่อง ข้อมูล หรือสินทรัพย์ที่ได้รับผลกระทบ (เช่น จังหวัด ตำบล ตึก ห้อง):

โปรดระบุ

ชื่อผู้ให้บริการเครือข่ายที่ให้บริการแก่ระบบ บริการ หรือข้อมูลที่ได้รับผลกระทบ :

โปรดระบุ

บริการของระบบ ข้อมูล หรือสินทรัพย์ที่ได้รับผลกระทบ (เช่น บริการการโอนเงิน):

โปรดระบุ

ฮาร์ดแวร์ ซอฟต์แวร์ที่ได้รับผลกระทบ (โปรดระบุรายละเอียด เช่น ผู้ผลิตหรือยี่ห้อ รุ่นของเครื่องคอมพิวเตอร์): โปรดระบุรายละเอียด

มีผลกระทบต่อการสื่อสาร (ทางโทรศัพท์ หรือ การใช้งานเครือข่าย): โปรดระบุ

รายละเอียดอื่น ๆ: โปรดระบุ

หมวด ค: ข้อมูลการรับมือภัยคุกคาม
ค๑. สถานการณ์หรือการแก้ไขเหตุภัยคุกคาม (เลือกได้มากกว่า ๑ รายการ) ☐ เพิ่งพบเหตุการณ์ ☐ อยู่ในขั้นตอนการขอความช่วยเหลือ ☐ อยู่ในขั้นตอนการสอบสวน ☐ กำลังลุกลาม ☐ อยู่ในขั้นตอนการระงับภัย ☐ สามารถระงับภัยได้แล้ว ☐ รายงานปิดเหตุการณ์ภัยคุกคามแล้ว ☐ อื่น ๆ: โปรดระบุ
ค๒. สิ่งที่ได้ดำเนินการหรือได้แก้ไขไปแล้ว ☐ ยังไม่ได้ดำเนินการแก้ไขใด ๆ ☐ ยกเลิกการเชื่อมต่อระบบออกจากเครือข่ายแล้ว ☐ ตรวจสอบข้อมูลจราจร (Log) แล้ว ☐ ตรวจสอบโปรแกรม (แฟ้ม binaries/.exe) แล้ว ☐ กู้คืนกลับมาด้วยระบบหรือข้อมูลสำรองที่ตรวจสอบความถูกต้องแล้ว ☐ รายละเอียดการแก้ไขภัยคุกคามที่เกิดขึ้นเพิ่มเติม: โปรดระบุ
ค๓. รายละเอียดการรับมือภัยคุกคามอื่น ๆ (ถ้ามี) โปรดระบุ

ส่วนที่ ๒

หมวด ง : รายละเอียดภัยคุกคาม

ง๑. ข้อมูลการตรวจจับและการวิเคราะห์

ง๑.๑ <u>วัน เวลา ที่ผู้โจมตีได้เริ่มต้นเข้าถึงระบบ</u> (System Access)

วันที่: เลือกวันที่ เวลา: โปรดระบุ ไม่ทราบ: ☐

ง๑.๒ ข้อมูลการพบเห็นเหตุภัยคุกคามทางไซเบอร์

รายละเอียดแหล่งที่มา หรือต้นเหตุของเหตุภัยคุกคาม (เท่าที่ทราบ เช่น คน, ความผิดพลาดของระบบ, ภัยธรรมชาติ, การจู่โจม, ความผิดพลาดจากคนนอกองค์กร):

โปรดระบุ

บุคคล วิธี หรือเครื่องมือที่ตรวจพบภัยคุกคาม (เช่น ผู้ใช้, ผู้ดูแลระบบ, โปรแกรม Anti-virus, IDS, การวิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์, ไม่ทราบ):

โปรดระบุ

รายละเอียดของปัญหาลักษณะคล้ายกันที่หน่วยงานเคยพบมาก่อน (ถ้ามี โปรดระบุรายละเอียด):

โปรดระบุ

ง๑.๓ รายละเอียดผลกระทบจากเหตุภัยคุกคาม (ระบุผลกระทบที่มีเกิดขึ้นต่อ ระบบ คน หรือข้อมูล)

จำนวนระบบ บริการ หรือสินทรัพย์ที่เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่ได้รับผลกระทบ (โดยประมาณ): โปรดระบุ

ทรัพย์สินที่สำคัญอื่น ๆ ที่อาจได้รับผลกระทบ: โปรดระบุ

จำนวนผู้ได้รับผลกระทบ (โดยประมาณ): โปรดระบุ

มูลค่าความเสียหาย (โดยประมาณ): โปรดระบุ

ในกรณีที่ข้อมูลที่ระบุตัวบุคคลได้รั่วไหล (หรือถูกขโมย):

จำนวนบุคคลที่เป็นเจ้าของข้อมูล : โปรดระบุ

ชนิดของข้อมูล (เลือกทุกข้อที่ใช่):

☐ ข้อมูลไบโอเมตริกซ์ ☐ ข้อมูลการติดต่อ

☐ ข้อมูลการเงิน ☐ ข้อมูลบุคลากรของรัฐ

☐ หมายเลขบัตรประชาชน ☐ ข้อมูลการติดต่อกับหน่วยงานต่าง ๆ

☐ ข้อมูลทางการแพทย์

☐ อื่น ๆ : โปรดระบุ

จำนวนข้อมูล (Record) ที่ได้รับผลกระทบ: โปรดระบุ

ผลกระทบอื่น ๆ ที่เกิดขึ้น: โปรดระบุ

๑.๔ <u>รายละเอียดของระบบ หรือข้อมูลที่ได้รับผลกระทบ (Information of Affected System)</u>

หมายเลข CVE: โปรดระบุ

ช่องโหว่ที่ถูกใช้จู่โจม: โปรดระบุ

การใช้ระบบหรือเครื่องที่ได้รับผลกระทบเป็นฐานเพื่อจู่โจมขยายผลไปยังระบบหรือเครื่องอื่น:
โปรดระบุ

อาการหรือสิ่งผิดปกติ (เลือกได้มากกว่า ๑ รายการ)

☐ ระบบล่ม ☐ รายการข้อมูลจราจรทางคอมพิวเตอร์ที่ผิดปกติ
☐ บัญชีผู้ใช้ถูกสร้างขึ้นมาใหม่โดยไม่ทราบสาเหตุ หรือ บัญชีผู้ใช้มีความผิดปกติ
☐ การจู่โจมด้วยวิศวกรรมสังคม (Social Engineering) ทั้งที่สำเร็จและไม่สำเร็จ
☐ ประสิทธิภาพของระบบด้อยลง (ทั้งที่รู้ว่าเป็นเพราะเหตุภัยคุกคามและที่ไม่รู้สาเหตุ)
☐ การเปลี่ยนแปลงใน DNS หรือ กฎของ Router หรือกฎไฟร์วอลล์ โดยไม่ทราบสาเหตุ
☐ การยกระดับสิทธิ์การเข้าถึงระบบโดยไม่ทราบสาเหตุ
☐ การตรวจพบการทำงานของโปรแกรมหรืออุปกรณ์ Sniffer เพื่อจับการรับส่งข้อมูลภายในเครือข่าย
☐ การเข้าใช้งานครั้งสุดท้ายของผู้ใช้ที่ไม่สอดคล้องกับการใช้งานครั้งสุดท้ายที่เกิดขึ้นจริง
☐ การแจ้งเตือนจากเครื่องมือตรวจจับการบุกรุก
☐ การเข้ามาลาดตระเวน (Probing) หรือการเรียกดู (Browsing) ที่น่าสงสัย
☐ รูปแบบการใช้งานที่ผิดปกติ ☐ การเปลี่ยนแปลงขนาดไฟล์ไปจากเดิมแบบผิดปกติ
☐ ความพยายามที่จะเขียนไฟล์ของระบบ ☐ การเปลี่ยนแปลงวันที่ของไฟล์ไปจากเดิมแบบผิดปกติ
☐ การแก้ไขหรือลบข้อมูลที่ผิดปกติ ☐ การจู่โจมให้เกิดการปฏิเสธการให้บริการ (DOS, DDOS)
☐ ไฟล์ใหม่ถูกสร้างขึ้นโดยไม่ทราบสาเหตุ ☐ การใช้งานหรือมีกิจกรรมที่เกิดในเวลาที่ผิดปกติ
☐ การแก้ไขหน้าเว็บ ☐ การสร้างแฟ้มข้อมูล setuid หรือ setgid ใหม่ที่ผิดปกติเกิดขึ้น
☐ การเปลี่ยนแปลงในไดเรกทอรีและแฟ้มข้อมูลของระบบปฏิบัติการที่ผิดปกติ
☐ การตรวจพบโปรแกรมเจาะระบบ (Crack utility)
☐ สิ่งที่ผิดปกติไปจากเดิมอื่น ๆ: โปรดระบุ

๑.๕ รายละเอียดของเหตุภัยคุกคามตามลำดับเวลา ตั้งแต่การจู่โจมครั้งแรก จนถึงปัจจุบัน (เช่น ลำดับของการจู่โจม, Attack vector, เทคนิคหรือเครื่องมือที่ผู้จู่โจมใช้ ฯลฯ)
โปรดระบุ

๑.๖ รายละเอียดอื่น ๆ ที่พบเกี่ยวข้องกับเหตุภัยคุกคาม: โปรดระบุ

๒. ข้อมูลการระงับ ปราบปราม และฟื้นฟู

๒.๑ รายละเอียดการดำเนินการเพื่อแก้ไขเหตุภัยคุกคาม: โปรดระบุ

๒.๒ การคาดการณ์ความสามารถฟื้นฟู
โปรดระบุรายละเอียดการฟื้นฟู ทรัพยากรที่ต้องใช้และที่ต้องการเพิ่ม และประมาณระยะเวลาการฟื้นฟู

๓. ข้อมูลกิจกรรมภายหลังการแก้ปัญหา (ถ้ามี)

๓.๑ วัน เวลา ที่เหตุภัยคุกคามสิ้นสุด วันที่: เลือกวันที่ เวลา: โปรดระบุ

๓.๒ การดำเนินการเพื่อป้องกันเหตุภัยคุกคามที่คล้ายคลึงกัน: โปรดระบุ

๓.๓ บทเรียนที่ได้จากเหตุภัยคุกคาม: โปรดระบุ

เอกสาร ก๓ แบบรายงานสรุปภัยคุกคามทางไซเบอร์ในหนึ่งรอบปี

ข้อ ๑ สถิติรายปีจำแนกตามหมวดหมู่ของภัยคุกคามทางไซเบอร์[๕]

หมวดหมู่	คำอธิบาย	จำนวน
๐	เหตุการณ์จำลองและการฝึกจู่โจมของหน่วยงาน (Training and Exercises)	
๑	การพยายามเข้าถึงระบบที่ไม่สำเร็จ (Unsuccessful Activity Attempt)	
๒	การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance)	
๓	การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยที่หน่วยงานกำหนด (Non-Compliance Activity)	
๔	การบุกรุกโดยการใช้มัลแวร์ (Malicious Logic)	
๕	การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion)	
๖	การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion)	
๗	การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)	
๘	เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating)	
๙	เหตุการณ์ผิดปกติที่ได้รับการวิเคราะห์แล้วว่าไม่ใช่เหตุการณ์ที่เป็นภัยคุกคาม (Explained Anomaly)	

ข้อ ๒ สถิติรายปีจำแนกตามทรัพย์สินที่ได้รับผลกระทบ

ทรัพย์สินที่ได้รับผลกระทบ	จำนวน
เครื่องแม่ข่าย / แอคทีฟ ไดเรกทอรี (Active Directory)	
เครื่องเวิร์กสเตชัน (Workstation)	
สวิตช์ (Switch) /เราเตอร์ (Router)	
เว็บไซต์ (Website)	
อื่น ๆ	

ข้อ ๓ สถิติรายปีจำแนกตามระดับภัยคุกคามทางไซเบอร์[๖]

ระดับภัยคุกคาม	จำนวน
ไม่ร้ายแรง	
ร้ายแรง	
วิกฤต (ก)	
วิกฤต (ข)	

[๕] หมวดหมู่ตามข้อ ๑ ของภาคผนวกท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์ แต่ละระดับ พ.ศ. ๒๕๖๔

[๖] ระดับภัยคุกคามทางไซเบอร์ตามมาตรา ๖๐ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒



ฉบับภาษาอังกฤษ
English Version

Notification of the Cybersecurity Regulating Committee

Re: Cyber Incident Reporting Criteria and Procedure

B.E.2566 (2023)

Whereas the Cybersecurity Act B.E. 2562 (2019) stipulates that the Cybersecurity Regulating Committee establishes reporting criteria and procedure in the event of a Significant Cyber Incident occurring to systems of Government Agencies or Organizations of Critical Information Infrastructure.

By virtue of Section 13 (5) and Section 57 of the Cybersecurity Act B.E. 2562 (2019), the Cybersecurity Regulating Committee hereby issues the following notification:

Clause 1 This notification shall be called the "Notification of the Cybersecurity Regulating Committee Re: Cyber Incident Reporting Criteria and Procedure B.E. 2566 (2023)".

Clause 2 This notification shall come into force on the date after its publication in the Royal Thai Government Gazette.

Clause 3 In this notification,

"Significant Cyber Incident" shall mean a cyber incident that causes an impact on the information system that is deemed a critical information infrastructure according to Section 49, whereas the characteristics of a cyber incident are determined by the National Cyber Security Committee in Section 60 of the Cybersecurity Act B.E. 2562 (2019).

Clause 4 If there is an occurrence or a potential occurrence of a cyber incident to the information system of an agency (whether a Government Agency or an Organization of Critical Information Infrastructure), the affected agency shall inspect data related to its computer data, computer systems, and surrounding circumstances to confirm the incident occurrence and assess the level of its impact. If a cyber incident occurrence is confirmed, the affected agency should prevent, handle, and mitigate the incident risks according to its cybersecurity code of practice and standard framework, and promptly notify the National

Cyber Security Agency after the incident is detected or has occurred. In the event of a cyber incident occurring to Organizations of Critical Information Infrastructure, they shall also notify their Regulator within the time stipulated by the Regulator. Such a notification shall include the required information stipulated in Enclosure A1 Required Information.

To fulfil the incident report procedure stipulated in paragraph one, the Secretary-General of the National Cyber Security Committee shall have the duties and powers in establishing guidelines, procedure, and other criteria to facilitate an effective execution of tasks in accordance with this notification.

Clause 5 In the event of a Significant Cyber Incident occurring to the system of an Organization of Critical Information Infrastructure, the affected agency shall prepare a cyber incident report by filling Enclosure A2 Cyber Incident Report Form, in the attached enclosures, and submit the report to the National Cyber Security Agency within 24 hours after the incident is detected or has occurred. The report shall also be submitted to the Regulator within the time stipulated by the Regulator.

Organizations of Critical Information Infrastructure shall consider submitting important information necessary for maintaining cybersecurity, in accordance with their confidentiality policy. They shall update the details of the incident report and the incident response status to ensure that the report content is up-to-date and reflects new information obtained during the latest investigation and handling of the incident. An incident closure report shall also be submitted.

Paragraph one and paragraph two shall apply *mutatis mutandis* to Government Agencies in the event of a Significant Cyber Incident occurring to their information system.

Clause 6 Government Agencies or Regulators shall prepare and submit an annual summary report of all incidents that have impacted the information or information systems of Government Agencies or Organizations of Critical Information Infrastructure under their supervision to the National Cyber Security Agency by the 31st of January of the following year. The summary report shall include statistics in each category as prescribed in Enclosure A3, Annual Cyber Incident Summary Report.

Clause 7 Notifications, reports, and summaries prepared in compliance with this notification may be issued as a letter or by an electronic means.

Clause 8 The Chairperson of the Cybersecurity Regulating Committee shall have charge and control of this notification.

If a problem related to the compliance with this notification has occurred, or the notification does not cover a particular matter, the Chairperson of the Cybersecurity Regulating Committee shall have the powers to provide interpretations and render decisions, and the decisions shall be deemed final.

Given on the of March B.E. 2566 (2023)

Chaiwut Thanakamanusorn

(Mr. Chaiwut Thanakamanusorn)

Minister of Digital Economy and Society

Chairperson of the Cybersecurity Regulating Committee

Enclosures of the Notification of the Cybersecurity Regulating Committee
Re: Cyber Incident Reporting Criteria and Procedure B.E. 2566 (2023)
on Required Information and Cyber Incident Report Form

Introduction

Whereas the Cybersecurity Act B.E. 2562 (2019) defines the characteristics of cyber incidents by dividing them into 3 levels, i.e., non-critical, critical, and crisis levels, and prescribes that Government Agencies and Organizations of Critical Information Infrastructure issue a notification of an occurrence or an expected occurrence of a cyber incident that may have an impact on the information system under their responsibility. Furthermore, Organizations of Critical Information Infrastructure shall prepare a report in the event of a Significant Cyber Incident occurring to their Information Infrastructure.

To provide a clear guideline for Organizations of Critical Information Infrastructure to report their compliance with the measures stipulated in the notification of the National Cyber Security Committee Re: Cyber Incident Characteristics and Measures for Prevention, Response, Assessment, Eradication, and Containment of Incidents at Each Level, the Cybersecurity Regulating Committee, therefore, stipulates that Organizations of Critical Information Infrastructure shall prepare a report of Significant Cyber Incidents occurring to their Information Infrastructure by following the list of items specified in these enclosures. The report may be submitted via e-mail, fax, or any secure electronic means, e.g., a PGP-encrypted report submission via e-mail (at minimum).

Timely incident report submissions by Organizations of Critical Information Infrastructure are vital.[1,2] If they are unable to provide complete information in the report form within 24 hours, they may submit a report with only information available at the time. As progress in handling the incidents is made or additional information becomes available, they shall periodically notify the National Cyber Security Agency, and prepare and submit a complete report to the Agency without delay. To perform such a task, they shall consider submitting important information necessary for maintaining cybersecurity, in accordance with their confidentiality policy.

[1] A significant impact cyber incident must be reported within the timeframe stipulated by the Regulator. (The Regulator may allow the agency to determine the timeframe that aligns with its incident recovery plan.) The example in Clause 3 of the appendix attached to the Notification of the National Cyber Security Committee Re: Cyber Incident Characteristics and Measures for Prevention, Response, Assessment, Eradication, And Containment of Incidents at Each Level B.E. 2564 (2021) may also be used as a case comparison.

[2] Section 73 stipulates that organizations of critical information infrastructure that fail to submit a cyber incident report shall be subject to a fine not exceeding 200,000 Baht.

If Organizations of Critical Information Infrastructure are unable to prepare information for the report due to a certain reason, they shall inform their Regulator and the National Cyber Security Agency without delay.

In order to provide a clear reporting guideline for Government Agencies in the event of a Significant Cyber Incident occurring to their information system, the reporting procedure and guideline for Organizations of Critical Information Infrastructure above may also apply *mutatis mutandis* to Government Agencies.

Enclosure A1 Required Information

Coordination Information and Preliminary Incident Analysis Results
1. Information for Coordination Name of the agency responsible for tracking the cyber incident Date and time of notification
2. Agency's missions or services, and name of the agency affected by the incident Name of the agency affected by the incident Address of the agency or subdivision affected by the incident
3. Contact Information of the Directly Responsible Person Name-Surname Job Title Name of the Agency E-mail Phone (Work / Mobile)
4. Continuity of the Incident ☐ A new incident ☐ Continuing report on a previous incident
5. Cyber Incident Characteristics Is the affected system critical to the main mission of the agency? What level of cyber incident does the event fall into?[3] (Section 60) ☐ Non-critical ☐ Critical ☐ Crisis (a) ☐ Crisis (b) ☐ Currently undeterminable

[3] The Cybersecurity Act B.E. 2562 (2019) specifies that "Cyber Incident" shall mean any action or unlawful undertaking committed through a computer, computer system, or undesirable program with an intention to cause any harm to the computer systems, computer data, or other relevant data, and be an imminent danger that could cause damage or disrupt the operation of the computer, computer system, or other relevant data.

6. Incident Categories (more than 1 category can be notified)

Category*	Description
Category 2	Activity that seeks to gather information of the agency before attacks (Reconnaissance)
Category 3	Activity that does not comply with the cybersecurity standard of the agency (Non-Compliance Activity)
Category 4	Intrusion using a malware (Malicious Logic)
Category 5	Intrusion at the user level (User Level Intrusion)
Category 6	Intrusion at the root level (Root Level Intrusion)
Category 7	Intrusion that prevents access to services (Denial of Service)
Category 8	Event that is being investigated (Investigating)

* These categories are in accordance with the appendix of the Notification of the National Cyber Security Committee Re: Cyber Incident Characteristics and Measures for Prevention, Response, Assessment, Eradication, and Containment of Incidents at Each Level, B.E. 2564 (2021) (Incidents in Categories 0, 1, and 9 do not require reporting.)

Enclosure A2 Cyber Incident Report Form

Part 1
Category A: Coordination Information and Preliminary Incident Analysis Results
Reference Number (for NCSA officer): Please specify **Agency responsible for tracking the cyber incident (if any):** Please specify **Date:** Select date **Time:** Please specify
A1. Missions or services of the agency and name of the agency affected by the incident Name of the agency affected by the incident: **Please specify** Address of the agency or subdivision affected by the incident: **Please specify**
A2. Contact Information of the Directly Responsible Person Name-Surname: **Please specify** Job Title: **Please specify** Name of the Agency: **Please specify** E-mail: **Please specify** Phone (Work / Mobile): **Please specify**
A3. Continuity of the Incident ☐ A new incident ☐ Continuing report on a previous incident
A4. Cyber Incident Characteristics The system affected is critical to the main mission of the agency. ☐ Yes ☐ No What level of cyber incident does the event fall into?[4] (Section 60) ☐ Non-critical ☐ Critical ☐ Crisis (a) ☐ Crisis (b) ☐ Currently undeterminable

[4] The Cybersecurity Act B.E. 2562 (2019) specifies that "Cyber Incident" shall mean any action or unlawful undertaking committed through a computer, computer system, or undesirable program with an intention to cause any harm to the computer systems, computer data, other relevant data, and be an imminent danger that could cause damage or disrupt the operation of the computer, computer system, or other relevant data.

Category B: Cyber Incident Detection Information

B1. Date and Time of the incident

Date: **Select date** Time: **Please specify**

Date and time that the Organization of Critical Information Infrastructure became aware of the incident

Date: **Select date** Time: **Please specify**

B2. Date and time that the Regulator was notified of the incident

☐ Not yet notified ☐ Notified _____

B3. Incident Categories (more than 1 category can be selected)

Category*	Description
☐ **Category 2**	Activity that seeks to gather information about the agency before attacks (Reconnaissance)
☐ **Category 3**	Activity that does not comply with the cybersecurity standard of the agency (Non-Compliance Activity)
☐ **Category 4**	Intrusion using a malware (Malicious Logic)
☐ **Category 5**	Intrusion at the user level (User Level Intrusion)
☐ **Category 6**	Intrusion at the root level (Root Level Intrusion)
☐ **Category 7**	Intrusion that prevents access to services (Denial of Service)
☐ **Category 8**	Event that is being investigated (Investigating)
☐ Others	Please specify

* These categories are in accordance with the appendix of the Notification of the National Cyber Security Committee Re: Cyber Incident Characteristics and Measures for Prevention, Response, Assessment, Eradication, and Containment of Incidents at Each Level, B.E. 2564 (2021) (Incidents in Categories 0, 1, and 9 do not require reporting.)

B4. Preliminary information about the impacted computer system, computer, service, and data:

Location of the impacted computer, data, or asset (e.g., province, subdistrict, building, room):

Please specify

Name of the network service provider who provides services to the impacted system, service, or data:

Please specify

Service of the impacted system, data, or asset (e.g., money transfer service):

Please specify

The impacted hardware and software (Please provide details, e.g., name of manufacturer or brand, computer model): Please provide details

Impact on communication (via phone or network): Please specify

Other details: Please specify

Category C: Incident Handling Information
C1. Situation or Resolution of the Incident (more than 1 item can be selected) ☐ Event just detected ☐ Assistance request phase ☐ Investigation phase ☐ Spreading ☐ Containment phase ☐ Incident contained ☐ Incident closure reported ☐ Others: Please specify
C2. Actions taken or issues resolved ☐ Haven't taken any action ☐ System disconnected from the network ☐ Log data examined ☐ Program examined (binaries/.exe files) ☐ Restored using the backup system or backup data that have already been verified ☐ Additional details on resolving the occurring incident: Please specify
C3. Other incident handling details (if any) Please specify

Part 2
Category D: Incident Details
D1. Detection and Analysis Information
D1.1 Date and Time when the Attacker Initially Access the System Date: **Select Date** Time: **Please specify** Unknown: ☐
D1.2 Information on Incident Detection Details of the source or root cause of the incident (e.g., human errors, system failures, natural disasters, malicious actions, third-party failures): **Please specify** Person, method, or tool used to detect the incident (e.g., user, system administrator, anti-virus program, IDS, computer log data analysis, unknown): **Please specify** Details of a similar problem previously detected by the agency (if any, please provide details here.): **Please specify**
D1.3 Details of the Impact of the Incident (Please explain the impact on the system, human, or data) Number of impacted systems, services, or assets that are a critical information infrastructure (in an estimate): **Please specify** Other important assets that may be impacted: **Please specify** Number of persons impacted (in an estimate): **Please specify** Cost of damage (in an estimate): **Please specify** In case personal identifiable information are breached (or stolen): Number of data owners: **Please specify** Type of information (select all that is relevant): ☐ Biometric information ☐ Contact information ☐ Financial information ☐ Information of government officers ☐ Identification number ☐ Information about contact with various agencies ☐ Medical information ☐ Others: Please specify Number of impacted records: **Please specify**

Other impacts that might occur: **Please specify**

D1.4 Information of Impacted System

CVE ID: Please specify

Exploited Vulnerability: Please specify

The use of affected system or computer as a base to launch further attacks on other systems or computers:

Please specify

Anomalies (more than 1 item can be selected)

- ☐ System failures
- ☐ Suspicious log data
- ☐ Unexplainable new user accounts or suspicious user accounts
- ☐ Successful and unsuccessful social engineering
- ☐ Lower system efficiency (due to a known incident or an unknown cause)
- ☐ Unknown causes of change in DNS or router rules or firewall rules
- ☐ Unexplainable elevation of system access privileges
- ☐ Detection of sniffer programs or tools used to capture data flow in the network
- ☐ Inconsistency between an indicated last user access and the actual last assess made by the user
- ☐ Alert from a detection tool
- ☐ Suspicious probing or browsing
- ☐ Abnormal usage pattern
- ☐ Abnormal file size change
- ☐ Attempt to write a system file
- ☐ Abnormal change to a file's date
- ☐ Abnormal edit or deletion of data
- ☐ DOS and DDOS attack
- ☐ Unexplainable new file creation
- ☐ Usage or activity at an unusual time
- ☐ Webpage edit/defacement
- ☐ Abnormal new setuid or setgid files
- ☐ Abnormal change in directory and file of the operation system
- ☐ Crack utility detection
- ☐ Other anomalies: **Please specify**

D1.5 Details of the incident timeline from the first attack to the present (e.g., the order of attack, attack vector, techniques or tools used by the attacker.)

Please specify

D1.6 Other details found relevant to the incident: Please specify

D2. Information about Incident Containment, Eradication, and Recovery

D2.1 Details of the Incident Resolution: Please specify

D2.2 Estimation on Recoverability Please provide information regarding recovery, required resources and any further resources that are needed, and an estimate of recovery time
D3. Post-incident Activity Information (if any)
D3.1 Date and time that the incident ended. Date: **Select date** Time: **Please specify**
D3.2 Actions taken to prevent similar incidents: Please specify
D3.3 Lessons learned from the incident: Please specify

Enclosure A3 Annual Summary Report Form

1. Annual Statistics by Incident Categories[5]

Category	Description	Amount
0	Simulation event for training purposes (Training and Exercises)	
1	Unsuccessful attempt to gain unauthorized access (Unsuccessful Activity Attempt)	
2	Activity that seeks to gather information of the agency before attacks (Reconnaissance)	
3	Activity that does not comply with the cybersecurity standard of the agency (Non-Compliance Activity)	
4	Intrusion using a malware (Malicious Logic)	
5	Intrusion at the user level (User Level Intrusion)	
6	Intrusion at the root level (Root Level Intrusion)	
7	Intrusion that prevents access to services (Denial of Service)	
8	Event that is being investigated (Investigating)	
9	Suspicious event determined to be non-malicious (Explained Anomaly)	

2. Annual Statistics by Affected Assets

Affected Assets	Amount
Server/Active Directory	
Workstation	
Switch/Router	
Website	
Others	

[5] These categories are in accordance with Clause 1 in the appendix of the Notification of the National Cyber Security Committee Re: Cyber Incident Characteristics and Measures for Prevention, Response, Assessment, Eradication, and Containment of Incidents at Each Level, B.E. 2564 (2021).

3. Annual Statistics by Incident Levels[6]

Incident Levels	Amount
Non-critical	
Critical	
Crisis (a)	
Crisis (b)	

[6] The cyber incident levels are in accordance with Section 60 of the Cybersecurity Act B.E.2562 (2019).

11

ประกาศ สกมช.

เรื่อง หลักเกณฑ์และอัตราค่าธรรมเนียมค่าบำรุง ค่าตอบแทน และค่าบริการในการดำเนินงาน พ.ศ. 2566

มีผลใช้บังคับตั้งแต่วันที่ 10 พ.ค. 66 เป็นต้นไป

Notification of NCSA

Re: Criteria and Rates of Fees, Maintenance Fees, Compensation Fees, and Service Fees for Operations B.E. 2566 (2023)

effective from September 6, 2023, onwards.



ฉบับภาษาไทย
Thai Version

ประกาศสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

เรื่อง หลักเกณฑ์และอัตราค่าธรรมเนียม ค่าบำรุง ค่าตอบแทน และค่าบริการในการดำเนินงาน

พ.ศ. ๒๕๖๖

โดยที่เป็นการสมควรกำหนดหลักเกณฑ์และอัตราค่าธรรมเนียม ค่าบำรุง ค่าตอบแทน และค่าบริการในการดำเนินงานของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

อาศัยอำนาจตามความในมาตรา ๒๓ (๔) แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ โดยความเห็นชอบของคณะกรรมการบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ ในคราวการประชุมครั้งที่ ๓/๒๕๖๖ เมื่อวันที่ ๔ สิงหาคม ๒๕๖๖ จึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง หลักเกณฑ์และอัตราค่าธรรมเนียม ค่าบำรุง ค่าตอบแทน และค่าบริการในการดำเนินงาน พ.ศ. ๒๕๖๖”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ข้อ ๓ ในประกาศนี้

“ผู้รับบริการ” หมายความว่า บุคคลธรรมดา คณะบุคคล นิติบุคคล หน่วยงานของรัฐ หรือหน่วยงานเอกชน รวมทั้งหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานควบคุมหรือกำกับดูแลที่ได้รับบริการจากสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

“หน่วยงานของรัฐ” หมายความว่า ราชการส่วนกลาง ราชการส่วนภูมิภาค ราชการส่วนท้องถิ่น รัฐวิสาหกิจ องค์กรฝ่ายนิติบัญญัติ องค์กรฝ่ายตุลาการ องค์กรอิสระ องค์การมหาชน และหน่วยงานอื่นของรัฐ

“หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ” หมายความว่า หน่วยงานของรัฐหรือหน่วยงานเอกชน ซึ่งมีภารกิจหรือให้บริการโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

“หน่วยงานควบคุมหรือกำกับดูแล” หมายความว่า หน่วยงานของรัฐ หน่วยงานเอกชน หรือบุคคลซึ่งมีกฎหมายกำหนดให้มีหน้าที่และอำนาจในการควบคุมหรือกำกับดูแลการดำเนินกิจการของหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

“สำนักงาน” หมายความว่า สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

“เลขาธิการ” หมายความว่า เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

ข้อ ๔ ให้สำนักงานเรียกเก็บค่าธรรมเนียมและ/หรือค่าบริการจากผู้รับบริการ สำหรับกรณีดังต่อไปนี้

(๑) การใช้ระบบหรือบริการสารสนเทศ เครื่องมือหรืออุปกรณ์ หรือสิ่งอำนวยความสะดวกและพื้นที่หรือสถานที่

(๒) การใช้บริการสำรวจ การวางแผน การจัดการ หรือการวิจัย ในลักษณะการว่าจ้าง

(๓) การใช้บริการจัดฝึกอบรม สัมมนา หรือประชุมเชิงปฏิบัติการ

(๔) การรับรองมาตรฐานผู้ให้บริการเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

(๕) การใช้บริการดำเนินโครงการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์หรือบริการอื่นที่เกี่ยวกับหรือเกี่ยวเนื่องกับการรักษาความมั่นคงปลอดภัยไซเบอร์

ข้อ ๕ อัตราค่าธรรมเนียมและ/หรือค่าบริการตามข้อ ๔ ให้คำนวณโดยพิจารณาจากปัจจัยดังต่อไปนี้ ประกอบกับปัจจัยเฉพาะที่กำหนดไว้ในแต่ละรายการ ตามตาราง ๑ แนบท้ายประกาศนี้

(๑) จำนวนและความเชี่ยวชาญของทรัพยากรบุคคล

(๒) ระยะเวลาที่ใช้

(๓) ค่าติดตั้งระบบหรืออุปกรณ์

(๔) ค่าบำรุงดูแลรักษาระบบ บริการสารสนเทศ เครื่องมือ อุปกรณ์ หรือสิ่งอำนวยความสะดวก

(๕) จำนวนเครื่อง จำนวนอุปกรณ์ จำนวนซอฟต์แวร์ จำนวนผู้ใช้ จำนวนที่อยู่ไอพี จำนวนเครือข่ายย่อย และปริมาณข้อมูลที่ต้องให้บริการ

(๖) ค่าเช่าหรือค่าใช้จ่ายในการใช้เครื่องมือ อุปกรณ์ ซอฟต์แวร์หรือสิ่งอำนวยความสะดวก รวมถึงค่าสิทธิบัตร และลิขสิทธิ์ซอฟต์แวร์ที่เกี่ยวข้อง

(๗) ค่าพาหนะ ค่าที่พัก หรือค่าเดินทางสำหรับการขนส่งหรือติดตั้ง ระบบ บริการสารสนเทศ เครื่องมือ อุปกรณ์ หรือสิ่งอำนวยความสะดวก

(๘) ค่าเสื่อมราคา

(๙) ค่าใช้จ่ายวัสดุสิ้นเปลือง

(๑๐) ค่าใช้จ่ายในการดำเนินงาน (ไม่เกินร้อยละ ๒๐ ของอัตราค่าธรรมเนียมและ/หรือค่าบริการที่เรียกเก็บ)

ข้อ ๖ ในกรณีที่สำนักงานให้บริการตามข้อ ๔ และมีเหตุจำเป็นต้องใช้ทรัพยากรบุคคลของสำนักงานนอกเหนือจากการปฏิบัติงานตามปกติ หรือใช้บุคลากรภายนอกสำนักงานเป็นผู้ดำเนินการให้บริการ ให้สำนักงานมีสิทธิเรียกค่าตอบแทนจากผู้รับบริการได้

อัตราค่าตอบแทนตามวรรคหนึ่ง ให้เป็นไปตามตาราง ๒ แนบท้ายประกาศนี้

ข้อ ๗ ให้สำนักงานเรียกเก็บค่าบำรุงจากสมาชิกเป็นรายปี โดยอัตราค่าบำรุง ให้เป็นไปตามตาราง ๓ แนบท้ายประกาศนี้

การสมัครเป็นสมาชิกให้เป็นไปตามหลักเกณฑ์และวิธีการที่สำนักงานกำหนด

ข้อ ๘ การเรียกเก็บค่าธรรมเนียมหรือค่าบริการตามข้อ ๔ และ/หรือค่าตอบแทนตามข้อ ๖ สำหรับการให้บริการในแต่ละกรณี ให้สำนักงานตกลงกับผู้รับบริการก่อนการให้บริการ ทั้งนี้ การเรียกเก็บค่าธรรมเนียม หรือค่าบริการหรือค่าตอบแทนดังกล่าว ให้นำราคาตามท้องตลาดหรือจะใช้วิธีการถัวเฉลี่ยราคาตามท้องตลาดมาประกอบการพิจารณาด้วยก็ได้

ในกรณีที่ไม่มีราคาตามท้องตลาดตามวรรคหนึ่ง สำนักงานอาจเรียกเก็บค่าธรรมเนียมหรือค่าบริการ หรือค่าตอบแทน ตามราคาที่ตกลงกับผู้รับบริการโดยคำนึงถึงต้นทุนการดำเนินการ โดยให้อ้างอิงข้อมูลของหน่วยงานควบคุมหรือกำกับดูแล หน่วยงานรัฐ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานเอกชนที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือหน่วยงานในต่างประเทศ

ข้อ ๙ ในกรณีที่ผู้รับบริการเป็นบุคคลที่สำนักงานมีหน้าที่หรือได้รับมอบหมายให้ตรวจสอบการรักษาความมั่นคงปลอดภัยไซเบอร์ของผู้รับบริการ สำนักงานอาจพิจารณาให้บริการแก่ผู้รับบริการได้ ทั้งนี้ โดยให้คำนึงถึงหลักผลประโยชน์ทับซ้อน (conflict of interest) และไม่ขัดต่อกลไกการตรวจสอบและถ่วงดุล (check and balance)

ข้อ ๑๐ ให้เลขาธิการรักษาการตามประกาศนี้ และให้มีอำนาจกำหนดวิธีปฏิบัติเพื่อประโยชน์ในการดำเนินการตามประกาศนี้

ในกรณีที่มีปัญหาเกี่ยวกับการปฏิบัติตามประกาศนี้ หรือประกาศนี้ไม่ได้กำหนดเรื่องใดไว้ให้เลขาธิการมีอำนาจตีความและวินิจฉัยชี้ขาด การตีความและคำวินิจฉัยของเลขาธิการให้เป็นที่สุด

ประกาศ ณ วันที่ ๑๖ สิงหาคม พ.ศ. ๒๕๖๖
พลอากาศตรี อมร ชมเชย
เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

เอกสารแนบท้ายประกาศสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
เรื่อง หลักเกณฑ์และอัตราค่าธรรมเนียม ค่าบำรุง ค่าตอบแทน และค่าบริการในการดำเนินงาน
พ.ศ. ๒๕๖๖

ตาราง ๑ อัตราค่าธรรมเนียมและค่าบริการ

ประเภท	รายการ	เกณฑ์หรืออัตรา
๑. การใช้ระบบหรือบริการสารสนเทศ เครื่องมือหรืออุปกรณ์หรือสิ่งอำนวยความสะดวกและพื้นที่หรือสถานที่	๑.๑ ค่าบริการใช้ระบบหรือบริการสารสนเทศ เครื่องมือ อุปกรณ์หรือสิ่งอำนวยความสะดวก	เป็นรายกรณี ไม่ต่ำกว่า ๕๐,๐๐๐ บาท โดยให้คำนวณจากปัจจัยที่ประกาศกำหนดในข้อ ๕ และรวมถึงปัจจัยเฉพาะต่อไปนี้ (๑) ค่าอบรมการใช้ระบบ บริการสารสนเทศ หรือสิ่งอำนวยความสะดวก (๒) ต้นทุนการพัฒนาระบบ บริการสารสนเทศ หรือสิ่งอำนวยความสะดวก (๓) ค่าทดสอบไอเดียธุรกิจก่อนเริ่มโปรเจค (proof of concept) (๔) ค่าใช้จ่ายอื่น ๆ
	๑.๒ ค่าบริการใช้พื้นที่หรือสถานที่	คำนวณรายวัน (หนึ่งวันไม่เกิน ๘ ชั่วโมง) ดังนี้ - ห้องสัมมนา ๑๐ - ๑๐๐ คน ๒๐๐ บาท ต่อคน ต่อวัน - ห้องฝึกอบรม ๑๕ - ๑๐๐ คน ๕๐๐ บาท ต่อคน ต่อวัน - หอประชุม ๑๖๐ - ๒๘๕ คน ๒๐๐ บาท ต่อคน ต่อวัน
๒. การใช้บริการสำรวจ การวางแผน การจัดการหรือการวิจัยในลักษณะการว่าจ้าง	๒.๑ ค่าบริการในการวิเคราะห์และประเมินความเสี่ยงให้สอดคล้องกับมาตรฐานหลักธรรมาภิบาล และกฎหมาย	เป็นรายกรณี ไม่ต่ำกว่า ๒๐๐,๐๐๐ บาท โดยให้คำนวณจากปัจจัยที่ประกาศกำหนดในข้อ ๕ และรวมถึงปัจจัยเฉพาะต่อไปนี้ (๑) ขนาดขององค์กรผู้รับบริการ (๒) ความซับซ้อน และรายละเอียดของมาตรฐานการประเมินความเสี่ยง (๓) ค่าใช้จ่ายอื่น ๆ
	๒.๒ ค่าบริการในการจัดการเหตุภัยคุกคามทางไซเบอร์	เป็นรายกรณี ไม่ต่ำกว่า ๓๐,๐๐๐ บาท โดยให้คำนวณจากปัจจัยที่ประกาศกำหนดในข้อ ๕ และรวมถึงปัจจัยเฉพาะต่อไปนี้ (๑) ระดับผลกระทบของภัยคุกคามทางไซเบอร์และความเร่งด่วน (๒) ความซับซ้อนของภัยคุกคามที่เกิดขึ้น (๓) จำนวนสถานที่ที่ได้รับผลกระทบ

ประเภท	รายการ	เกณฑ์หรืออัตรา
		(๔) ค่าประกันความเสียหายที่อาจเกิดขึ้นจากการจัดการเหตุภัยคุกคาม (๕) ค่าขนย้ายอุปกรณ์เครื่องมือ (๖) ค่าใช้จ่ายอื่น ๆ
	๒.๓ ค่าบริการในการวิเคราะห์เพื่อจัดทำ/ทบทวนนโยบายหรือแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์[๑]	เป็นรายกรณี ไม่ต่ำกว่า ๒๐๐,๐๐๐ บาท โดยให้คำนวณจากปัจจัยที่ประกาศกำหนดในข้อ ๕ และรวมถึงปัจจัยเฉพาะต่อไปนี้ (๑) ขนาดขององค์กรผู้รับบริการ (๒) ความซับซ้อนของนโยบายหรือแผน (๓) จำนวนนโยบายหรือแผน (๔) ค่าใช้จ่ายอื่น ๆ
	๒.๔ ค่าบริหารจัดการระบบความมั่นคงปลอดภัยไซเบอร์ (Managed Security Service)	เป็นรายกรณีไม่ต่ำกว่า ๒,๐๐๐,๐๐๐บาท โดยให้คำนวณจากปัจจัยที่ประกาศกำหนดในข้อ ๕ และรวมถึงปัจจัยเฉพาะต่อไปนี้ (๑) จำนวนอาคารที่ต้องให้บริการ (๒) ความซับซ้อนของประเภทบริการ และระดับการให้บริการ (service levels) (๓) ค่าใช้จ่ายอื่น ๆ
	๒.๕ ค่าบริการทำวิจัย	เป็นรายกรณีไม่ต่ำกว่า ๑๐๐,๐๐๐ บาท โดยให้คำนวณจากปัจจัยที่ประกาศกำหนดในข้อ ๕ และรวมถึงปัจจัยเฉพาะต่อไปนี้ (๑) ขอบเขตงานวิจัย (๒) ต้นทุนการพัฒนาระบบสารสนเทศ หรืออุปกรณ์ที่เกี่ยวข้องกับงานวิจัย (๓) มูลค่าทางเศรษฐศาสตร์ในปัจจุบันของงานวิจัยและรายได้จากการนำงานวิจัยไปพัฒนาหรือใช้ประโยชน์ (๔) ค่าใช้จ่ายอื่น ๆ
๓. การใช้บริการจัดฝึกอบรม สัมมนาหรือประชุมเชิงปฏิบัติการ	ค่าบริการจัดฝึกอบรม สัมมนาหรือประชุมเชิงปฏิบัติการ	เป็นรายกรณีไม่ต่ำกว่า ๑๐๐,๐๐๐ บาท โดยให้คำนวณจากปัจจัยที่ประกาศกำหนดในข้อ ๕ และรวมถึงปัจจัยเฉพาะต่อไปนี้ (๑) ค่าบริหารหลักสูตร (๒) ค่าตอบแทนอาจารย์ประจำหลักสูตร วิทยากร ผู้ช่วยวิทยากร ที่ปรึกษาโครงการ และบุคลากรฝ่ายสนับสนุน (๓) เรื่องหรือหัวข้อในการฝึกอบรม (๔) ค่าเช่าอาคารสถานที่สำหรับการฝึกอบรม

<table>
<tr><th>ประเภท</th><th>รายการ</th><th colspan="3">เกณฑ์หรืออัตรา</th></tr>
<tr><td></td><td></td><td colspan="3">(๕) จำนวนผู้เข้าอบรม
(๖) เงินอุดหนุนที่ได้รับการสนับสนุนจากรัฐ หรืองบประมาณสนับสนุนจากแหล่งอื่น
(๗) ค่าใช้จ่ายอื่น ๆ</td></tr>
<tr><td rowspan="4">๔. การรับรองมาตรฐานผู้ให้บริการเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์
(ทั้งนี้ หากมีค่าใช้จ่ายในการดำเนินการในการส่งพนักงานหรือบุคลากรภายนอกสำนักงานไปดำเนินการ สำนักงานมีสิทธิเรียกค่าตอบแทนจากผู้รับบริการได้)</td><td rowspan="2">๔.๑ ค่าธรรมเนียมการรับรองมาตรฐานผู้ให้บริการด้านความมั่นคงปลอดภัยไซเบอร์[๒]</td><td>ขั้นต้น
(บาท)</td><td>ขั้นก้าวหน้า
(บาท/วัน)</td><td>ขั้นสูง
(บาท/วัน)</td></tr>
<tr><td>(๑) ประเภทบุคคลธรรมดาหรือคณะบุคคล
(๒) ประเภทนิติบุคคล</td><td>๑๐,๐๐๐
๒๐,๐๐๐</td><td>๑๘,๐๐๐
๔๐,๐๐๐</td><td>-
๔๐,๐๐๐</td></tr>
<tr><td rowspan="2">๔.๒ ค่าธรรมเนียมการต่ออายุการรับรองมาตรฐานผู้ให้บริการด้านความมั่นคงปลอดภัยไซเบอร์[๒]</td><td>ขั้นต้น
(บาท)</td><td>ขั้นก้าวหน้า
(บาท/วัน)</td><td>ขั้นสูง
(บาท/วัน)</td></tr>
<tr><td>(๑) ประเภทบุคคลธรรมดาหรือคณะบุคคล
(๒) ประเภทนิติบุคคล</td><td>๕,๐๐๐
๑๐,๐๐๐</td><td>๑๘,๐๐๐
๔๐,๐๐๐</td><td>-
๔๐,๐๐๐</td></tr>
<tr><td colspan="5">หมายเหตุ :
(๑) ตามที่กำหนดในประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔
(๒) การเก็บค่าธรรมเนียมการรับรองมาตรฐานตามข้อ ๔.๑ และ ๔.๒ เป็นการเก็บค่าธรรมเนียมแยกแต่ละประเภทของผู้ให้บริการด้านความมั่นคงปลอดภัยไซเบอร์ ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ว่าด้วยมาตรฐานและแนวทางส่งเสริมพัฒนาระบบการให้บริการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ ทั้งนี้การคิดค่าธรรมเนียมการรับรองมาตรฐานขั้นก้าวหน้าและขั้นสูงให้คิดตามจำนวนวันที่สัมภาษณ์หรือเข้าตรวจประเมินขั้นตอน กระบวนการดำเนินงาน และการให้บริการ ณ สถานประกอบการ</td></tr>
<tr><td>๕. การใช้บริการดำเนินโครงการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์หรือบริการอื่นที่เกี่ยวกับหรือเกี่ยวเนื่องกับการรักษาความมั่นคงปลอดภัยไซเบอร์</td><td>๕.๑ ค่าธรรมเนียมการใช้งานทรัพย์สินทางปัญญา</td><td colspan="3">เป็นรายกรณีไม่ต่ำกว่า ๕๐๐,๐๐๐ บาท ให้คำนวณจากปัจจัยที่ประกาศกำหนดในข้อ ๕ และรวมถึงปัจจัยเฉพาะต่อไปนี้
(๑) ต้นทุนต่าง ๆ เพื่อให้ได้มาซึ่งทรัพย์สินทางปัญญา
(๒) มูลค่าเชิงเศรษฐศาสตร์ของทรัพย์สินทางปัญญาในปัจจุบัน และรายได้ของผู้รับบริการที่อาจเกิดขึ้นจากการใช้งานทรัพย์สินทางปัญญา
(๓) ระยะเวลาและปริมาณการใช้ทรัพย์สินทางปัญญา
(๔) ค่าใช้จ่ายในการจดทะเบียนทรัพย์สินทางปัญญาทั้งในและต่างประเทศ
(๕) ค่าใช้จ่ายอื่น ๆ</td></tr>
</table>

ประเภท	รายการ	เกณฑ์หรืออัตรา
	๕.๒ ค่าธรรมเนียมหรือค่าบริการอื่นตามที่สำนักงานกำหนด	เป็นรายกรณีโดยให้พิจารณาเทียบเคียงจากการให้บริการที่ใกล้เคียงกันหรือมีลักษณะในทำนองเดียวกัน

หมายเหตุ : ๑. เกณฑ์หรืออัตราที่กำหนดยังไม่รวมภาษีมูลค่าเพิ่ม (ถ้ามี)

๒. ในกรณีที่ผู้รับบริการไม่ได้รับบริการหรือสำนักงานมีเหตุขัดข้องที่ไม่อาจให้บริการได้ตามประกาศนี้ สำนักงานมีอำนาจพิจารณาคืนเงินค่าธรรมเนียมหรือค่าบริการ ค่าบำรุง หรือค่าตอบแทนทั้งหมดหรือบางส่วนให้แก่ผู้รับบริการได้

ตาราง ๒ อัตราค่าตอบแทน

รายการ	อัตรา (บาท)	หน่วย
๑. ค่าตอบแทนในการใช้ทรัพยากรบุคคลของสำนักงานนอกเหนือจากการปฏิบัติงานตามปกติ	กรณีบุคลากรในตำแหน่งต่ำกว่าผู้อำนวยการ ให้เป็นไปตามอัตราค่าตอบแทนการปฏิบัติงานนอกเวลาราชการในอัตราสูงสุดของตำแหน่งนั้น ตามระเบียบ ข้อบังคับ ประกาศ หรือหลักเกณฑ์อื่นที่สำนักงานกำหนด กรณีบุคลากรในตำแหน่งสูงกว่าผู้อำนวยการขึ้นไป ให้ได้รับในอัตรา ๒,๕๐๐ บาท/ชั่วโมง	ชั่วโมง/วัน
๒. ค่าตอบแทนในการจัดหาบุคลากรภายนอกสำนักงานเพื่อดำเนินกิจกรรมหรือโครงการ	รายกรณี	กิจกรรม/โครงการ

ตาราง ๓ อัตราค่าบำรุง

ประเภทสมาชิก	อัตรา (บาท)
๑. ค่าบำรุง (รายปี) (สำหรับนิติบุคคล)	๑๕๐,๐๐๐
๒. ค่าบำรุง (รายปี) (สำหรับบุคคลธรรมดาหรือคณะบุคคล)	๕,๐๐๐



ฉบับภาษาอังกฤษ
English Version

Notification of the National Cyber Security Agency

Re: Criteria and Rates of Fees, Maintenance Fees, Compensation Fees, and Service Fees for Operations

B.E. 2566 (2023)

Whereas it is deemed appropriate to determine criteria and rates of fees, maintenance fees, compensation fees, and service fees for operations performed by the National Cyber Security Agency.

By virtue of Section 23 (4) of the Cybersecurity Act B.E. 2562 (2019), the National Cyber Security Agency, with approval of the Committee Managing the Office of the National Cyber Security Committee from the meeting no. 3/2566 on 4 August B.E. 2566 (2023), hereby issues the following notification:

Clause 1 This notification shall be called the "Notification of the National Cyber Security Agency Re: Criteria and Rates of Fees, Maintenance Fees, Compensation Fees, and Service Fees for Operations B.E.2566 (2023)".

Clause 2 This notification shall come into force on the date after its publication in the Royal Thai Government Gazette.

Clause 3 In this notification,

"Service Recipient" shall mean a person, a group of persons, a juristic person, a Government Agency, or a private organization, which include Organizations of Critical Information Infrastructure and Regulators that receive services from the National Cyber Security Agency;

"Government Agency" shall mean the central government, regional government, local government, state enterprises, legislative institutions, judicial institutions, independent institutions, public organizations, and other agencies belonging to the Government;

"Organization of Critical Information Infrastructure" shall mean a Government Agency or a private organization who provides Critical Information Infrastructure services or has a mission to do so;

"Regulator" shall mean a Government Agency, a private organization, or a person that is appointed by law to have the duties and powers to supervise or regulate operations of the Government Agency or Organization of Critical Information Infrastructure;

"Agency" shall mean the National Cyber Security Agency;

"Secretary-General" shall mean the Secretary-General of the National Cyber Security Committee.

Clause 4 The Agency shall collect fees and/or service fees from the Service Recipient in the following cases:

(1) use of information systems or services, tools or equipment, or facilities, and spaces or venues;

(2) use of survey, planning, managing, or research services as a work for hire;

(3) use of training, seminar, or workshop services;

(4) standard cybersecurity certification for service providers;

(5) use of services in running a cybersecurity project or other services related to or in connection with cybersecurity.

Clause 5 Rates of fees and/or service fees in Clause 4 shall consider the following factors together with specific factors prescribed for each item in Table 1 in the attached enclosure:

(1) number and expertise of human resources;

(2) usage duration;

(3) system and equipment installation costs

(4) costs for maintaining systems, information services, tools, equipment or facilities;

(5) number of machines, equipment, software, users, IP addresses, subnets, and amount of data required to provide services;

(6) rental or usage costs for machines, tools, equipment, software, or facilities, including patent and software copyright fees;

(7) vehicle costs, accommodations, or transportation expenses for transporting or setting up systems, information services, tools, equipment, or facilities;

(8) depreciation;

(9) cost of consumables;

(10) operating expenses (not exceeding 20 percent of the collected fee and/or service fee).

Clause 6 In providing services in Clause 4, should the Agency require the use of human resources overtime or a third party to provide the services, the Agency shall have the rights to collect compensation fees from the Service Recipient.

The fee rate in paragraph one shall be in accordance with Table 2 in the attached enclosure.

Clause 7 The Agency shall collect the annual maintenance fee from the members. The fee shall be in accordance with Table 3 in the attached enclosure.

Membership application shall follow the criteria and procedures prescribed by the Agency.

Clause 8 Any fee or service fee collected in accordance with Clause 4 and/or Clause 6 for a service shall be mutually agreed by the Agency and the Service Recipient in advance. Nonetheless, the calculation of such fee or service fee or compensation fee may take into account the market price or the average market price.

If the market price mentioned in paragraph one is unavailable, the Agency may collect fees or service fees or compensation fees in the rate agreed with the Service Recipient. The calculation of such fees shall take into account the initial investment cost and refer to information from the Regulator, Government Agencies, Organizations of Critical Information Infrastructure, private organizations specialized in cybersecurity or foreign agencies.

Clause 9 If the Service Recipient is a person for whom the Agency has duties or is assigned to evaluate/audit the cybersecurity posture, the Agency may consider providing services to the Service Recipient. However, the Agency shall take into account the conflict of interest and ensure that any services provided do not compromise the check and balance.

Clause 10 The Secretary-General shall have charge and control of this notification and shall have the powers to prescribe procedures that are conducive to the effective execution of tasks in accordance with the provisions outlined in this notification.

If a problem related to the compliance with this notification has occurred, or the notification does not cover a particular matter, the Secretary-General shall have the powers to provide interpretations and render decisions on matters related to the enforcement of compliance with this notification, and the decision shall be deemed final.

Given on the 16th of August B.E. 2566 (2023)

Air Vice Marshal Amorn Chomchoey

(Amorn Chomchoey)

Secretary-General of the National Cyber Security Committee

Enclosure of the Notification of the National Cyber Security Agency

Re: Criteria and Rates of Fees, Maintenance Fees, Compensation Fees, and Service Fees for Operations

B.E. 2566 (2023)

Table 1 Rates of Fees and Service Fees

Category	Item	Criteria or Rate
1.1 Usage of information systems or services, tools or equipment, or facilities, and spaces or venues	1.1 Usage fees for information systems or services, tools, equipment, or facilities	On a case-by-case basis but not less than 50,000 Baht, calculated from the factors prescribed in Clause 5 of this notification and the following specific factors: (1) fees for training on how to use systems, information services, or facilities; (2) investment costs of developing systems, information services, or facilities; (3) costs of running proof-of-concept; (4) other expenses.
	1.2 Usage fees for spaces and venues	Daily calculation (no more than 8 hours per day) as follows: - seminar room for 10-100 people 200 Baht per person per day - training room for 15-100 people 500 Baht per person per day - auditorium for 160-285 people 200 Baht per person per day.
2. Usage of surveying, planning, managing, or researching services as a work for hire	2.1 Service fees for risk analysis and assessment in accordance with the standards, good governance, and laws.	On a case-by-case basis but not less than 200,000 Baht, calculated from the factors prescribed in Clause 5 of this notification and the following specific factors: (1) size of the organization of the Service Recipient; (2) complexity and details of risk assessment standards;

Category	Item	Criteria or Rate
		(3) other expenses.

Category	Item	Criteria or Rate
	2.2 Fees for managing cyber incidents	On a case-by-case basis but not less than 30,000 Baht, calculated from the factors prescribed in Clause 5 of this notification and the following specific factors: (1) impact and urgency level of cyber incidents; (2) incident complexity; (3) number of locations affected; (4) insurance premium that may occur from handling the incident; (5) costs of transporting equipment and tools; (6) other expenses.
	2.3 Analysis service fees for preparing/reviewing cybersecurity policies or plans(1)	On a case-by-case basis but not less than 200,000 Baht, calculated from the factors prescribed in Clause 5 of this notification and the following specific factors: (1) size of the organization of the Service Recipient; (2) complexity of the policies or plans; (3) number of policies or plans; (4) other expenses.
	2.4 Managed Security Service fees	On a case-by-case basis but not less than 2,000,000 Baht, calculated from the factors prescribed in Clause 5 of this notification and the following specific factors: (1) number of buildings covered; (2) complexity of service type and service level; (3) other expenses.
	2.5 Researching service	On a case-by-case basis but not less than 100,000 baht, calculated from the factors

Category	Item	Criteria or Rate
		prescribed in Clause 5 of this notification and the following specific factors: (1) scope of research; (2) investment cost of developing IT systems or equipment relevant to the research; (3) current economic value of the research and income from implementation or utilization of the research; (4) Other expenses.
3. Usage of training, seminar, or workshop services	Training, seminar, or workshop service fees	On a case-by-case basis but not less than 100,000 baht, calculated from the factors prescribed in Clause 5 of this notification and the following specific factors: (1) course management fee; (2) compensation fee for course instructors, trainers, trainer assistants, course consultants, and supporting personnel; (3) training subjects or topics; (4) training venue rental fee; (5) number of participants; (6) government funding or external source of finance; (7) other expenses.

Category	Item	Criteria or Rate		
4. Standard certification accreditation for cybersecurity service providers (If an expense occurs from deploying employees or external personnel to deliver services outside the Agency, the Agency shall have the rights to collect compensation fees from the Service Recipient.)	4.1 Standard certification accreditation fee for cybersecurity service providers[(2)]	Primary (Baht)	Progressive (Baht/Day)	Advance (Baht/Day)
	(1) persons or group of persons	10,000	18,000	-
	(2) juristic persons	20,000	40,000	40,000
	4.2 Standard certification renewal fee for cybersecurity service providers[(2)]	Primary (Baht)	Progressive (Baht/Day)	Advance (Baht/Day)
	(1) persons or groups of persons	5,000	18,000	-
	(2) juristic persons	10,000	40,000	40,000

Notes:

(1) As prescribed in the Notification of the Cybersecurity Regulating Committee Re: Codes of Practice and Cybersecurity Standard Frameworks for Government Agencies and Organizations of Critical Information Infrastructure B.E. 2564 (2021)

(2) Standard certification fee in Clause 4.1 and 4.2 will be categorized by the type of cybersecurity service providers in accordance with the Notification of the National Cyber Security Committee Re: Standard and Guideline in Supporting and Developing Cybersecurity Service System. The progress and advance standard certification fee will be calculated from the number of days required to conduct interviews or examine procedures, the process of operation, and the delivery of service at the establishment.

Category	Item	Criteria or Rate
5. Usage of services in running cybersecurity projects or other cybersecurity related services	5.1 Intellectual property usage fee	On a case-by-case basis but not less than 500,000 baht, calculated from the factors prescribed in Clause 5 and the following specific factors: (1) costs in acquiring intellectual property; (2) current economic value of intellectual properties and the income that the Service Recipient may receive from the use of the intellectual property; (3) usage duration and usage amount of intellectual property; (4) intellectual property registration cost domestically and abroad; (5) other expenses.
	5.2 Other fees and service fees as prescribed by the Agency	Will be considered on a case-by-case basis by comparing with similar services or services of the same nature

Notes : 1. The prescribed criteria or rates have not yet included vat (if any).

2. If the Service Recipient does not receive the service, or a cause arises and prevents the Agency from providing services in this notification, the Agency has the powers to consider refunding the fee or service fee, maintenance fee or compensation fee to the Service Recipient in part or in full.

Table 2 Compensation Fee Rate

Item	Rate (Baht)	Unit
1. Compensation fee for using the Agency's personnel overtime	If the person holds a position below the directorship level, the compensation fee shall be at the highest overtime rate applicable to the position, as outlined in the regulations, rules, notifications, or other criteria provided by the Agency. If a person holds a position above the directorship level, the compensation fee shall be at 2,500 Baht/hour.	hour/day
2. Compensation fee for recruiting personnel outside the Agency to carry out activities or projects	on a case-by-case basis	activity/project

Table 3 Maintenance Fee Rate

Membership Type	Rate (Baht)
1. Maintenance fee (annual) (for juristic persons)	150,000
2. Maintenance fee (annual) (for persons or groups of persons)	5,000

12

ประกาศ กมช.

เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. 2566

มีผลใช้บังคับตั้งแต่วันที่ 18 ม.ค. 68 เป็นต้นไป

Notification of NCSC

Re: Standards for defining cybersecurity characteristics for data or information systems B.E. 2566 (2023)

effective from January 18, 2025, onwards.



ฉบับภาษาไทย
Thai Version

ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์
ให้แก่ข้อมูลหรือระบบสารสนเทศ
พ.ศ. ๒๕๖๖

โดยที่พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดให้คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติมีหน้าที่และอำนาจสร้างมาตรฐานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ และกำหนดมาตรฐานขั้นต่ำที่เกี่ยวข้องกับคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือโปรแกรมคอมพิวเตอร์ จึงสมควรมีมาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ เพื่อประเมินและจัดระดับผลกระทบที่อาจเกิดขึ้นแก่ข้อมูลหรือระบบสารสนเทศอันจะนำไปสู่การเลือกมาตรการในการควบคุมความมั่นคงปลอดภัยไซเบอร์ที่เหมาะสม เพื่อให้การดำเนินงานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์เป็นไปอย่างมีประสิทธิภาพ

อาศัยอำนาจตามความในมาตรา ๙ (๔) แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ประกอบกับมติที่ประชุมคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ในคราวการประชุมครั้งที่ ๔/๒๕๖๖ เมื่อวันที่ ๒๘ พฤศจิกายน ๒๕๖๖ คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ จึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. ๒๕๖๖”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับเมื่อพ้นกำหนดหนึ่งปีนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ข้อ ๓ ในประกาศนี้

“ประเภทข้อมูล” หมายความว่า หมวดหมู่ข้อมูลที่ถูกกำหนดขึ้นโดยหน่วยงานตามแนวทางที่สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติประกาศกำหนด

“ระบบสารสนเทศ” หมายความว่า ระบบหรือชุดทรัพยากรด้านสารสนเทศที่ถูกใช้สำหรับการเก็บรวบรวม การประมวลผล การบำรุงรักษา การใช้ การเผยแพร่ หรือการทำลายข้อมูล

“คุณลักษณะความมั่นคงปลอดภัยไซเบอร์” (Security category) หมายความว่า ลักษณะเฉพาะของข้อมูลหรือระบบสารสนเทศในด้านความมั่นคงปลอดภัยไซเบอร์ ตามการประเมินและจัดระดับผลกระทบต่อการดำเนินงานของหน่วยงาน ทรัพย์สินของหน่วยงาน หรือความปลอดภัยของผู้ใช้บริการของหน่วยงาน บุคลากรของหน่วยงาน หรือประชาชน ที่อาจเกิดขึ้นเมื่อข้อมูลลับของหน่วยงานรั่วไหล ข้อมูลของหน่วยงานถูกลบถูกบิดเบือน หรือถูกทำลาย หรือข้อมูลหรือระบบสารสนเทศของหน่วยงานไม่อยู่ในสภาพพร้อมใช้งาน

“การรักษาความลับ” (Confidentiality) หมายความว่า การรักษาหรือสงวนไว้ ซึ่งการจำกัดการเข้าถึงหรือการเปิดเผยข้อมูลให้แก่บุคคล หน่วยงานอื่น หรือชุดคำสั่งที่ไม่ได้รับอนุญาต

“การรักษาความถูกต้องครบถ้วน” (Integrity) หมายความว่า การรักษาหรือสงวนไว้ ซึ่งความถูกต้องและความครบถ้วนของข้อมูล

“การรักษาสภาพพร้อมใช้งาน” (Availability) หมายความว่า การดำเนินการ เพื่อให้บุคคล หน่วยงาน หรือชุดคำสั่งที่ได้รับอนุญาตสามารถเข้าถึงและใช้งานข้อมูลหรือระบบสารสนเทศได้ตามต้องการและได้อย่างมีประสิทธิภาพ

“หน่วยงาน” หมายความว่า หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

ข้อ ๔ ให้หน่วยงานกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ โดยพิจารณาวัตถุประสงค์ด้านความมั่นคงปลอดภัยไซเบอร์ (Security objectives) ในเรื่องดังต่อไปนี้

(๑) การรักษาความลับ (Confidentiality)

(๒) การรักษาความถูกต้องครบถ้วน (Integrity)

(๓) การรักษาสภาพพร้อมใช้งาน (Availability)

ในกรณีที่ข้อมูลหรือระบบสารสนเทศได้เผยแพร่ต่อสาธารณะแล้ว หน่วยงานไม่ต้องพิจารณาวัตถุประสงค์ตามวรรคหนึ่ง (๑)

ข้อ ๕ การพิจารณาวัตถุประสงค์ตามข้อ ๔ วรรคหนึ่ง (๑) (๒) และ (๓) ให้ประเมินและจัดระดับผลกระทบที่อาจเกิดขึ้นเป็นสามระดับ ได้แก่ ระดับต่ำ ระดับกลาง และระดับสูง

ข้อ ๖ การจัดระดับผลกระทบที่อาจเกิดขึ้นในแต่ละระดับตามข้อ ๕ ให้หน่วยงานพิจารณาการประเมินผลกระทบในแต่ละด้าน ดังต่อไปนี้

(๑) ผลกระทบต่อมูลค่าความเสียหายทางการเงินหรือทรัพย์สิน หรือต่อชื่อเสียงของหน่วยงาน

(๒) ผลกระทบต่อจำนวนของผู้ใช้บริการของหน่วยงาน บุคลากรของหน่วยงาน หรือประชาชนที่อาจได้รับอันตรายต่อชีวิต ร่างกาย อนามัย ทรัพย์สิน หรือความเสียหายอื่นใด

(๓) ผลกระทบต่อความสามารถในการดำเนินการตามหน้าที่ของหน่วยงาน

(๔) ผลกระทบต่อความมั่นคงของรัฐและความสงบเรียบร้อยภายในประเทศ

ในกรณีหน่วยงานที่จัดระดับผลกระทบที่อาจเกิดขึ้นเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ให้หน่วยงานควบคุมหรือกำกับดูแลกำหนดแนวทางการประเมินผลกระทบตามวรรคหนึ่งให้แก่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ทั้งนี้ ในกรณีที่สถานการณ์ด้านความมั่นคงปลอดภัยไซเบอร์เปลี่ยนแปลงไป หน่วยงานควบคุมหรือกำกับดูแลอาจกำหนดผลกระทบเพิ่มเติม หรือยกเว้นหรือยกเลิกผลกระทบข้อใดข้อหนึ่งหรือหลายข้อก็ได้

ข้อ ๗ การประเมินและจัดระดับผลกระทบที่อาจเกิดขึ้นสำหรับการพิจารณาวัตถุประสงค์ในการรักษาความลับตามข้อ ๔ (๑) ให้มีเกณฑ์การประเมินและจัดระดับ ดังต่อไปนี้

(๑) ในกรณีที่การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตไม่ว่าทั้งหมดหรือบางส่วน อาจส่งผลกระทบต่อการดำเนินงาน ทรัพย์สิน หรือชื่อเสียงของหน่วยงานหรือบุคคลเพียงเล็กน้อยหรืออย่างจำกัดให้จัดเป็นผลกระทบระดับต่ำ

(๒) ในกรณีที่การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตไม่ว่าทั้งหมดหรือบางส่วน อาจส่งผลกระทบต่อการดำเนินงาน ทรัพย์สิน หรือชื่อเสียงของหน่วยงานหรือบุคคลอย่างร้ายแรง ให้จัดเป็นผลกระทบระดับกลาง

(๓) ในกรณีที่การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตไม่ว่าทั้งหมดหรือบางส่วน อาจส่งผลกระทบต่อการดำเนินงาน ทรัพย์สิน หรือชื่อเสียงของหน่วยงานหรือบุคคลอย่างร้ายแรงมากให้จัดเป็นผลกระทบระดับสูง

ในกรณีที่การดำเนินการของหน่วยงานอาจเปิดเผยข้อมูลที่ถูกกำหนดชั้นความลับตามระเบียบว่าด้วยการรักษาความลับของทางราชการและระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ ให้มีเกณฑ์การประเมินและจัดระดับ ดังต่อไปนี้

(๑) กรณีที่อาจเปิดเผยข้อมูลลับที่ถูกกำหนดชั้นความลับเป็นชั้นลับ ให้จัดเป็นผลกระทบระดับต่ำเป็นอย่างน้อย

(๒) กรณีที่อาจเปิดเผยข้อมูลลับที่ถูกกำหนดชั้นความลับเป็นชั้นลับมาก ให้จัดเป็นผลกระทบระดับกลางเป็นอย่างน้อย

(๓) กรณีที่อาจเปิดเผยข้อมูลลับที่ถูกกำหนดชั้นความลับเป็นชั้นลับที่สุด ให้จัดเป็นผลกระทบระดับสูง

ข้อ ๘ การประเมินและจัดระดับผลกระทบที่อาจเกิดขึ้นสำหรับการพิจารณาวัตถุประสงค์ในการรักษาความถูกต้องครบถ้วนตามข้อ ๔ (๒) ให้มีเกณฑ์การประเมินและจัดระดับ ดังต่อไปนี้

(๑) ในกรณีที่การแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบต่อการดำเนินงานหรือทรัพย์สินของหน่วยงานหรือบุคคลเพียงเล็กน้อยหรืออย่างจำกัด ให้จัดเป็นผลกระทบระดับต่ำ

(๒) ในกรณีที่การแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบต่อการดำเนินงานหรือทรัพย์สินของหน่วยงานหรือบุคคลอย่างร้ายแรง ให้จัดเป็นผลกระทบระดับกลาง

(๓) ในกรณีที่การแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบต่อการดำเนินงานหรือทรัพย์สินของหน่วยงานหรือบุคคลอย่างร้ายแรงมาก ให้จัดเป็นผลกระทบระดับสูง

ข้อ ๙ การประเมินและจัดระดับผลกระทบที่อาจเกิดขึ้นสำหรับการพิจารณาวัตถุประสงค์ในการรักษาสภาพพร้อมใช้งานตามข้อ ๔ (๓) ให้มีเกณฑ์การประเมินและจัดระดับ ดังต่อไปนี้

(๑) ในกรณีที่หน่วยงานไม่สามารถเข้าถึงและใช้งานข้อมูลหรือระบบสารสนเทศได้ อาจส่งผลกระทบต่อการดำเนินงานหรือทรัพย์สินของหน่วยงานหรือบุคคลเพียงเล็กน้อยหรืออย่างจำกัด ให้จัดเป็นผลกระทบระดับต่ำ

(๒) ในกรณีที่หน่วยงานไม่สามารถเข้าถึงและใช้งานข้อมูลหรือระบบสารสนเทศได้ อาจส่งผลกระทบต่อการดำเนินงานหรือทรัพย์สินของหน่วยงานหรือบุคคลอย่างร้ายแรง ให้จัดเป็นผลกระทบระดับกลาง

(๓) ในกรณีที่หน่วยงานไม่สามารถเข้าถึงและใช้งานข้อมูลหรือระบบสารสนเทศได้ อาจส่งผลกระทบต่อการดำเนินงานหรือทรัพย์สินของหน่วยงานหรือบุคคลอย่างร้ายแรงมาก ให้จัดเป็นผลกระทบระดับสูง

ข้อ ๑๐ การกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ของระบบสารสนเทศ ในกรณีที่ระบบสารสนเทศมีข้อมูลหลายประเภทข้อมูล ให้หน่วยงานดำเนินการ ดังต่อไปนี้

(๑) ประเมินและจัดระดับผลกระทบที่อาจเกิดขึ้นสำหรับการพิจารณาวัตถุประสงค์ด้านความมั่นคงปลอดภัยไซเบอร์ตามข้อ ๔ ให้แก่แต่ละประเภทข้อมูล

(๒) พิจารณากำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ของระบบสารสนเทศ โดยใช้ระดับผลกระทบของประเภทข้อมูลตามวัตถุประสงค์ด้านความมั่นคงปลอดภัยไซเบอร์ตามข้อ ๔ ในแต่ละเรื่องที่มีระดับผลกระทบมากที่สุด

หน่วยงานอาจดำเนินการกำหนดประเภทข้อมูลตามหลักเกณฑ์ของหน่วยงาน หรือตามแนวทางในประกาศสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ว่าด้วยแนวทางการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ

ข้อ ๑๑ ให้หน่วยงานพิจารณาทบทวนการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศทุก ๓ ปีเป็นอย่างน้อย หรือทบทวนเมื่อข้อมูล ระบบสารสนเทศ หรือหน้าที่ของหน่วยงานมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ และบันทึกผลการพิจารณาทบทวนพร้อมเหตุผลในการคงไว้ หรือแก้ไขเปลี่ยนแปลงระดับผลกระทบที่อาจเกิดขึ้นของวัตถุประสงค์ด้านความมั่นคงปลอดภัยไซเบอร์ ตามข้อ ๔ ในแต่ละเรื่องด้วย

ข้อ ๑๒ ให้เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ รักษาการตามประกาศนี้ และให้มีอำนาจออกประกาศ คำสั่ง หลักเกณฑ์และวิธีการเพื่อปฏิบัติตามประกาศนี้

ในกรณีที่มีปัญหาเกี่ยวกับการปฏิบัติตามประกาศนี้ หรือประกาศนี้ไม่ได้กำหนดเรื่องใดไว้ ให้ประธานกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เป็นผู้มีอำนาจตีความและวินิจฉัยชี้ขาด ทั้งนี้ การตีความและคำวินิจฉัยของประธานกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติให้เป็นที่สุด

ประกาศ ณ วันที่ ๑๘ ธันวาคม พ.ศ. ๒๕๖๖
ภูมิธรรม เวชยชัย
รองนายกรัฐมนตรี ปฏิบัติหน้าที่
ประธานกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ



ฉบับภาษาอังกฤษ
English Version

อยู่ระหว่างดำเนินการแปลเอกสารเป็นฉบับภาษาอังกฤษ

The translation of the document into English is underway.

13

ประกาศ กมช.

เรื่อง มาตรฐานขั้นต่ำของข้อมูลหรือระบบสารสนเทศ พ.ศ. 2566

มีผลใช้บังคับตั้งแต่วันที่ 18 ม.ค. 68 เป็นต้นไป

Notification of NCSC

Re: standards for data or information systems B.E. 2566 (2023)

effective from January 18, 2025, onwards.



ฉบับภาษาไทย
Thai Version

ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

เรื่อง มาตรฐานขั้นต่ำของข้อมูลหรือระบบสารสนเทศ

พ.ศ. ๒๕๖๖

โดยที่พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดให้คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติมีหน้าที่และอำนาจสร้างมาตรฐานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ และกำหนดมาตรฐานขั้นต่ำที่เกี่ยวข้องกับคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือโปรแกรมคอมพิวเตอร์ จึงสมควรกำหนดมาตรฐานขั้นต่ำของข้อมูลหรือระบบสารสนเทศ เพื่อให้การปฏิบัติงานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์เป็นไปอย่างมีประสิทธิภาพ

อาศัยอำนาจตามความในมาตรา ๙ (๔) แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ประกอบกับมติที่ประชุมคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติในคราวการประชุมครั้งที่ ๔/๒๕๖๖ เมื่อวันที่ ๒๘ พฤศจิกายน ๒๕๖๖ คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ จึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานขั้นต่ำของข้อมูลหรือระบบสารสนเทศ พ.ศ. ๒๕๖๖”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับเมื่อพ้นกำหนดหนึ่งปีนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ข้อ ๓ ในประกาศนี้

“หน่วยงาน” หมายความว่า หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแลและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

“มาตรการควบคุมความมั่นคงปลอดภัยไซเบอร์” หมายความว่า มาตรการที่กำหนดขึ้นเพื่อดำเนินการรักษาความลับ (Confidentiality) การรักษาความถูกต้องครบถ้วน (Integrity) และการรักษาสภาพพร้อมใช้งาน (Availability) สำหรับข้อมูลหรือระบบสารสนเทศ

“ประกาศประมวลแนวทางปฏิบัติและกรอบมาตรฐาน” หมายความว่า ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

ข้อ ๔ ภายหลังจากหน่วยงานได้กำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ ซึ่งพิจารณาจากวัตถุประสงค์ด้านความมั่นคงปลอดภัยไซเบอร์ในเรื่องการรักษาความลับ การรักษาความถูกต้องครบถ้วน และการรักษาสภาพพร้อมใช้งาน และได้ระดับผลกระทบที่อาจเกิดขึ้นตามวัตถุประสงค์แต่ละเรื่องเป็นระดับต่ำ ระดับกลาง หรือระดับสูง ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศแล้ว ให้หน่วยงานกำหนดมาตรการควบคุมความมั่นคงปลอดภัยไซเบอร์ขั้นต่ำ สำหรับข้อมูลหรือระบบสารสนเทศนั้นในแต่ละระดับตามหัวข้อของประกาศประมวลแนวทางปฏิบัติและกรอบมาตรฐานที่กำหนดในตารางท้ายประกาศนี้ ทั้งนี้ โดยพิจารณาจากคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ ดังต่อไปนี้

(๑) ในกรณีที่ข้อมูลหรือระบบสารสนเทศมีคุณลักษณะความมั่นคงปลอดภัยไซเบอร์อยู่ในระดับต่ำ ให้กำหนดมาตรการควบคุมความมั่นคงปลอดภัยไซเบอร์ขั้นต่ำสำหรับข้อมูลหรือระบบสารสนเทศ ตามหัวข้อต่อไปนี้

(ก) การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Assessment)

(ข) แผนการรับมือภัยคุกคามทางไซเบอร์ (Incident Response Plan) (ทั้งในส่วนของประมวลแนวทางปฏิบัติ และกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ตามประกาศประมวลแนวทางปฏิบัติและกรอบมาตรฐาน)

(ค) การจัดการทรัพย์สิน (Asset Management)

(ง) การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy)

(จ) การควบคุมการเข้าถึง (Access Control)

(ฉ) การทำให้ระบบมีความแข็งแกร่ง (System Hardening)

(ช) การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)

(ซ) การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring)

(ฌ) แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)

(ญ) การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise)

(๒) ในกรณีที่ข้อมูลหรือระบบสารสนเทศมีคุณลักษณะความมั่นคงปลอดภัยไซเบอร์อยู่ในระดับกลาง ให้กำหนดมาตรการควบคุมความมั่นคงปลอดภัยไซเบอร์ขั้นต่ำสำหรับข้อมูลหรือระบบสารสนเทศ ตามหัวข้อ ต่อไปนี้

(ก) ให้ดำเนินการตามข้อ (๑)

(ข) แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Audit Plan)

(ค) การเชื่อมต่อระยะไกล (Remote Connection)

(ง) สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media)

(๓) ในกรณีที่ข้อมูลหรือระบบสารสนเทศมีคุณลักษณะความมั่นคงปลอดภัยไซเบอร์อยู่ในระดับสูง ให้กำหนดมาตรการควบคุมความมั่นคงปลอดภัยไซเบอร์ขั้นต่ำสำหรับข้อมูลหรือระบบสารสนเทศ ตามหัวข้อ ต่อไปนี้

(ก) ให้ดำเนินการตามข้อ (๒)

(ข) การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing)

(ค) การจัดการผู้ให้บริการภายนอก (Third Party Management)

(ง) การแบ่งปันข้อมูล (Information Sharing)

(จ) การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery)

ข้อ ๕ ให้เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ รักษาการตามประกาศนี้ และให้มีอำนาจออกประกาศ คำสั่ง หลักเกณฑ์และวิธีการเพื่อปฏิบัติตามประกาศนี้

ในกรณีที่มีปัญหาเกี่ยวกับการปฏิบัติตามประกาศนี้ หรือประกาศนี้ไม่ได้กำหนดเรื่องใดไว้ ให้ประธานกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เป็นผู้มีอำนาจตีความและวินิจฉัยชี้ขาด ทั้งนี้ การตีความและคำวินิจฉัยของประธานกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติให้เป็นที่สุด

ประกาศ ณ วันที่ ๑๘ ธันวาคม พ.ศ. ๒๕๖๖
ภูมิธรรม เวชยชัย
รองนายกรัฐมนตรี ปฏิบัติหน้าที่
ประธานกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

ตารางหัวข้อในการกำหนดมาตรการควบคุมความมั่นคงปลอดภัยไซเบอร์ขั้นต่ำ
สำหรับข้อมูลหรือระบบสารสนเทศ
ท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
เรื่อง มาตรฐานขั้นต่ำของข้อมูลหรือระบบสารสนเทศ พ.ศ. ๒๕๖๖

หัวข้อในการกำหนด มาตรการควบคุมความมั่นคงปลอดภัยไซเบอร์ขั้นต่ำ สำหรับข้อมูลหรือระบบสารสนเทศ	ระดับคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ของข้อมูลหรือระบบสารสนเทศ		
	ต่ำ	กลาง	สูง
ประมวลแนวทางปฏิบัติ			
องค์ประกอบที่ ๑ แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Audit Plan)		●	●
องค์ประกอบที่ ๒ การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Assessment)	●	●	●
องค์ประกอบที่ ๓ แผนการรับมือภัยคุกคามทางไซเบอร์ (Incident Response Plan)	●	●	●
กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์			
๑. การระบุความเสี่ยงที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล (Identify)			
๑.๑ การจัดการทรัพย์สิน (Asset Management)	●	●	●
๑.๒ การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy)	●	●	●
๑.๓ การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing)			●
๑.๔ การจัดการผู้ให้บริการภายนอก (Third Party Management)			●
๒. มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect)			
๒.๑ การควบคุมการเข้าถึง (Access Control)	●	●	●
๒.๒ การทำให้ระบบมีความแข็งแกร่ง (System Hardening)	●	●	●
๒.๓ การเชื่อมต่อระยะไกล (Remote Connection)		●	●
๒.๔ สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media)		●	●
๒.๕ การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)	●	●	●
๒.๖ การแบ่งปันข้อมูล (Information Sharing)			●
๓. มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)			
๓.๑ การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring)	●	●	●

หัวข้อในการกำหนด มาตรการควบคุมความมั่นคงปลอดภัยไซเบอร์ขั้นต่ำ สำหรับข้อมูลหรือระบบสารสนเทศ	ระดับคุณลักษณะ ความมั่นคงปลอดภัยไซเบอร์ ของข้อมูลหรือระบบสารสนเทศ		
	ต่ำ	กลาง	สูง
๔. มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)			
๔.๑ แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)	●	●	●
๔.๒ แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)	●	●	●
๔.๓ การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise)	●	●	●
๕. มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)			
๕.๑ การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery)			●



ฉบับภาษาอังกฤษ
English Version

อยู่ระหว่างดำเนินการแปลเอกสารเป็นฉบับภาษาอังกฤษ

The translation of the document into English is underway.

14

ประกาศ กมช.

เรื่อง มาตรฐานและแนวทางส่งเสริมพัฒนาระบบการให้บริการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2566

มีผลใช้บังคับตั้งแต่วันที่ 6 ก.ย. 66 เป็นต้นไป

Notification of NCSC

Re: standards and guidelines for promoting the development of Cybersecurity service delivery systems B.E. 2566 (2023)

effective from September 6, 2023, onwards.



ฉบับภาษาไทย
Thai Version

ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

เรื่อง มาตรฐานและแนวทางส่งเสริมพัฒนาระบบการให้บริการ
เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์
พ.ศ. ๒๕๖๖

โดยที่พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดให้คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ มีหน้าที่และอำนาจกำหนดมาตรฐานและแนวทางส่งเสริมพัฒนาระบบการให้บริการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ จึงสมควรกำหนดมาตรฐานและแนวทางส่งเสริมพัฒนาระบบการให้บริการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อกำหนดมาตรฐานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์และการรับรองคุณภาพของผู้ให้บริการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมถึงกำหนดแนวทางส่งเสริมพัฒนาการให้บริการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้การปฏิบัติงานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์เป็นไปอย่างมีประสิทธิภาพ

อาศัยอำนาจตามความในมาตรา ๙ (๔) แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ประกอบกับมติที่ประชุมคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติในคราวการประชุมครั้งที่ ๔/๒๕๖๖ เมื่อวันที่ ๒๘ พฤศจิกายน ๒๕๖๖ คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ จึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานและแนวทางส่งเสริมพัฒนาระบบการให้บริการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๖”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ข้อ ๓ ในประกาศนี้

“สำนักงาน” หมายความว่า สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

“ผู้ให้บริการด้านความมั่นคงปลอดภัยไซเบอร์” หมายความว่า ผู้ให้บริการที่เกี่ยวข้องกับการระบุ ป้องกัน ตรวจสอบ เฝ้าระวัง รับมือ ลดความเสี่ยง รักษาและฟื้นฟูความเสียหายจากภัยคุกคามทางไซเบอร์

“การรับรองคุณภาพ” หมายความว่า กระบวนการตรวจสอบและรับรองการดำเนินงานของผู้ให้บริการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ไม่ว่าจะเป็นกระบวนการดำเนินงาน ระบบหรือเครื่องมือที่ใช้ในการดำเนินงาน หรือบุคลากรที่เกี่ยวข้องในการดำเนินงาน ว่ามีคุณภาพเป็นไปตามมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์

“คณะทำงานตรวจประเมิน” หมายความว่า คณะทำงานที่สำนักงานแต่งตั้งขึ้นเพื่อทำหน้าที่ตรวจสอบคุณภาพเกี่ยวกับการดำเนินงานของผู้ให้บริการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

ไม่ว่าจะเป็นกระบวนการดำเนินงาน ระบบหรือเครื่องมือที่ใช้ในการดำเนินงาน หรือบุคลากรที่เกี่ยวข้องในการดำเนินงาน

“องค์กรที่ทำหน้าที่ตรวจคุณภาพ” หมายความว่า หน่วยงานที่ให้บริการตรวจสอบคุณภาพเกี่ยวกับการดำเนินงานของผู้ให้บริการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ไม่ว่าจะเป็นกระบวนการดำเนินงาน ระบบหรือเครื่องมือ ที่ใช้ในการดำเนินงาน หรือบุคลากรที่เกี่ยวข้องในการดำเนินงาน

ข้อ ๔ เพื่อประโยชน์ในการรักษาความมั่นคงปลอดภัยไซเบอร์และป้องกันความเสียหายอันอาจเกิดขึ้นจากการดำเนินงานของผู้ให้บริการด้านความมั่นคงปลอดภัยไซเบอร์หรือจากภัยคุกคามทางไซเบอร์ผู้ให้บริการด้านความมั่นคงปลอดภัยไซเบอร์ที่ได้รับการยอมรับว่ามีมาตรฐานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ต้องเป็นผู้ให้บริการที่ได้รับการรับรองคุณภาพตามหลักเกณฑ์ วิธีการ และเงื่อนไขที่กำหนดในประกาศนี้ ทั้งนี้ การรับรองคุณภาพดังกล่าว ไม่ใช่การอนุญาตการเป็นผู้ให้บริการด้านความมั่นคงปลอดภัยไซเบอร์

ข้อ ๕ การรับรองคุณภาพของผู้ให้บริการด้านความมั่นคงปลอดภัยไซเบอร์มี ๓ ระดับ ได้แก่

(๑) การรับรองคุณภาพขั้นต้น

(๒) การรับรองคุณภาพขั้นก้าวหน้า

(๓) การรับรองคุณภาพขั้นสูง

การรับรองคุณภาพตามวรรคหนึ่ง (๑) หรือ (๒) สำนักงานอาจรับรองให้แก่บุคคลธรรมดา คณะบุคคล หรือนิติบุคคลก็ได้ แต่การรับรองคุณภาพตามวรรคหนึ่ง (๓) ให้สำนักงานรับรองให้แก่นิติบุคคลเท่านั้น

สำนักงานอาจจัดให้มีการรับรองคุณภาพของผู้ให้บริการด้านความมั่นคงปลอดภัยไซเบอร์ตามวรรคหนึ่ง สำหรับประเภทบริการที่ขอรับการรับรองเฉพาะบางประเภทบริการหรือบางระดับก็ได้ ทั้งนี้แล้วแต่ความพร้อมของสำนักงานในการรับรองคุณภาพของผู้ให้บริการด้านความมั่นคงปลอดภัยไซเบอร์

ข้อ ๖ ผู้ให้บริการด้านความมั่นคงปลอดภัยไซเบอร์รายใดประสงค์ได้รับการรับรองคุณภาพให้ยื่นคำขอต่อสำนักงานตามแบบที่สำนักงานกำหนด พร้อมทั้งเอกสารหรือหลักฐาน ดังต่อไปนี้

(๑) เอกสารแสดงความเชี่ยวชาญของบุคลากรของผู้ยื่นคำขอที่สอดคล้องกับประเภทบริการที่ขอรับการรับรอง ได้แก่ เอกสารแสดงวุฒิการศึกษา หนังสือรับรองประสบการณ์การทำงาน และเอกสารที่แสดงว่าได้รับการรับรองตามมาตรฐานสำหรับประเภทบริการที่ขอรับการรับรองตามที่สำนักงานประกาศกำหนดในกรณีที่ผู้ยื่นคำขอเป็นนิติบุคคล ผู้ยื่นคำขอต้องยื่นเอกสารแสดงความเชี่ยวชาญของบุคลากรสำหรับการรับรองคุณภาพในแต่ละระดับ ตามจำนวนที่กำหนด โดยบุคลากรดังกล่าวต้องเป็นบุคลากรที่ทำงานเต็มเวลาตามจำนวนที่กำหนด ดังต่อไปนี้

ระดับการรับรองคุณภาพ	จำนวนบุคลากรที่ต้องยื่นเอกสารแสดงความเชี่ยวชาญ	จำนวนบุคลากรที่ทำงานเต็มเวลา
ขั้นต้น	อย่างน้อย ๑ คน	อย่างน้อย ๑ คน
ขั้นก้าวหน้า	อย่างน้อย ๒ คน	อย่างน้อย ๒ คน
ขั้นสูง	อย่างน้อย ๕ คน	อย่างน้อย ๓ คน

ทั้งนี้ บุคลากรที่ทำงานเต็มเวลาอย่างน้อยหนึ่งคนต้องมีเอกสารที่แสดงว่าได้รับการรับรองตามมาตรฐานสำหรับประเภทบริการที่ขอรับการรับรองคุณภาพตามที่สำนักงานประกาศกำหนด และหากขอรับการรับรองคุณภาพขั้นสูง ผู้ยื่นคำขอต้องแสดงเอกสารการรับรองด้านกระบวนการตามมาตรฐานสากลของหน่วยงานผู้ยื่นคำขอด้วย

(๒) เอกสารแสดงประสบการณ์การทำงานในประเภทบริการที่ขอรับการรับรอง โดยอย่างน้อยต้องมีเอกสารแสดงประสบการณ์ในโครงการที่ดำเนินการแล้วเสร็จตามเป้าหมาย สำหรับการขอรับรองคุณภาพขั้นต้น การรับรองคุณภาพขั้นก้าวหน้า และการรับรองคุณภาพขั้นสูง เป็นจำนวนไม่น้อยกว่าหนึ่งโครงการ สามโครงการ และห้าโครงการ ตามลำดับ

(๓) เอกสารการรับรองตนเองตามแบบที่สำนักงานกำหนดที่แสดงว่าผู้ยื่นคำขอเป็นผู้ให้บริการด้านความมั่นคงปลอดภัยไซเบอร์ที่ปฏิบัติตามมาตรฐานที่กำหนดในประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ ว่าด้วยประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (เฉพาะในกรณีที่ผู้ยื่นคำขอเป็นนิติบุคคล)

การยื่นคำขอตามวรรคหนึ่งให้ดำเนินการโดยวิธีการทางอิเล็กทรอนิกส์เป็นหลัก โดยต้องมีการพิสูจน์ตัวตน (Identity Assurance Level) ไม่น้อยกว่าระดับ ๒ และใช้การเข้ารหัสด้วยวิธีการ Pretty Good Privacy (PGP) ในกรณีที่ยังไม่สามารถดำเนินการหรือมีเหตุอื่นใดทำให้ไม่สามารถดำเนินการโดยวิธีการทางอิเล็กทรอนิกส์ได้ ให้การดำเนินการดังกล่าวกระทำ ณ สำนักงาน

ผู้ยื่นคำขอตามข้อนี้ต้องชำระค่าธรรมเนียมตามที่สำนักงานกำหนด

ข้อ ๗ ประกาศสำนักงานตามข้อ ๖ (๑) ต้องมีรายละเอียดเกี่ยวกับประเภทบริการ รายละเอียดการตรวจประเมินบริการแต่ละประเภท และรายชื่อมาตรฐานหรือประกาศนียบัตรที่สามารถใช้เป็นหลักฐานในการขอรับการรับรองคุณภาพการให้บริการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์แต่ละประเภทบริการสำหรับการรับรองคุณภาพขั้นต้น การรับรองคุณภาพขั้นก้าวหน้า และการรับรองคุณภาพขั้นสูง โดยให้พิจารณากำหนดรายชื่อมาตรฐานและประกาศนียบัตรในการรับรองคุณภาพแต่ละระดับโดยคำนึงถึงปัจจัย ดังต่อไปนี้

(๑) ระดับความยากง่ายของมาตรฐานหรือประกาศนียบัตร

(๒) การใช้ทักษะเฉพาะทาง

(๓) การทดสอบแบบลงมือปฏิบัติจริง

(๔) การได้รับการยอมรับ

ทั้งนี้ มาตรฐานหรือประกาศนียบัตรที่สามารถใช้เป็นหลักฐานในการขอรับการรับรองคุณภาพขั้นสูงต้องเป็นมาตรฐานหรือประกาศนียบัตรที่แสดงให้เห็นได้ว่าผู้ที่ได้รับจะต้องมีความเชี่ยวชาญเฉพาะด้านที่เกี่ยวข้องกับประเภทบริการนั้นเป็นที่ประจักษ์

ข้อ ๘ เมื่อได้รับคำขอรับการรับรองคุณภาพ ให้สำนักงานตรวจสอบคำขอรวมทั้งเอกสารหรือหลักฐานว่าถูกต้องและครบถ้วนหรือไม่ หากไม่ถูกต้องหรือไม่ครบถ้วน ให้สำนักงานแจ้งให้ผู้ยื่นคำขอแก้ไขเพิ่มเติมคำขอ หรือจัดส่งเอกสารหรือหลักฐาน ให้ถูกต้องและครบถ้วนภายในระยะเวลา

ที่สำนักงานกำหนด ในกรณีที่ผู้ยื่นคำขอไม่แก้ไขเพิ่มเติมคำขอ หรือไม่จัดส่งเอกสารหรือหลักฐานให้ครบถ้วนภายในระยะเวลาที่สำนักงานกำหนด ให้ถือว่าผู้ยื่นคำขอไม่ประสงค์จะให้ดำเนินการต่อไป และให้สำนักงานจำหน่ายเรื่องออกจากสารบบ

ในกรณีที่คำขอรับการรับรองคุณภาพ รวมทั้งเอกสารหรือหลักฐานครบถ้วน ให้สำนักงานมอบหมายองค์กรที่ทำหน้าที่ตรวจคุณภาพที่คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติให้ความเห็นชอบ หรือแต่งตั้งคณะทำงานตรวจประเมิน เพื่อทำหน้าที่ในการตรวจสอบข้อมูล ขั้นตอนและกระบวนการดำเนินงานเพื่อการรับรองคุณภาพของผู้ยื่นคำขอ จำนวนอย่างน้อยสามคน ประกอบด้วยบุคคลที่ไม่มีผลประโยชน์ที่อาจทำให้การตรวจสอบไม่เป็นกลาง และเป็นผู้ที่มีความเชี่ยวชาญหรือประสบการณ์ในด้าน ดังต่อไปนี้

(๑) การรักษาความมั่นคงปลอดภัยไซเบอร์

(๒) การรับรองคุณภาพตามมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามที่กำหนดสำหรับประเภทบริการที่ขอรับการรับรอง

(๓) ความเชี่ยวชาญเฉพาะทางที่เกี่ยวข้องกับบริการที่ขอรับการรับรอง

การแต่งตั้งคณะทำงานตรวจประเมินตามวรรคสอง สำนักงานจะแต่งตั้งคณะทำงานตรวจประเมินโดยจำแนกตามประเภทบริการที่ขอรับการรับรองก็ได้ โดยให้ทำหน้าที่คราวละสามปี ซึ่งคณะทำงานตรวจประเมินอย่างน้อยหนึ่งคนต้องเป็นผู้ที่มีประกาศนียบัตรแสดงถึงระดับความเชี่ยวชาญเฉพาะทางที่เกี่ยวข้องกับประเภทบริการที่ทำการตรวจประเมิน

ข้อ ๙ เมื่อองค์กรที่ทำหน้าที่ตรวจคุณภาพหรือคณะทำงานตรวจประเมินตามข้อ ๘ ได้รับคำขอรับการรับรองคุณภาพ พร้อมทั้งเอกสารหรือหลักฐานของผู้ยื่นคำขอจากสำนักงานแล้ว ให้ดำเนินการ ดังต่อไปนี้

(๑) กรณีขอรับการรับรองคุณภาพขั้นต้น ให้ตรวจสอบข้อมูลในคำขอรับการรับรองคุณภาพและเอกสารหรือหลักฐาน หากพิจารณาแล้วเห็นว่าผู้ยื่นคำขอเป็นผู้ให้บริการด้านความมั่นคงปลอดภัยไซเบอร์ที่ปฏิบัติตามมาตรฐานที่กำหนดในประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และเอกสารหรือหลักฐานที่ผู้ยื่นคำขอเป็นเอกสารที่ถูกต้อง ให้แจ้งผลการตรวจสอบให้สำนักงานทราบภายในเจ็ดวันนับแต่วันตรวจสอบแล้วเสร็จ ทั้งนี้ องค์กรที่ทำหน้าที่ตรวจคุณภาพหรือคณะทำงานตรวจประเมินต้องดำเนินการให้แล้วเสร็จภายในสามสิบวันนับแต่วันที่ได้รับคำขอพร้อมด้วยเอกสารหรือหลักฐานครบถ้วนจากสำนักงาน

(๒) กรณีขอรับการรับรองคุณภาพขั้นก้าวหน้า ให้ตรวจสอบข้อมูลในคำขอรับการรับรองคุณภาพและเอกสารหรือหลักฐาน หากพิจารณาแล้วเห็นว่าผู้ยื่นคำขอเป็นผู้ให้บริการด้านความมั่นคงปลอดภัยไซเบอร์ที่ปฏิบัติตามมาตรฐานที่กำหนดในประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ ว่าด้วยประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และเอกสารหรือหลักฐานที่ผู้ยื่นคำขอเป็นเอกสารที่ถูกต้อง ให้องค์กรที่ทำหน้าที่ตรวจคุณภาพหรือคณะทำงานตรวจประเมินดำเนินการตรวจสอบข้อมูล ขั้นตอนและกระบวนการดำเนินงานและการให้บริการด้วยวิธีการสัมภาษณ์

โดยให้เรียกเก็บค่าธรรมเนียมได้ไม่เกินสามวัน และองค์กรที่ทำหน้าที่ตรวจคุณภาพหรือคณะทำงานตรวจประเมินต้องดำเนินการตรวจสอบให้แล้วเสร็จภายในหกสิบวันนับแต่วันที่ได้รับคำขอพร้อมด้วยเอกสารหรือหลักฐานครบถ้วนจากสำนักงาน ทั้งนี้ เมื่อองค์กรที่ทำหน้าที่ตรวจคุณภาพหรือคณะทำงานตรวจประเมินได้ตรวจสอบแล้วว่าข้อมูล ขั้นตอนและกระบวนการดำเนินงานและการให้บริการของผู้ยื่นคำขอถูกต้องและได้มาตรฐานตามที่กำหนดสำหรับประเภทบริการที่ขอรับการรับรอง ให้แจ้งผลการตรวจสอบให้สำนักงานทราบภายในเจ็ดวันนับแต่วันตรวจสอบแล้วเสร็จ

(๓) กรณีขอรับการรับรองคุณภาพขั้นสูงให้ดำเนินการตาม (๒) โดยองค์กรที่ทำหน้าที่ตรวจคุณภาพหรือคณะทำงานตรวจประเมินต้องตรวจสอบด้วยว่าผู้ขอรับการรับรองคุณภาพขั้นสูงเป็นผู้ที่ได้รับการรับรองด้านกระบวนการตามมาตรฐานสากล และให้องค์กรที่ทำหน้าที่ตรวจคุณภาพหรือคณะทำงานตรวจประเมินดำเนินการตรวจสอบข้อมูล ขั้นตอนและกระบวนการดำเนินงานและการให้บริการ ณ สถานประกอบการหรือสถานที่ให้บริการของผู้ยื่นคำขอด้วย โดยผู้ยื่นคำขอต้องเตรียมความพร้อมทั้งบุคลากร เอกสารหรือหลักฐาน สถานที่และเครื่องมือที่จำเป็นในการตรวจสอบ รวมทั้งอำนวยความสะดวกแก่องค์กรที่ทำหน้าที่ตรวจคุณภาพหรือคณะทำงานตรวจประเมินในการเข้าถึงระบบสารสนเทศที่เกี่ยวข้อง โดยให้เรียกเก็บค่าธรรมเนียมได้ไม่เกินห้าวัน ทั้งนี้ เมื่อองค์กรที่ทำหน้าที่ตรวจคุณภาพหรือคณะทำงานตรวจประเมินได้ตรวจสอบแล้วว่าข้อมูล ขั้นตอนและกระบวนการดำเนินงานและการให้บริการของผู้ยื่นคำขอถูกต้องและได้มาตรฐานตามที่กำหนดสำหรับประเภทบริการที่ขอรับการรับรอง ให้แจ้งผลการตรวจสอบให้สำนักงานทราบภายในเจ็ดวันนับแต่วันตรวจสอบแล้วเสร็จ

ในการดำเนินการตามวรรคหนึ่ง (๑) (๒) หรือ (๓) องค์กรที่ทำหน้าที่ตรวจคุณภาพหรือคณะทำงานตรวจประเมินอาจแจ้งให้ผู้ยื่นคำขอส่งข้อมูลหรือเอกสารที่จำเป็นเพิ่มเติมก็ได้ ในการนี้มิให้นับระยะเวลาตั้งแต่วันที่แจ้งจนถึงวันที่ได้รับข้อมูลหรือเอกสารดังกล่าวจากผู้ยื่นคำขอรวมเข้าเป็นระยะเวลาที่องค์กรที่ทำหน้าที่ตรวจคุณภาพหรือคณะทำงานตรวจประเมินต้องดำเนินการตรวจสอบให้แล้วเสร็จ

ข้อ ๑๐ เมื่อสำนักงานได้รับแจ้งผลการตรวจสอบตามข้อ ๙ วรรคหนึ่ง (๑) (๒) หรือ (๓) แล้ว ให้สำนักงานแต่งตั้งคณะทำงานรับรองคุณภาพของผู้ให้บริการด้านความมั่นคงปลอดภัยไซเบอร์จำนวนอย่างน้อยสามคน เพื่อพิจารณาผลการตรวจสอบว่าข้อมูล ขั้นตอนและกระบวนการดำเนินงานและการให้บริการของผู้ยื่นคำขอถูกต้องและได้มาตรฐานตามที่กำหนดสำหรับประเภทบริการที่ขอรับการรับรองจริง และให้แจ้งให้สำนักงานออกใบรับรองคุณภาพขั้นต้น ใบรับรองคุณภาพขั้นก้าวหน้าหรือใบรับรองคุณภาพขั้นสูง แล้วแต่กรณี ให้แก่ผู้ยื่นคำขอ

ข้อ ๑๑ ให้ใบรับรองคุณภาพมีอายุนับตั้งแต่วันที่ออกใบรับรองคุณภาพ ดังต่อไปนี้

ระดับใบรับรองคุณภาพ	อายุใบรับรองคุณภาพ
ขั้นต้น	๒ ปี
ขั้นก้าวหน้า	๓ ปี
ขั้นสูง	๓ ปี

นอกจากการสิ้นอายุใบรับรองคุณภาพตามวรรคหนึ่ง ใบรับรองคุณภาพ จะสิ้นอายุเมื่อมีเหตุดังต่อไปนี้

(๑) ผู้ให้บริการด้านความมั่นคงปลอดภัยไซเบอร์เลิกประกอบกิจการ

(๒) ผู้ให้บริการด้านความมั่นคงปลอดภัยไซเบอร์ตาย เลิกคณะบุคคล หรือสิ้นสภาพการเป็นนิติบุคคล

(๓) สำนักงานเพิกถอนใบรับรองคุณภาพ

ข้อ ๑๒ ภายหลังการออกใบรับรองคุณภาพขั้นต้น ใบรับรองคุณภาพขั้นก้าวหน้า หรือใบรับรองคุณภาพขั้นสูงตามข้อ ๑๐ เมื่อสำนักงานหรือคณะทำงานตรวจประเมินได้รับการร้องเรียนหรือมีเหตุสงสัยว่า มีการปฏิบัติไม่เป็นไปตามมาตรฐานตามที่กำหนดสำหรับประเภทบริการที่ขอรับการรับรอง ให้สำนักงานหรือคณะทำงานตรวจประเมินมีอำนาจเรียกให้ผู้ให้บริการด้านความมั่นคงปลอดภัยไซเบอร์จัดส่งเอกสารหรือหลักฐานตามที่สำนักงานหรือคณะทำงานตรวจประเมินกำหนดเพื่อตรวจสอบรวมถึงมีอำนาจเข้าไปตรวจสอบข้อมูลขั้นตอนและกระบวนการดำเนินงานและการให้บริการของผู้ให้บริการด้านความมั่นคงปลอดภัยไซเบอร์ และหากปรากฏว่าการให้บริการของผู้ให้บริการด้านความมั่นคงปลอดภัยไซเบอร์ไม่เป็นไปตามมาตรฐานตามที่กำหนดสำหรับประเภทบริการที่ขอรับการรับรอง ให้สำนักงานเพิกถอนใบรับรองคุณภาพขั้นต้น ใบรับรองคุณภาพขั้นก้าวหน้า หรือใบรับรองคุณภาพขั้นสูง แล้วแต่กรณี

ในระหว่างใบรับรองคุณภาพยังไม่สิ้นอายุ ในกรณีที่ผู้ให้บริการด้านความมั่นคงปลอดภัยไซเบอร์มีการเปลี่ยนแปลงขั้นตอนหรือกระบวนการ บุคลากร หรือเทคโนโลยีที่ใช้ในกระบวนการของบริการที่ได้รับการรับรองคุณภาพแล้ว ให้ผู้ให้บริการด้านความมั่นคงปลอดภัยไซเบอร์ดังกล่าวมีหน้าที่แจ้งให้สำนักงานทราบภายในสามสิบวันนับแต่วันที่มีการเปลี่ยนแปลง และให้สำนักงานแจ้งให้คณะทำงานตรวจประเมินเพื่อดำเนินการตรวจสอบว่าการให้บริการของผู้ให้บริการด้านความมั่นคงปลอดภัยไซเบอร์ยังคงเป็นไปตามมาตรฐานตามที่กำหนดสำหรับประเภทบริการที่ขอรับการรับรองหรือไม่ หากปรากฏว่าผู้ให้บริการด้านความมั่นคงปลอดภัยไซเบอร์ไม่ดำเนินการตามหลักเกณฑ์ วิธีการ และเงื่อนไขที่กำหนดในประกาศนี้ สำหรับประเภทบริการที่ขอรับการรับรอง ให้สำนักงานเพิกถอนใบรับรองคุณภาพขั้นต้น ใบรับรองคุณภาพขั้นก้าวหน้า หรือใบรับรองคุณภาพขั้นสูง แล้วแต่กรณี และลบรายชื่อผู้ให้บริการด้านความมั่นคงปลอดภัยไซเบอร์ดังกล่าวออกจากรายชื่อที่ได้ประกาศตามข้อ ๑๐ วรรคสอง

การเปลี่ยนแปลงขั้นตอนหรือกระบวนการ บุคลากร หรือเทคโนโลยีที่ต้องแจ้งตามวรรคสอง ให้รวมถึงกรณีที่ผู้ให้บริการด้านความมั่นคงปลอดภัยไซเบอร์ได้ควบรวมกิจการหรือรับโอนกิจการจากบุคคลอื่นในส่วนที่เกี่ยวกับบริการที่ขอรับการรับรอง

ข้อ ๑๓ ผู้ให้บริการด้านความมั่นคงปลอดภัยไซเบอร์ที่ได้รับใบรับรองคุณภาพรายใดประสงค์จะต่ออายุใบรับรองคุณภาพ ให้ยื่นคำขอต่อสำนักงานไม่น้อยกว่าหนึ่งร้อยยี่สิบวันก่อนใบรับรองคุณภาพสิ้นอายุ โดยให้ดำเนินการตามข้อ ๖ และให้สำนักงานดำเนินการตามข้อ ๘ ทั้งนี้ หากผู้ให้บริการด้านความมั่นคง

ปลอดภัยไซเบอร์ไม่ยื่นขอต่ออายุใบรับรองคุณภาพภายในระยะเวลาที่กำหนดข้างต้น ให้ถือว่าผู้ให้บริการด้านความมั่นคงปลอดภัยไซเบอร์ไม่ประสงค์ต่ออายุใบรับรองคุณภาพ

เมื่อองค์กรที่ทำหน้าที่ตรวจคุณภาพหรือคณะทำงานตรวจประเมินได้รับคำขอรับการรับรองคุณภาพ พร้อมทั้งเอกสารหรือหลักฐานของผู้ยื่นคำขอจากสำนักงานแล้ว ให้ดำเนินการตามข้อ ๙ ทั้งนี้ ในกรณีขอรับการรับรองคุณภาพขั้นก้าวหน้าหรือใบรับรองคุณภาพขั้นสูงตามข้อ ๙ วรรคหนึ่ง (๒) หรือ (๓) คณะทำงานตรวจประเมินอาจตรวจสอบข้อมูล ขั้นตอนและกระบวนการดำเนินงานของผู้ยื่นคำขอโดยใช้วิธีการสุ่มตรวจก็ได้

ข้อ ๑๔ ให้เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ รักษาการตามประกาศนี้ และให้มีอำนาจออกประกาศ คำสั่ง หลักเกณฑ์และวิธีการเพื่อปฏิบัติตามประกาศนี้

ในกรณีที่มีปัญหาเกี่ยวกับการปฏิบัติตามประกาศนี้ หรือประกาศนี้ไม่ได้กำหนดเรื่องใดไว้ ให้เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติมีอำนาจตีความและวินิจฉัยชี้ขาดแล้วรายงานให้คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติทราบ ทั้งนี้ การตีความและคำวินิจฉัยของเลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติให้เป็นที่สุด

ประกาศ ณ วันที่ ๑๘ ธันวาคม พ.ศ. ๒๕๖๖
ภูมิธรรม เวชยชัย
รองนายกรัฐมนตรี ปฏิบัติหน้าที่
ประธานกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ



ฉบับภาษาอังกฤษ
English Version

อยู่ระหว่างดำเนินการแปลเอกสารเป็นฉบับภาษาอังกฤษ

The translation of the document into English is underway.

15

ประกาศ กมช.

เรื่อง มาตรการและแนวทางในการยกระดับทักษะความรู้และความเชี่ยวชาญในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2567

มีผลใช้บังคับตั้งแต่วันที่ 10 ก.ย. 68 เป็นต้นไป

Notification of NCSC

Re: measures and guidelines to enhance the knowledge and expertise in Cybersecurity B.E. 2567 (2024)

effective from September 10, 2025, onwards.



ฉบับภาษาไทย
Thai Version

ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

เรื่อง มาตรการและแนวทางในการยกระดับทักษะความรู้และความเชี่ยวชาญ
ในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

พ.ศ. ๒๕๖๗

โดยที่พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดให้คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ มีหน้าที่และอำนาจกำหนดมาตรการและแนวทางในการยกระดับทักษะความรู้และความเชี่ยวชาญในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของพนักงานเจ้าหน้าที่หรือเจ้าหน้าที่ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานเอกชนที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์และให้ระดับความรู้ความชำนาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของพนักงานเจ้าหน้าที่เป็นไปตามที่คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติกำหนด จึงสมควรกำหนดมาตรการและแนวทางในการยกระดับทักษะความรู้และความเชี่ยวชาญในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้หน่วยงานใช้ในการสร้างความตระหนักรู้ การฝึกอบรม และการศึกษาสำหรับการพัฒนาความรู้ความเชี่ยวชาญของพนักงานเจ้าหน้าที่และบุคลากรที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์อันจะนำไปสู่การยกระดับความมั่นคงปลอดภัยในการป้องกันและรับมือภัยคุกคามทางไซเบอร์ในภาพรวม เพื่อให้การปฏิบัติงานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์เป็นไปอย่างมีประสิทธิภาพ

อาศัยอำนาจตามความในมาตรา ๙ (๕) แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ประกอบกับมติที่ประชุมคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติในคราวการประชุมครั้งที่ ๒/๒๕๖๗ เมื่อวันที่ ๓๑ กรกฎาคม ๒๕๖๗ คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ จึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรการและแนวทางในการยกระดับทักษะความรู้และความเชี่ยวชาญในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๗”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับเมื่อพ้นกำหนดหนึ่งปีนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ข้อ ๓ ในประกาศนี้

“หน่วยงาน” หมายความว่า หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน่วยงานเอกชนที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์

“บุคลากรของหน่วยงาน” หมายความว่า เจ้าหน้าที่ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานเอกชนที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ ทั้งนี้ ไม่หมายความรวมถึงพนักงานเจ้าหน้าที่ที่รัฐมนตรีแต่งตั้งให้ปฏิบัติการตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

“การสร้างความตระหนักรู้” (Awareness) หมายความว่า กระบวนการที่มุ่งสร้างความรู้ความเข้าใจเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ โดยมีวัตถุประสงค์ให้บุคคลที่เกี่ยวข้องรับทราบข้อกังวลที่เกี่ยวข้องและตอบสนองได้อย่างถูกต้อง

“การฝึกอบรม” (Training) หมายความว่า กระบวนการที่เสริมสร้าง ความรู้ ทักษะ สมรรถนะ และความสามารถของบุคคล หรือกลุ่มบุคคลด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่จำเป็นตามสายงานที่เกี่ยวข้อง

“การศึกษา” (Education) หมายความว่า กระบวนการเรียนรู้ที่ผสานระหว่างทักษะและสมรรถนะเฉพาะด้านเข้าไว้ด้วยกันเป็นองค์ความรู้ด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อผลิตผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์ที่มีวิสัยทัศน์และสามารถตอบสนองในเชิงรุกต่อภัยคุกคามทางไซเบอร์

“แผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรม” (Cybersecurity Awareness and Training Program) หมายความว่า แผนงานหรือโครงการที่ใช้เป็นแนวทางให้หน่วยงานใช้ในการออกแบบ พัฒนา นำไปใช้ และบำรุงรักษาเพื่อสร้างความตระหนักรู้และการฝึกอบรม

“สำนักงาน” หมายความว่า สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

“มาตรการในการยกระดับทักษะความรู้และความเชี่ยวชาญ” หมายความว่า มาตรการที่ดำเนินการโดยสำนักงานและหน่วยงาน เพื่อยกระดับทักษะความรู้และความเชี่ยวชาญในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของพนักงานเจ้าหน้าที่หรือบุคลากรของหน่วยงาน ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

“แนวทางในการยกระดับทักษะความรู้และความเชี่ยวชาญ” หมายความว่า แนวปฏิบัติที่สำนักงานและหน่วยงานสามารถใช้ในการยกระดับทักษะความรู้และความเชี่ยวชาญในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของพนักงานเจ้าหน้าที่หรือบุคลากรของหน่วยงาน

ข้อ ๔ ให้เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติรักษาการตามประกาศนี้ และให้มีอำนาจออกประกาศ คำสั่ง หลักเกณฑ์และวิธีการเพื่อปฏิบัติตามประกาศนี้

ในกรณีที่มีปัญหาเกี่ยวกับการปฏิบัติตามประกาศนี้ หรือประกาศนี้ไม่ได้กำหนดเรื่องใดไว้ ให้เลขาธิการมีอำนาจตีความและวินิจฉัยชี้ขาด แล้วรายงานให้คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ทั้งนี้ การตีความและคำวินิจฉัยของเลขาธิการให้เป็นที่สุด

หมวด ๑
มาตรการในการยกระดับทักษะความรู้และความเชี่ยวชาญให้แก่บุคลากรของหน่วยงาน

ส่วนที่ ๑
มาตรการของสำนักงาน

ข้อ ๕ เพื่อส่งเสริมและสนับสนุนการเรียนรู้และการพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ ให้สำนักงานสนับสนุนหน่วยงาน ดังต่อไปนี้

(๑) ส่งเสริมให้เกิดการพัฒนามาตรฐานและกฎเกณฑ์ เพื่อสร้างความเชื่อมั่น และอำนวยความสะดวกในการดำเนินการภายใต้การกำกับดูแลอย่างเหมาะสม เป็นธรรม และแข่งขันได้

(๒) สนับสนุนให้เกิดการเรียนรู้อิเล็กทรอนิกส์ (e-Learning) ผ่านโครงสร้างพื้นฐานโครงข่ายอินเทอร์เน็ต ให้ครอบคลุมการเข้าถึงทุกภาคส่วนอย่างมีประสิทธิภาพ

(๓) สนับสนุนให้หน่วยงานที่มีความเสี่ยงต่อภัยคุกคามทางไซเบอร์สูงมีมาตรการควบคุมความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ โดยพัฒนาทักษะความรู้และความเชี่ยวชาญของบุคลากรให้ครอบคลุมในทุกด้าน

(๔) ส่งเสริมให้เกิดการลงทุนเพื่อการพัฒนาบุคลากรและการวิจัยเชิงนโยบาย รวมถึงพัฒนานวัตกรรมเพื่อสร้างองค์ความรู้และทักษะด้านความมั่นคงปลอดภัยไซเบอร์

ข้อ ๖ เพื่อประโยชน์ในการยกระดับทักษะความรู้และความเชี่ยวชาญในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของบุคลากรของหน่วยงาน ให้สำนักงานดำเนินการ ดังต่อไปนี้

(๑) กำกับและติดตามการดำเนินมาตรการและแนวทางในการยกระดับทักษะความรู้และความเชี่ยวชาญในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของบุคลากรของหน่วยงาน

(๒) เป็นศูนย์กลางข้อมูล ให้คำปรึกษา และถ่ายทอดองค์ความรู้ด้านความมั่นคงปลอดภัยไซเบอร์

(๓) สร้างหลักสูตรหรือกิจกรรมมารองรับ เพื่อเป็นหลักสูตรกลางสำหรับหน่วยงานใช้ในการยกระดับทักษะความรู้และความเชี่ยวชาญของบุคลากร และเพิ่มผลลัพธ์ตัวชี้วัดดัชนีความมั่นคงปลอดภัยไซเบอร์ในระดับนานาชาติ

(๔) สนับสนุนการจัดหาทุนสำหรับการอบรมและการสอบใบรับรองผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้แก่หน่วยงาน

ข้อ ๗ ให้สำนักงานประสานงานกับสำนักงบประมาณ สำนักงานคณะกรรมการข้าราชการพลเรือน และหน่วยงานอื่นที่มีอำนาจหน้าที่ในการพิจารณาจัดสรรงบประมาณและอัตรากำลังที่เพียงพอให้แก่หน่วยงานที่เกี่ยวข้อง เพื่อสนับสนุนการยกระดับทักษะความรู้และความเชี่ยวชาญในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

ส่วนที่ ๒
มาตรการของหน่วยงาน

ข้อ ๘ เพื่อเป็นการยกระดับทักษะความรู้และความเชี่ยวชาญของบุคลากรของหน่วยงาน ให้หน่วยงานจัดให้มีมาตรการในการพัฒนาศักยภาพบุคลากรของหน่วยงานของตนในด้านทักษะของบุคลากร โดยให้มีการส่งเสริมและสนับสนุนการเรียนรู้ และการพัฒนาบุคลากรอย่างต่อเนื่อง

การดำเนินการตามมาตรการในการพัฒนาด้านทักษะของบุคลากรตามวรรคหนึ่ง ให้หน่วยงานกำหนดแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรม โดยอาจดำเนินการในรูปแบบใดรูปแบบหนึ่ง ดังต่อไปนี้

(๑) แบบรวมศูนย์

(๒) แบบกระจายอำนาจบางส่วน

(๓) แบบกระจายอำนาจอย่างเต็มที่

ข้อ ๙ ให้หน่วยงานทบทวนแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรม รวมถึงเอกสาร สื่อ หรือเนื้อหาที่ใช้ในการดำเนินการตามแผนงานหรือโครงการดังกล่าวให้สอดคล้องกับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่มากขึ้นอยู่เสมอ ทั้งนี้ ให้ทบทวนอย่างน้อยปีละหนึ่งครั้ง

หมวด ๒
มาตรการในการยกระดับทักษะความรู้และความเชี่ยวชาญให้แก่พนักงานเจ้าหน้าที่

ข้อ ๑๐ เพื่อประโยชน์ในการยกระดับทักษะความรู้และความเชี่ยวชาญของพนักงานเจ้าหน้าที่ ให้สำนักงานดำเนินการ ดังต่อไปนี้

(๑) จัดให้มีโครงการพัฒนาศักยภาพพนักงานเจ้าหน้าที่และหลักสูตร หรือโครงการสร้างความตระหนักรู้และการฝึกอบรม รวมถึงแผนงานที่เกี่ยวข้อง โดยสำนักงานต้องดำเนินการจัดประเภทของพนักงานเจ้าหน้าที่ จัดโครงการ จัดทำหลักสูตร และกำหนดแผนงานดังกล่าวให้เหมาะสมกับพนักงานเจ้าหน้าที่แต่ละประเภท ทั้งนี้ ให้เป็นไปตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ว่าด้วยการกำหนดระดับความรู้ความชำนาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อแต่งตั้งเป็นพนักงานเจ้าหน้าที่

(๒) จัดให้มีการฝึกซ้อมตามแผนเผชิญเหตุการณ์ภัยคุกคามไซเบอร์ หรือฝึกซ้อมการดำเนินการตามหน้าที่ร่วมกันอย่างน้อยปีละครั้ง เพื่อให้พนักงานเจ้าหน้าที่แต่ละประเภทตระหนักถึงบทบาทและหน้าที่ของตน และการประสานงานระหว่างพนักงานเจ้าหน้าที่แต่ละประเภทเป็นไปอย่างมีประสิทธิภาพ

(๓) กำกับและติดตามการดำเนินมาตรการและแนวทางในการยกระดับทักษะความรู้และความเชี่ยวชาญในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของพนักงานเจ้าหน้าที่

(๔) จัดทำทะเบียนประวัติทักษะ ความรู้ ความเชี่ยวชาญของพนักงานเจ้าหน้าที่เพื่อติดตามและส่งเสริมการพัฒนาทักษะ ความรู้ ความเชี่ยวชาญ

(๕) จัดทำลำดับทักษะ ความรู้ ความเชี่ยวชาญ รวมถึงผลงานของพนักงานเจ้าหน้าที่ตลอดจนส่งเสริม ยกย่อง และเชิดชูเกียรติพนักงานเจ้าหน้าที่ที่มีพัฒนาการดีเด่น และมีการปฏิบัติงานดีเด่นเพื่อเป็นการเสริมสร้างขวัญกำลังใจในการเรียนรู้และการปฏิบัติหน้าที่

(๖) สนับสนุนการจัดหาทุนสำหรับการอบรมและการสอบใบรับรองผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้แก่พนักงานเจ้าหน้าที่ รวมถึงการอบรมด้านกฎหมายที่เกี่ยวข้องเพื่อป้องกันการดำเนินการที่ไม่สอดคล้องกับกฎหมาย

(๗) จัดอบรมและสัมมนาเพื่อแนะนำเทคนิคใหม่ที่ผู้ไม่ประสงค์ดีใช้ในการจู่โจมรวมถึงกระบวนการหรือเทคโนโลยีใหม่ ๆ ในการป้องกันภัยคุกคามทางไซเบอร์

(๘) กำหนดให้พนักงานเจ้าหน้าที่ต้องเข้ารับการอบรมที่จัดโดยสำนักงาน เพื่อเพิ่มทักษะความสามารถอย่างน้อยปีละหนึ่งครั้ง

(๙) สนับสนุนให้พนักงานเจ้าหน้าที่มีโอกาสมาฝึกงานที่สำนักงาน (On the job training)

(๑๐) สนับสนุนให้พนักงานเจ้าหน้าที่แลกเปลี่ยนความรู้และประสบการณ์ทางด้านความมั่นคงปลอดภัยไซเบอร์ ผ่านการจัดกิจกรรมการทำงานร่วมกับผู้เชี่ยวชาญเฉพาะทาง และกิจกรรมการเรียนรู้นอกสถานที่ (Outing)

(๑๑) ส่งเสริมและสนับสนุนการแลกเปลี่ยนองค์ความรู้ที่เกี่ยวข้องระหว่างหน่วยงาน

(๑๒) จัดทำจดหมายข่าว เว็บบอร์ด หรือการสื่อสารในรูปแบบอื่นใด เพื่อแบ่งปันข้อมูลเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ระหว่างพนักงานเจ้าหน้าที่

หมวด ๓

แนวทางในการยกระดับทักษะความรู้และความเชี่ยวชาญ
ให้แก่พนักงานเจ้าหน้าที่และบุคลากรของหน่วยงาน

ข้อ ๑๑ การดำเนินการตามมาตรการในข้อ ๕ และข้อ ๑๐ (๑) ให้เป็นไปตามแนวทางในการยกระดับทักษะความรู้และความเชี่ยวชาญในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่กำหนดท้ายประกาศนี้

ข้อ ๑๒ ให้สำนักงานพิจารณาปรับปรุงแนวทางในการยกระดับทักษะความรู้และความเชี่ยวชาญในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้แก่พนักงานเจ้าหน้าที่หรือบุคลากรของหน่วยงานอย่างน้อยหนึ่งครั้งทุกสามปี และแจ้งให้หัวหน้าหน่วยงานทราบถึงแนวทางดังกล่าว

ประกาศ ณ วันที่ ๓ กันยายน พ.ศ. ๒๕๖๗
ภูมิธรรม เวชยชัย
รองนายกรัฐมนตรี ปฏิบัติหน้าที่
ประธานกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

แนวทางในการยกระดับทักษะความรู้และความเชี่ยวชาญ
ในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

บทนำ

เพื่อให้เป็นไปตามมาตรา ๙ (๕) แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ จึงสมควรกำหนดแนวทางการยกระดับทักษะความรู้และความเชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้แก่พนักงานเจ้าหน้าที่หรือบุคลากรของหน่วยงานที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์

ขอบเขตการใช้

หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานของรัฐ และหน่วยงานเอกชนที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์

แนวทางการยกระดับทักษะความรู้และความเชี่ยวชาญในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๑. ขอบเขตการพัฒนา

แนวทางการพัฒนาพนักงานเจ้าหน้าที่หรือบุคลากรของหน่วยงานได้กำหนดการดำเนินการไว้ ๒ เรื่อง ดังนี้

๑.๑ ทักษะของบุคลากร (Skillsets) เพื่อกำหนดแนวทางการพัฒนาพนักงานเจ้าหน้าที่ เจ้าหน้าที่ของหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หรือบุคลากรอื่นที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ ให้มีกรอบความคิดและทักษะที่จำเป็นเหมาะสมในการปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ส่งเสริมให้มีการเรียนรู้และทำงานร่วมกัน หรือร่วมกันเป็นเครือข่ายแลกเปลี่ยนองค์ความรู้ และสนับสนุนบุคลากรพัฒนาร่วมกัน ผ่านการปฏิบัติงานในโครงการต่าง ๆ เพื่อสร้างผลลัพธ์ที่เป็นประโยชน์ต่อหน่วยงานอย่างมีประสิทธิภาพ โดยการประเมินและวางแผนการพัฒนาอย่างต่อเนื่อง

๑.๒ ระบบนิเวศในการทำงาน (Ecosystem) ที่ส่งเสริมและสนับสนุนการเรียนรู้และการพัฒนาบุคลากรอย่างต่อเนื่อง เพื่อส่งเสริมให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล มีสภาพแวดล้อมและระบบการทำงานที่เอื้อต่อการเรียนรู้และการพัฒนากรอบความคิดและกรอบทักษะ สำหรับการทำงานด้านความมั่นคงปลอดภัยไซเบอร์อย่างต่อเนื่อง และแสดงพฤติกรรมที่คาดหวังออกมาได้อย่างมีประสิทธิผล

๒. การพัฒนาทักษะของบุคลากร (Skillsets)

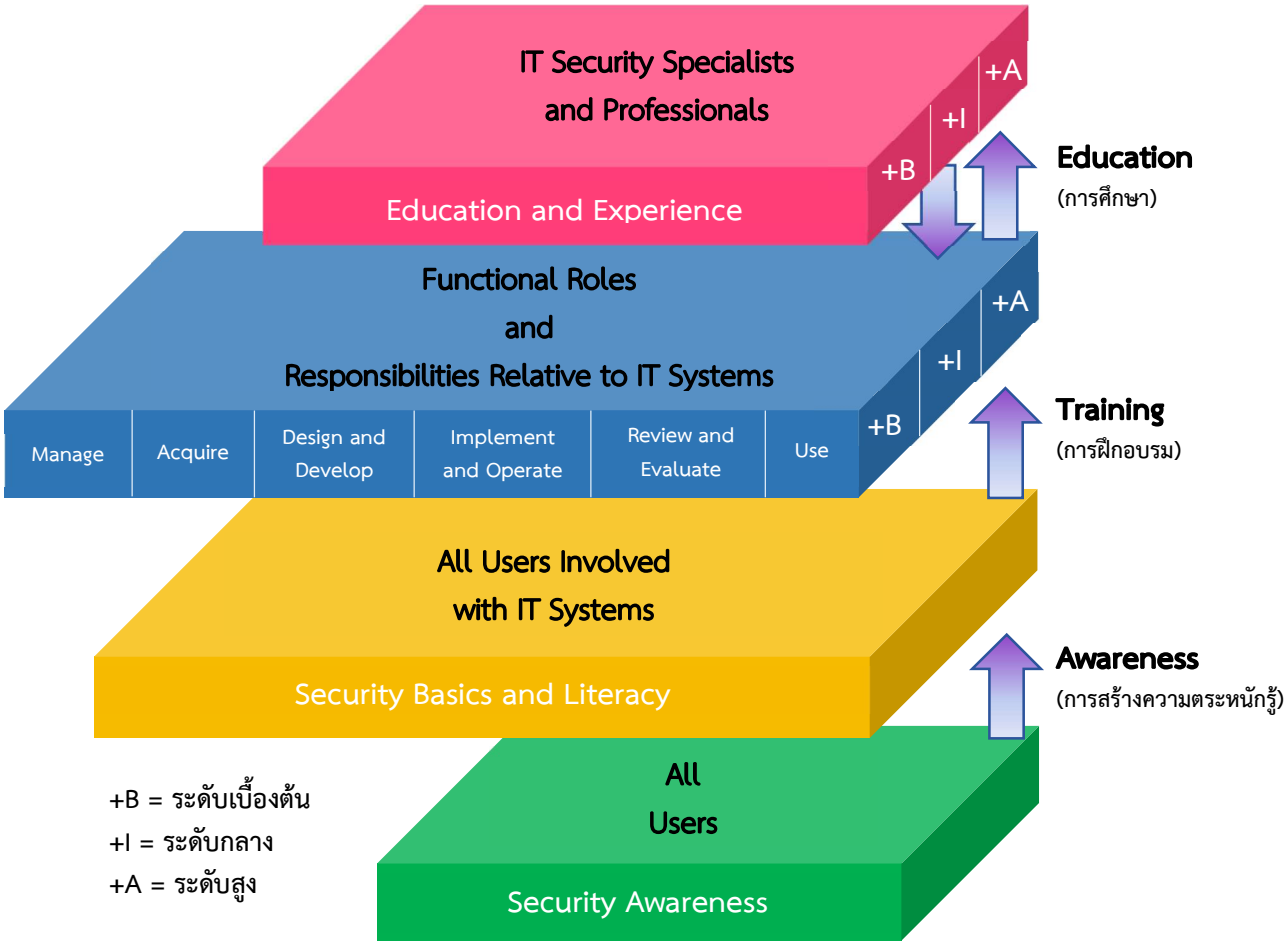
เพื่อให้เป็นไปตามแนวทางการสร้างความตระหนักรู้และการฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานซึ่งเป็นที่ยอมรับเป็นการทั่วไปว่าเชื่อถือได้ แนวทางการสร้างความตระหนักรู้และการฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์ มีการดำเนินการเพื่อส่งเสริมการเรียนรู้ ดังนี้

๒.๑ การสร้างความตระหนักรู้ (Awareness)

๒.๒ การฝึกอบรม (Training)

๒.๓ การศึกษา (Education)

การเรียนรู้ทั้ง ๓ ประการข้างต้น นำมากำหนดความต่อเนื่องของการพัฒนาทักษะของบุคลากรในการเรียนรู้ด้านความมั่นคงปลอดภัยไซเบอร์ โดยเริ่มจากการสร้างความตระหนักรู้ สร้างการฝึกอบรมและพัฒนาไปสู่การศึกษา จะได้ดังภาพความต่อเนื่องของการเรียนรู้ด้านความมั่นคงปลอดภัยไซเบอร์ ด้านล่าง



ภาพความต่อเนื่องของการเรียนรู้ด้านความมั่นคงปลอดภัยไซเบอร์

นอกจากนี้ การดำเนินงานดังกล่าว มีการเปรียบเทียบเพื่อให้เกิดความเข้าใจที่ชัดเจน ดังตารางกรอบการเปรียบเทียบการสร้างความตระหนักรู้ การฝึกอบรม และการศึกษา

ตารางกรอบการเปรียบเทียบการสร้างความตระหนักรู้ การฝึกอบรม และการศึกษา

กรอบการเปรียบเทียบ (Comparative Framework)			
	การสร้างความตระหนักรู้	**การอบรม**	**การศึกษา**
เพื่อ	ให้รู้ว่าคืออะไร	ให้รู้ว่าทำอย่างไร	ให้รู้ว่าทำไมต้องทำ
ระดับ	ข้อมูล	ความรู้	ข้อมูลเชิงลึก
จุดประสงค์การเรียนรู้	สร้างการรับรู้และความจำ	สร้างทักษะ	สร้างความเข้าใจ
ตัวอย่างวิธีสอน	<u>เนื้อหาและสื่อการเรียนรู้</u> - วีดิทัศน์ - จดหมายข่าว/บทความ - โปสเตอร์/สื่อสิ่งพิมพ์	<u>คำแนะนำการปฏิบัติ</u> - การสอนและการสาธิต - ศึกษาจากกรณีศึกษา - ลงมือปฏิบัติจริง	<u>การสอนเชิงทฤษฎี</u> - การสัมมนาและอภิปราย - การอ่านและการศึกษา - การวิจัย
วิธีการวัดผลการเรียนรู้	การเรียนรู้แบบแยกแยะ - คำถามตัวเลือกถูกผิด - คำถามแบบหลายตัวเลือก	<u>การเรียนรู้แบบประยุกต์</u> - การแก้ปัญหา - การวิเคราะห์สถานการณ์เพื่อแก้ปัญหา	<u>การเรียนรู้แบบตีความ</u> - สัมภาษณ์ - เขียนเรียงความ

กรอบการเปรียบเทียบ (Comparative Framework)			
	การสร้างความตระหนักรู้	**การอบรม**	**การศึกษา**
ระยะเวลา	ระยะเวลาสั้น (๓ - ๖ ชั่วโมง)	ระยะเวลาปานกลาง (๓ - ๕ วัน)	ระยะเวลานาน (๑ - ๒ สัปดาห์)

หมายเหตุ : แผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์มีความแตกต่างกันได้ โดยขึ้นอยู่กับจำนวนบุคลากร เงินทุน และการสนับสนุนขั้นพื้นฐาน

๓. บุคคลที่เกี่ยวข้องกับการพัฒนาทักษะของพนักงานเจ้าหน้าที่หรือบุคลากรของหน่วยงาน

เพื่อให้หน่วยงานมั่นใจได้ว่า การจัดทำและดำเนินการตามแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์เป็นไปอย่างมีประสิทธิภาพ หน่วยงานต้องเข้าใจบทบาทและความรับผิดชอบของตำแหน่งสำคัญ ๆ ดังต่อไปนี้

๓.๑ หัวหน้าหน่วยงาน (Agency Head)

หัวหน้าหน่วยงานมีความสำคัญอย่างสูงต่อความสำเร็จในการสร้างความตระหนักรู้และการฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์สำหรับบุคลากรของหน่วยงาน ซึ่งรวมถึงการดำเนินแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์ที่มีองค์ประกอบที่แข็งแกร่งด้วย ดังนั้น หัวหน้าหน่วยงานควรดำเนินการ ดังนี้

(๑) แต่งตั้งผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer: CIO) หัวหน้าแผนงานหรือโครงการด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Program Manager) และหัวหน้าส่วนงาน (Manager)

(๒) มอบหมายความรับผิดชอบด้านความมั่นคงปลอดภัยไซเบอร์ให้บุคลากรที่เกี่ยวข้อง

(๓) กำหนดนโยบายสำหรับการสร้างความตระหนักรู้และการฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน

(๔) กำกับและติดตามการดำเนินการตามแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์ทั่วทั้งหน่วยงาน เพื่อให้แผนงานหรือโครงการได้รับการสนับสนุนทรัพยากรและงบประมาณเป็นอย่างดี และมีประสิทธิภาพ

(๕) วิเคราะห์ผลการประเมินสมรรถนะของบุคลากรและจัดให้มีบุคลากรที่ผ่านการฝึกอบรมอย่างเพียงพอ สำหรับการปกป้องทรัพยากรด้านสารสนเทศ

๓.๒ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer: CIO)

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงเป็นตำแหน่งที่ทำหน้าที่จัดการการสร้างความตระหนักรู้และการฝึกอบรม และดูแลบุคลากรซึ่งมีความสำคัญต่อการรักษาความมั่นคงปลอดภัยไซเบอร์โดยผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ควรทำงานร่วมกับหัวหน้าแผนงานหรือโครงการด้านความมั่นคงปลอดภัยไซเบอร์และหัวหน้าส่วนงาน เพื่อประโยชน์ในการดำเนินการ ดังนี้

(๑) จัดทำแผนและกำหนดกลยุทธ์โดยรวมสำหรับแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์

(๒) ประชาสัมพันธ์นโยบาย แนวคิดและกลยุทธ์ของแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์ ของหัวหน้าหน่วยงาน เจ้าของระบบ เจ้าของข้อมูลและบุคลากรอื่นของหน่วยงาน รวมถึงประเมินความเข้าใจนโยบาย แนวคิดและกลยุทธ์ดังกล่าว เพื่อปรับปรุงแนวทางประชาสัมพันธ์

(๓) รับทราบและประเมินความก้าวหน้าของการดำเนินแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์ และเสนอรายงานความก้าวหน้าของแผนงานหรือโครงการต่อหัวหน้าหน่วยงาน

(๔) กำหนดแหล่งเงินทุนและดำเนินการให้มีการสนับสนุนงบประมาณสำหรับแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานอย่างเพียงพอ

(๕) ตรวจสอบว่าบุคลากรของหน่วยงานที่มีหน้าที่รับผิดชอบด้านความมั่นคงปลอดภัยไซเบอร์ที่สำคัญได้รับการฝึกอบรมที่เพียงพอต่อความรับผิดชอบ

(๖) ประเมินและจัดให้มีการฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์อย่างเพียงพอต่อการปฏิบัติงานที่อยู่ในความรับผิดชอบของผู้ใช้แต่ละคน

(๗) ดำเนินการให้มีกลไกการติดตาม และกลไกการรายงานผลที่มีประสิทธิภาพ

๓.๓ หัวหน้าแผนงานหรือโครงการด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Program Manager)

หัวหน้าแผนงานหรือโครงการด้านความมั่นคงปลอดภัยไซเบอร์ (หน่วยงานอาจแต่งตั้งบุคคลที่ดำรงตำแหน่งผู้บริหารระดับสูงที่มีหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Chief Information Security Officer: CISO) ในกรณีที่หน่วยงานมีเจ้าหน้าที่ในตำแหน่งนี้ หรืออาจแต่งตั้งบุคคลผู้ดำรงตำแหน่งผู้บริหารหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Head of Information Security) เพื่อทำหน้าที่เป็นหัวหน้าแผนงานหรือโครงการด้านความมั่นคงปลอดภัยไซเบอร์) มีหน้าที่รับผิดชอบระดับยุทธวิธีสำหรับแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรม ในบทบาทนี้ หัวหน้าแผนงานหรือโครงการควรดำเนินการ ดังนี้

(๑) กำหนดกลวิธีและสร้างข้อกำหนดด้านการสร้างความตระหนักรู้และการฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์

(๒) ขับเคลื่อนการดำเนินการจัดทำเอกสาร/สื่อ เนื้อหาการสร้างความตระหนักรู้และการฝึกอบรม ที่พัฒนาขึ้นนั้นเหมาะสมและเป็นปัจจุบันต่อกลุ่มเป้าหมาย

(๓) กำกับและติดตามการเข้าถึงและการใช้เอกสาร/สื่อ เนื้อหาการสร้างความตระหนักรู้และการฝึกอบรม ของกลุ่มเป้าหมายอย่างมีประสิทธิภาพ

(๔) กำหนดวิธีการสำหรับการรับข้อเสนอแนะเกี่ยวกับเอกสาร/สื่อ เนื้อหาการสร้างความตระหนักรู้และการฝึกอบรมและวิธีการนำเสนอจากผู้ใช้งานและหัวหน้าส่วนงาน

(๕) ขับเคลื่อนการดำเนินการทบทวนเอกสาร/สื่อ เนื้อหาการสร้างความตระหนักรู้และการฝึกอบรม เป็นระยะ ๆ เพื่อปรับปรุง เมื่อจำเป็นหรือมีการเปลี่ยนแปลงทางเทคโนโลยี

(๖) สนับสนุนการดำเนินการของผู้บริหารเทคโนโลยีสารสนเทศระดับสูงในการสร้างกลยุทธ์การติดตาม และการรายงานผลการดำเนินการ

๓.๔ หัวหน้าส่วนงาน (Manager)

หัวหน้าส่วนงานที่มีหน้าที่รับผิดชอบในด้านการสร้างความตระหนักรู้และการฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์ให้แก่บุคลากรของส่วนงาน ดังนี้

(๑) ทำงานร่วมกับผู้บริหารเทคโนโลยีสารสนเทศระดับสูง และหัวหน้าแผนงานหรือโครงการด้านความมั่นคงปลอดภัยไซเบอร์

(๒) สนับสนุนบุคลากรของหน่วยงานที่เกี่ยวข้องในการดำเนินการตามแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์ ในบทบาทของเจ้าของระบบสารสนเทศหรือเจ้าของสารสนเทศ

(๓) พิจารณาจัดทำแผนพัฒนาส่วนบุคคล (Individual Development Plan: IDP) สำหรับผู้ใช้งานในบทบาทที่มีความรับผิดชอบสูงด้านความมั่นคงปลอดภัยไซเบอร์

(๔) ส่งเสริมการพัฒนาวิชาชีพและการออกใบรับรองของเจ้าหน้าที่แผนงานหรือโครงการด้านความมั่นคงปลอดภัยไซเบอร์ เจ้าหน้าที่รักษาความมั่นคงปลอดภัยไซเบอร์เต็มเวลาหรือเจ้าหน้าที่รักษาความมั่นคงปลอดภัยไซเบอร์นอกเวลา และอื่น ๆ ที่มีหน้าที่สำคัญในการรักษาความมั่นคงปลอดภัยไซเบอร์

(๕) กำกับและติดตามการฝึกอบรมของผู้ใช้งานระบบทั้งหมด (ทั้งนี้อาจรวมถึงหน่วยงานภายนอกที่ทำหน้าที่ดูแลระบบ) ทั้งระบบสนับสนุนทั่วไปและระบบงานหลัก ได้รับการฝึกอบรมเกี่ยวกับวิธีการปฏิบัติตามความรับผิดชอบด้านความมั่นคงปลอดภัยไซเบอร์อย่างเหมาะสมก่อนที่จะอนุญาตให้เข้าถึงระบบ

(๖) กำกับและติดตามความเข้าใจข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ของแต่ละระบบสารสนเทศที่ผู้ใช้งาน (ทั้งนี้อาจรวมถึงหน่วยงานภายนอกที่ทำหน้าที่ดูแลระบบ) ต้องใช้งาน

(๗) ประเมินการทำงานของผู้ใช้งานระบบ เพื่อลดข้อผิดพลาดและการละเว้นของผู้ใช้งานเนื่องจากขาดความตระหนักรู้หรือการฝึกอบรม

๓.๕ ผู้ใช้งาน (Users)

ผู้ใช้งานมีส่วนสำคัญต่อการลดข้อผิดพลาดที่เกิดขึ้นอย่างไม่ตั้งใจ และลดช่องโหว่ของเทคโนโลยีสารสนเทศ ทั้งนี้ ผู้ใช้งานประกอบไปด้วย พนักงาน ผู้ที่มาติดต่อ นักวิจัยทั้งภายในและภายนอก ผู้มาเยี่ยมชม บุคคลอื่นในหน่วยงาน (เช่น ฝ่ายบุคคล ฝ่ายฝึกอบรม ฝ่ายประชาสัมพันธ์/สื่อสารองค์กร) และผู้ทำงานร่วมกันหรือผู้ร่วมงานอื่น ๆ ที่ต้องการใช้ระบบสารสนเทศ โดยผู้ใช้งานต้องดำเนินการ ดังนี้

(๑) ทำความเข้าใจและปฏิบัติตามนโยบายและขั้นตอนการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน

(๒) ได้รับการฝึกอบรมอย่างเหมาะสมในเรื่องระเบียบปฏิบัติสำหรับระบบสารสนเทศที่ผู้ใช้มีสิทธิ์เข้าถึงได้

(๓) ประเมินตนเองและเสนอความต้องการด้านการฝึกอบรมต่อหัวหน้าส่วนงานและให้ความร่วมมือกับการสร้างความตระหนักรู้และการฝึกอบรม

(๔) ปรับปรุง (Update Patch) ซอฟต์แวร์และแอปพลิเคชันอย่างสม่ำเสมอ

(๕) ตระหนักถึงการดำเนินการปกป้องข้อมูลของหน่วยงานให้มีประสิทธิผลมากขึ้น การดำเนินการเหล่านี้รวมถึงการใช้รหัสผ่านที่เหมาะสม การสำรองข้อมูล การป้องกันไวรัสที่เหมาะสม การรายงานเหตุการณ์ที่น่าสงสัยหรือการละเมิดนโยบายความมั่นคงปลอดภัยไซเบอร์ การปฏิบัติตามกฎที่กำหนดขึ้นเพื่อหลีกเลี่ยงการโจมตีทางวิศวกรรมสังคม (Social Engineering) และกฎเพื่อยับยั้งการแพร่กระจายของสแปมหรือไวรัสและเวิร์ม

ทั้งนี้ หน่วยงานอาจพัฒนาหรือยกระดับความรู้ความเชี่ยวชาญของบุคลากร ให้มีทักษะและความรู้ความสามารถ ดังตัวอย่างใน *ผนวก ก ตัวอย่างทักษะและความรู้ของบุคลากร* ท้ายแนวทางนี้ โดยการดำเนินการดังกล่าวต้องคำนึงถึงกฎหมายและหลักเกณฑ์ ระบบและเทคโนโลยีที่สำคัญสำหรับดำเนินการทางธุรกิจ และภาพรวมภัยคุกคามทางไซเบอร์ (Threat landscape) รวมถึงกระบวนการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์ที่เกี่ยวข้องกับภารกิจหรือการให้บริการเฉพาะด้านของตนด้วย

๔. ขั้นตอนการพัฒนาทักษะของพนักงานเจ้าหน้าที่หรือบุคลากรของหน่วยงาน

ในการสร้างความตระหนักรู้ การฝึกอบรม และการศึกษา เมื่อมีการกำหนดบทบาทและความรับผิดชอบแล้วนั้น ต้องทำความเข้าใจเกี่ยวกับขั้นตอนการสร้างความตระหนักรู้ การฝึกอบรมและการศึกษา โดยการดำเนินการการสร้างความตระหนักรู้ การฝึกอบรม และการศึกษา ประกอบด้วย ๔ ขั้นตอน ดังนี้

๔.๑ การออกแบบแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรม (Awareness and Training Program Design)

๔.๒ การพัฒนาเอกสาร/สื่อ เนื้อหาสำหรับแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรม (Awareness and Training Material Development)

๔.๓ การดำเนินการแผนงานหรือโครงการ (Program Implementation)

๔.๔ หลังดำเนินการแผนงานหรือโครงการ (Post-Implementation)

โดยในแต่ละขั้นตอน มีรายละเอียดการดำเนินงาน ดังต่อไปนี้

ขั้นตอนที่ ๑ การออกแบบแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรม

ในขั้นตอนนี้จะมีการประเมินความต้องการทั่วทั้งหน่วยงาน มีการพัฒนาและอนุมัติกลยุทธ์การฝึกอบรม เอกสารการวางแผนเชิงกลยุทธ์นี้จะระบุงานการดำเนินการที่จะดำเนินการเพื่อสนับสนุนเป้าหมายการฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานที่จัดตั้งขึ้น โดยมีขั้นตอนย่อย ดังนี้

๑.๑ การกำหนดโครงสร้างของแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรม

การกำหนดโครงสร้างของแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรม สามารถออกแบบ พัฒนาและนำไปใช้ได้หลายรูปแบบ ตามมาตรฐานที่ยอมรับโดยทั่วไป มีการอธิบายแนวทางหรือแบบจำลองไว้ ๓ รูปแบบ คือ

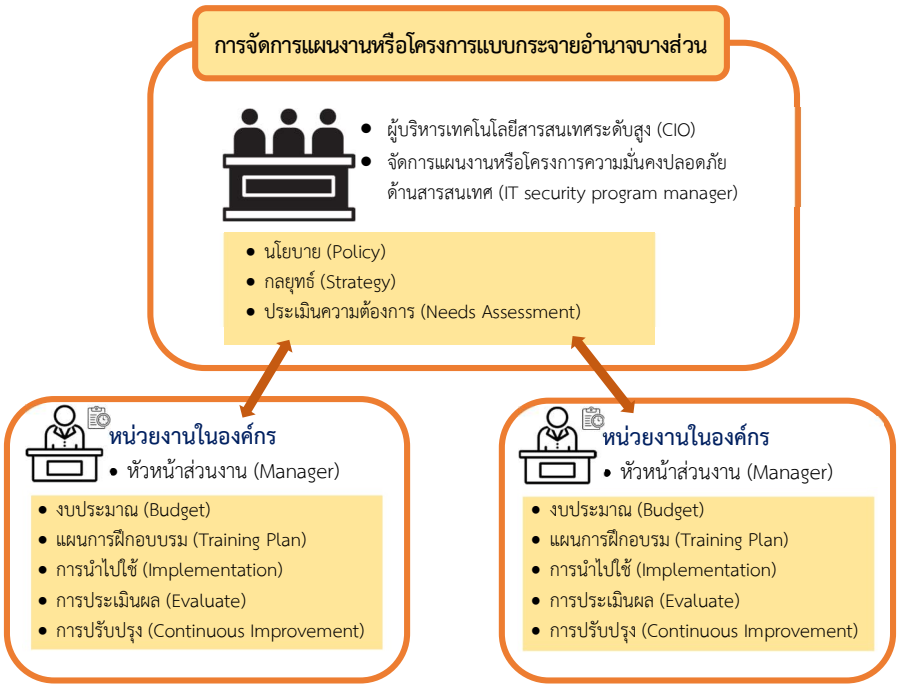
(๑) รูปแบบการจัดการแผนงานหรือโครงการแบบรวมศูนย์ (นโยบาย กลยุทธ์ งบประมาณ แผนการฝึกอบรม และการดำเนินการ อำนาจหน้าที่ทั้งหมดอยู่ที่หน่วยงานส่วนกลาง) เหมาะสมกับหน่วยงานที่มีขนาดเล็ก หรือหน่วยงานที่มีรูปแบบการบริหารแบบบนลงล่าง (Top to Down) ในแบบรูปแบบนี้หน่วยงานส่วนกลางจะสื่อสารและแนะนำหน่วยงานย่อย ในประเด็น (๑.๑) นโยบายและคำสั่งของส่วนกลางเกี่ยวกับการสร้างความตระหนักรู้และการฝึกอบรมเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (๑.๒) กลยุทธ์ เอกสาร/สื่อเนื้อหาความมั่นคงปลอดภัยไซเบอร์ และ (๑.๓) วิธีการนำแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรมไปใช้ หน่วยงานส่วนกลางอาจขอความคิดเห็นจากหน่วยงานย่อยเกี่ยวกับประสิทธิภาพของเอกสาร/สื่อ เนื้อหาการสร้างความตระหนักรู้ วิธีการสื่อสาร หรือการฝึกอบรมด้วยตนเอง ข้อเสนอแนะนี้จะช่วยให้หน่วยงานส่วนกลางสามารถปรับปรุง เอกสาร/สื่อ เนื้อหาตามความจำเป็น เพื่อปรับปรุงแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรม รายละเอียดเพิ่มเติมดังภาพรูปแบบการจัดการแบบรวมศูนย์ ด้านล่าง



ภาพรูปแบบการจัดการแบบรวมศูนย์

(๒) รูปแบบการจัดการแผนงานหรือโครงการแบบกระจายอำนาจบางส่วน (นโยบายและกลยุทธ์แบบรวมศูนย์ที่ส่วนกลาง งบประมาณ แผนการฝึกอบรม และการดำเนินการ จะเป็นแบบกระจายตามหน่วยงานย่อย) เหมาะกับหน่วยงานที่ค่อนข้างใหญ่ มีโครงสร้างที่ค่อนข้างกระจายอำนาจและมีหน้าที่รับผิดชอบที่ชัดเจน หน่วยงานมีหน่วยงานย่อยที่มีความหลากหลาย ในรูปแบบนี้ หน่วยงานส่วนกลางจะสื่อสารนโยบายการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ กลยุทธ์การดำเนินแผนงานหรือโครงการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ และการจัดสรรงบประมาณโดยรวมสำหรับแต่ละหน่วยงานย่อย หน่วยงานส่วนกลางยังดำเนินการประเมินความต้องการของหน่วยงานย่อย เนื่องจากการประเมินนี้จะเป็นแนวทางในการกำหนดกลยุทธ์สำหรับแผนงานหรือโครงการสร้างความตระหนักรู้ หน่วยงานส่วนกลางอาจให้คำแนะนำแก่หน่วยงานย่อยในการจัดทำแผนการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ อย่างไรก็ตาม การจัดการงบประมาณและการนำไปใช้เป็นความรับผิดชอบของหน่วยงานย่อย

ในบทบาทการกำกับดูแล หน่วยงานกลางอาจร้องขอข้อมูลจากหน่วยงานย่อยในรายการต่าง ๆ เป็นประจำ เช่น สถานะของการพัฒนาโปรแกรมการสร้างความตระหนักรู้และการฝึกอบรม ความคืบหน้าในการดำเนินการและการพัฒนาเอกสาร/สื่อ เนื้อหา และงบประมาณ เมื่อแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรมถูกนำมาใช้แล้ว หน่วยงานกลางอาจขอข้อมูลจำนวนผู้เข้าร่วมในการฝึกอบรมการสร้างความตระหนักรู้จำนวนคนที่ผ่านการฝึกอบรมในหัวข้อเฉพาะ และจำนวนผู้ที่ยังไม่ได้เข้าร่วมในกิจกรรมการสร้างความตระหนักรู้ข้อมูลเหล่านี้สามารถช่วยหน่วยงานในการกำหนดระดับการปฏิบัติตามและประสิทธิผลของการนำแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรมของหน่วยงานย่อย รายละเอียดเพิ่มเติมดังภาพรูปแบบการจัดการแผนงานหรือโครงการแบบกระจายอำนาจบางส่วน ด้านล่าง



ภาพรูปแบบการจัดการแผนงานหรือโครงการแบบกระจายอำนาจบางส่วน

(๓) รูปแบบการจัดการแผนงานหรือโครงการแบบกระจายอำนาจอย่างเต็มที่ (นโยบายแบบรวมศูนย์ที่ส่วนกลางแต่กลยุทธ์ งบประมาณ แผนการฝึกอบรม และการดำเนินการเป็นรูปแบบกระจาย หน่วยงานย่อยสามารถออกแบบและดำเนินการเองได้) เหมาะกับหน่วยงานที่ค่อนข้างใหญ่ มีการกระจายอำนาจมาก มีหน่วยงานย่อยแบบกึ่งอิสระ มีภารกิจแยกจากหน่วยงานหลัก ในรูปแบบนี้ หน่วยงานส่วนกลางจะสื่อสารนโยบายการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ที่ครอบคลุมของหน่วยงาน

และความคาดหวังเกี่ยวกับการดำเนินการและการจัดการโปรแกรม ในรูปแบบนี้ หน่วยงานย่อยมีหน้าที่รับผิดชอบในการจัดทำงบประมาณ สร้าง ดำเนินการ และจัดการแผนงานหรือโครงการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ คำสั่งและความคาดหวังต่อหน่วยงานย่อยจะกำหนดโดยหน่วยงานส่วนกลาง นอกจากนี้ การประเมินความต้องการจะดำเนินการโดยแต่ละหน่วยงานย่อย เนื่องจากหน่วยงานย่อยจะใช้ผลการประเมินมากำหนดกลยุทธ์ที่ดีที่สุดสำหรับแผนงานหรือโครงการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ หน่วยงานย่อยจึงพัฒนาแผนการสร้างความตระหนักรู้และการฝึกอบรม วิธีการสื่อสารที่เหมาะสมที่สุดสำหรับความต้องการของตน หน่วยงานกลางอาจร้องขอสถานะของค่าใช้จ่ายแผนงานหรือโครงการสร้างความตระหนักรู้ ผลการประเมินความต้องการการดำเนินการแผนงานหรือโครงการ และผลการฝึกอบรมที่ดำเนินการจนถึงปัจจุบัน รายละเอียดเพิ่มเติมดังภาพรูปแบบการจัดการแผนงานหรือโครงการแบบกระจายอำนาจอย่างเต็มที่ ด้านล่าง



ภาพรูปแบบการจัดการแผนงานหรือโครงการแบบกระจายอำนาจอย่างเต็มที่

ทั้งนี้การเลือกใช้งานในแต่ละรูปแบบนั้นขึ้นอยู่กับ ๑) ขนาดและการกระจายทางภูมิศาสตร์ของหน่วยงาน ๒) การกำหนดบทบาทและความรับผิดชอบของหน่วยงาน และ ๓) การจัดสรรงบประมาณและอำนาจการบริหาร

๑.๒ การดำเนินการ การประเมินตามความต้องการ

การประเมินความต้องการเป็นกระบวนการที่สามารถใช้เพื่อกำหนดการสร้างความตระหนักรู้และการฝึกอบรมของหน่วยงาน โดยผลลัพธ์ของการประเมินความต้องการสามารถให้เหตุผลเพื่อโน้มน้าวให้ฝ่ายบริหารจัดสรรทรัพยากรที่เพียงพอเพื่อตอบสนองความต้องการกำหนดการสร้างความตระหนักรู้และการฝึกอบรม

ในการดำเนินการประเมินความต้องการ สิ่งสำคัญคือ บุคลากรของหน่วยงานโดยหลักต้องมีส่วนร่วม บุคคลต่อไปนี้ควรมีบทบาทการกำหนดความต้องการฝึกอบรมเพิ่มเติม

(๑) ฝ่ายบริหาร (Executive Management) (หัวหน้าหน่วยงาน ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ผู้บริหารหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ) จำเป็นต้องเข้าใจการสั่งการและกฎหมายที่เป็นพื้นฐานสำหรับแผนงานหรือโครงการรักษาความมั่นคงปลอดภัย นอกจากนี้ยังต้องเข้าใจบทบาทและความเป็นผู้นำเพื่อสร้างความมั่นใจให้กับบุคลากรในหน่วยงานของตนเอง

(๒) บุคลากรด้านการรักษาความมั่นคงปลอดภัย (Security Personnel) (ผู้จัดการแผนงานหรือโครงการรักษาความมั่นคงปลอดภัย (Security Program Manager) เจ้าหน้าที่รักษาความมั่นคงปลอดภัย (Security Officer) หรือ เจ้าหน้าที่รักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Staff)) ทำหน้าที่เป็นที่ปรึกษาผู้เชี่ยวชาญสำหรับหน่วยงาน ดังนั้น จึงต้องมีความรู้เกี่ยวกับนโยบายความมั่นคงปลอดภัยและแนวทางปฏิบัติที่ดีซึ่งได้รับการยอมรับเป็นอย่างดี

(๓) เจ้าของระบบสารสนเทศ (Information System Owners) เจ้าของระบบต้องมีความเข้าใจอย่างกว้างขวางเกี่ยวกับนโยบายความมั่นคงปลอดภัย และความเข้าใจในระดับสูงเกี่ยวกับการควบคุมความมั่นคงปลอดภัยและข้อกำหนดที่ใช้กับระบบที่ตนจัดการ

(๔) ผู้ดูแลระบบและบุคลากรของหน่วยงานฝ่ายสนับสนุนด้านเทคโนโลยีสารสนเทศ (System Administrators and IT Support Personnel) ได้รับความไว้วางใจจากผู้มีอำนาจระดับสูงในการดำเนินการสนับสนุนที่มีความสำคัญต่อแผนงานหรือโครงการความมั่นคงปลอดภัยที่ประสบความสำเร็จ บุคคลเหล่านี้ต้องการความรู้ด้านเทคนิคในระดับที่สูงด้านความมั่นคงปลอดภัย และแนวทางปฏิบัติเพื่อการนำไปใช้งาน

(๕) ผู้จัดการฝ่ายปฏิบัติการและผู้ใช้ระบบ (Operational Managers and System Users) บุคคลเหล่านี้ต้องการความรู้ระดับสูงด้านการตระหนักรู้และการฝึกอบรม เกี่ยวกับการควบคุมความมั่นคงปลอดภัยและพฤติกรรมระบบที่ใช้ในการดำเนินธุรกิจ

แนวทางสำหรับการจัดเก็บความต้องการด้านการสร้างความตระหนักรู้และการฝึกอบรมของหน่วยงาน

- การสัมภาษณ์กับทุกกลุ่มเป้าหมายที่เกี่ยวข้องและบุคคลที่หน่วยงานกำหนด
- การสำรวจหน่วยงาน
- การทบทวนและประเมินทรัพยากรที่มีอยู่ เช่น เอกสาร/สื่อ เนื้อหาที่ใช้ในการสร้างความตระหนักรู้และการฝึกอบรมที่มีอยู่ ณ ปัจจุบัน ตารางการฝึกอบรม และรายการของผู้เข้าร่วมแผนงานหรือโครงการ
- การวิเคราะห์ที่เกี่ยวข้องกับการสร้างความตระหนักรู้และการฝึกอบรม เช่น จำนวนร้อยละ (เปอร์เซ็นต์) ของพนักงานที่ผ่านพื้นฐานของการสร้างความตระหนักรู้และการฝึกอบรม จำนวนร้อยละ (เปอร์เซ็นต์) ของพนักงานที่ได้รับการฝึกอบรมตามหน้าที่เฉพาะ
- การทบทวนแผนการรักษาความมั่นคงปลอดภัยสำหรับระบบสนับสนุนทั่วไปและแอปพลิเคชันหลัก เพื่อกำหนดการเป็นเจ้าของระบบและแอปพลิเคชัน และการรักษาความมั่นคงปลอดภัย
- ตรวจสอบระบบคงคลังและฐานข้อมูลรหัสผู้ใช้งานแอปพลิเคชันเพื่อกำหนดว่าใครมีสิทธิ์เข้าถึงได้
- ทบทวนข้อค้นพบหรือคำแนะนำจากหน่วยงานกำกับดูแล หรือการตรวจสอบแผนงานหรือโครงการเกี่ยวกับข้องกับแผนงานหรือโครงการความมั่นคงปลอดภัยไซเบอร์
- การสนทนาและสัมภาษณ์ผู้บริหาร เจ้าของระบบสนับสนุนทั่วไปและแอปพลิเคชันหลักและพนักงานในหน่วยงานอื่น ๆ ที่ทำงานเกี่ยวข้องกับเทคโนโลยีสารสนเทศ

ทั้งนี้ ตัวอย่างคำถามและรายการตรวจสอบความต้องการของบุคลากรในหน่วยงานเพื่อการสร้างความตระหนักรู้และการฝึกอบรม อยู่ใน*ผนวก ข ตัวอย่างการวัดผลการสร้างความตระหนักรู้และการฝึกอบรม* ท้ายแนวทางนี้

๑.๓ การวางแผนและการพัฒนาแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรม

การประเมินความต้องการที่เสร็จสมบูรณ์จะช่วยให้หน่วยงานสามารถพัฒนากลยุทธ์สำหรับการพัฒนาการนำไปใช้ และการบำรุงรักษาแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์ แผนงานจะเป็นเอกสารการทำงานที่มีองค์ประกอบหลากหลายประกอบกันเป็นกลยุทธ์ โดยแผนควรพิจารณาเกี่ยวกับองค์ประกอบต่อไปนี้

- นโยบายระดับชาติและระดับท้องถิ่นที่มีความต้องการสร้างความตระหนักรู้และการฝึกอบรมให้สำเร็จ
- ขอบเขตของแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรม
- บทบาทและความรับผิดชอบของเจ้าหน้าที่ของหน่วยงานที่ทำหน้าที่ออกแบบพัฒนานำไปใช้ และการบำรุงรักษาเอกสาร/สื่อ เนื้อหาการสร้างความตระหนักรู้ และผู้รับผิดชอบในการตรวจสอบความถูกต้องของการเข้าร่วมของพนักงานหรือการดูเอกสาร/สื่อ เนื้อหาที่เกี่ยวข้อง
- เป้าหมายที่ต้องทำให้สำเร็จในแต่ละด้านของแผนงานหรือโครงการ เช่น การสร้างความตระหนักรู้ การฝึกอบรม การศึกษา การพัฒนาวิชาชีพ (การรับรอง)
- กลุ่มเป้าหมายของแผนงานหรือโครงการแต่ละด้าน
- หลักสูตรหรือเอกสารที่จำเป็น (ถ้ามี) สำหรับกลุ่มเป้าหมายแต่ละกลุ่ม
- จุดประสงค์การเรียนรู้ของแผนงานหรือโครงการแต่ละด้าน
  - หัวข้อที่จะนำเสนอในแต่ละช่วงกิจกรรมหรือหลักสูตร
  - วิธีการปรับใช้สำหรับความคาดหวังของแผนงานหรือโครงการแต่ละด้าน
- เอกสาร ข้อเสนอแนะและหลักฐานการเรียนรู้ของแผนงานหรือโครงการแต่ละด้าน
- การประเมินและการปรับปรุงเนื้อหาสำหรับแผนงานหรือโครงการแต่ละด้านและความถี่ที่เข้าถึงเอกสาร/สื่อของกลุ่มเป้าหมายแต่ละราย

ทั้งนี้ จากองค์ประกอบด้านบน สามารถนำมาเขียนโครงร่างแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรมได้ดังตัวอย่างใน*ผนวก ค ตัวอย่างโครงร่างแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรม*

๑.๔ การลำดับความสำคัญ

เมื่อแผนและกลยุทธ์การสร้างความตระหนักรู้และการฝึกอบรมด้านความมั่นคงปลอดภัยได้รับการสรุปแล้วจะต้องมีการกำหนดตารางการดำเนินการ หากเกิดความจำเป็นบางอย่างในขั้นตอนนี้ เช่น ข้อจำกัดด้านงบประมาณและความพร้อมใช้งานของทรัพยากร การเลือกว่าจะกำหนดตารางการดำเนินการอย่างไรและลำดับแบบใดเป็นสิ่งสำคัญที่ต้องตัดสินใจ ดังนั้น ปัจจัยสำคัญที่ควรพิจารณา มีดังนี้

- **ความพร้อมใช้งานของเอกสาร/สื่อ เนื้อหาหรือทรัพยากร (Availability of Material/ Resources)** หากเอกสาร/สื่อ เนื้อหาการสร้างความตระหนักรู้และการฝึกอบรมและทรัพยากรที่จำเป็น พร้อมใช้งาน การเริ่มกำหนดแผนงานเป็นกิจกรรมที่ควรทำก่อน อย่างไรก็ตาม หากต้องมีการพัฒนาเนื้อหาหลักสูตรหรือผู้สอน ต้องมีการระบุและกำหนดเวลา ข้อกำหนดเหล่านี้ควรนำมาพิจารณาในการกำหนดลำดับความสำคัญ

• **บทบาทและผลกระทบต่อหน่วยงาน (Role and Organization Impact)**
เป็นเรื่องปกติที่หน่วยงานจะให้ความสำคัญกับบทบาทและความเสี่ยง การสร้างความตระหนักรู้ให้กับคนทั้งหน่วยงานมีความสำคัญระดับสูง เนื่องจากจำเป็นต้องให้พนักงานเข้าใจถึงกฎของแนวทางปฏิบัติที่ดีด้านความมั่นคงปลอดภัยไซเบอร์ นอกจากนี้ ตำแหน่งในหน่วยงานที่ได้รับความไว้วางใจสูงหรือมีผลกระทบสูง เช่น ผู้จัดการแผนงานหรือโครงการความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Program Manager) เจ้าหน้าที่รักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Officers) ผู้ดูแลระบบ (System Administrators) และผู้ดูแลระบบความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Administrators) ตำแหน่งเหล่านี้จะถูกพิจารณาเป็นกลุ่มที่มีผลกระทบสูง การตรวจสอบให้แน่ใจว่ากลุ่มคนเหล่านี้ได้รับการจัดลำดับความสำคัญ ในระดับสูงในกลยุทธ์การดำเนินการ ตำแหน่งประเภทนี้มักจะสอดคล้องกับประเภทของการเข้าถึงระบบและความเป็นเจ้าของระบบ

• **สถานะของการปฏิบัติในปัจจุบัน (State of Current Compliance)**
เป็นการมองหาจุดบกพร่องที่สำคัญในแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรม เช่น การวิเคราะห์จุดบกพร่อง (Gap Analysis) และการกำหนดเป้าหมายไปที่จุดบกพร่องนั้น ในช่วงแรกของการดำเนินแผนงานหรือโครงการ

• **แผนงานหรือโครงการที่สำคัญที่เกี่ยวข้อง (Critical Project Dependencies)**
หากมีแผนงานหรือโครงการที่เกี่ยวข้องกับส่วนของการฝึกอบรมด้านความมั่นคงปลอดภัย เพื่อเตรียมข้อกำหนดที่จำเป็นสำหรับระบบที่เกี่ยวข้อง เช่น ระบบปฏิบัติการ อุปกรณ์ป้องกันการบุกรุกเครือข่าย เครือข่ายส่วนตัวเสมือน (Virtual Private Network: VPN) การกำหนดการฝึกอบรมจำเป็นต้องตรวจสอบให้แน่ใจว่าการฝึกอบรมที่เกิดขึ้นนั้นอยู่ภายใต้กรอบเวลาที่กำหนดซึ่งจำเป็นต่อการจัดการส่วนที่เกี่ยวข้องเหล่านี้

๑.๕ การกำหนดตัวชี้วัดพื้นฐาน

การกำหนดตัวชี้วัดพื้นฐาน คือ การตัดสินใจเกี่ยวกับความซับซ้อนของเอกสาร/สื่อเนื้อหาที่จะใช้ในการพัฒนาการสร้างความตระหนักรู้และฝึกอบรมด้านความมั่นคงปลอดภัย ซึ่งขึ้นอยู่กับความเหมาะสมและบทบาทของบุคคลที่จะพัฒนา โดยเอกสาร/สื่อ เนื้อหาที่จะใช้ในการพัฒนามีหลักเกณฑ์สำคัญในการพิจารณา ๒ ประการ ดังนี้

(๑) ตำแหน่งภายในหน่วยงาน ของกลุ่มเป้าหมายที่เข้าร่วม

(๒) ทักษะ ความรู้ด้านความมั่นคงปลอดภัยที่จำเป็นสำหรับตำแหน่งนั้น

ต้องมีการกำหนดความซับซ้อนของเอกสาร/สื่อ เนื้อหาก่อนที่จะเริ่มการพัฒนาและมีการกำหนดตัวชี้วัดพื้นฐานให้กับการเรียนรู้ทั้งสามประเภท คือ การสร้างความตระหนักรู้ การฝึกอบรม และการศึกษา

การกำหนดตัวชี้วัดพื้นฐานสำหรับการเรียนรู้นั้น ควรเน้นที่ข้อกำหนดพฤติกรรมที่คาดหวังสำหรับการใช้ระบบสารสนเทศ ซึ่งข้อกำหนดนี้ควรมาจากนโยบายของหน่วยงานการนำไปใช้กับทุกคนในหน่วยงาน ดังนั้นควรอธิบายให้ชัดเจนเพียงพอเพื่อไม่ให้เกิดความสับสนหรือเข้าใจผิดเมื่อแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรมของหน่วยงานเกิดขึ้น และผู้ใช้งานส่วนใหญ่ได้เริ่มเข้าถึงเอกสาร/สื่อ เนื้อหา

การกำหนดตัวชี้วัดพื้นฐาน มีหลายวิธีในการดำเนินการ ตัวอย่างเช่น การพัฒนาหลักสูตรพื้นฐานและการสร้างความตระหนักรู้ โดยในเอกสาร NIST Special Publication 800-16 บทที่ ๓ มีคำแนะนำวิธีการการกำหนดตัวชี้วัดพื้นฐาน และในส่วนที่ ๖ มีการให้ข้อเสนอแนะเพิ่มเติมในการยกระดับการกำหนดตัวชี้วัดพื้นฐาน

๑.๖ เตรียมเงินทุนสำหรับแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรม

เมื่อกลยุทธ์การสร้างความตระหนักรู้และการฝึกอบรมได้รับการยอมรับและมีการกำหนดลำดับความสำคัญแล้ว การกำหนดด้านเงินทุนจะต้องเพิ่มเข้าไปในแผนด้วย ต้องมีการกำหนดเกี่ยวกับขอบเขตของการสนับสนุนเงินทุนที่จะจัดสรรตามรูปแบบการดำเนินการ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) ของหน่วยงานต้องมีการสื่อสารที่ชัดเจนเกี่ยวกับความคาดหวังในการปฏิบัติ แนวทางที่ใช้ในการกำหนดแหล่งเงินทุน จะพิจารณาตามงบประมาณที่มีอยู่หรือที่คาดการณ์ไว้และลำดับความสำคัญของหน่วยงานอื่น ๆ แผนงานการสร้างความตระหนักรู้และการฝึกอบรมต้องพิจารณาตามข้อกำหนดขั้นต่ำที่ต้องปฏิบัติตามและข้อกำหนดเหล่านั้นต้องได้รับการสนับสนุนจากมุมมองด้านงบประมาณหรือตามสัญญา ข้อกำหนดการฝึกอบรมตามสัญญาควรระบุในเอกสารที่มีผลผูกพัน เช่น บันทึกความเข้าใจ (MOU) วิธีการที่ใช้ในการแสดงความต้องการเงินทุนอาจรวมถึง

- ร้อยละ (เปอร์เซ็นต์) ของงบประมาณการฝึกอบรมโดยรวม
- การจัดสรรต่อผู้ใช้ตามบทบาท เช่น การฝึกอบรมเจ้าหน้าที่รักษาความมั่นคงปลอดภัยหลักและผู้ดูแลระบบ จะมีค่าใช้จ่ายสูงกว่าการฝึกอบรมด้านความมั่นคงปลอดภัยทั่วไปสำหรับผู้ที่อยู่ในหน่วยงานที่ไม่ได้ทำหน้าที่เฉพาะด้านความมั่นคงปลอดภัย
- ร้อยละ (เปอร์เซ็นต์) ของงบประมาณด้านเทคโนโลยีสารสนเทศโดยรวม หรือ
- การจัดสรรเงินทุนอย่างชัดเจนตามองค์ประกอบตามค่าใช้จ่ายการใช้งานโดยรวม

ปัญหาในการดำเนินการการสร้างความตระหนักรู้และการฝึกอบรมด้านความมั่นคงปลอดภัย อาจเกิดขึ้นเมื่อการตระหนักด้านความมั่นคงปลอดภัยและความคิดริเริ่มแผนงานหรือโครงการใหม่ในการฝึกอบรมถูกมองว่ามีลำดับความสำคัญต่ำกว่าความคิดริเริ่มงานใหม่อื่น ๆ ของหน่วยงาน ดังนั้น จึงเป็นความรับผิดชอบของผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ในการประเมินลำดับความสำคัญและพัฒนากลยุทธ์เพื่อจัดการกับการขาดแคลนเงินทุน ที่อาจส่งผลกระทบต่อความสามารถของหน่วยงานในการปฏิบัติตามข้อกำหนดการสร้างความตระหนักรู้และการฝึกอบรมด้านความมั่นคงปลอดภัยที่มีอยู่ ซึ่งอาจหมายถึงการปรับการรับรู้และกลยุทธ์การสร้างความตระหนักรู้และการฝึกอบรมให้สอดคล้องกับงบประมาณที่มีอยู่ การจัดหาเงินทุนเพิ่มเติม หรือการจัดสรรทรัพยากรที่มีอยู่ในปัจจุบันใหม่ อาจหมายความว่าแผนการดำเนินการอาจถูกแบ่งเป็นระยะ (Phase) ในช่วงเวลาที่กำหนดจากเงินทุนที่มีอยู่

ขั้นตอนที่ ๒ การพัฒนาเอกสาร/สื่อ เนื้อหาสำหรับแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรม

เมื่อแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรมได้รับการออกแบบแล้วนั้น การพัฒนาเอกสาร/สื่อ เนื้อหาเพื่อสนับสนุน ควรมีการคำนึงถึง

(๑) ต้องการเสริมพฤติกรรมอะไร (การรับรู้) และ

(๒) ทักษะหรือกลุ่มทักษะใด ที่ต้องการให้ผู้รับการอบรมได้เรียนรู้ หรือนำไปใช้ (การฝึกอบรม)

การพัฒนาเอกสาร/สื่อ เนื้อหาทั้งสองกรณี ควรเน้นเนื้อหาเฉพาะของผู้ใช้งานควรรวมเข้ากับงานของตน หากผู้ใช้งานรู้สึกได้ว่าเนื้อหานั้นถูกพัฒนาขึ้นมาเพื่อพวกเขาโดยเฉพาะ จะทำให้ผู้ใช้งานเห็นว่า “เขามาทำการฝึกอบรมเพราะอะไร และทำไมพวกเขาถึงต้องมา” ทำให้แผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรมมีประสิทธิภาพ นอกจากนี้การฝึกอบรมยังเป็นส่วนหนึ่งของการดำเนินงานประจำปีอีกด้วย อย่างไรก็ตาม เอกสาร/สื่อ เนื้อหาจำเป็นต้องมีความน่าสนใจและเป็นปัจจุบัน

ขั้นตอนนี้เน้นที่ทรัพยากรการฝึกอบรมที่มีอยู่ เช่น แหล่งข้อมูล ขอบเขต เนื้อหา และการพัฒนาเอกสาร/สื่อ เนื้อหาในการฝึกอบรม รวมถึงการขอความช่วยเหลือจากผู้รับจ้างภายนอกหากจำเป็น โดยมีขั้นตอนย่อย ดังนี้

๒.๑ การพัฒนาเอกสาร/สื่อ เนื้อหาของการสร้างความตระหนักรู้

คำถามที่ต้องตอบเมื่อเริ่มพัฒนาเอกสาร/สื่อ เนื้อหาสำหรับแผนงานหรือโครงการหรือการรณรงค์ การสร้างความตระหนักรู้ทั่วทั้งหน่วยงาน คือ “เราต้องการให้บุคลากรทุกคนในหน่วยงานตระหนักถึงอะไรเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์” แผนการสร้างความตระหนักรู้และการฝึกอบรมควรประกอบด้วยหัวข้อต่าง ๆ ดังนี้ คำแนะนำทางอีเมล เว็บไซต์ข่าวรายวันด้านความมั่นคงปลอดภัยไซเบอร์ออนไลน์ และวารสารต่าง ๆ เป็นแหล่งแนวคิดและเอกสาร/สื่อ เนื้อหาที่ดี นอกจากนี้อาจจะเพิ่มเติมหัวข้อ นโยบายของหน่วยงาน การทบทวนแผนงานหรือโครงการ การตรวจสอบภายใน การทบทวนแผนงานหรือโครงการควบคุมภายในการประเมินตนเอง และการตรวจสอบเฉพาะจุดได้อีกด้วย

๒.๒ การพัฒนาเอกสาร/สื่อ เนื้อหาของการฝึกอบรม

คำถามที่ต้องตอบเมื่อเริ่มพัฒนาเอกสาร/สื่อ เนื้อหาสำหรับหลักสูตรการฝึกอบรมเฉพาะ คือ “ทักษะหรือกลุ่มทักษะใด ที่ต้องการให้ผู้รับการอบรมได้เรียนรู้” แผนการสร้างความตระหนักรู้และการฝึกอบรม ควรระบุผู้ใช้งานหรือกลุ่มของผู้ใช้งาน ที่ควรได้รับการฝึกอบรมปรับให้เหมาะกับความรับผิดชอบด้านความมั่นคงปลอดภัยไซเบอร์ซึ่งวิธีการในการสร้างหลักสูตรการฝึกอบรมสำหรับกลุ่มของผู้ใช้งาน ใน NIST Special Publication 800-16, Information Technology Security Training Requirements: A Role-Based and Performance-Based Model มีวิธีการแนะนำในการหาความต้องการและหัวข้อในการสร้างความตระหนักรู้ ไว้ดังตัวอย่าง IT Security Training Matrix – System Administrator ซึ่งเป็นการกำหนดเนื้อหา/หลักสูตรในการฝึกอบรมเฉพาะด้านสำหรับตำแหน่งงานผู้ดูและระบบ (System Administrator)

ตัวอย่าง IT Security Training Matrix — System Administrator

Training Areas	Functional Specialties						
	A Manage	B Acquire	C Design and Develop	D Implement and Operate	E Review and Evaluate	F Use	G Other
1. Laws and Regulations				1D			
2. Security Program							
2.1 Planning							
2.2 Management				2.2D			
3. System Life Cycle Security							
3.1 Initiation							
3.2 Development				3.2D			
3.3 Test and Evaluation				3.3D			
3.4 Implementation			3.4C	3.4D			

Training Areas	Functional Specialties						
	A Manage	B Acquire	C Design and Develop	D Implement and Operate	E Review and Evaluate	F Use	G Other
3.5 Operations	3.5A		3.5C	3.5D			
3.6 Termination				3.6D			
4. Other							

โดยตารางตัวอย่างนี้ แบ่งลักษณะงานของผู้ดูแลระบบออกเป็น ๖ กลุ่ม ซึ่งอิงกับปัจจัยพื้นฐานเนื้อหาในการฝึกอบรมหรือขอบเขตการฝึกอบรม โดยมีรายละเอียดดังนี้

(๑) ผู้จัดการ หมายความว่า บุคคลที่ทำหน้าที่ในการจัดการงาน หรือลักษณะงานด้านเทคโนโลยีสารสนเทศในหน่วยงาน

(๒) ผู้จัดหา หมายความว่า บุคคลที่มีส่วนร่วมในการซื้อผลิตภัณฑ์หรือบริการด้านเทคโนโลยีสารสนเทศ เช่น ทำหน้าที่ในคณะกรรมการคัดเลือกแหล่งที่มาเพื่อประเมินข้อเสนอของผู้จำหน่ายสำหรับระบบสารสนเทศ

(๓) ผู้ออกแบบและพัฒนา หมายความว่า บุคคลที่เป็นผู้ออกแบบและพัฒนาระบบสารสนเทศ หรือโปรแกรมประยุกต์

(๔) ผู้ดำเนินการ หมายความว่า บุคคลที่ดำเนินการ (ดูแล) ระบบสารสนเทศ เช่น เครื่องแม่ข่ายให้บริการเว็บไซต์ เครื่องแม่ข่ายให้บริการจดหมายอิเล็กทรอนิกส์ ระบบเครือข่ายระยะใกล้ (LAN) ระบบเครือข่ายระยะไกล (WAN) เครื่องแม่ข่ายอื่นในระบบ

(๕) ผู้ตรวจสอบและประเมิน หมายความว่า บุคคลที่ทำหน้าที่ตรวจสอบและประเมินการดำเนินงานด้านเทคโนโลยีสารสนเทศ ซึ่งการดำเนินการตรวจสอบและประเมินนี้ เป็นส่วนหนึ่งของโปรแกรมการควบคุมภายในของหน่วยงาน การตรวจสอบภายใน หรือโปรแกรมการตรวจสอบภายนอก

(๖) ผู้ใช้งาน หมายความว่า บุคคลที่เข้าถึงทรัพยากรด้านเทคโนโลยีสารสนเทศหรือใช้เทคโนโลยีสารสนเทศในการทำงาน

แหล่งที่มาของเอกสาร/สื่อ เนื้อหาของการฝึกอบรม

การพิจารณาแหล่งที่มาของเอกสาร/สื่อ และเนื้อหาการฝึกอบรมเพื่อสร้างหลักสูตร คือ การตัดสินใจว่าจะพัฒนาเอกสาร/สื่อ และเนื้อหาภายในหน่วยงานหรือจ้างเหมา หากหน่วยงานมีความเชี่ยวชาญภายในหน่วยงานและสามารถจัดสรรทรัพยากรที่จำเป็นเพื่อพัฒนาเอกสาร/สื่อ เนื้อหาการสอนและหลักสูตรการฝึกอบรมได้ ก็สามารถใช้ NIST Special Publication 800-16 เป็นแนวทางในการกำหนดแหล่งที่มาได้ ตัวอย่างคำถามสำคัญ เพื่อใช้ในการตัดสินใจจะพัฒนาเอกสาร/สื่อ เนื้อหาภายในหน่วยงานหรือจ้างเหมา เช่น

- เรามีทรัพยากรภายในหน่วยงานเพื่อทำงานนี้หรือไม่ รวมถึงคนที่มีทักษะที่เหมาะสมและมีคนเพียงพอที่จะทำงาน
- การพัฒนาเอกสาร/สื่อ และเนื้อหาภายในหน่วยงานคุ้มค่ากว่าเมื่อเทียบกับการจ้างเหมาจากภายนอกหรือไม่
- มีกลไกการจัดหาเงินทุน (งบประมาณ) หรือไม่

• เรามีบุคลากรที่สามารถทำหน้าที่เป็นตัวแทนเจ้าหน้าที่ด้านเทคนิคการทำสัญญา (COTR) และติดตามกิจกรรมของผู้รับจ้างเหมาได้อย่างมีประสิทธิภาพหรือไม่

• หน่วยงานมีทรัพยากรที่จำเป็น เช่น เงินทุนและพนักงานที่มีความเชี่ยวชาญที่จำเป็นเพื่อบำรุงรักษาเอกสาร/สื่อ เนื้อหาหรือไม่ หากได้รับการพัฒนาโดยผู้รับจ้างเหมา

• ความละเอียดอ่อนของเนื้อหาหลักสูตร ห้ามไม่ให้มีผู้รับจ้างเหมาหรือไม่

• การใช้ผู้เชี่ยวชาญภายนอก (Outsource) ช่วยให้สามารถจัดตารางการฝึกอบรมที่สำคัญได้หรือไม่

หากหน่วยงานตัดสินใจว่า จ้างบุคคลภายนอกให้พัฒนาหลักสูตรการฝึกอบรม มีผู้ให้บริการหลายรายที่เสนอหลักสูตร “หลักสูตรเฉพาะ” ที่เหมาะสำหรับผู้ใช้งานเฉพาะกลุ่ม หรือสามารถพัฒนาหลักสูตรสำหรับผู้ใช้งานเฉพาะกลุ่มได้ ก่อนที่จะเลือกผู้ให้บริการรายใดรายหนึ่งนั้น หน่วยงานควรมีความเข้าใจอย่างถ่องแท้เกี่ยวกับความต้องการในการฝึกอบรมของผู้ใช้งาน และสามารถระบุได้ว่าหลักสูตรของผู้ให้บริการนั้นตรงตามความคาดหวังของผู้ใช้งานหรือไม่

ขั้นตอนที่ ๓ การดำเนินการแผนงานหรือโครงการ

ขั้นตอนนี้ระบุถึงการสื่อสารที่มีประสิทธิภาพและการเปิดตัวของแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรม นอกจากนี้ยังระบุทางเลือกสำหรับการเผยแพร่สื่อสารเอกสาร/สื่อ เนื้อหาในการสร้างความตระหนักรู้และการฝึกอบรม ตัวอย่างเช่น ทางเว็บไซต์ การเรียนรู้ทางไกล วิดีโอ การฝึกอบรมในสถานที่ตั้ง การดำเนินการแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์นั้น ต้องมีการดำเนินการดังต่อไปนี้ ก่อนนำไปใช้

• ดำเนินการประเมินความต้องการ

• มีการกำหนดกลยุทธ์เรียบร้อยแล้ว

• มีการกำหนดแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรมสำหรับการดำเนินการตามกลยุทธ์เสร็จสมบูรณ์แล้ว

• พัฒนาเอกสาร/สื่อ เนื้อหาแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรมแล้ว การดำเนินการแผนงานหรือโครงการ โดยมีขั้นตอนย่อย ดังนี้

๓.๑ การสื่อสารแผนงานหรือโครงการ

การดำเนินการของแผนงานหรือโครงการ ต้องทำการสื่อสารไปยังทุกส่วนของหน่วยงานเพื่อให้ได้รับการสนับสนุนสำหรับการดำเนินการ และการจัดการทรัพยากรที่จำเป็นต้องใช้งาน โดยต้องคำนึงถึงความคาดหวังของหน่วยงานในการจัดการ และการสนับสนุนของพนักงาน ซึ่งผลของความคาดหวังของแผนงานหรือโครงการจะมีประโยชน์ต่อหน่วยงาน โดยจะมีการกำหนดเงินทุนที่จะใช้ในแผนงานหรือโครงการ ตัวอย่างเช่น หัวหน้าหน่วยงานต้องรู้ว่าจะต้องใช้งบประมาณโดยรวมในการดำเนินการแผนงานหรือโครงการสร้างความตระหนักรู้จากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง หรืองบประมาณในแผนงานหรือโครงการด้านความมั่นคงปลอดภัยไซเบอร์ จำเป็นอย่างยิ่งที่ผู้เกี่ยวข้องในการดำเนินแผนงานหรือโครงการ ต้องเข้าใจบทบาทและความรับผิดชอบของตน นอกจากนี้ ต้องมีการสื่อสารกำหนดการและความคาดหวังเมื่อดำเนินการแล้วเสร็จ

การสื่อสารแผนควรจะมีการกำหนดให้สอดคล้องกับรูปแบบการดำเนินการตามที่อธิบายไว้ในขั้นตอนที่ ๑

๓.๒ การถ่ายทอดเอกสาร/สื่อ เนื้อหาของแผนงานหรือโครงการสร้างความตระหนักรู้

การถ่ายทอดเอกสาร/สื่อ เนื้อหาของแผนงานหรือโครงการสร้างความตระหนักรู้เป็นการสร้างการรับรู้ในเรื่องความมั่นคงปลอดภัยไซเบอร์ไปยังทั่วทั้งหน่วยงาน สามารถทำได้หลายวิธีการ

และขึ้นอยู่กับความพร้อมของทรัพยากรและความซับซ้อนของเนื้อหา ตัวอย่างเช่น โปสเตอร์ ภาพพักหน้าจอ แผ่นพับ จดหมายอิเล็กทรอนิกส์ รวมถึงเว็บไซต์ สื่อวิดีโอ การจัดอบรม ณ สถานที่ตั้ง หรือการจัดอบรมออนไลน์ การสัมมนาในหัวข้อที่สนใจ (Brown Bag Seminar)

ตัวอย่างของเทคนิคที่ใช้ในการถ่ายทอด มีหลายรูปแบบ ตัวอย่างเช่น

• เทคนิคที่ใช้เพื่อเผยแพร่หรือสื่อสารข้อความเดียว ได้แก่ โปสเตอร์ รายการเข้าถึง ภาพพักหน้าจอและป้ายเตือน ข้อความอีเมลของหน่วยงาน สัมมนาในหัวข้อที่สนใจ และแผนงานหรือโครงการให้รางวัล

• เทคนิคที่สามารถรวมข้อความจำนวนมากได้ง่ายขึ้น ได้แก่ รายการที่ควรทำและไม่ควรทำจดหมายข่าว วิดีโอ เว็บไซต์ การประชุมทางไกล การสอนด้วยตนเอง การสัมมนาในหัวข้อที่สนใจ

• เทคนิคที่ใช้งบประมาณต่ำในการนำไปปฏิบัติ ได้แก่ ข้อความบนโปสเตอร์ รายการเข้าถึง รายการที่ควรทำและไม่ควรทำ รายการตรวจสอบ ภาพพักหน้าจอและป้ายเตือน การสอนด้วยตนเอง การสัมมนาในหัวข้อที่สนใจ

• เทคนิคที่อาจต้องใช้ทรัพยากรมากขึ้น ได้แก่ จดหมายข่าว วิดีโอ เว็บไซต์ การประชุมทางไกล

ทั้งนี้ นอกเหนือจากการทำให้เอกสาร/สื่อ เนื้อหาการสร้างความตระหนักรู้น่าสนใจและเป็นปัจจุบันแล้ว การทำซ้ำข้อความการสร้างความตระหนักรู้ และใช้วิธีต่าง ๆ ในการนำเสนอข้อความนั้น สามารถเพิ่มความจำในบทเรียนหรือประเด็นปัญหาของผู้ใช้งานในการสร้างความตระหนักรู้ได้อย่างมาก ตัวอย่างเช่น การอภิปรายโดยผู้สอนเกี่ยวกับการหลีกเลี่ยงการตกเป็นเหยื่อของการโจมตีแบบวิศวกรรมสังคม สามารถเสริมด้วยโปสเตอร์ ข้อความอีเมลเป็นระยะ

๓.๓ การถ่ายทอดเอกสาร/สื่อ เนื้อหาของแผนงานหรือโครงการฝึกอบรม

การถ่ายทอดเอกสาร/สื่อ เนื้อหาของแผนงานหรือโครงการฝึกอบรม กระบวนการที่เสริมสร้างความรู้ ทักษะ สมรรถนะและความสามารถของบุคคล หรือกลุ่มบุคคลด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่จำเป็นตามสายงานที่เกี่ยวข้อง เทคนิคในการถ่ายทอดเอกสาร/สื่อ เนื้อหาการฝึกอบรมอย่างมีประสิทธิภาพควรใช้ประโยชน์จากเทคโนโลยีที่สนับสนุนคุณลักษณะต่อไปนี้

• ใช้งานง่าย (Ease of Use) เช่น เข้าถึงง่าย ปรับปรุง/บำรุงรักษาง่าย

• การปรับขนาดได้ (Scalability) เช่น ใช้ได้กับจำนวนผู้ใช้งานที่หลากหลายและหลากหลายสถานที่

• รับผิดชอบ (Accountability) เช่น มีการบันทึกและใช้สถิติเกี่ยวกับระดับความสำเร็จ

• ฐานการสนับสนุนอุตสาหกรรมที่กว้างขวาง (Broad Base of Industry Support) เช่น จำนวนผู้ขายที่มีศักยภาพเพียงพอ โอกาสที่ดีกว่าในการติดตามผลและสนับสนุนเทคนิคทั่วไป

บางอย่างที่หน่วยงานสามารถนำไปใช้ได้ ได้แก่

• การฝึกอบรมผ่านวิดีโอเชิงโต้ตอบ (Interactive Video Training)

• การฝึกอบรมบนเว็บไซต์ (Web-based Training)

• การฝึกอบรมผ่านคอมพิวเตอร์ที่ไม่ใช่เว็บไซต์ (Non-web, Computer-based Training)

• การฝึกอบรมนอกสถานที่โดยผู้สอน (Outsite, Instructor-led Training) รวมถึงการนำเสนอโดยผู้เกี่ยวข้องและการให้คำปรึกษา

ทั้งนี้ การผสมผสานเทคนิคการถ่ายทอดการฝึกอบรมต่าง ๆ ในการดำเนินการเดียวเป็นวิธีที่มีประสิทธิภาพในการถ่ายทอดเอกสาร/สื่อ เนื้อหา และดึงความสนใจของผู้ใช้งาน

ขั้นตอนที่ ๔ หลังดำเนินการแผนงานหรือโครงการ

ขั้นตอนนี้จะเป็นการให้คำแนะนำในการทำให้แผนงานหรือโครงการเป็นปัจจุบันอยู่เสมอ และการตรวจสอบประสิทธิภาพของแผนงานหรือโครงการ มีการอธิบายวิธีการรับฟังผลสะท้อนกลับที่มีประสิทธิภาพ ตัวอย่างเช่น แบบสำรวจ การรับฟังความคิดเห็นกลุ่มเป้าหมาย การเปรียบเทียบ โดยพิจารณาโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศและการเปลี่ยนแปลงของหน่วยงาน การเปลี่ยนแปลงภารกิจและลำดับความสำคัญของหน่วยงาน ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง และหัวหน้าแผนงานหรือโครงการด้านความมั่นคงปลอดภัยไซเบอร์ จำเป็นต้องรับรู้ถึงปัญหาที่อาจเกิดขึ้นและนำกลไกต่าง ๆ รวมเข้ากับกลยุทธ์ เพื่อให้แน่ใจว่าแผนงานหรือโครงการยังคงมีความเกี่ยวข้องและสอดคล้องกับวัตถุประสงค์โดยรวมของหน่วยงาน

การปรับปรุงอย่างต่อเนื่องควรเป็นหัวข้อสำคัญในการเริ่มดำเนินการสำหรับการสร้างความตระหนักรู้และการฝึกอบรม ขั้นตอนหลังการดำเนินแผนงานหรือโครงการ มีขั้นตอนย่อย ดังนี้

๔.๑ การตรวจสอบการปฏิบัติตาม

เมื่อจัดแผนงานหรือโครงการเป็นที่เรียบร้อยแล้ว จะต้องวางกระบวนการเพื่อตรวจสอบการปฏิบัติตามและประสิทธิผลของแผนงานหรือโครงการ มีระบบติดตามอัตโนมัติที่ได้รับการออกแบบเพื่อเก็บข้อมูลสำคัญเกี่ยวกับกิจกรรมของแผนงานหรือโครงการ เช่น หลักสูตร วันที่ ผู้เข้าร่วม ค่าใช้จ่าย แหล่งที่มา โดยระบบติดตามนี้ควรเก็บข้อมูลระดับหน่วยงาน เพื่อให้สามารถใช้ในการวิเคราะห์ภาพรวมและรายงานเกี่ยวกับการสร้างความตระหนักรู้ การฝึกอบรม และการริเริ่มด้านการศึกษา ข้อกำหนดสำหรับฐานข้อมูล ควรรวบรวมความต้องการของผู้ใช้งานทั้งหมด โดยทั่วไปผู้ใช้งานฐานข้อมูลดังกล่าวจะรวมถึง

- ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง สามารถใช้ฐานข้อมูลเพื่อสนับสนุนการวางแผนเชิงกลยุทธ์ แจ้งหัวหน้าหน่วยงานและเจ้าหน้าที่บริหารระดับสูงอื่น ๆ เกี่ยวกับสถานภาพของแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์ ระบุความสามารถภายในหน่วยงานและความต้องการที่สำคัญในด้านบุคลากรด้านความมั่นคงปลอดภัย ดำเนินการวิเคราะห์แผนงานหรือโครงการ ระบุกิจกรรมทั่วทั้งหน่วยงาน ช่วยเหลือในเรื่องงบประมาณด้านการรักษาความมั่นคงปลอดภัยและงบประมาณด้านเทคโนโลยีสารสนเทศ ระบุความจำเป็นในการปรับปรุงแผนงานหรือโครงการ และประเมินการปฏิบัติตามหัวหน้าแผนงานหรือโครงการด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Program Manager) สามารถใช้ฐานข้อมูลเพื่อสนับสนุนการวางแผนการรักษาความมั่นคงปลอดภัย รายงานสถานะต่อผู้บริหารเทคโนโลยีสารสนเทศระดับสูงฝ่ายบริหาร และเจ้าหน้าที่รักษาความมั่นปลอดภัย ระบุคำของบประมาณ แสดงให้เห็นถึงการปฏิบัติตามเป้าหมายและวัตถุประสงค์ที่หน่วยงานกำหนดขึ้น ระบุผู้ให้การฝึกอบรมและแหล่งข้อมูลการฝึกอบรมอื่น ๆ ตอบสนองต่อข้อซักถามที่เกี่ยวข้องกับความมั่นคงปลอดภัย ระบุความครอบคลุมของแผนงานในปัจจุบัน และทำการปรับเปลี่ยนเมื่อมีเหตุจำเป็นต้องดำเนินการ และละเว้นการดำเนินการ
- แผนกทรัพยากรบุคคล (Human Resource Department) สามารถใช้ฐานข้อมูลเพื่อให้แน่ใจว่ามีกลไกที่มีประสิทธิภาพสำหรับการรวบรวมข้อมูลการฝึกอบรมที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยทั้งหมด ระบุค่าใช้จ่ายที่เกี่ยวข้องกับการฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์ ช่วยเหลือในการจัดทำคำอธิบายตำแหน่ง สนับสนุนการรายงานสถานะ ตอบคำถามเกี่ยวกับการฝึกอบรม และช่วยเหลือในพัฒนาด้านวิชาชีพ
- แผนกฝึกอบรมหน่วยงาน (Agency Training Department) สามารถใช้ฐานข้อมูล เพื่อช่วยในการพัฒนากลยุทธ์การฝึกอบรมหน่วยงานโดยรวม สร้างข้อกำหนดฐานข้อมูลการฝึกอบรมที่เชื่อมโยงโดยตรงกับด้านความมั่นคงปลอดภัย ระบุแหล่งการฝึกอบรมที่เป็นไปได้ สนับสนุนคำขอฝึกอบรม ระบุความเกี่ยวข้องและความนิยมของหลักสูตร สนับสนุนกิจกรรมการจัดทำงบประมาณและตอบข้อซักถาม

• หัวหน้างาน (Functional Manager) สามารถใช้ฐานข้อมูลเพื่อตรวจสอบความคืบหน้าในการฝึกอบรมของผู้ใช้งานและปรับแผนการฝึกอบรมตามความจำเป็น รับรายงานสถานะและตอบข้อซักถามเกี่ยวกับส่วนเสริมในการฝึกอบรมด้านความมั่นคงปลอดภัย และระบุแหล่งฝึกอบรมและค่าใช้จ่ายเพื่อช่วยเหลือเกี่ยวกับข้อเสนอและคำของบประมาณ

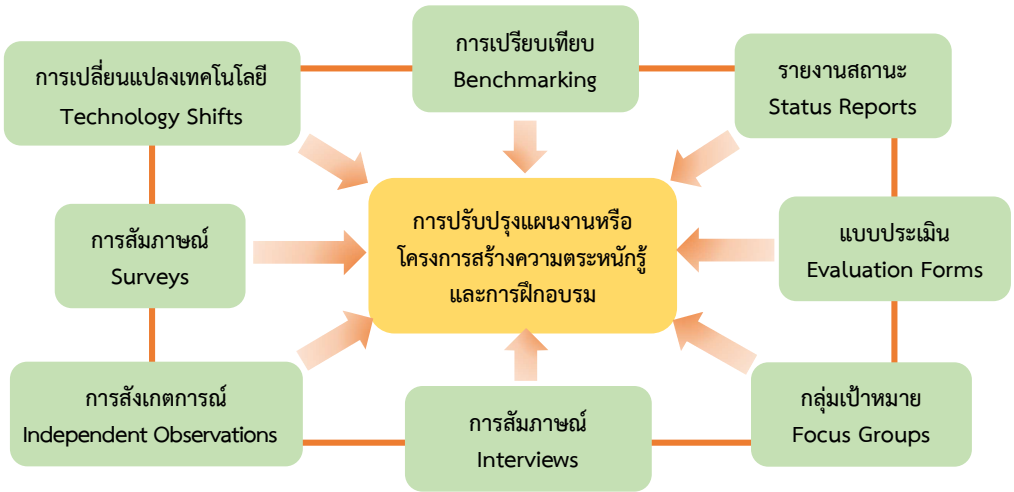
• ผู้ตรวจสอบ (Auditor) สามารถใช้ข้อมูลจากฐานข้อมูลเพื่อตรวจสอบการปฏิบัติตามข้อกำหนดด้านความมั่นคงปลอดภัยและนโยบายของหน่วยงาน

• หัวหน้าฝ่ายการเงิน (CFO) สามารถใช้ข้อมูลจากฐานข้อมูลเพื่อตอบข้อซักถามเกี่ยวกับงบประมาณ ช่วยในการวางแผนทางการเงิน และจัดทำรายงานต่อหัวหน้าหน่วยงานและหัวหน้าอาวุโสเกี่ยวกับเงินทุนสำหรับกิจกรรมการฝึกอบรมด้านความมั่นคงปลอดภัย

ทั้งนี้ การติดตามการปฏิบัติตามเกี่ยวข้องกับการประเมินสถานะของแผนงานหรือโครงการตามที่ระบุโดยข้อมูลในฐานข้อมูล และทำการเทียบกับมาตรฐานที่กำหนดโดยหน่วยงานสามารถสร้างรายงานและนำไปใช้เพื่อระบุความแตกต่างหรือปัญหา ซึ่งจะถูกนำมาใช้ในการดำเนินการแก้ไขและติดตามผลที่จำเป็น อาจอยู่ในรูปแบบของการแจ้งเตือนอย่างเป็นทางการถึงฝ่ายบริหาร รวมไปถึงการสร้างความตระหนักรู้ การฝึกอบรมหรือข้อเสนอด้านการศึกษา หรือการจัดทำแผนการแก้ไขที่มีการกำหนดวันแล้วเสร็จ

๔.๒ การประเมินผลและข้อเสนอแนะ

เมื่อจัดแผนงานหรือโครงการเป็นที่เรียบร้อยแล้ว จะต้องทำการประเมินการรับรู้และความเข้าใจที่ได้รับจากการจัดแผนงานหรือโครงการ โดยการกำหนดรูปแบบการประเมินผลให้สอดคล้องกับระดับของแผนงานหรือโครงการ การประเมินผลอย่างเป็นทางการและกลไกของข้อเสนอแนะเป็นองค์ประกอบที่สำคัญของแผนงานหรือโครงการสร้างความตระหนักรู้ การฝึกอบรม และการศึกษาด้านความมั่นคงปลอดภัยการปรับปรุงอย่างต่อเนื่องไม่สามารถเกิดขึ้นได้หากปราศจากความเข้าใจว่าแผนงานหรือโครงการที่มีอยู่ทำงานอย่างไร นอกจากนี้ กลไกของข้อเสนอแนะ ต้องได้รับการออกแบบเพื่อระบุวัตถุประสงค์เบื้องต้นในการจัดตั้งแผนงานหรือโครงการ เมื่อข้อกำหนดพื้นฐานมีความมั่นคงแล้ว กลยุทธ์ของข้อเสนอแนะสามารถออกแบบและถูกนำไปใช้ การประเมินผลและกลไกของข้อเสนอแนะที่หลากหลาย สามารถใช้เพื่อปรับปรุงแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรมได้ รายละเอียดดังภาพเทคนิคการประเมินและข้อเสนอแนะ ด้านล่าง



ภาพเทคนิคการประเมินและข้อเสนอแนะ

กลยุทธ์ของข้อเสนอแนะจำเป็นต้องรวมองค์ประกอบที่กล่าวถึงคุณภาพ ขอบเขต ระดับความยากง่ายในการใช้งาน ระยะเวลาดำเนินการ ความเกี่ยวข้อง วิธีการปรับใช้ เช่น บนเว็บไซต์ในสถานที่ตั้ง และคำแนะนำสำหรับการปรับเปลี่ยน

การขอความคิดเห็นหรือข้อเสนอแนะ สามารถทำได้หลายวิธี ที่พบมากที่สุด ได้แก่

• แบบประเมิน/แบบสอบถาม (Evaluation Form/Questionnaire) สามารถใช้งานได้หลากหลายรูปแบบ การออกแบบประเมินที่ดีโดยการช่วยลดความจำเป็นในการเขียนจำนวนมาก ในส่วนที่ผู้ทำการประเมินต้องกรอก ปัจจัยสำคัญคือการออกแบบแบบฟอร์มให้ “เป็นมิตรกับผู้ใช้” มากที่สุด การออกแบบเครื่องมือในการประเมินควรทำงานร่วมกับผู้เชี่ยวชาญภายในหน่วยงานที่คุ้นเคยกับเทคนิคการประเมิน หรือขอความช่วยเหลือจากผู้เชี่ยวชาญภายนอก

• กลุ่มเป้าหมาย (Focus Groups) นำหัวข้อของการฝึกอบรมมาหารือในที่ประชุมแบบเปิด เพื่อรับฟังมุมมองของกลุ่มเป้าหมายเกี่ยวกับประสิทธิผลของแผนงานหรือโครงการฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์ และขอแนวคิดของกลุ่มเป้าหมายสำหรับการปรับปรุง

• การสัมภาษณ์แบบเจาะจง (Selective Interviews) แนวทางนี้จะระบุกลุ่มเป้าหมายการฝึกอบรมตามผลกระทบ ลำดับความสำคัญ หรือเกณฑ์ที่กำหนดขึ้นอื่น ๆ ก่อน และระบุประเด็นเฉพาะสำหรับข้อเสนอแนะ โดยปกติแล้วจะใช้การสัมภาษณ์แบบตัวต่อตัวหรือกลุ่มเล็ก ๆ (ไม่เกินสิบคน) แนวทางนี้ให้ความสนใจเฉพาะบุคคลและเป็นส่วนตัวมากกว่าแนวทางตามกลุ่มเป้าหมาย และอาจกระตุ้นให้ผู้เข้าร่วมมีความพร้อมมากขึ้นในการวิจารณ์แผนงาน/แผนงานหรือโครงการ

• การสังเกตการณ์/การวิเคราะห์โดยอิสระ (Independent Observation/Analysis) อีกแนวทางหนึ่งสำหรับการขอความคิดเห็น คือ การเข้าร่วมการตรวจสอบแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์ เป็นงานสำหรับผู้ให้บริการฝึกอบรมภายนอกหรือบุคคลที่สามอื่น ๆ ซึ่งเป็นหน่วยงานตรวจสอบ หน่วยงานจะทำเช่นนี้นอกเหนือจากกิจกรรมการกำกับดูแลตามปกติ เพื่อรับความคิดเห็นที่เป็นกลางเกี่ยวกับประสิทธิผลของแผนงานหรือโครงการ

• รายงานสถานะอย่างเป็นทางการ (Formal Status Report) เป็นวิธีที่ดีในการให้ความสำคัญกับข้อกำหนดการสร้างความตระหนักรู้และการฝึกอบรมด้านความมั่นคงปลอดภัยทั่วทั้งหน่วยงาน ที่นำมาใช้เป็นข้อกำหนดสำหรับการรายงานสถานะปกติโดยหัวหน้างาน

• การเปรียบเทียบแผนงานหรือโครงการด้านความมั่นคงปลอดภัยไซเบอร์ (มุมมองภายนอก) หลายหน่วยงานนำเอาแผนงานหรือโครงการด้านความมั่นคงปลอดภัยไซเบอร์ เป็นส่วนหนึ่งของการเทียบมาตรฐานของกลยุทธ์ในการปรับปรุงอย่างต่อเนื่องและมุ่งมั่นสู่ความเป็นเลิศ รูปแบบการเทียบมาตรฐานความมั่นคงปลอดภัยที่มุ่งเน้นภายนอก จะเปรียบเทียบประสิทธิภาพของหน่วยงานกับองค์กรอื่น ๆ จำนวนหนึ่ง และจัดทำรายงานกลับไปยังหน่วยงานว่าหน่วยงานอยู่ในตำแหน่งใด โดยอ้างอิงจากการสังเกตพื้นฐานที่ได้จากทุกหน่วยงานที่มีข้อมูลอยู่ในปัจจุบัน องค์ประกอบของการเปรียบเทียบประเภทนี้ ควรรวมถึงการสร้างความตระหนักรู้และการฝึกอบรมด้านความมั่นคงปลอดภัย การเปรียบเทียบประเภทนี้ โดยปกติจะทำโดยผู้เชี่ยวชาญในเทคนิคการเปรียบเทียบซึ่งมีข้อมูลมากมายจากหลากหลายหน่วยงานในระยะเวลาค่อนข้างนาน (ห้าปีขึ้นไป)

๔.๓ การจัดการปรับปรุงเปลี่ยนแปลงเอกสาร/สื่อ เนื้อหา

ทำการปรับปรุงเนื้อหาของแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรม เพื่อให้รองรับกับเทคโนโลยีใหม่ที่นำมาใช้ และให้สอดคล้องกับข้อกำหนด ระเบียบ มาตรฐาน หรือกฎหมาย ที่อาจมีการเปลี่ยนแปลงในช่วงเวลาที่ผ่านมา

มีความจำเป็นอย่างยิ่งเพื่อให้แน่ใจได้ว่าแผนงานหรือโครงการที่เป็นไปตามโครงสร้าง จะได้รับการปรับปรุงอย่างต่อเนื่อง เมื่อมีเทคโนโลยีใหม่และประเด็นด้านความมั่นคงปลอดภัยที่เกี่ยวข้องเกิดขึ้น ความต้องการในการฝึกอบรมจะเปลี่ยนไป เมื่อมีทักษะและความสามารถใหม่ ๆ ที่จำเป็นต่อการตอบสนองการเปลี่ยนแปลงทางสถาปัตยกรรมและเทคโนโลยี การเปลี่ยนแปลงภารกิจหรือวัตถุประสงค์ของหน่วยงาน มีอิทธิพลต่อแนวคิดเกี่ยวกับการออกแบบสถานที่ฝึกอบรมและเนื้อหา

ประเด็นปัญหาที่เกิดขึ้นใหม่ เช่น การป้องกันมาตุภูมิ จะส่งผลกระทบต่อลักษณะและขอบเขตของกิจกรรมการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยที่จำเป็น เพื่อให้ผู้รับการอบรมทราบ/ให้ความรู้เกี่ยวกับการหาประโยชน์และมาตรการตอบโต้ล่าสุด กฎหมายใหม่และคำตัดสินของศาลอาจส่งผลกระทบต่อนโยบายของหน่วยงาน ซึ่งอาจส่งผลต่อการพัฒนาหรือการใช้เอกสาร/สื่อ เนื้อหาการสร้างความตระหนักรู้และการฝึกอบรม เมื่อแนวทางด้านความมั่นคงปลอดภัยเปลี่ยนแปลงหรือได้รับการปรับปรุง เอกสาร/สื่อ เนื้อหาการสร้างความตระหนักรู้และการฝึกอบรมควรสะท้อนถึงการเปลี่ยนแปลงเหล่านี้ด้วย

๔.๔ การปรับปรุงอย่างต่อเนื่อง (“การยกระดับขอบเขตการพัฒนาทักษะ”)

ขั้นตอนนี้มุ่งเน้นไปที่การสร้างระดับการรับรู้ด้านความมั่นคงปลอดภัยและความเป็นเลิศที่บรรลุการรักษาความมั่นคงปลอดภัยในหลายหน่วยงาน กระบวนการที่สร้างความตระหนักรู้ การฝึกอบรม และการศึกษาแก่พนักงาน ควรรวมทั้งหมดเข้ากับกลยุทธ์ทางธุรกิจ แผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์ ที่ครบกำหนดจะมีการกำหนดระดับตัวชี้วัดพื้นฐานควรมีการนำระบบอัตโนมัติมาใช้เพื่อรองรับการบันทึกข้อมูลเชิงปริมาณและการจัดส่งข้อมูลการดำเนินการไปยังฝ่ายที่รับผิดชอบเป็นประจำตามรอบที่กำหนด มีการกำหนดรอบการติดตามผลและขั้นตอนการแก้ไขมีการกำหนดอย่างชัดเจนและเรียบง่าย

ในขั้นตอนนี้ หน่วยงานต่าง ๆ ได้รวมกลไกของแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรมเข้ากับการวิจัยด้านความก้าวหน้าทางเทคโนโลยี แนวปฏิบัติที่ดี และโอกาสในการเปรียบเทียบ

๔.๕ สรุปความสำเร็จของแผนงานหรือโครงการจากตัวบ่งชี้

ทำการสรุปผลความสำเร็จของแผนงานหรือโครงการตามตัวบ่งชี้ที่กำหนดขึ้นมาเพื่อให้ทั่วทั้งหน่วยงานรับทราบระดับความสำเร็จของแผนงานหรือโครงการ เนื้อหาควรมีเรื่องเหล่านี้ งบประมาณและทรัพยากร บทบาทและหน้าที่ของคนในหน่วยงาน ข้อความของผู้บริหารที่ต้องการสื่อสาร ความครอบคลุมของการสร้างความตระหนักรู้และการฝึกอบรม และการสรุปข้อมูลด้านความมั่นคงปลอดภัยไซเบอร์ ควรจัดทำรายงานสรุปในเอกสาร/สื่อ เนื้อหาที่สามารถเผยแพร่ได้สะดวกทั้งหน่วยงาน

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง เจ้าหน้าที่แผนงานหรือโครงการและหัวหน้าแผนงานหรือโครงการ ควรเป็นผู้สนับสนุนหลักสำหรับการปรับปรุงอย่างต่อเนื่องและสนับสนุนการสร้างความตระหนักรู้ การฝึกอบรม และการศึกษาของหน่วยงาน จำเป็นอย่างยิ่งที่ทุกคนจะต้องมีความสามารถและเต็มใจที่จะปฏิบัติตามข้อกำหนดบทบาทด้านความมั่นคงปลอดภัย (Security Role) ที่ได้รับมอบหมายในหน่วยงาน การรักษาความมั่นคงปลอดภัยข้อมูลและโครงสร้างพื้นฐานของหน่วยงานเป็นความพยายามและหน้าที่ของทีม

รายการด้านล่างเป็นตัวบ่งชี้บางประการเพื่อวัดการสนับสนุนและการยอมรับของแผนงานหรือโครงการ

• งบประมาณเพียงพอที่จะดำเนินการกลยุทธ์ตามที่ได้ตกลงไว้

• การจัดตำแหน่งหน่วยงานที่เหมาะสมเพื่อให้ผู้ที่มีหน้าที่รับผิดชอบหลัก (ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง เจ้าหน้าที่แผนงานหรือโครงการ และหัวหน้าแผนงานหรือโครงการ) สามารถดำเนินการกลยุทธ์ได้อย่างมีประสิทธิภาพ

• รองรับการเผยแพร่ในวงกว้าง เช่น เว็บไซต์ อีเมล โทรทัศน์ และการประกาศรายการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์

• ข้อความจากผู้บริหาร/ระดับอาวุโสถึงพนักงานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ เช่น การประชุมพนักงาน การถ่ายทอดจากหัวหน้าหน่วยงานไปยังผู้ใช้ทุกคนตามหน่วยงาน

• การใช้การวัดผล (Metric) เช่น การระบุการลดลงของเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์หรือการละเมิด การระบุข้อแตกต่างระหว่างการสร้างความตระหนักรู้ที่มีอยู่และความครอบคลุมของการฝึกอบรมและการระบุความต้องการที่กำลังลดลง ร้อยละ (เปอร์เซ็นต์) ของผู้รับการอบรมที่ได้รับเอกสาร/สื่อเนื้อหาการสร้างความตระหนักรู้ที่เพิ่มขึ้น ร้อยละ (เปอร์เซ็นต์) ของผู้รับการฝึกอบรมที่รับผิดชอบด้านความมั่นคงปลอดภัยไซเบอร์ที่สำคัญซึ่งได้รับการฝึกอบรมอย่างเหมาะสมเพิ่มขึ้น

• ผู้จัดการหรือหัวหน้าไม่ได้ปฏิบัติตามสถานะของตนในหน่วยงานเพื่อหลีกเลี่ยงการควบคุมความมั่นคงปลอดภัยไซเบอร์

• ระดับของผู้เข้าร่วมที่จำเป็นในการประชุม/การบรรยายสรุปด้านความมั่นคงปลอดภัยไซเบอร์

• การยอมรับผลงานด้านความมั่นคงปลอดภัยไซเบอร์ เช่น การให้รางวัลการแข่งขัน

• แรงจูงใจที่แสดงให้เห็นโดยผู้ที่มีบทบาทสำคัญในการจัดการ/ประสานงานแผนงานหรือโครงการด้านความมั่นคงปลอดภัยไซเบอร์

๔.๖ การพัฒนาสู่ความเป็นผู้เชี่ยวชาญ (Professional Development)

การพัฒนาสู่ความเชี่ยวชาญ เป็นความตั้งใจที่จะทำให้แน่ใจว่าพนักงานหรือบุคลากรของหน่วยงานจากพนักงานทั่วไปจนถึงระดับเชี่ยวชาญ มีความรู้ความสามารถเหมาะสมกับบทบาทและหน้าที่ของตน การพัฒนาสู่ความเป็นผู้เชี่ยวชาญ จะวัดจากทักษะผ่านทางใบรับรอง (Certification) ดังนั้น การพัฒนาตนเองและได้รับใบรับรอง จะสามารถยืนยันได้ว่าเป็นผู้เชี่ยวชาญ การเตรียมเพื่อขอทดสอบใบรับรองดังกล่าว โดยปกติจะรวมถึงการเรียนตามหลักสูตรที่กำหนดหรือเนื้อหาทางเทคนิค อาจรวมถึงการฝึกประสบการณ์จากการทำงานจริง การพัฒนาสู่ความเป็นผู้เชี่ยวชาญไม่ได้ระบุแค่สายงานด้านเทคโนโลยีสารสนเทศหรือความมั่นคงปลอดภัยไซเบอร์เท่านั้น แต่อาจรวมถึง พนักงานด้านความมั่นคงปลอดภัยไซเบอร์ ผู้ตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ ผู้ดูแลระบบ หรืออื่น ๆ ที่เกี่ยวข้อง

ใบรับรอง สามารถแบ่งออกได้เป็น ๒ ประเภท คือ ๑) ใบรับรองประเภททั่วไป และ ๒) ใบรับรองทางเทคนิค โดยใบรับรองประเภททั่วไปจะมุ่งเน้นไปที่การสร้างพื้นฐานความรู้ในหลาย ๆ ด้านเกี่ยวกับวิชาชีพด้านความมั่นคงปลอดภัยไซเบอร์ ส่วนใบรับรองทางเทคนิคนั้น เป็นประเด็นเกี่ยวกับหลักการด้านความมั่นคงปลอดภัยทางเทคนิคที่เกี่ยวข้องกับแพลตฟอร์มเฉพาะ ระบบปฏิบัติการ ผลิตภัณฑ์ของผู้จัดจำหน่าย และอื่น ๆ

บางหน่วยงาน จะมุ่งเน้นความเชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์ด้วยใบรับรอง โดยใช้เป็นส่วนหนึ่งในการรับสมัครบุคคลเข้าทำงาน บางหน่วยงานเสนอการขึ้นเงินเดือน ค่าประสบการณ์ และโบนัสเพิ่มเติมสำหรับพนักงานที่มีใบรับรอง และสนับสนุนให้พนักงานในสายงานด้านความมั่นคงปลอดภัยไซเบอร์ขอใบรับรอง

๔.๗ การศึกษาและประสบการณ์ (Education and Experience)

ระดับของการศึกษาของการเรียนรู้อย่างต่อเนื่องทางด้านความมั่นคงปลอดภัยไซเบอร์ จะบอกถึงการเพิ่มเติมความรู้ใหม่ สองกรณี คือ

(๑) ทักษะความรู้ในปัจจุบัน

(๒) ทักษะความรู้ด้านเทคโนโลยีสารสนเทศหรือความมั่นคงปลอดภัยไซเบอร์

ระดับผู้เชี่ยวชาญที่คาดหวังที่จะสร้างหรือพัฒนาให้เกิดเป็นองค์ความรู้หรือทักษะนั้น เมื่อเข้ามาทำงานด้านเทคโนโลยีสารสนเทศหรือความมั่นคงปลอดภัยไซเบอร์ จะมีความรู้พื้นฐานทั่วไปที่จำเป็นต่อลักษณะงานที่ตนทำ ประเด็นการศึกษาจะไม่ได้พูดถึงประเด็นการเรียนรู้อย่างต่อเนื่องเพียงอย่างเดียว แต่จะหมายถึงการเพิ่มความสามารถด้านเทคโนโลยีสารสนเทศหรือความมั่นคงปลอดภัยไซเบอร์ โดยมุ่งเน้นการศึกษาที่จะเพิ่มเติมการเรียนรู้หรือประสบการณ์ การศึกษาในทางอุตสาหกรรมรวมถึงการได้มาซึ่งใบรับรองของโครงการหรือหลักสูตรที่สนับสนุนโดยสถาบันการศึกษาระดับสูงการผ่านกระบวนการศึกษา ในสาขาที่มีความต้องการ ซึ่งการศึกษาเพื่อพัฒนาความเชี่ยวชาญนั้น รวมถึงการฝึกอบรม การศึกษาและประสบการณ์ที่สร้างขึ้นจากกระบวนการวัดผลความรู้และทักษะ โดยผ่านใบรับรองผลลัพธ์ที่กำหนดขึ้นในแต่ละระดับ ทั้งนี้ ตัวอย่างของการศึกษาที่จะนำไปสู่การเป็นผู้เชี่ยวชาญ คือ การศึกษาระดับปริญญา หรือการสอบใบรับรอง

ผนวก ก
ตัวอย่างทักษะและความรู้ของบุคลากร

ตำแหน่ง : ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง **(CHIEF INFORMATION OFFICER: CIO)**	
คำอธิบาย บทบาท	ผู้ที่ทำหน้าที่จัดการโครงสร้างพื้นฐาน งบประมาณ การวางแผน การรายงานการดำเนินการด้านความมั่นคงปลอดภัยไซเบอร์ และดูแลบุคลากรซึ่งมีความสำคัญต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ ทำงานร่วมกับหัวหน้าแผนงานหรือโครงการด้านความมั่นคงปลอดภัยไซเบอร์ และหัวหน้าส่วนงาน
ด้านความรู้	๑. มีความรู้เกี่ยวกับการดำเนินธุรกิจของหน่วยงาน ๒. มีความรู้เกี่ยวกับนโยบาย ขั้นตอน และมาตรฐานความมั่นคงปลอดภัยไซเบอร์ รวมถึงเข้าใจบทบาทในการจัดการการเปลี่ยนแปลงด้านความมั่นคงปลอดภัยไซเบอร์ ๓. มีความรู้เกี่ยวกับการพัฒนาและบำรุงรักษาโครงสร้างพื้นฐานสารสนเทศเพื่อสนับสนุนและปรับปรุงผลิตภัณฑ์ บริการ และการดำเนินการ รวมถึงการวางแผน การรายงาน และการดำเนินกิจกรรมต่าง ๆ ๔. มีความรู้เกี่ยวกับการวางแผนเชิงกลยุทธ์ด้านความมั่นคงปลอดภัยไซเบอร์ รวมถึงการจัดสรรงบประมาณและการวางแผนทรัพยากรบุคคล ระบบสารสนเทศ และการเพิ่มประสิทธิภาพกระบวนการ ๕. มีความรู้เกี่ยวกับแนวคิดการประเมินและปรับปรุงกระบวนการในการสร้างความตระหนักรู้และการพัฒนาทักษะ ความรู้ความสามารถของบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ ๖. มีความรู้เกี่ยวกับการสื่อสารและการเจรจาต่อรอง ภาวะผู้นำและการนำทีม
ด้านทักษะ	๑. สามารถจัดทำแผนและกำหนดกลยุทธ์โดยรวมสำหรับแผนงานหรือโครงการด้านความมั่นคงปลอดภัยไซเบอร์ ๒. สามารถประชาสัมพันธ์นโยบาย แนวคิดและกลยุทธ์ของแผนงานหรือโครงการด้านความมั่นคงปลอดภัยไซเบอร์ของหัวหน้าหน่วยงาน เจ้าของระบบ เจ้าของข้อมูล และบุคลากรอื่นของหน่วยงาน รวมถึงประเมินความเข้าใจนโยบาย แนวคิด และกลยุทธ์ดังกล่าว เพื่อปรับปรุงแนวทางประชาสัมพันธ์ ๓. รับทราบและประเมินความก้าวหน้าของการดำเนินแผนงานหรือโครงการด้านความมั่นคงปลอดภัยไซเบอร์ และเสนอรายงานความก้าวหน้าของแผนงานหรือโครงการต่อหัวหน้าหน่วยงาน ๔. สามารถกำหนดแหล่งเงินทุนและดำเนินการให้มีการสนับสนุนงบประมาณสำหรับแผนงานหรือโครงการด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานอย่างเพียงพอ ๕. สามารถตรวจสอบ ประเมินและจัดให้มีการฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์อย่างเพียงพอต่อการปฏิบัติงานที่อยู่ในความรับผิดชอบของผู้ใช้แต่ละคน ๖. ดำเนินการให้มีกลไกการติดตาม การพัฒนาและการดำเนินการตามนโยบายและมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ และกลไกการรายงานผลที่มีประสิทธิภาพ ๗. มีความเป็นผู้นำและสามารถกระตุ้นทีม และสามารถไกล่เกลี่ยความขัดแย้ง ๘. สามารถติดตามความก้าวหน้าทางเทคโนโลยีและนวัตกรรมด้านความมั่นคงปลอดภัยไซเบอร์

ตำแหน่ง : ผู้บริหารระดับสูงที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (CHIEF INFORMATION SECURITY OFFICER: CISO)	
คำอธิบาย บทบาท	ผู้ที่เข้าใจในระบบธุรกิจขององค์กรและการจัดการกับความเสี่ยงที่มีโอกาสเกิดขึ้น ทำหน้าที่จัดการเกี่ยวกับผลกระทบของความมั่นคงปลอดภัยไซเบอร์ต่อองค์กร แผนงาน หรือโครงการเฉพาะ หรือขอบเขตความรับผิดชอบอื่น รวมถึงการกำหนดเป้าหมายกลยุทธ์ นโยบายด้านการรักษาความมั่นคงปลอดภัยที่สอดคล้องกับแผนยุทธศาสตร์ขององค์กร พัฒนานโยบายด้านการรักษาความปลอดภัยของข้อมูล มาตรฐาน ขั้นตอนและแนวปฏิบัติ การบริหารทรัพยากรบุคคล โครงสร้างพื้นฐาน การบังคับใช้นโยบาย การวางแผนรองรับสถานการณ์ฉุกเฉิน การสร้างความตระหนักรู้ และทรัพยากรอื่น
ด้านความรู้	๑. มีความรู้และประสบการณ์เกี่ยวกับการจัดการธุรกิจ การจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ เทคโนโลยีด้านความมั่นคงปลอดภัยไซเบอร์ การกำหนดกลยุทธ์ การประกันสารสนเทศ ๒. มีความรู้เกี่ยวกับระบบปฏิบัติการ การออกแบบโครงสร้างพื้นฐานสารสนเทศ การจัดการระบบสารสนเทศและเครือข่าย การกำหนดสิทธิ์การเข้าถึง ข้อกำหนดของระบบเฉพาะที่อาจเป็นโครงสร้างสร้างพื้นฐานสารสนเทศสำคัญที่อาจไม่ใช้เทคโนโลยีสารสนเทศมาตรฐาน ๓. มีความรู้เกี่ยวกับการจัดการระบบ มาตรฐานซอฟต์แวร์ นโยบายและการได้รับอนุญาตเกี่ยวกับการออกแบบระบบ การจัดการวงรอบของระบบ (การใช้งานและความมั่นคงปลอดภัยไซเบอร์) ข้อกำหนดของระบบเฉพาะที่อาจเป็นโครงสร้างระบบ ๔. มีความรู้เกี่ยวกับหลักการและเครื่องมือในการสำรองข้อมูล ชนิดของการสำรองข้อมูล การกู้คืน และความต่อเนื่องของการดำเนินการ ๕. มีความรู้เกี่ยวกับภัยคุกคาม ช่องโหว่ การโจมตีระบบและแอปพลิเคชัน ขั้นตอนการรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์ การทดสอบระบบ ๖. มีความรู้เกี่ยวกับกฎหมาย ข้อบังคับ การกำกับดูแล นโยบาย ขั้นตอน มาตรฐาน และจริยธรรมที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ ๗. มีความรู้เกี่ยวกับมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ ตัวอย่างเช่น NIST, ISO, SANS, COBIT, CERT ๘. มีความรู้เกี่ยวกับข้อมูล มาตรฐานความมั่นคงปลอดภัยข้อมูล การจำแนกประเภทข้อมูล และขั้นตอนการบุกรุกสารสนเทศ

ตำแหน่ง : ผู้บริหารระดับสูงที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (CHIEF INFORMATION SECURITY OFFICER: CISO)	
ด้านทักษะ	๑. สามารถกำหนดกลวิธีและสร้างข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ ๒. สามารถขับเคลื่อนการดำเนินการด้านความมั่นคงปลอดภัยไซเบอร์ที่พัฒนาขึ้นนั้นเหมาะสมและเป็นปัจจุบันต่อกลุ่มเป้าหมาย หรือสามารถปรับเปลี่ยนตามเงื่อนไขกระบวนการ หรือสภาพแวดล้อมที่ส่งผลกระทบต่อผลลัพธ์ ๓. สามารถกำกับและติดตามการเข้าถึงและการใช้งานระบบสารสนเทศเพื่อการสร้างความตระหนักรู้ และการฝึกอบรม ของกลุ่มเป้าหมายอย่างมีประสิทธิภาพ ๔. สามารถกำหนดวิธีการสำหรับการรับข้อเสนอแนะเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์และวิธีการนำเสนอจากผู้ใช้งานและหัวหน้าส่วนงาน ๕. สามารถกำหนดมาตรการ หรือตัวชี้วัดประสิทธิภาพของระบบและความพร้อมใช้งานที่ส่งผลต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ ๖. สามารถขับเคลื่อนการดำเนินการทบทวนแผนงานหรือโครงการด้านความมั่นคงปลอดภัยไซเบอร์เป็นระยะ ๆ เพื่อปรับปรุง เมื่อมีความจำเป็นหรือมีการเปลี่ยนแปลงความเสี่ยงสูงขึ้น ๗. สามารถสนับสนุนการดำเนินการของผู้บริหารเทคโนโลยีสารสนเทศระดับสูงในการสร้างกลยุทธ์การติดตามและการรายงานผลการดำเนินการ ๘. สามารถไกล่เกลี่ยลดความขัดแย้งในการดำเนินการและกิจกรรมด้านความมั่นคงปลอดภัยไซเบอร์ ๙. สามารถประเมิน หรือรับรองความน่าเชื่อถือของบุคคลหรือองค์กรที่ทำหน้าที่จัดหาผลิตภัณฑ์หรือบริการ

ตำแหน่ง : ผู้บริหารที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (HEAD OF INFORMATION SECURITY)	
คำอธิบาย บทบาท	ผู้ที่มีความรู้หรือประสบการณ์ด้านเทคโนโลยีสารสนเทศ การบริหารความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการรับมือกับภัยคุกคามทางไซเบอร์ สามารถสื่อสาร ประสานงาน บูรณาการ และรับผิดชอบต่อความสำเร็จโดยรวมของแผนงานหรือโครงการด้านความมั่นคงปลอดภัยไซเบอร์ และตรวจสอบว่าแผนงานหรือโครงงานได้สอดคล้องต่อลำดับความสำคัญของหน่วยงาน
ด้านความรู้	๑. มีความรู้เกี่ยวกับกระบวนการทางธุรกิจ การจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ เทคโนโลยีด้านความมั่นคงปลอดภัยไซเบอร์ การกำหนดกลยุทธ์การประกันสารสนเทศ ๒. มีความรู้เกี่ยวกับระบบปฏิบัติการ การออกแบบโครงสร้างพื้นฐานสารสนเทศ การจัดการระบบสารสนเทศและเครือข่าย การกำหนดสิทธิ์การเข้าถึง ข้อกำหนดของระบบเฉพาะที่อาจเป็นโครงสร้างสร้างพื้นฐานสารสนเทศสำคัญที่อาจไม่ใช้เทคโนโลยีสารสนเทศมาตรฐาน ๓. มีความรู้เกี่ยวกับการจัดการระบบ มาตรฐานซอฟต์แวร์ นโยบายและการได้รับอนุญาตเกี่ยวกับการออกแบบระบบ การจัดการวงจรชีวิตของระบบ (การใช้งานและความมั่นคงปลอดภัยไซเบอร์) ผลกระทบต่อการดำเนินการเมื่อความมั่นปลอดภัยไซเบอร์ถูกระงับข้อกำหนดของระบบเฉพาะที่อาจเป็นโครงสร้างพื้นฐาน ๔. มีความรู้เกี่ยวกับหลักการและเครื่องมือในการสำรองข้อมูล ชนิดของการสำรองข้อมูล การกู้คืน และความต่อเนื่องของการดำเนินการ ๕. มีความรู้เกี่ยวกับภัยคุกคาม ช่องโหว่ การโจมตีระบบและแอปพลิเคชัน ขั้นตอนการรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์ การทดสอบระบบ ๖. มีความรู้เกี่ยวกับกฎหมาย ข้อบังคับ การกำกับดูแล นโยบาย ขั้นตอน มาตรฐานและจริยธรรมที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ ๗. มีความรู้เกี่ยวกับมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ ตัวอย่างเช่น NIST, ISO, SANS, COBIT, CERT ๘. มีความรู้เกี่ยวกับข้อมูล ข้อมูลส่วนบุคคล มาตรฐานความมั่นคงปลอดภัยข้อมูล การจำแนกประเภทข้อมูล และขั้นตอนการบุกรุกสารสนเทศ
ด้านทักษะ	๑. สามารถกำหนดกลวิธีและสร้างข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ที่สะท้อนต่อวัตถุประสงค์ ๒. สามารถขับเคลื่อนการดำเนินการด้านความมั่นคงปลอดภัยไซเบอร์ที่พัฒนาขึ้นนั้นให้เหมาะสมและเป็นปัจจุบันต่อกลุ่มเป้าหมาย หรือสามารถปรับเปลี่ยนตามเงื่อนไขกระบวนการ หรือสภาพแวดล้อมที่ส่งผลกระทบต่อผลลัพธ์ ๓. สามารถกำกับและติดตามการเข้าถึงและการใช้งานระบบสารสนเทศเพื่อการสร้างความตระหนักรู้และการฝึกอบรมของกลุ่มเป้าหมายอย่างมีประสิทธิภาพ ๔. สามารถกำหนดวิธีการสำหรับการรับข้อเสนอแนะเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์และวิธีการนำเสนอจากผู้ใช้งานและหัวหน้าส่วนงาน

ตำแหน่ง : ผู้บริหารที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (HEAD OF INFORMATION SECURITY)	
ด้านทักษะ	๕. สามารถกำหนดมาตรการ หรือตัวชี้วัดประสิทธิภาพของระบบและความพร้อมใช้งาน ที่ส่งผลต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ ๖. สามารถขับเคลื่อนการดำเนินการทบทวนแผนงานหรือโครงการด้านความมั่นคงปลอดภัยไซเบอร์เป็นระยะ ๆ เพื่อปรับปรุง เมื่อมีความจำเป็นหรือมีการเปลี่ยนแปลงความเสี่ยงสูงขึ้น ๗. สามารถสนับสนุนการดำเนินการของผู้บริหารเทคโนโลยีสารสนเทศระดับสูงในการสร้างกลยุทธ์การติดตามและการรายงานผลการดำเนินการ ๘. สามารถไกล่เกลี่ยลดความขัดแย้งในการดำเนินการและกิจกรรมด้านความมั่นคงปลอดภัยไซเบอร์ ๙. สามารถประเมิน หรือรับรองความน่าเชื่อถือของบุคคลหรือองค์กรที่ทำหน้าที่จัดหาผลิตภัณฑ์หรือบริการ

ตำแหน่ง : หัวหน้าส่วนงาน (MANAGER)	
คำอธิบาย บทบาท	ทำหน้าที่รับผิดชอบ กำกับและติดตามการดำเนินการด้านการสร้างความตระหนักรู้และการฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์ให้แก่บุคลากรของส่วนงานให้เป็นไปตามนโยบายด้านไซเบอร์ขององค์กร
ด้านความรู้	๑. มีความรู้เกี่ยวกับหลักการและเทคนิคในการจัดการทรัพยากรของหน่วยงาน ๒. มีความรู้เกี่ยวกับนโยบายความมั่นคงปลอดภัยไซเบอร์ขององค์กร การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ และการกำหนดวัตถุประสงค์และเป้าหมายของการฝึกอบรม ๓. มีความรู้เกี่ยวกับการแปลความหมาย การติดตาม และการจัดลำดับความสำคัญของความต้องการด้านความมั่นคงปลอดภัยไซเบอร์ และการรวบรวมความต้องการทั้งหน่วยงาน ๔. มีความรู้เกี่ยวกับการดำเนินการและภารกิจของหน่วยงาน ๕. มีความรู้เกี่ยวกับฟังก์ชันการทำงาน คุณภาพ และข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์และวิธีการนำไปใช้เสริมกับองค์ประกอบหรือกระบวนการทำงาน ๖. มีความรู้เกี่ยวกับแนวคิดการปรับปรุงกระบวนการในการสร้างความตระหนักรู้และการพัฒนาทักษะความรู้ความสามารถของบุคลากร ๗. มีความรู้เกี่ยวกับความต้องการในการจัดหา หรือการจัดหาเทคโนโลยีสารสนเทศ ๘. มีความรู้เกี่ยวกับประบวนการในการจัดซื้อจัดจ้าง
ด้านทักษะ	๑. สามารถทำงานร่วมกับผู้บริหารเทคโนโลยีสารสนเทศระดับสูง และหัวหน้าแผนงานหรือโครงการด้านความมั่นคงปลอดภัยไซเบอร์ ๒. สามารถกำกับการดำเนินงานตามแผนงานหรือนโยบายด้านไซเบอร์ขององค์กร ๓. สามารถจัดทำแผนพัฒนาส่วนบุคคล (Individual Development Plan : IDP) สำหรับผู้ใช้งานในบทบาทที่มีความรับผิดชอบสูงด้านความมั่นคงปลอดภัยไซเบอร์ ๔. สามารถกำกับและติดตามความตระหนักรู้และทักษะของผู้ใช้งานระบบทั้งหมด (ทั้งนี้อาจรวมถึงหน่วยงานภายนอกที่ทำหน้าที่ดูแลระบบ) ทั้งระบบสนับสนุนทั่วไปและระบบงานหลัก และได้รับการฝึกอบรมเกี่ยวกับวิธีการปฏิบัติตามความรับผิดชอบด้านความมั่นคงปลอดภัยไซเบอร์อย่างเหมาะสมก่อนที่จะอนุญาตให้เข้าถึงระบบ ๕. สามารถกำกับและติดตามความเข้าใจข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ของแต่ละระบบสารสนเทศที่ผู้ใช้งาน (อาจรวมถึงหน่วยงานภายนอกที่ทำหน้าที่ดูแลระบบ) ต้องใช้งาน ๖. สามารถกำกับและติดตามการพัฒนาและปรับปรุงการประมาณการค่าใช้จ่าย ๗. สามารถประเมิน หรือรับรองความน่าเชื่อถือของบุคคลหรือองค์กรที่ทำหน้าที่จัดหาผลิตภัณฑ์หรือบริการ ๘. สามารถตรวจสอบการปฏิบัติตามแนวทางปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์ให้เป็นไปตามกระบวนการที่กำหนด

ตำแหน่ง : ผู้ปฏิบัติงานด้านความมั่นคงปลอดภัยสารสนเทศ (INFORMATION SECURITY OFFICER)	
คำอธิบาย บทบาท	ผู้ทำหน้าที่ดำเนินการด้านความมั่นคงปลอดภัยไซเบอร์ในการรวบรวม ประมวลผล และ/หรือระบุตำแหน่งทางภูมิศาสตร์ของระบบ เพื่อใช้ประโยชน์ในการค้นหา และ/หรือติดตามเป้าหมายที่สนใจ ดำเนินการติดตามระบบเครือข่าย วิเคราะห์ทางยุทธวิธีทางนิติวิทยาศาสตร์ และเมื่อได้รับคำสั่งให้ดำเนินการบนเครือข่าย
ด้านความรู้	๑. มีความรู้เกี่ยวกับอัลกอริทึมการเข้ารหัส ความสามารถในการเข้ารหัส ข้อจำกัด และการมีส่วนร่วมในการปฏิบัติการทางไซเบอร์ ๒. มีความรู้เกี่ยวกับเครือข่ายทั่วไปและโปรโตคอลกำหนดเส้นทาง การบริการ และวิธีการสื่อสารเครือข่าย อุปกรณ์เครือข่ายทางกายภาพและทางตรรกะ ๓. มีความรู้เกี่ยวกับโครงสร้าง แนวทาง และกลยุทธ์ของเครื่องมือเจาะระบบ และเทคนิคการเจาะระบบ ๔. มีความรู้เกี่ยวกับพื้นฐานการพัฒนาซอฟต์แวร์และช่องโหว่ ซอฟต์แวร์ไม่พึงประสงค์ ๕. มีความรู้เกี่ยวกับผลิตภัณฑ์ความมั่นคงปลอดภัยบนโฮสต์และผลกระทบต่อการถูกโจมตีและช่องโหว่ ๖. มีความรู้เกี่ยวกับกระบวนการและเทคนิคที่ใช้ในการตรวจจับกิจกรรมการโจมตี กลยุทธ์ และเทคนิคการหลบเลี่ยง ๗. มีความรู้เกี่ยวกับขั้นตอนพื้นฐานการสำรองข้อมูลและการกู้คืน รวมถึงความแตกต่างของชนิดการสำรองข้อมูล (การสำรองข้อมูลแบบเต็ม/ปกติ การสำรองข้อมูลส่วนต่าง และการสำรองข้อมูลส่วนเพิ่มเติม) ๘. มีความรู้เกี่ยวกับตัวเลือกด้านฮาร์ดแวร์และซอฟต์แวร์การรักษาความมั่นคงปลอดภัยไซเบอร์ สิ่งประดิษฐ์ด้านระบบเครือข่ายที่มีผลต่อการโจมตี และผลกระทบด้านความมั่นคงปลอดภัยของการกำหนดค่าซอฟต์แวร์ ๙. มีความรู้เกี่ยวกับพื้นฐานเครือข่ายไร้สาย ช่องโหว่เครือข่ายไร้สายแบบต่างอัลกอริทึมการเข้ารหัสของเครือข่ายไร้สาย ๑๐. มีความรู้เกี่ยวกับการตรวจสอบและขั้นตอนการบันทึกเหตุการณ์ เพื่อนำมาวิเคราะห์การโจมตีหรือช่องโหว่ ๑๑. ความรู้พื้นฐานทางนิติวิทยาศาสตร์ดิจิทัล โครงสร้างระบบปฏิบัติการและการปฏิบัติเพื่อดึงข้อมูลมาดำเนินการทางนิติวิทยาศาสตร์
ด้านทักษะ	๑. สามารถวิเคราะห์เพื่อสกัดข้อมูลจากการถ่ายโอนข้อมูลหน่วยความจำ ๒. สามารถระบุการทำงานของอุปกรณ์ในแต่ละระดับของรูปแบบโปรโตคอล ๓. สามารถวิเคราะห์เป้าหมายการสื่อสารทั้งภายในและภายนอกที่รวบรวมจากเครือข่ายไร้สาย ๔. สามารถตรวจสอบการทำงานของระบบและการสนองต่อเหตุการณ์เพื่อตอบสนองการกระตุ้น การสังเกตแนวโน้ม หรือกิจกรรมที่ผิดปกติ ๕. สามารถดำเนินการกลวิธี เทคนิค และขั้นตอนการรวบรวมข้อมูลเครือข่าย เครือข่ายไร้สาย รวมถึงความสามารถในการถอดรหัส/เครื่องมือ ๖. สามารถใช้เครื่องมือ เทคนิค และขั้นตอนเพื่อใช้ประโยชน์จากการโจมตีจากระยะไกลและการระบุเป้าหมายได้

ตำแหน่ง : ผู้ปฏิบัติงานด้านความมั่นคงปลอดภัยสารสนเทศ **(INFORMATION SECURITY OFFICER)**	
ด้านทักษะ	๗. สามารถสกัดข้อมูลจากการจับข้อมูลเครือข่าย เพื่อวิเคราะห์การโจมตีหรือช่องโหว่ ๘. สามารถใช้พื้นฐานทางนิติวิทยาศาสตร์ดิจิทัลในการเก็บรักษาหลักฐาน และปฏิบัติเกี่ยวกับการตรวจสอบการโจมตีและช่องโหว่ ๙. สามารถเก็บรวบรวมข้อมูลกิจกรรมบนระบบเครือข่ายและเครือข่ายไร้สาย

ตำแหน่ง : ผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (INFORMATION TECHNOLOGY OFFICER)	
คำอธิบายบทบาท	ผู้ทำหน้าที่เป็นผู้ดูแลระบบ ติดตั้ง กำหนดค่า แก้ไขปัญหา บำรุงรักษาฮาร์ดแวร์และซอฟต์แวร์ และจัดการบัญชีผู้ใช้ระบบ
ด้านความรู้	๑. มีความรู้เกี่ยวกับหลักการด้านระบบเครือข่ายคอมพิวเตอร์ โปรโตคอล สถาปัตยกรรม และวิธีการรักษาความมั่นคงปลอดภัยเครือข่าย รวมถึงหลักการจัดการบริการบนเครือข่ายที่เกี่ยวข้องกับมาตรฐาน ๒. มีความรู้เกี่ยวหลักการของผู้ดูแลระบบ พื้นฐานการดูแลระบบ ระบบเครือข่าย และเทคนิคการสร้างความแข็งแกร่งระบบปฏิบัติการและเครื่องแม่ข่าย เครื่องมือและเทคนิคการปรับแต่งประสิทธิภาพ ระบบแฟ้มข้อมูล ประเภทและความถี่ของการบำรุงรักษาตามปกติเพื่อให้อุปกรณ์ทำงานได้อย่างถูกต้อง ๓. มีความรู้เกี่ยวกับนโยบายผู้ใช้งานด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ เช่น บัญชีผู้ใช้งาน การสร้างบัญชีผู้ใช้งาน กฎของรหัสผ่าน การควบคุมการเข้าถึง เป็นต้น ๔. มีความรู้เกี่ยวกับสถาปัตยกรรมเทคโนโลยีสารสนเทศ เทคโนโลยีการจำลองเสมือนและเครื่องเสมือน (Virtual Technology and Virtual Machine) ความมั่นคงปลอดภัยเครือข่ายเสมือน รวมถึงรูปแบบระบบเครือข่าย ๕. มีความรู้เกี่ยวกับเครื่องมือในการวิเคราะห์และเทคนิคในการระบุข้อผิดพลาดเครื่องแม่ข่าย/ระบบ ๖. มีความรู้เกี่ยวกับข้อมูล ข้อมูลส่วนบุคคล มาตรฐานความมั่นคงปลอดภัยข้อมูล การจำแนกประเภทข้อมูล และขั้นตอนการบุกรุกสารสนเทศ ๗. มีความรู้เกี่ยวกับทฤษฎี แนวคิดและวิธีการทางวิศวกรรมระบบ หลักการและวิธีการรวมส่วนประกอบของระบบ
ด้านทักษะ	๑. สามารถติดตั้ง ตั้งค่า และปรับแต่งการทำงานของซอฟต์แวร์และเครื่องแม่ข่าย และมีทักษะในการดูแลระบบปฏิบัติการ ๒. สามารถวิเคราะห์ปัญหาการเชื่อมต่อเครือข่าย และวิเคราะห์ข้อผิดพลาดจากการเชื่อมต่อ ๓. สามารถบำรุงรักษาบริการบัญชีผู้ใช้ ๔. สามารถใช้งานบนเทคโนโลยีการจำลองเสมือนและเครื่องเสมือน (Virtual Technology and Virtual Machine) ๕. สามารถตั้งค่าและใช้ซอฟต์แวร์เครื่องมือป้องกันคอมพิวเตอร์ เช่น ซอฟต์แวร์ป้องกันการบุกรุกเครือข่าย โปรแกรมป้องกันไวรัส โปรแกรมป้องกันสปายแวร์ ๖. สามารถดำเนินการวางแผน การจัดการ การบำรุงรักษาระบบและเครื่องแม่ข่าย การแก้ปัญหาทางกายภาพและทางเทคนิคที่ส่งผลต่อประสิทธิภาพระบบและเครื่องแม่ข่าย ๗. สามารถแก้ปัญหาความล้มเหลวขององค์ประกอบของระบบและกู้คืน ๘. สามารถระบุและคาดการณ์ประสิทธิภาพของระบบและเครื่องแม่ข่าย ความพร้อมใช้งาน สมรรถนะ หรือปัญหาการกำหนดค่า

ตำแหน่ง : ผู้ปฏิบัติงานด้านระบบควบคุมอุตสาหกรรมและเทคโนโลยีการปฏิบัติงาน (INDUSTRIAL CONTROL SYSTEMS AND OPERATIONAL TECHNOLOGIES OFFICER)	
คำอธิบายบทบาท	ผู้ทำหน้าที่เกี่ยวข้องกับการกำกับดูแลความปลอดภัยทางไซเบอร์ การบริหารความเสี่ยงและการปฏิบัติตาม การออกแบบและการพัฒนา การดำเนินงานและการบริหารการปกป้องและป้องกันระบบเทคโนโลยีการปฏิบัติงาน (OT) เช่น ระบบควบคุมอุตสาหกรรม (ICS) และการกำกับดูแลระบบควบคุมและเก็บข้อมูล (SCADA) สามารถแยกย่อยตามลักษณะงานได้ ดังนี้ ๑. สถาปนิกด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Architect) ๒. ผู้เชี่ยวชาญด้านโครงสร้างพื้นฐานความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Infrastructure Specialist) ๓. นักวิเคราะห์การป้องกันด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Defense Analyst) ๔. เจ้าหน้าที่ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Officer) ๕. เจ้าหน้าที่รับมือเหตุภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Responder)
ด้านความรู้	๑. มีความรู้เกี่ยวกับหลักการด้านระบบเครือข่ายคอมพิวเตอร์ ส่วนประกอบของระบบเครือข่ายโปรโตคอลสื่อสาร เทคโนโลยีระบบเครือข่ายทั้งด้านสารนเทศและด้านระบบควบคุมอุตสาหกรรมและเทคโนโลยีการปฏิบัติงาน การดำเนินการและความเหมาะสมของการกระบวนการและการความคุมด้านความมั่นคงปลอดภัยเครือข่าย ๒. มีความรู้ด้านอุปกรณ์ระบบควบคุมอุตสาหกรรมและภาษาการโปรแกรมสำหรับอุตสาหกรรม สภาพแวดล้อมและการทำงาน การควบคุมดูแลและองค์ประกอบของระบบเก็บข้อมูล ๓. มีความรู้เกี่ยวกับหลักการของความมั่นคงปลอดภัยไซเบอร์และความเป็นส่วนตัว ภัยคุกคาม ช่องโหว่ของระบบ การพิสูจน์ตัวตน การกำหนดสิทธิ์ และกระบวนการควบคุมการเข้าถึง ข้อกำหนดทางกฎหมายและข้อบังคับที่เกี่ยวข้องกับจริยธรรมและความเป็นส่วนตัว ๔. มีความรู้เกี่ยวกับภาพรวมของภัยคุกคามต่อระบบควบคุมอุตสาหกรรม ภัยคุกคามและช่องโหว่ในระบบควบคุมอุตสาหกรรมและสภาพแวดล้อม กระบวนการและเทคโนโลยีด้านความมั่นคงปลอดภัยระบบควบคุมอุตสาหกรรม ๕. มีความรู้เกี่ยวกับวิธีการตรวจจับการบุกรุกและเทคนิคในการตรวจจับการบุกรุกสำหรับระบบควบคุมอุตสาหกรรม ๖. มีความรู้ความเข้าใจเกี่ยวกับการประเมินความเสี่ยง การลดความเสี่ยง และวิธีการจัดการผลกระทบจากการปฏิบัติงานที่อาจเกิดขึ้นกับองค์กรจากการละเมิดความมั่นคงปลอดภัยไซเบอร์ ๗. มีความรู้เกี่ยวกับแนวปฏิบัติที่ดีที่สุดสำหรับการตอบสนองเหตุการณ์และการจัดการเหตุการณ์ ๘. มีความรู้เกี่ยวกับกฎระเบียบความมั่นคงปลอดภัยไซเบอร์และข้อกำหนดที่เกี่ยวข้องกับองค์กร การจัดประเภทเอกสารและข้อมูลระดับชาติและระดับองค์กร มาตรฐานการทำเครื่องหมาย นโยบายและระเบียบปฏิบัติความรู้ข้างต้นเป็นความรู้พื้นฐานสำหรับตำแหน่ง

ตำแหน่ง : ผู้ปฏิบัติงานด้านระบบควบคุมอุตสาหกรรมและเทคโนโลยีการปฏิบัติงาน (INDUSTRIAL CONTROL SYSTEMS AND OPERATIONAL TECHNOLOGIES OFFICER)	
ด้านความรู้	ผู้ปฏิบัติงานด้านระบบควบคุมอุตสาหกรรมและเทคโนโลยีการปฏิบัติงาน หน่วยงานอาจกำหนดความรู้เพิ่มเติมให้เหมาะสมกับลักษณะงานได้ เช่น - มีความรู้เกี่ยวกับการตั้งค่า ปรับแต่ง เครื่องมือสำหรับป้องกันเครื่องคอมพิวเตอร์และอุปกรณ์ระบบเครือข่าย - มีความรู้เกี่ยวกับเครื่องมือวิเคราะห์การจราจรเครือข่าย ทั้งด้านวิธีการวิเคราะห์และกระบวนการทำงาน - มีความรู้เกี่ยวกับการดูแลระบบ การจัดการเครือข่าย และวิธีการทำให้ระบบปฏิบัติการมีความรู้เกี่ยวกับต่อการโจมตีพอร์ตและบริการของระบบปฏิบัติการวินโดวส์และยูนิกซ์ - มีความรู้เกี่ยวกับแหล่งข้อมูลข่าวกรองภัยคุกคาม ความสามารถและข้อจำกัด - มีความรู้เกี่ยวกับวิธีการทดสอบและประเมินความมั่นคงปลอดภัยของระบบ - มีความรู้เกี่ยวกับระบบฝังตัวและวิธีการควบคุมความมั่นคงปลอดภัยไซเบอร์ที่สามารถนำไปใช้กับระบบเหล่านี้ได้
ด้านทักษะ	ทักษะข้างต้นเป็นทักษะพื้นฐานสำหรับตำแหน่งผู้ปฏิบัติงานด้านระบบควบคุมอุตสาหกรรมและเทคโนโลยีการปฏิบัติงาน หน่วยงานอาจกำหนดทักษะเพิ่มเติมให้เหมาะสมกับลักษณะงานได้ เช่น - สามารถสแกนช่องโหว่และระบุช่องโหว่จากผลลัพธ์ที่ดำเนินการได้ - สามารถใช้เครื่องมือ วิธีการ และเทคนิคในการออกแบบระบบที่ปลอดภัย - สามารถทำงานร่วมกับเจ้าหน้าที่ด้านความมั่นคงปลอดภัยไซเบอร์เพื่อให้คำแนะนำที่มีประสิทธิภาพในเรื่องต่างๆ ด้านความมั่นคงปลอดภัยไซเบอร์แก่ผู้นำขององค์กร - สามารถทำงานร่วมกับสถาปนิกองค์กร วิศวกรความมั่นคงปลอดภัยของระบบ เจ้าของระบบ เจ้าของการควบคุม และเจ้าหน้าที่รักษาความมั่นคงปลอดภัยของระบบเพื่อใช้การควบคุมความมั่นคงปลอดภัยในการควบคุมระบบเฉพาะ ระบบผสมผสานหรือระบบทั่วไป ในสภาพแวดล้อมด้านเทคโนโลยีสารสนเทศและด้านระบบควบคุมอุตสาหกรรมและเทคโนโลยีการปฏิบัติงาน - สามารถรวบรวมข้อมูลจากแหล่งข้อมูลความมั่นคงปลอดภัยไซเบอร์ที่หลากหลาย - สามารถทำงานร่วมกับผู้นำขององค์กรในการพัฒนากลยุทธ์การจัดการความเสี่ยงเพื่อจัดการกับความเสี่ยงที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ - สามารถทำงานร่วมกับผู้นำขององค์กรเพื่อกำหนดสถานะความเสี่ยงขององค์กรโดยพิจารณาจากความเสี่ยงโดยรวมจากการดำเนินงานและการใช้ระบบ - สามารถประเมินความเพียงพอของการออกแบบระบบรักษาความมั่นคงปลอดภัยไซเบอร์ - สามารถวิเคราะห์เครื่องมือ เทคนิค และกระบวนการที่ผู้บุกรุกใช้ในการโจมตีจากระยะไกลเพื่อแสวงหาประโยชน์และการฝังตัวเพื่อดำเนินการต่อไปกับเป้าหมาย - มีความสามารถในการทบทวนกลยุทธ์ขององค์กรหรือเอกสารทางกฎหมาย ระเบียบข้อบังคับ หรือนโยบายที่เกี่ยวข้อง เพื่อระบุประเด็นที่ต้องชี้แจงหรือดำเนินการ - สามารถประเมินศักยภาพของแหล่งข้อมูลเพื่อสร้างความน่าเชื่อถือในการสืบสวนทางไซเบอร์

ตำแหน่ง : ผู้ตรวจสอบภายใน (INTERNAL AUDITOR)	
คำอธิบาย บทบาท	ผู้ตรวจสอบภายใน เป็นผู้ดำเนินการประเมินระบบสารสนเทศ ประเมินความมั่นคงปลอดภัยไซเบอร์ หรือส่วนประกอบอื่นแต่ละรายการ เพื่อพิจารณาการปฏิบัติตามมาตรฐานที่องค์กรกำหนด และมาตรฐานที่เผยแพร่สาธารณะ
ด้านความรู้	๑. มีความรู้เกี่ยวกับหลักการด้านระบบเครือข่ายคอมพิวเตอร์ โปรโตคอล และวิธีการรักษาความมั่นคงปลอดภัยเครือข่าย รวมถึงหลักการจัดการบริการบนเครือข่ายที่เกี่ยวข้องกับมาตรฐาน ๒. มีความรู้เกี่ยวกับกระบวนการจัดการความเสี่ยง การประเมินความเสี่ยง วิธีการลดความเสี่ยง ความต้องการตามกรอบแนวคิดการจัดการความเสี่ยง ๓. มีความรู้เกี่ยวกับกฎหมาย ข้อบังคับ การกำกับดูแล นโยบาย และจริยธรรมที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ รวมถึงหลักการและวิธีการวิเคราะห์ที่เป็นมาตรฐานในอุตสาหกรรมและเป็นที่ยอมรับขององค์กร ๔. มีความรู้เกี่ยวกับหลักการด้านความมั่นคงปลอดภัยไซเบอร์ ภัยคุกคามทางไซเบอร์ และช่องโหว่ ๕. มีความรู้เกี่ยวกับหลักการและกรอบแนวคิดของสถาปัตยกรรมเทคโนโลยีสารสนเทศ หลักการของวงจรการจัดการระบบ รวมถึงความมั่นคงปลอดภัยซอฟต์แวร์ และการนำไปใช้ ๖. มีความรู้เกี่ยวกับข้อกำหนดในการจัดซื้อจัดจ้างด้านสารสนเทศ และกระบวนการของวงจรการจัดซื้อจัดจ้าง ๗. มีความรู้เกี่ยวกับการแปลความหมาย การติดตาม และการจัดลำดับความสำคัญของความต้องการด้านความมั่นคงปลอดภัยไซเบอร์ และการรวบรวมความต้องการจากทั้งหน่วยงาน ๘. มีความรู้เกี่ยวกับหลักการและเทคนิคในการจัดการทรัพยากรของหน่วยงาน
ด้านทักษะ	๑. สามารถระบุมาตรการหรือตัวชี้วัดประสิทธิภาพของระบบ และการดำเนินการที่จำเป็นในการปรับปรุงหรือแก้ไขประสิทธิภาพ ที่สัมพันธ์กับเป้าหมายของระบบ ๒. สามารถดำเนินการตรวจสอบหรือทบทวนระบบทางเทคนิค ๓. สามารถรับรองได้ว่ามีการปฏิบัติตามแนวทางปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์ตามกระบวนการที่กำหนด ๔. สามารถตรวจสอบการวางแผนและปฏิบัติงานตรวจสอบภายในที่ได้รับมอบหมายโดยสอดคล้องกับมาตรฐานที่เกี่ยวข้อง ๕. สามารถระบุและดำเนินการกับความเสี่ยงที่มีโดยเฉพาะต่อความมั่นคงปลอดภัยไซเบอร์และต่อสภาพแวดล้อมองค์กร ๖. สามารถกำหนดทิศทางเชิงกลยุทธ์ด้านความมั่นคงปลอดภัยไซเบอร์ และสื่อสารอย่างมีประสิทธิผล รักษาความสัมพันธ์ และบริหารบุคลากรและกระบวนการของการตรวจสอบภายใน

ตำแหน่ง : เจ้าหน้าที่ปฏิบัติงานด้านการกำกับดูแล ความเสี่ยง และการปฏิบัติตามข้อกำหนด (GOVERNANCE, RISK AND COMPLIANCE OFFICER)	
คำอธิบาย บทบาท	ผู้ทำหน้าที่บริหารจัดการและกำกับดูแลองค์กร ให้คำแนะนำแก่ผู้บริหารเพื่อดำเนินการให้เป็นไปตามกฎระเบียบที่เกี่ยวข้อง มีการบริหารความเสี่ยงที่เป็นระบบและตรงประเด็น สามารถจัดกระบวนการทำงานให้ปฏิบัติตามระเบียบและการควบคุมภายในอย่างเหมาะสม สามารถสื่อสารข้อมูลที่ถูกต้องเหมาะสมต่อผู้เกี่ยวข้องทุกระดับ
ด้านความรู้	๑. มีความรู้เกี่ยวกับหลักการด้านระบบเครือข่ายคอมพิวเตอร์ โปรโตคอล และวิธีการรักษาความมั่นคงปลอดภัยเครือข่าย รวมถึงหลักการจัดการบริการบนเครือข่ายที่เกี่ยวข้องกับมาตรฐาน ๒. มีความรู้เกี่ยวกับกระบวนการจัดการความเสี่ยง การประเมินความเสี่ยง วิธีการลดความเสี่ยง ความต้องการตามกรอบแนวคิดการจัดการความเสี่ยง ๓. มีความรู้เกี่ยวกับกฎหมาย ข้อบังคับ การกำกับดูแล นโยบาย และจริยธรรมที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ รวมถึงหลักการและวิธีการวิเคราะห์ที่เป็นมาตรฐานในอุตสาหกรรมและเป็นที่ยอมรับขององค์กร ๔. มีความรู้เกี่ยวกับหลักการด้านความมั่นคงปลอดภัยไซเบอร์ ภัยคุกคามและช่องโหว่ การป้องกันทางไซเบอร์ เครื่องมือประเมินช่องโหว่ เครื่องมือและเทคนิคการทดสอบการเจาะระบบ การจัดการความเสี่ยงที่เกี่ยวกับการใช้งาน กระบวนการ การเก็บข้อมูลและการสื่อสารข้อมูลหรือสารสนเทศ ๕. มีความรู้เกี่ยวกับหลักการและกรอบแนวคิดของสถาปัตยกรรมเทคโนโลยีสารสนเทศ หลักการของวงจรการจัดการระบบ รวมถึงความมั่นคงปลอดภัยซอฟต์แวร์ และการนำไปใช้ ๖. มีความรู้เกี่ยวกับข้อมูล ข้อมูลส่วนบุคคล มาตรฐานความมั่นคงปลอดภัยข้อมูล การจำแนกประเภทข้อมูล และขั้นตอนการบุกรุกสารสนเทศ ๗. มีความรู้เกี่ยวกับวิธีการทางอุตสาหกรรมในปัจจุบันสำหรับการประเมินการนำไปใช้และการเผยแพร่การประเมินความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ การตรวจสอบการตรวจจับ และเครื่องมือและขั้นตอนการแก้ไขโดยใช้แนวคิดและสมรรถนะตามมาตรฐาน ๘. มีความรู้เกี่ยวกับกระบวนการกำหนดเป้าหมาย วัตถุประสงค์ ภารกิจหลักขององค์กรด้านความมั่นคงปลอดภัยสารสนเทศ
ด้านทักษะ	๑. สามารถกำกับและติดตามการดำเนินการขององค์กร ให้เป็นไปตามกฎระเบียบที่เกี่ยวข้อง ๒. สามารถแยกแยะความต้องการในการป้องกันระบบสารสนเทศและเครือข่าย เช่น การควบคุมความมั่นคงปลอดภัยของระบบและแอปพลิเคชัน การสำรองข้อมูล การบริการบนเครือข่าย เป็นต้น ๓. สามารถใช้หลักการด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อการรักษาความลับ ความถูกต้องครบถ้วน ความพร้อมใช้งาน การพิสูจน์ตัวตน และการห้ามปฏิเสธความรับผิดชอบ ต่อการใช้งานระบบ ๔. สามารถพิจารณาว่าความมั่นคงปลอดภัยของระบบควรทำงานอย่างไร และสามารถปรับเปลี่ยนตามเงื่อนไข กระบวนการ หรือสภาพแวดล้อมที่ส่งผลกระทบต่อผลลัพธ์

ตำแหน่ง : เจ้าหน้าที่ปฏิบัติงานด้านการกำกับดูแล ความเสี่ยง และการปฏิบัติตามข้อกำหนด (GOVERNANCE, RISK AND COMPLIANCE OFFICER)	
ด้านทักษะ	๕. สามารถระบุมาตรการหรือตัวชี้วัดประสิทธิภาพของระบบและการดำเนินการที่จำเป็นในการปรับปรุงหรือแก้ไขประสิทธิภาพ ที่สัมพันธ์กับเป้าหมายของระบบ ๖. สามารถเลือกใช้เครื่องมือและเทคนิคการเจาะระบบเพื่อตรวจสอบความมั่นคงปลอดภัยไซเบอร์และระบุช่องโหว่ของระบบและสามารถระบุความเสี่ยงที่เกิดขึ้น ๗. สามารถประเมินหรือรับรองความน่าเชื่อถือของบุคคลหรือองค์กรที่ทำหน้าที่จัดหาผลิตภัณฑ์หรือบริการ ๘. สามารถแยกแยะและกำหนดปัจจัยเสี่ยงต่อระบบสารสนเทศและความมั่นคงปลอดภัยไซเบอร์ รวมถึงดัชนีชี้วัดความสำเร็จของการบริหารความเสี่ยงและการรายงานสถานะความเสี่ยง

ผนวก ข

ตัวอย่างการวัดผลการสร้างความตระหนักรู้และการฝึกอบรม

๑. คำถามหลัก (Critical Element)	บุคลากรได้รับการฝึกอบรมอย่างเพียงพอเพื่อตอบสนองความรับผิดชอบด้านความมั่นคงปลอดภัยไซเบอร์หรือไม่
๒. คำถามลำดับรอง (Subordinate Question)	มีการบันทึกและติดตามการฝึกอบรมและการพัฒนาวิชาชีพของบุคลากรหรือไม่
๓. การวัด/ค่าที่ใช้ในการวัด (Metric)	สัดส่วนของบุคลากรที่มีหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยไซเบอร์ที่ได้รับการฝึกอบรมเฉพาะทาง
๔. วัตถุประสงค์ (Purpose)	เพื่อวัดระดับความเชี่ยวชาญระหว่างหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยไซเบอร์ที่กำหนดและความรับผิดชอบด้านความมั่นคงปลอดภัยไซเบอร์สำหรับระบบสารเทศเฉพาะภายในหน่วยงาน
๕. หลักฐานการดำเนินการ (Implementation Evidence)	๑. มีการกำหนดหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยไซเบอร์ที่สำคัญพร้อมเกณฑ์คุณสมบัติและจัดทำเป็นเอกสารหรือไม่ ☐ มี ☐ ไม่มี ๒. มีการเก็บบันทึกว่าบุคลากรคนใดมีหน้าที่ความรับผิดชอบเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์เป็นพิเศษหรือไม่ ☐ มี ☐ ไม่มี ๓. มีบุคลากรที่มีหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยไซเบอร์ที่สำคัญจำนวนกี่คนในหน่วยงาน ..... ๔. มีการบันทึกการฝึกอบรมที่บ่งบอกได้ว่าการอบรมของบุคลากรตรงกับความรู้ที่บุคลากรควรได้รับหรือไม่ ☐ มี ☐ ไม่มี ๕. แผนการฝึกอบรมระบุว่าการฝึกอบรมนั้นจำเป็นต้องมีในการฝึกอบรมเฉพาะทางหรือไม่ ☐ มี ☐ ไม่มี ๖. มีบุคลากรที่มีหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยไซเบอร์ที่สำคัญเท่าใด ที่ได้รับการฝึกอบรมที่จำเป็นตามที่ระบุไว้ในแผนการฝึกอบรม ..... ๗. หากมีบุคลากรที่ไม่ได้รับการฝึกอบรม ให้ระบุเหตุผลทั้งหมดที่เกี่ยวข้อง: ☐ งบประมาณไม่เพียงพอ ☐ เวลาไม่เพียงพอ ☐ ไม่มีหลักสูตร/ไม่สามารถระบุหลักสูตรได้ ☐ บุคลากรยังไม่ได้บรรจุลงกรอบอัตราจ้าง ☐ อื่นๆ (ระบุ) .....
๖. ความถี่ (Frequency)	อย่างน้อยปีละครั้ง

๗. สูตรการคำนวน (Formula)	จำนวนบุคลากรที่มีหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยไซเบอร์ที่สำคัญที่ได้รับการฝึกอบรมที่จำเป็นตามที่ระบุไว้ในแผนการฝึกอบรม (คำถามที่ ๖) / จำนวนบุคลากรที่มีหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยไซเบอร์ที่สำคัญในหน่วยงาน (คำถามที่ ๓)
๘. แหล่งที่มาของข้อมูล (Data Source)	ฐานข้อมูลหรือบันทึกการฝึกอบรม หัวข้อข้อมูลของบุคลากรที่ได้รับใบรับรองหรือผ่านหลักสูตร
๙. ตัวชี้วัด (Indicators)	เป้าหมาย คือ ร้อยละ ๑๐๐ (๑๐๐%) หากไม่ครบ หน่วยงานอาจไม่มีความพร้อมในการต่อสู้กับภัยคุกคามทางไซเบอร์และช่องโหว่ล่าสุด เพราะข้อกำหนดและเครื่องมือสำหรับควบคุมความมั่นคงปลอดภัยไซเบอร์เฉพาะมีการเปลี่ยนแปลงและพัฒนาอย่างรวดเร็ว การฝึกอบรมอย่างต่อเนื่องจึงมีความสำคัญต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ตัวชี้วัดนี้จะสัมพันธ์กับจำนวนเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ และจำนวนการป้องกันช่องโหว่ เพื่อพิสูจน์ว่าการเพิ่มจำนวนของการฝึกอบรมให้บุคลากรที่มีหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยไซเบอร์ที่ได้รับการฝึกอบรมเฉพาะทาง สามารถลดจำนวนเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์บางประเภท และจำนวนช่องโหว่ได้

หมายเหตุ : คำถามที่ ๑ และ ๒ ใช้เพื่อวัดความน่าเชื่อถือของข้อมูลสำหรับการวัดผลนี้ ต้องกำหนดบทบาทและความรับผิดชอบในนโยบายและระเบียบปฏิบัติ และระบุบุคลากรเพื่อดำเนินการตามบทบาท คำถามที่ ๔ และ ๕ ให้ข้อมูลเพื่อช่วยระบุการฝึกอบรมเฉพาะทางที่บุคลากรต้องการ หากไม่มีการฝึกอบรมบุคลากรอย่างเพียงพอ คำถามที่ ๗ ช่วยระบุสาเหตุของการฝึกอบรมที่ไม่เพียงพอ ฝ่ายบริหารสามารถดำเนินการเพื่อแก้ไขจากข้อบกพร่องนี้ได้

ผนวก ค

ตัวอย่างโครงร่างแผนงานหรือโครงการสร้างความตระหนักรู้และการฝึกอบรม

บทสรุปผู้บริหาร (Executive Summary)
ข้อมูลพื้นฐาน (Background) ● OMB A-130, Appendix III ● Federal Information Security Management Act (FISMA) ● นโยบายเฉพาะของแผนก/ส่วนงานหรือหน่วยงาน (ข้อมูลหรือเหตุผลที่เกี่ยวข้องอื่น ๆ ที่อาจผลักดันการสร้างความตระหนักรู้ แผนงานหรือโครงการและแผนการฝึกอบรม)
นโยบายความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน (Agency Cybersecurity Policy) ● เป้าหมาย (Goals) ● วัตถุประสงค์ (Objectives) ● บทบาท/ความรับผิดชอบ (Roles/Responsibilities)
การสร้างความตระหนักรู้ (Awareness) ● กลุ่มเป้าหมายที่เข้าร่วม (Audience; Management and All Employees) ● กิจกรรมและวันที่จัดกิจกรรม (Activities and Target Dates) ● กำหนดการ (Schedule) ● ทบทวนและปรับปรุงเอกสาร/สื่อ เนื้อหา และกระบวนการ (Review and Updating of Materials and Methods)
การฝึกอบรม/การศึกษา (Training/Education) ● **บทบาท ๑ : ผู้บริหารระดับสูง และหัวหน้าส่วนงาน (Executives and Managers)** ○ ผลลัพธ์การเรียนรู้ (Learning Objectives) ○ ประเด็นที่ให้ความสนใจ (Focus Areas) ○ วิธีการ/กิจกรรม (Methods/Activities) ○ กำหนดการ (Schedule) ○ เกณฑ์การประเมิน (Evaluation Criteria) ● **บทบาท ๒ : เจ้าหน้าที่รักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Staff)** ○ ผลลัพธ์การเรียนรู้ (Learning Objectives) ○ ประเด็นที่ให้ความสนใจ (Focus Areas) ○ วิธีการ/กิจกรรม (Methods/Activities) ○ กำหนดการ (Schedule) ○ เกณฑ์การประเมิน (Evaluation Criteria) ● **บทบาท ๓ : ผู้ดูแลระบบ/ผู้ดูแลระบบเครือข่าย (System/Network Administrators)** ○ ผลลัพธ์การเรียนรู้ (Learning Objectives) ○ ประเด็นที่ให้ความสนใจ (Focus Areas) ○ วิธีการ/กิจกรรม (Methods/Activities) ○ กำหนดการ (Schedule)

บทสรุปผู้บริหาร (Executive Summary)	
○ เกณฑ์การประเมิน (Evaluation Criteria) . . และบทบาทอื่นที่มีความสำคัญต่อความรับผิดชอบด้านความมั่นคงปลอดภัยไซเบอร์	
ใบรับรองความเป็นผู้เชี่ยวชาญ (Professional Certification) ● **บทบาท ๑ : เจ้าหน้าที่รักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Staff)** ○ ผลลัพธ์การเรียนรู้ (Learning Objectives) ○ ประเด็นที่ให้ความสนใจ (Focus Areas) ○ วิธีการ/กิจกรรม (Methods/Activities) ○ กำหนดการ (Schedule) ○ เกณฑ์การประเมิน (Evaluation Criteria) ● **บทบาท ๒ : ผู้ดูแลระบบ/ผู้ดูแลระบบเครือข่าย (System/Network Administrators)** ○ ผลลัพธ์การเรียนรู้ (Learning Objectives) ○ ประเด็นที่ให้ความสนใจ (Focus Areas) ○ วิธีการ/กิจกรรม (Methods/Activities) ○ กำหนดการ (Schedule) ○ เกณฑ์การประเมิน (Evaluation Criteria) . . และบทบาทอื่นที่มีความสำคัญต่อความรับผิดชอบด้านความมั่นคงปลอดภัยไซเบอร์	
ความต้องการด้านทรัพยากร (Resource Requirements)	**ค่าใช้จ่าย (Cost)**
● คณะทำงาน (Staffing) ● สนับสนุนการทำสัญญา (Contracting Support) ● สิ่งอำนวยความสะดวก (Facilities) เช่น ห้องฝึกอบรม ห้องประชุมทางไกล ● สื่อ (Media) เช่น เครื่องแม่ข่ายสำหรับเอกสาร/สื่อ เนื้อหาบนเว็บไซต์และคอมพิวเตอร์	xxx,xxx บาท xxx,xxx บาท xxx,xxx บาท xxx,xxx บาท



ฉบับภาษาอังกฤษ
English Version

อยู่ระหว่างดำเนินการแปลเอกสารเป็นฉบับภาษาอังกฤษ

The translation of the document into English is underway.

16

ประกาศ กกม.

เรื่อง หน้าที่ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและหน่วยงานควบคุมหรือกำกับดูแล พ.ศ. 2567

มีผลใช้บังคับตั้งแต่วันที่ 21 มิ.ย. 68 เป็นต้นไป

Notification of CRC

Re: the duties of Critical Information Infrastructure organizations and duties of Regulators B.E. 2567 (2024)

effective from June 21, 2025, onwards.



ฉบับภาษาไทย
Thai Version

ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์

เรื่อง หน้าที่ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
และหน่วยงานควบคุมหรือกำกับดูแล
พ.ศ. ๒๕๖๗

โดยที่พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดหน้าที่ให้หน่วยงานควบคุมหรือกำกับดูแล ต้องกำหนดมาตรฐานที่เหมาะสม เพื่อรับมือกับภัยคุกคามทางไซเบอร์ของแต่ละหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน่วยงานของรัฐ เพื่อให้การปฏิบัติงานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ เป็นไปอย่างเหมาะสมและมีประสิทธิภาพ

อาศัยอำนาจตามความในมาตรา ๑๓ วรรคหนึ่ง (๕) แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ประกอบกับมติที่ประชุมคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ ในคราวการประชุมครั้งที่ ๒/๒๕๖๖ เมื่อวันที่ ๑๕ ธันวาคม ๒๕๖๖ คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ ออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง หน้าที่ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและหน่วยงานควบคุมหรือกำกับดูแล พ.ศ. ๒๕๖๗”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับเมื่อพ้นกำหนดหนึ่งร้อยยี่สิบวันนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ข้อ ๓ ในประกาศนี้

“กมช.” หมายความว่า คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

“กกม.” หมายความว่า คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์

“สำนักงาน” หมายความว่า สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

“ประกาศประมวลแนวทางปฏิบัติ” หมายความว่า ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔

ข้อ ๔ ให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ มีหน้าที่ดังต่อไปนี้

(๑) ป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ตามหลักเกณฑ์ที่กำหนดในประกาศประมวลแนวทางปฏิบัติและตามมาตรฐานที่หน่วยงานควบคุมหรือกำกับดูแลกำหนดและดำเนินการตามนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ กมช. ประกาศกำหนด

(๒) จัดทำเอกสารดังต่อไปนี้ของหน่วยงานของตนให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ กมช. ประกาศกำหนด ตามหลักเกณฑ์ที่กำหนดในประกาศประมวลแนวทางปฏิบัติให้แล้วเสร็จภายในระยะเวลา ๑ ปีนับแต่วันที่ประกาศนี้มีผลใช้บังคับ

(ก) ประมวลแนวทางปฏิบัติ ประกอบด้วย แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์และแผนการรับมือภัยคุกคามทางไซเบอร์

(ข) กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ประกอบด้วยการระบุความเสี่ยงที่อาจจะเกิดขึ้น มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ และมาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์

(๓) จัดให้มีการทบทวนเพื่อปรับปรุงหรือแก้ไขเพิ่มเติมนโยบาย มาตรฐาน และประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานอย่างน้อยปีละหนึ่งครั้งหรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญต่อการปฏิบัติการเกี่ยวกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของหน่วยงาน

(๔) ให้ความร่วมมือและมีส่วนร่วมในการฝึกซ้อมรับมือกับภัยคุกคามทางไซเบอร์ รวมถึงการปฏิบัติตามคำขอใด ๆ ของ กมช. กกม. และสำนักงาน โดยให้ข้อมูลที่เกี่ยวข้องกับบริการที่สำคัญของตนเพื่อวัตถุประสงค์ในการวางแผนและดำเนินการฝึกซ้อมรับมือภัยคุกคามทางไซเบอร์

(๕) แจ้งรายชื่อเจ้าหน้าที่ระดับบริหารและระดับปฏิบัติการ พร้อมด้วยข้อมูลการติดต่อที่สามารถติดต่อได้ในกรณีมีเหตุฉุกเฉินภายในระยะเวลาหกสิบนาที เพื่อประสานงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ไปยังสำนักงาน และหน่วยงานควบคุมหรือกำกับดูแล ทั้งนี้ ในกรณีที่มีการเปลี่ยนแปลงข้อมูล ให้แจ้งรายชื่อหรือข้อมูลการติดต่อที่เปลี่ยนแปลงให้สำนักงานและหน่วยงานควบคุมหรือกำกับดูแลทราบภายในระยะเวลา ๑๕ วันนับแต่วันที่มีการเปลี่ยนแปลง

(๖) แจ้งรายชื่อหน่วยงานภายในหรือบุคคลที่เป็นเจ้าของกรรมสิทธิ์ ผู้ครอบครองคอมพิวเตอร์และผู้ดูแลระบบคอมพิวเตอร์ พร้อมด้วยข้อมูลการติดต่อที่สามารถติดต่อได้ในกรณีมีเหตุฉุกเฉินภายในระยะเวลาหกสิบนาทีไปยังสำนักงาน หน่วยงานควบคุมหรือกำกับดูแล และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยบุคคลดังกล่าวต้องเป็นบุคคล ผู้ซึ่งรับผิดชอบในการบริหารงานของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนั้น ทั้งนี้ ในกรณีที่มีการเปลี่ยนแปลงข้อมูล ให้แจ้งรายชื่อหรือข้อมูลการติดต่อที่เปลี่ยนแปลงให้สำนักงาน หน่วยงานควบคุมหรือกำกับดูแล และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ก่อนการเปลี่ยนแปลงล่วงหน้าไม่น้อยกว่า ๗ วัน เว้นแต่มีเหตุจำเป็นอันไม่อาจก้าวล่วงได้ให้แจ้งภายในระยะเวลา ๑๕ วันนับแต่วันที่มีการเปลี่ยนแปลง

การเปลี่ยนแปลงข้อมูลตามวรรคหนึ่งให้รวมถึงการดำเนินการที่มีผลเป็นการเปลี่ยนแปลงเจ้าของกรรมสิทธิ์ ผู้ครอบครองคอมพิวเตอร์ และผู้ดูแลระบบคอมพิวเตอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เช่น การเปลี่ยนแปลงหน่วยงานต้นสังกัดของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ การยุบหรือควบรวมกิจการ การเพิ่มหน่วยงานย่อยภายในหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(๗) ดำเนินการตามนโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ที่กำหนดในนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ กมช. ประกาศกำหนด โดยให้ครอบคลุมโครงสร้างองค์กรและบทบาทหน้าที่ของผู้ที่เกี่ยวข้องในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์และนำนโยบายดังกล่าว มาจัดทำระเบียบวิธีปฏิบัติและกระบวนการในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมทั้งกำหนดระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยที่ยอมรับได้ (Risk Appetite) และให้นำส่งระเบียบวิธีปฏิบัติและกระบวนการในการบริหารความเสี่ยงดังกล่าวให้หน่วยงานควบคุมหรือกำกับดูแลของตนรับทราบและให้ความเห็นชอบก่อนนำส่งสำนักงาน

(๘) จัดให้มีการทบทวนระเบียบวิธีปฏิบัติและกระบวนการในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่จัดทำขึ้นตาม (๗) อย่างน้อยปีละหนึ่งครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เช่น การเปลี่ยนแปลงของระบบความมั่นคงปลอดภัยไซเบอร์ความเสี่ยงมาตรฐานสากล อย่างมีนัยสำคัญ

(๙) จัดให้มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละหนึ่งครั้ง โดยต้องประกอบด้วยรายละเอียดตามที่กำหนดในข้อ ๑๘ องค์ประกอบที่ ๒ การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ของประกาศประมวลแนวทางปฏิบัติ และจัดทำผลสรุปรายงานการดำเนินการ แยกต่างหากจากรายงานการประเมินความเสี่ยงของหน่วยงาน และส่งผลสรุปรายงานการดำเนินการดังกล่าวต่อสำนักงานภายใน ๓๐ วันนับแต่วันที่ดำเนินการแล้วเสร็จ แต่ไม่เกินวันที่ ๓๑ มกราคมของปีถัดไป พร้อมส่งสำเนาให้หน่วยงานควบคุมหรือกำกับดูแลด้วย ทั้งนี้ ผลสรุปรายงานดังกล่าว สำนักงานต้องไม่เปิดเผยต่อหน่วยงานอื่นใด เว้นแต่เป็นกรณีที่มีกฎหมายกำหนดให้กระทำได้

(๑๐) จัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ ซึ่งเป็นบุคลากรภายในหน่วยงานของตนหรือเป็นผู้ตรวจสอบอิสระภายนอกอย่างน้อยปีละหนึ่งครั้ง และจัดส่งผลสรุปรายงานการดำเนินการต่อสำนักงานภายใน ๓๐ วันนับแต่วันที่ดำเนินการแล้วเสร็จแต่ไม่เกินวันที่ ๓๑ มกราคมของปีถัดไป พร้อมส่งสำเนาให้หน่วยงานควบคุมหรือกำกับดูแลด้วย ทั้งนี้ ขอบเขตของการตรวจสอบและกรณีที่รายงานการตรวจสอบระบุว่าการดำเนินการของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศไม่สอดคล้องกับหลักเกณฑ์

หรือมาตรฐานการปฏิบัติงาน ให้เป็นไปตามหลักเกณฑ์ที่กำหนดในข้อ ๑๗ องค์ประกอบที่ ๑ แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของประกาศประมวลแนวทางปฏิบัติ

(๑๑) กำหนดกลไก ขั้นตอนหรือกระบวนการเพื่อตรวจสอบหรือเฝ้าระวังภัยคุกคามทางไซเบอร์ หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศของตนตามมาตรฐานซึ่งกำหนดโดยหน่วยงานควบคุมหรือกำกับดูแล และตามที่กำหนดในประกาศประมวลแนวทางปฏิบัติ รวมถึงระบบมาตรการที่ใช้แก้ปัญหาเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ที่ กมช. หรือ กกม. กำหนด

(๑๒) จัดให้มีการทบทวนกลไก ขั้นตอนหรือกระบวนการตาม (๑๑) อย่างน้อยปีละหนึ่งครั้ง

(๑๓) เข้าร่วมการทดสอบสถานะความพร้อมในการรับมือกับภัยคุกคามทางไซเบอร์ที่สำนักงานจัดขึ้น

(๑๔) ตรวจสอบข้อมูลที่เกี่ยวข้อง ข้อมูลคอมพิวเตอร์ และระบบคอมพิวเตอร์ รวมถึงพฤติกรรมแวดล้อมของตน ในกรณีที่เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ต่อระบบสารสนเทศซึ่งอยู่ในความดูแลรับผิดชอบของตน เพื่อประเมินว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้นหรือไม่

(๑๕) ในกรณีที่มีภัยคุกคามทางไซเบอร์เกิดขึ้น ให้ดำเนินการต่อไปนี้

(ก) เก็บรักษาข้อมูลและพยานหลักฐานตามที่กำหนดในขั้นตอนที่ ๒ - การตรวจจับและวิเคราะห์ (Detection and Analysis) ของเอกสารแนบ ๓ แนวทางการจัดทำประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ หัวข้อแผนการรับมือภัยคุกคามทางไซเบอร์ และแนวทางการจัดทำกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ หัวข้อมาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond) ท้ายประกาศสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง แนวทางการจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

(ข) แจ้งเหตุและส่งรายงานภัยคุกคามทางไซเบอร์ไปยังสำนักงานและหน่วยงานควบคุมหรือกำกับดูแล ภายในระยะเวลาและปฏิบัติตามหลักเกณฑ์และวิธีการตามที่กำหนดในประกาศที่ออกโดยอาศัยอำนาจตามมาตรา ๕๗

(ค) ให้ความร่วมมือกับพนักงานเจ้าหน้าที่ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ในการปฏิบัติการตามมาตรา ๖๖ รวมถึงให้ความร่วมมือกับพนักงานเจ้าหน้าที่หรือเจ้าหน้าที่ที่เกี่ยวข้องในการสืบสวนสอบสวนและรวบรวมพยานหลักฐานเกี่ยวกับภัยคุกคามทางไซเบอร์

(๑๖) จัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan : BCP) ตามหลักเกณฑ์และวิธีการที่สำนักงานประกาศกำหนด เพื่อให้แน่ใจได้ว่าบริการที่สำคัญของตนยังสามารถให้บริการต่อไปได้

(๑๗) จัดให้มีการฝึกซ้อมตามแผนความต่อเนื่องทางธุรกิจตาม (๑๖) อย่างน้อยปีละหนึ่งครั้ง เพื่อประเมินประสิทธิภาพต่อภัยคุกคามทางไซเบอร์และเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

(๑๘) จัดทำรายงานประจำปี ส่งรายงานดังกล่าวให้สำนักงานและหน่วยงานควบคุมหรือกำกับดูแลภายในวันที่ ๓๑ มกราคมของปีถัดไป โดยรายงานต้องมีรายละเอียด ดังต่อไปนี้

(ก) ระบุจำนวนและลักษณะของเหตุการณ์ภัยคุกคามทางไซเบอร์ของตน ตามแบบรายงานสรุปภัยคุกคามทางไซเบอร์ในหนึ่งรอบปี ที่กำหนดท้ายประกาศที่ออกโดยอาศัยอำนาจตามมาตรา ๕๗

(ข) วิเคราะห์สาเหตุหรือผลกระทบที่เกิดขึ้นจากภัยคุกคามไซเบอร์ทางไซเบอร์ที่เกิดขึ้น

(ค) ปัญหาและอุปสรรคในการดำเนินงาน

(ง) ข้อเสนอแนะต่าง ๆ ซึ่งรวมถึงข้อเสนอแนะเชิงนโยบาย

(๑๙) ในกรณีที่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศเป็นหน่วยงานของรัฐ ให้หน่วยงานดังกล่าวร่วมมือ สนับสนุนหรือดำเนินการเพื่อให้มีศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ สำหรับบริการในด้านตามประกาศที่ออกโดยอาศัยอำนาจตามมาตรา ๔๙ หรือเมื่อยังไม่มีความพร้อมในการทำหน้าที่เป็นศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศดังกล่าวให้แจ้งเหตุขัดข้องให้หน่วยงานควบคุมหรือกำกับดูแลของตนทราบถึงเหตุผลที่ยังไม่พร้อมในการทำหน้าที่เป็นศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ทั้งนี้ ลักษณะ หน้าที่และความรับผิดชอบของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศเป็นไปตามหลักเกณฑ์ที่ กมช. ประกาศกำหนด

(๒๐) ให้ความร่วมมือหรือสนับสนุนแก่ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ในการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยเฉพาะเรื่องการติดตามการตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ ผลกระทบเกี่ยวกับภัยคุกคามทางไซเบอร์และผลการตอบสนองและรับมือเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น

(๒๑) ดำเนินการตามที่ กมช. หรือ กกม. มอบหมายหรือประกาศกำหนด หรือให้ความร่วมมือกับสำนักงานหรือหน่วยงานควบคุมหรือกำกับดูแลเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมทั้งส่งเอกสารที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ตามที่สำนักงานหรือหน่วยงานควบคุมหรือกำกับดูแลร้องขอ

ข้อ ๕ ให้หน่วยงานควบคุมหรือกำกับดูแล มีหน้าที่ดังต่อไปนี้

(๑) กำหนดมาตรฐานที่เหมาะสมในการรับมือกับภัยคุกคามทางไซเบอร์ของแต่ละหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ภายใต้การควบคุมหรือกำกับดูแลของตน โดยต้องสอดคล้องและไม่ต่ำกว่ามาตรฐานขั้นต่ำที่ กมช. ประกาศกำหนด

(๒) กำกับดูแลหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ภายใต้การควบคุมหรือกำกับดูแลของตน เฉพาะบริการที่เป็นภารกิจหรือให้บริการของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Services) ตามประกาศที่ออกโดยอาศัยอำนาจตามมาตรา ๔๙ ให้อยู่ในระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยที่ยอมรับได้ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนั้นและเป็นไปตามมาตรฐานที่เหมาะสมตาม (๑) และมาตรฐานขั้นต่ำที่ กมช. ประกาศกำหนดด้วย

(๓) ตรวจสอบการดำเนินการของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ภายใต้การควบคุมหรือกำกับดูแลของตน ให้เป็นไปตามมาตรฐานขั้นต่ำที่ กมช. ประกาศกำหนด และจัดทำรายงานสรุปผลการตรวจสอบให้แก่สำนักงานภายใน ๓๐ วัน หลังกระบวนการตรวจสอบเสร็จสิ้น ทั้งนี้ ในการดำเนินการดังกล่าว ให้หน่วยงานควบคุมหรือกำกับดูแลแต่งตั้งกลุ่มบุคคลทำหน้าที่เป็นผู้ตรวจสอบอันประกอบไปด้วยหัวหน้าทีมผู้ตรวจสอบ (Lead Auditor) และผู้ตรวจสอบ (Auditor) ที่มีความรู้ความเชี่ยวชาญด้านการตรวจสอบเรื่องความมั่นคงปลอดภัยไซเบอร์ ในกรณีที่พบว่าการดำเนินการไม่เป็นไปตามมาตรฐานขั้นต่ำที่ กมช. ประกาศกำหนด ให้หน่วยงานควบคุมหรือกำกับดูแลแจ้งหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศแก้ไขให้ได้มาตรฐาน พร้อมทั้งกำหนดเวลาให้ดำเนินการหากหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ไม่ดำเนินการภายในระยะเวลาที่กำหนด ให้หน่วยงานควบคุมหรือกำกับดูแลแจ้ง กกม. เพื่อดำเนินการตามมาตรา ๕๓ วรรคสอง ต่อไป

(๔) ให้ความช่วยเหลือ สนับสนุน หรือประสานงานในการจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ภายใต้การควบคุมหรือกำกับดูแลของตน

เมื่อมีการจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศในด้านตามประกาศที่ออกโดยอาศัยอำนาจตามมาตรา ๔๙ ด้านใดแล้ว ให้หน่วยงานควบคุมหรือกำกับดูแลแจ้งการจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศในด้านดังกล่าว พร้อมกับรายชื่อหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ภายใต้การดูแลและข้อมูลอื่น ๆ ที่เกี่ยวข้อง ให้สำนักงานทราบภายใน ๓๐ วันนับแต่วันที่จัดตั้ง

(๕) ให้ความช่วยเหลือ สนับสนุน หรือประสานงานในการประเมินความเสี่ยง ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ภายใต้การควบคุมหรือกำกับดูแลของตน

(๖) ป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ และดำเนินการให้เป็นไปตามนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ กมช. ประกาศกำหนด

(๗) จัดทำเอกสารดังต่อไปนี้ของหน่วยงานของตนให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ กมช. ประกาศกำหนด ตามหลักเกณฑ์ที่กำหนดในประกาศประมวลแนวทางปฏิบัติให้แล้วเสร็จภายในระยะเวลา ๑ ปีนับแต่วันที่ประกาศนี้มีผลใช้บังคับ

(ก) ประมวลแนวทางปฏิบัติ ประกอบด้วย แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และแผนการรับมือภัยคุกคามทางไซเบอร์

(ข) กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ประกอบด้วย การระบุความเสี่ยงที่อาจจะเกิดขึ้น มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ และมาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์

(๘) จัดให้มีการทบทวนเพื่อปรับปรุงหรือแก้ไขเพิ่มเติมนโยบาย มาตรฐานและประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่งคงปลอดภัยไซเบอร์ของหน่วยงานอย่างน้อยปีละหนึ่งครั้งหรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญต่อการปฏิบัติการเกี่ยวกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของหน่วยงาน

(๙) เข้าร่วมการดำเนินการ ประสานงาน และให้การสนับสนุน กกม. ดูแลและดำเนินการเพื่อรับมือกับภัยคุกคามทางไซเบอร์ ตามมาตรา ๖๑ มาตรา ๖๒ มาตรา ๖๓ มาตรา ๖๔ มาตรา ๖๕ และมาตรา ๖๖

(๑๐) แจ้งรายชื่อเจ้าหน้าที่ระดับบริหารและระดับปฏิบัติการ พร้อมด้วยข้อมูลการติดต่อที่สามารถติดต่อได้ในกรณีมีเหตุฉุกเฉินภายในระยะเวลาหกสิบนาที เพื่อประสานงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ไปยังสำนักงาน ทั้งนี้ ในกรณีที่มีการเปลี่ยนแปลงข้อมูล ให้แจ้งรายชื่อหรือข้อมูลการติดต่อที่เปลี่ยนแปลงให้สำนักงานทราบภายในระยะเวลา ๑๕ วัน นับแต่วันที่มีการเปลี่ยนแปลง

(๑๑) รับแจ้งและเก็บรักษาข้อมูลรายชื่อและข้อมูลการติดต่อของเจ้าหน้าที่ระดับบริหารและระดับปฏิบัติการ และของเจ้าของกรรมสิทธิ์ ผู้ครอบครองคอมพิวเตอร์ และผู้ดูแลระบบคอมพิวเตอร์ที่ได้รับจากหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้ปลอดภัย

(๑๒) เก็บรักษาข้อมูลที่จำเป็นของหน่วยงานที่ได้รับการแต่งตั้งหรือถูกยกเลิกจากการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(๑๓) รับแจ้งข้อมูลจากหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศภายใต้ที่อยู่ในการควบคุมหรือกำกับดูแลของตน และดำเนินการรวบรวมข้อมูล ตรวจสอบ วิเคราะห์สถานการณ์และประเมินผลกระทบเกี่ยวกับภัยคุกคามทางไซเบอร์ และดำเนินการตามที่กำหนดในมาตรา ๕๙ เมื่อปรากฏภัยคุกคามทางไซเบอร์แก่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศเกิดขึ้น

(๑๔) ดำเนินการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ตามหลักเกณฑ์ที่กำหนดในประกาศประมวลแนวทางปฏิบัติ และในกรณีที่มีภัยคุกคามทางไซเบอร์เกิดขึ้น ให้ดำเนินการต่อไปนี้ด้วย

(ก) เก็บรักษาข้อมูลและพยานหลักฐานตามที่กำหนดในขั้นตอนที่ ๒ - การตรวจจับและวิเคราะห์ (Detection and Analysis) ของเอกสารแนบ ๓ แนวทางการจัดทำประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ หัวข้อแผนการรับมือภัยคุกคามทางไซเบอร์ และแนวทางการจัดทำกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ หัวข้อมาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond) ท้ายประกาศสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง แนวทางการจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

(ข) แจ้งเหตุไปยังสำนักงานภายในระยะเวลาและปฏิบัติตามหลักเกณฑ์และวิธีการตามที่กำหนดในประกาศที่ออกโดยอาศัยอำนาจตามมาตรา ๕๗

(ค) ให้ความร่วมมือกับพนักงานเจ้าหน้าที่ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ในการปฏิบัติการตามมาตรา ๖๖ รวมถึงให้ความร่วมมือกับพนักงานเจ้าหน้าที่หรือเจ้าหน้าที่อื่นที่เกี่ยวข้องในการสืบสวนสอบสวนและรวบรวมพยานหลักฐานเกี่ยวกับภัยคุกคามทางไซเบอร์

(๑๕) รับทราบและให้ความเห็นหรือข้อเสนอแนะเกี่ยวกับระเบียบวิธีปฏิบัติและกระบวนการในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ที่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำก่อนส่งให้แก่สำนักงาน

(๑๖) จัดทำรายงานประจำปี และส่งรายงานดังกล่าวให้สำนักงาน ภายในวันที่ ๓๑ มกราคมของปีถัดไป โดยรายงานต้องมีรายละเอียดดังต่อไปนี้

(ก) ระบุจำนวนและลักษณะของเหตุการณ์ภัยคุกคามทางไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ในการควบคุมหรือกำกับดูแลของตน ตามแบบรายงานสรุปภัยคุกคามทางไซเบอร์ในหนึ่งรอบปี ที่กำหนดท้ายประกาศที่ออกโดยอาศัยอำนาจตามมาตรา ๕๗

(ข) วิเคราะห์สาเหตุหรือผลกระทบที่เกิดขึ้นจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้น

(ค) ปัญหาและอุปสรรคในการดำเนินงาน

(ง) ข้อเสนอแนะต่าง ๆ ซึ่งรวมถึงข้อเสนอแนะเชิงนโยบาย

หากหน่วยงานเป็นทั้งหน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่มีภารกิจหรือการให้บริการตามประกาศที่ออกโดยอาศัยอำนาจตามมาตรา ๔๙ ให้จัดทำรายงานโดยรวมข้อมูลของตนในบทบาทที่เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศด้วย

(๑๗) ให้ความช่วยเหลือหรือสนับสนุนหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ในควบคุมหรือกำกับดูแลของตน ในการจัดทำหรือปรับปรุงมาตรการป้องกัน รับมือ ปราบปรามและระงับภัยคุกคามทางไซเบอร์ ให้มีความเหมาะสมและเป็นปัจจุบัน และเก็บรักษาข้อมูลดังกล่าวให้ปลอดภัย

(๑๘) ให้ความช่วยเหลือหรือสนับสนุนหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ในควบคุมหรือกำกับดูแลของตน ในการฝึกซ้อมรับมือภัยคุกคามทางไซเบอร์ และการทดสอบสถานะความพร้อมในการรับมือกับภัยคุกคามทางไซเบอร์ที่สำนักงานจัดขึ้น

(๑๙) ให้ความร่วมมือ สนับสนุนหรือดำเนินการเพื่อให้มีศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ในด้านของตนตามประกาศที่ออกโดยอาศัยอำนาจตามมาตรา ๔๙

ในกรณีที่ไม่มีหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่เป็นหน่วยงานของรัฐใดมีความพร้อมและหน่วยงานกำกับหรือดูแลไม่พร้อมทำหน้าที่เป็นศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศดังกล่าวให้แจ้งเหตุขัดข้องให้สำนักงานทราบถึงเหตุผลที่ยังไม่พร้อมในการทำหน้าที่เป็นศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ทั้งนี้ ลักษณะ หน้าที่และความรับผิดชอบของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศเป็นไปตามหลักเกณฑ์ที่ กมช. ประกาศกำหนด

(๒๐) ให้ความร่วมมือหรือสนับสนุนแก่ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ในการติดตามการตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ ผลกระทบเกี่ยวกับภัยคุกคามทางไซเบอร์ และผลการตอบสนองและรับมือเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น

(๒๑) ประสานงาน ให้ความร่วมมือ หรือสนับสนุน แก่หน่วยงานควบคุมหรือกำกับดูแลอื่นเพื่อให้การควบคุมหรือกำกับดูแลหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศมีความสอดคล้องกัน

(๒๒) ดำเนินการตามที่ กมช. หรือ กกม. มอบหมายหรือประกาศกำหนด หรือให้ความร่วมมือกับสำนักงานหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์

ข้อ ๖ ให้สำนักงานพิจารณาทบทวนหน้าที่ของหน่วยงานของโครงสร้างพื้นฐานสำคัญทางสารสนเทศและหน่วยงานควบคุมหรือกำกับดูแลอย่างน้อยทุก ๒ ปี หรือเมื่อมีการเปลี่ยนแปลงที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์อย่างมีนัยสำคัญ

ข้อ ๗ ให้ประธานกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์รักษาการตามประกาศนี้และให้มีอำนาจออกประกาศ คำสั่ง หลักเกณฑ์และวิธีการเพื่อปฏิบัติตามประกาศนี้

ในกรณีที่มีปัญหาเกี่ยวกับการปฏิบัติตามประกาศนี้ หรือประกาศนี้ไม่ได้กำหนดเรื่องใดไว้ ให้ประธานกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์เป็นผู้มีอำนาจตีความและวินิจฉัยชี้ขาด ทั้งนี้ การตีความและคำวินิจฉัยของประธานกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ให้เป็นที่สุด

ประกาศ ณ วันที่ ๕ กุมภาพันธ์ พ.ศ. ๒๕๖๗
ประเสริฐ จันทรรวงทอง
รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
ประธานกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์



ฉบับภาษาอังกฤษ
English Version

อยู่ระหว่างดำเนินการแปลเอกสารเป็นฉบับภาษาอังกฤษ

The translation of the document into English is underway.

17

ประกาศ กมช.

เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567

มีผลใช้บังคับตั้งแต่วันที่ 10 ก.ย. 69 เป็นต้นไป

Notification of NCSC

Re: the duties of Critical Information Infrastructure organizations and duties of Regulators B.E. 2567 (2024)

effective from September 10, 2026, onwards.



ฉบับภาษาไทย
Thai Version

ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์

พ.ศ. ๒๕๖๗

โดยที่พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดให้คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ มีหน้าที่และอำนาจสร้างมาตรฐานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ และกำหนดมาตรฐานขั้นต่ำที่เกี่ยวข้องกับคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือโปรแกรมคอมพิวเตอร์ จึงสมควรมีมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ เพื่อให้การดำเนินงานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์เป็นไปอย่างมีประสิทธิภาพ

อาศัยอำนาจตามความในมาตรา ๙ (๔) แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ประกอบกับมติที่ประชุมคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติในคราวการประชุมครั้งที่ ๒/๒๕๖๗ เมื่อวันที่ ๓๑ กรกฎาคม ๒๕๖๗ คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติจึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. ๒๕๖๗”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับเมื่อพ้นกำหนดสองปีนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ข้อ ๓ ในประกาศนี้

“หน่วยงาน” หมายความว่า หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแลและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

“การประมวลผลคลาวด์” (Cloud Computing) หมายความว่า แนวคิดการเข้าถึงเครือข่ายสารสนเทศซึ่งเป็นกลุ่มทรัพยากรทางกายภาพหรือเสมือนที่สามารถแบ่งปัน (Shareable) มีความยืดหยุ่น (Elastic) และขยายขนาดได้ (Scalable) ด้วยการจัดหาตัวเอง (Self-service Provisioning) และการจัดการตามความต้องการ (Administration On-demand)

“บริการคลาวด์” (Cloud Service) หมายความว่า ความสามารถ (Capability) ในการประมวลผลคลาวด์ ซึ่งถูกเรียกใช้โดยอินเทอร์เฟซที่กำหนดให้

“ประเภทบริการคลาวด์” (Cloud Service Category) หมายความว่า กลุ่มของบริการคลาวด์ที่มีคุณสมบัติร่วมกันบางอย่าง โดยมีรูปแบบ ดังนี้

(๑) การให้บริการโครงสร้างพื้นฐานหลัก (Infrastructure as a Service : IaaS) ประกอบด้วยระบบประมวลผลข้อมูล ระบบการจัดเก็บข้อมูล ระบบเครือข่าย และทรัพยากรพื้นฐานอื่น ๆ ที่เกี่ยวข้องกับระบบประมวลผล ผู้ใช้บริการสามารถใช้งานซอฟต์แวร์บนโครงสร้างพื้นฐานและทรัพยากรที่ผู้ให้บริการจัดหาให้ได้อย่างมีประสิทธิภาพ โดยไม่ต้องบริหารจัดการโครงสร้างพื้นฐานที่จำเป็นด้วยตนเอง หรือ

(๒) การให้บริการแพลตฟอร์ม (Platform as a Service : PaaS) ประกอบด้วยระบบโปรแกรมงานคอมพิวเตอร์ ระบบฐานข้อมูล และระบบจัดการหรืองานบริการจากคอมพิวเตอร์ ผู้ใช้บริการสามารถพัฒนา ติดตั้ง และปรับแต่งซอฟต์แวร์ได้ โดยไม่ต้องบริหารจัดการในส่วนที่เกี่ยวข้องกับโครงสร้างพื้นฐาน เครือข่าย ระบบปฏิบัติการ และระบบจัดการฐานข้อมูล หรือ

(๓) การให้บริการซอฟต์แวร์ (Software as a Service : SaaS) ผู้ให้บริการจัดเตรียมซอฟต์แวร์สำเร็จรูปแล้ว โดยผู้ใช้บริการสามารถกำหนดค่าความต้องการ พารามิเตอร์ ปริมาณหน่วยประมวลผลข้อมูล หน่วยเก็บข้อมูล และบริหารจัดการเพื่อให้ได้บริการตามวัตถุประสงค์ หรือ

(๔) การให้บริการใดที่เป็นการรวมกันของสองบริการขึ้นไป จาก ข้อ (๑) ถึง (๓) หรือ

(๕) การให้บริการอื่นที่สำนักงานประกาศกำหนด

“คลาวด์สาธารณะ” (Public Cloud) หมายความว่า รูปแบบการใช้คลาวด์ที่บริการคลาวด์สามารถใช้ได้กับผู้ใช้บริการคลาวด์ใด ๆ และทรัพยากรถูกควบคุมโดยผู้ให้บริการคลาวด์

“ผู้ใช้บริการคลาวด์” (Cloud Service Customer : CSC) หมายความว่า หน่วยงานที่มีข้อตกลงทางสัญญาอย่างเป็นทางการในการใช้บริการคลาวด์ที่ให้บริการโดยผู้ให้บริการคลาวด์

“ผู้ให้บริการคลาวด์” (Cloud Service Provider : CSP) หมายความว่า หน่วยงานของรัฐหรือเอกชนที่ทำให้บริการคลาวด์สามารถใช้ได้กับผู้ใช้บริการคลาวด์ รวมถึงจัดการทรัพยากรเหล่านี้เพื่อให้มั่นใจว่ามีความพร้อมใช้งานความมั่นคงปลอดภัย และความสามารถในการขยายตัวสำหรับผู้ใช้บริการคลาวด์ของตน

“ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูลส่วนบุคคลตามที่กำหนดไว้ในมาตรา ๖ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

“สำนักงาน” หมายความว่า สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

ข้อ ๔ ให้หน่วยงานที่ใช้บริการคลาวด์สาธารณะดำเนินการตามมาตรฐานฉบับนี้ โดยคำนึงถึงระดับผลกระทบของข้อมูลหรือระบบสารสนเทศ ตามที่กำหนดไว้ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. ๒๕๖๖ และดำเนินการไม่น้อยกว่าข้อกำหนดขั้นต่ำท้ายประกาศนี้

ข้อ ๕ การดำเนินการตามข้อ ๔ กรณีเป็นข้อมูลส่วนบุคคล ให้จัดระดับผลกระทบด้านการรักษาความลับระดับกลางเป็นอย่างน้อย ตามที่กำหนดไว้ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. ๒๕๖๖ และดำเนินการไม่น้อยกว่าข้อกำหนดขั้นต่ำท้ายประกาศนี้

ข้อ ๖ ให้หน่วยงานจัดส่งผลสรุปรายงานการดำเนินการต่อสำนักงานภายในสามสิบวันนับแต่วันที่ดำเนินการแล้วเสร็จ

ข้อ ๗ ให้เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติรักษาการตามประกาศนี้ และให้มีอำนาจออกประกาศ คำสั่ง หลักเกณฑ์และวิธีการเพื่อปฏิบัติตามประกาศนี้

ในกรณีที่มีปัญหาเกี่ยวกับการปฏิบัติตามประกาศนี้ หรือประกาศนี้ไม่ได้กำหนดเรื่องใดไว้ ให้ประธานกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเป็นผู้มีอำนาจตีความ และวินิจฉัยชี้ขาด ทั้งนี้ การตีความและคำวินิจฉัยของประธานกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติให้เป็นที่สุด

ประกาศ ณ วันที่ ๓ กันยายน พ.ศ. ๒๕๖๗
ภูมิธรรม เวชยชัย
รองนายกรัฐมนตรี ปฏิบัติหน้าที่
ประธานกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

แนบท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. ๒๕๖๗

๑. บทนำ

๑.๑ เหตุผลความจำเป็น

จากการประชุมคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ ครั้งที่ ๑/๒๕๖๖ เมื่อวันที่ ๒๒ ธันวาคม ๒๕๖๖ ณ ตึกบัญชาการ ๑ ทำเนียบรัฐบาล และผ่านสื่ออิเล็กทรอนิกส์ ที่ประชุมฯ ได้ให้ความเห็นชอบแนวทางการขับเคลื่อนตามนโยบายการใช้คลาวด์เป็นหลัก (Cloud First Policy) ทั้งในส่วนของข้อกำหนดหน่วยงานรัฐ ผู้รับบริการ แนวทางปฏิบัติ ข้อมูล มาตรฐาน ประเภทของบริการคลาวด์ ผู้ให้บริการคลาวด์ และการบริหารจัดการบริการ ซึ่งได้กำหนดแนวทางการดำเนินงานด้านบริการคลาวด์ (Cloud Service) ในระยะ ๕ ปี โดยเห็นชอบให้จัดตั้งคณะกรรมการเฉพาะด้านการขับเคลื่อนตามนโยบายการใช้คลาวด์เป็นหลัก (Cloud First Policy) เพื่อกำกับ ติดตาม และให้ข้อแนะนำในการขับเคลื่อนการดำเนินงาน

นอกจากนี้ จากการที่สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ได้เปิดเผยสถิติภัยคุกคามทางไซเบอร์ ประจำปี พ.ศ. ๒๕๖๖ พบว่าหน่วยงานที่ถูกโจมตีมากที่สุด ได้แก่ หน่วยงานด้านการศึกษา จำนวน ๖๓๒ ครั้ง ขณะที่อันดับที่ ๒ เป็นหน่วยงานรัฐอื่น ๆ ที่โดนโจมตีไป จำนวน ๑๔๕ ครั้ง และอันดับที่ ๓ ได้แก่ ผู้ประกอบการพาณิชย์ที่เป็นบริษัทเอกชนสัญชาติไทย โดนโจมตีสูงสุด จำนวน ๑๔๘ ครั้ง ทั้งนี้ รูปแบบภัยคุกคามทางไซเบอร์ที่พบได้บ่อยที่สุดในปี พ.ศ. ๒๕๖๖ อันดับ ๑ ได้แก่ เว็บพนันออนไลน์จำนวน ๕๑๕ ครั้ง อันดับ ๒ ได้แก่เว็บไซต์ที่ถูกแฮ็กจำนวน ๓๓๖ ครั้ง และอันดับ ๓ ได้แก่ เว็บไซต์ปลอม จำนวน ๓๐๑ ครั้ง ทำให้เห็นแนวโน้มของภัยคุกคามทางไซเบอร์ที่มีต่อข้อมูลและระบบสารสนเทศของหน่วยงานต่าง ๆ เพิ่มสูงขึ้นอย่างต่อเนื่อง โดยเฉพาะภัยคุกคามทางไซเบอร์ที่มีต่อหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

จากสถานการณ์ดังกล่าวข้างต้น ทำให้การที่จะส่งเสริมให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมถึงหน่วยงานเอกชน หันมาใช้งานระบบคลาวด์มากขึ้น แม้ว่าจะเกิดผลดีในแง่ของการพัฒนาเศรษฐกิจและสังคมของประเทศไทย และการเพิ่มความสามารถในการเข้าถึงทักษะด้านดิจิทัล แต่ก็มีความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่มีต่อหน่วยงานดังกล่าวเพิ่มสูงขึ้นด้วย จึงเป็นเหตุผลสำคัญที่สำนักงานจะต้องจัดทำมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ฉบับนี้

๑.๒ วัตถุประสงค์

เพื่อลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่มีต่อการใช้บริการคลาวด์สาธารณะให้กับหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๑.๓ ฐานอำนาจ

มาตรา ๙ (๔) แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดให้คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ มีหน้าที่และอำนาจกำหนดมาตรฐานและแนวทางส่งเสริมพัฒนาระบบการให้บริการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ สร้างมาตรฐานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ และกำหนดมาตรฐานขั้นต่ำที่เกี่ยวข้องกับคอมพิวเตอร์ ระบบคอมพิวเตอร์ โปรแกรมคอมพิวเตอร์ รวมถึงส่งเสริมการรับรองมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานเอกชน

๑.๔ หลักการสำคัญที่เกี่ยวข้อง

- ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. ๒๕๖๖

- ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานและแนวทางส่งเสริมพัฒนาระบบการให้บริการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๖

- ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔

๑.๕ ความเสี่ยงจากการใช้บริการคลาวด์

มาตรฐานฉบับนี้ กำหนดความเสี่ยงจากการใช้บริการระบบคลาวด์เป็น ๒ ประเภท ได้แก่ ความเสี่ยงจากผู้ใช้บริการคลาวด์ (Cloud Service Customer : CSC) และความเสี่ยงจากผู้ให้บริการคลาวด์ (Cloud Service Provider : CSP)

๑.๖ โครงสร้างของมาตรฐาน

มาตรฐานฉบับนี้ แบ่งข้อกำหนด (Requirements) ออกได้เป็น ๒ ส่วน (Areas) ดังนี้

๑. การกำกับดูแลด้านความมั่นคงปลอดภัยระบบคลาวด์ (Cloud Security Governance)

๑.๑ นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Policies)

๑.๒ โครงสร้างองค์กรด้านความมั่นคงปลอดภัยสารสนเทศ (Organization of Information Security)

๑.๓ การปฏิบัติตามกฎ ระเบียบ ข้อบังคับ (Compliance)

๒. การปฏิบัติการและการรักษาความมั่นคงปลอดภัยโครงสร้างพื้นฐานระบบคลาวด์ (Cloud Infrastructure Security and Operation)

๒.๑ การบริหารทรัพยากรมนุษย์ (Human Resource Security)

๒.๒ การจัดการทรัพย์สิน (Asset Management)

๒.๓ การควบคุมการเข้าถึง (Access Control)

๒.๔ การเข้ารหัส (Cryptography)

๒.๕ การรักษาความปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and Environment Security)

๒.๖ การรักษาความมั่นคงปลอดภัยการปฏิบัติการ (Operations Security)

๒.๗ การรักษาความมั่นคงปลอดภัยเครือข่าย (Communication Security)

๒.๘ การจัดหา การพัฒนา และการบำรุงรักษา (System Acquisition, Development, and Maintenance)

๒.๙ การจัดการผู้ให้บริการภายนอก (Supplier Relationships)

๒.๑๐ การจัดการเหตุภัยคุกคามทางสารสนเทศ (Information Security Incident Management)

๑.๗ กรอบแนวคิด

เนื่องจากความเสี่ยงจากการใช้บริการคลาวด์มาจาก ๒ ส่วน คือ ความเสี่ยงอันเกิดจากผู้ใช้บริการคลาวด์และความเสี่ยงอันเกิดจากผู้ให้บริการคลาวด์ ดังนั้น มาตรฐานฉบับนี้จึงอาศัยหลักการเรื่องความร่วมรับผิดชอบ (Share Responsibilities) ให้กับทั้งผู้ใช้บริการคลาวด์ (CSC) และผู้ให้บริการคลาวด์ (CSP) ซึ่งจะทำให้สามารถลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่มีต่อระบบคลาวด์ได้อย่างครอบคลุมและมีประสิทธิภาพ

นอกจากนี้ หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มีการใช้งานระบบสารสนเทศและข้อมูลสารสนเทศซึ่งมีระดับผลกระทบ (Criticality) และระดับความอ่อนไหว (Sensitivity) ที่แตกต่างกัน ประกอบกับประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. ๒๕๖๖ กำหนดให้หน่วยงานดังกล่าวมีการประเมินและจัดระดับผลกระทบที่อาจเกิดขึ้นตามวัตถุประสงค์ด้านความมั่นคงปลอดภัยไซเบอร์ (Security Objectives) ดังนั้น มาตรฐานฉบับนี้จึงกำหนดให้มีข้อกำหนดขั้นต่ำด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Baseline) เป็น ๓ ระดับ คือ ระดับต่ำ ระดับกลาง และระดับสูง เพื่อให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ สามารถปฏิบัติตามมาตรฐานฉบับนี้ได้อย่างมีประสิทธิภาพ โดยมีค่าใช้จ่ายที่เหมาะสมกับประโยชน์ที่จะได้รับ

นอกจากนี้ ผู้ให้บริการคลาวด์ (Cloud Service Provider : CSP) ที่จะให้บริการกับหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ มีหน้าที่ต้องดำเนินการให้เป็นไปตามที่หน่วยงานดังกล่าวร้องขอด้วย

<u>๑.๘ กระบวนการตรวจรับรองมาตรฐาน</u>

มาตรฐานฉบับนี้ กำหนดแนวทางการตรวจรับรองมาตรฐานสำหรับผู้ใช้บริการคลาวด์ และผู้ให้บริการคลาวด์ ที่จะขอรับการรับรอง ดังนี้

๑.๘.๑ ประเภทของการตรวจรับรอง

- <u>การประเมินตนเอง (Self-assessment)</u> เป็นการประเมินหน่วยงานของตนตามรูปแบบที่สำนักงานกำหนด พร้อมแนบหลักฐานและขออนุมัติไปยังผู้บริหารสูงสุดของหน่วยงาน โดยเก็บรักษาไว้ที่หน่วยงานและส่งให้สำนักงานด้วย

- <u>การตรวจรับรองโดยหน่วยงานควบคุมหรือกำกับดูแล (Attestation)</u> เป็นการตรวจให้การรับรองโดยหน่วยงานควบคุมหรือกำกับดูแลตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง การกำหนดหลักเกณฑ์ ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการมอบหมายการควบคุมและกำกับดูแล

- <u>การตรวจรับรองโดยหน่วยงานให้บริการตรวจรับรอง (Certify Body)</u> เป็นการตรวจให้การรับรองโดยหน่วยงานให้บริการตรวจรับรองในระดับขั้นก้าวหน้า หรือสูงกว่า ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานและแนวทางส่งเสริมพัฒนาระบบการให้บริการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๖ ทั้งนี้ ในช่วงแรกของการดำเนินการที่สำนักงานยังมิได้ให้การรับรองหน่วยงานให้บริการตรวจรับรอง อาจดำเนินการโดยหน่วยงานให้บริการตรวจรับรองตามมาตรฐานสากลที่สำนักงานประกาศกำหนด ก็ได้

๑.๘.๒ ความถี่ในการตรวจรับรอง

- <u>กรณีของผู้ใช้บริการคลาวด์</u>

- ผลกระทบระดับต่ำ : ให้ดำเนินการประเมินตนเอง (Self-assessment) รวมทั้งมีการทบทวนอย่างน้อยปีละ ๑ ครั้ง

- ผลกระทบระดับกลาง : ได้รับการรับรองโดยหน่วยงานควบคุมหรือกำกับดูแล (Attestation) หรือ ได้รับการรับรองโดยหน่วยงานให้บริการตรวจรับรอง (Certify Body) ตามวงรอบ ๓ ปี ประกอบด้วยการตรวจรับรองในปีที่ ๑ และการตรวจสำรวจในปีที่ ๒ และ ๓

- ผลกระทบระดับสูง : ได้รับการรับรองโดยหน่วยงานให้บริการตรวจรับรอง (Certify Body) ตามวงรอบ ๓ ปี ประกอบด้วยการตรวจรับรองในปีที่ ๑ และการตรวจสำรวจในปีที่ ๒ และ ๓

- กรณีของผู้ให้บริการคลาวด์

- ผลกระทบระดับต่ำ : ได้รับการรับรองโดยหน่วยงานให้บริการตรวจรับรอง (Certify Body) ตามวงรอบ ๓ ปี ประกอบด้วยการตรวจรับรองในปีที่ ๑ และการตรวจสำรวจในปีที่ ๒ และ ๓ และได้รับการรับรองตามมาตรฐาน ISO/IEC 27001 Certification และ CSA STAR Level 1/CCM Lite เป็นอย่างน้อย

- ผลกระทบระดับกลาง : ได้รับการรับรองโดยหน่วยงานให้บริการตรวจรับรอง (Certify Body) ตามวงรอบ ๓ ปี ประกอบด้วยการตรวจรับรองในปีที่ ๑ และการตรวจสำรวจในปีที่ ๒ และ ๓ และได้รับการรับรองตามมาตรฐาน CSA STAR Level 2/CCM และ ISO/IEC 27701 Certification เป็นอย่างน้อย

- ผลกระทบระดับสูง : ได้รับการรับรองโดยหน่วยงานให้บริการตรวจรับรอง (Certify Body) ตามวงรอบ ๓ ปี ประกอบด้วยการตรวจรับรองในปีที่ ๑ และการตรวจสำรวจในปีที่ ๒ และ ๓ และได้รับการรับรองตามมาตรฐาน ISO/IEC 27017 Certification หรือ CSA STAR Level 2/CCM และ ISO/IEC 27018 Certification และ ISO/IEC 27701 Certification เป็นอย่างน้อย

๑.๘.๓ ในกรณีที่ผู้ให้บริการคลาวด์ ได้รับการรับรองโดยหน่วยงานให้บริการตรวจรับรอง (Certify Body) แล้ว ก็ไม่จำเป็นต้องดำเนินการประเมินตนเอง (Self-assessment)

๑.๘.๔ ในกรณีที่ผู้ให้บริการคลาวด์ ได้รับการรับรองตามมาตรฐาน CSA STAR Level 2/CCM แล้ว ก็ไม่จำเป็นต้องดำเนินการตรวจรับรองตามมาตรฐาน CSA STAR Level 1/CCM Lite

๒. ขอบเขต (Scope)

- มาตรฐานฉบับนี้ ใช้บังคับกับหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ รวมถึงผู้ให้บริการคลาวด์กับหน่วยงานดังกล่าวข้างต้นด้วย

- มาตรฐานฉบับนี้ กำหนดมาตรการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์สำหรับผู้ใช้บริการคลาวด์ รวมถึงผู้ให้บริการคลาวด์สาธารณะ (Public Cloud Service Provider) เฉพาะที่ต้องให้บริการกับผู้ใช้บริการคลาวด์ที่เป็นหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ เท่านั้น โดยใช้ฐานสัญญาระหว่างผู้ใช้บริการคลาวด์ ดังกล่าวข้างต้น กับผู้ให้บริการคลาวด์

- ผู้ที่เกี่ยวข้องกับมาตรฐานฉบับนี้ ประกอบด้วย หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ รวมถึงผู้ให้บริการคลาวด์สาธารณะ ผู้ตรวจสอบภายในด้านความมั่นคงปลอดภัยไซเบอร์ และหน่วยงานให้บริการตรวจรับรอง (Certify Body)

๓. การอ้างอิงที่เกี่ยวข้อง (Normative Reference)

- ISO/IEC 27017:2015 Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services

- ISO/IEC 27018:2019 Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

- ISO/IEC 22123-1:2023 Information technology — Cloud computing Part 1: Vocabulary

- ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. ๒๕๖๖

- ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานและแนวทางส่งเสริมพัฒนาระบบการให้บริการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๖

- ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔

๔. ข้อกำหนดขั้นต่ำและการตรวจรับรองสำหรับผู้ใช้บริการคลาวด์และผู้ให้บริการคลาวด์

ตารางข้อกำหนดขั้นต่ำและการตรวจรับรองสำหรับผู้ใช้บริการคลาวด์และผู้ให้บริการคลาวด์

ประเภทของข้อมูลหรือระบบสารสนเทศ[๑]	ข้อกำหนดขั้นต่ำ	การตรวจรับรองสำหรับผู้ใช้บริการคลาวด์	การตรวจรับรองสำหรับผู้ให้บริการคลาวด์
ผลกระทบระดับต่ำ	ข้อกำหนดส่วนที่ ๑ - เฉพาะข้อ ๕.๑.๑, ๕.๑.๒ ข้อกำหนดส่วนที่ ๒ - เฉพาะข้อ ๕.๒.๑, ๕.๒.๒, ๕.๒.๓, ๕.๒.๔, ๕.๒.๘, ๕.๒.๙	ประเมินตนเอง (Self-assessment) พร้อมแนบหลักฐานและขออนุมัติไปยังผู้บริหารสูงสุดของหน่วยงาน โดยเก็บรักษาไว้ที่หน่วยงานและส่งให้สำนักงานด้วย	ได้รับการรับรองโดยหน่วยงานให้บริการตรวจรับรอง (Certify Body) ตามวงรอบ ๓ ปี ประกอบด้วยการตรวจรับรองในปีที่ ๑ และการตรวจสำรวจในปีที่ ๒ และ ๓ และได้รับการรับรองตามมาตรฐาน ISO/IEC 27001 Certification และ CSA STAR Level 1/CCM Lite เป็นอย่างน้อย
ผลกระทบระดับกลาง	ข้อกำหนดส่วนที่ ๑ - ทุกข้อ ข้อกำหนดส่วนที่ ๒ - เฉพาะข้อ ๕.๒.๑, ๕.๒.๒, ๕.๒.๓, ๕.๒.๔, ๕.๒.๗, ๕.๒.๘, ๕.๒.๙, ๕.๒.๑๐	ได้รับการรับรองโดยหน่วยงานควบคุมหรือกำกับดูแล (Attestation) หรือ ได้รับการรับรองโดยหน่วยงานให้บริการตรวจรับรอง (Certify Body) ตามวงรอบ ๓ ปี ประกอบด้วยการตรวจรับรองในปีที่ ๑ และการตรวจสำรวจในปีที่ ๒ และ ๓	ได้รับการรับรองโดยหน่วยงานให้บริการตรวจรับรอง (Certify Body) ตามวงรอบ ๓ ปี ประกอบด้วยการตรวจรับรองในปีที่ ๑ และการตรวจสำรวจในปีที่ ๒ และ ๓ และได้รับการรับรองตามมาตรฐาน CSA STAR Level 2/CCM และ ISO/IEC 27701 Certification เป็นอย่างน้อย
ผลกระทบระดับสูง	ข้อกำหนดส่วนที่ ๑ - ทุกข้อ ข้อกำหนดส่วนที่ ๒ - ทุกข้อ	ได้รับการรับรองโดยหน่วยงานให้บริการตรวจรับรอง (Certify Body) ตามวงรอบ ๓ ปี ประกอบด้วยการตรวจรับรองในปีที่ ๑ และการตรวจสำรวจในปีที่ ๒ และ ๓	ได้รับการรับรองโดยหน่วยงานให้บริการตรวจรับรอง (Certify Body) ตามวงรอบ ๓ ปี ประกอบด้วยการตรวจรับรองในปีที่ ๑ และการตรวจสำรวจในปีที่ ๒ และ ๓ และได้รับการรับรองตามมาตรฐาน ISO/IEC 27017 Certification

[๑] ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. ๒๕๖๖

ประเภทของข้อมูลหรือระบบสารสนเทศ๑	ข้อกำหนดขั้นต่ำ	การตรวจรับรองสำหรับผู้ใช้บริการคลาวด์	การตรวจรับรองสำหรับผู้ให้บริการคลาวด์
			หรือ CSA STAR Level 2/CCM และ ISO/IEC 27018 Certification และ ISO/IEC 27701 Certification เป็นอย่างน้อย

๕. มาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์

๕.๑ การกำกับดูแลด้านความมั่นคงปลอดภัยระบบคลาวด์ (Cloud Security Governance)

๕.๑.๑ นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Policies)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ใช้บริการคลาวด์ต้องกำหนดนโยบายความมั่นคงปลอดภัยสารสนเทศสำหรับการประมวลผลบนคลาวด์ให้เป็นนโยบายเฉพาะหัวข้อของผู้ใช้บริการคลาวด์ นโยบายความมั่นคงปลอดภัยสารสนเทศสำหรับการประมวลผลบนคลาวด์ของผู้ใช้บริการคลาวด์ ต้องสอดคล้องกับระดับความเสี่ยงที่ยอมรับได้ด้านความมั่นคงปลอดภัยสารสนเทศ ที่มีต่อข้อมูลและทรัพย์สินอื่น ๆ ขององค์กร ข) เมื่อกำหนดนโยบายความมั่นคงปลอดภัยสารสนเทศ สำหรับการประมวลผลบนคลาวด์ ผู้ใช้บริการคลาวด์ ต้องคำนึงถึงสิ่งต่อไปนี้ – ข้อมูลที่จัดเก็บในสภาพแวดล้อมการประมวลผลบนคลาวด์อาจอยู่ภายใต้การเข้าถึงและการจัดการโดย ผู้ให้บริการคลาวด์ – ทรัพย์สินขององค์กรอาจจะได้รับการดูแลรักษาในสภาพแวดล้อมการประมวลผลบนคลาวด์ เช่น โปรแกรมแอปพลิเคชัน – กระบวนการต่าง ๆ สามารถทำงานบนบริการคลาวด์เสมือนจริงที่มีผู้ใช้หลายราย – ผู้ใช้บริการคลาวด์และบริบทที่ใช้บริการคลาวด์ – ผู้ดูแลระบบบริการคลาวด์ของผู้ใช้บริการคลาวด์ที่ได้รับสิทธิพิเศษในการเข้าถึง – ตำแหน่งทางภูมิศาสตร์ขององค์กรของผู้ให้บริการคลาวด์ และประเทศที่ผู้ให้บริการคลาวด์สามารถจัดเก็บข้อมูลผู้ใช้บริการคลาวด์ ได้ (แม้จะเป็นการชั่วคราว) ค) นโยบายคุ้มครองข้อมูลส่วนบุคคลของผู้ใช้บริการคลาวด์ต้องระบุข้อความเกี่ยวกับข้อตกลงทางสัญญา	ก) ผู้ให้บริการคลาวด์ต้องเพิ่มนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศเพื่อจัดการกับการจัดหาและใช้บริการคลาวด์ โดยคำนึงถึงสิ่งต่อไปนี้ – ข้อกำหนดขั้นต่ำด้านความมั่นคงปลอดภัยสารสนเทศที่ใช้กับการออกแบบและการใช้งานบริการคลาวด์ – ความเสี่ยงจากบุคคลภายในที่ได้รับอนุญาต – การเช่าหลายรายและการแยก ผู้ใช้บริการคลาวด์ (รวมถึงการจำลองเสมือน) – การเข้าถึงทรัพย์สินของผู้ใช้บริการคลาวด์โดยเจ้าหน้าที่ของผู้ให้บริการคลาวด์ – ขั้นตอนการควบคุมการเข้าถึง เช่น การยืนยันตัวตน ที่เข้มงวดสำหรับการเข้าถึงบริการคลาวด์ของผู้ดูแลระบบ – การสื่อสารกับผู้ใช้บริการคลาวด์ระหว่างการจัดการการเปลี่ยนแปลง – ความปลอดภัยของการจำลองเสมือน – การเข้าถึงและปกป้องข้อมูลของผู้ใช้บริการคลาวด์ – การจัดการวงจรชีวิตของบัญชีผู้ใช้บริการคลาวด์ – การสื่อสารกรณีเกิดเหตุละเมิดและแนวทางการแบ่งปันข้อมูลเพื่อช่วยในการสืบสวนและนิติเวช

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ระหว่างผู้ประมวลผลข้อมูลส่วนบุคคลบนคลาวด์และผู้ใช้บริการคลาวด์ ง) ข้อตกลงทางสัญญาต้องกำหนดความรับผิดชอบระหว่างผู้ประมวลผลข้อมูลส่วนบุคคลบนคลาวด์ ผู้รับจ้างช่วง (Sub-contractors) และผู้ใช้บริการคลาวด์อย่างชัดเจน โดยพิจารณาจากประเภทของบริการคลาวด์ (เช่น บริการประเภท IaaS, PaaS หรือ SaaS) ตัวอย่างเช่น การกำหนดความรับผิดชอบในการควบคุมระดับแอปพลิเคชันอาจแตกต่างกันขึ้นอยู่กับว่าผู้ประมวลผลข้อมูลส่วนบุคคลบนคลาวด์นั้นให้บริการ SaaS หรือ PaaS หรือ IaaS	

๕.๑.๒ โครงสร้างองค์กรด้านความมั่นคงปลอดภัยสารสนเทศ (Organization of Information Security)

๕.๑.๒.๑ บทบาทและความรับผิดชอบด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ (Information Security Roles and Responsibilities)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ใช้บริการคลาวด์ต้องมีการตกลงกับผู้ให้บริการคลาวด์เกี่ยวกับการแบ่งบทบาทหน้าที่และความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศอย่างเหมาะสม และยืนยันว่า ผู้ใช้บริการคลาวด์ สามารถทำหน้าที่และความรับผิดชอบที่จัดสรรได้ ต้องระบุบทบาทและความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศของทั้งสองฝ่ายไว้ในข้อตกลง ข) ผู้ใช้บริการคลาวด์ต้องระบุและจัดการความสัมพันธ์กับส่วนงานที่เกี่ยวกับการสนับสนุนลูกค้าและฟังก์ชันการดูแลของผู้ให้บริการคลาวด์	ก) ผู้ให้บริการคลาวด์ต้องตกลงและบันทึกการแบ่งบทบาทหน้าที่และความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศอย่างเหมาะสมกับ ผู้ใช้บริการคลาวด์, ผู้ให้บริการคลาวด์ และผู้ให้บริการภายนอก ข) ผู้ให้บริการคลาวด์ต้องแต่งตั้งผู้ประสานงานด้านการคุ้มครองข้อมูลส่วนบุคคล เพื่อประสานงานกับผู้ใช้บริการคลาวด์

๕.๑.๒.๒ การติดต่อกับเจ้าหน้าที่ (Contact with Authorities)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ใช้บริการคลาวด์ต้องระบุหน่วยงานที่เกี่ยวข้องกับการดำเนินการร่วมกันระหว่างผู้ใช้บริการคลาวด์และผู้ให้บริการคลาวด์	ก) ผู้ให้บริการคลาวด์ควรแจ้งให้ผู้ใช้บริการคลาวด์ทราบถึงที่ตั้งทางภูมิศาสตร์ขององค์กรที่เป็นเจ้าของผู้ให้บริการคลาวด์ และประเทศที่ผู้ให้บริการคลาวด์สามารถจัดเก็บข้อมูล ผู้ใช้บริการคลาวด์ได้

๕.๑.๓ การปฏิบัติตามกฎ ระเบียบ ข้อบังคับ (Compliance)

๕.๑.๓.๑ การระบุกฎหมายที่บังคับใช้และข้อกำหนดตามสัญญา (Identification of Applicable Legislation and Contractual Requirements)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ใช้บริการคลาวด์ต้องพิจารณาประเด็นที่ว่ากฎหมายและข้อบังคับที่เกี่ยวข้องอาจเป็นกฎหมายของเขตอำนาจศาลที่ควบคุมผู้ให้บริการคลาวด์นอกเหนือจากกฎหมายที่ควบคุมผู้ใช้บริการคลาวด์ ข) ผู้ใช้บริการคลาวด์ต้องขอหลักฐานว่าผู้ให้บริการคลาวด์ได้ปฏิบัติตามกฎระเบียบและมาตรฐานที่เกี่ยวข้องกับผู้ใช้บริการคลาวด์ โดยหลักฐานดังกล่าวอาจเป็นการรับรองที่จัดทำโดยผู้ตรวจสอบภายนอก	ก) ผู้ให้บริการคลาวด์ต้องแจ้งให้ผู้ใช้บริการคลาวด์ทราบถึงเขตอำนาจศาลทางกฎหมายที่ควบคุมบริการคลาวด์ ข) ผู้ให้บริการคลาวด์ต้องระบุข้อกำหนดทางกฎหมายที่เกี่ยวข้องของตนเอง (เช่น เกี่ยวกับการเข้ารหัสเพื่อปกป้องข้อมูลส่วนบุคคล) และต้องให้ข้อมูลนี้แก่ผู้ใช้บริการคลาวด์เมื่อได้รับการร้องขอ ค) ผู้ให้บริการคลาวด์ต้องแสดงหลักฐานให้ผู้ใช้บริการคลาวด์ทราบถึงการปฏิบัติตามกฎหมายที่บังคับใช้ในปัจจุบันและข้อกำหนดตามสัญญา

๕.๑.๓.๒ สิทธิในทรัพย์สินทางปัญญา (Intellectual Property Rights)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) การติดตั้งซอฟต์แวร์ที่ได้รับอนุญาตในเชิงพาณิชย์ในบริการคลาวด์อาจทำให้เกิดการละเมิดเงื่อนไขการอนุญาตให้ใช้สิทธิสำหรับซอฟต์แวร์ได้ ผู้ใช้บริการคลาวด์ต้องมีขั้นตอนในการระบุข้อกำหนดในการให้สิทธิการใช้งานเฉพาะระบบคลาวด์ก่อนที่จะอนุญาตให้ติดตั้งซอฟต์แวร์ที่ได้รับอนุญาตในบริการคลาวด์ และต้องให้ความสนใจเป็นพิเศษกับกรณีที่บริการคลาวด์มีความยืดหยุ่นและสามารถปรับขนาดได้ และสามารถใช้งานซอฟต์แวร์บนระบบหรือแกนประมวลผลได้มากกว่าที่อนุญาตโดยเงื่อนไขการอนุญาตให้ใช้สิทธิ	ก) ผู้ให้บริการคลาวด์ต้องกำหนดกระบวนการในการตอบสนองต่อการร้องเรียนเรื่องสิทธิในทรัพย์สินทางปัญญา

๕.๑.๓.๓ การปกป้องบันทึกข้อมูล (Protection of Records)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ใช้บริการคลาวด์ต้องขอข้อมูลจากผู้ให้บริการคลาวด์เกี่ยวกับการปกป้องบันทึกข้อมูลที่รวบรวมและจัดเก็บโดยผู้ให้บริการคลาวด์ที่เกี่ยวข้องกับการใช้บริการคลาวด์ของผู้ใช้บริการคลาวด์	ก) ผู้ให้บริการคลาวด์ต้องให้ข้อมูลแก่ผู้ใช้บริการคลาวด์เกี่ยวกับการปกป้องบันทึกข้อมูลที่รวบรวมและจัดเก็บโดยผู้ให้บริการคลาวด์ที่เกี่ยวข้องกับการใช้บริการคลาวด์ของผู้ใช้บริการคลาวด์

๕.๑.๓.๔ กฎระเบียบที่เกี่ยวกับมาตรการควบคุมการเข้ารหัสข้อมูล (Regulation of Cryptographic Controls)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ใช้บริการคลาวด์ต้องตรวจสอบให้แน่ใจว่าชุดของมาตรการควบคุมการเข้ารหัสข้อมูลที่ใช้กับการใช้บริการคลาวด์สอดคล้องกับข้อตกลง กฎหมาย และระเบียบข้อบังคับที่เกี่ยวข้อง	ก) ผู้ให้บริการคลาวด์ต้องให้คำอธิบายกับ ผู้ใช้บริการคลาวด์เกี่ยวกับมาตรการควบคุมการเข้ารหัสข้อมูลที่ดำเนินการโดยผู้ให้บริการคลาวด์ เพื่อใช้ในการทบทวนการปฏิบัติตามข้อตกลง กฎหมาย และข้อบังคับที่เกี่ยวข้อง

๕.๑.๓.๕ การทบทวนด้านการรักษาความมั่นคงปลอดภัยสารสนเทศอย่างเป็นอิสระ (Independent Review of Information Security)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ใช้บริการคลาวด์ต้องขอหลักฐานที่เป็นเอกสารว่ามีการนำมาตรการควบคุมและแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศสำหรับบริการคลาวด์ไปปฏิบัติ และมีความสอดคล้องกับที่ผู้ให้บริการคลาวด์กล่าวอ้าง ทั้งนี้ หลักฐานดังกล่าวอาจรวมถึงการรับรองมาตรฐานที่เกี่ยวข้องด้วย	ก) ผู้ให้บริการคลาวด์ต้องให้หลักฐานที่เป็นเอกสารแก่ผู้ใช้บริการคลาวด์เพื่อยืนยันข้อเรียกร้องของ ผู้ให้บริการคลาวด์ในการนำมาตรการควบคุมความมั่นคงปลอดภัยสารสนเทศและการคุ้มครองข้อมูลส่วนบุคคลไปใช้ ข) ในกรณีที่การตรวจสอบโดยผู้ใช้บริการคลาวด์แต่ละรายการไม่สามารถกระทำได้หรืออาจเพิ่มความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศได้ ผู้ให้บริการคลาวด์ต้องแสดงหลักฐานที่เป็นอิสระว่ามีการนำไปปฏิบัติและดำเนินการด้านความมั่นคงปลอดภัยสารสนเทศและการคุ้มครองข้อมูลส่วนบุคคลตามนโยบายและขั้นตอนของผู้ให้บริการคลาวด์ ทั้งนี้ ผู้ให้บริการคลาวด์ต้องแสดงหลักฐานดังกล่าวให้กับผู้ที่คาดว่าจะเป็น ผู้ใช้บริการคลาวด์ก่อนเข้าทำสัญญา โดยปกติแล้วการตรวจสอบอิสระที่เกี่ยวข้องตามที่ผู้ให้บริการคลาวด์เลือก ควรเป็นวิธีการที่เป็นที่ยอมรับเพื่อตอบสนองความต้องการของ ผู้ใช้บริการคลาวด์ ในการตรวจสอบการดำเนินงานของ ผู้ให้บริการคลาวด์ หากมีความโปร่งใสเพียงพอ เมื่อการตรวจสอบที่เป็นอิสระไม่สามารถทำได้ ผู้ให้บริการคลาวด์ ต้องทำการประเมินตนเอง และเปิดเผยกระบวนการและผลลัพธ์ต่อผู้ใช้บริการคลาวด์

๕.๒ การปฏิบัติการและการรักษาความมั่นคงปลอดภัยโครงสร้างพื้นฐานระบบคลาวด์ (Cloud Infrastructure Security and Operation)

๕.๒.๑ การบริหารทรัพยากรมนุษย์ (Human Resource Security)

๕.๒.๑.๑ การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศ การศึกษาและการฝึกอบรม (Information Security Awareness, Education and Training)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ใช้บริการคลาวด์ ต้องเพิ่มรายการต่อไปนี้ในโปรแกรมสร้างความตระหนักรู้ การศึกษา และการฝึกอบรมสำหรับผู้จัดการธุรกิจบริการคลาวด์ ผู้ดูแลระบบบริการคลาวด์ ผู้ประกอบบริการคลาวด์ และผู้ใช้บริการคลาวด์ รวมถึงพนักงานและผู้รับจ้างที่เกี่ยวข้อง – มาตรฐานและขั้นตอนการใช้บริการคลาวด์ – ความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องกับบริการคลาวด์และวิธีการจัดการความเสี่ยงเหล่านั้น – ความเสี่ยงด้านสภาพแวดล้อมของระบบและเครือข่ายจากการใช้บริการคลาวด์ – การคุ้มครองข้อมูลส่วนบุคคล – ข้อพิจารณาทางกฎหมายและข้อบังคับที่เกี่ยวข้อง ข) ต้องจัดให้มีโปรแกรมการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศ การศึกษา และการฝึกอบรมเกี่ยวกับบริการคลาวด์แก่ผู้บริหารและผู้จัดการที่กำกับดูแล รวมถึงหน่วยงานธุรกิจ (Business Units)	ก) ผู้ให้บริการคลาวด์ ต้องสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศและด้านการคุ้มครองข้อมูลส่วนบุคคล การศึกษาและการฝึกอบรมแก่พนักงาน รวมทั้งให้ผู้รับจ้างดำเนินการเช่นเดียวกันเกี่ยวกับการจัดการข้อมูลของผู้ใช้บริการคลาวด์ และข้อมูลที่ได้จากบริการคลาวด์อย่างเหมาะสม โดยข้อมูลนี้อาจมีข้อมูลที่เป็นความลับต่อผู้ใช้บริการคลาวด์หรืออยู่ภายใต้ข้อจำกัดเฉพาะ รวมถึงข้อจำกัดด้านกฎระเบียบในการเข้าถึงและใช้งานโดย ผู้ให้บริการคลาวด์

๕.๒.๒ การจัดการทรัพย์สิน (Asset Management)

๕.๒.๒.๑ ทะเบียนทรัพย์สิน (Inventory of Assets)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ทะเบียนทรัพย์สินของผู้ใช้บริการคลาวด์ต้องคำนึงถึงข้อมูลและทรัพย์สินที่เกี่ยวข้องซึ่งจัดเก็บในสภาพแวดล้อมการประมวลผลบนคลาวด์ ทั้งนี้ บันทึกทะเบียนทรัพย์สินต้องระบุสถานที่จัดเก็บทรัพย์สิน เช่น ชื่อของผู้ให้บริการคลาวด์	ก) ทะเบียนทรัพย์สินของผู้ให้บริการคลาวด์ต้องระบุอย่างชัดเจนในเรื่อง - ข้อมูลของผู้ใช้บริการคลาวด์ - ข้อมูลที่เกิดจากการใช้บริการคลาวด์

๕.๒.๒.๒ การบ่งชี้ข้อมูล (Labelling of Information)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ใช้บริการคลาวด์ต้องบ่งชี้ข้อมูลและทรัพย์สินขององค์กรที่ใช้งานหรือเก็บรักษาไว้บนระบบคลาวด์ตามขั้นตอนปฏิบัติสำหรับการบ่งชี้ข้อมูลขององค์กร	ก) ผู้ให้บริการคลาวด์ต้องจัดทำเอกสารและเปิดเผยฟังก์ชันการทำงานของบริการใด ๆ ที่ผู้ใช้บริการคลาวด์ สามารถนำไปใช้เพื่อการบ่งชี้ข้อมูลและทรัพย์สินที่เกี่ยวข้องได้

๕.๒.๓ การควบคุมการเข้าถึง (Access Control)

๕.๒.๓.๑ การควบคุมเข้าถึงเครือข่ายและบริการเครือข่าย (Access to Networks and Network Services)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) นโยบายการควบคุมการเข้าถึงของผู้ใช้บริการคลาวด์สำหรับการใช้บริการเครือข่ายต้องระบุข้อกำหนดสำหรับผู้ใช้งานในการเข้าถึงบริการคลาวด์ตามแต่ละบริการที่ใช้งาน	

๕.๒.๓.๒ การลงทะเบียนและยกเลิกการลงทะเบียนสำหรับผู้ใช้ (User Registration and Deregistration)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ขั้นตอนการลงทะเบียนและยกเลิกการลงทะเบียนสำหรับผู้ใช้ต้องครอบคลุมถึงสถานการณ์ที่การควบคุมการเข้าถึงของผู้ใช้ถูกคุกคาม เช่น การที่รหัสผ่านหรือข้อมูลการลงทะเบียนผู้ใช้อื่น ๆ (ยกตัวอย่างเช่นจากการเปิดเผยโดยไม่ได้ตั้งใจ) ถูกทำให้เสียหายหรือถูกคุกคาม	ก) เพื่อจัดการการเข้าถึงบริการคลาวด์โดยผู้ใช้งานของผู้ใช้บริการคลาวด์ ผู้ให้บริการคลาวด์ต้องจัดเตรียมฟังก์ชันการลงทะเบียนและการยกเลิกการลงทะเบียนผู้ใช้งาน รวมถึงข้อกำหนดสำหรับการใช้งานฟังก์ชันเหล่านี้แก่ ผู้ใช้บริการคลาวด์

๕.๒.๓.๓ การจัดสรรการเข้าถึงของผู้ใช้ (User Access Provisioning)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
	ก) ผู้ให้บริการคลาวด์ต้องจัดเตรียมฟังก์ชันสำหรับการจัดการสิทธิการเข้าถึงของผู้ใช้บริการคลาวด์ รวมถึงข้อกำหนดสำหรับการใช้งานฟังก์ชันเหล่านี้

๕.๒.๓.๔ การจัดการสิทธิการเข้าถึงที่ได้รับสิทธิพิเศษ (Management of Privileged Access Rights)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ใช้บริการคลาวด์ต้องใช้เทคนิคการยืนยันตัวตนที่เพียงพอ (เช่น การยืนยันตัวตนแบบหลายปัจจัย) สำหรับการตรวจสอบสิทธิของผู้ดูแลระบบบริการคลาวด์ของ ผู้ใช้บริการคลาวด์ ให้มีความสามารถในการจัดการบริการคลาวด์ที่สอดคล้องตามความเสี่ยงที่ระบุไว้	ก) ผู้ให้บริการคลาวด์ต้องมีเทคนิคการยืนยันตัวตนที่เพียงพอ (เช่น การยืนยันตัวตนแบบหลายปัจจัย) สำหรับการตรวจสอบสิทธิของผู้ดูแลระบบบริการคลาวด์ของผู้ใช้บริการคลาวด์ ให้มีความสามารถในการบริหารจัดการระบบคลาวด์ ที่สอดคล้องตามความเสี่ยงที่ระบุไว้

๕.๒.๓.๕ การจัดการข้อมูลการพิสูจน์ตัวตนที่เป็นความลับของผู้ใช้ (Management of Secret Authentication Information of Users)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ใช้บริการคลาวด์ต้องตรวจสอบว่ากระบวนการจัดการของผู้ให้บริการคลาวด์สำหรับการจัดสรรข้อมูลการตรวจสอบความลับ (Secret Authentication Information) เช่น รหัสผ่าน เป็นไปตามข้อกำหนดของผู้ใช้บริการคลาวด์	ก) ผู้ให้บริการคลาวด์ต้องให้ข้อมูลเกี่ยวกับขั้นตอนการจัดการข้อมูลการตรวจสอบความลับ (Secret Authentication Information) ของผู้ใช้บริการคลาวด์ รวมถึงขั้นตอนในการจัดสรรข้อมูลดังกล่าวสำหรับการตรวจสอบสิทธิผู้ใช้งาน

๕.๒.๓.๖ การจำกัดการเข้าถึงข้อมูล (Information Access Restriction)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ใช้บริการคลาวด์ต้องตรวจสอบให้แน่ใจว่าสามารถจำกัดการเข้าถึงข้อมูลในบริการคลาวด์ได้ตามนโยบายการควบคุมการเข้าถึงและปฏิบัติตามข้อจำกัดดังกล่าว ซึ่งรวมถึงการจำกัดการเข้าถึงบริการต่าง ๆ บนระบบคลาวด์ และข้อมูล ผู้ใช้บริการคลาวด์ที่เก็บไว้ในบริการ	ก) ผู้ให้บริการคลาวด์ต้องให้การควบคุมการเข้าถึงที่อนุญาตให้กับผู้ใช้บริการคลาวด์ เพื่อจำกัดการเข้าถึงบริการต่าง ๆ บนระบบคลาวด์ และข้อมูลผู้ใช้บริการคลาวด์ที่เก็บไว้ในบริการ

๕.๒.๓.๗ การใช้โปรแกรมอรรถประโยชน์พิเศษ (Use of Privilege Utility Programs)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) หากอนุญาตให้ใช้โปรแกรมอรรถประโยชน์ได้ ผู้ใช้บริการคลาวด์ต้องระบุโปรแกรมอรรถประโยชน์ที่จะใช้ในสภาพแวดล้อมการประมวลผลบนคลาวด์ และตรวจสอบให้มั่นใจว่าโปรแกรมเหล่านั้น ไม่รบกวนการควบคุมของบริการคลาวด์	ก) ผู้ให้บริการคลาวด์ต้องระบุข้อกำหนดสำหรับโปรแกรมอรรถประโยชน์ใด ๆ ที่ใช้ในบริการคลาวด์ ผู้ให้บริการคลาวด์ต้องตรวจสอบให้มั่นใจว่าการใช้โปรแกรมอรรถประโยชน์ใด ๆ ที่สามารถข้ามขั้นตอนการทำงานตามปกติหรือการรักษาความปลอดภัยนั้น จำกัดเฉพาะบุคลากรที่ได้รับอนุญาตเท่านั้น และต้องมีการทบทวนและตรวจสอบการใช้โปรแกรมดังกล่าวอย่างสม่ำเสมอ

๕.๒.๓.๘ ขั้นตอนการเข้าสู่ระบบอย่างปลอดภัย (Secure Log-on Procedures)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ใช้บริการคลาวด์ต้องกำหนดให้ผู้ใช้ที่อยู่ภายใต้การควบคุมของผู้ใช้บริการคลาวด์ปฏิบัติตามขั้นตอนการเข้าสู่ระบบอย่างปลอดภัยสำหรับบัญชีใด ๆ	ก) ในกรณีที่จำเป็น ผู้ให้บริการคลาวด์ต้องจัดให้มีขั้นตอนการเข้าสู่ระบบอย่างปลอดภัยสำหรับบัญชีใด ๆ ที่ผู้ใช้บริการคลาวด์ร้องขอสำหรับผู้ใช้ที่อยู่ภายใต้การควบคุมของผู้ใช้บริการคลาวด์

๕.๒.๔ การเข้ารหัส (Cryptography)

๕.๒.๔.๑ นโยบายเกี่ยวกับการใช้มาตรการควบคุมการเข้ารหัส (Policy on the Use of Cryptographic Controls)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ใช้บริการคลาวด์ต้องใช้มาตรการควบคุมการเข้ารหัสสำหรับการใช้บริการระบบคลาวด์ที่มีความแข็งแรงเพียงพอ และสอดคล้องตามความเสี่ยงที่ได้ระบุไว้ ไม่ว่าผู้ใช้บริการคลาวด์หรือผู้ให้บริการคลาวด์จะเป็นผู้จัดหามาตรการควบคุมการเข้ารหัสเหล่านั้นก็ตาม ข) เมื่อผู้ให้บริการคลาวด์นำเสนอการเข้ารหัสใด ๆ ผู้ใช้บริการคลาวด์ต้องตรวจสอบข้อมูลที่ผู้ให้บริการคลาวด์จัดหาให้เพื่อยืนยันว่ามีความสามารถในการเข้ารหัสดังนี้หรือไม่ – ปฏิบัติตามข้อกำหนดด้านนโยบายของ ผู้ใช้บริการคลาวด์ – เข้ากันได้กับการป้องกันการเข้ารหัสลับอื่น ๆ ที่ใช้โดยผู้ใช้บริการคลาวด์ – ใช้กับข้อมูลขณะจัดเก็บและระหว่างโอนถ่ายภายในบริการคลาวด์และนอกระบบคลาวด์	ก) ผู้ให้บริการคลาวด์ต้องให้ข้อมูลแก่ผู้ใช้บริการคลาวด์เกี่ยวกับการเข้ารหัสเพื่อปกป้องข้อมูลและข้อมูลส่วนบุคคล ที่ผู้ให้บริการคลาวด์ประมวลผล นอกจากนี้ ผู้ให้บริการคลาวด์ต้องให้ข้อมูลแก่ผู้ใช้บริการคลาวด์เกี่ยวกับความสามารถใด ๆ ที่ผู้ให้บริการคลาวด์มอบให้ซึ่งสามารถช่วยผู้ใช้บริการคลาวด์ในการใช้การเข้ารหัสดังกล่าว

๕.๒.๔.๒ การจัดการกุญแจ (Key Management)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ใช้บริการคลาวด์ต้องระบุกุญแจสำหรับการเข้ารหัสในแต่ละบริการคลาวด์ และดำเนินการตามขั้นตอนสำหรับการจัดการกุญแจ ข) ในกรณีที่บริการคลาวด์มีฟังก์ชันการจัดการกุญแจสำหรับการใช้งานโดยผู้ใช้บริการคลาวด์ ผู้ใช้บริการคลาวด์ต้องขอข้อมูลดังต่อไปนี้เกี่ยวกับขั้นตอนที่ใช้ในการจัดการกุญแจสำหรับการเข้ารหัสที่เกี่ยวข้องกับบริการคลาวด์ – ประเภทของกุญแจ	

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
– ข้อกำหนดเฉพาะของระบบการจัดการ รวมถึงขั้นตอนต่าง ๆ ตลอดอายุการใช้งานของกุญแจเข้ารหัส เช่น การสร้าง เปลี่ยนแปลง หรือปรับปรุง จัดเก็บ หมดอายุการใช้งาน เรียกคืน เก็บรักษา และทำลาย – ขั้นตอนการจัดการกุญแจที่แนะนำสำหรับการใช้งานโดยผู้ใช้บริการคลาวด์ ค) ผู้ใช้บริการคลาวด์ต้องไม่อนุญาตให้ ผู้ให้บริการคลาวด์ จัดเก็บและจัดการกุญแจสำหรับการเข้ารหัสเมื่อผู้ใช้บริการคลาวด์ ใช้กุญแจเข้ารหัสของตนเอง	

๕.๒.๕ การรักษาความปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and Environment Security)

๕.๒.๕.๑ ตำแหน่งของศูนย์ข้อมูล (Data Center Location)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ต้องใช้ศูนย์ข้อมูลหลักในประเทศไทย (Data Localization)	ก) ต้องจัดตั้งศูนย์ข้อมูลหลักในประเทศไทย (Data Localization) ข) ต้องจัดตั้งศูนย์ข้อมูลสำรองในประเทศไทย (Data Localization) หรือ อยู่ในภูมิภาคเอเชียตะวันออกเฉียงใต้ที่ใกล้กับการใช้งานหลักของผู้ใช้บริการคลาวด์ให้มากที่สุด รวมถึงสิงคโปร์และเขตปกครองพิเศษฮ่องกง

๕.๒.๕.๒ การกำจัดหรือนำอุปกรณ์กลับมาใช้ใหม่อย่างปลอดภัย (Secure Disposal or Reuse of Equipment)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ใช้บริการคลาวด์ต้องร้องขอการยืนยันว่าผู้ให้บริการคลาวด์มีนโยบายและขั้นตอนในการกำจัดหรือนำทรัพยากรกลับมาใช้ใหม่อย่างปลอดภัย	ก) ผู้ให้บริการคลาวด์ต้องตรวจสอบให้แน่ใจว่ามีการเตรียมการสำหรับการกำจัดหรือนำทรัพยากร (เช่น อุปกรณ์ ที่เก็บข้อมูล ไฟล์ หน่วยความจำ) กลับมาใช้ใหม่อย่างปลอดภัยและทันท่วงที ข) เพื่อวัตถุประสงค์ในการกำจัดหรือนำกลับมาใช้ใหม่อย่างมั่นคงปลอดภัย และไม่สามารถกู้คืนข้อมูลกลับมาได้ อุปกรณ์ที่มีสื่อจัดเก็บข้อมูลที่อาจมีข้อมูลส่วนบุคคลต้องได้รับการปฏิบัติเสมือนว่ามีข้อมูลส่วนบุคคลจริง

๕.๒.๖ การรักษาความมั่นคงปลอดภัยการปฏิบัติการ (Operations Security)

๕.๒.๖.๑ การจัดการการเปลี่ยนแปลง (Change Management)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) กระบวนการจัดการการเปลี่ยนแปลงของผู้ใช้บริการคลาวด์ ต้องคำนึงถึงผลกระทบของการเปลี่ยนแปลงใด ๆ ที่เกิดขึ้นจาก ผู้ให้บริการคลาวด์	ก) ผู้ให้บริการคลาวด์ ต้องให้ข้อมูลแก่ ผู้ใช้บริการคลาวด์ เกี่ยวกับการเปลี่ยนแปลงในบริการคลาวด์ที่อาจส่งผลเสียต่อบริการคลาวด์ ข้อมูลต่อไปนี้จะช่วยให้ ผู้ใช้บริการคลาวด์ ระบุถึงผลกระทบของการเปลี่ยนแปลงที่อาจมีผลต่อความมั่นคงปลอดภัยสารสนเทศ – ประเภทของการเปลี่ยนแปลง – วันที่และเวลาที่วางแผนไว้ของการเปลี่ยนแปลง – คำอธิบายทางเทคนิคเกี่ยวกับการเปลี่ยนแปลงของบริการคลาวด์และระบบที่เกี่ยวข้อง (Underlying Systems) – การแจ้งเตือนการเริ่มต้นและการเปลี่ยนแปลงที่เสร็จสมบูรณ์ ข) เมื่อ ผู้ให้บริการคลาวด์ ให้บริการคลาวด์ที่ขึ้นอยู่กับผู้ให้บริการรายย่อยของ ผู้ให้บริการคลาวด์ ผู้ให้บริการคลาวด์ อาจจำเป็นต้องแจ้งการเปลี่ยนแปลงที่เกิดขึ้นให้ ผู้ใช้บริการคลาวด์ ทราบ

๕.๒.๖.๒ การบริหารจัดการความจุ (Capacity Management)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ใช้บริการคลาวด์ ต้องตรวจสอบให้แน่ใจว่าขีดความสามารถของทรัพยากรที่ตกลงกันไว้ในบริการคลาวด์นั้นตรงตามข้อกำหนดของ ผู้ใช้บริการคลาวด์ ข) ผู้ใช้บริการคลาวด์ ต้องตรวจสอบการใช้บริการคลาวด์และคาดการณ์ความต้องการด้านขีดความสามารถของทรัพยากรของบริการคลาวด์เพื่อให้มั่นใจในประสิทธิภาพของบริการคลาวด์เมื่อเวลาผ่านไป	ก) ผู้ให้บริการคลาวด์ ต้องตรวจสอบขีดความสามารถของทรัพยากรทั้งหมดเพื่อป้องกันไม่ให้เกิดเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่เกิดจากการขาดแคลนทรัพยากร

๕.๒.๖.๓ การสำรองข้อมูล (Information Backup)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ในกรณีที่ ผู้ให้บริการคลาวด์ มีความสามารถในการสำรองข้อมูลซึ่งเป็นส่วนหนึ่งของบริการคลาวด์ ผู้ใช้บริการคลาวด์ ต้องขอข้อมูลจำเพาะของความสามารถในการสำรองข้อมูลจาก ผู้ให้บริการคลาวด์ นอกจากนี้ ผู้ใช้บริการคลาวด์	ก) ผู้ให้บริการคลาวด์ ต้องให้ข้อมูลจำเพาะของความสามารถในการสำรองข้อมูลแก่ ผู้ใช้บริการคลาวด์ ข้อมูลจำเพาะควรมีข้อมูลต่อไปนี้ตามความเหมาะสม – ขอบเขตและกำหนดการของการสำรองข้อมูล

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ต้องทำการตรวจสอบเพื่อให้แน่ใจว่าเป็นไปตามข้อกำหนดในการสำรองข้อมูลหรือไม่ ข) ผู้ใช้บริการคลาวด์ มีหน้าที่รับผิดชอบในการดำเนินการสำรองข้อมูลเมื่อ ผู้ให้บริการคลาวด์ ไม่ได้ให้บริการนี้	– วิธีการสำรองข้อมูลและรูปแบบข้อมูล รวมถึงวิธีการเข้ารหัส หากมีความเกี่ยวข้อง – ระยะเวลาเก็บรักษาข้อมูลสำรอง – ขั้นตอนการตรวจสอบความสมบูรณ์ของข้อมูลสำรอง – ขั้นตอนและระยะเวลาที่เกี่ยวข้องกับการกู้คืนข้อมูลจากการสำรองข้อมูล – ขั้นตอนในการทดสอบความสามารถในการสำรองข้อมูล – สถานที่จัดเก็บข้อมูลสำรอง ข) ผู้ให้บริการคลาวด์ ต้องให้บริการการเข้าถึงข้อมูลสำรองที่ปลอดภัยและแยกออกจากกัน หากบริการดังกล่าวมีการนำเสนอให้ ผู้ใช้บริการคลาวด์

๕.๒.๖.๔ การบันทึกเหตุการณ์ (Event Logging)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ใช้บริการคลาวด์ ต้องจัดทำข้อกำหนดสำหรับการบันทึกเหตุการณ์และตรวจสอบว่าบริการคลาวด์ตรงตามข้อกำหนดเหล่านั้นหรือไม่	ก) ผู้ให้บริการคลาวด์ ต้องให้ผู้ใช้บริการสามารถบันทึกเหตุการณ์ ข) ในกรณีที่เป็นไปได้ บันทึกเหตุการณ์ควรบันทึกว่าข้อมูลส่วนบุคคลได้รับการเปลี่ยนแปลงหรือไม่ (เพิ่ม แก้ไข หรือลบ) จากเหตุการณ์นั้น และโดยใคร (Audit Log) ในกรณีที่มีผู้ให้บริการหลายรายเข้ามาเกี่ยวข้องในการให้บริการจากหลากหลายประเภทบริการของสถาปัตยกรรมอ้างอิงประมวลผลคลาวด์ อาจมีบทบาทที่แตกต่างหรือแบ่งปันกันในการปฏิบัติตามข้อนี้

๕.๒.๖.๕ การปกป้องข้อมูลในบันทึกเหตุการณ์ (Protection of Log information)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ข้อมูลที่บันทึกไว้ในบันทึกเหตุการณ์เพื่อวัตถุประสงค์ต่าง ๆ เช่น การตรวจสอบความปลอดภัยและการวินิจฉัยการทำงาน อาจมีข้อมูลส่วนบุคคลอยู่ด้วย จึงต้องมีมาตรการ เช่น การควบคุมการเข้าถึง เพื่อให้มั่นใจว่าข้อมูลที่บันทึกไว้ในบันทึกเหตุการณ์จะถูกนำไปใช้ตามวัตถุประสงค์ที่ตั้งไว้เท่านั้น ข) ต้องมีขั้นตอนการดำเนินการ ซึ่งดีที่สุดคือเป็นระบบอัตโนมัติ เพื่อให้มั่นใจว่าข้อมูลที่บันทึกไว้ใน	ก) ข้อมูลที่บันทึกไว้ในบันทึกเหตุการณ์เพื่อวัตถุประสงค์ต่าง ๆ เช่น การตรวจสอบความปลอดภัยและการวินิจฉัยการทำงาน อาจมีข้อมูลส่วนบุคคลอยู่ด้วย จึงต้องมีมาตรการ เช่น การควบคุมการเข้าถึง เพื่อให้มั่นใจว่าข้อมูลที่บันทึกไว้ในบันทึกเหตุการณ์จะถูกนำไปใช้ตามวัตถุประสงค์ที่ตั้งไว้เท่านั้น ข) ต้องมีขั้นตอนการดำเนินการ ซึ่งดีที่สุดคือเป็นระบบอัตโนมัติ เพื่อให้มั่นใจว่าข้อมูลที่บันทึกไว้ใน

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
บันทึกเหตุการณ์จะถูกลบภายในระยะเวลาที่กำหนด (Log Retention) และเอกสารระบุไว้	บันทึกเหตุการณ์จะถูกลบภายในระยะเวลาที่กำหนด (Log Retention) และเอกสารระบุไว้

๕.๒.๖.๖ บันทึกเหตุการณ์ของผู้ดูแลระบบและผู้ปฏิบัติงาน (Administrator and Operator Logs)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) หากมีการให้สิทธิพิเศษให้แก่ ผู้ใช้บริการคลาวด์ การใช้สิทธิพิเศษนั้นต้องมีการบันทึกเหตุการณ์และประสิทธิภาพของการดำเนินการเหล่านั้น ผู้ใช้บริการคลาวด์ ต้องพิจารณาว่าความสามารถในการบันทึกเหตุการณ์ที่ ผู้ให้บริการคลาวด์ จัดหาให้นั้นเหมาะสมหรือไม่ หรือ ผู้ใช้บริการคลาวด์ ต้องใช้ความสามารถในการบันทึกเหตุการณ์เพิ่มเติมหรือไม่	

๕.๒.๖.๗ การซิงโครไนซ์นาฬิกา (Clock Synchronization)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ใช้บริการคลาวด์ต้องขอข้อมูลเกี่ยวกับการซิงโครไนซ์นาฬิกาที่ใช้ในระบบของผู้ให้บริการคลาวด์	ก) ผู้ให้บริการคลาวด์ต้องให้ข้อมูลแก่ผู้ใช้บริการคลาวด์เกี่ยวกับนาฬิกาที่ระบบของผู้ให้บริการคลาวด์ใช้และข้อมูลเกี่ยวกับวิธีที่ผู้ใช้บริการคลาวด์สามารถซิงโครไนซ์นาฬิกาภายในกับนาฬิกาในบริการคลาวด์

๕.๒.๖.๘ การจัดการช่องโหว่ทางเทคนิค (Management of Technical Vulnerabilities)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ใช้บริการคลาวด์ ต้องขอข้อมูลจาก ผู้ให้บริการคลาวด์ เกี่ยวกับการจัดการช่องโหว่ทางเทคนิคที่อาจส่งผลกระทบต่อบริการคลาวด์ที่ให้บริการ ผู้ใช้บริการคลาวด์ ต้องระบุช่องโหว่ทางเทคนิคที่ผู้ใช้บริการคลาวด์ จะเป็นผู้รับผิดชอบในการจัดการและกำหนดกระบวนการในการจัดการให้ชัดเจน	ก) ผู้ให้บริการคลาวด์ ต้องให้ข้อมูล ผู้ใช้บริการคลาวด์ เกี่ยวกับการจัดการช่องโหว่ทางเทคนิคที่อาจส่งผลกระทบต่อบริการคลาวด์ที่ให้บริการ

๕.๒.๖.๙ การแยกสภาพแวดล้อมสำหรับการพัฒนา การทดสอบ และการปฏิบัติงาน (Separation of Development, Testing and Operational Environments)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ในกรณีที่ไม่สามารถหลีกเลี่ยงการใช้ข้อมูลส่วนบุคคลสำหรับวัตถุประสงค์ในการทดสอบได้ ต้องมีการประเมินความเสี่ยง มาตรการด้านเทคนิคและการจัดการองค์กรต้องถูกนำมาใช้เพื่อลดความเสี่ยงที่ระบุไว้ให้น้อยที่สุด	ก) ในกรณีที่ไม่สามารถหลีกเลี่ยงการใช้ข้อมูลส่วนบุคคลสำหรับวัตถุประสงค์ในการทดสอบได้ ต้องมีการประเมินความเสี่ยง มาตรการด้านเทคนิคและการจัดการองค์กรต้องถูกนำมาใช้เพื่อลดความเสี่ยงที่ระบุไว้ให้น้อยที่สุด

๕.๒.๗ การรักษาความมั่นคงปลอดภัยเครือข่าย (Communication Security)

๕.๒.๗.๑ นโยบายและขั้นตอนปฏิบัติในการถ่ายโอนข้อมูล (Information Transfer Policies and Procedures)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) เมื่อใดก็ตามที่มีการใช้สื่อทางกายภาพสำหรับการถ่ายโอนข้อมูล ต้องมีระบบที่จะบันทึกสื่อทางกายภาพที่เข้ามาและออกไปซึ่งมีข้อมูลส่วนบุคคล รวมถึงประเภทของสื่อทางกายภาพ ผู้ส่ง/ผู้รับที่ได้รับอนุญาต วันที่และเวลา และจำนวนสื่อทางกายภาพ ข) ผู้ใช้บริการคลาวด์ต้องขอให้ผู้ให้บริการคลาวด์ใช้มาตรการเพิ่มเติม (เช่น การเข้ารหัส) เพื่อให้มั่นใจว่าข้อมูลสามารถเข้าถึงได้เฉพาะจุดปลายทางเท่านั้น ไม่ใช่ระหว่างทาง	ก) เมื่อใดก็ตามที่มีการใช้สื่อทางกายภาพสำหรับการถ่ายโอนข้อมูล ต้องมีระบบที่จะบันทึกสื่อทางกายภาพที่เข้ามาและออกไปซึ่งมีข้อมูลส่วนบุคคล รวมถึงประเภทของสื่อทางกายภาพ ผู้ส่ง/ผู้รับที่ได้รับอนุญาต วันที่และเวลา และจำนวนสื่อทางกายภาพ ข) หากเป็นไปได้ ต้องขอให้ผู้ใช้บริการคลาวด์ใช้มาตรการเพิ่มเติม (เช่น การเข้ารหัส) เพื่อให้มั่นใจว่าข้อมูลสามารถเข้าถึงได้เฉพาะจุดปลายทางเท่านั้น ไม่ใช่ระหว่างทาง

๕.๒.๗.๒ การแบ่งแยกในเครือข่าย (Segregation in Networks)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ใช้บริการคลาวด์ ต้องจัดทำข้อกำหนดสำหรับการแยกเครือข่ายเพื่อให้เกิดการแยกผู้เช่า (Tenant) ในสภาพแวดล้อมที่เป็นการใช้บริการคลาวด์ร่วมกัน และตรวจสอบว่า ผู้ให้บริการคลาวด์ มีคุณสมบัติตรงตามข้อกำหนดเหล่านั้นหรือไม่	ก) ผู้ให้บริการคลาวด์ ต้องบังคับใช้การแยกการเข้าถึงเครือข่ายในกรณีต่อไปนี้ – การแบ่งแยกระหว่างผู้เช่าในสภาพแวดล้อมที่มีผู้เช่าหลายราย – การแยกระหว่างสภาพแวดล้อมการดูแลระบบภายในของ ผู้ให้บริการคลาวด์ และสภาพแวดล้อมการประมวลผลบนคลาวด์ของ ผู้ใช้บริการคลาวด์ ข) ผู้ให้บริการคลาวด์ ต้องช่วย ผู้ใช้บริการคลาวด์ตรวจสอบการแบ่งแยกที่ดำเนินการโดยผู้ให้บริการคลาวด์

๕.๒.๘ การจัดหา การพัฒนา และการบำรุงรักษา (System Acquisition, Development, and Maintenance)

๕.๒.๘.๑ การวิเคราะห์และข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Requirements Analysis and Specification)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ใช้บริการคลาวด์ ต้องกำหนดข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศสำหรับการใช้บริการคลาวด์ จากนั้นประเมินว่าบริการของผู้ให้บริการคลาวด์ สามารถตอบสนองความต้องการเหล่านี้ได้หรือไม่	ก) ผู้ให้บริการคลาวด์ ต้องให้ข้อมูลแก่ ผู้ใช้บริการคลาวด์ เกี่ยวกับความสามารถในการรักษาความมั่นคงปลอดภัยสารสนเทศที่ตนใช้ ข้อมูลนี้ต้องเป็นข้อมูลโดยไม่เปิดเผยข้อมูลที่อาจเป็นประโยชน์ต่อบุคคลที่มีเจตนาร้าย

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ข) สำหรับการประเมินนี้ ผู้ใช้บริการคลาวด์ ต้องขอข้อมูลเกี่ยวกับความสามารถในการรักษาความมั่นคงปลอดภัยสารสนเทศจาก ผู้ให้บริการคลาวด์	

๕.๒.๘.๒ นโยบายการพัฒนาที่ปลอดภัย (Secure Development Policy)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ใช้บริการคลาวด์ ต้องขอข้อมูลจาก ผู้ให้บริการคลาวด์ เกี่ยวกับการใช้ขั้นตอนและวิธีปฏิบัติในการพัฒนาที่ปลอดภัยของ ผู้ให้บริการคลาวด์	ก) ผู้ให้บริการคลาวด์ ต้องให้ข้อมูลเกี่ยวกับการใช้ขั้นตอนและวิธีปฏิบัติในการพัฒนาความปลอดภัยของตนในขอบเขตที่สอดคล้องกับนโยบายในการเปิดเผยข้อมูล

๕.๒.๙ การจัดการผู้ให้บริการภายนอก (Supplier Relationships)

๕.๒.๙.๑ นโยบายความมั่นคงปลอดภัยสารสนเทศสำหรับความสัมพันธ์กับผู้ให้บริการภายนอก (Information Security Policy for Supplier Relationships)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ใช้บริการคลาวด์ ต้องระบุว่า ผู้ให้บริการคลาวด์เป็นผู้ให้บริการภายนอกประเภทหนึ่งในนโยบายความมั่นคงปลอดภัยสารสนเทศสำหรับความสัมพันธ์กับผู้ให้บริการภายนอก ซึ่งจะช่วยลดความเสี่ยงที่เกี่ยวข้องกับการเข้าถึงและจัดการข้อมูล ผู้ใช้บริการคลาวด์ ของ ผู้ให้บริการคลาวด์	

๕.๒.๙.๒ การจัดการกับการรักษาความมั่นคงปลอดภัยภายในข้อตกลงของผู้ให้บริการภายนอก (Addressing Security within Supplier Agreements)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ใช้บริการคลาวด์ ต้องยืนยันบทบาทและความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องกับบริการคลาวด์ ดังที่อธิบายไว้ในข้อตกลงการให้บริการ สิ่งเหล่านี้อาจรวมถึงกระบวนการต่อไปนี้ – การป้องกันมัลแวร์ – การสำรองข้อมูล – มาตรการควบคุมการเข้ารหัส – การจัดการช่องโหว่ – การจัดการเหตุการณ์ – การตรวจสอบการปฏิบัติตามข้อกำหนดทางเทคนิค – การทดสอบความปลอดภัย	ก) ผู้ให้บริการคลาวด์ ต้องระบุมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องซึ่งผู้ให้บริการคลาวด์ จะนำมาใช้เป็นส่วนหนึ่งของข้อตกลงเพื่อให้แน่ใจว่าจะไม่เกิดความเข้าใจผิดระหว่าง ผู้ให้บริการคลาวด์ และ ผู้ใช้บริการคลาวด์ สิ่งเหล่านี้อาจรวมถึงกระบวนการต่อไปนี้ – การป้องกันมัลแวร์ – การสำรองข้อมูล – มาตรการควบคุมการเข้ารหัส – การจัดการช่องโหว่ – การจัดการเหตุการณ์ – การตรวจสอบการปฏิบัติตามข้อกำหนดทางเทคนิค

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
– การตรวจสอบ – การรวบรวม การบำรุงรักษา และการปกป้องหลักฐาน รวมถึงบันทึกและเส้นทางการตรวจสอบ – การปกป้องข้อมูลเมื่อสิ้นสุดข้อตกลงการให้บริการ – การยืนยันตัวตน และการควบคุมการเข้าถึง – การจัดการข้อมูลประจำตัวและการเข้าถึง	– การทดสอบความปลอดภัย – การตรวจสอบ – การรวบรวม การบำรุงรักษา และการปกป้องหลักฐาน รวมถึงบันทึกและเส้นทางการตรวจสอบ – การปกป้องข้อมูลเมื่อสิ้นสุดข้อตกลงการให้บริการ – การยืนยันตัวตน และการควบคุมการเข้าถึง – การจัดการข้อมูลประจำตัวและการเข้าถึง ข) มาตรการรักษาความมั่นคงปลอดภัยสารสนเทศที่ผู้ให้บริการคลาวด์ จะใช้อาจแตกต่างกันออกไปตามประเภทของบริการคลาวด์ที่ ผู้ใช้บริการคลาวด์ใช้งานอยู่

๕.๒.๙.๓ ห่วงโซ่อุปทานของเทคโนโลยีสารสนเทศและการสื่อสาร (Information and Communication Technology Supply Chain)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
	ก) หาก ผู้ให้บริการคลาวด์ ใช้บริการคลาวด์ของผู้ให้บริการรายย่อย ผู้ให้บริการคลาวด์ ต้องตรวจสอบให้แน่ใจว่าระดับความมั่นคงปลอดภัยสารสนเทศของผู้ให้บริการรายย่อยนั้นได้รับการดูแลไม่น้อยกว่าผู้ใช้บริการคลาวด์ ข) เมื่อผู้ให้บริการคลาวด์ ให้บริการคลาวด์ตามห่วงโซ่อุปทาน ผู้ให้บริการคลาวด์ ต้องกำหนดวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศแก่ผู้ให้บริการภายนอก และขอให้ผู้ให้บริการภายนอกแต่ละรายดำเนินกิจกรรมการบริหารความเสี่ยงเพื่อให้บรรลุวัตถุประสงค์

๕.๒.๑๐ การจัดการเหตุภัยคุกคามทางสารสนเทศ (Information Security Incident Management)

๕.๒.๑๐.๑ ความรับผิดชอบและขั้นตอน (Responsibilities and Procedures)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ใช้บริการคลาวด์ ต้องตรวจสอบการจัดสรรความรับผิดชอบสำหรับการจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ และต้องตรวจสอบให้แน่ใจว่าเป็นไปตามข้อกำหนดของผู้ใช้บริการคลาวด์ ข) เหตุภัยคุกคามทางสารสนเทศต้องนำไปสู่การทบทวนโดยผู้ใช้บริการคลาวด์ หรือทบทวนร่วมกันระหว่างผู้ให้บริการคลาวด์และผู้ใช้บริการคลาวด์	ก) ผู้ให้บริการคลาวด์ ต้องกำหนดขอบเขตความรับผิดชอบและขั้นตอนการจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศระหว่างผู้ใช้บริการคลาวด์ และ ผู้ให้บริการคลาวด์ โดยเป็นส่วนหนึ่งของข้อกำหนดบริการ ข) ผู้ให้บริการคลาวด์ ต้องจัดเตรียมเอกสารให้ผู้ใช้บริการคลาวด์ ครอบคลุม

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ในฐานะที่เป็นส่วนหนึ่งของกระบวนการจัดการเหตุภัยคุกคามทางสารสนเทศของตน เพื่อพิจารณาว่าได้มีการละเมิดข้อมูลที่เกี่ยวข้องกับข้อมูลส่วนบุคคลเกิดขึ้นหรือไม่	– ขอบเขตของเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่ ผู้ให้บริการคลาวด์จะรายงานต่อผู้ใช้บริการคลาวด์ – ระดับการเปิดเผยการตรวจพบเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศและการตอบสนองที่เกี่ยวข้อง – กรอบเวลาเป้าหมายที่จะมีการแจ้งเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศเกิดขึ้น – ขั้นตอนการแจ้งเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ – ข้อมูลติดต่อสำหรับการจัดการปัญหาที่เกี่ยวข้องกับเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ – การเยียวยาใด ๆ ที่สามารถนำไปใช้ได้หากเกิดเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศบางอย่างขึ้น ค) เหตุภัยคุกคามทางสารสนเทศต้องนำไปสู่การทบทวนโดยผู้ใช้บริการคลาวด์ หรือทบทวนร่วมกันระหว่างผู้ให้บริการคลาวด์และผู้ใช้บริการคลาวด์ในฐานะที่เป็นส่วนหนึ่งของกระบวนการจัดการเหตุภัยคุกคามทางสารสนเทศของตน เพื่อพิจารณาว่าได้มีการละเมิดข้อมูลที่เกี่ยวข้องกับข้อมูลส่วนบุคคลเกิดขึ้นหรือไม่

๕.๒.๑๐.๒ การรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Reporting Information Security Events)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ใช้บริการคลาวด์ ต้องขอข้อมูลจาก ผู้ให้บริการคลาวด์ เกี่ยวกับกลไกสำหรับ – ผู้ใช้บริการคลาวด์ รายงานเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศที่ตรวจพบต่อผู้ให้บริการคลาวด์ – ผู้ให้บริการคลาวด์ เพื่อรับรายงานเกี่ยวกับเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศที่ตรวจพบโดยผู้ให้บริการคลาวด์ – ผู้ใช้บริการคลาวด์ เพื่อติดตามสถานะของเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศที่รายงาน	ก) ผู้ให้บริการคลาวด์ ต้องมีกลไกสำหรับ – ผู้ใช้บริการคลาวด์ รายงานเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศต่อ ผู้ให้บริการคลาวด์ – ผู้ให้บริการคลาวด์ เพื่อรายงานเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศต่อ ผู้ใช้บริการคลาวด์ – ผู้ใช้บริการคลาวด์ เพื่อติดตามสถานะของเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศที่รายงาน



ฉบับภาษาอังกฤษ
English Version

(Unofficial Translation)

Notification of the National Cyber Security Committee
Re: Cybersecurity Standards for Cloud Systems

B.E. 2567 (2024)

In accordance with the provisions stipulated in the Cybersecurity Act B.E. 2562, the National Cyber Security Committee is mandated to issue cybersecurity standards, including minimum standards concerning computers, computer systems, or computer programs. It is appropriate to set the cybersecurity standards for cloud systems to ensure efficient cybersecurity operations.

By virtue of Section 9(4) of the Cybersecurity Act, B.E. 2562 (2019), and the resolution of the National Cyber Security Committee meeting no. 2/2567 on July 31, 2024, the National Cyber Security Committee has issued a notification, as follows:

Clause 1: This notification shall be called the Notification of the National Cyber Security Committee Re: Cybersecurity Standards for Cloud Systems, B.E. 2567 (2024)."

Clause 2: This notification shall come into force two years after its publication in the Royal Thai Government Gazette.

Clause 3: In this notification:

"Agency" refers to government agencies, regulators, and organizations of critical information infrastructure as defined by the Cybersecurity Act, B.E. 2562 (2019).

"Cloud Computing" refers to the concept of accessing information networks consisting of shareable, elastic, and scalable physical or virtual resources through self-service provisioning and on-demand administration.

"Cloud Service" refers to the capability to perform cloud computing, which is accessible via a designated interface.

"Cloud Service Category" refers to a group of cloud services with certain shared characteristics, categorized as follows:

(1) Infrastructure as a Service (IaaS): Comprising computing systems, data storage, networks, and other relevant resources, where users can efficiently use software on provided infrastructure without managing the underlying infrastructure.

(2) Platform as a Service (PaaS): Comprising application platforms, databases, and computer services, where users can develop, deploy, and configure software without managing the underlying infrastructure.

(3) Software as a Service (SaaS): Where providers offer ready-to-use software, and users manage configurations, parameters, processing units, and storage to achieve their service objectives.

(4) Any combination of services from (1) to (3).

(5) Other services as notified by the Office.

"Public Cloud" refers to cloud services accessible by any cloud service user, with resources controlled by the cloud service provider.

"Cloud Service Customer" (CSC) refers to an agency with a formal contract to use cloud services provided by a cloud service provider.

"Cloud Service Provider" (CSP) refers to a public or private entity that makes cloud services available to customers, managing resources to ensure availability, security, and scalability for its users.

"Personal Data" refers to personal data as defined in Section 6 of the Personal Data Protection Act, B.E. 2562 (2019).

"Office" refers to the Office of the National Cyber Security Agency.

Clause 4: Agencies using public cloud services must comply with this standard, taking into account the impact level of data or information systems as specified in the Notification of the National Cyber Security Committee Re: Standards for Cybersecurity Categorization of Data or

Information Systems, B.E. 2566 (2023), and must meet at least the minimum requirements set out at the end of this notification.

Clause 5: For personal data, the impact level for confidentiality must be classified at least as medium, as specified in the Notification of the National Cyber Security Committee Re: Standards for Cybersecurity Categorization of Data or Information Systems, B.E. 2566 (2023), and must meet at least the minimum requirements set out at the end of this notification.

Clause 6: Agencies must submit a summary report of the actions taken to the Office within 30 days of completion.

Clause 7: The Secretary-General of the National Cyber Security Committee is responsible for enforcing this notification and is authorized to issue notifications, orders, criteria, and procedures to comply with this notification.

In case of any issues related to compliance with this notification or matters not specified herein, the Chairman of the National Cyber Security Committee shall have the authority to interpret and adjudicate, and such interpretation and decision shall be final.

Given on 10 September B.E. 2567 (2024)

Phumtham Wechayachai

Deputy Prime Minister as

Chairman of the National Cyber Security Committee

Annex to the Notification of the National Cyber Security Committee
Re: Cybersecurity Standards for Cloud Systems
B.E. 2567 (2024)

1. Introduction

1.1 Rationale

The National Digital Economy and Society Commission, in its 1/2566 meeting on December 22, 2023, at the Government House, approved the "Cloud First Policy" for government agencies and cloud service providers, outlining standards, cloud service types, and a five-year operational plan for cloud services.

Additionally, the National Cyber Security Committee (NCSC) reported the cybersecurity threat statistics for 2023, highlighting those educational institutions faced 632 cyberattacks, followed by government agencies with 145 attacks, and private companies with 148 attacks. The most common types of threats were online gambling websites (515 cases), hacked websites (336 cases), and fake websites (301 cases).

These growing threats to public and private organizations make it necessary for Thailand's government agencies to adopt robust cybersecurity standards for cloud systems to mitigate the risks posed by these threats.

1.2 Objectives

To mitigate cybersecurity risks for public cloud services used by government agencies, regulators, and Organization of Critical Information Infrastructure.

1.3 Legal Authority

This standard is issued under Section 9(4) of the Cybersecurity Act B.E. 2562 (2019), empowering the National Cyber Security Committee to issue cybersecurity standards.

1.4 Key References

- Notification of the National Cyber Security Committee Re: Standards for Cybersecurity Categorization of Data or Information Systems, B.E. 2566 (2023)

- Notification of the National Cybersecurity Committee Re: Standards and Guidelines for the Development of Cybersecurity Services, B.E. 2566 (2023)

- Notification of the Cybersecurity Regulating Committee Re: Codes of Practice and Standards Framework for Government Agencies and Organization of Critical Information Infrastructure Agencies, B.E. 2564 (2021)

1.5 Risks of Cloud Services

The standard identifies two types of risks: risks from Cloud Service Customers (CSC) and risks from Cloud Service Providers (CSP).

1.6 Structure of the Standard

The standard is divided into two sections:

1. Cloud Security Governance
    - 1.1 Information Security Policies
    - 1.2 Organizational of Information Security
    - 1.3 Compliance
2. Cloud Infrastructure Security and Operation
    - 2.1 Human Resource Security
    - 2.2 Asset Management
    - 2.3 Access Control
    - 2.4 Cryptography
    - 2.5 Physical and Environmental Security
    - 2.6 Operations Security
    - 2.7 Communication Security
    - 2.8 System Acquisition, Development, and Maintenance
    - 2.9 Supplier Relationships
    - 2.10 Information Security Incident Management

1.7 Conceptual Framework

The standard emphasizes shared responsibilities between Cloud Service Customers (CSC) and Cloud Service Providers (CSP) to mitigate cybersecurity threats effectively.

Furthermore, government agencies, regulators, and Organization of Critical Information Infrastructure, as defined by the Cybersecurity Act B.E. 2562 (2019), utilize information systems and data with varying levels of criticality and sensitivity. In accordance with the notification of the National Cyber Security Committee Re: Standards for Cybersecurity Categorization of Data or Information Systems B.E. 2566 (2023), these agencies are required to assess and classify the potential impacts according to cybersecurity objectives. As a result, this standard sets out minimum cybersecurity baseline at three levels: low, moderate, and high. This ensures that government agencies, regulators, and organization of Critical Information Infrastructure can effectively comply with the standard while balancing costs and the benefits received.

Additionally, Cloud Service Providers (CSPs) that provide services to government agencies, regulators, and organization of critical information infrastructure are required to comply with the demands of these agencies as stipulated.

1.8 Certification Process

The standard defines the certification process for both CSCs and CSPs

1.8.1 Types of Certifications

- Self-assessment: This involves evaluating the organization according to the format prescribed by the office, attaching evidence, and requesting approval from the highest executive of the organization. The assessment results must be kept at the organization and submitted to the office.

- Attestation: This involves certification by a regulator, in accordance with the Notification of the National Cyber Security Committee Re:

Criteria and Characteristics for Designating Agencies with Missions or Services as Organizations of Critical Information Infrastructure and the Regulation Assignment B.E. 2564 (2021)

- Certification by a Certifying Body: This involves certification by an accredited certifying body at an advanced or higher level, in accordance with the notification of the National Cyber Security Committee Re: Standards and Guidelines for the Development of Cybersecurity Services, B.E. 2566 (2023). During the initial phase, if the office has not yet accredited certifying bodies, certification may be conducted by international certifying bodies as specified by the office.

1.8.2 Certification Frequency

For Cloud Service Customers:

- Low impact: Self-assessment should be conducted, including a review at least once a year.
- Moderate impact: Certification by a regulator (Attestation) or a certifying body every three years, which includes full certification in the first year and follow-up reviews in the second and third years.
- High impact: Certification by a certifying body every three years, which includes full certification in the first year and follow-up reviews in the second and third years.

For Cloud Service Providers:

- Low impact: Certification by a certifying body every three years, which includes full certification in the first year and follow-up reviews in the second and third years. Providers must also be certified at least ISO/IEC 27001 and CSA STAR Level 1/CCM Lite.
- Moderate impact: Certification by a certifying body every three years, which includes full certification in the first year and follow-up reviews in the second and third years. Providers must also be certified at least CSA STAR Level 2/CCM and ISO/IEC 27701.

- High impact: Certification by a certifying body every three years, which includes full certification in the first year and follow-up reviews in the second and third years. Providers must also be certified either ISO/IEC 27017 or CSA STAR Level 2/CCM, and ISO/IEC 27018 and ISO/IEC 27701.

1.8.3 In cases where a Cloud Service Provider is already certified by a certifying body, self-assessment is not required.

1.8.4 In cases where a Cloud Service Provider is certified to CSA STAR Level 2/CCM, certification under CSA STAR Level 1/CCM Lite is not required.

2. Scope

- This standard applies to government agencies, regulators, and Organizations of Critical Information Infrastructure as defined by the Cybersecurity Act B.E. 2562, including cloud service providers offering services to these entities.

- This standard prescribes cybersecurity measures for cloud systems, specifically for cloud service customers (CSC) and public cloud service providers (CSPs). It is applicable solely to cloud services provided to government agencies, regulators, and Organizations of Critical Information Infrastructure under the Cybersecurity Act B.E. 2562. The terms of service between the cloud service customers and providers form the contractual basis for compliance.

- Stakeholders involved in this standard include government agencies, regulators, and Organizations of Critical Information Infrastructure as defined by the Cybersecurity Act B.E. 2562. This also includes public cloud service providers, internal cybersecurity auditors, and certify bodies.

3. Normative Reference

- ISO/IEC 27017:2015 Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services.
- ISO/IEC 27018:2019 Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors.
- ISO/IEC 22123-1:2023 Information technology — Cloud computing Part 1: Vocabulary.
- Notification of the National Cyber Security Committee Re: Standards for Cybersecurity Categorization of Data or Information Systems, B.E. 2566 (2023)
- Notification of the National Cybersecurity Committee Re: Standards and Guidelines for the Development of Cybersecurity Services, B.E. 2566 (2023)
- Notification of the Cybersecurity Regulating Committee Re: Codes of Practice and Standards Framework for Government Agencies and Organization of Critical Information Infrastructure Agencies, B.E. 2564 (2021

4. Minimum Requirements and Certification for Cloud Service Customers and Cloud Service Providers

Table of Minimum Requirements and Certification for Cloud Service Customers and Cloud Service Providers

Type of Data or Information Systems[1]	**Minimum Requirements**	**Certification for Cloud Service Customers**	**Certification for Cloud Service Providers**
Low Impact	**Part One**: 5.1.1 and 5.1.2 **Part Two**: 5.2.1, 5.2.2, 5.2.3, 5.2.4, 5.2.8, and 5.2.9 ***Without 5.2.5***	**Self-assessment** along with supporting documentation and approval from the highest executive of the organization, the assessment must be retained by the organization and submitted to the office	**Certified by certify bodies** on a 3-year cycle, consisting of certification the 1st year and surveillance audits in the 2nd and 3rd years, certification must also be certified to at least ISO/IEC 27001 and CSA STAR Level 1/CCM Lite.

Type of Data or Information Systems[1]	Minimum Requirements	Certification for Cloud Service Customers	Certification for Cloud Service Providers
Moderate Impact	**Part One**: All **Part Two**: 5.2.1, 5.2.2, 5.2.3, 5.2.4, 5.2.7, 5.2.8, 5.2.9, and 5.2.10 ***Without 5.2.5***	**Certified by the regulators (Attestation) or certified by a certify body** on a 3-year cycle. This includes a full certification in the 1st year and a surveillance audit in the 2nd and 3rd years.	**Certified by a certify body** on a 3-year cycle. This includes a full certification in the 1st year and a surveillance audit in the 2nd and 3rd years. Additionally, it must also be certified at least to CSA STAR Level 2/CCM and ISO/IEC 27701.
High Impact	**Part One**: All **Part Two**: All	**Certified by a certify body** on a 3-year cycle. This includes a full certification in the 1st year and a surveillance audit in the 2nd and 3rd years.	**Certified by a certify body** on a 3-year cycle. This includes a full certification in the 1st year and a surveillance audit in the 2nd and 3rd years. Additionally, it must also be certified to either ISO/IEC 27017 or CSA STAR Level 2/CCM, and ISO/IEC 27018 and ISO/IEC 27701.

[1] Notification of the National Cyber Security Committee Re: Standards for Cybersecurity Categorization of Data or Information Systems, B.E. 2566 (2023)

5. Standards for Cybersecurity of Cloud Systems

5.1 Cloud Security Governance

5.1.1 Information Security Policies

Cloud Service Customer	Cloud Service Provider
a) Cloud service customers (CSC) must establish a specific information security policy for cloud computing tailored to their operations. This policy must align with the acceptable levels of information security risk related to the organization's data and other assets.	**a)** Cloud service providers must enhance their information security policies to manage the provision and use of cloud services, taking into account the following: - Minimum information security requirements for the design and operation of cloud services

Cloud Service Customer	Cloud Service Provider
b) When establishing the information security policy for cloud computing, the cloud service customers must consider the following: - Data stored in the cloud computing environment may be accessed and managed by the cloud service provider (CSP). - Organizational assets may be maintained in the cloud computing environment, such as application programs. - Processes may operate on virtual cloud services shared by multiple users. - The cloud service customers and the context in which cloud services are used. - The cloud service customer's privileged cloud service administrators who have special access rights. - The geographical location of the cloud service provider's organization and the countries where the cloud service provider may store the cloud service customer's data (even temporarily). **c)** The cloud service customer's personal data protection policy must include provisions regarding contractual agreements between the cloud data processor and the cloud service customer. **d)** The contractual agreement must clearly define the responsibilities between the cloud data processor, subcontractors, and the cloud service customer, considering the type of cloud service (e.g., IaaS, PaaS, or SaaS). For example, the responsibility for controlling the application layer may vary depending on whether the cloud data processor is providing SaaS, PaaS, or IaaS services	- Risks from authorized internal personnel - Multi-tenancy and the separation of cloud service customers (including virtualization) - Access to cloud service customers' assets by cloud service provider staff - Access control procedures, such as strict authentication for cloud service administrator access - Communication with cloud service customers during change management - Security of virtualization - Access to and protection of cloud service customers' data - Lifecycle management of cloud service customers accounts - Communication in the event of a breach and procedures for sharing information to assist with investigation and forensics

5.1.2 Organization of Information Security

5.1.2.1 Information Security Roles and Responsibilities

Cloud Service Customer	Cloud Service Provider
a) Cloud service customers must agree with cloud service providers on the proper allocation of roles and responsibilities regarding information security. Cloud service providers must ensure that they can perform the assigned roles and responsibilities. The agreement must clearly outline the information security roles and responsibilities of both parties. **b)** Cloud service customers must identify and manage relationships with support functions and customer care functions of the Cloud service providers.	**a)** Cloud service providers must agree and document the allocation of roles and responsibilities regarding information security with cloud service providers, the Cloud service providers itself, and any third-party providers. **b)** Cloud service providers must appoint a data protection coordinator to liaise with the cloud service providers.

5.1.2.2 Contact with Authorities

Cloud Service Customer	Cloud Service Provider
a) Cloud service customers must identify the relevant authorities involved in the collaboration between the cloud service customers and the cloud service providers.	**a)** Cloud service providers should inform the cloud service customers of the geographic location of the provider's organization and the countries where the cloud service provider can store the cloud service customer's data.

5.1.3 Compliance

5.1.3.1 Identification of Applicable Legislation and Contractual Requirements

Cloud Service Customer	Cloud Service Provider
a) Cloud service customers must consider the fact that applicable laws and regulations may include the governing the cloud service	**a)** Cloud service providers must inform cloud service customers of the legal jurisdiction governing the cloud services.

Cloud Service Customer	Cloud Service Provider
provider, in addition to those governing the cloud service customer. **b)** Cloud service customers must request evidence that the cloud service provider complies with relevant regulations and standards applicable to the customer. Such evidence may include certification provided by an external auditor.	**b)** Cloud service providers must specify their own relevant legal requirements (e.g., regarding encryption to protect personal data) and provide this information to cloud service customers upon request. **c)** Cloud service providers must provide evidence to cloud service customers showing compliance with applicable laws and contractual requirements.

5.1.3.2 Intellectual Property Rights

Cloud Service Customer	Cloud Service Provider
a) Installing commercially licensed software in cloud services may lead to a violation of the software's licensing terms. Cloud service customers must have procedures in place to identify the specific licensing requirements for cloud systems before permitting the installation of licensed software in cloud services. Special attention should be given to cases where the cloud service is flexible and scalable, and the software may be used on more systems or processing cores than allowed by the licensing terms.	**a)** Cloud service providers must establish processes for addressing intellectual property rights complaints.

5.1.3.3 Protection of Records

Cloud Service Customer	Cloud Service Provider
a) Cloud service customers must request information from cloud service providers regarding the protection of records collected and stored by the cloud service providers, which are related to the cloud service usage by the cloud service customers.	**a)** Cloud service providers must provide information to cloud service customers regarding the protection of records collected and stored by the cloud service providers,

Cloud Service Customer	Cloud Service Provider
	which are related to the cloud service usage by the cloud service customers.

5.1.3.4 Regulation of Cryptographic Controls

Cloud Service Customer	Cloud Service Provider
a) Cloud service customers must ensure that the set of cryptographic controls used for cloud services complies with the relevant agreements, laws, and regulations.	**a)** Cloud service providers must provide explanations to cloud service customers regarding the cryptographic controls implemented by the providers, which will be used for reviewing compliance with agreements, laws, and regulations.

5.1.3.5 Independent Review of Information Security

Cloud Service Customer	Cloud Service Provider
a) Cloud service customers must request documented evidence that the information security controls and practices for cloud services have been implemented and are consistent with the claims made by the cloud service provider. This evidence may include relevant certifications.	**a)** Cloud service providers must provide documented evidence to the cloud service customers to confirm the provider's claims regarding the implementation of information security controls and personal data protection. **b)** In cases where individual assessments by cloud service customers cannot be conducted or may pose additional information security risks, the cloud service provider must provide independent evidence that the information security controls and personal data protection measures have been implemented in accordance with the provider's policies and procedures. This evidence must be shown to potential cloud service customers before entering into an agreement. Normally, the independent audit selected by the cloud

Cloud Service Customer	Cloud Service Provider
	service provider should be an accepted method to meet the cloud service customers' needs for operational verification of the cloud service provider's practices. If an independent audit cannot be conducted, the cloud service provider must conduct a self-assessment and disclose the process and results to the cloud service customers.

5.2 Cloud Infrastructure Security and Operation

5.2.1 Human Resource Security

5.2.1.1 Information Security Awareness, Education and Training

Cloud Service Customer	Cloud Service Provider
a) Cloud service customers must include the following in their awareness, education, and training programs for cloud business managers, cloud system administrators, cloud service operators, and cloud users, including relevant employees and contractors: - Standards and procedures for cloud service usage - Information security risks associated with cloud services and how to manage those risks - Environmental and network system risks from using cloud services - Personal data protection - Legal and regulatory considerations **b)** A program for raising awareness of information security, education, and training on cloud services must be provided to	**a)** Cloud service providers must raise awareness of information security and personal data protection, and provide education and training for employees, as well as ensure that contractors follow the same practices. This should cover the appropriate handling of cloud service customers data and information generated from cloud services, which may include sensitive information subject to specific regulatory restrictions on access and use by the cloud service provider.

Cloud Service Customer	Cloud Service Provider
executives and managers overseeing these services, including business units.	

5.2.2 Asset Management

5.2.2.1 Inventory of Assets

Cloud Service Customer	Cloud Service Provider
a) The asset inventory of the cloud service customers must take into consideration the information and assets associated with the processing environment on the cloud. The asset register must specify the location where the assets are stored, such as the name of the cloud service provider.	**a)** The asset register of the cloud service provider must clearly identify: - The information of the cloud service customer - Information generated from the use of cloud services

5.2.2.2 Labelling of Information

Cloud Service Customer	Cloud Service Provider
a) Cloud service customers must identify the information and assets of the organization that are used or stored on the cloud system according to the organization's information identification procedures.	**a)** Cloud service providers must document and disclose the functionalities of any service that cloud service customers can use to identify relevant information and assets.

5.2.3 Access Control

5.2.3.1 Access to Networks and Network Services

Cloud Service Customer	Cloud Service Provider
a) Cloud service customer' access control policies for using network services must specify the requirements for users when accessing cloud services, according to each service being used	

5.2.3.2 User Registration and Deregistration

Cloud Service Customer	Cloud Service Provider
a) The registration and deregistration process for users must cover scenarios where user access controls are compromised, such as when passwords or other user registration information (e.g., unintentional disclosure) are damaged or compromised.	**a)** To manage cloud service access by cloud service customer, the cloud service provider must provide registration and deregistration functions for users, including requirements for the use of these functions for cloud service customer.

5.2.3.3 User Access Provisioning

Cloud Service Customer	Cloud Service Provider
	a) Cloud service providers must provide functionalities for managing the access rights of cloud service customer, including the requirements for utilizing these functionalities

5.2.3.4 Management of Privileged Access Rights

Cloud Service Customer	Cloud Service Provider
a) Cloud service customers must use adequate authentication techniques (e.g., multi-factor authentication) for verifying the privileges of their cloud service administrators to ensure their ability to manage cloud services in alignment with identified risks.	**a)** Cloud service providers must employ adequate authentication techniques (e.g., multi-factor authentication) for verifying the privileges of the cloud service administrators of the cloud service customers to ensure the secure management of cloud systems in accordance with identified risks.

5.2.3.5 Management of Secret Authentication Information of Users

Cloud Service Customer	Cloud Service Provider
a) Cloud service customers must verify that the cloud service provider's process for managing secret authentication information, such as passwords, complies with the customer's requirements.	**a)** Cloud service providers must provide information regarding their process for managing the cloud service customer's secret authentication information, including the procedures for allocating such information for user authentication.

5.2.3.6 Information Access Restriction

Cloud Service Customer	Cloud Service Provider
a) Cloud service customers must ensure that access to data in cloud services is restricted in accordance with access control policies and complies with the specified limitations. This includes restricting access to various services on the cloud platform and to the data of cloud service customers stored within the service.	**a)** Cloud service providers must provide access control mechanisms that allow cloud service customers to restrict access to various services on the cloud platform and to the data of cloud service customers stored within the service.

5.2.3.7 Use of Privilege Utility Programs

Cloud Service Customer	Cloud Service Provider
a) If the use of utility programs is allowed, the cloud service customers must specify the utility programs that will be used in the cloud computing environment and ensure that these programs do not interfere with the controls of the cloud services.	**a)** The cloud service provider must specify the requirements for any utility programs used in the cloud services. The cloud service provider must ensure that the use of any utility programs that can bypass standard procedures or security measures is restricted only to authorized personnel.

Cloud Service Customer	Cloud Service Provider
	Regular reviews and audits of the use of such programs must also be conducted.

5.2.3.8 Secure Log-on Procedures

Cloud Service Customer	Cloud Service Provider
a) Cloud service customers must require users under their control to follow secure log-on procedures for any account.	**a)** When necessary, cloud service providers must provide secure log-on procedures for any account requested by the cloud service customers for users under the control of the cloud service customer.

5.2.4 Cryptography

5.2.4.1 Policy on the Use of Cryptographic Controls

Cloud Service Customer	Cloud Service Provider
a) Cloud service customers must implement encryption controls for using cloud services with sufficient strength and aligned with the identified risks. This applies regardless of whether the cloud service customers or the cloud service provider supplies the encryption controls. **b)** When the cloud service provider offers any encryption, the cloud service customers must verify the information provided by the cloud service provider to ensure it meets the following requirements: - Complies with the cloud service customer's policy requirements.	**a)** The cloud service provider must provide information to the cloud service customers regarding encryption to protect data and personal information processed by the cloud service provider. Additionally, the cloud service provider must offer information on any capabilities that can assist the cloud service customers in using the provided encryption.

Cloud Service Customer	Cloud Service Provider
- Is compatible with other encryption protections used by the cloud service customer. - Applies to data both at rest and in transit within and outside the cloud service.	

5.2.4.2 Key Management

Cloud Service Customer	Cloud Service Provider
a) Cloud service customers must identify encryption keys for each cloud service and follow procedures for key management. **b)** In cases where the cloud service provides a key management function for use by cloud customers, the cloud customer must request the following information regarding the procedures used to manage encryption keys related to the cloud service: - Type of keys - Specific requirements of the key management system, including steps throughout the encryption key's lifecycle such as creation, modification, storage, expiration, recovery, retention, and destruction. - Recommended key management procedures for use by the cloud customer. **c)** Cloud customers must not allow the cloud service provider to store and manage encryption keys when the cloud customer uses their own encryption keys.	

5.2.5 Physical and Environment Security

5.2.5.1 Data Center Location

Cloud Service Customer	Cloud Service Provider
a) Must use a primary data center located in Thailand (Data Localization).	**a)** A primary data center must be located in Thailand (Data Localization). b) A backup data center must be established in Thailand (Data Localization), or within the Southeast Asia region, as close as possible to the primary usage area of the cloud service customer, including Singapore and the Hong Kong Special Administrative Region.

5.2.5.2 Secure Disposal or Reuse of Equipment

Cloud Service Customer	Cloud Service Provider
a) Cloud service customers must request confirmation that cloud service providers have policies and procedures in place for the secure disposal or reuse of resources.	**a)** Cloud service providers must ensure that arrangements are made for the secure and timely disposal or reuse of resources (such as equipment, data storage devices, files, memory). **b)** For secure disposal or reuse, ensuring that data cannot be recovered, any equipment with data storage media that may contain personal information must be treated as if it contains actual personal information.

5.2.6 Operations Security

5.2.6.1 Change Management

Cloud Service Customer	Cloud Service Provider
a) The cloud service customer's change management process must consider any impacts resulting from changes initiated by the cloud service provider.	**a)** The cloud service provider must provide information to the cloud service customers regarding changes in the cloud service that could negatively affect the cloud service. The following information will help the cloud service customers identify the potential impacts of changes on information security: - Type of change - Scheduled date and time of the change - Technical description of the change in the cloud service and underlying systems - Notifications of the start and completion of the change **b)** When the cloud service provider's cloud services rely on a third-party provider, the cloud service provider may need to notify the cloud service customers of any changes made.

5.2.6.2 Capacity Management

Cloud Service Customer	Cloud Service Provider
a) Cloud service customers must ensure that the resource capacities agreed upon in the cloud services meet the customer's requirements. **b)** Cloud service customers must monitor their use of cloud services and anticipate future resource capacity needs to ensure the	**a)** Cloud service providers must monitor the total resource capacity to prevent security incidents caused by resource shortages.

Cloud Service Customer	Cloud Service Provider
ongoing effectiveness of cloud services over time.	

5.2.6.3 Information Backup

Cloud Service Customer	Cloud Service Provider
a) In cases where the cloud service provider has the ability to offer backup services as part of the cloud service, the cloud service customers must request specifications of the backup capability from the cloud service provider. In addition, the cloud service customers must verify that the backup service complies with the established backup requirements. **b)** The cloud service customers are responsible for carrying out backup processes when the cloud service provider does not offer this service.	**a)** The cloud service provider must provide specifications of the backup capability to the cloud service customer. The specifications should include the following information as appropriate: - The scope and schedule of the backups - Backup methods and data formats, including encryption methods, if applicable - Data retention period for backups - Procedures for verifying the integrity of backups - Steps and timelines for restoring data from backups - Procedures for testing backup capabilities - Location of the backup storage **b)** The cloud service provider must provide access to secure and segregated backups if this service is offered to the cloud service customer

5.2.6.4 Event Logging

Cloud Service Customer	Cloud Service Provider
a) Cloud service customers must establish requirements for event logging and verify that the cloud service complies with these requirements.	**a)** Cloud service providers must enable cloud service customers to log events. **b)** Where possible, event logs should record whether personal data has been altered

Cloud Service Customer	Cloud Service Provider
	(added, modified, or deleted) as a result of the event and by whom (Audit Log). In cases where multiple service providers are involved in delivering various types of services from the reference cloud architecture, they may have different or shared roles in fulfilling this requirement.

5.2.6.5 Protection of Log information

Cloud Service Customer	Cloud Service Provider
a) Information recorded in event logs For purposes such as security auditing and operational diagnostics, personal data may be included. Therefore, access control measures must be implemented to ensure that the recorded log information is only used for its intended purposes. **b)** Operational procedures must be implemented. Ideally, these procedures should be automated to ensure that the event log information is deleted within the specified retention period, as documented.	**a)** Information recorded in event logs For purposes such as security auditing and operational diagnostics, personal data may be included. Therefore, access control measures must be implemented to ensure that the recorded log information is only used for its intended purposes. **b)** Operational procedures must be implemented. Ideally, these procedures should be automated to ensure that the event log information is deleted within the specified retention period, as documented

5.2.6.6 Administrator and Operator Logs

Cloud Service Customer	Cloud Service Provider
a) If privileged access is granted to the cloud service customer, the use of that privileged access must be logged, and the performance of those actions must be recorded. The cloud service customers must assess whether the logging capability provided by the cloud service provider is adequate or if the cloud service customers need to employ additional logging capabilities.	

5.2.6.7 Clock Synchronization

Cloud Service Customer	Cloud Service Provider
a) Cloud service customers must request information regarding the clock synchronization used in the cloud service provider's system.	**a)** Cloud service providers must provide information to the cloud service customers about the clocks used in their system and how customers can synchronize their internal clocks with the clocks in the cloud services.

5.2.6.8 Management of Technical Vulnerabilities

Cloud Service Customer	Cloud Service Provider
a) Cloud service customers must request information from cloud service providers about how technical vulnerabilities that could affect the provided cloud services are managed. The cloud service customers must identify the technical vulnerabilities for which they are responsible and establish clear processes for managing them.	**a)** Cloud service providers must provide information to cloud service customers regarding the management of technical vulnerabilities that may impact the cloud services being offered.

5.2.6.9 Separation of Development, Testing and Operational Environments

Cloud Service Customer	Cloud Service Provider
a) In cases where the use of personal data for testing purposes cannot be avoided, a risk assessment must be conducted. Technical and organizational measures must be implemented to minimize the identified risks as much as possible.	**a)** In cases where the use of personal data for testing purposes cannot be avoided, a risk assessment must be conducted. Technical and organizational measures must be implemented to minimize the identified risks as much as possible.

5.2.7 Communication Security

5.2.7.1 Information Transfer Policies and Procedures

Cloud Service Customer	Cloud Service Provider
a) Whenever physical media is used for the transfer of data, a system must be in place to log the physical media entering and leaving, which contains personal data. This log should include the type of physical media, the authorized sender/receiver, the date and time, and the quantity of physical media. **b)** Cloud service customer must request cloud service providers to implement additional measures (e.g., encryption) to ensure that data can only be accessed at the destination point and not during transit.	**a)** Whenever physical media is used for the transfer of data, a system must be in place to log the physical media entering and leaving, which contains personal data. This log should include the type of physical media, the authorized sender/receiver, the date and time, and the quantity of physical media. **b)** If possible, cloud service customers should be requested to implement additional measures (e.g., encryption) to ensure that data can only be accessed at the destination and not during transit.

5.2.7.2 Segregation in Networks

Cloud Service Customer	Cloud Service Provider
a) The cloud service customers must establish requirements for network segregation to ensure the separation of tenants in a shared cloud service environment and verify whether the cloud service provider meets those requirements.	**a)** The cloud service provider must enforce network access segregation in the following cases: - Segregation between tenants in a multi-tenant environment. - Segregation between the cloud service provider's internal administrative environment and the cloud processing environment of the cloud service customer. **b)** The cloud service provider must assist the cloud service customers in verifying the segregation implemented by the cloud service provider.

5.2.8 System Acquisition, Development, and Maintenance

5.2.8.1 Information Security Requirements Analysis and Specification

Cloud Service Customer	Cloud Service Provider
a) Cloud service customers must define the information security requirements for using cloud services and then assess whether the cloud service provider's services can meet these needs. **b)** For this assessment, cloud service customers must request information about the information security capabilities from the cloud service provider.	**a)** Cloud service providers must provide cloud service customers with information about the information security measures they use. This information must be shared without disclosing details that could benefit malicious actors

5.2.8.2 Secure Development Policy

Cloud Service Customer	Cloud Service Provider
a) The cloud service customers must request information from the cloud service provider regarding the use of secure development processes and practices by the cloud service provider.	**a)** The cloud service provider must provide information about the secure development processes and practices it uses, within the scope that aligns with its disclosure policy.

5.2.9 Supplier Relationships

5.2.9.1 Information Security Policy for Supplier Relationships

Cloud Service Customer	Cloud Service Provider
a) The cloud service customers must specify that the cloud service provider is categorized as an external provider within the information security policy for supplier relationships. This will help mitigate risks associated with access to and management	

Cloud Service Customer	Cloud Service Provider
of the cloud customer's data by the cloud service provider	

5.2.9.2 Addressing Security within Supplier Agreements

Cloud Service Customer	Cloud Service Provider
a) Cloud service customers must confirm the roles and responsibilities regarding information security related to cloud services, as described in the service agreement. These may include the following processes: - Malware protection - Data backup - Encryption control measures - Vulnerability management - Incident management - Compliance with technical requirements - Security testing - Auditing - Collection, maintenance, and protection of evidence, including logs and audit trails - Data protection upon the termination of the service agreement - Authentication and access control - Identity and access management	**a)** Cloud service providers must specify the relevant information security measures they will implement as part of the agreement to ensure there is no misunderstanding between the cloud service provider and the cloud service customer. These measures may include the following processes: - Malware protection - Data backup - Encryption control measures - Vulnerability management - Incident management - Compliance with technical requirements - Security testing - Auditing - Collection, maintenance, and protection of evidence, including logs and audit trails - Data protection upon the termination of the service agreement - Authentication and access control - Identity and access management **b)** The information security measures implemented by the cloud service provider may vary depending on the type of cloud services being utilized by the cloud service customer.

5.2.9.3 Information and Communication Technology Supply Chain

Cloud Service Customer	Cloud Service Provider
	a) If a cloud service provider uses the cloud services of a subcontracted cloud provider, the cloud service provider must ensure that the information security level of the subcontracted provider is maintained at least equal to that of the cloud service provider. **b)** When the cloud service provider offers cloud services as part of a supply chain, the cloud service provider must establish information security objectives for the external providers and request that each external provider conduct risk management activities to meet these objectives.

5.2.10 Information Security Incident Management

5.2.10.1 Responsibilities and Procedures

Cloud Service Customer	Cloud Service Provider
a) If the Cloud Service Provider (CSP) utilizes the services of a sub-cloud service provider, the CSP must verify the allocation of responsibilities for managing information security incidents, ensuring compliance with the requirements of the Cloud service customers (CSC). **b)** Information security incidents must lead to a review by the CSC, or jointly between the CSP and the CSC, as part of their information security incident management process, to determine if there has been any breach related to personal data.	**a)** The CSP must define the scope of responsibilities and procedures for handling information security incidents between the CSC and the CSP, as part of the service agreement requirements. **b)** The CSP must provide documentation to the CSC, covering: - The scope of information security incidents that the CSP will report to the CSC. - The level of disclosure for detected information security incidents and the associated responses.

Cloud Service Customer	Cloud Service Provider
	- Target timeframes for notifying the CSC when an information security incident occurs. - Procedures for reporting information security incidents. - Contact information for handling issues related to information security incidents. - Any remedies that may apply if specific information security incidents occur. **c)** Information security incidents must lead to a review by the CSC, or jointly between the CSP and the CSC, as part of their incident management process, to determine if there has been any breach of personal data

5.2.10.2 Reporting Information Security Events

Cloud Service Customer	Cloud Service Provider
a) Cloud service customers must request information from cloud service providers regarding mechanisms for: - Cloud service customers to report detected information security incidents to the cloud service provider. - The cloud service provider to receive reports of information security incidents detected by the cloud service provider. - Cloud service customers to track the status of reported information security incidents.	**a)** Cloud service providers must have mechanisms in place for: - Cloud service customers to report information security incidents to the cloud service provider. - The cloud service provider to report information security incidents to cloud service customers. - Cloud service customers to track the status of reported information security incidents.

* * * * * * * * * *

18

ประกาศ กมช.

เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัย
สำหรับเว็บไซต์ พ.ศ. 2568

มีผลใช้บังคับตั้งแต่วันที่ 16 ก.ย. 69 เป็นต้นไป

Notification of NCSC

Re: Website Security Standards B.E. 2568 (2025)

effective from September 16, 2026, onwards.



ฉบับภาษาไทย
Thai Version

ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์

พ.ศ. ๒๕๖๘

โดยที่พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดให้คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติมีหน้าที่และอำนาจสร้างมาตรฐานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ และกำหนดมาตรฐานขั้นต่ำที่เกี่ยวข้องกับคอมพิวเตอร์ ระบบคอมพิวเตอร์หรือโปรแกรมคอมพิวเตอร์ จึงสมควรมีมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ เพื่อให้การดำเนินงานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์เป็นไปอย่างมีประสิทธิภาพ

อาศัยอำนาจตามความในมาตรา ๙ (๔) มาตรา ๒๒ (๑๓) และ (๑๖) แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ประกอบกับมติคณะกรรมการบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ ในคราวการประชุมครั้งที่ ๖/๒๕๖๕ เมื่อวันที่ ๔ พฤศจิกายน ๒๕๖๕ มติคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ในคราวการประชุมครั้งที่ ๔/๒๕๖๖ เมื่อวันที่ ๒๖ พฤศจิกายน ๒๕๖๖ และมติคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ในคราวการประชุมครั้งที่ ๓/๒๕๖๘ เมื่อวันที่ ๒๙ สิงหาคม ๒๕๖๘ คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ จึงออกประกาศไว้ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ พ.ศ. ๒๕๖๘”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับเมื่อพ้นกำหนดหนึ่งปีนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ข้อ ๓ ให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ดำเนินการให้เว็บไซต์ของตน เป็นไปตามมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ ที่กำหนดท้ายประกาศนี้

ให้สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ดำเนินการส่งเสริมและสนับสนุนให้หน่วยงานเอกชนนำมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ตามแนบท้ายประกาศนี้ ไปปรับใช้เป็นแนวทางในสร้างมาตรฐานการรักษาความมั่นคงปลอดภัยเว็บไซต์ของตนด้วย

ข้อ ๔ เพื่อประโยชน์ในการดำเนินการตามมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ตามข้อ ๓ วรรคหนึ่ง ให้หน่วยงานควบคุมหรือกำกับดูแลและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ดำเนินการ ดังต่อไปนี้

(๑) กำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศของเว็บไซต์

(๒) ประเมินและจัดระดับผลกระทบในแต่ละด้าน

(๓) ระบุข้อกำหนดขั้นต่ำที่ต้องดำเนินการ และระบุการปฏิบัติตามมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์

(๔) ประเมินตนเอง (Self-Assessment) เพื่อตรวจสอบการดำเนินการตามมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์

การดำเนินการตามวรรคหนึ่ง ให้เป็นไปตามแบบฟอร์ม ค๑ แบบตรวจรายการเพื่อตรวจสอบสถานะความมั่นคงปลอดภัยสำหรับเว็บไซต์ ท้ายประกาศนี้ โดยให้หน่วยงานดำเนินการอย่างน้อยปีละ ๑ ครั้ง

ข้อ ๕ เมื่อหน่วยงานดำเนินการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์และประเมินและจัดระดับผลกระทบตามข้อ ๔ วรรคหนึ่ง (๑) และ (๒) แล้ว ให้ดำเนินการ ดังนี้

(๑) กรณีผลกระทบระดับต่ำหรือระดับกลาง ให้หน่วยงานรายงานผลการประเมินตนเองตามแบบฟอร์ม ค๑ แบบตรวจรายการเพื่อตรวจสอบสถานะความมั่นคงปลอดภัยสำหรับเว็บไซต์ท้ายประกาศนี้ พร้อมแนบเอกสารหลักฐานที่เกี่ยวข้อง เสนอต่อผู้บริหารระดับสูงสุดของหน่วยงานและเก็บรักษาไว้ที่หน่วยงานเพื่อให้สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติตรวจสอบ

(๒) กรณีผลกระทบระดับสูง ให้หน่วยงานรายงานผลการประเมินตนเอง ตามแบบฟอร์ม ค๑ แบบตรวจรายการเพื่อตรวจสอบสถานะความมั่นคงปลอดภัยสำหรับเว็บไซต์ ท้ายประกาศนี้ พร้อมแนบเอกสารหลักฐานที่เกี่ยวข้อง เสนอต่อผู้บริหารสูงสุดของหน่วยงาน และหน่วยงานควบคุมหรือกำกับดูแล พร้อมส่งสำเนาให้สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

ข้อ ๖ กรณีที่หน่วยงานดำเนินการประเมินตนเองตามข้อ ๔ วรรคหนึ่ง (๔) แล้วปรากฏว่า หน่วยงานยังมิได้ดำเนินการตามมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ของหน่วยงานหรือดำเนินการแล้วแต่ยังไม่สอดคล้องกับมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ตามประกาศนี้ ทั้งหมดหรือบางส่วน หน่วยงานต้องดำเนินการปรับปรุงให้สอดคล้องกับมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ตามประกาศนี้กำหนด แล้วแต่กรณี

ก่อนการดำเนินการตามวรรคหนึ่ง ให้หน่วยงานจัดทำแบบฟอร์ม ค๒ แบบรายงานรายการที่ยังต้องปรับปรุง ท้ายประกาศนี้ แล้วแจ้งต่อผู้บริหารระดับสูงสุดของหน่วยงานเพื่อใช้อำนาจในทางบริหารสั่งการไปยังผู้ที่เกี่ยวข้องเพื่อดำเนินการให้สอดคล้องกับมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ตามประกาศนี้กำหนด

ข้อ ๗ ให้เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติรักษาการตามประกาศนี้ และให้มีอำนาจออกประกาศ คำสั่ง หลักเกณฑ์และวิธีการเพื่อปฏิบัติตามประกาศนี้

ในกรณีที่มีปัญหาเกี่ยวกับการปฏิบัติตามประกาศนี้ หรือประกาศนี้ไม่ได้กำหนดเรื่องใดไว้ ให้เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ มีอำนาจตีความและวินิจฉัยชี้ขาดแล้วรายงานให้คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ทั้งนี้ การตีความและคำวินิจฉัยของเลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติให้เป็นที่สุด

ประกาศ ณ วันที่ ๑๐ กันยายน พ.ศ. ๒๕๖๘
ประเสริฐ จันทรรวงทอง
รองนายกรัฐมนตรี
ประธานกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

มาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์

เว็บไซต์เป็นองค์ประกอบที่สำคัญเพราะเป็นช่องทางในการเข้าถึงข้อมูล ผลิตภัณฑ์ หรือบริการของหน่วยงาน ถือเป็นประตูที่ใช้เชื่อมหน่วยงานกับอินเทอร์เน็ต หากเกิดภัยคุกคามทางไซเบอร์เพื่อขโมย แก้ไข หรือลบข้อมูลที่สำคัญของหน่วยงาน เช่น ข้อมูลลูกค้า ข้อมูลทางการเงิน จะส่งผลกระทบต่อการดำเนินการของหน่วยงาน จากสถิติในการรับมือภัยคุกคามทางไซเบอร์ ปี ๒๕๖๖ - ๒๕๖๗ พบว่า ร้อยละ ๔๔ ของภัยคุกคามไซเบอร์ทั้งหมดเกิดขึ้นกับเว็บไซต์ ประกอบด้วย Hacked Website (Defacement และ Gambling) และ Fake Website (๔) อย่างไรก็ตาม นอกจากภัยคุกคามทางไซเบอร์จะส่งผลกระทบต่อข้อมูลหรือระบบสารสนเทศของหน่วยงานแล้ว ยังส่งผลกระทบต่อการดำเนินงาน การให้บริการของหน่วยงาน อาจทำให้หน่วยงานสูญเสียรายได้ เสียชื่อเสียง และขาดความน่าเชื่อถืออีกด้วย ตัวอย่างเช่น การโจมตีเว็บไซต์เพื่อเปลี่ยนแปลงข้อมูลหน้าเว็บ (Web Defacement) การโจมตีเว็บไซต์เพื่อใช้เป็นฐานในการเผยแพร่มัลแวร์ (Malware Distribution) หรือการใช้เว็บไซต์เพื่อการหลอกลวง (Phishing Website) ซึ่งอาจทำให้หน่วยงานมีความเสี่ยงทางกฎหมาย และสำคัญที่สุดอาจส่งผลกระทบต่อความมั่นคงปลอดภัยในระดับประเทศ

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ได้เล็งเห็นถึงความสำคัญในการป้องกัน รับมือ และบรรเทาผลกระทบจากภัยคุกคามที่จะเกิดขึ้นกับเว็บไซต์ จึงอาศัยหน้าที่และอำนาจในพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ (๕) มาตรา ๙ (๔) ซึ่งกำหนดให้คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) มีหน้าที่และอำนาจในการกำหนดมาตรฐานและแนวทางส่งเสริมพัฒนาระบบการให้บริการรักษาความมั่นคงปลอดภัยไซเบอร์ สร้างมาตรฐานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ และกำหนดมาตรฐานขั้นต่ำที่เกี่ยวกับคอมพิวเตอร์ ระบบคอมพิวเตอร์ โปรแกรมคอมพิวเตอร์ รวมถึงส่งเสริมการรับรองมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานเอกชน และมาตรา ๒๒ (๑๓) ได้กำหนดให้ สกมช. มีหน้าที่และอำนาจในการศึกษาและวิจัยข้อมูลที่จำเป็นสำหรับการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อจัดทำข้อเสนอแนะเกี่ยวกับมาตรการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมทั้งดำเนินการอบรมและฝึกซ้อมการรับมือกับภัยคุกคามทางไซเบอร์ให้แก่หน่วยงานที่เกี่ยวข้องเป็นประจำ ดังนั้น สกมช. จึงได้แต่งตั้งคณะทำงานเพื่อจัดทำมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ โดยมีหน้าที่ในการจัดทำ “มาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ เวอร์ชัน ๑.๐ หรือ Website Security Standard Version 1.0” เพื่อใช้เป็นข้อกำหนดด้านความมั่นคงปลอดภัยทางเว็บไซต์ขั้นต่ำให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องปฏิบัติตาม รวมถึงส่งเสริมและสนับสนุนให้หน่วยงานเอกชนนำไปปรับใช้เป็นแนวทางการรักษาความมั่นคงปลอดภัยเว็บไซต์ต่อไป

๑. ขอบเขต (Scope)

มาตรฐานฉบับนี้มีวัตถุประสงค์เพื่อรักษาความมั่นคงปลอดภัยให้กับเว็บไซต์ของหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมถึงหน่วยงานเอกชน ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ (๕) ซึ่งใช้เป็นข้อกำหนดขั้นต่ำให้เว็บไซต์ที่เชื่อมต่อกับอินเทอร์เน็ต (Internet Facing) เว็บไซต์ที่มีข้อมูลสำคัญ เว็บไซต์ที่ให้บริการข้อมูลประชาชน เว็บไซต์ให้บริการเกี่ยวกับโครงสร้างพื้นฐานสำคัญของประเทศ และเว็บไซต์ของหน่วยงานที่มีการดำเนินการธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งมาตรฐานฉบับนี้ครอบคลุมถึงเว็บไซต์บนระบบขององค์กร (On-Premises) เว็บไซต์บนระบบคลาวด์ (Cloud Service) และเว็บไซต์ที่ใช้บริการเว็บโฮสติ้ง (Web Hosting) โดยขอบเขตของมาตรฐานฉบับนี้ แบ่งเป็น ๒ องค์ประกอบ ดังนี้

๑.๑ องค์ประกอบตามขอบเขต ประกอบด้วย

๑.๑.๑ การกำกับดูแลด้านความมั่นคงปลอดภัยสำหรับเว็บไซต์

เป็นการบริหารจัดการและการดูแลด้านอื่น ๆ ที่เกี่ยวข้อง รวมถึงการบริหารจัดการและมาตรการควบคุมเชิงบริหาร เช่น นโยบายการพัฒนาและจัดการเว็บไซต์ และมาตรการควบคุมเชิงเทคนิค เช่น การควบคุมการเข้าถึงเว็บไซต์และข้อมูล เป็นต้น

๑.๑.๒ การรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์

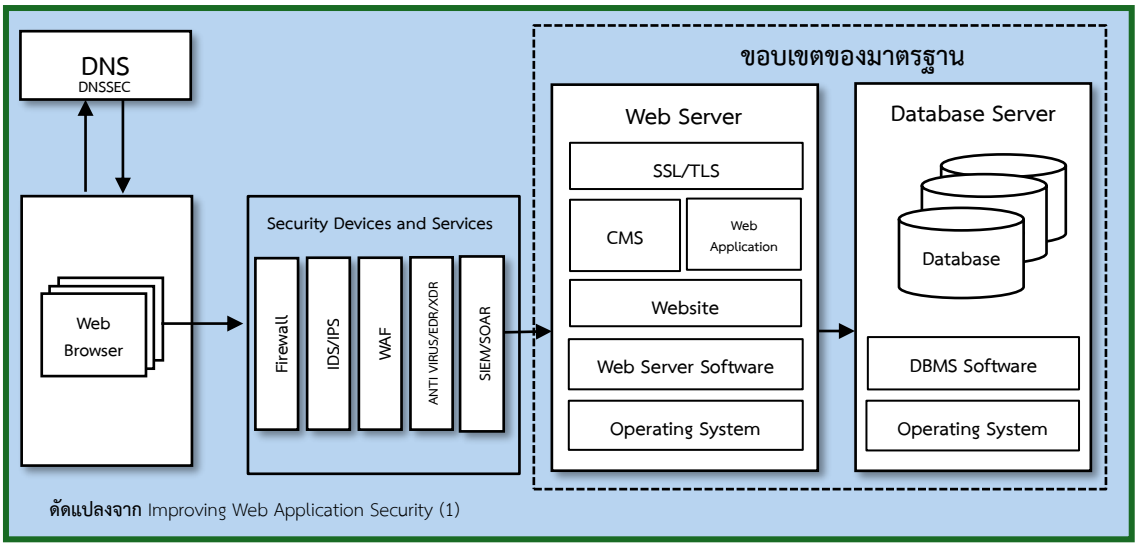
เป็นการดำเนินการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ ใน ๒ ส่วน ดังนี้

๑.๑.๒.๑ เครื่องบริการเว็บ (Web Server) ซึ่งประกอบด้วย เว็บไซต์ (Website) โปรแกรมสำหรับให้บริการเว็บ (Web Server Software) โปรแกรมประยุกต์บนเว็บ (Web Application) ระบบบริหารจัดการเว็บไซต์ (Content Management System: CMS) ระบบปฏิบัติการ (Operating System) และโพรโทคอลสร้างความมั่นคงปลอดภัยในการสื่อสาร SSL/TLS

๑.๑.๒.๒ เครื่องบริการฐานข้อมูล (Database Server) ซึ่งประกอบด้วย ระบบฐานข้อมูล (Database System) ระบบปฏิบัติการ (Operating System) และระบบการจัดการฐานข้อมูล (DBMS Software)

๑.๒ องค์ประกอบอื่น ๆ นอกเหนือขอบเขต เป็นองค์ประกอบที่เกี่ยวข้องกับสภาพแวดล้อมความมั่นคงปลอดภัยของโครงสร้างพื้นฐานทางเทคโนโลยีสารสนเทศของหน่วยงาน ประกอบด้วย ซอฟต์แวร์ด้านความมั่นคงปลอดภัย Endpoint Detection and Response (EDR) ระบบ Extended Detection and Response (XDR) ไฟร์วอลล์ (Firewall) การให้บริการป้องกัน Web Application (Web Application Firewall: WAF) เครื่องคอมพิวเตอร์แม่ข่าย Domain Name System (DNS Server) และ Domain Name System Security Extensions (DNSSEC) รวมถึงมาตรการควบคุมเชิงกายภาพ เช่น การควบคุมการเข้าถึงเครื่องบริการเว็บ (Web Server) ทางกายภาพ เป็นต้น ซึ่งเป็นองค์ประกอบที่หน่วยงานควรจะพิจารณาดำเนินการเพื่อให้เว็บไซต์มีความมั่นคงปลอดภัยจากภัยคุกคามทางไซเบอร์

ซึ่งขอบเขตของมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ แสดงได้ดังภาพที่ ๑



ภาพที่ ๑ ขอบเขตของมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์

มาตรฐานฉบับนี้อ้างอิงข้อกำหนด ข้อเสนอแนะ และแนวปฏิบัติฯ จากมาตรฐานอื่น ๆ ที่เกี่ยวข้อง ตามหัวข้อ ๔ เอกสารอ้างอิง (Normative Reference) โดยมีรูปแบบของคำที่ใช้แสดงในมาตรฐานฉบับนี้ ดังนี้

“จะต้อง” (shall) ใช้ระบุสิ่งที่เป็นข้อกำหนด (Requirement) ซึ่งจะต้องปฏิบัติตาม

“ควรจะ” (should) ใช้ระบุสิ่งที่เป็นข้อเสนอแนะ (Recommendation) ซึ่งควรจะปฏิบัติตาม

“อาจจะ” (may) ใช้ระบุสิ่งที่ยินยอมหรืออนุญาตให้ทำได้ (Permission) ซึ่งอาจจะปฏิบัติตาม

๒. โครงสร้างเอกสาร (Documents Structure)

มาตรฐานฉบับนี้มีโครงสร้างเอกสารดังแสดงในภาพที่ ๒ ประกอบด้วย

๒.๑. ข้อกำหนดในการกำกับดูแลด้านความมั่นคงปลอดภัยสำหรับเว็บไซต์ (Website Security Governance) โดยอ้างอิงจากกรอบทำงานด้านความมั่นคงปลอดภัยไซเบอร์ (NIST Cybersecurity Framework: CSF 2.0) (๒) (หัวข้อที่ ๕)

๒.๒. ข้อกำหนดในการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ (Website Security Operation) โดยอ้างอิงจากประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (๓) (หัวข้อที่ ๖) ประกอบด้วย

๒.๒.๑ การระบุความเสี่ยงที่จะเกิดขึ้นกับเว็บไซต์ (Website Security Identification)

๒.๒.๒ การป้องกันความเสี่ยงที่อาจจะเกิดขึ้นกับเว็บไซต์ (Website Security Protection)

๒.๒.๓ การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Website Security Detection)

๒.๒.๔ การเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Website Incident Response)

๒.๒.๕ การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Website Recovery)

๒.๓. การดำเนินการตามข้อกำหนดขั้นต่ำและแนวทางในการตรวจสอบให้เป็นไปตามมาตรฐานฉบับนี้ (หัวข้อที่ ๗) ประกอบด้วย

๒.๓.๑ การดำเนินการตามข้อกำหนดขั้นต่ำ

๒.๓.๒ แนวทางในการตรวจสอบและปฏิบัติเพื่อให้เป็นไปตามมาตรฐานฉบับนี้

๒.๔. ข้อเสนอแนะนำและคำอธิบายเพิ่มเติม (ภาคผนวก ก และ ข) ซึ่งเป็นข้อเสนอแนะและเป็นการให้ข้อมูลเพิ่มเติมเพื่อการดำเนินการตามหัวข้อที่ ๕ และหัวข้อที่ ๖ ประกอบด้วย

๒.๔.๑ ข้อเสนอแนะนำและคำอธิบายเพิ่มเติมตามข้อกำหนด (หัวข้อ ๕) ในการกำกับดูแลด้านความมั่นคงปลอดภัยสำหรับเว็บไซต์ (ภาคผนวก ก)

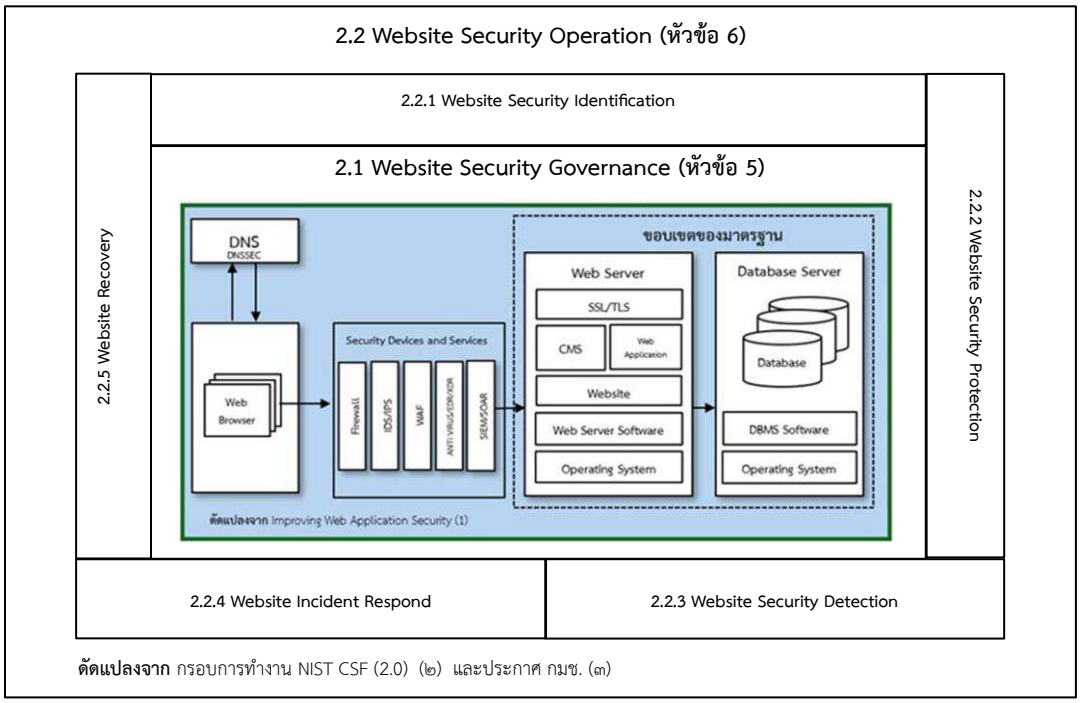
๒.๔.๒ ข้อเสนอแนะนำและคำอธิบายเพิ่มเติมตามข้อกำหนด (หัวข้อ ๖) ในการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ (ภาคผนวก ข)

๒.๕. แบบฟอร์มเพื่อใช้ในการตรวจสอบให้เป็นไปตามมาตรฐานฉบับนี้ (ภาคผนวก ค)

๒.๕.๑ แบบฟอร์ม ค๑ แบบตรวจรายการเพื่อตรวจสอบสถานะการรักษาความมั่นคงปลอดภัยของเว็บไซต์

๒.๕.๒ แบบฟอร์ม ค๒ แบบรายงานการแก้ไขรายการที่ยังต้องปรับปรุง

ซึ่งโครงสร้างของเอกสารมาตรฐานฉบับนี้ แสดงได้ดังภาพที่ ๒



ภาพที่ ๒ โครงสร้างของเอกสารมาตรฐานฉบับนี้

๓. นิยาม (Definitions)

ความหมายของศัพท์และศัพท์ทางเทคนิคที่ใช้กับมาตรฐานฉบับนี้ ฉบับนี้

๓.๑ การรักษาความมั่นคงปลอดภัย (Security) (๖) หมายถึง การทำให้มั่นใจได้ว่าทรัพยากรสารสนเทศที่มีอยู่มีความถูกต้องสมบูรณ์ และพร้อมใช้งานสำหรับผู้ใช้งานที่ได้รับสิทธิ์ในการเข้าถึงทรัพยากรนั้น ๆ ประกอบด้วย ความมั่นคงปลอดภัยเชิงกายภาพ การดำเนินงาน การสื่อสาร เครือข่าย ข้อมูลข่าวสาร และส่วนบุคคล

๓.๒ เว็บไซต์ (Website) (๗, ๘) หมายถึง การรวบรวมหน้าเว็บเพจหลายหน้าที่แสดงข้อมูลบนอินเทอร์เน็ตเกี่ยวกับเรื่องใดเรื่องหนึ่ง เผยแพร่โดยบุคคลหรือองค์กรเดียว โดยมีการเชื่อมโยงกันผ่านทางไฮเปอร์ลิงก์ (Hyperlink) และเปิดด้วยโปรแกรมที่เรียกว่า เว็บเบราว์เซอร์ (Web Browser) โดยจัดเก็บไว้ในเวิลด์ไวด์เว็บ (WWW) เว็บเพจแรกที่พบ เรียกว่า โฮมเพจ (Homepage) ที่มีหัวข้อของข้อมูลในเว็บไซต์ จึงเปรียบเหมือนสารบัญที่ใช้ค้นหาข้อมูลต่อไป

๓.๓ เว็บเพจ (Webpage) (๘) หมายถึง เอกสารเว็บที่สร้างด้วยภาษา HTML หรือ Hypertext Markup Language ซึ่งเป็นภาษามาตรฐานที่ใช้ในการสร้างเว็บเพจ เพื่อแสดงข้อมูลบนอินเทอร์เน็ตเกี่ยวกับหัวข้อใดหัวข้อหนึ่ง ซึ่งประกอบเป็นส่วนหนึ่งของเว็บไซต์

๓.๔ เว็บเบราว์เซอร์ (Web Browser) (๘) หมายถึง โปรแกรมคอมพิวเตอร์ที่ใช้เรียกข้อมูลเว็บจากเครื่องบริการเว็บผ่านระบบเครือข่าย ทำให้สามารถแสดงข้อมูลบนอินเทอร์เน็ตได้

๓.๕ เว็บไซต์ที่ใช้ระบบขององค์กร (On-Premises) (๙, ๑๐) หมายถึง เว็บไซต์ที่เนื้อหาโปรแกรมสำหรับให้บริการเว็บ และโปรแกรมที่เกี่ยวข้องกับการให้บริการเว็บของเว็บไซต์ถูกเก็บอยู่ในเครือข่ายของผู้ให้บริการเว็บไซต์

๓.๖ เว็บไซต์ที่ใช้บริการกับเว็บโฮสติ้ง (Web Hosting) (๙) หมายถึง เว็บไซต์ที่เนื้อหาโปรแกรมสำหรับให้บริการเว็บ และโปรแกรมที่เกี่ยวข้องกับการให้บริการเว็บของเว็บไซต์ถูกเก็บอยู่ในเครือข่ายของผู้ให้บริการเครื่องบริการเว็บ

๓.๗ เว็บไซต์ที่ใช้ระบบคลาวด์ (Cloud Service) (๙, ๑๐) หมายถึง เว็บไซต์ที่มีเนื้อหาโปรแกรมสำหรับให้บริการเว็บ และโปรแกรมที่เกี่ยวข้องกับการให้บริการเว็บของเว็บไซต์ถูกเก็บอยู่ในเครื่องบริการเสมือนบนคลาวด์

๓.๘ เครื่องบริการเว็บ (Web Server) (๘, ๑๑) หมายถึง ระบบคอมพิวเตอร์ที่ให้บริการเวิลด์ไวด์เว็บ บนอินเทอร์เน็ต ซึ่งประกอบด้วย ฮาร์ดแวร์ ระบบปฏิบัติการ โปรแกรมคอมพิวเตอร์สำหรับให้บริการเว็บ และเนื้อหาเว็บไซต์ (เว็บเพจ) ที่ให้บริการเว็บไซต์และข้อมูลไปยังผู้ใช้อินเทอร์เน็ตผ่านระบบเครือข่าย

๓.๙ โปรแกรมสำหรับให้บริการเว็บ (Web Server Software) (๑๒) หมายถึง โปรแกรมคอมพิวเตอร์ที่ติดตั้งบนเครื่องบริการเว็บเพื่อจัดการคำร้องขอข้อมูลเว็บจากผู้ใช้งาน เช่น โปรแกรม Apache โปรแกรม nginx และโปรแกรม Internet Information Service (IIS) เป็นต้น

๓.๑๐ โปรแกรมประยุกต์บนเว็บ (Web Application) หมายถึง โปรแกรมประยุกต์ที่มีความสามารถในการประมวลผลข้อมูลและการทำงานต่าง ๆ โดยเข้าถึงได้ผ่านเว็บเบราว์เซอร์

บนอินเทอร์เน็ต หรืออินทราเน็ต ซึ่งเขียนด้วยภาษาต่าง ๆ เช่น ภาษา HTML ภาษา JavaScript หรือภาษา Java และต้องอาศัยเว็บเบราว์เซอร์ในการเข้าถึง และเรียกใช้งานผ่านระบบเครือข่าย

๓.๑๑ ระบบบริหารจัดการเว็บไซต์ (Content Management System: CMS) หมายถึง โปรแกรมที่ใช้ในการดูแลบริหารจัดการเว็บไซต์ผ่านส่วนต่อประสานแบบเว็บ ซึ่งง่ายต่อการบริหารจัดการเว็บเพจและการปรับปรุงค่าติดตั้งต่าง ๆ ที่เกี่ยวข้อง

๓.๑๒ ระบบปฏิบัติการ (Operating System) (๑๓) หมายถึง ชุดของซอฟต์แวร์ที่บริหารจัดการทรัพยากรฮาร์ดแวร์ของคอมพิวเตอร์ และให้บริการทั่วไปกับโปรแกรมคอมพิวเตอร์

๓.๑๓ โพรโทคอลสร้างความมั่นคงปลอดภัยในการสื่อสาร Secure Sockets Layer (SSL) และ Transport Layer Security (TLS) (๑๔) หมายถึง โพรโทคอลปกป้องความมั่นคงปลอดภัยการสื่อสารผ่านระบบเครือข่าย ในการตรวจสอบสิทธิ์และความมั่นคงปลอดภัยที่ใช้กันอย่างแพร่หลายในเบราว์เซอร์และเว็บเซิร์ฟเวอร์ โดยมีแนวทางการเลือกและใช้งานการใช้งาน Transport Layer Security (TLS) ตาม NIST SP 800-52 ซึ่งระบุถึงวิธีการใช้ TLS ในโปรแกรมประยุกต์ของหน่วยงานภาครัฐ ในปัจจุบันควรใช้โพรโทคอล TLS เวอร์ชันที่มีความมั่นคงปลอดภัยและไม่พบช่องโหว่หรือการโจมตี

๓.๑๔ เครื่องบริการฐานข้อมูล (Database Server) (๑๕) หมายถึง คอมพิวเตอร์หรืออุปกรณ์บนเครือข่ายที่ประมวลผลการร้องขอข้อมูลในฐานข้อมูล

๓.๑๕ ระบบฐานข้อมูล (Database System) หมายถึง โครงสร้างหรือชุดของข้อมูลที่ถูกจัดเก็บและจัดการเพื่อการเข้าถึง แก้ไข และประมวลผลข้อมูลอย่างมีประสิทธิภาพ ระบบนี้มักใช้เพื่อจัดเก็บข้อมูลที่ใช้ในการดำเนินธุรกรรมหรือการจัดการข้อมูลต่าง ๆ ในรูปแบบที่สามารถเข้าถึงได้อย่างรวดเร็วและปลอดภัย สามารถแบ่งได้เป็น ๒ ประเภท ได้แก่ ระบบฐานข้อมูลเชิงสัมพันธ์ (Relational Database) และระบบฐานข้อมูลแบบไม่มีโครงสร้าง (NoSQL Database)

๓.๑๖ ระบบการจัดการฐานข้อมูล (DBMS Software) (๑๖) หมายถึง ซอฟต์แวร์ที่ถูกออกแบบมาเพื่อช่วยในการบำรุงรักษาและใช้ประโยชน์ชุดข้อมูลที่มีขนาดใหญ่

๓.๑๗ เครื่องคอมพิวเตอร์แม่ข่าย Domain Name System (DNS Server) (๑๕, ๑๗) หมายถึง คอมพิวเตอร์หรืออุปกรณ์บนเครือข่ายที่เก็บรักษารายชื่อโดเมนเนม และให้บริการแปลงชื่อโดเมนเป็นเลขที่อยู่ไอพี

๓.๑๘ ส่วนขยายโพรโทคอล DNS (Domain Name System Security Extensions :DNSSEC (๑๘) หมายถึง ส่วนขยายที่ช่วยในการยืนยันความถูกต้องของที่มาและความสมบูรณ์ (Integrity) ของข้อมูลที่ส่งผ่านโพรโทคอล DNS

๓.๑๙ ไฟร์วอลล์ (Firewall) (๑๙) หมายถึง ฮาร์ดแวร์หรือซอฟต์แวร์ที่ป้องกันการเข้าถึงข้อมูลภายในเครือข่ายขององค์กรจากอินเทอร์เน็ตโดยไม่ได้รับอนุญาตเครื่องบริการเว็บ (Web Server)

๓.๒๐ การให้บริการป้องกัน Web Application (Web Application Firewall: WAF) (๒๐) หมายถึง ไฟร์วอลล์สำหรับโปรแกรมประยุกต์ที่ใช้โพรโทคอล HTTP โดยจะใช้กฎการกรองกับการติดต่อสื่อสารผ่านโพรโทคอล HTTP

๓.๒๑ ซอฟต์แวร์ด้านความมั่นคงปลอดภัย Endpoint Detection and Response (EDR) (๒๑) หมายถึง เครื่องมือบันทึกและจัดเก็บพฤติกรรมในระดับของระบบของอุปกรณ์ปลายทางและวิเคราะห์ข้อมูลเหล่านั้น เพื่อตรวจจับพฤติกรรมต้องสงสัย ให้ข้อมูลเกี่ยวกับบริบทของอุปกรณ์ปลายทาง ยับยั้งกิจกรรมที่มุ่งร้ายต่อระบบและให้คำแนะนำในการแก้ปัญหาระบบที่โดนโจมตี

๓.๒๒ ระบบ Extended Detection and Response (XDR) (๒๒) หมายถึง แพลตฟอร์มผสานการตรวจจับและตอบสนองเหตุการณ์ทางด้านความมั่นคงปลอดภัย โดยจะรวบรวมและหาความสัมพันธ์ของข้อมูลจากอุปกรณ์รักษาความมั่นคงปลอดภัยแต่ละประเภทโดยอัตโนมัติ

๔. เอกสารอ้างอิง (Normative References)

เอกสารที่ระบุต่อไปนี้ ให้ถือเป็นส่วนหนึ่งของมาตรฐานฉบับนี้ด้วย เอกสารที่มีการอ้างอิงโดยระบุปีให้ใช้เอกสารฉบับตามปีที่ระบุไว้ สำหรับเอกสารที่มีการอ้างอิงโดยไม่ระบุปี ให้ใช้เอกสารล่าสุด (รวมถึงการเพิ่มเติมต่าง ๆ)

๔.๑ ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. ๒๕๖๖ (๒๓)

๔.๒ ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานขั้นต่ำของข้อมูลหรือระบบสารสนเทศ พ.ศ.๒๕๖๖ (๒๔)

๔.๓ ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (๓)

๔.๔ ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. ๒๕๖๗ (๒๕)

๔.๕ คำแนะนำของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง แนวปฏิบัติการรักษาความมั่นคงปลอดภัยเว็บไซต์ (Website Security Guideline) สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (๒๖)

๔.๖ ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับโปรแกรมประยุกต์บนเว็บ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (๒๗)

๔.๗ มาตรฐานเว็บไซต์ภาครัฐ เวอร์ชัน ๓.๐ (Government Website Standard Version 3.0) สำนักงานพัฒนารัฐบาลดิจิทัล (๒๘)

๔.๘ ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕ (๒๙)

๔.๙ คำแนะนำของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง แนวทางปฏิบัติในการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

และการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (๓๐)

๔.๑๐ กรอบการทำงานด้านความมั่นคงปลอดภัยไซเบอร์ของ NIST Cybersecurity Framework (CSF) 2.0 (๒)

๔.๑๑ ข้อเสนอแนะของ NIST Special Publication 800-88 Guidelines for Media Sanitization (๓๑)

๔.๑๒ ปัจจัยเสี่ยงด้านความมั่นคงปลอดภัยของเว็บไซต์ที่พบได้บ่อยที่ ของมูลนิธิ Open Worldwide Application Security Project (OWASP) (๓๒)

๕. ข้อกำหนดการกำกับดูแลด้านความมั่นคงปลอดภัยสำหรับเว็บไซต์ (Website Security Governance Requirement)

หน่วยงานจะต้องดำเนินการกำกับดูแลด้านความมั่นคงปลอดภัยสำหรับเว็บไซต์ โดยดำเนินการในส่วนที่เกี่ยวข้อง[๑] [๒] อ้างอิงกรอบทำงานด้านความมั่นคงปลอดภัยไซเบอร์ (NIST Cybersecurity Framework: CSF 2.0) (๒) และประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (๓) ดังนี้

๕.๑. การสำรวจบริบทของหน่วยงาน (Organization Context)

๕.๑.๑. หน่วยงานจะต้องมีการทำความเข้าใจสถานการณ์ต่าง ๆ ประกอบด้วย ภารกิจ ความคาดหวังของผู้มีส่วนได้ส่วนเสีย การขึ้นต่อกัน และกฎหมาย กฎระเบียบ และข้อกำหนดของสัญญาที่เกี่ยวข้องกับการตัดสินใจในการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสำหรับเว็บไซต์ของหน่วยงาน ซึ่งมาตรฐานฉบับนี้ มีข้อเสนอแนะและรายละเอียดเพิ่มเติม ตามภาคผนวก ก

๕.๒. นโยบายด้านความมั่นคงปลอดภัยสำหรับเว็บไซต์ (Website Security Policies)

๕.๒.๑. หน่วยงานจะต้องมีการกำหนดนโยบายความมั่นคงปลอดภัยสำหรับเว็บไซต์ตามบริบทขององค์กรและกลยุทธ์ด้านความมั่นคงปลอดภัยเว็บไซต์ โดยมีการจัดลำดับความสำคัญ มีการสื่อสาร รวมถึงมีการบังคับใช้ ซึ่งมาตรฐานฉบับนี้ มีข้อเสนอแนะและรายละเอียดเพิ่มเติม ตามภาคผนวก ก

๕.๒.๒. หน่วยงานจะต้องมีการทบทวน ปรับปรุง สื่อสาร และบังคับใช้นโยบายความมั่นคงปลอดภัยสำหรับเว็บไซต์ เพื่อสะท้อนการเปลี่ยนแปลงความต้องการ ภัยคุกคาม เทคโนโลยี รวมถึงภารกิจของหน่วยงาน

---

[๑] National Institute of Standards and Technology. The NIST Cybersecurity Framework (CSF) 2.0

[๒] คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์. ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๕.๓. กลยุทธ์การจัดการความเสี่ยง (Risk Management Strategy)

๕.๓.๑. หน่วยงานจะต้องกำหนดวัตถุประสงค์การบริหารความเสี่ยงโดยได้รับความเห็นชอบจากผู้มีส่วนได้ส่วนเสียของหน่วยงาน และจะต้องมีการจัดทำกรอบการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสำหรับเว็บไซต์เป็นลายลักษณ์อักษร โดยกรอบรวมถึงเกณฑ์ประเมินความเสี่ยงด้านความมั่นคงปลอดภัยและระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) ค่าเบี่ยงเบนของระดับความเสี่ยงที่ยอมรับได้ (Risk Tolerance) วิธีการประเมินความเสี่ยง การเฝ้าระวังและติดตามความเสี่ยง ซึ่งมาตรฐานฉบับนี้ มีข้อเสนอแนะและรายละเอียดเพิ่มเติม ตามภาคผนวก ก

๕.๓.๒. หน่วยงานจะต้องพิจารณาดำเนินการตามคำแนะนำของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง แนวทางปฏิบัติในการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ในกรณีที่เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (๓๐)

๕.๓.๓. หน่วยงานจะต้องมีการจัดทำ สื่อสาร และมีการเก็บรักษารายการความเสี่ยงที่ระบุไว้ในทะเบียนความเสี่ยง (Risk Register) ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) และค่าเบี่ยงเบนของระดับความเสี่ยงที่ยอมรับได้ (Risk Tolerance) ให้เป็นปัจจุบัน และติดตามระดับความเสี่ยงให้อยู่ในเกณฑ์ที่ยอมรับได้

๕.๔. บทบาทและความรับผิดชอบด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ (Information Security Roles and Responsibilities)

๕.๔.๑. หน่วยงานจะต้องมีการจัดโครงสร้างองค์กรให้มีการถ่วงดุล พร้อมกำหนดอำนาจบทบาทหน้าที่ และความรับผิดชอบ (Authorities, Roles and Responsibilities) ที่ชัดเจนในการบริหารจัดการความมั่นคงปลอดภัยสำหรับเว็บไซต์ ซึ่งมาตรฐานฉบับนี้มีข้อเสนอแนะและรายละเอียดเพิ่มเติมตามภาคผนวก ก

๕.๔.๒. หน่วยงานจะต้องกำหนดให้มีผู้รับผิดชอบในการจัดทำ และบริการจัดการเว็บไซต์ของหน่วยงาน รวมถึงการดำเนินการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ ซึ่งต้องเป็นนิติบุคคลหรือเป็นส่วนหนึ่งของนิติบุคคลที่สามารถรับผิดตามกฎหมายได้ และมีการมอบหมายหน้าที่จะต้องทำโดยไม่ขาดช่วง

๕.๔.๓. หน่วยงานจะต้องมีการกำหนด สื่อสาร ทำความเข้าใจ และบังคับใช้บทบาท ความรับผิดชอบ และอำนาจที่เกี่ยวข้องกับการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสำหรับเว็บไซต์ รวมถึงจัดสรรทรัพยากรให้เพียงพอตามกลยุทธ์ บทบาท ความรับผิดชอบ และนโยบายความเสี่ยงด้านความมั่นคงปลอดภัยสำหรับเว็บไซต์

๕.๕. การวางแผนกำหนดความต้องการด้านความมั่นคงปลอดภัยของเว็บไซต์

๕.๕.๑. หน่วยงานจะต้องมีการกำหนดวัตถุประสงค์และความต้องการในการจัดทำเว็บไซต์ด้านฟังก์ชัน ด้านประสิทธิภาพ และที่สำคัญความต้องการด้านความมั่นคงปลอดภัย ซึ่งมาตรฐานฉบับนี้มีข้อเสนอแนะและรายละเอียดเพิ่มเติมตามภาคผนวก ก

๕.๖. การกำหนดแนวทางด้านความมั่นคงปลอดภัยสำหรับเว็บไซต์

๕.๖.๑. หน่วยงานจะต้องมีแนวทางด้านความมั่นคงปลอดภัยในระดับพื้นฐานตามคุณลักษณะด้านความมั่นคงปลอดภัยพื้นฐาน ๓ ด้าน คือ การรักษาความลับ (Confidentiality) การรักษาความครบถ้วนสมบูรณ์ (Integrity) และการเตรียมความพร้อมใช้งาน (Availability) ซึ่งมาตรฐานฉบับนี้ มีข้อเสนอแนะและรายละเอียดเพิ่มเติม ตามภาคผนวก ก

๕.๖.๒. หน่วยงานจะต้องกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้กับข้อมูลหรือสารสนเทศของเว็บไซต์ ให้ประเมินและจัดระดับผลกระทบที่อาจจะเกิดขึ้น ๓ ระดับ ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. ๒๕๖๖ (๒๓) เพื่อระบุข้อกำหนดขั้นต่ำในการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์

๕.๖.๓. หน่วยงานจะต้องดำเนินการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ตามข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับโปรแกรมประยุกต์บนเว็บ (๒๗) รวมถึงประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕ (๒๙) ในกรณีที่เว็บไซต์หน่วยงานมีการดำเนินการธุรกรรมทางอิเล็กทรอนิกส์

๕.๖.๔. หน่วยงานจะต้องดำเนินการตามมาตรฐานเว็บไซต์ภาครัฐ เวอร์ชัน ๓.๐ (Government Website Standard Version 3.0) หัวข้อที่ ๗ ความมั่นคงปลอดภัยสำหรับเว็บไซต์ในกรณีที่เป็นเว็บไซต์หน่วยงานภาครัฐ (๒๘)

๕.๖.๕. หน่วยงานจะต้องดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับเว็บไซต์ที่ใช้บริการคลาวด์ (Cloud Service) ให้เป็นไปตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. ๒๕๖๗ (๒๕)

๕.๖.๖. หน่วยงานจะต้องพิจารณาเลือกผู้ให้บริการด้านความมั่นคงปลอดภัยไซเบอร์สำหรับเว็บไซต์ เช่น การดำเนินการประเมินช่องโหว่ (Vulnerability Assessment) การทดสอบเจาะระบบ (Penetration Testing) ของเว็บไซต์ ที่ได้รับการรับรองและได้รับประกาศนียบัตร (Accreditations and Certifications) ที่เป็นที่ยอมรับในอุตสาหกรรม

๕.๖.๗. หน่วยงานจะต้องปฏิบัติตามคำแนะนำของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง แนวปฏิบัติการรักษาความมั่นคงปลอดภัยเว็บไซต์ (Website Security Guideline) ในกรณีที่เป็นเว็บไซต์หน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (๒๖)

๕.๖.๘. หน่วยงานจะต้องมีการกำหนดแนวทางในการสำรองข้อมูลเพื่อลดผลกระทบที่เกิดขึ้น หากเว็บไซต์ของหน่วยงานโดนโจมตีจากภัยคุกคามทางไซเบอร์ รวมถึงความเสียหายจากภัยธรรมชาติหรือข้อผิดพลาดจากมนุษย์ ซึ่งมาตรฐานฉบับนี้ มีข้อเสนอแนะและรายละเอียดเพิ่มเติม ตามภาคผนวก ก

๕.๖.๙. หน่วยงานจะต้องมีการจัดการข้อมูลจราจรทางคอมพิวเตอร์ (Log Management) ให้เป็นไปตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และที่แก้ไขเพิ่มเติม ซึ่งมาตรฐานฉบับนี้มีข้อเสนอแนะและรายละเอียดเพิ่มเติมตามภาคผนวก ก

๕.๖.๑๐. หน่วยงานจะต้องกำหนดหลักปฏิบัติในการเลิกใช้งานเว็บไซต์ เพื่อป้องกันภัยคุกคามไซเบอร์ที่อาจจะเกิดกับผู้ใช้บริการเว็บไซต์ ผู้ใช้งานอินเทอร์เน็ตทั่วไป ผู้ให้บริการ โดยหน่วยงานอาจจะพิจารณาปฏิบัติตามข้อเสนอแนะของ NIST Special Publication 800-88 Guidelines for Media Sanitization (๓๑) ซึ่งมาตรฐานฉบับนี้มีข้อเสนอแนะและรายละเอียดเพิ่มเติมตามภาคผนวก ก

๖. ข้อกำหนดการดำเนินการและการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ (Security and Operation Requirements)

หน่วยงานจะต้องดำเนินการและรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ (Website Security and Operation Requirements) โดยดำเนินการในส่วนที่เกี่ยวข้อง[๓] อ้างอิงประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (๓) ดังนี้

๖.๑. การระบุความเสี่ยงที่จะเกิดขึ้นกับเว็บไซต์ (Website Security Identification)

๖.๑.๑. หน่วยงานจะต้องมีการจัดการทรัพย์สิน (Asset Management) การประเมินความเสี่ยง (Risk Assessment) การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing) และการจัดการผู้ให้บริการภายนอก (Third Party Management) ให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (๓) ซึ่งมาตรฐานฉบับนี้มีข้อเสนอแนะและรายละเอียดเพิ่มเติมตามภาคผนวก ข

๖.๒. การป้องกันความเสี่ยงที่อาจจะเกิดขึ้นกับเว็บไซต์ (Website Security Protection)

๖.๒.๑. หน่วยงานจะต้องกำหนดแนวทางในการพัฒนาโปรแกรมประยุกต์บนเว็บ (Web Application) อย่างมั่นคงปลอดภัย เช่น พิจารณาใช้หลักการ DevSecOps ตั้งแต่ขั้นตอนการพัฒนาจนถึงการใช้งานจริงโดยมีการคำนึงถึงสิ่งสำคัญในการรักษาความมั่นคงปลอดภัยในการพัฒนาโปรแกรมประยุกต์บนเว็บ และอาจจะพิจารณาตัวอย่างการออกแบบเว็บไซต์ที่มีความมั่นคงปลอดภัย ซึ่งมาตรฐานฉบับนี้มีข้อเสนอแนะและรายละเอียดเพิ่มเติมตามภาคผนวก ข

๖.๒.๒. หน่วยงานจะต้องพิจารณาถึงปัจจัยเสี่ยงด้านความมั่นคงปลอดภัยของเว็บไซต์ที่พบได้บ่อย ของมูลนิธิ OWASP (๓๒) ในการพัฒนาโปรแกรมประยุกต์บนเว็บ (Web Application) ซึ่งมาตรฐานฉบับนี้มีข้อเสนอแนะและรายละเอียดเพิ่มเติมตามภาคผนวก ข

๖.๒.๓. หน่วยงานจะต้องพิจารณาการออกแบบสถาปัตยกรรมเว็บไซต์อย่างมั่นคงปลอดภัย ในส่วนของโครงสร้างของเว็บไซต์หรือโปรแกรมประยุกต์บนเว็บ โดยอาจจะมีส่วนประกอบ

---

[๓] คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์. ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

ของการออกแบบที่คำนึงถึงการแบ่งส่วนเครือข่าย (Network segmentation) มีการจัดวางเครื่องบริการเว็บ (Web Server) และเครื่องบริการฐานข้อมูล (Database Server) ร่วมกับอุปกรณ์รักษาความมั่นคงปลอดภัย เช่น

(๑) ไฟร์วอลล์ (Firewall)

(๒) ระบบตรวจจับการบุกรุกและระบบป้องกันการบุกรุก (Intrusion Detection Systems: IDS/Intrusion Prevention Systems: IPS)

(๓) ซอฟต์แวร์ตรวจจับและตอบสนองภัยคุกคาม เช่น ซอฟต์แวร์ป้องกันไวรัส (Antivirus) ซอฟต์แวร์ EDR

(๔) การให้บริการป้องกัน Web Application (WAF)

หากหน่วยงานที่มีทรัพยากรเพียงพออาจจะพิจารณาผลิตภัณฑ์การรักษาความมั่นคงปลอดภัยเพิ่มเติม ดังนี้

(๕) ระบบการจัดการเหตุการณ์และตอบสนองด้านความมั่นคงปลอดภัย (Security Information and Event Management: SIEM)

(๖) ระบบ XDR

(๗) ระบบ SOAR (Security Orchestration, Automation, and Response)

ซึ่งมาตรฐานฉบับนี้ มีข้อเสนอแนะและรายละเอียดเพิ่มเติม ตามภาคผนวก ข

๖.๒.๔. หน่วยงานจะต้องมีการควบคุมการเข้าถึง (Access Control) การทำให้ระบบมีความแข็งแกร่ง (System Hardening) มีการบริหารจัดการเชื่อมต่อระยะไกล (Remote Connection) การบริหารจัดการสื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media) และมีบริหารจัดการแบ่งปันข้อมูล (Information Sharing) และมีการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยสำหรับเว็บไซต์ (Website Security Awareness) ให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ซึ่งมาตรฐานฉบับนี้ มีข้อเสนอแนะและรายละเอียดเพิ่มเติม ตามภาคผนวก ข

๖.๒.๕. หน่วยงานจะต้องพิจารณาการพิสูจน์ตัวตนแบบหลายปัจจัย (Multi-Factor Authentication: MFA) หรือพิจารณาการพิสูจน์ตัวตนจากระบบเชื่อมโยงข้อมูลเพื่อการพิสูจน์และยืนยันตัวตนทางดิจิทัล (Digital ID) ตามข้อเสนอแนะของ สพร. นอกเหนือจากการควบคุมการเข้าถึง (Access Control) ข้อ ๖.๒.๔ เพื่อเพิ่มความมั่นคงปลอดภัยให้กับเว็บไซต์ โดยอาจจะพิจารณาเลือกจากสิ่งที่ผู้ใช้รู้ (Something they know) เช่น รหัสผ่าน สิ่งที่ผู้ใช้มี (Something they have) เช่น โทเค็นการตรวจสอบ หรือสิ่งที่ผู้ใช้เป็น (Something they are) เช่น ลายนิ้วมือ ลายฝ่ามือ หรือข้อมูลชีวมิติอื่น ซึ่งมาตรฐานฉบับนี้ มีข้อเสนอแนะและรายละเอียดเพิ่มเติม ตามภาคผนวก ข

๖.๒.๖. หน่วยงานจะต้องตั้งค่าความมั่นคงปลอดภัยพื้นฐานของโปรแกรมสำหรับให้บริการเว็บ (Web Server Software) โปรแกรมประยุกต์บนเว็บ (Web Application) ระบบบริหารจัดการเว็บไซต์ (CMS) ระบบปฏิบัติการ (Operating System) และการตั้งค่าฐานข้อมูล ซึ่งมาตรฐานฉบับนี้มีข้อเสนอแนะและรายละเอียดเพิ่มเติม ตามภาคผนวก ข

๖.๒.๗. หน่วยงานจะต้องกำหนดแนวทางและการเลือกบริการที่เกี่ยวข้องกับเว็บไซต์ ประกอบด้วย เครื่องบริการเว็บ (Web Server) ระบบบริหารจัดการเว็บไซต์ (CMS) เลือกบริการโดเมนและชื่อโดเมน และขั้นตอนวิธีการเข้ารหัส Cipher Suite ของ TLS Certificate ซึ่งมาตรฐานฉบับนี้ มีข้อเสนอแนะและรายละเอียดเพิ่มเติม ตามภาคผนวก ข

๖.๒.๘. หน่วยงานจะต้องตั้งค่าไฟร์วอลล์เพื่อควบคุมและป้องกันการบุกรุกต่าง ๆ ที่เกิดขึ้นกับเว็บไซต์ โดยควรจะพิจารณาหลักการตั้งค่าอย่างน้อย ดังนี้ การกำหนดนโยบายความมั่นคงปลอดภัย (Define Security Policies) การตั้งค่ากฎการกรอง (Configure Filtering Rules) การจำกัด การเข้าถึงโดยภูมิศาสตร์ (Geographic Restrictions) การป้องกันการโจมตี (Protect Against Attacks) การตรวจสอบและบันทึก (Monitoring and Logging) และการปรับปรุงและอัปเดตเป็นประจำ (Regular Updates) ซึ่งมาตรฐานฉบับนี้ มีข้อเสนอแนะและรายละเอียดเพิ่มเติม ตามภาคผนวก ข

๖.๓. มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์สำหรับเว็บไซต์ (Website Security Detection)

๖.๓.๑. หน่วยงานจะต้องมีการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring) ให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (๓) ซึ่งมาตรฐานฉบับนี้ มีข้อเสนอแนะและรายละเอียดเพิ่มเติม ตามภาคผนวก ข

๖.๔. การเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์สำหรับเว็บไซต์ (Website Incident Response)

๖.๔.๑. หน่วยงานจะต้องจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์สำหรับเว็บไซต์ (Website security Incident Response Plan) และมีการสื่อสาร ฝึกซ้อม ทบทวน และปรับปรุงแผนการรับมือภัยคุกคามทางไซเบอร์ของเว็บไซต์ รวมถึงแผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan) และการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์สำหรับเว็บไซต์ (Website Security Exercise) ให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (๓) ซึ่งมาตรฐานฉบับนี้ มีคำอธิบายเพิ่มเติม ตามภาคผนวก ข

๖.๕. การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์สำหรับเว็บไซต์ (Website Recovery)

๖.๕.๑. หน่วยงานจะต้องมีการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์สำหรับเว็บไซต์ (Website Security Resilience and Recovery) โดยจะต้องจัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP) โดยอาจจะพิจารณารายละเอียดของแผนให้เป็นไปตามการบริหารความพร้อมต่อสภาวะวิกฤติ (การทำแผน BCP) ของสำนักงานคณะกรรมการพัฒนาระบบราชการ (๓๓) และจะต้องจัดให้มีการฝึกซ้อมให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (๓)

๗. แนวทางในการดำเนินการตามข้อกำหนดขั้นต่ำ และแนวทางในตรวจสอบและปฏิบัติให้เป็นไปตามมาตรฐานฉบับนี้

๗.๑ แนวทางในการดำเนินการตามข้อกำหนดขั้นต่ำ

๗.๑.๑ ให้หน่วยงานกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้กับข้อมูลหรือสารสนเทศของเว็บไซต์ของหน่วยงานครบทั้ง ๓ ด้าน ซึ่งประกอบด้วย ด้านการรักษาความลับ (Confidentiality) การรักษาความถูกต้องครบถ้วน (Integrity) และการรักษาสภาพพร้อมใช้ (Availability) ตามส่วนที่ ๒ (ตาราง ค๑-ตาราง ค๕) ของแบบตรวจรายการเพื่อตรวจสอบสถานะความมั่นคงปลอดภัยสำหรับเว็บไซต์ (แบบฟอร์ม ค๑) ในภาคผนวก ค

๗.๑.๒ ให้หน่วยงานนำผลที่ได้ (ตาราง ค๑-ตาราง ค๕) มาระบุเกณฑ์การดำเนินการตามข้อกำหนดขั้นต่ำในการปฏิบัติตามมาตรฐานฉบับนี้ ในตาราง ค๖

๗.๑.๓ ให้หน่วยงานตรวจสอบหน่วยงานตนเพื่อ “ต้องปฏิบัติตาม” หรือ “ส่งเสริมให้ปฏิบัติตาม” ข้อกำหนดขั้นต่ำ ตามตาราง ค๗ จากนั้นดำเนินการตามแนวทางในการตรวจสอบและปฏิบัติให้เป็นไปตามมาตรฐาน ข้อ ๗.๒

๗.๒ แนวทางในการตรวจสอบและปฏิบัติเพื่อให้เป็นไปตามมาตรฐานฉบับนี้

๗.๒.๑ กรณีที่หน่วยงานยังไม่ได้รับรอง ISO/IEC 27001 หรือที่ได้รับการรับรองแต่ขอบเขตของการรับรองไม่ครอบคลุมถึงเว็บไซต์ของหน่วยงาน จะต้องดำเนินการ ดังนี้

๗.๒.๑.๑ หน่วยงานกลุ่มที่ ๑ (หน่วยงานที่ต้องปฏิบัติตาม) หน่วยงานจะต้องประเมินตนเอง (Self-Assessment) ตามแบบตรวจรายการเพื่อตรวจสอบสถานะความมั่นคงปลอดภัยสำหรับเว็บไซต์ (แบบฟอร์ม ค๑) ในภาคผนวก ค อย่างน้อยปีละ ๑ ครั้ง เพื่อตรวจสอบการดำเนินการให้เป็นไปตามข้อกำหนดขั้นต่ำของมาตรฐานฉบับนี้ ดังนี้

๑) เว็บไซต์ของหน่วยงานที่มีผลกระทบระดับต่ำ หรือระดับกลาง ให้หน่วยงานจัดทำรายงานผลการประเมินตนเอง (Self-Assessment) (แบบฟอร์ม ค๑) ในภาคผนวก ค และรายงานผลการแก้ไขรายการที่ยังต้องปรับปรุง (แบบฟอร์ม ค๒) ในภาคผนวก ค พร้อมแนบหลักฐาน เสนอต่อผู้บริหารสูงสุดของหน่วยงาน และเก็บรักษาไว้ที่หน่วยงาน

๒) หากเว็บไซต์ของหน่วยงานมีผลกระทบระดับสูง ให้หน่วยงานจัดทำรายงานผลการประเมินตนเอง (Self-Assessment) (แบบฟอร์ม ค๑) ในภาคผนวก ค และรายงานผลการแก้ไขรายการที่ยังต้องปรับปรุง (แบบฟอร์ม ค๒) ในภาคผนวก ค พร้อมแนบหลักฐาน เสนอต่อผู้บริหารสูงสุดของหน่วยงาน หน่วยงานควบคุมหรือกำกับดูแล และส่งสำเนาให้สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

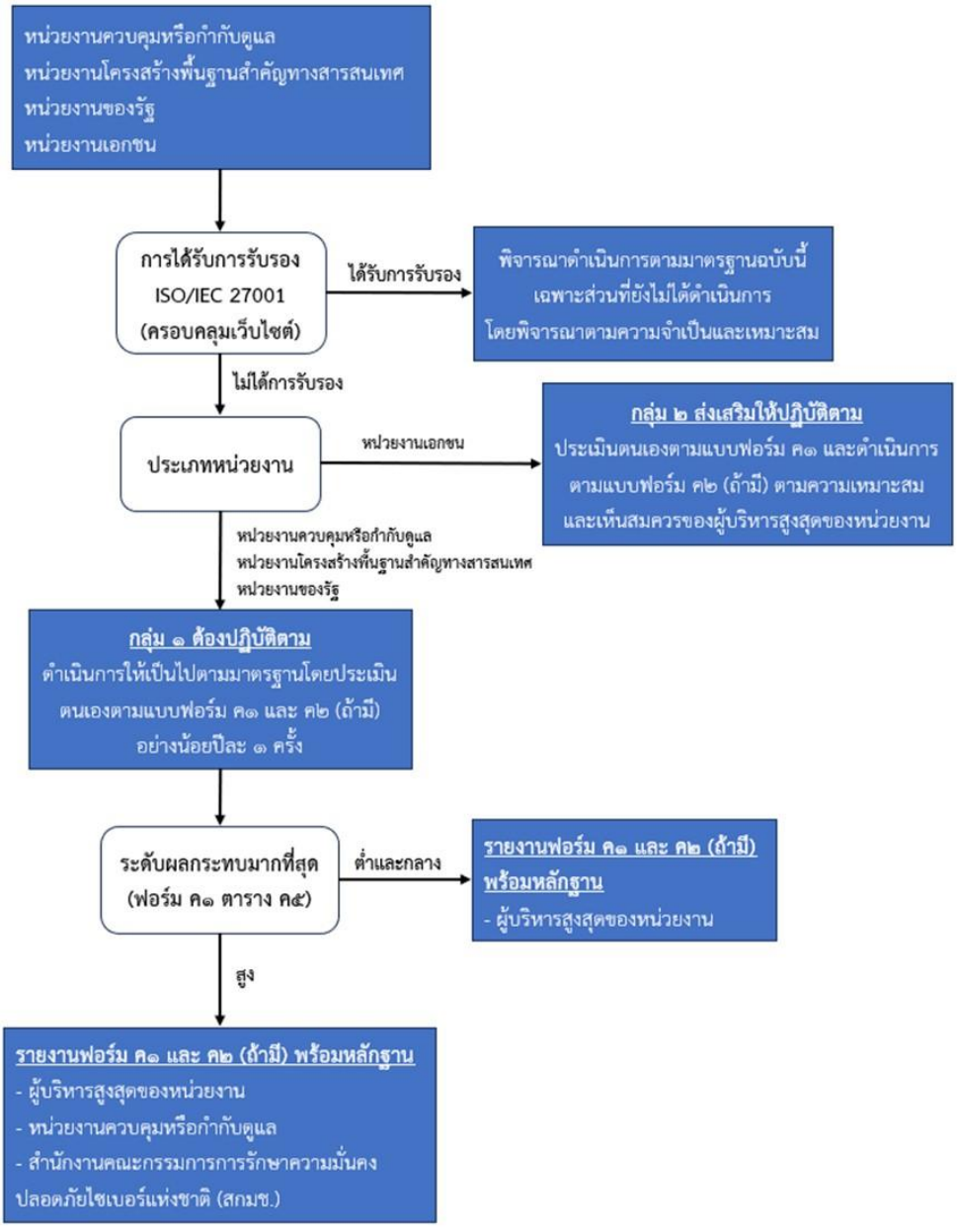
๓) หากหน่วยงานประเมินตนเองแล้ว พบว่า เว็บไซต์ของหน่วยงานมีข้อกำหนดที่มีผลการประเมิน “ยังต้องปรับปรุง” ให้หน่วยงานดำเนินการปรับปรุงตามแบบรายงานรายการที่ยังต้องปรับปรุง (แบบฟอร์ม ค๒) ในภาคผนวก ค

๗.๒.๑.๒ หน่วยงานกลุ่มที่ ๒ (หน่วยงานที่ส่งเสริมให้ปฏิบัติตาม) หน่วยงานจะต้องประเมินตนเอง (Self-Assessment) ตามแบบตรวจรายการเพื่อตรวจสอบสถานะความมั่นคง

ปลอดภัยสำหรับเว็บไซต์ (แบบฟอร์ม ค๑) ในภาคผนวก ค ซึ่งหากมีข้อกำหนดที่มีผลการประเมิน “ยังต้องปรับปรุง” หน่วยงานอาจจะพิจารณาดำเนินการปรับปรุงตามรายการที่ยังต้องปรับปรุง (แบบฟอร์ม ค๒) ในภาคผนวก ค ตามความเหมาะสมและเห็นสมควรของผู้บริหารสูงสุดของหน่วยงาน

๗.๒.๒ กรณีหน่วยงานได้รับการรับรอง ISO/IEC 27001 ที่มีขอบเขตในการรับรองที่ครอบคลุมถึงเว็บไซต์ของหน่วยงานแล้ว หน่วยงานอาจจะพิจารณาดำเนินการตามมาตรฐานฉบับนี้เฉพาะส่วนที่ยังไม่ได้ดำเนินการตามมาตรฐาน ISO/IEC 27001 ตามที่หน่วยงานได้รับการรับรองนั้น โดยพิจารณาตามความจำเป็นและเหมาะสม

หน่วยงานสามารถศึกษาแนวทางในการปฏิบัติเพื่อให้เป็นไปตามมาตรฐานฉบับนี้ ได้จากแผนผังในภาพที่ ๓



ภาพที่ ๓ แนวทางในการปฏิบัติเพื่อให้เป็นไปตามมาตรฐานฉบับนี้

ภาคผนวก ก

รายละเอียดข้อเสนอแนะและคำอธิบายเพิ่มเติม
(ข้อ ๕)
(เป็นข้อมูลเพิ่มเติม)

ข้อ ๕.๑ ตัวอย่างในการดำเนินการในส่วนบริบทขององค์กร

การดำเนินการในส่วนบริบทองค์กรในหัวข้อการสำรวจบริบทของหน่วยงาน (Organization Context) ตามข้อกำหนดในการกำกับดูแลด้านความมั่นคงปลอดภัยสำหรับเว็บไซต์ (Website Security Governance Requirement) หน่วยงานอาจจะพิจารณาดำเนินการ โดยมีรายละเอียดตามตารางที่ ก๑

ตาราง ก๑ ตัวอย่างในการดำเนินการในส่วนบริบทองค์กร

หัวข้อ	ตัวอย่างการดำเนินการ
ภารกิจของหน่วยงาน หน่วยงานจะต้องทำความเข้าใจภารกิจและรายงานการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์	ตัวอย่างที่ ๑ หน่วยงานมีการเผยแพร่พันธกิจของหน่วยงาน ตัวอย่างเช่น เผยแพร่ผ่านวิสัยทัศน์ พันธกิจ กลยุทธ์ทางการตลาดและบริการเพื่อใช้เป็นพื้นฐานในการระบุความเสี่ยงที่จะส่งผลกระทบต่อภารกิจของหน่วยงาน
ผู้มีส่วนได้ส่วนเสียภายในและภายนอก หน่วยงานมีความเข้าใจในความต้องการและความคาดหวังเกี่ยวกับการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์ของผู้มีส่วนได้ส่วนเสียภายในและภายนอก	ตัวอย่างที่ ๑ หน่วยงานระบุผู้มีส่วนได้ส่วนเสียภายในที่มีส่วนเกี่ยวข้องและมีความคาดหวังทางด้านความมั่นคงปลอดภัยไซเบอร์ ตัวอย่างเช่น ความคาดหวังด้านประสิทธิภาพและด้านเสี่ยงของเจ้าหน้าที่ ผู้อำนวยการและที่ปรึกษา ความคาดหวังด้านวัฒนธรรมของพนักงาน ตัวอย่างที่ ๒ หน่วยงานระบุผู้มีส่วนได้ส่วนเสียภายนอกที่เกี่ยวข้องและความคาดหวังทางด้านความมั่นคงปลอดภัยไซเบอร์ ตัวอย่างเช่น ความคาดหวังด้านความเป็นส่วนตัว ความคาดหวังทางธุรกิจของหุ้นส่วน ความคาดหวังในการปฏิบัติตามกฎระเบียบของหน่วยงานกำกับดูแล ความคาดหวังด้านจริยธรรมของสังคม
ข้อกำหนดทางกฎหมาย ข้อบังคับและสัญญา หน่วยงานมีความเข้าใจและมีการจัดการด้านข้อกำหนดทางกฎหมาย ข้อบังคับและข้อกำหนดของสัญญาที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์ รวมถึง ข้อผูกพันด้านความเป็นส่วนตัวและเสรีภาพของประชาชน	ตัวอย่างที่ ๑ หน่วยงานกำหนดกระบวนการเพื่อติดตามและจัดการข้อกำหนดทางกฎหมาย และข้อบังคับเกี่ยวกับการปกป้องข้อมูลส่วนบุคคล ตัวอย่างที่ ๒ หน่วยงานกำหนดกระบวนการในการติดตามและจัดการข้อกำหนดตามสัญญาของการจัดการความมั่นคงปลอดภัยทางไซเบอร์ของข้อมูลซัพพลายเออร์ ลูกค้า และคู่ค้า ตัวอย่างที่ ๓ หน่วยงานจัดกลยุทธ์ความมั่นคงปลอดภัยทางไซเบอร์สำหรับเว็บไซต์ของหน่วยงานให้สอดคล้องกับข้อกำหนดทางกฎหมาย ข้อบังคับ และข้อกำหนดตามสัญญา

หัวข้อ	ตัวอย่างการดำเนินการ
หน่วยงานได้ทำความเข้าใจและสื่อสารวัตถุประสงค์ ความสามารถและบริการที่สำคัญที่ขึ้นอยู่กับความคาดหวังของผู้มีส่วนได้ส่วนเสียของหน่วยงาน	ตัวอย่างที่ ๑ หน่วยงานกำหนดเกณฑ์ในการพิจารณาความสำคัญของสมรรถนะและบริการตามมุมมองของผู้มีส่วนได้ส่วนเสียทั้งภายในและภายนอก ตัวอย่างที่ ๒ หน่วยงานกำหนดการดำเนินงานของหน่วยงาน (จากการวิเคราะห์ผลกระทบทางธุรกิจ) สินทรัพย์และการดำเนินงานที่เป็นส่วนสำคัญต่อการบรรลุวัตถุประสงค์ของภารกิจ และมีผลกระทบของการสูญเสียทั้งหมด (หรือบางส่วน) ตัวอย่างที่ ๓ หน่วยงานจัดตั้งและสื่อสารวัตถุประสงค์ในการฟื้นตัวของการดำเนินการ เช่น ระยะเวลาสูงสุดที่จะกู้ข้อมูลได้ (RTO) เพื่อส่งมอบประสิทธิภาพและบริการที่สำคัญหลายสถานการณ์ เช่น หลังการโจมตี ระหว่างการกู้คืน และสภาวะปกติ
ผลลัพธ์ ความสามารถ และบริการหน่วยงานควรทำความเข้าใจและสื่อสาร วัตถุประสงค์ความสามารถ และบริการที่สำคัญของหน่วยงาน	ตัวอย่างที่ ๑ หน่วยงานสร้างรายการทรัพย์สินของที่เป็นทรัพยากรภายนอก (เช่น สิ่งอำนวยความสะดวก ผู้ให้บริการโฮสติ้งบนคลาวด์) และความสัมพันธ์กับสินทรัพย์ขององค์กรและฟังก์ชันทางธุรกิจ) ตัวอย่างที่ ๒ หน่วยงานระบุและจัดทำเอกสารการขึ้นต่อภายนอกซึ่งเป็นส่วนสำคัญที่จะกระทบต่อความสามารถหน่วยงาน รวมถึงการแบ่งปันข้อมูลกับหน่วยงานหรือบุคคลที่เหมาะสม

ข้อ ๕.๒ นโยบายการรักษาความมั่นคงปลอดภัยเว็บไซต์ (Website Security Policy)

ในการจัดทำนโยบายการรักษาความมั่นคงปลอดภัยเว็บไซต์ (Website Security Policy) ควรจะพิจารณาแนวทางได้จากประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕ ในภาคผนวก ค ตัวอย่างการประกาศนโยบาย ข้อ ๔ โดยครอบคลุมมาตรการและวิธีการรักษาความมั่นคงปลอดภัยเว็บไซต์ อุปกรณ์ หรือเทคโนโลยี ข้อแนะนำเกี่ยวกับการรักษาความมั่นคงปลอดภัยเบื้องต้นสำหรับผู้ใช้บริการเว็บไซต์ เป็นต้น หรืออาจจะพิจารณาจัดทำนโยบายตามตัวอย่างนโยบายการรักษาความมั่นคงปลอดภัยเว็บไซต์ (Website Security Policy) ของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) (๓๔)

หากหน่วยงานมีนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ หรือนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์อยู่แล้ว ควรจะพิจารณาถึงความครอบคลุมและสอดคล้องกับมาตรฐานฉบับนี้

ข้อ ๕.๓ กลยุทธ์การจัดการความเสี่ยง (Risk Management Strategy)

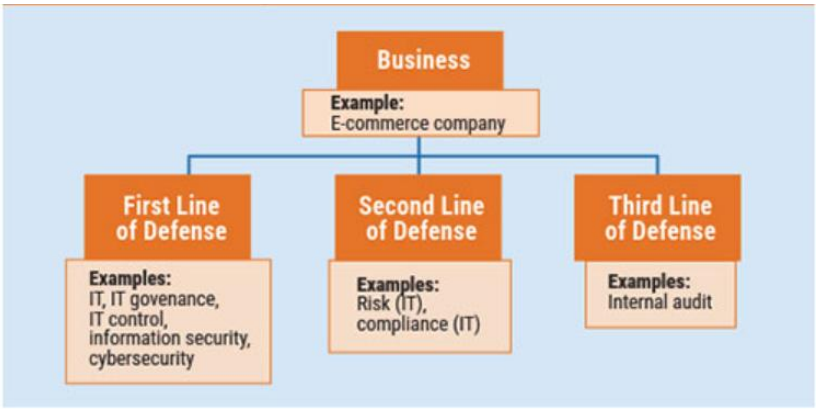
ความเสี่ยงที่ยอมรับได้ (Risk Appetite) หมายถึง ความไม่แน่นอนโดยรวมที่องค์กรยอมรับได้ โดยธุรกิจยังคงดำเนินการได้บรรลุตามเป้าหมาย ส่วนความเสี่ยงและกำกับดูแลความเสี่ยงที่ยอมรับได้กำหนดขึ้นเพื่อใช้เป็นแนวทางกำหนดกลยุทธ์ขององค์กร ทั้งนี้ ความเสี่ยงที่ยอมรับได้ควรได้รับการกำหนดโดยผู้บริหารและอนุมัติโดยคณะกรรมการ การกำหนดความเสี่ยงที่ยอมรับได้ควรพิจารณาถึงความสมดุลระหว่างการเติบโต ความเสี่ยงและผลตอบแทนของหน่วยงาน ในขณะเดียวกันองค์กรควรบริหารความเสี่ยงที่เกิดขึ้นให้อยู่ในระดับที่ยอมรับได้ (๓๕)

ระดับความเสี่ยงที่ยอมให้เบี่ยงเบนได้ (Risk Tolerance) หมายถึง ระดับความเบี่ยงเบนจากความเสี่ยงที่ยอมรับได้ การดำเนินธุรกิจภายใต้ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) ทำให้ผู้บริหารมั่นใจได้ว่า การดำเนินงานขององค์กรอยู่ภายในเกณฑ์หรือระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) ซึ่งมีผลให้คณะกรรมการ และผู้บริหารขององค์กรมีความมั่นใจมากขึ้นว่าการดำเนินการของหน่วยงานจะสามารถบรรลุวัตถุประสงค์ที่กำหนดไว้ได้ (๓๕)

ข้อ ๕.๔ บทบาทและความรับผิดชอบด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ (Information Security Roles and Responsibilities)

การถ่วงดุลตามหลักการควบคุม กำกับ และตรวจสอบ (Three Lines of Defense) เป็นแนวคิดการบริหารความเสี่ยงและตรวจสอบที่เชื่อมโยงการทำงานของหน่วยงานต่าง ๆ เข้าด้วยกันในลักษณะของ “ชั้น” โดยหน่วยงานชั้นแรก (1st Line of Defense) คือ หน่วยงานที่เจ้าของความเสี่ยง (Risk Owner) ที่เผชิญกับความเสี่ยงโดยตรง เป็นผู้กำหนดการควบคุมต่อความเสี่ยง ที่อาจทำให้องค์กรไม่บรรลุวัตถุประสงค์ของหน่วยงานชั้นที่สอง (2nd Line of Defense) ประกอบด้วย หน่วยงานบริหารความเสี่ยงและกำกับการปฏิบัติงาน ภายใต้การควบคุมและกำกับดูแลของผู้บริหารระดับสูง และหน่วยงานชั้นที่สาม (3rd Line of Defense) คือ หน่วยงานตรวจสอบภายใน ทำหน้าที่ในการประเมินความเพียงพอของมาตรการต่าง ๆ โดยอยู่ภายใต้การดูแลของผู้ตรวจสอบภายนอกและหน่วยงานทางการ (๓๖)

หน่วยงานอาจจะพิจารณาประยุกต์หลักการควบคุม กำกับ และตรวจสอบ (Three Lines of Defense) กับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับเว็บไซต์ (๓๗) แสดงได้ดังภาพที่ ก๑



ภาพที่ ก๑ ตัวอย่างการประยุกต์หลักการควบคุม กำกับ และตรวจสอบ (Three Lines of Defense)

จากภาพที่ ก๑ การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศจะต้องเป็นส่วนหนึ่งของกรอบการบริหารความเสี่ยงระดับองค์กร โดยมีโครงสร้างตามหลักการควบคุม กำกับ และตรวจสอบ (Three Lines of Defense) ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ ดังนี้ หน่วยงานชั้นแรก (1st Line of Defense) คือ หน่วยงานด้านเทคโนโลยีสารสนเทศ (IT) ที่เป็นเจ้าของความเสี่ยง (Risk Owner) เช่น IT governance, IT control, Information Security หรือ Cyber Security ที่เผชิญกับความเสี่ยงโดยตรง เป็นผู้กำหนดการควบคุมต่อความเสี่ยงที่อาจทำให้องค์กรไม่บรรลุวัตถุประสงค์ของ หน่วยงานชั้นที่สอง (2nd Line of Defense) ประกอบด้วย หน่วยงานบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Management) และหน่วยงานกำกับการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT Compliance) ภายใต้การควบคุมและกำกับดูแลของผู้บริหารระดับสูง และหน่วยงานชั้นที่สาม (3rd Line of Defense) คือ หน่วยงานตรวจสอบภายในด้านเทคโนโลยีสารสนเทศ (IT Internal Audit) ทำหน้าที่ในการประเมินความเพียงพอของมาตรการต่าง ๆ โดยอยู่ภายใต้การดูแลของผู้ตรวจสอบภายนอกและหน่วยงานทางการ (๓๗)

ข้อ ๕.๕ การวางแผนกำหนดความต้องการด้านความมั่นคงปลอดภัยของเว็บไซต์

หน่วยงานควรจะมีการวางแผนกำหนดความต้องการด้านความมั่นคงปลอดภัยของเว็บไซต์ โดยมีขั้นตอนที่เสนอแนะไว้ ดังนี้

๑. การระบุขอบเขตและช่องทางการเข้าถึงเว็บไซต์ โดยมีการพิจารณาและระบุว่าเว็บไซต์ที่จะพัฒนาเปิดให้บริการเฉพาะบางกลุ่มงานภายในหน่วยงาน ทุกกลุ่มงานภายในหน่วยงาน หน่วยงานพันธมิตร ผู้ใช้งานบางกลุ่มที่อยู่นอกหน่วยงาน หรือเปิดให้บริการสาธารณะ รวมถึงกำหนดขอบเขตและช่องทางการเข้าถึงเว็บไซต์ซึ่งเป็นปัจจัยสำคัญในการพิจารณามาตรการและระดับในการรักษาความมั่นคงปลอดภัยของเว็บไซต์

๒. การระบุข้อมูล ระดับความสำคัญ และระดับความละเอียดอ่อนของข้อมูลที่มีการจัดเก็บ ประมวลผล และแสดงบนเว็บไซต์ เว็บไซต์มีการเก็บรวบรวม ประมวลผล และแสดงข้อมูลเฉพาะข้อมูลที่เป็นข้อมูลที่เปิดเผยต่อสาธารณะได้ หรือเป็นข้อมูลที่มีความสำคัญต่อหน่วยงาน เป็นความลับสามารถใช้งานได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น หากมีการเก็บรวบรวมและประมวลผลข้อมูลส่วนบุคคลควรมีมาตรฐานในการรักษาความเป็นส่วนตัวของเจ้าของข้อมูลอย่างเหมาะสม ให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (๓๘) ตัวอย่างเช่น การเก็บรวบรวม และประมวลผลข้อมูลส่วนบุคคล มีการกำหนดให้มีกล่องข้อความยินยอมให้เก็บและประมวลผลข้อมูลส่วนบุคคล และควรระบุวัตถุประสงค์ในการจัดเก็บข้อมูลส่วนบุคคล

๓. การระบุคุณสมบัติด้านความมั่นคงปลอดภัยที่ต้องการ เช่น หากต้องการรักษาความลับของข้อมูลควรมีการพิจารณาการเข้ารหัสข้อมูล (Encryption) ที่เหมาะสม หากต้องการรักษาความครบถ้วนแท้จริงของข้อมูลควรมีการพิจารณาใช้รหัสยืนยันข้อความ (Message Authentication Code: MAC) หรือลายมือชื่อดิจิทัล (Digital Signature) หากเป็นเว็บไซต์ที่ต้องมีความพร้อมใช้งานสูง ควรมีการเฝ้าระวังความพร้อมใช้งาน (Uptime Monitoring) และการเตรียมทรัพยากรสำรอง (Redundancy หรือ High Availability)

๔. การระบุกลุ่มผู้ใช้งาน พิจารณาถึงการกำหนดสิทธิการเข้าถึง และมาตรการควบคุมการเข้าถึงที่เหมาะสม ในแต่ละกลุ่มผู้ใช้งาน รวมถึงกำหนดสิทธิ์ในการเข้าถึง การกำหนดมาตรการควบคุมการเข้าถึงข้อมูล สารสนเทศ และระบบงานอย่างมั่นคงปลอดภัย

๕. การระบุระดับการรักษาความมั่นคงปลอดภัยตามที่กฎหมายและกฎระเบียบที่เกี่ยวข้องสำหรับหน่วยงานที่มีให้การบริการบนเว็บไซต์จะมีกฎหมายหรือกฎระเบียบเฉพาะเกี่ยวกับความมั่นคงปลอดภัยและระดับการรักษาความมั่นคงปลอดภัย เช่น ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (Identity Assurance Level: IAL) และระดับความน่าเชื่อถือของการยืนยันตัวตน (Authentication Assurance Level: AAL) ของบริการสำคัญ และการจัดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการตามประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ (๓๙)

ข้อ ๕.๖ การกำหนดแนวทางด้านความมั่นคงปลอดภัยสำหรับเว็บไซต์

ข้อ ๕.๖.๑ แนวทางด้านความมั่นคงปลอดภัยในระดับพื้นฐาน

การกำหนดแนวทางด้านความมั่นคงปลอดภัยเพื่อปกป้องเว็บไซต์และข้อมูลอย่างเหมาะสมตามลำดับความสำคัญของทรัพย์สินและทรัพยากร แนวทางด้านความมั่นคงปลอดภัยที่หน่วยงานควรจะคำนึงถึงคุณลักษณะด้านความมั่นคงปลอดภัยพื้นฐาน ๓ ด้าน ได้แก่

๑. การรักษาความลับ (Confidentiality) กรณีเว็บไซต์มีการจัดเก็บหรือใช้งานข้อมูลที่มีความละเอียดอ่อน และเข้าถึงได้เฉพาะกลุ่มผู้ใช้ที่ได้รับอนุญาตเท่านั้น เช่น ข้อมูลส่วนบุคคล ข้อมูลภายในหน่วยงาน หรือข้อมูลผลิตภัณฑ์ ควรจะมีมาตรการควบคุมการรักษาความลับที่เหมาะสม เช่น การเข้ารหัสและการควบคุมการเข้าถึง ทั้งระหว่างการจัดเก็บ (Data-at-rest) การส่งต่อ (Data-in-transit) และการใช้งาน (Data-in-use) โดยหน่วยงานควรจะพิจารณาถึงมาตรฐานการเข้ารหัสของแต่ละข้อมูลจะมีการเข้ารหัสมาตรฐานไม่เหมือนกัน เช่น ใช้มาตรฐานเข้ารหัสแบบ RSA ในข้อมูลละเอียดอ่อน การกรอกบัญชีผู้ใช้และรหัสผ่านเพื่อเข้าถึงข้อมูลที่ใช้ภายในหน่วยงาน

๒. การรักษาความครบถ้วนสมบูรณ์ (Integrity) กรณีที่เว็บไซต์มีข้อมูลสำคัญที่ต้องได้รับการปกป้องเพื่อให้มีความครบถ้วนสมบูรณ์ไม่ถูกแก้ไขโดยไม่ได้รับอนุญาต และสามารถตรวจสอบได้หากข้อมูลถูกแก้ไข หน่วยงานควรจะพิจารณามาตรการการรักษาความครบถ้วนสมบูรณ์ของข้อมูล เช่น รหัสยืนยันข้อความ (Message Authentication Code: MAC) ลายมือชื่อดิจิทัล (Digital signature) หรือโพรโทคอลด้านความมั่นคงปลอดภัยอื่น ๆ นอกจากนี้ ควรจะมีมาตรการทบทวนข้อมูลให้มีความถูกต้องเป็นปัจจุบัน เพื่อปกป้องความถูกต้องของข้อมูลในระหว่างจัดเก็บ ส่งต่อ และใช้งาน

๓. การเตรียมความพร้อมใช้งาน (Availability) กรณีที่เว็บไซต์หน่วยงานไม่สามารถให้บริการกับผู้ใช้งานหรือประชาชนได้ ซึ่งมีสาเหตุมาจากหลายปัจจัย เช่น ภัยคุกคามทางไซเบอร์ ถูกโจมตีด้วยมัลแวร์เรียกค่าไถ่ อุปกรณ์เครือข่ายหรือเครื่องคอมพิวเตอร์แม่ข่ายชำรุดหรือไฟฟ้าดับ ดังนั้น หน่วยงานควรจะมีแผนการรับมือกับภัยคุกคาม หรือเหตุการณ์ไม่คาดคิดที่จะส่งผลต่อการให้บริการของเว็บไซต์ และควรจะมีมาตรการควบคุมปริมาณข้อมูลจราจรผ่านระบบเครือข่ายและมาตรการอื่นเพื่อป้องกันและลดผลกระทบจากการโจมตีแบบ Denial of Service (DoS) หรือ

Distributed Denial of Service (DDoS) รวมถึงควรจะพิจารณาสำรองข้อมูลและทดสอบการกู้คืนข้อมูลอย่างสม่ำเสมอ ซึ่งหากหน่วยงานมีทรัพยากรเพียงพออาจจะพิจารณาจัดตั้งสถานที่เก็บข้อมูลสำรองในกรณีฉุกเฉิน

ข้อ ๕.๖.๘ รายละเอียดแนวทางในการสำรองข้อมูลเพื่อลดผลกระทบ

การสำรองข้อมูล (Backup) เป็นกระบวนการที่สำคัญในการรักษาความมั่นคงปลอดภัยของข้อมูลของหน่วยงาน และลดผลกระทบที่เกิดขึ้นหากถูกโจมตีจากภัยคุกคามทางไซเบอร์ รวมถึงเกิดเหตุการณ์ที่ไม่คาดคิด หรือความเสียหายจากภัยธรรมชาติ หรือข้อผิดพลาดจากมนุษย์ โดยหน่วยงานอาจจะพิจารณาองค์ประกอบในการสำรองข้อมูลอย่างน้อย ดังนี้

๑) กำหนดข้อมูลที่ต้องการสำรอง ในการบริหารจัดการเว็บไซต์เพื่อความมั่นคงปลอดภัยของหน่วยงาน จะต้องมีการกำหนดรายการข้อมูลที่จำเป็นสำหรับการสำรองข้อมูล ที่รองรับต่อการกู้คืนระบบจากปัญหาด้านต่าง ๆ เช่น ฐานข้อมูลระบบเว็บไซต์ ไฟล์การตั้งค่าระบบเว็บไซต์ ไฟล์เนื้อหาเว็บไซต์

๒) กำหนดเทคโนโลยี วิธีการสำรองข้อมูล และไซต์สำรอง ระบุเทคโนโลยีในการสำรองข้อมูล และรูปแบบการดำเนินการจัดเก็บฐานข้อมูลที่เหมาะสม เช่น การสำรองข้อมูลแบบเต็ม (Full backup) การสำรองข้อมูลแบบเพิ่มเติม (Incremental backup) หรือการสำรองข้อมูลแบบส่วนต่าง (Differential backup) รวมถึงการจัดทำไซต์สำรองเพื่อการกู้คืนในภาวะฉุกเฉินให้เป็นไปตามแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP) ข้อ ๖.๕.๑ โดยอาจจะพิจารณารูปแบบการสำรองข้อมูลแบ่งตามประเภทของข้อมูล ตามตาราง ก๒

ตาราง ก๒ รูปแบบการสำรองข้อมูลแบ่งตามประเภทของข้อมูล

ประเภทข้อมูล	ความถี่ในการสำรองข้อมูล	ประเภทการสำรองข้อมูล	หมายเหตุ
ฐานข้อมูลที่มีการเปลี่ยนแปลงสูง	ทุก ๆ ๒๔ ชั่วโมง	Full Backup ประจำสัปดาห์ + Incremental ทุกวัน	สำรองข้อมูลที่เปลี่ยนแปลงตั้งแต่การสำรองล่าสุด
ไฟล์เอกสารสำคัญ	ทุก ๆ ๔๘ ชั่วโมง	Full Backup ประจำเดือน + Differential ทุกสัปดาห์	สำรองข้อมูลที่เปลี่ยนแปลงตั้งแต่การสำรองเต็มล่าสุด
ระบบไฟล์ทั่วไป	ทุกสัปดาห์	Full Backup	เหมาะสำหรับไฟล์ที่ไม่มีการเปลี่ยนแปลงบ่อย
ไฟล์สื่อ (วิดีโอ, ภาพ)	ทุกเดือน	Full Backup	ข้อมูลขนาดใหญ่ที่มีการเปลี่ยนแปลงน้อย
เอกสารที่ใช้งานไม่บ่อย	ทุก ๓-๖ เดือน	Full Backup	เอกสารที่ไม่จำเป็นต้องอัปเดตบ่อย

๓) กำหนดความถี่และพื้นที่ในการสำรองข้อมูล การกำหนดความถี่ในการสำรองข้อมูลควรจะพิจารณาจากความสำคัญของข้อมูล เช่น เป็นฐานข้อมูลหลักในการดำเนินการของหน่วยงาน เป็นฐานข้อมูลผู้ใช้งาน เป็นข้อมูลที่มีความสำคัญสูง จึงมีความจำเป็นต้องกำหนดให้มีการสำรองข้อมูลโดยมีความถี่ในการสำรองข้อมูลสูง พร้อมทั้งระบุตำแหน่งของการจัดเก็บข้อมูลสำรอง โดยจะต้อง

เป็นพื้นที่แยกจากพื้นที่ดำเนินการหลัก ซึ่งอาจจะใช้พื้นที่ในระบบคลาวด์ ไดรฟ์ภายนอก หรือเครื่องบริการอื่น ๆ

๔) ทดสอบแผนการสำรองข้อมูลและการกู้คืน การทดสอบแผนการสำรองข้อมูลและการสำรองข้อมูลอย่างครบถ้วนสมบูรณ์ภายในเวลาที่เหมาะสม รวมถึงทดสอบการกู้คืนและทดสอบการดำเนินการ เพื่อให้มั่นใจว่าหากเกิดเหตุการณ์ภัยคุกคามทางไซเบอร์กับเว็บไซต์แล้ว ข้อมูลที่สำรองไว้จะนำกลับมาใช้งานได้จริง

ข้อ ๕.๖.๙ การจัดการข้อมูลจราจรทางคอมพิวเตอร์ (Log Management)

การจัดการข้อมูลจราจรทางคอมพิวเตอร์ เป็นกระบวนการที่มุ่งเน้นการเก็บรวบรวมและการจัดการกับบันทึกเหตุการณ์ที่เกิดขึ้นในระบบของหน่วยงาน เช่น บันทึกการเข้าถึงระบบ บันทึกการเปลี่ยนแปลงในการตั้งค่า หรือบันทึกเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย โดยมีเป้าหมายหลักคือการเพิ่มการระบุและการตรวจสอบเหตุการณ์ที่เกิดขึ้น เพื่อช่วยให้สามารถตรวจสอบและติดตามกิจกรรมที่เกิดขึ้นได้อย่างมีประสิทธิภาพ นอกจากนี้ ยังช่วยให้สามารถทำการตรวจสอบและบันทึกข้อมูลการเปลี่ยนแปลง ทำให้สามารถติดตามและตรวจสอบผู้ใช้หรือบุคลากรที่มีความเกี่ยวข้องกับเหตุการณ์นั้นได้อย่างมีประสิทธิภาพ

ข้อ ๕.๖.๑๐ หลักปฏิบัติในการเลิกใช้งานเว็บไซต์

หน่วยงานที่ต้องการยุติการให้บริการเว็บไซต์ควรจะมีหลักปฏิบัติในการหยุดให้บริการเว็บไซต์เพื่อป้องกันภัยคุกคามที่อาจจะเกิดกับผู้ใช้บริการเว็บไซต์ ผู้ใช้งานอินเทอร์เน็ต และผู้ให้บริการเว็บไซต์ โดยหน่วยงานอาจจะพิจารณาหลักปฏิบัติในการหยุดให้บริการเว็บไซต์ ดังนี้

๑) แจ้งเตือนผู้ใช้งานถึงการหยุดให้บริการและวันที่จะหยุดให้บริการก่อนหยุดบริการจริง

๒) สำรองข้อมูลเว็บไซต์และฐานข้อมูลเพื่อป้องกันข้อผิดพลาดที่อาจจะเกิดขึ้น

๓) นำข้อมูลออกจากผู้ให้บริการเครื่องบริการเว็บ โดยอาจเหลือหน้าเว็บไซต์ที่แจ้งว่าเว็บไซต์ปิดบริการแล้วไว้ระยะเวลาหนึ่ง

๔) ยกเลิกบริการจากผู้ให้บริการเครื่องบริการเว็บ

๕) แจ้งเปลี่ยนสถานะชื่อโดเมนกับผู้ดูแล

๖) ตรวจสอบข้อมูลที่ยังหลงเหลืออยู่กับผู้ให้บริการค้นหาข้อมูล โดยอาจลองค้นหาข้อมูลเกี่ยวกับเว็บไซต์ที่เคยให้บริการ ถ้าพบว่ายังมีอยู่ให้ยื่นคำขอลบข้อมูลไปยังผู้ให้บริการค้นหาข้อมูล

๗) ถึงแม้ว่าจะมีการหยุดให้บริการเว็บไซต์แล้ว ควรพิจารณาว่ามีความจำเป็นจะต้องรักษาชื่อโดเมนให้อยู่ในการครอบครองหรือควบคุมของหน่วยงานต่อไปหรือไม่ เพื่อป้องกันไม่ให้ชื่อโดเมนที่มีความเกี่ยวข้องกับหน่วยงานแต่หมดอายุแล้ว ถูกผู้ไม่ประสงค์ดีเข้าครอบครองและนำไปแอบอ้างใช้งาน ทำให้ผู้เข้าเยี่ยมชมเว็บไซต์ของผู้ไม่ประสงค์ดีเกิดความเข้าใจผิดหรือถูกหลอกลวงได้

๘) หน่วยงานอาจจะพิจารณาแนวทางการทำลายข้อมูลของเว็บไซต์ที่เลิกใช้งานอย่างเหมาะสม ทั้งในรูปแบบเว็บไซต์ที่ใช้ระบบขององค์กร (On-Premises) และเว็บไซต์ที่ใช้ระบบคลาวด์ (Cloud Service) โดยอาจจะจัดระดับความสำคัญของข้อมูลและการทำลายข้อมูลตาม NIST Special Publication 800-88 Guidelines for Media Sanitization รวมถึงอาจจะตรวจสอบการยืนยันการทำลายข้อมูลของบริการเว็บโฮสติ้ง (Web Hosting) หรือแนวทางการทำลายข้อมูลของผู้ให้บริการหรือเจ้าของผลิตภัณฑ์

ข้อเสนอแนะของ NIST Special Publication 800-88 Guidelines for Media Sanitization

มาตรฐาน NIST SP 800-88 เป็นหนึ่งในมาตรฐานที่สำคัญสำหรับการทำลายสื่อเก็บข้อมูลชนิดต่าง ๆ อย่างเหมาะสมและถูกวิธี เป็นการกำหนดวิธีการและกระบวนการสำหรับการล้างข้อมูล (Media Sanitization) ในสื่ออิเล็กทรอนิกส์ เช่น Hard disk, RAM , ROM , Mount Storage, USB Drive , Smart Thing Storage, Mobile และข้อมูลบนระบบเครือข่ายต่าง ๆ โดยเน้นการสร้างความมั่นใจภายหลังการล้างข้อมูลว่าไม่มีข้อมูลที่จะหลงเหลืออยู่บนอุปกรณ์ก่อนนำกลับมาใช้ใหม่ ในการทำลายข้อมูลขึ้นอยู่กับปัจจัยหลายอย่าง เช่น ชนิดของอุปกรณ์ งบประมาณ ความเสี่ยงและความสำคัญของข้อมูล และผลกระทบต่อสิ่งแวดล้อม ดังนั้น เจ้าของข้อมูลทั้งตัวบุคคล บริษัท และหน่วยงานต่าง ๆ ควรประเมินปัจจัยหลาย ๆ อย่างก่อนการเปลี่ยนหรือเลิกใช้อุปกรณ์อิเล็กทรอนิกส์ โดยเพื่อเลือกวิธีการกำจัด และทำลายให้เหมาะสมกับความต้องการ และมีความมั่นคงปลอดภัย เพื่อลดความเสี่ยงของข้อมูลรั่วไหลหรือเปิดเผยของข้อมูลโดยไม่ได้รับอนุญาต โดยมีขั้นตอนหลักในการทำลายข้อมูล ๓ ขั้นตอน ดังนี้

๑. การลบข้อมูลทั้งหมดที่จัดเก็บไว้ในอุปกรณ์ (Clear) โดยใช้คำสั่งอ่านและเขียน รวมถึงการตั้งค่าเครื่องใหม่ (Reset) อุปกรณ์ให้เป็นการตั้งค่าจากโรงงานโดยเขียนใหม่ด้วยค่าใหม่ เหตุผลสำคัญของข้อมูลหน่วยงาน หรือข้อมูลบนระบบหลังจากเลิกใช้แล้ว หรือมีการลาออกของพนักงาน โดยใช้หลักการ Sanitize Data ในกรณี NIST SP 800-88 จะใช้ในรูปแบบของ Secure Erase

๒. กระบวนการการขัดขวางการกู้คืนในทุกกรณีโดยวิธีการลบล้าง (Purge) โดยใช้เทคนิคทางวิทยาศาสตร์เข้ามาเกี่ยวข้อง การทำลายข้อมูลเชิงการลบแบบ Degaussing ทำลายสนามแม่เหล็กก่อกวน รบกวนไม่ให้สามารถนำมาจัดเรียงได้ใหม่

๓. การทำลายข้อมูล (Destroy) ขั้นตอนกรณีเราไม่ใช้แล้วกับอุปกรณ์ในการเก็บข้อมูลทั้งหลาย ขั้นตอนการทำลายเป็นขั้นตอนที่ดีที่สุด ที่จะทำให้ปลอดภัยในทุกด้านทั้งทางกายภาพและเชิงการนำไปกู้ข้อมูลต่อ โดยอาจจะเป็นการหลอมละลาย ทุบทิ้งให้แหลกละเอียด หรือเผาไหม้ให้ไม่เหลือชิ้นส่วนที่สามารถนำมาใช้ได้

ภาคผนวก ข
รายละเอียดข้อเสนอแนะและคำอธิบายเพิ่มเติม
(ข้อ ๖)
(เป็นข้อมูลเพิ่มเติม)

ข้อ ๖.๑ การระบุความเสี่ยงที่จะเกิดขึ้นกับเว็บไซต์ (Website Security Identification)
การจัดการความเสี่ยง

ในบริบทของการรักษาความมั่นคงปลอดภัย ความเสี่ยง หมายถึง ระดับของผลกระทบต่อการดำเนินการของหน่วยงาน ทรัพย์สินของหน่วยงาน หรือบุคคลที่เกิดจากการใช้งานระบบสารสนเทศ โดยคำนึงถึงผลกระทบที่อาจเกิดขึ้นจากภัยคุกคามและความน่าจะเป็นที่ภัยคุกคามอาจเกิดขึ้น การจัดการความเสี่ยง หมายถึง กระบวนการในการจัดการความเสี่ยงต่อการดำเนินการของหน่วยงาน ทรัพย์สินของหน่วยงาน หรือบุคคลที่เกิดขึ้นจากการใช้งานระบบสารสนเทศ รวมถึงการประเมินความเสี่ยง การดำเนินการตามกลยุทธ์บรรเทาความเสี่ยง และการใช้เทคนิคและขั้นตอนในการเฝ้าระวังสถานะความมั่นคงปลอดภัยของระบบสารสนเทศอย่างต่อเนื่อง (๔๐)

ในทางปฏิบัติหน่วยงานไม่สามารถกำจัดความเสี่ยงทั้งหมดหรือทำให้ความเสี่ยงเป็นศูนย์ได้ แต่หน่วยงานสามารถลดความเสี่ยงให้อยู่ระดับที่หน่วยงานรับได้ เฝ้าระวังและรักษาระดับความเสี่ยงไม่ให้เกินระดับที่ตั้งไว้ได้ โดยอาจจะพิจารณาวิธีการและขั้นตอนการจัดการความเสี่ยงจากมาตรฐาน ISO/IEC 27005 ซึ่งเป็นมาตรฐานการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Risk Management) และสำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศอาจจะพิจารณาปฏิบัติตามคำแนะนำของ สกมช. เรื่อง แนวปฏิบัติในการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (๓๐) ซึ่งกระบวนการพื้นฐานสำหรับการจัดการความเสี่ยงสำหรับเว็บไซต์ แบ่งเป็น ๔ กระบวนการ ดังนี้

การจัดการทรัพย์สิน (Asset Management)

การจัดทำรายการทรัพย์สินเป็นขั้นตอนแรกของการวางแผนการดำเนินการรักษาความมั่นคงปลอดภัยเพื่อให้ทราบว่าหน่วยงานมีทรัพย์สินใดที่จะต้องปกป้อง มีความเสี่ยงใดที่จะต้องจัดการตามลำดับความสำคัญด้วยทรัพยากรที่มีจำกัด และมีทรัพย์สินใดที่มีช่องโหว่ความมั่นคงปลอดภัยที่ต้องได้รับป้องกันก่อนเกิดการโจมตีทรัพย์สินหรือข้อมูลของหน่วยงาน

การจัดทำรายการทรัพย์สินควรรวมถึงทรัพย์สินที่จับต้องได้ เช่น เครื่องบริการเว็บ และทรัพย์สินที่จับต้องไม่ได้ เช่น โปรแกรมสำหรับให้บริการเว็บ สัญญา รวมถึงทรัพย์สินทางปัญญา รวมถึงบุคลากรและเอกสารที่เกี่ยวข้อง เช่น แผนภาพระบบ (System Diagram) โดยรายการทรัพย์สินควรระบุ และบันทึกข้อมูลที่เกี่ยวข้องกับทรัพย์สินอย่างน้อย ดังแสดงในตาราง ข๑

ตาราง ข๑ รายละเอียดที่ระบุในรายการทรัพย์สิน

รายการ	รายละเอียด
รหัสประจำทรัพย์สิน	ใช้สำหรับการระบุ ติดตาม และจัดการทรัพย์สิน ซึ่งประกอบด้วย รหัสซีเรียล ป้ายกำกับทรัพย์สิน และรหัสบาร์โค้ดหรือคิวอาร์โค้ด เป็นอย่างน้อย
ชื่อเรียกทรัพย์สิน	เพื่อใช้ในการระบุทรัพย์สิน

รายการ	รายละเอียด
คำอธิบายทรัพย์สิน	เพื่อให้ข้อมูลเพิ่มเติมเกี่ยวกับทรัพย์สินและวัตถุประสงค์ของการใช้งานทรัพย์สินโดยสังเขป
ฟังก์ชันที่สำคัญของทรัพย์สิน	เพื่อใช้ในการระบุหน้าที่และความสำคัญของทรัพย์สิน สนับสนุนการตรวจประเมินและการปฏิบัติตามข้อกำหนด
การจำแนกทรัพย์สิน	เพื่อจัดกลุ่มทรัพย์สินที่มีลักษณะที่เหมือนกัน โดยอาจแบ่งจำแนกกลุ่มตามประเภท ตำแหน่งที่อยู่ หรือความเป็นเจ้าของ เป็นต้น
เจ้าของและ/หรือผู้ดำเนินการ และ/หรือผู้ดูแลทรัพย์สิน	เป็นการระบุผู้ดูแลและรับผิดชอบทรัพย์สิน ซึ่งเป็นผู้ใช้งาน หรือจัดการทรัพย์สิน โดยอาจจะระบุช่องทางติดต่อด้วย
ตำแหน่งทางกายภาพของทรัพย์สิน	ระบุว่าทรัพย์สินมีการติดตั้ง การใช้งาน และจัดเก็บอยู่ที่ใด เพื่อใช้ในการติดตามทรัพย์สิน
วันเวลาการตรวจสอบทรัพย์สิน	เพื่อให้ทราบว่าทรัพย์สินยังสามารถติดตามได้และข้อมูลเกี่ยวกับทรัพย์สินยังมีความถูกต้อง
มูลค่าของทรัพย์สิน	เป็นปัจจัยในการพิจารณาระดับความสำคัญ และมาตรการที่จะต้องรักษาความมั่นคงปลอดภัยของทรัพย์สิน
วันที่บันทึกทรัพย์สินเข้าระบบ	บันทึกวันที่จดบันทึกรายการทรัพย์สินเข้าระบบของหน่วยงาน
สถานะใช้งานทรัพย์สิน	เพื่อระบุว่าทรัพย์สินอยู่ระหว่างการใช้งาน ใช้งานได้ปกติ ชำรุด หมดอายุ หรือจำหน่ายออก เป็นต้น
อายุการใช้งานของทรัพย์สิน	เพื่อให้ทราบอายุการใช้งานของทรัพย์สิน และเป็นข้อมูลแจ้งเตือนการดำเนินการใด ๆ กับทรัพย์สินที่หมดอายุการใช้งาน เช่น การต่ออายุการใช้งาน การต่ออายุการบำรุงรักษา การตัดบัญชีสินทรัพย์ และการจำหน่ายทรัพย์สิน
ระดับความสำคัญของทรัพย์สิน	โดยพิจารณาจากมูลค่าของทรัพย์สิน ผลกระทบที่จะเกิดขึ้นเมื่อทรัพย์สินเกิดชำรุด เสียหาย หรือถูกละเมิด เป็นต้น
ผู้ที่มีสิทธิ์ในการใช้งานทรัพย์สิน	โดยระบุว่าบุคคลที่สามารถเข้าถึงทรัพย์สิน รวมถึงสิทธิ์ในการใช้งานทรัพย์สิน
การขึ้นต่อกันของทรัพย์สิน	เพื่อระบุความสัมพันธ์ที่ทรัพย์สินหนึ่งต้องพึ่งพาหรือเชื่อมโยงกับอีกทรัพย์สินหนึ่งในการทำงานหรือให้บริการ
ลักษณะอื่นๆ ของทรัพย์สิน	เป็นการระบุข้อมูลอื่น ๆ ของทรัพย์สิน เช่น เวอร์ชันของโปรแกรม การตั้งค่า ระยะเวลาการรับประกัน ประวัติการซ่อมบำรุง รูปภาพของทรัพย์สิน

การประเมินความเสี่ยง (Risk Assessment)

การประเมินความเสี่ยงเป็นหนึ่งในกระบวนการสำคัญในการบริหารจัดการความเสี่ยง เพื่อให้หน่วยงานสามารถจัดสรรทรัพยากรที่มีจำกัดเพื่อจัดการความเสี่ยงตามลำดับความสำคัญให้อยู่ในระดับที่หน่วยงานสามารถรับได้และคงระดับความเสี่ยงนั้นให้อยู่ในระดับที่กำหนด โดยหน่วยงานควรจะพิจารณาประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ

๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ และควรจะมีการปรับปรุงทะเบียนความเสี่ยงทุกครั้งหลังการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับเว็บไซต์

ในการประเมินความเสี่ยง หน่วยงานอาจจะพิจารณาประเมินความเสี่ยงได้ ๒ รูปแบบ ได้แก่ การประเมินความเสี่ยงเชิงปริมาณ ซึ่งเป็นการกำหนดค่าตัวแปรที่ใช้ในการประเมินความเสี่ยงแบบละเอียด และการประเมินความเสี่ยงเชิงคุณภาพ ซึ่งเป็นการแบ่งค่าตัวแปรเป็นกลุ่มหรือระดับ เช่น ต่ำ กลาง สูง หรือแบ่งเป็นระดับ ๑ ถึง ระดับ ๕ ถึงแม้ว่าการประเมินความเสี่ยงเชิงปริมาณจะช่วยให้สามารถเปรียบเทียบความเสี่ยงได้ชัดเจน แต่มีข้อเสียเนื่องจากใช้เวลามากและมีขั้นตอนยุ่งยาก ดังนั้น หลายสถานการณ์จึงเลือกใช้การประเมินความเสี่ยงเชิงคุณภาพ ซึ่งดำเนินการง่ายกว่าและสะท้อนความเสี่ยงได้ในภาพกว้าง ซึ่งในแต่ละหน่วยงานสามารถกำหนดระดับค่าตัวแปรให้เหมาะสมแต่ละหน่วยงาน ทั้งนี้ หน่วยงานควรใช้เกณฑ์เดียวกันเพื่อให้สามารถเปรียบเทียบระดับความเสี่ยงของแต่ละหน่วยย่อยภายในหน่วยงานได้

หน่วยงานอาจจะพิจารณาขั้นตอนหลักในการประเมินความเสี่ยง ดังนี้

๑) การระบุภัยคุกคาม เป็นขั้นตอนของการระบุภัยคุกคามที่อาจเกิดขึ้น และสร้างความเสียหายให้กับทรัพย์สิน รวมถึงภัยคุกคามที่เกิดจากบุคคล เช่น การละเมิดและโจรกรรมข้อมูล การติดมัลแวร์ และการขัดขวางการทำงานของระบบ และภัยคุกคามที่เกิดจากภัยธรรมชาติ เช่น น้ำท่วม ไฟไหม้ แผ่นดินไหว

๒) การระบุช่องโหว่ความมั่นคงปลอดภัย เป็นการระบุจุดอ่อนของระบบ ที่ผู้ไม่ประสงค์ดีสามารถใช้เพื่อเข้าถึงระบบและข้อมูลโดยไม่ได้รับอนุญาต นอกจากการระบุช่องโหว่ความมั่นคงปลอดภัยของซอฟต์แวร์แล้ว ยังต้องระบุช่องโหว่ความมั่นคงปลอดภัยของฮาร์ดแวร์ และของระบบอื่น ๆ ด้วย แหล่งข้อมูลที่สำคัญที่รวบรวมข้อมูลช่องโหว่ความมั่นคงปลอดภัย คือ โครงการ CVE Program โดย MITRE (๔๑) ซึ่งมีการรวบรวมช่องโหว่ความมั่นคงปลอดภัยที่มีการเปิดเผยสู่สาธารณะไว้

๓) การระบุความถี่ เป็นการประมาณการโอกาสเกิดภัยคุกคาม ในการประเมินความเสี่ยงเชิงปริมาณการระบุความถี่จะระบุเป็นค่าเฉลี่ยจำนวนครั้งที่ภัยคุกคามเกิดขึ้นต่อปี เช่น ๒ ครั้งต่อปี หรือ ๐.๑ ครั้งต่อปี (เกิด ๑ ครั้งทุก ๆ ๑๐ ปี) ส่วนการประเมินความเสี่ยงเชิงคุณภาพ การระบุความถี่มักจะระบุเป็นระดับ เช่น น้อย กลาง มาก หรือระดับ ๑ ถึงระดับ ๕

๔) การระบุผลกระทบ เป็นการประมาณการระดับความรุนแรงของผลกระทบที่อาจเกิดขึ้นจากภัยคุกคามต่อครั้ง ในการประเมินความเสี่ยงเชิงปริมาณ การระบุผลกระทบมักจะกำหนดเป็นมูลค่าของทรัพย์สินและค่าใช้จ่ายอื่น ๆ ที่เกี่ยวข้องหากทรัพย์สินเกิดความเสียหาย เช่น เครื่องบริการเว็บเสียหายจากไฟไหม้ มีมูลค่า ๒ แสนบาท ส่วนการประเมินความเสี่ยงเชิงคุณภาพการระบุผลกระทบมักจะระบุเป็นระดับ เช่น ต่ำ กลาง สูง หรือระดับ ๑ ถึง ระดับ ๕

๕) การวิเคราะห์ระดับความเสี่ยง เป็นการคำนวณได้จากโอกาสเกิดและผลกระทบ ในการวิเคราะห์ความเสี่ยงเชิงปริมาณ คำนวณได้จากความถี่ที่จะเกิดภัยคุกคามเฉลี่ยต่อปีคูณกับมูลค่าความเสียหายที่เกิดขึ้นต่อครั้ง เช่น โอกาสไฟไหม้เครื่องบริการเว็บเฉลี่ย ๐.๑ ครั้งต่อปี ไฟไหม้ต่อครั้ง

ทำให้เกิดความเสียหาย ๒๐๐,๐๐๐ บาท จะได้ความเสี่ยงเป็น ๒๐,๐๐๐ บาทต่อปี ส่วนการประเมินความเสี่ยงเชิงคุณภาพจะมีการทำตารางความเสี่ยงและกำหนดระดับความเสี่ยงดังแสดงในตาราง ข๒

ตาราง ข๒ ตัวอย่างตารางประเมินความเสี่ยงเชิงคุณภาพ

ระดับผลกระทบ / ระดับความถี่	๑	๒	๓
๓	กลาง	สูง	สูง
๒	ต่ำ	กลาง	สูง
๑	ต่ำ	กลาง	สูง

หลังจากการวิเคราะห์ความเสี่ยงหน่วยงานอาจจะเลือกวิธีการจัดการความเสี่ยงของแต่ละทรัพย์สินตามความเหมาะสม โดยควรจะพิจารณาตามลำดับความสำคัญ และทรัพยากรที่หน่วยงานมี โดยรายการที่มีความเสี่ยงสูงควรได้รับการจัดการและใช้มาตรการควบคุมที่เข้มงวด ในขณะที่รายการที่มีความเสี่ยงต่ำกว่า อาจจะพิจารณาปรับลดความเข้มข้นของมาตรการควบคุมได้ตามความเหมาะสม

การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing)

การประเมินความเสี่ยงจากช่องโหว่ (Vulnerability Assessment) เป็นกระบวนการที่ใช้เพื่อตรวจสอบและระบุช่องโหว่ของระบบคอมพิวเตอร์ โครงสร้างเครือข่ายสื่อสารข้อมูล เครื่องบริการเว็บ และเว็บแอปพลิเคชัน ที่อาจทำให้เกิดความเสี่ยงต่อความมั่นคงปลอดภัยของข้อมูลและระบบ เช่น ช่องโหว่ในส่วนเสริมของระบบบริหารจัดการเว็บไซต์ ที่ยังไม่ได้รับการปรับปรุง การกำหนดค่าระบบที่ไม่ปลอดภัย หรือการปรับแต่งการตั้งค่าที่ไม่ถูกต้อง เป้าหมายหลักของการประเมินความเสี่ยงจากช่องโหว่ คือ การทำให้ระบบมีความแข็งแรงและปลอดภัยจากการโจมตีของผู้ไม่ประสงค์ดี โดยมีแนวทางในการดำเนินการ ดังนี้

๑) การสแกนช่องโหว่ ผู้ดูแลระบบใช้เครื่องมือในการสแกนช่องโหว่ เพื่อค้นหาช่องโหว่ของระบบคอมพิวเตอร์ ระบบเครือข่าย หรือเว็บไซต์ ที่อาจเสี่ยงต่อการถูกโจมตี หน่วยงานควรมีการสแกนช่องโหว่เป็นประจำตามระยะเวลาที่เหมาะสม[๙] แต่ไม่ควรเกิน ๙๐ วัน

๒) การวิเคราะห์ผลการสแกน หลังจากการสแกนช่องโหว่เสร็จสิ้น ผู้ดูแลระบบจะวิเคราะห์ผลลัพธ์เพื่อระบุช่องโหว่ที่มีความเสี่ยงสูงและต้องการการแก้ไขโดยเร่งด่วน

๓) การสร้างรายงานและแนะนำ ผู้ดูแลระบบจะสร้างรายงานที่รวมข้อมูลเกี่ยวกับช่องโหว่ที่พบระดับความรุนแรง และข้อแนะนำเพื่อปรับปรุงความมั่นคงปลอดภัยของระบบ ซึ่งสามารถนำไปใช้เพื่อการปรับปรุงความมั่นคงปลอดภัยในหน่วยงานได้อย่างมีประสิทธิภาพ

---

[๙] ในการพิจารณาระยะเวลาที่เหมาะสมในการสแกนช่องโหว่ อาจจะพิจารณาอ้างอิงจากระยะเวลาของการใช้ประโยชน์จากช่องโหว่ ตัวอย่างเช่น รายงานของ Threat Research Unit, Qualys 42. Abbasi S. 2023 Threat Landscape Year in Review: If Everything Is Critical, Nothing Is 2023 [Available from: https://blog.qualys.com/vulnerabilities-threat-research/2023/12/19/2023-threat-landscape-year-in-review-part-one. ระบุว่าระยะเวลาในการใช้ประโยชน์จากช่องโหว่ของระบบในการโจมตีมีค่าเฉลี่ยอยู่ที่ 44 วัน หน่วยงานควรมีการสแกนช่องโหว่เป็นประจำทุก 30 วัน

การทดสอบการเจาะระบบ (Penetration Testing: Pentest)

การทดสอบการเจาะระบบ (Penetration Testing) เป็นกระบวนการที่ใช้เพื่อทดสอบความเข้าถึง และความแข็งแกร่งของระบบคอมพิวเตอร์ หรือโครงสร้างเครือข่าย โดยมีวัตถุประสงค์เพื่อค้นหาช่องโหว่ ที่มีโอกาสถูกโจมตีและเสี่ยงต่อความมั่นคงปลอดภัย โดยการทดสอบเจาะระบบจะดำเนินการโจมตีแบบเสมือนจริง ที่อาจมาจากผู้ไม่ประสงค์ดี เพื่อทราบถึงจุดอ่อนของระบบหรือแอปพลิเคชัน หน่วยงานอาจจะพิจารณาดำเนินการ ดังนี้

๑) การทดสอบการเจาะระบบเว็บแอปพลิเคชัน ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยจะดำเนินการการทดสอบการเจาะระบบโดยลอกเลียนแบบการโจมตีจริง ๆ กับเป้าหมาย ซึ่งเป็นเว็บแอปพลิเคชัน เช่น การโจมตีแบบ SQL Injection การโจมตีแบบ Cross-Site Scripting (XSS) หรือการเจาะระบบจากการแอบอ้างเป็นผู้ใช้ (User Impersonation)

๒) การทดสอบการเจาะระบบ โดยผู้เชี่ยวชาญจะทำการทดสอบการเจาะระบบ โดยพิจารณาจากการเข้าถึงโดยไม่ได้รับอนุญาต (Unauthorized Access Control) และการหลบเลี่ยงการตรวจจับของอุปกรณ์ด้านความมั่นคงปลอดภัย เช่น หลบเลี่ยงการป้องกันไฟร์วอลล์ (Bypass Firewall) และหลบเลี่ยงการตรวจจับการบุกรุก (Bypass IDS/IPS) เป็นสำคัญ

ปัจจัยในการดำเนินการทดสอบการเจาะระบบเว็บไซต์อาจจะดำเนินการอย่างน้อย ดังนี้

๑) ขอบเขตของการทดสอบ โดยอาจจะทดสอบทั้งระบบหรือทดสอบเฉพาะส่วน เช่น ระบบเครือข่าย และระบบเว็บแอปพลิเคชัน

๒) ผู้ทดสอบระบบ โดยอาจจะใช้ผู้ปฏิบัติงานจากภายในหรือใช้บริการทดสอบเจาะระบบจากภายนอก

๓) รูปแบบการทดสอบ สามารถแบ่งตามข้อมูลที่ใช้ในการเจาะระบบ คือ การเจาะระบบแบบไม่มีข้อมูลหรือการจำลองการเจาะระบบจากภายนอก การเจาะระบบแบบมีข้อมูลทั้งหมดหรือการจำลองการเจาะระบบจากภายใน และการเจาะระบบแบบมีข้อมูลบางส่วน

๔) ค่าใช้จ่ายที่ใช้ในการทดสอบเจาะระบบ

๕) รายงานผลการทดสอบ โดยระบุรายละเอียดที่ต้องการ และรูปแบบในการรายงานที่สามารถนำไปใช้งานได้

หน่วยงานอาจจะพิจารณาเลือกผู้ให้บริการทดสอบเจาะระบบอย่างน้อย ดังนี้

๑) รูปแบบของการให้บริการ โดยเลือกผู้ให้บริการที่ทดสอบเจาะระบบทั้งด้วยระบบอัตโนมัติและผู้เชี่ยวชาญ

๒) ความสามารถของผู้เชี่ยวชาญที่ดำเนินการทดสอบเจาะระบบ โดยสามารถพิจารณาจากใบรับรองด้านการทดสอบเจาะระบบที่ได้รับ เช่น OSCP OSWE GPEN GWAPT หรือใบรับรองอื่นที่เกี่ยวข้อง

๓) ความน่าเชื่อถือของผู้ให้บริการ โดยสามารถพิจารณาได้จากผลการปฏิบัติงานที่ผ่านมา ชื่อเสียงของบริษัท และความพึงพอใจของผู้รับบริการในอดีต

๔) ความสามารถในการรักษาความมั่นคงปลอดภัยของข้อมูล โดยสามารถพิจารณาได้จากมาตรฐานทางด้านความมั่นคงปลอดภัยในการปฏิบัติงาน การตรวจสอบประวัติพนักงานในการจ้างงาน และการรับประกันความเสียหาย

๕) ค่าใช้จ่ายที่ใช้ในการทดสอบเจาะระบบ โดยอาจจะพิจารณาขอใบเสนอราคาจากผู้บริการหลายราย

ข้อ ๖.๒ การป้องกันความเสี่ยงที่อาจจะเกิดขึ้นกับเว็บไซต์ (Website Security Protection)

ข้อ ๖.๒.๑ การพัฒนาโปรแกรมประยุกต์บนเว็บอย่างมั่นคงปลอดภัย

การพัฒนาโปรแกรมประยุกต์บนเว็บอย่างมั่นคงปลอดภัย หมายถึง การปฏิบัติและมาตรการที่ใช้ระหว่างการสร้างโปรแกรมประยุกต์บนเว็บเพื่อลดความเสี่ยง และปิดช่องโหว่ด้านความมั่นคงปลอดภัยที่เป็นไปได้ ซึ่งรวมถึงขั้นตอนต่าง ๆ ของวงจรชีวิตการพัฒนา ตั้งแต่การวางแผนและออกแบบ ไปจนถึงการนำไปใช้ และการดูแลรักษา หน่วยงานอาจจะพิจารณาสิ่งสำคัญในการรักษาความมั่นคงปลอดภัยของการพัฒนาโปรแกรมประยุกต์บนเว็บไซต์ ดังนี้

๑) การสร้างแบบจำลองภัยคุกคาม (Threat Modeling) เพื่อระบุความเสี่ยงด้านความมั่นคงปลอดภัย ช่องโหว่ และเวกเตอร์โจมตีที่อาจมีผลต่อโปรแกรมประยุกต์บนเว็บไซต์

๒) การเขียนโค้ดที่ปลอดภัย (Secure Coding Practices) หน่วยงานควรจะปฏิบัติตามข้อแนะนำและการสร้างโค้ดที่ปลอดภัย เพื่อลดความเสี่ยงที่พบบ่อย เช่น การโจมตีแบบ SQL Injection การโจมตีแบบ XSS และ การโจมตีแบบ Cross-Site Request Forgery (CSRF)

๓) การตรวจสอบและทำความสะอาดข้อมูลที่รับเข้า (Input Validation and Sanitization) เพื่อป้องกันการป้อนข้อมูลที่เจาะจงจากผู้ไม่ประสงค์ดี การรับรองตนเองและการอนุญาต การนำเอากลไกการรับรองตนเองที่แข็งแกร่งเข้าไปเพื่อยืนยันตัวตนของผู้ใช้

๔) การควบคุมการเข้าถึง เพื่อจำกัดการเข้าถึงไปยังฟังก์ชันและทรัพยากรที่มีความสำคัญตามบทบาทและสิทธิ์ของผู้ใช้ การบริหารจัดการเซสชัน การใช้เทคนิคการบริหารจัดการเซสชันที่ปลอดภัยเพื่อปกป้องรหัสเซสชัน ป้องกันการโจมตีการปิดเซสชัน และรักษาความลับและความสมบูรณ์ของข้อมูลเซสชัน

๕) การเข้ารหัสข้อมูล มีความสำคัญที่พักอยู่และต่อเนื่อง โดยใช้ขั้นตอนวิธีการเข้ารหัสและโพรโทคอลการสื่อสารที่เป็นมาตรฐาน เพื่อป้องกันการเข้าถึงข้อมูลและการละเมิดข้อมูล

๖) การกำหนด Header ที่เหมาะสมในการตอบสนอง HTTP เพื่อเพิ่มความมั่นคงปลอดภัยต่อการโจมตีที่พบบ่อยในเว็บ เช่น การโจมตีแบบ XSS การโจมตีแบบ CSRF และการโจมตีด้วยการคลิก ไลบรารีและโปรแกรมช่วย การอัปเดตและแก้ไขไลบรารี และโปรแกรมช่วยที่ใช้ในแอปพลิเคชันเพื่อลดความเสี่ยงจากช่องโหว่ด้านความมั่นคงปลอดภัยที่ทราบ

๗) การทดสอบความมั่นคงปลอดภัยอย่างเป็นระบบ รวมถึงการทดสอบซึ่งเป็นการแทรกแซงการเข้าถึงการสแกนช่องโหว่

การออกแบบเว็บไซต์ที่มีความมั่นคงปลอดภัยเป็นขั้นตอนสำคัญในการพัฒนาเว็บไซต์ เพราะเป็นการป้องกันการโจมตีและการขโมยข้อมูลที่อาจเกิดขึ้น ควรพิจารณามาตรการป้องกันการโจมตีที่เข้มงวด เพื่อป้องกันภัยคุกคามทางไซเบอร์ต่าง ๆ เช่น การโจมตีแบบ SQL Injection การโจมตีแบบ XSS และการโจมตี CSRF ซึ่งอาจทำให้ข้อมูลลูกค้าหรือข้อมูลที่สำคัญถูกขโมยหรือเปิดเผย หน่วยงานอาจจะพิจารณาแนวทางตัวอย่างในการออกแบบเว็บไซต์ที่มีความมั่นคงปลอดภัย ดังนี้

๑) การใช้ HTTPS เพื่อเข้ารหัสข้อมูลที่ถูกส่งระหว่างเครื่องบริการเว็บและผู้ใช้งาน

๒) การใช้กลไกการรับรองตัวตนสองขั้นตอน (Two-Factor Authentication) หรือการรับรองตัวตนหลายขั้นตอน (Multi-Factor Authentication) เพื่อเพิ่มความมั่นคงปลอดภัยในการเข้าถึงข้อมูล

๓) การตรวจสอบและวางแผนการป้องกันการโจมตีอย่างเป็นระบบ โดยใช้ระบบตรวจจับการบุกรุกและระบบป้องกันการบุกรุก IDS/ IPS หรือเครื่องมือตรวจสอบช่องโหว่ (Vulnerability Assessment Tool) เพื่อตรวจสอบและป้องกันการโจมตีต่าง ๆ ที่เป็นไปได้

๔) การเลือกใช้ Web Application Framework ที่มีความมั่นคงปลอดภัย

หลักการ DevSecOps

หลักการ DevSecOps เป็นแนวคิดในการผสานการพัฒนาซอฟต์แวร์ (Dev) ความมั่นคงปลอดภัย (Sec) และการดำเนินงาน (Ops) เข้าด้วยกันอย่างรวดเร็วและต่อเนื่อง โดยเน้นการสร้างซอฟต์แวร์ที่มีความมั่นคงปลอดภัยอย่างเร็วและมั่นคงตั้งแต่ขั้นตอนการพัฒนาจนถึงการใช้งานจริง หลักการนี้ทำให้ทีมพัฒนาซอฟต์แวร์มีความรับผิดชอบต่อความมั่นคงปลอดภัยเป็นส่วนหนึ่งของกระบวนการ พัฒนาและการดำเนินงานทุกขั้นตอน หน่วยงานอาจจะพิจารณาแนวทางตัวอย่างในการปรับใช้หลักการ DevSecOps ดังนี้

๑) ทีมพัฒนาซอฟต์แวร์อาจใช้เครื่องมือการทดสอบความมั่นคงปลอดภัยในขั้นตอนการพัฒนาเพื่อตรวจสอบช่องโหว่และบั๊กของโค้ดอย่างเป็นระบบ

๒) ทีมพัฒนายังสามารถนำหลักการ Infrastructure as Code (IaC) มาใช้เพื่อสร้างและบริหารจัดการสถาปัตยกรรมของระบบที่มีความมั่นคงปลอดภัยอย่างมั่นคงและเป็นระบบ

๓) การใช้หลักการ Continuous Integration (CI) และ Continuous Deployment (CD) เป็นส่วนหนึ่งของการใช้ DevSecOps ที่ช่วยให้การพัฒนาซอฟต์แวร์และปรับปรุงระบบเป็นไปอย่างรวดเร็วและมีประสิทธิภาพ

หน่วยงานอาจจะพิจารณาถึงการใช้หลักการ DevSecOps Maturity Model (DSOMM) ของมูลนิธิ OWASP (๔๓) มาใช้เพื่อวัดระดับวุฒิภาวะในการประยุกต์ใช้หลักการ DevSecOps ในการพัฒนาเว็บไซต์ให้มีความมั่นคงปลอดภัยในแต่ละมิติ ประกอบด้วย พัฒนาและการปรับใช้ (Build and Deployment) วัฒนธรรมและองค์กร (Culture and Organization) การนำไปปฏิบัติ (Implementation) การรวบรวมข้อมูล (Information Gathering) การทดสอบและการตรวจสอบ (Test and Verification)

ข้อ ๖.๒.๒ รายละเอียดปัจจัยเสี่ยงด้านความมั่นคงปลอดภัยของเว็บไซต์ที่พบได้บ่อยของ OWASP

มูลนิธิ OWASP ซึ่งเป็นมูลนิธิที่ต้องการส่งเสริมความมั่นคงปลอดภัยที่เกี่ยวข้องกับการพัฒนาและใช้งานแอปพลิเคชัน ได้มีการรวบรวมและเผยแพร่ปัจจัยเสี่ยงทางความมั่นคงปลอดภัยของเว็บแอปพลิเคชันที่พบได้บ่อย ๑๐ อันดับแรก ซึ่งหน่วยงานสามารถพิจารณานำไปใช้ประโยชน์ในการพัฒนาแอปพลิเคชันบนเว็บไซต์เพื่อให้มีความมั่นคงปลอดภัย

ข้อ ๖.๒.๓ การออกแบบสถาปัตยกรรมเว็บไซต์อย่างมั่นคงปลอดภัย

ออกแบบโครงสร้างเว็บไซต์โดยการเชื่อมต่อ Front End, Back End, Database, Reverse Proxy

การเชื่อมต่อระหว่างส่วนหน้า (Front End) ส่วนหลัง (Back End) ฐานข้อมูล (Database) และ พร็อกซีย้อนกลับ (Reverse Proxy) เป็นส่วนสำคัญในโครงสร้างของเว็บไซต์หรือแอปพลิเคชันเพื่อให้ระบบทำงานได้อย่างมีประสิทธิภาพและเป็นระบบ โดยหน่วยงานอาจจะพิจารณาออกแบบโครงสร้างเว็บไซต์ ดังนี้

๑) ส่วนหน้า (Front End) เป็นส่วนที่ผู้ใช้งานสามารถเห็นและปฏิสัมพันธ์กับเว็บไซต์ได้ ซึ่งประกอบด้วย องค์ประกอบที่แสดงผลบนหน้าจอของผู้ใช้ เช่น หน้า HTML CSS และ JavaScript

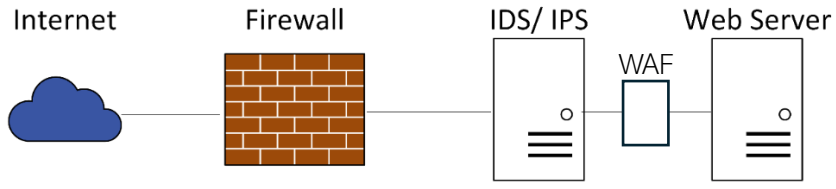
๒) ส่วนหลัง (Back End) เป็นส่วนที่ดูแลการประมวลผลและการจัดการข้อมูลของเว็บไซต์ โดยทำหน้าที่รับคำขอจากส่วนหน้า เพื่อการประมวลผล และส่งข้อมูลกลับไปยังส่วนหน้า รวมถึงการจัดการธุรกรรมกับฐานข้อมูล

๓) ฐานข้อมูล (Database) เป็นส่วนที่ใช้เก็บข้อมูลที่จำเป็นสำหรับการทำงานของเว็บไซต์หรือแอปพลิเคชัน เช่น ข้อมูลผู้ใช้ ข้อมูลสินค้า หรือข้อมูลการทำธุรกรรม

๔) พร็อกซีย้อนกลับ (Reverse Proxy) เป็นเทคโนโลยีที่ใช้เป็นตัวกลางในการจัดการและกระจายการร้องขอ (Requests) จากฝั่งผู้ใช้งาน (Client) ไปยังฝั่งเครื่องคอมพิวเตอร์แม่ข่าย (Server) (เครื่องบริการเว็บ) โดยช่วยเพิ่มประสิทธิภาพและความมั่นคงปลอดภัยในการให้บริการข้อมูลจากเว็บไซต์หรือแอปพลิเคชัน โดยสามารถใช้งานร่วมกับส่วนหลังและฐานข้อมูลได้เพื่อการจัดการและควบคุมการเข้าถึงข้อมูลอย่างมีประสิทธิภาพ

การวางเครื่องบริการเว็บ (Web Server) ร่วมกับอุปกรณ์ป้องกันความมั่นคงปลอดภัย

การวางเครื่องบริการเว็บและอุปกรณ์ป้องกันความมั่นคงปลอดภัยอื่น ๆ ในระบบเครือข่ายสื่อสารข้อมูลเป็นขั้นตอนสำคัญในการสร้างและรักษาพื้นที่ทำงานของเว็บไซต์หรือแอปพลิเคชันให้ปลอดภัย โดยการวางอุปกรณ์เหล่านี้ในตำแหน่งที่เหมาะสมภายในโครงสร้างของเครือข่ายเพื่อป้องกันการบุกรุกและความเสี่ยงต่าง ๆ ที่อาจเกิดขึ้นจากภัยคุกคามภายนอก ตัวอย่างเช่น อุปกรณ์ที่วางเข้าใช้ในการป้องกันความมั่นคงปลอดภัย เช่น ไฟร์วอลล์ (Firewall) ระบบตรวจจับการบุกรุกและระบบป้องกันการบุกรุก IDS/IPS และการให้บริการป้องกัน Web Application (WAF) สามารถจัดเป็นอุปกรณ์ที่รับผิดชอบในการรักษาความมั่นคงปลอดภัยของระบบเครือข่ายได้ โดยการตั้งค่าและวางอุปกรณ์เหล่านี้ให้เข้ากับโครงสร้างเครือข่ายอย่างเหมาะสม เพื่อให้สามารถตรวจจับและป้องกันการโจมตีได้อย่างมีประสิทธิภาพ ส่วนเครื่องบริการเว็บถือเป็นส่วนสำคัญที่รับผิดชอบในการให้บริการเนื้อหาและแอปพลิเคชันที่ถูกต้องต่อผู้ใช้งาน โดยมีความสำคัญที่จะติดตั้งและปรับแต่งเครื่องบริการเว็บเพื่อให้มีความเสถียรและปลอดภัยในการให้บริการ หน่วยงานอาจจะพิจารณาตัวอย่างการวางเครื่องบริการเว็บร่วมกับอุปกรณ์ความมั่นคงปลอดภัยเป็นอย่างน้อยดังแสดงในภาพที่ ข๑



ภาพที่ ข๑ การวางเครื่องบริการเว็บและอุปกรณ์ป้องกันความมั่นคงปลอดภัย

อุปกรณ์และบริการการรักษาความมั่งคงปลอดภัยพื้นฐาน

๑) ไฟร์วอลล์ (Firewall) เป็นเทคโนโลยีที่ใช้ในการป้องกันความมั่นคงปลอดภัยของเครือข่ายคอมพิวเตอร์ โดยการควบคุมและกรองการเข้าถึงข้อมูลที่เข้ามาหรือออกจากเครือข่าย เพื่อป้องกัน

การบุกรุกจากผู้ไม่ประสงค์ดี หรือการเข้าถึงที่ไม่ได้รับอนุญาตในเครือข่าย ไฟร์วอลล์จะทำหน้าที่เป็นกำแพงป้องกันระหว่างเครือข่ายภายในกับเครือข่ายภายนอก โดยตรวจสอบและบล็อกการเข้าถึงที่มีภาพลักษณ์ของการโจมตี หรือข้อมูลที่ไม่พึงประสงค์ โดยไฟร์วอลล์สามารถกำหนดกฎ (Rule) หรือนโยบายในการทำงานเพื่อป้องกันการบุกรุกจากภายนอก โดยตรวจจับและบล็อกการเข้าถึงที่มีความเสี่ยงได้ เช่น การโจมตีด้วยวิธีการหรือการเข้าถึงที่มิชอบด้วยการสแกนพอร์ต (Port Scanning) หรือการโจมตีด้วยการเข้าถึงที่ไม่เกี่ยวข้องด้วยการบล็อก IP ที่ไม่ได้รับอนุญาต การใช้ไฟร์วอลล์เป็นวิธีที่มีประสิทธิภาพในการป้องกันเครือข่ายจากการโจมตีต่าง ๆ และเป็นเครื่องมือสำคัญที่ช่วยให้เครือข่ายมีความมั่นคงปลอดภัยและป้องกันข้อมูลสำคัญของหน่วยงานไม่ให้ถูกเข้าถึงหรือโจมตีโดยผู้ไม่ประสงค์ดี

๒) ระบบตรวจจับการบุกรุกและระบบป้องกันการบุกรุก (Intrusion Detection Systems: IDS/Intrusion Prevention Systems: IPS) เป็นเทคโนโลยีที่ใช้ในการตรวจสอบและป้องกันความมั่นคงปลอดภัยของเครือข่ายคอมพิวเตอร์ โดยการตรวจจับและตอบสนองต่อพฤติกรรมที่เป็นอันตรายบนเครือข่าย ระบบตรวจจับการบุกรุก IDS มีหน้าที่ตรวจจับการกระทำที่มีความเสี่ยงหรือเป็นอันตรายบนเครือข่าย เช่น การสแกนพอร์ต (Port Scanning) การใช้งานช่องโหว่ (Exploits) หรือการโจมตีด้วยวิธีการอื่น ๆ โดย IDS จะทำหน้าที่แจ้งเตือนผู้ดูแลระบบเมื่อพบการกระทำที่เป็นอันตราย ส่วนระบบป้องกันการบุกรุก IPS มีหน้าที่ตรวจจับการบุกรุกและป้องกันการกระทำที่เป็นอันตรายโดยตรง ด้วยการบล็อกหรือตัดการเชื่อมต่อของผู้ไม่พึงประสงค์หรืออุปกรณ์ที่มีพฤติกรรมที่เป็นอันตราย เช่น การบล็อก IP address ที่มีลักษณะการโจมตี การบล็อกการเข้าถึงช่องโหว่ ช่วยลดความเสี่ยงในการสูญหายของข้อมูลหรือการเข้าถึงที่ไม่เหมาะสมในเครือข่าย

๓) การให้บริการป้องกัน Web Application (Web Application Firewall: WAF) เป็นเทคโนโลยีที่ใช้ในการป้องกันการโจมตีที่เป็นอันตรายต่อเว็บแอปพลิเคชัน โดยระบบนี้ทำหน้าที่ในการตรวจสอบและกรองข้อมูลที่มีการส่งผ่านมายังเว็บแอปพลิเคชัน เพื่อป้องกันการโจมตีที่อาจก่อให้เกิดความเสียหาย หรือการขโมยข้อมูล การให้บริการป้องกัน WAF จะมีความสามารถในการตรวจจับ และป้องกันการโจมตีต่าง ๆ ที่เป็นที่รู้จัก เช่น การโจมตีแบบ SQL Injection การโจมตีแบบ XSS การโจมตีแบบ CSRF และอื่น ๆ โดยการเปรียบเทียบข้อมูลที่ส่งผ่านมากับกฎหรือรูปแบบที่เป็นไปได้ของการโจมตี และบล็อกหรือจำกัดการเข้าถึงข้อมูลที่มีความเสี่ยง ดังนั้น การใช้บริการป้องกัน Web Application (WAF) เป็นส่วนสำคัญในการปกป้องเว็บแอปพลิเคชันจากการโจมตีและการหลอกลวง โดยช่วยลดความเสี่ยงในการสูญหายของข้อมูล การรั่วไหลของข้อมูล หรือการโจมตีที่เกิดขึ้นจากช่องโหว่ที่ไม่ได้รับการคาดหวัง นอกจากนี้ยังช่วยให้ผู้ดูแลระบบมีความสามารถในการตรวจจับและระบุการโจมตีอย่างรวดเร็วและมีประสิทธิภาพ

ผลิตภัณฑ์การรักษาความมั่นคงปลอดภัยที่แนะนำเพิ่มเติม

๑) ระบบการจัดการเหตุการณ์และตอบสนองด้านความมั่นคงปลอดภัย (Security Information and Event Management: SIEM) เป็นเทคโนโลยีที่ใช้ในการรวบรวม การวิเคราะห์และการรายงานเหตุการณ์ที่เกิดขึ้นกับระบบคอมพิวเตอร์และเครือข่าย เพื่อตรวจจับและตอบสนองต่อความเสี่ยงหรือการบุกรุกต่าง ๆ ที่อาจเกิดขึ้น SIEM มุ่งเน้นไปที่การรวบรวมข้อมูลจากแหล่งต่าง ๆ

เช่น เหตุการณ์จากเครื่องคอมพิวเตอร์แม่ข่าย ระบบเครือข่าย และแอปพลิเคชัน จากนั้น ระบบ SIEM จะทำการวิเคราะห์ข้อมูลเหล่านี้ เพื่อตรวจจับรูปแบบที่เป็นไปได้ของการโจมตี และให้การแจ้งเตือนแก่ผู้ดูแลระบบเมื่อพบความเสี่ยง หรือการเกิดเหตุการณ์ที่น่าสนใจ ระบบ SIEM มักมีความสามารถในการจัดการเหตุการณ์และตอบสนองต่อความเสี่ยง รวมถึงการสร้างรายงานเพื่อการวิเคราะห์และการสืบค้นข้อมูล ทำให้ผู้ดูแลระบบสามารถตอบสนองต่อเหตุการณ์ที่เกิดขึ้นได้อย่างรวดเร็วและมีประสิทธิภาพ ช่วยให้หน่วยงานมีความมั่นคงปลอดภัยและสามารถตอบสนองต่อการโจมตีได้อย่างมีประสิทธิภาพ

๒) ระบบ Extended Detection and Response หรือ XDR เป็นแนวคิดใหม่ในด้านความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศ ซึ่งเน้นการรวบรวมข้อมูลจากแหล่งต่าง ๆ เช่น เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย และอุปกรณ์ในบริษัท และนำข้อมูลเหล่านี้มาวิเคราะห์เพื่อตรวจจับและตอบสนองต่อการโจมตีที่เกิดขึ้น ระบบ XDR มุ่งเน้นไปที่การรวบรวมข้อมูลจากแหล่งต่าง ๆ เพื่อสร้างมุมมองที่ครอบคลุมและลึกซึ้งของสถานการณ์ความมั่นคงปลอดภัย ทำให้ผู้ดูแลระบบสามารถตรวจจับการโจมตีที่มีรูปแบบซับซ้อนและความหลากหลายได้อย่างมีประสิทธิภาพ การใช้ระบบ XDR จะช่วยให้หน่วยงานมีความสามารถในการตรวจจับและตอบสนองต่อการโจมตีที่เกิดขึ้นได้อย่างรวดเร็วและมีประสิทธิภาพ ทำให้หน่วยงานค้นหาและแก้ไขปัญหาความมั่นคงปลอดภัยได้อย่างมีประสิทธิภาพมากยิ่งขึ้น และช่วยลดความเสี่ยงในการเกิดความเสียหาย หรือสูญหายของข้อมูลสำคัญของหน่วยงาน

๓) Security Orchestration, Automation, and Response หรือ SOAR เป็นแนวคิดและเทคโนโลยีเพื่อการทำงานอัตโนมัติ และการรวมกลุ่มขั้นตอนการตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัย เพื่อเพิ่มประสิทธิภาพและความรวดเร็วในการจัดการกับการละเมิดความมั่นคงปลอดภัยของเครือข่ายและระบบสารสนเทศ โดย SOAR มุ่งเน้นที่การรวมกลุ่ม และการประสานงานระหว่างกระบวนการต่าง ๆ ทำให้ผู้ดูแลระบบสามารถตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยได้อย่างมีประสิทธิภาพ โดยมีความสามารถในการประมวลผลข้อมูลการรายงานเหตุแบบอัตโนมัติ ทำให้การดำเนินการที่เกี่ยวข้องกับการตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยเป็นไปอย่างมีระบบ การใช้ SOAR ทำให้หน่วยงานตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยได้อย่างมีประสิทธิภาพมากยิ่งขึ้น ลดภาระงานที่ต้องอาศัยมนุษย์ ทำให้หน่วยงานสามารถระบุ และการป้องกันการละเมิดความมั่นคงปลอดภัยของเครือข่ายและระบบสารสนเทศได้อย่างมีประสิทธิภาพ

<u>ข้อ ๖.๒.๔</u> การควบคุมการเข้าถึง (Access Control)

การกำหนดบทบาทและสิทธิ์การใช้งาน

บทบาทและสิทธิ์ในการควบคุมการเข้าถึงเป็นส่วนสำคัญในการจัดการความมั่นคงปลอดภัยของเว็บไซต์ โดยการกำหนดบทบาทและสิทธิ์ให้แก่ผู้ใช้แต่ละคนเพื่อให้ได้รับการเข้าถึงข้อมูลและทรัพยากรในระบบที่เหมาะสม เช่น เจ้าหน้าที่ด้านการเงินอาจมีสิทธิ์ในการเข้าถึงข้อมูลทางการเงิน ในขณะที่เจ้าหน้าที่ด้านการตลาดอาจมีสิทธิ์ในการเข้าถึงข้อมูลเกี่ยวกับการตลาดและ การส่งเสริมการตลาด ตัวอย่างเช่น ในระบบบริษัท XYZ มีการกำหนดบทบาทและสิทธิ์ให้แก่พนักงานแต่ละคน โดยเจ้าหน้าที่ด้านการเงินได้รับสิทธิ์การเข้าถึงและแก้ไขข้อมูลทางการเงินเท่านั้น ในขณะที่เจ้าหน้าที่

ด้านการตลาดมีสิทธิ์ในการอ่านข้อมูลเกี่ยวกับการตลาดและการส่งเสริมการตลาด แต่ไม่สามารถแก้ไขข้อมูลได้ ดังนั้นเมื่อมีการเข้าถึงระบบ ระบบจะต้องตรวจสอบบทบาทของผู้ใช้และให้สิทธิ์ที่เหมาะสมตามบทบาทที่กำหนดไว้ ทำให้มีการควบคุมการเข้าถึงข้อมูลและทรัพยากรในระบบอย่างมั่นคงและปลอดภัย

การกำหนดและรักษารหัสผ่าน

การกำหนดค่าและการรักษารหัสผ่านเป็นส่วนสำคัญในการควบคุมการเข้าถึงในระบบสารสนเทศ เนื่องจากรหัสผ่านเป็นองค์ประกอบสำคัญในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบที่เปิดใช้งาน การกำหนดค่ารหัสผ่านที่มีความมั่นคงปลอดภัยและมีการป้องกันอย่างเหมาะสม จะช่วยลดความเสี่ยงจากการโจมตีและการขโมยข้อมูล โดยหน่วยงานอาจจะพิจารณาการดำเนินการกำหนดและรักษารหัสผ่าน ดังนี้

(๑) กำหนดข้อกำหนดในการสร้างรหัสผ่าน ระบบสามารถกำหนดข้อกำหนดเกี่ยวกับความยาวของรหัสผ่าน โดยหน่วยงานอาจจะพิจารณาอ้างอิงตามเอกสาร NIST SP 800-63B (๔๔)

(๒) การใช้เทคโนโลยีการเข้ารหัส ระบบสามารถใช้เทคโนโลยีการเก็บค่า Hash ของรหัสผ่านแทนการเก็บรหัสผ่านจริงในฐานข้อมูล และใช้โพรโทคอล HTTPS เพื่อรักษาความมั่นคงปลอดภัยขณะส่งข้อมูลรหัสผ่านผ่านเครือข่าย

(๓) การตั้งค่าการรักษาความมั่นคงปลอดภัย หน่วยงานจะต้องบังคับให้เปลี่ยนรหัสผ่านหากมีหลักฐานการถูกเจาะข้อมูล หรือขโมยข้อมูล

(๔) ขั้นตอนการเปลี่ยนรหัสผ่านควรเป็นขั้นตอนที่ปลอดภัย เช่น มีการส่งอีเมลเพื่อยืนยันตัวตนไปยังผู้ใช้งาน และยอมให้เปลี่ยนรหัสผ่านก็ต่อเมื่อมีการพิสูจน์ว่าผู้ใช้งานเข้าถึงอีเมลได้จริง

(๕) การเปลี่ยนรหัสผ่านควรเพิ่มขั้นตอนการยืนยันตัวตนเพื่อระบุได้ว่าไม่ใช่การใช้โปรแกรมอัตโนมัติ เช่น การใช้ CAPTCHA กรณีที่มีการเปลี่ยนแปลงข้อมูล โดยจะมีรูปภาพให้กรอกหรือเลือกในช่องยืนยันตัวตน

(๖) ตั้งค่า Session Lock เมื่อไม่มีการใช้งานเกิน ๑๕ นาทีหรือน้อยกว่า (๔๕)

(๗) ป้องกันการโจมตีแบบ Brute Force ด้วยการตั้งค่าให้จำกัดจำนวนครั้งที่ล็อกอินผิด เช่น เมื่อล็อกอินผิดต่อเนื่องเกิน ๕ ครั้ง ให้ระงับการใช้งานบัญชีนั้นชั่วคราว (อย่างน้อย ๑๕ นาที) รวมถึงตั้งค่าให้มีการแจ้งเตือนผู้ดูแลระบบเมื่อมีการล็อกอินผิดพลาดเกินจำนวนครั้งที่กำหนด

(๘) หากบัญชีใดที่ไม่มีการล็อกอินเกิน ๔๕ วัน หรือพิจารณาตามความเหมาะสมของหน่วยงาน ควรตั้งค่าให้ระงับการใช้งานบัญชีนั้นโดยอัตโนมัติ

การตั้งค่ารหัสผ่านใหม่

การตั้งรหัสผ่านใหม่หรือการต่ออายุรหัสผ่านในการควบคุมการเข้าถึงเป็นส่วนสำคัญในการรักษาความมั่นคงปลอดภัยของระบบ โดยรหัสผ่านที่มีอายุยืนยาวอาจเสี่ยงต่อการถูกโจมตีและการเข้าถึงอย่างไม่พึงประสงค์ ดังนั้น การต่ออายุรหัสผ่านเป็นกระบวนการที่สำคัญในการบริหารจัดการรหัสผ่านอย่างปลอดภัย ตัวอย่างเช่น

(๑) การตั้งค่านโยบายรหัสผ่าน โดยกำหนดให้ระบบอนุญาตให้รหัสผ่านมีความยาวสูงสุดอย่างน้อย ๖๔ ตัวอักษร และต้องเปลี่ยนรหัสผ่านทุกครั้งที่มีหลักฐานว่ารหัสผ่านรั่วไหล (๔๔)

(๒) การตั้งค่าให้ยอมรับอักขระ ASCII [RFC20] ที่สามารถพิมพ์ได้ทุกตัวและอักขระช่องว่างในรหัสผ่าน (๔๔)

(๓) การตั้งค่าควรตรวจสอบว่ารหัสผ่านที่ผู้ใช้ตั้งนั้นไม่ตรงกับรายการรหัสผ่านที่เคยรั่วไหลมาก่อนหน้านี้ และไม่ซ้ำกับรหัสผ่าน ๕ ชุดล่าสุดที่ผู้ใช้เคยตั้งมาแล้วก่อนหน้านี้ (๔๕)

(๔) การตั้งรหัสใหม่ควรเพิ่มขั้นตอนการยืนยันตัวตนเพื่อระบุได้ว่าไม่ใช่การใช้โปรแกรมอัตโนมัติ เช่น การใช้ CAPTCHA กรณีที่มีการเปลี่ยนแปลงข้อมูล โดยจะมีรูปภาพให้กรอกหรือเลือกในช่องยืนยันตัวตน

ข้อ ๖.๒.๕ การพิสูจน์ตัวตนแบบหลายปัจจัย (Multi-Factor Authentication: MFA) หรือการพิสูจน์ตัวตนจากระบบเชื่อมโยงข้อมูลเพื่อการพิสูจน์และยืนยันตัวตนทางดิจิทัล (Digital ID)

หน่วยงานควรจะกำหนดให้ใช้การยืนยันตัวตนผ่านระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล เช่น ระบบ ThaID (ไทยดี) หรือหน่วยงานอาจจะพิจารณาใช้งาน MFA ในลักษณะอื่นในการเพิ่มความมั่นคงปลอดภัยให้กับระบบงาน ซึ่งใช้การพิสูจน์ตัวตนก่อนที่จะมีการเข้าถึงทรัพยากรและระบบที่สำคัญ เป็นการตรวจสอบตัวตนของผู้ใช้งานโดยใช้ปัจจัยที่แตกต่างกันมากกว่าหนึ่งปัจจัย ประกอบด้วย สิ่งที่ผู้ใช้รู้ (Something they know) เช่น รหัสผ่าน สิ่งที่ผู้ใช้มี (Something they have) เช่น โทเค็นการตรวจสอบ หรือสิ่งที่ผู้ใช้เป็น (Something they are) เช่น ลายนิ้วมือ ลายฝ่ามือ หรือข้อมูลชีวมิติอื่น

หน่วยงานอาจจะพิจารณาตัวอย่างการใช้งาน MFA ดังนี้

(๑) การใช้รหัสผ่านและโทเค็น ผู้ใช้จะต้องป้อนรหัสผ่านที่ถูกต้องและยังต้องใช้โทเค็นการตรวจสอบที่ส่งไปยังโทรศัพท์มือถือหรืออุปกรณ์อื่น ๆ เพื่อรับรหัสยืนยันเพิ่มเติม

(๒) การใช้รหัสผ่านและลายนิ้วมือ ผู้ใช้จะต้องป้อนรหัสผ่านและใช้สแกนลายนิ้วมือเพื่อพิสูจน์และยืนยันตัวตน

(๓) การใช้รหัสผ่านและตรวจสอบใบหน้า ผู้ใช้จะต้องป้อนรหัสผ่านและต้องให้ระบบทำการตรวจสอบใบหน้าเพื่อพิสูจน์และยืนยันตัวตน

ข้อ ๖.๒.๖ การตั้งค่าเพื่อความมั่นคงปลอดภัยพื้นฐาน

การตั้งค่าระบบปฏิบัติการ (Operating System)

หน่วยงานอาจจะพิจารณาคำแนะนำของ NIST SP 800-123 (๔๖) เพื่อการตั้งค่าความมั่นคงปลอดภัยของระบบปฏิบัติการเบื้องต้นที่สามารถนำไปประยุกต์ใช้กับระบบปฏิบัติการทุกประเภท โดยแบ่งออกเป็น ๓ ส่วน ดังนี้

๑) การถอนการติดตั้งส่วนของบริการ ซอฟต์แวร์ โพรโทคอลเครือข่าย และอื่นๆ ที่ยังไม่มีความจำเป็นต้องใช้งานออก โดยมีแนวปฏิบัติ คือ เมื่อเริ่มการติดตั้งระบบปฏิบัติการให้ติดตั้งในขั้นต่ำที่สุดให้เพียงพอต่อการตั้งค่าและปรับแต่งระบบเว็บไซต์แล้ว ค่อยติดตั้งส่วนของบริการอื่นที่ต้องการใช้งานเพิ่มเติมเท่าที่จำเป็น และหมั่นตรวจสอบและถอนการติดตั้งส่วนของบริการอื่นที่ไม่มีความจำเป็นต้องใช้งานออกหรือปิดการใช้งานหากไม่สามารถถอนการติดตั้งได้

๒) การตั้งค่าการยืนยันตัวตนของผู้ใช้งาน ดังนี้

(๑) ลบหรือปิดการใช้งานบัญชีผู้ใช้ที่มาพร้อมกับการติดตั้งในครั้งแรก

(๒) ปิดการใช้งานบัญชีผู้ใช้งานที่จำเป็นต้องมีในระบบแต่ยังไม่มีความจำเป็นต้องลงชื่อเข้าใช้งาน

(๓) สร้างกลุ่มของบัญชีผู้ใช้งานที่มีความสามารถในการเข้าถึงที่เหมาะสมและตรงกับหน้าที่ความรับผิดชอบ

(๔) สร้างบัญชีผู้ใช้งานเท่าที่จำเป็นและหลีกเลี่ยงการเปิดให้ใช้งานบัญชีผู้ใช้งานร่วมกัน

(๕) ตั้งค่าการตั้งเวลา (Time Synchronization) ให้ตรงกับ Time Server ที่เหมาะสมแบบอัตโนมัติ

(๖) ตั้งค่าข้อกำหนดของรหัสผ่านตามนโยบายการตั้งรหัสผ่านของหน่วยงาน

(๗) ตั้งค่าเพื่อป้องกันการเดารหัสผ่าน เช่น การตั้งค่าให้มีการหน่วงเวลาระหว่างการป้อนรหัสผ่านแต่ละครั้ง

(๘) ติดตั้งระบบการยืนยันตัวตนเพิ่มเติมที่จำเป็น เช่น ระบบตรวจสอบข้อมูลชีวมิติเพื่อการยืนยันตัวตน

๓) การตั้งค่าการควบคุมทรัพยากรอย่างเหมาะสม เช่น การตั้งค่าสิทธิ์ในการเข้าถึง สิทธิ์ในการเปลี่ยนแปลง และสิทธิ์ในการใช้งานทรัพยากรที่แตกต่างกันของผู้ใช้งานแต่ละประเภท และมีการสร้างสิ่งแวดล้อมเสมือน (Sandbox) สำหรับบางบริการ

หน่วยงานอาจจะพิจารณาการตั้งค่าเพื่อความมั่นคงปลอดภัยของแต่ละระบบปฏิบัติการ โดยสามารถศึกษาเพิ่มเติมได้จาก Security Technical Implementation Guides (STIGS) ของกระทรวงกลาโหมของสหรัฐอเมริกา (๔๗) และ CIS Benchmark ของบริษัท Center for Internet Security (CIS) (๔๘)

การตั้งค่าโปรแกรมสำหรับให้บริการเว็บ (Web Server Software)

การตั้งค่าโปรแกรมสำหรับให้บริการเว็บเป็นกระบวนการที่สำคัญในการเริ่มต้นใช้งานเครื่องบริการเว็บ เมื่อทำการตั้งค่าโปรแกรมสำหรับให้บริการเว็บอย่างถูกต้องและเหมาะสมกับความต้องการของเว็บไซต์ จะช่วยให้การทำงานของเว็บไซต์เป็นไปอย่างมีประสิทธิภาพและปลอดภัยมากยิ่งขึ้น ตัวอย่างเช่น กำหนดค่าต่าง ๆ เช่น การกำหนดค่าพอร์ต (Port) การกำหนดค่าโฮสต์ (Host) และการกำหนดค่าการเชื่อมต่อฐานข้อมูล รวมถึงการใช้ Official Software ให้ปฏิบัติตามคำแนะนำเฉพาะของซอฟต์แวร์นั้นๆ เพื่อให้สามารถทำงานได้อย่างมีประสิทธิภาพ

หน่วยงานอาจจะพิจารณาการตั้งค่าเพื่อความมั่นคงปลอดภัยพื้นฐานของโปรแกรมสำหรับให้บริการเว็บตาม CIS Benchmark (๔๘) ดังนี้

๑) การติดตั้งโปรแกรมสำหรับให้บริการเว็บให้ติดตั้งเวอร์ชันล่าสุด ตั้งค่าการอัปเดตให้มีการอัปเดตเป็นปัจจุบันอยู่เสมอ และเปิดการใช้งานเฉพาะโมดูลที่เกี่ยวข้องและจำเป็นกับการให้บริการเว็บไซต์เท่านั้น

๒) บัญชีการเข้าใช้งาน ควรเป็นบัญชีบริการที่ไม่สามารถถูกลงชื่อเข้าใช้โดยบุคคลอื่นได้ โดยให้มีการจำกัดสิทธิการใช้งานอยู่เฉพาะแค่โปรแกรมสำหรับให้บริการเว็บ

๓) ความเป็นเจ้าของและการอนุญาต ให้ Root หรือ Administrator เป็นเจ้าของแฟ้มและเอกสารของโปรแกรมสำหรับให้บริการเว็บ และมีการจำกัดสิทธิการเข้าถึง

๔) การตั้งค่าเครือข่าย ให้เชื่อมต่อกับพอร์ตที่จำเป็นต้องใช้งานในการให้บริการเว็บไซต์เท่านั้น และมีการตั้งค่า timeout เพื่อป้องกันการโจมตีประเภท DoS เช่น ค่าระยะเวลาการรักษาการติดต่อ (keep alive) ควรมีค่ามากกว่า ๐ และต่ำกว่า ๑๐ วินาที

๕) การปกปิดข้อมูล โดยพยายามลดการเปิดเผยข้อมูลจากการเชื่อมต่อ เช่น ข้อความแสดงโปรแกรมสำหรับให้บริการเว็บ และระบบปฏิบัติการที่ใช้งาน เช่น ปิดการแสดงค่ารายละเอียดของระบบกรณีที่มีปัญหาในการให้บริการเว็บไซต์

๖) การบันทึกการใช้งาน มีการตั้งค่าให้มีการบันทึกโดยละเอียดเกี่ยวกับการเข้าใช้งานและข้อผิดพลาดที่เกิดขึ้น

๗) การเข้ารหัสข้อมูล โดยให้มีการใช้งานโพรโทคอล HTTPS และ TLS เวอร์ชันล่าสุด โดยจะต้องมีการส่งต่อการติดต่อจากโพรโทคอล HTTP ไปยังโพรโทคอล HTTPS

๘) การกรองและจำกัดคำขอ โดยจำกัด IP ที่รับคำขอและจำกัดลักษณะของคำขอ เช่น ค่า timeout และความยาวของบัฟเฟอร์

การตั้งค่าระบบบริหารจัดการเว็บไซต์ (CMS)

การตั้งค่าระบบบริหารจัดการเว็บไซต์ (CMS) เป็นส่วนสำคัญในการดำเนินการเพื่อความมั่นคงปลอดภัย สำหรับการป้องกันการโจมตีจากภายนอกและป้องกันข้อมูลรั่วไหล หน่วยงานอาจจะพิจารณาหลักการที่สำคัญที่ต้องตั้งค่าระบบ CMS เพื่อเพิ่มความมั่นคงปลอดภัย

๑) แนวทางการใช้ส่วนเสริม (Plugin) อย่างมั่นคงปลอดภัย

การใช้ส่วนเสริมหรือปลั๊กอิน (Plugin) ใน CMS เป็นปัจจัยสำคัญที่ต้องพิจารณาอย่างรอบคอบ เพื่อป้องกันการโจมตีและไม่ให้เกิดข้อบกพร่องด้านความมั่นคงปลอดภัย ซึ่งส่วนเสริมที่มีให้บริการจำนวนมากอาจมีช่องโหว่ ภายหลังจากการสนับสนุนของผู้ให้บริการส่วนเสริมหยุดลง ดังนั้น การใช้งานส่วนเสริมหน่วยงานต้องให้ความสำคัญและมีความระมัดระวังในการใช้งาน โดยหน่วยงานอาจจะพิจารณาส่วนเสริมสำหรับความมั่นคงปลอดภัยของเว็บไซต์เป็นเครื่องมือที่ช่วยเสริมความมั่นคงปลอดภัยให้กับเว็บไซต์โดยเฉพาะ โดยการเพิ่มความสามารถพิเศษ หรือเพิ่มชั้นความมั่นคงปลอดภัยที่มีอยู่แล้วให้มีประสิทธิภาพในการตรวจสอบและป้องกันการภัยคุกคามอย่างมีประสิทธิภาพ ตัวอย่างส่วนเสริมที่น่าสนใจสำหรับความมั่นคงปลอดภัยของเว็บไซต์ ได้แก่ "Wordfence Security" สำหรับ WordPress ซึ่งมีความสามารถในการตรวจสอบและป้องกันการโจมตีต่าง ๆ ที่เป็นที่รู้จัก เช่น การโจมตีแบบ XSS การโจมตีแบบ SQL Injection และการบุกรุกแบบ brute force ร่วมกับการตรวจสอบไฟล์ที่เสี่ยงต่อภัยคุกคาม และการจัดการระดับความมั่นคงปลอดภัยของรหัสผ่านผู้ใช้งาน ทำให้ผู้ดูแลระบบสามารถป้องกัน และตรวจจับการละเมิดความมั่นคงปลอดภัยของเว็บไซต์ได้อย่างมีประสิทธิภาพ

๒) แนวทางการซ่อนหน้า Login

หน่วยงานอาจจะพิจารณาเปลี่ยนลิงก์ login ของเว็บไซต์จากค่า default เช่น aaa.go.th/wp-login.php ไปเป็นค่าอื่น เนื่องจากเป็นการป้องกันผู้ไม่หวังดีเข้ามาโจมตีหน้า Login ของเว็บไซต์ได้ โดยสามารถใช้ส่วนเสริม เช่น WPS hide login เป็นต้น

๓) การทำให้ CMS มีความแข็งแกร่ง (CMS Hardening)

การตั้งค่าความมั่นคงปลอดภัยให้กับระบบ CMS ของ Wordpress สามารถศึกษาได้จาก Developer Resource ของ Wordpress[๕] และระบบ CMS ของ Joomla สามารถศึกษาได้จากเว็บไซต์ Joomla! Documentation[๖] และระบบ CMS รายอื่น สามารถศึกษาได้จากเว็บไซต์ของระบบ CMS นั้นๆ โดยสามารถปรับให้เหมาะกับความต้องการ และสภาพแวดล้อมของแต่ละหน่วยงาน

การตั้งค่าโปรแกรมประยุกต์บนเว็บ

หน่วยงานควรจะตั้งค่าความมั่นคงปลอดภัยให้กับโปรแกรมประยุกต์บนเว็บ ตามหัวข้อที่ ๔ ของเอกสารข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ว่าด้วยมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับโปรแกรมประยุกต์บนเว็บ โดยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (๒๗) โดยหน่วยงานอาจจะพิจารณาตัวอย่างการตั้งค่า เช่น การจัดทำ Prepared Statement และ/หรือ Store Procedure เพื่อป้องกันการโจมตีประเภท SQL Injection และการทำ Output Validation ในลักษณะ Sanitization เพื่อป้องกันการโจมตีประเภท XSS

ทั้งนี้ หากหน่วยงานต้องการตรวจสอบการตั้งค่าความมั่นคงปลอดภัยของโปรแกรมประยุกต์บนเว็บ หน่วยงานอาจจะพิจารณาใช้รายการตรวจสอบโปรแกรมประยุกต์บนเว็บของโครงการ Open Web Application Security Project (OWASP) ที่จัดตั้งโดย มูลนิธิ OWASP (๔๙) เพื่อเป็นการสร้างแนวปฏิบัติและกระบวนการที่ดีในระหว่างการตรวจสอบโค้ดและขั้นตอนการออกแบบเว็บไซต์ แบบรายการการตรวจสอบโปรแกรมประยุกต์บนเว็บ มีการจัดหมวดหมู่ตามการควบคุมเชิงรุก ๑๐ อันดับแรกของ OWASP ซึ่งหน่วยงานควรปรับให้เหมาะกับความต้องการและสภาพแวดล้อมของแต่ละหน่วยงาน

การตั้งค่าฐานข้อมูล

การตั้งค่าฐานข้อมูลเป็นกระบวนการสำคัญในการเริ่มต้นใช้งานเครื่องคอมพิวเตอร์แม่ข่ายฐานข้อมูลเพื่อเก็บข้อมูลและจัดการกับข้อมูลภายในระบบ เมื่อทำการตั้งค่าเครื่องคอมพิวเตอร์แม่ข่ายฐานข้อมูลอย่างถูกต้องและเหมาะสมกับความต้องการของระบบ จะช่วยให้การทำงานกับข้อมูลเป็นไปอย่างมีประสิทธิภาพและปลอดภัยมากยิ่งขึ้น การกำหนดค่าเครื่องคอมพิวเตอร์แม่ข่ายฐานข้อมูล ประกอบด้วย การตั้งค่าที่เกี่ยวข้องกับการเชื่อมต่อฐานข้อมูล การตั้งค่าระดับความมั่นคงปลอดภัย และการตั้งค่าความเร็วในการดำเนินการของฐานข้อมูล เพื่อให้เครื่องคอมพิวเตอร์แม่ข่ายฐานข้อมูลสามารถจัดการกับข้อมูลได้อย่างมีประสิทธิภาพและปลอดภัย สำหรับตัวอย่างการกำหนดค่าเครื่องคอมพิวเตอร์แม่ข่ายฐานข้อมูล เช่น ในการกำหนดค่าการเชื่อมต่อระหว่างฐานข้อมูลและแอปพลิเคชัน การกำหนดค่าสิทธิ์และการเข้าถึงข้อมูล และการกำหนดค่าการสำรองข้อมูล เพื่อให้การจัดการกับข้อมูลในฐานข้อมูลสามารถดำเนินการได้อย่างมีประสิทธิภาพและมีความมั่นคงปลอดภัย โดยหน่วยงานอาจจะพิจารณารายละเอียดในการตั้งค่าฐานข้อมูล ดังนี้

[5] https://developer.wordpress.org/advanced-administration/security/hardening/

[6] https://docs.joomla.org/Security_Checklist/Joomla!_Setup

๑) การตั้งค่าการยืนยันตัวตน ใช้รหัสผ่านที่มีความมั่นคงปลอดภัยสูง

๒) การกำหนดสิทธิและบทบาท ใช้การจัดการการเข้าถึงตามบทบาท (Role-Based Access Control) ซึ่งจะแบ่งกลุ่มผู้ใช้งานตามบทบาทและให้สิทธิและการเข้าถึงตามบทบาท โดยจะใช้หลักการสิทธิ์ขั้นต่ำ (Least Privilege) ที่ให้สิทธิ์ที่จำเป็นในแต่ละบทบาทเพื่อเข้าใช้งานฐานข้อมูลเท่านั้น เพื่อจำกัดความเสียหายในกรณีที่ถูกโจมตี

๓) การตั้งค่าเครือข่าย เปิดรับการเข้าถึงข้อมูลจากพอร์ตที่จำเป็นและ IP ที่ได้รับอนุญาต และเปิดใช้งานการเข้ารหัส TLS ในการเชื่อมต่อฐานข้อมูล

๔) การสำรองข้อมูลและการกู้คืน ตั้งค่าให้มีการสำรองข้อมูลอย่างสม่ำเสมอและจัดเก็บในที่ที่ปลอดภัย และทดสอบการกู้คืนเป็นระยะเพื่อให้แน่ใจว่าสามารถกู้คืนข้อมูลได้เมื่อต้องการ

๕) การอัปเดต ตรวจสอบและอัปเดตซอฟต์แวร์ฐานข้อมูลให้เป็นเวอร์ชันล่าสุดอยู่เสมอ

๖) การตรวจสอบและแจ้งเตือน เก็บบันทึกการเข้าถึงฐานข้อมูล (Access Logs) และตรวจสอบอย่างสม่ำเสมอ มีการแจ้งเตือนเมื่อตรวจพบการเข้าถึงฐานข้อมูลที่ผิดปกติ

ข้อ ๖.๒.๗ แนวทางและการเลือกบริการที่เกี่ยวข้องกับเว็บไซต์

การเลือกบริการจากผู้ให้บริการภายนอก ต้องใช้ความรอบคอบและการวางแผนเป็นอย่างดี โดยต้องคำนึงถึงปัจจัยด้านต่าง ๆ เช่น ความเชี่ยวชาญและประสบการณ์ คุณภาพและมาตรฐาน การสื่อสารและการรายงาน ความยืดหยุ่นและการปรับตัว และที่สำคัญความมั่นคงปลอดภัยและการปกป้องข้อมูล เป็นต้น มาตรฐานฉบับนี้ มีข้อเสนอแนะและแนวทางในการเลือกผู้ให้บริการภายนอกแบ่งตามบริการที่อยู่ในขอบเขตของเว็บไซต์ ดังนี้

การเลือกบริการเครื่องบริการเว็บ (Web Server)

กรณีที่หน่วยงานพิจารณาว่ามีความจำเป็นที่ต้องเลือกใช้บริการเครื่องบริการเว็บจากผู้ให้บริการภายนอก เช่น การใช้บริการเครื่องบริการเว็บบนคลาวด์ หน่วยงานอาจจะพิจารณาข้อควรคำนึงในการพิจารณาเลือกบริการเครื่องบริการเว็บ ดังนี้

๑) ขอบเขตความรับผิดชอบ หน่วยงานควรพิจารณาเลือกบริการเครื่องบริการเว็บตามขอบเขตความรับผิดชอบในการดูแลความมั่นคงปลอดภัยของเครื่องบริการเว็บ ซึ่งผู้ให้บริการมีบริการเครื่องบริการเว็บหลายรูปแบบ เช่น การให้บริการเครื่องคอมพิวเตอร์แม่ข่ายเสมือน โดยผู้ใช้งานสามารถติดตั้งระบบปฏิบัติการและซอฟต์แวร์ที่เกี่ยวข้องด้วยตนเองทั้งหมด การให้บริการทรัพยากรการคำนวณและซอฟต์แวร์แพลตฟอร์มในการพัฒนาต่อยอดหรือการให้บริการเว็บแบบสำเร็จรูปโดยผู้ใช้งานสามารถตั้งค่าเครื่องบริการเว็บและติดตั้งส่วนเสริมด้วยตนเองได้ ซึ่งการให้บริการแต่ละรูปแบบจะมีการแบ่งความรับผิดชอบในการดูแลความมั่นคงปลอดภัยของเครื่องบริการเว็บที่ไม่เท่ากัน

๒) รูปแบบการจัดสรรทรัพยากร การเลือกรูปแบบการจัดสรรทรัพยากร มี ๒ รูปแบบ ประกอบด้วย แบบใช้ร่วมกัน (Shared) หรือแบบเป็นส่วนตัว (Dedicated หรือ Private) โดยการจัดสรรทรัพยากรแบบใช้ร่วมกันจะมีค่าบริการที่ต่ำกว่า แต่จะต้องใช้ทรัพยากรร่วมกันกับหน่วยงานอื่น ดังนั้น ควรมีการศึกษามาตรการในการควบคุมการเข้าถึงระบบและข้อมูลเพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาต เช่น ผู้ใช้ต่างหน่วยงานหรือบุคคลภายนอก เข้าถึงระบบและข้อมูล

ได้ การจัดสรรทรัพยากรแบบเป็นส่วนตัว ผู้ให้บริการจะแบ่งทรัพยากรและบริการให้ใช้เฉพาะผู้ใช้งานรายนั้น ๆ และส่วนใหญ่จะมีมาตรการควบคุมการเข้าถึงระบบและข้อมูลที่เข้มงวดกว่าแบบใช้ร่วมกัน

๓) การพิจารณาจากรูปแบบนโยบายการจัดการช่องโหว่ หน่วยงานอาจจะพิจารณาผู้ให้บริการที่มีนโยบายที่ชัดเจนในการค้นหาช่องโหว่ของซอฟต์แวร์ในเครื่องบริการเว็บ รวมถึงการป้องกันความเสียหายที่อาจจะเกิดจากช่องโหว่นั้น ๆ เช่น การแจ้งให้ผู้ใช้บริการทราบในทันที การ Patch หรือแก้ไขปัญหาเฉพาะหน้า (Workaround) ตามที่ผู้ผลิตซอฟต์แวร์หรือผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยที่น่าเชื่อถือแนะนำ ตลอดจนมีแผนสำรองในกรณีที่เป็นช่องโหว่ที่ไม่สามารถหาวิธีแก้ไขหรือป้องกันความเสียหายได้ในระยะเวลาอันสั้น โดยต้องพิจารณาถึงความรับผิด (Liability) ที่ผู้ให้บริการที่ต้องชดเชยในกรณีที่เกิดความเสียหาย และในกรณีที่เกิดความบกพร่องจากการจัดการกับช่องโหว่จากผลกระทบที่คาดว่าจะได้รับ และระยะเวลาที่สามารถดำเนินการหาวิธีแก้ไขหรือป้องกันความเสียหายได้จนสำเร็จ

๔) นโยบายการรักษาความเป็นส่วนตัว การศึกษานโยบายความเป็นส่วนตัว (Privacy Policy) ของผู้ให้บริการเครื่องบริการเว็บ เพื่ออธิบายเกี่ยวกับการดำเนินการกับข้อมูลของผู้ใช้งานโดยผู้ให้บริการเครื่องบริการเว็บ เพื่อให้ผู้ใช้งานได้ทราบถึงการเก็บข้อมูล การใช้งานข้อมูล การแบ่งปันข้อมูลให้กับหน่วยงานอื่น การรักษาความมั่นคงปลอดภัยของข้อมูล และการปฏิบัติตามกฎหมายเกี่ยวกับข้อมูลที่จะเกิดขึ้นกับข้อมูลของตน

๕) ความพร้อมใช้งาน (Uptime) การเลือกผู้ให้บริการเครื่องบริการเว็บที่มีความพร้อมใช้งาน (Uptime) ไม่ต่ำกว่าร้อยละ ๙๙.๙ โดยสามารถพิจารณาได้จากสถิติการให้บริการการรับรองความพร้อมใช้งานขั้นต่ำ และคำวิจารณ์ที่ผู้ให้บริการได้รับ

๖) การสำรองข้อมูลและกู้คืนข้อมูล (Backup and Restore) การเลือกผู้ให้บริการเครื่องบริการเว็บที่มีระบบสำรองข้อมูลอัตโนมัติ ตัวอย่างเช่น มีความถี่ในการสำรองข้อมูลอย่างน้อยวันละ ๑ ครั้ง และมีเครื่องมือในการสำรองข้อมูลที่อนุญาตให้ผู้ใช้งานสามารถสำรองข้อมูลด้วยตนเองตามความเหมาะสม และสอดคล้องกับความต้องการในการใช้งาน ทั้งนี้ จำเป็นต้องศึกษาวิธีการสำรองและกู้คืนข้อมูล หรือเลือกผู้ให้บริการที่มีเครื่องมือในการสำรองและกู้คืนข้อมูลที่ใช้งานได้ง่ายเพื่อตอบสนองต่อเหตุการณ์ที่เกิดได้อย่างรวดเร็ว เพื่อให้เว็บไซต์มีความพร้อมใช้งาน

๗) การได้รับการรับรองคุณภาพและมาตรฐาน ศึกษาข้อมูลเกี่ยวกับการได้รับการรับรองคุณภาพและมาตรฐานของผู้ให้บริการเครื่องบริการเว็บ เช่น การรับรองมาตรฐาน ISO/IEC 27001 หรือใบรับรองคุณภาพด้านเครือข่ายจากผู้จำหน่ายผลิตภัณฑ์ ซึ่งเป็นปัจจัยสำคัญที่บ่งบอกถึงคุณภาพการให้บริการ

๘) การให้บริการรักษาความมั่นคงปลอดภัย การเลือกผู้ให้บริการเครื่องบริการเว็บที่มีบริการเครื่องมือในการรักษาความมั่นคงปลอดภัย เช่น ไฟร์วอลล์ การให้บริการป้องกัน Web Application (WAF) เครื่องมือป้องกันการโจมตี DDoS ระบบตรวจจับการบุกรุกและระบบป้องกันการบุกรุก IDS/IPS และเครื่องมือป้องกันมัลแวร์ (Malware Protection)

๙) รูปแบบการให้บริการโอนย้ายไฟล์ข้อมูล (Remote File Transfer) การโอนย้ายไฟล์ข้อมูลระหว่างเครื่องของผู้ใช้บริการและเครื่องบริการเว็บ ควรต้องพิจารณาผู้ให้บริการ

เครื่องบริการเว็บที่มีช่องทางการโอนย้ายไฟล์ที่มั่นคงปลอดภัย รวมถึงมีการเข้ารหัสเพื่อรักษาความลับของข้อมูลระหว่างที่มีการโอนย้าย เช่น มีบริการ Secure File Transfer Protocol (SFTP) สำหรับกระบวนการโอนย้ายไฟล์

๑๐) การให้บริการสนับสนุน การเลือกผู้ให้บริการที่มีช่องทางการติดต่อฉุกเฉิน ในกรณีที่เกิดเหตุการณ์ด้านความมั่นคงปลอดภัย เพื่อใช้ในการประสานงานทั้งจากผู้ใช้บริการและหน่วยงานอื่นในการรับมือต่อเหตุการณ์ภัยคุกคามอย่างทันท่วงที นอกจากนี้ การมีช่องทางการติดต่อฉุกเฉินโดยเฉพาะแสดงให้เห็นถึงการให้ความสำคัญกับความมั่นคงปลอดภัยของผู้ให้บริการ

๑๑) การรับรองอิเล็กทรอนิกส์ การเลือกผู้ให้บริการเครื่องบริการที่มีการขอใบรับรองอิเล็กทรอนิกส์ที่น่าเชื่อถือ TLS Certificate ซึ่งเป็นเครื่องมือที่สำคัญในการรักษาความมั่นคงปลอดภัยของข้อมูลสำคัญ เช่น ข้อมูลลูกค้า ข้อมูลบัตรเครดิต ที่มีการรับส่งกันระหว่างเครื่องของผู้ใช้บริการและเครื่องบริการเว็บ ซึ่งเป็นบริการที่จำเป็นสำหรับเว็บไซต์ด้านพาณิชย์อิเล็กทรอนิกส์ (e-Commerce Website) หรือหน่วยงานภาครัฐที่มีการทำธุรกรรมทางอิเล็กทรอนิกส์ โดยหน่วยงานอาจจะพิจารณาจากหัวข้อการเลือกประเภท TLS Certificate

การเลือกระบบบริหารจัดการเว็บไซต์ (Content Management System: CMS)

หน่วยงานที่ใช้เว็บไซต์เป็นช่องทางในการเผยแพร่ข้อมูลของหน่วยงานที่มีการเปลี่ยนแปลงเนื้อหาน้อย เช่น ประวัติความเป็นมา และโครงสร้างองค์กร หรือการเปลี่ยนแปลงเป็นประจำ เช่น ข้อมูลข่าวสาร หลายหน่วยงานจึงพัฒนา และจัดทำเว็บไซต์ โดยระบบบริหารจัดการเว็บไซต์ CMS เพื่อความสะดวกในการบริหารจัดการ ซึ่งมีทั้งที่พัฒนาจากต่างประเทศ สามารถนำไปใช้งานต่อได้ฟรี และที่พัฒนาโดยบริษัทในประเทศไทย ซึ่งอาจมีการคิดค่าบริการหรือลิขสิทธิ์ในการใช้งาน ตัวอย่าง ระบบบริหารจัดการเว็บไซต์ CMS ที่นิยม เช่น WordPress, Joomla และ Drupal ถึงแม้ว่าการนำระบบบริหารจัดการเว็บไซต์ CMS มาใช้ในหน่วยงานจะมีประโยชน์ แต่ก็อาจมีช่องโหว่ด้านความมั่นคงปลอดภัยก่อให้เกิดความเสี่ยงได้ หน่วยงานจำเป็นต้องคำนึงถึงและมีมาตรการในการจัดการช่องโหว่ด้านความมั่นคงปลอดภัยอย่างเหมาะสม โดยหน่วยงานอาจจะพิจารณาแนวทางในการเลือกระบบบริหารจัดการเว็บไซต์ CMS ที่มีความมั่นคงปลอดภัย ดังนี้

๑) พิจารณาจากระบบบริหารจัดการเว็บไซต์ CMS มีการบริหารจัดการด้านการรักษาความมั่นคงปลอดภัย รวมถึงควรมีเอกสารแนะนำแนวทางการติดตั้งและการตั้งค่าอย่างมั่นคงปลอดภัย (Security Best Practice) และ มีส่วนเสริม (Plugin) ที่ติดตั้งเพื่อรักษาความมั่นคงปลอดภัยที่ตรงตามความต้องการของหน่วยงาน

๒) พิจารณาจากคุณภาพของประชาคมนักพัฒนาระบบบริหารจัดการเว็บไซต์ CMS ในกรณีที่เป็น Open Source ซึ่งต้องอาศัยประชาคมของนักพัฒนาในการปรับปรุงระบบบริหารจัดการเว็บไซต์ CMS ให้ดีขึ้น ซึ่งการมีประชาคมนักพัฒนาที่มีขนาดใหญ่จะมีการสื่อสารภายใน และพัฒนาอย่างต่อเนื่อง (Active Developer Community) จะเป็นระบบบริหารจัดการเว็บไซต์ CMS ที่มีฟังก์ชันการทำงานตอบสนองต่อความต้องการของผู้ใช้งานได้มากกว่า รวมถึงมีการปรับเวอร์ชันหรือปรับปรุงระบบ เพื่อแก้ไขข้อบกพร่องและช่องโหว่ของระบบบริหารจัดการเว็บไซต์ CMS ซึ่งสังเกต

ได้จากความถี่ของการปรับเวอร์ชันหรือปรับปรุงระบบบริหารจัดการเว็บไซต์ CMS เพื่อแก้ไขช่องโหว่ หรือระยะเวลาใช้ในการพัฒนาตัวปรับรุ่น (Patch)

๓) พิจารณาจากแหล่งข้อมูลที่เกี่ยวกับการติดตั้ง การตั้งค่า และแนวทางการรักษาความมั่นคงปลอดภัยของระบบบริหารจัดการเว็บไซต์ CMS ที่ดี จะมีแหล่งข้อมูลและเอกสารสนับสนุนที่เกี่ยวข้องกับการติดตั้ง การตั้งค่า การปรับแต่งและแนวทางการรักษาความมั่นคงปลอดภัยให้กับระบบบริหารจัดการเว็บไซต์ CMS

การเลือกบริการโดเมนและชื่อโดเมน

การระบุเครื่องบริการเว็บที่เชื่อมต่อกับระบบเครือข่าย สามารถใช้ URL เพื่ออำนวยความสะดวกในการอ้างถึงเครื่องบริการเว็บบนเครือข่ายอินเทอร์เน็ต ซึ่ง URL จะมีความสัมพันธ์กับชื่อโดเมน ตัวอย่าง เช่น https://www.ncsa.or.th จะมีชื่อโดเมนที่มีการใช้เป็น ncsa.or.th ดังนั้น หน่วยงานต้องจดทะเบียนชื่อโดเมนของเว็บไซต์ก่อนการพัฒนาเว็บไซต์ ทำให้ชื่อโดเมนมีความสำคัญเป็นอันดับแรกในการจัดทำเว็บไซต์และการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ หลายครั้งเกิดเหตุการณ์ที่ชื่อโดเมนถูกแก้ไขและเปลี่ยนให้ชี้ไปยังเว็บไซต์หลอกลวง และเป็นช่องทางในการเข้าถึงบัญชีที่ใช้จดทะเบียนชื่อโดเมนโดยไม่ได้รับอนุญาต ทำให้ผู้ไม่หวังดีสามารถเข้าไปเปลี่ยนแปลงการตั้งค่าของชื่อโดเมนเพื่อนำไปใช้ในทางที่ผิด การเลือกผู้รับจดทะเบียนโดเมนจึงมีความสำคัญเป็นอย่างมาก หน่วยงานอาจจะพิจารณาแนวทางในการเลือกผู้รับจดทะเบียนชื่อโดเมน ดังนี้

๑) มีการยืนยันการลงทะเบียน โดยให้ผู้ขอจดทะเบียนยืนยันอีเมลของตนโดยการเข้าไปยังลิงก์บนเว็บเพจ ซึ่งระบุไว้ในอีเมลเปิดการใช้งาน (Activation Email) ที่ผู้รับจดทะเบียนส่งมา การบริการจดทะเบียนยังสามารถเพิ่มมาตรการความมั่นคงปลอดภัยโดยใช้การติดต่อไปยังหมายเลขโทรศัพท์ของผู้ขอจดทะเบียน เพื่อแจ้งหมายเลขสำหรับยืนยันการลงทะเบียน (Confirmation Number) ให้ผู้ขอจดทะเบียนนำหมายเลขมากรอกในแบบฟอร์มบนเว็บเพจเพื่อเปิดการใช้งานบัญชีหรืออนุญาตให้ทำธุรกรรมได้

๒) มีมาตรการในการเพิ่มความมั่นคงปลอดภัยให้กับรหัสผ่าน ให้เป็นไปตามแนวทางของ NIST SP 800-63B (๔๔)

๓) มีการแจ้งเตือนและการยืนยันการเปลี่ยนแปลงข้อมูลการลงทะเบียน ทั้งนี้ การเปลี่ยนแปลงข้อมูลต่าง ๆ ต้องมีการกำหนดขั้นตอนสำหรับการเปลี่ยนแปลงข้อมูลซึ่งต้องอาศัยการยืนยันจากหลายบุคคลที่เกี่ยวข้อง ซึ่งการยืนยันการเปลี่ยนแปลงลักษณะนี้จะช่วยป้องกันการเปลี่ยนแปลงจากผู้ประสงค์ร้ายที่อาจจะปลอมตัวเพื่อเข้ามาเอาข้อมูลจากบุคคลใดบุคคลหนึ่งได้

๔) มีรูปแบบการเลือกโดเมนระดับบนสุด (Top-Level Domain) และโดเมนระดับรอง (Second-Level Domain) เพื่อเพิ่มความน่าเชื่อถือของเว็บไซต์ จดจำได้ง่าย และช่วยในการกำหนดภาพลักษณ์ของเว็บไซต์ หน่วยงานอาจจะเลือกโดเมนระดับบนสุดให้เหมาะสมและสอดคล้องกับธุรกิจและเนื้อหาของเว็บไซต์ โดยหน่วยงานที่เป็นหน่วยงานในระดับสากลควรเลือกใช้โดเมนระดับสูงสุดหมวดทั่วไป .com .co หรือ .org ซึ่งเป็นโดเมนที่สามารถจดจำได้ง่ายและมีความน่าเชื่อถือ (๕๐) สำหรับเว็บไซต์ที่มีการเข้าถึงส่วนใหญ่จากประเทศไทยควรใช้โดเมนระดับบนสุดหมวดรหัสประเทศของไทย .th และใช้โดเมนระดับรองตามประเภทของหน่วยงานตามที่แสดงในตาราง ข๓

ในการขอใช้งาน .th ผู้ให้บริการจะดำเนินการตรวจสอบสิทธิ์การเป็นผู้ถือครอง ทำให้ชื่อโดเมนมีความน่าเชื่อถือมากยิ่งขึ้น

ตาราง ข๓ โดเมนระดับรองตามประเภทของหน่วยงาน

โดเมนระดับรอง	ประเภทของหน่วยงาน
.in	บุคคลทั่วไป
.ac	สถานศึกษา
.co	ธุรกิจเอกชน รัฐวิสาหกิจ และเครื่องหมายการค้า
.go	ส่วนราชการและหน่วยงานในกำกับของรัฐ
.mi	หน่วยงานทางทหาร
.or	องค์กรพัฒนาเอกชนหรือองค์กรเพื่อสังคม
.net	ผู้ได้รับอนุญาตประกอบกิจการโทรคมนาคม

๕) มีการเพิ่มความมั่นคงปลอดภัยด้วยการใช้ DNSSEC (Domain Name System Security Extensions) ซึ่งเป็นส่วนขยายการรักษาความมั่นคงปลอดภัยของระบบชื่อโดเมน ทำให้มั่นใจว่าข้อมูลที่ถูกส่งมานั้น ถูกส่งมาจากผู้ส่งที่ถูกต้องหรือเป็นเจ้าของที่แท้จริง และข้อมูลนั้นจะไม่ถูกรบกวนหรือปรับเปลี่ยนในระหว่างการจัดส่ง

การเลือกประเภท TLS Certificate

หน่วยงานอาจจะพิจารณาขั้นตอนวิธีการเข้ารหัส Cipher Suite ของ TLS Certificate ดังนี้

๑) ระดับความมั่นคงปลอดภัย (Security Level) โดยตรวจสอบให้แน่ใจว่ามีการใช้การเข้ารหัสที่มีความมั่นคงปลอดภัยสูง เช่น AES หรือ ChaCha20 มีการใช้กลไกการแลกเปลี่ยนกุญแจที่มีความมั่นคงปลอดภัยสูง และมีการใช้ฟังก์ชันแฮชที่มีความมั่นคงปลอดภัยสูง เช่น SHA-256 SHA-384

๒) ความเข้ากันได้ (Compatibility) โดยตรวจสอบความเข้ากันได้กับเว็บเบราว์เซอร์และ Client ที่เข้าถึงเว็บไซต์ โดยเว็บเบราว์เซอร์ที่ทันสมัยรองรับโพรโทคอล TLS 1.3 ดังนั้น จึงควรเลือกชุดรหัสที่เข้ากันได้กับเวอร์ชันนี้ และหลีกเลี่ยงโพรโทคอลที่เลิกใช้แล้ว (SSL 2.0, SSL 3.0) และการเข้ารหัสที่ไม่ปลอดภัย (RC4, DES)

๓) ประสิทธิภาพ (Performance) โดยพิจารณาเปรียบเทียบระหว่างระดับความมั่นคงปลอดภัยของการเข้ารหัสกับทรัพยากรที่ใช้ในการเข้ารหัส เช่น ChaCha20-Poly1305 ซึ่งเป็นการเข้ารหัสที่มีประสิทธิภาพสูงบนอุปกรณ์พกพา

๔) การรักษาความลับล่วงหน้า (Forward Secrecy) โดยเลือกใช้การเข้ารหัสที่รองรับการรักษาความลับล่วงหน้า (Forward Secrecy) เพื่อให้มีความมั่นใจว่ากุญแจที่ใช้ในการเชื่อมต่อจะไม่ถูกโจมตีแม้ว่ากุญแจส่วนตัวของเครื่องคอมพิวเตอร์แม่ข่ายจะถูกโจมตีในอนาคตก็ตาม

๕) การใช้ Cipher Suite ควรเลือกรหัสที่เป็นมาตรฐานรองรับการรักษาความลับล่วงหน้าและเข้ากันได้กับ Client เป้าหมายของผู้ให้บริการ

อีกหนึ่งปัจจัยสำคัญที่ต้องคำนึงถึงในการเลือก TLS Certificate คือ ระดับการรับรอง (Validation Level) การเลือกระดับการรับรองที่เหมาะสมจะเพิ่มความมั่นคงปลอดภัยและความน่าเชื่อถือของเว็บไซต์ ซึ่งบางหน่วยงานอาจมีกฎหมายหรือข้อบังคับในการเลือกระดับการรับรอง

ที่จะต้องปฏิบัติตาม จึงควรเลือกระดับการรับรองที่เหมาะสมกับเว็บไซต์ของหน่วยงาน โดยระดับการรับรอง แบ่งเป็น ๓ ระดับหลัก คือ Domain Validation (DV) Organization Validation (OV) และ Extended Validation (EV) หน่วยงานอาจจะพิจารณารายละเอียดในการเลือกระดับการรับรองโดยมีรายละเอียดดังแสดงในตาราง ข๔

ตาราง ข๔ แสดงรายละเอียดของระดับการรองรับของ TLS Certificate

รายการ	Domain Validation	Organization Validation	Extended Validation
การตรวจสอบ	- ความเป็นเจ้าของโดเมน	- ความเป็นเจ้าของโดเมน - การยืนยันตัวตนองค์กร	- ความเป็นเจ้าของโดเมน - การยืนยันการมีอยู่ของนิติบุคคลทางกฎหมาย ทางกายภาพ และการดำเนินงาน
ระยะเวลา	น้อย	ปานกลาง	มาก
ค่าใช้จ่าย	ต่ำ	ปานกลาง	สูง
ความน่าเชื่อถือ	ต่ำ	ปานกลาง	สูง
กรณีการใช้งาน	บล็อก เว็บไซต์ข้อมูล และเว็บไซต์ธุรกิจขนาดเล็กที่ความน่าเชื่อถือและความมั่นคงปลอดภัยมีความสำคัญแต่ไม่วิกฤติ	เว็บไซต์ธุรกิจ เว็บไซต์อีคอมเมิร์ซ และเว็บไซต์สาธารณะที่ต้องการความน่าเชื่อถือในระดับสูงขึ้น	เว็บไซต์ที่มีชื่อเสียง สถาบันการเงิน และเว็บไซต์อีคอมเมิร์ซที่ต้องการความน่าเชื่อถือในระดับสูงสุด

ข้อ ๖.๒.๘ รายละเอียดการตั้งค่าไฟร์วอลล์ขั้นต่ำ

ไฟร์วอลล์ (Firewall) เป็นเครื่องมือสำคัญในการควบคุมและป้องกันการบุกรุกต่าง ๆ ที่เกิดขึ้นกับเว็บไซต์ ซึ่งช่วยให้รักษาความมั่นคงปลอดภัยและความน่าเชื่อถือของข้อมูลในระบบเครือข่ายได้อย่างมีประสิทธิภาพ ไฟร์วอลล์ใช้ในการตรวจจับและควบคุมการเข้าถึงที่ไม่พึงประสงค์จากภายนอกเข้าสู่ระบบเครือข่าย โดยบล็อกการเข้าถึงที่มีความเสี่ยงและอนุญาตเฉพาะการเข้าถึงที่ถูกต้องตามกฎระเบียบที่กำหนดไว้ เช่น การบล็อก IP ที่มีความเสี่ยง การบล็อกการเข้าถึงตามพอร์ตที่ไม่ปลอดภัย หน่วยงานอาจจะพิจารณาหลักการตั้งค่าไฟร์วอลล์ ดังนี้

๑) กำหนดนโยบายความมั่นคงปลอดภัย (Define Security Policies) การกำหนดนโยบายความมั่นคงปลอดภัยที่ชัดเจน เป็นขั้นตอนที่สำคัญก่อนการตั้งค่าไฟร์วอลล์ เช่น การกำหนดถึงข้อมูลหรือบริการที่ต้องการการปกป้องและระบุถึงผู้ที่สามารถเข้าถึงได้

๒) ตั้งค่ากฎการกรอง (Configure Filtering Rules) การตั้งค่ากฎ (Rule) ในไฟร์วอลล์เพื่ออนุญาตหรือปฏิเสธการเข้าถึงข้อมูลบนเว็บไซต์ตามที่หน่วยงานกำหนดให้เหมาะสมกับกลุ่มเป้าหมาย ซึ่งจะต้องกำหนดกฎสำหรับการจราจร (Traffic) ทั้งขาเข้า (Inbound Rule) และขาออก (Outbound Rule)

การตั้งค่าไฟร์วอลล์ควรใช้หลักการ "Deny by Default" ซึ่งเป็นการตั้งค่าให้ระบบปฏิเสธการเข้าถึงทั้งหมดเป็นพื้นฐาน แล้วเพิ่มการอนุญาตการเข้าถึงที่จำเป็น ในส่วนที่เกี่ยวข้องกับการเข้าถึง

เว็บไซต์เท่านั้น โดยการเปิดเฉพาะพอร์ต 443 หรือ Hypertext Transfer Protocol Secure (HTTPS) ให้ปิดการใช้งานพอร์ต 80 ส่วนพอร์ตหรือบริการอื่น ๆ หากจำเป็นต้องเปิดใช้งาน ให้เลือกเปิดใช้งานโดยให้มีการเข้ารหัส ทั้งนี้ เพื่อเพิ่มความมั่นคงปลอดภัยให้ระบบ เป็นการลดโอกาสการถูกโจมตี และการเชื่อมต่อจากภายนอกจะทำได้ผ่านช่องทางที่จำเป็นและมีการอนุญาตไว้เท่านั้น ส่วนพอร์ตอื่น ๆ ให้หน่วยงานพิจารณาเปิดเฉพาะเท่าที่จำเป็น โดยให้กำหนดเฉพาะ IP ที่ใช้งาน

๓) จำกัดการเข้าถึงโดยภูมิศาสตร์ (Geographic Restrictions) กำหนดให้ไฟร์วอลล์ทำการปฏิเสธหรือจำกัดการเข้าถึงจากบางประเทศหรือภูมิภาคที่ไม่ต้องการหรือมีความเสี่ยงสูง

๔) ป้องกันการโจมตี (Protect Against Attacks) การใช้คุณสมบัติของไฟร์วอลล์เพื่อป้องกันการโจมตีต่าง ๆ เช่น DDoS, SQL injection และ XSS ด้วยการตั้งค่าความสามารถในการป้องกันการโจมตี

๕) การตรวจสอบและบันทึก (Monitoring and Logging) การตั้งค่าไฟร์วอลล์ ให้บันทึกกิจกรรมที่เกิดขึ้น เพื่อรองรับการตรวจสอบย้อนหลังและวิเคราะห์เหตุการณ์ที่เกิดขึ้น โดยการบันทึก Log ที่ดีจะช่วยให้สามารถตรวจสอบและตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยได้อย่างรวดเร็วและมีประสิทธิภาพมากยิ่งขึ้น

๖) การปรับปรุงและอัปเดตเป็นประจำ (Regular Updates) การอัปเดตซอฟต์แวร์ไฟร์วอลล์ และกฎการกรองอย่างสม่ำเสมอ เป็นสิ่งที่สำคัญที่ต้องดำเนินการเพื่อให้มั่นใจว่าไฟร์วอลล์สามารถป้องกันภัยคุกคามจากสถานการณ์ด้านความมั่นคงปลอดภัยได้อย่างครอบคลุม

ข้อ ๖.๔ การเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์สำหรับเว็บไซต์
การรับมือเหตุการณ์ไม่คาดคิด

เหตุการณ์ไม่คาดคิดอาจเกิดได้จากหลายสาเหตุและอาจอยู่นอกเหนือการควบคุมของผู้ใช้งานและหน่วยงาน เมื่อเกิดเหตุการณ์ไม่คาดคิดแล้วอาจส่งผลกระทบกับระบบต่าง ๆ รวมถึงระบบเว็บไซต์ การเตรียมตัวรับมือกับเหตุการณ์ภัยคุกคามทางไซเบอร์จึงเป็นสิ่งที่จำเป็นในการลดความเสียหายที่จะเกิดขึ้น ทั้งทางธุรกิจและชื่อเสียงภาพลักษณ์ โดยการมีแผนรับมือจะทำให้ระบบฟื้นฟูกลับมาใช้งานได้รวดเร็วยิ่งขึ้น ช่วยเพิ่มความเชื่อมั่นของลูกค้าและผู้มีส่วนได้ส่วนเสียกับธุรกิจและบริการ หน่วยงานอาจจะพิจารณาคำแนะนำและข้อควรพิจารณาในการตอบสนองต่อเหตุการณ์สำหรับการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์ของ NIST เพื่อช่วยให้หน่วยงานต่าง ๆ มีความสามารถในการรับมือเหตุการณ์ทางไซเบอร์ ลดความสูญเสียที่เกิดขึ้นและใช้เวลาในการฟื้นฟูระบบที่สั้นลง ประกอบด้วย ๖ ส่วน (๕๑) ดังนี้

๑) การควบคุมและกำกับดูแล (Govern: GV) คือ มีการจัดทำ สื่อสาร และติดตามตรวจสอบกลยุทธ์การบริหารจัดการความเสี่ยงของหน่วยงาน ความคาดหวังของผู้มีส่วนได้ส่วนเสีย และนโยบาย

๒) การระบุความเสี่ยง (Identify: ID) คือ หน่วยงานเข้าใจถึงความเสี่ยงด้านความมั่นคงปลอดภัยของระบบสารสนเทศที่เป็นปัจจุบัน

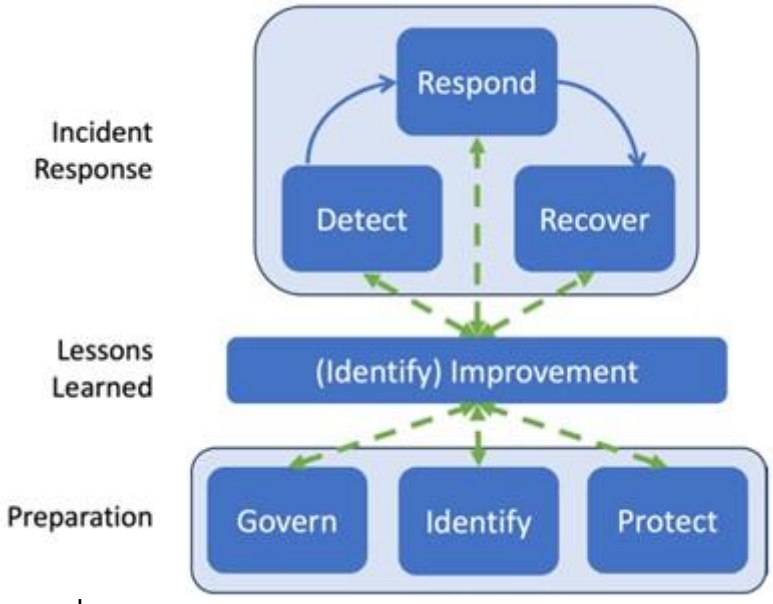
๓) การป้องกัน (Protect: PR) คือ การใช้เครื่องมือและกระบวนการต่าง ๆ ในการรับมือกับความเสี่ยงด้านความมั่นคงปลอดภัยของระบบสารสนเทศของหน่วยงาน

๔) การตรวจจับ (Detect: DT) คือ การตรวจจับและวิเคราะห์เหตุการณ์ที่มีลักษณะบ่งบอกถึงการถูกโจมตี

๕) การตอบสนอง (Respond: RS) คือ การดำเนินการเพื่อรับมือกับเหตุการณ์ทางด้านความมั่นคงปลอดภัยที่ตรวจพบ

๖) การฟื้นฟู (Recover: RC) คือ การทำให้ทรัพย์สินและกระบวนการที่ถูกโจมตีกลับมามีสภาพเดิม

โดยการทำงานทั้ง ๖ ส่วนจะมีความสัมพันธ์กันตามภาพที่ ข๒ กล่าวคือ การควบคุมและกำกับดูแล การระบุความเสี่ยง และการป้องกัน จะเป็นกิจกรรมที่สนับสนุนการรับมือเหตุการณ์ภัยคุกคามทางไซเบอร์ แต่จะไม่ได้เป็นส่วนหนึ่งของวงจรการรับมือเหตุการณ์ทางไซเบอร์โดยตรง ส่วนการตรวจจับ การตอบสนอง และการฟื้นฟูจะอยู่ในวงจรการรับมือเหตุการณ์ทางไซเบอร์ โดยมีการนำบทเรียนที่ได้จากทั้ง ๖ ส่วน มาทบทวนเพื่อพัฒนาแนวทางในการรับมือเหตุการณ์ที่ไม่คาดคิดอย่างต่อเนื่อง โดยจะมีกระบวนการวิเคราะห์ การจัดลำดับความสำคัญ และการนำผลที่ได้มาเป็นข้อมูลในการทำงานในทุกส่วน



ภาพที่ ข๒ รูปแบบวงจรการรับมือเหตุการณ์ทางไซเบอร์ตาม CSF 2.0

ภาคผนวก ค
แบบฟอร์มเพื่อใช้ในการตรวจสอบการดำเนินการให้เป็นไปตามมาตรฐานฉบับนี้

<u>โครงสร้างแบบฟอร์ม</u>

แบบฟอร์ม ค๑ แบบตรวจรายการเพื่อตรวจสอบสถานะความมั่นคงปลอดภัยสำหรับเว็บไซต์

แบบฟอร์ม ค๑ เป็นแบบตรวจรายการเพื่อการตรวจสอบสถานะความมั่นคงปลอดภัยสำหรับเว็บไซต์ เพื่อให้หน่วยงานใช้ในการประเมินตนเอง (Self-Assessment) ให้เป็นไปตามมาตรฐานฉบับนี้ ทั้งกลุ่มที่ปฏิบัติตาม หรือกลุ่มที่ส่งเสริมให้ปฏิบัติตามข้อกำหนดขั้นต่ำ

แบบฟอร์ม ค๒ แบบรายงานการแก้ไขรายการที่ยังต้องปรับปรุง

แบบฟอร์ม ค๒ เป็นแบบรายงานการแก้ไขรายการที่ยังต้องปรับปรุงในกรณีที่หน่วยงานพบรายการที่ไม่เป็นไปตามข้อกำหนด ตามแบบฟอร์ม ค๑ ให้ระบุรายการที่ต้องการปรับปรุงลงในแบบฟอร์มนี้

<u>คำแนะนำ</u>

๑. ให้หน่วยงานดำเนินการกรอกข้อมูลที่เกี่ยวกับเว็บไซต์หน่วยงานของท่านในส่วนที่ ๑ และกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้กับข้อมูลหรือสารสนเทศในส่วนที่ ๒ โดยใส่เครื่องหมาย ✔ ลงในช่องที่มีข้อมูลตรงกับหน่วยงานของท่านมากที่สุด

๒. ให้หน่วยงานดำเนินการตรวจสอบสถานะความมั่นคงปลอดภัยสำหรับเว็บไซต์ตามแบบฟอร์ม ค๑ ในส่วนที่ ๓ โดยใส่เครื่องหมาย ✔ ลงในช่อง “การประเมิน” ในส่วนของ **<u>ข้อเสนอแนะ</u>** ๓ ระดับ ดังนี้

“ดำเนินการแล้ว” กรณีที่หน่วยงานดำเนินการตามรายการในข้อเสนอแนะที่ระบุว่า “จะต้อง” และ “ควรจะ” ครบถ้วน โดยให้ใส่รายละเอียดของหลักฐานในช่อง “หลักฐาน” และแนบพร้อมแบบฟอร์มนี้

“อยู่ในระหว่างดำเนินการ” กรณีที่หน่วยงานกำลังดำเนินการตามรายการในข้อเสนอแนะที่ระบุว่า “จะต้อง” และ “ควรจะ”

“ยังไม่ได้ดำเนินการ” กรณีที่หน่วยงานยังไม่ดำเนินการตามรายการในข้อเสนอแนะที่ระบุว่า “จะต้อง” และ “ควรจะ”

๓. จากนั้นให้ตรวจสอบ**<u>ข้อเสนอแนะในแต่ละข้อกำหนด</u>** โดยให้ใส่เครื่องหมาย ✔ ลงในช่อง “การประเมิน” ในส่วนของ**<u>ข้อกำหนด</u>** ๒ ระดับ ดังนี้

“ดำเนินการแล้ว” กรณีที่หน่วยงานดำเนินการตามข้อกำหนดครบถ้วน และข้อเสนอแนะในแต่ละข้อกำหนดมีสถานะเป็น “ดำเนินการแล้ว” ครบทุกข้อ

“ยังต้องปรับปรุง” กรณีที่หน่วยงานดำเนินการตามข้อกำหนดยังไม่ครบถ้วน และข้อเสนอแนะในแต่ละข้อกำหนดมีสถานะเป็น “อยู่ในระหว่างดำเนินการ” หรือ “ยังไม่ได้ดำเนินการ”

๔. หากรายการ**<u>ข้อกำหนด</u>**มีผลการประเมินเป็น “ยังต้องปรับปรุง” ให้หน่วยงานดำเนินการกรอกรายละเอียดในแบบรายงานรายการที่ยังต้องปรับปรุง (แบบฟอร์ม ค๒) เพื่อดำเนินการปรับปรุงแก้ไขข้อกำหนดที่ยังต้องปรับปรุงแก้ไขให้เป็นไปตามมาตรฐานฉบับนี้

๕. หลังจากหน่วยงานดำเนินการกรอกแบบฟอร์ม ค๑ และแบบฟอร์ม ค๒ แล้วให้หน่วยงานดำเนินการตามแนวทางในการตรวจสอบและปฏิบัติให้เป็นไปตามมาตรฐาน ข้อที่ ๗.๒

แบบฟอร์ม ค๑

แบบตรวจรายการเพื่อการตรวจสอบสถานะความมั่นคงปลอดภัยสำหรับเว็บไซต์

สำหรับหน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
หน่วยงานของรัฐ และหน่วยงานเอกชน

<u>ส่วนที่ ๑</u> ข้อมูลเกี่ยวกับเว็บไซต์

ชื่อหน่วยงาน.....

ชื่อหน่วยงานควบคุมหรือกำกับดูแล ของท่าน.....

ประเภทหน่วยงาน ☐ หน่วยงานของรัฐ
☐ หน่วยงานควบคุมหรือกำกับดูแล (Regulator)
☐ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII)
☐ หน่วยงานเอกชน

เว็บไซต์ให้บริการด้าน.....

หน่วยงานภายในที่รับผิดชอบ (ระบุให้เป็นไปตามข้อ ๕.๔.๒).....

การเข้าถึงเว็บไซต์ หรือ URL.....

ประเภทของเว็บไซต์ ☐ เว็บไซต์หลักของหน่วยงาน ☐ เว็บไซต์ภายในหน่วยงาน (Intranet)
☐ อื่นๆ โปรดระบุ.....

วัตถุประสงค์ในการบริการเว็บไซต์ (เลือกได้มากกว่า ๑ ตัวเลือก)
☐ เว็บไซต์ที่ให้บริการข้อมูลของประชาชน
☐ เว็บไซต์ให้บริการเกี่ยวกับโครงสร้างพื้นฐานสำคัญของประเทศ
☐ เว็บไซต์ของหน่วยงานที่มีการดำเนินการธุรกรรมทางอิเล็กทรอนิกส์
☐ อื่น ๆ โปรดระบุ.....

รูปแบบการจัดทำเว็บไซต์ ☐ เว็บไซต์บนระบบขององค์กร (On-Premises)
☐ เว็บไซต์บนระบบคลาวด์ (Cloud Service)
☐ เว็บไซต์ที่ใช้บริการเว็บโฮสติ้ง (Web Hosting)
☐ อื่นๆ โปรดระบุ.....

วันที่ประเมินตนเอง (Self-Assessment).....

ผู้ตอบแบบสอบถาม.....ตำแหน่ง.....

สังกัดหน่วยงาน (ภายใน).....

เบอร์โทร.....อีเมล.....

<u>ส่วนที่ ๒</u> กำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้กับข้อมูลหรือสารสนเทศ

ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. ๒๕๖๖ (๒๓)

ผลกระทบด้านที่ ๑ มูลค่าความเสียหายทางการเงินหรือทรัพย์สิน หรือต่อชื่อเสียงของหน่วยงาน

ตาราง ค๑ การประเมินผลกระทบต่อมูลค่าความเสียหายทางการเงินหรือทรัพย์สินหรือต่อชื่อเสียงของหน่วยงาน

วัตถุประสงค์/ระดับ	การรักษาความลับ (Confidentiality)	การรักษาความถูกต้อง (Integrity)	การรักษาสภาพพร้อมใช้งาน (Availability)
ต่ำ	☐ ในกรณีที่การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตไม่ว่าทั้งหมดหรือบางส่วน อาจส่งผลกระทบต่อการดำเนินงาน ทรัพย์สิน หรือชื่อเสียงของหน่วยงานหรือบุคคลเพียง<u>เล็กน้อยหรืออย่างจำกัด</u> หรือ อาจเปิดเผยข้อมูลลับที่ถูกกำหนดชั้นความลับเป็น<u>ชั้นลับ</u>	☐ ในกรณีที่การแก้ไขหรือการทำลายข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบต่อการดำเนินงาน หรือทรัพย์สินของหน่วยงานหรือบุคคล<u>เพียงเล็กน้อยหรืออย่างจำกัด</u>	☐ ในกรณีที่หน่วยงานไม่สามารถเข้าถึงและใช้งานข้อมูลหรือระบบสารสนเทศได้ อาจส่งผลกระทบต่อการดำเนินงาน หรือทรัพย์สินของหน่วยงานหรือบุคคล<u>เพียงเล็กน้อยหรืออย่างจำกัด</u>
กลาง	☐ ในกรณีที่การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตไม่ว่าทั้งหมดหรือบางส่วน อาจส่งผลกระทบต่อการดำเนินงาน ทรัพย์สิน หรือชื่อเสียงของหน่วยงานหรือบุคคลอย่างร้ายแรง หรือ อาจเปิดเผยข้อมูลลับที่ถูกกำหนดชั้นความลับเป็น<u>ชั้นลับมาก</u>	☐ ในกรณีที่การแก้ไขหรือการทำลายข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบต่อการดำเนินงาน หรือทรัพย์สินของหน่วยงานหรือบุคคล<u>อย่างร้ายแรง</u>	☐ ในกรณีที่หน่วยงานไม่สามารถเข้าถึงและใช้งานข้อมูลหรือระบบสารสนเทศได้ อาจส่งผลกระทบต่อการดำเนินงาน หรือทรัพย์สินของหน่วยงานหรือบุคคล<u>อย่างร้ายแรง</u>
สูง	☐ ในกรณีที่การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตไม่ว่าทั้งหมดหรือบางส่วน อาจส่งผลกระทบต่อการดำเนินงาน ทรัพย์สิน หรือชื่อเสียงของหน่วยงานหรือบุคคล<u>อย่างร้ายแรงมาก</u> หรือ อาจเปิดเผยข้อมูลลับที่ถูกกำหนดชั้นความลับเป็น<u>ชั้นลับที่สุด</u>	☐ ในกรณีที่การแก้ไขหรือการทำลายข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบต่อการดำเนินงาน หรือทรัพย์สินของหน่วยงานหรือบุคคล<u>อย่างร้ายแรงมาก</u>	☐ ในกรณีที่หน่วยงานไม่สามารถเข้าถึงและใช้งานข้อมูลหรือระบบสารสนเทศได้ อาจส่งผลกระทบต่อการดำเนินงาน หรือทรัพย์สินของหน่วยงานหรือบุคคล<u>อย่างร้ายแรงมาก</u>

ผลการประเมิน (นำไปกรอกในตาราง ค๕)

ผลกระทบมากที่สุด **เรื่อง** ☐ ความลับ ☐ ความถูกต้อง☐ สภาพพร้อมใช้ **ระดับ** ☐ ต่ำ☐ กลาง☐ สูง

ผลกระทบด้านที่ ๒ จำนวนของผู้ใช้บริการของหน่วยงาน บุคลากรของหน่วยงานหรือประชาชนที่อาจได้รับอันตรายต่อชีวิต ร่างกาย อนามัย ทรัพย์สิน หรือความเสียหายอื่นใด

ตาราง ค๒ การประเมินผลกระทบต่อจำนวนของผู้ใช้บริการของหน่วยงาน บุคลากรของหน่วยงานหรือประชาชนที่อาจได้รับอันตรายต่อชีวิต ร่างกาย อนามัย ทรัพย์สิน หรือความเสียหายอื่นใด

วัตถุประสงค์/ระดับ	การรักษาความลับ (Confidentiality)	การรักษาความถูกต้อง (Integrity)	การรักษาสภาพพร้อมใช้งาน (Availability)
ต่ำ	☐ ในกรณีที่การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตไม่ว่าทั้งหมดหรือบางส่วน อาจส่งผลกระทบต่อจำนวนของผู้ใช้บริการของหน่วยงาน บุคลากรของหน่วยงานหรือประชาชนที่อาจได้รับอันตรายต่อชีวิต ร่างกาย อนามัย ทรัพย์สิน หรือความเสียหายอื่นใดเพียงเล็กน้อยหรืออย่างจำกัด หรือ อาจเปิดเผยข้อมูลลับที่ถูกกำหนดชั้นความลับเป็นชั้นลับ	☐ ในกรณีที่การแก้ไขหรือการทำลายข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบต่อจำนวนของผู้ใช้บริการของหน่วยงาน บุคลากรของหน่วยงานหรือประชาชนที่อาจได้รับอันตรายต่อชีวิต ร่างกาย อนามัย ทรัพย์สิน หรือความเสียหายอื่นใดอย่างเล็กน้อยหรืออย่างจำกัด	☐ ในกรณีที่หน่วยงานไม่สามารถเข้าถึงและใช้งานข้อมูลหรือระบบสารสนเทศได้ อาจส่งผลกระทบต่อจำนวนของผู้ใช้บริการของหน่วยงาน บุคลากรของหน่วยงานหรือประชาชนที่อาจได้รับอันตรายต่อชีวิต ร่างกาย อนามัย ทรัพย์สิน หรือความเสียหายอื่นใดอย่างเล็กน้อยหรืออย่างจำกัด
กลาง	☐ ในกรณีที่การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตไม่ว่าทั้งหมดหรือบางส่วน อาจส่งผลกระทบต่อจำนวนของผู้ใช้บริการของหน่วยงาน บุคลากรของหน่วยงานหรือประชาชนที่อาจได้รับอันตรายต่อชีวิต ร่างกาย อนามัย ทรัพย์สิน หรือความเสียหายอื่นใดอย่างร้ายแรง หรือ อาจเปิดเผยข้อมูลลับที่ถูกกำหนดชั้นความลับเป็นชั้นลับมาก	☐ ในกรณีที่การแก้ไขหรือการทำลายข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบต่อจำนวนของผู้ใช้บริการของหน่วยงาน บุคลากรของหน่วยงานหรือประชาชนที่อาจได้รับอันตรายต่อชีวิต ร่างกาย อนามัย ทรัพย์สิน หรือความเสียหายอื่นใดอย่างร้ายแรง	☐ ในกรณีที่หน่วยงานไม่สามารถเข้าถึงและใช้งานข้อมูลหรือระบบสารสนเทศได้ อาจส่งผลกระทบต่อจำนวนของผู้ใช้บริการของหน่วยงาน บุคลากรของหน่วยงานหรือประชาชนที่อาจได้รับอันตรายต่อชีวิต ร่างกาย อนามัย ทรัพย์สิน หรือความเสียหายอื่นใดอย่างร้ายแรง
สูง	☐ ในกรณีที่การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตไม่ว่าทั้งหมดหรือบางส่วน อาจส่งผลกระทบต่อจำนวนของผู้ใช้บริการของหน่วยงาน บุคลากรของหน่วยงานหรือประชาชนที่อาจได้รับอันตรายต่อชีวิต ร่างกาย อนามัย ทรัพย์สิน หรือความเสียหายอื่นใดอย่างร้ายแรงมาก หรือ อาจเปิดเผยข้อมูลลับที่ถูกกำหนดชั้นความลับเป็นชั้นลับที่สุด	☐ ในกรณีที่การแก้ไขหรือการทำลายข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบต่อจำนวนของผู้ใช้บริการของหน่วยงาน บุคลากรของหน่วยงานหรือประชาชนที่อาจได้รับอันตรายต่อชีวิต ร่างกาย อนามัย ทรัพย์สิน หรือความเสียหายอื่นใดอย่างร้ายแรงมาก	☐ ในกรณีที่หน่วยงานไม่สามารถเข้าถึงและใช้งานข้อมูลหรือระบบสารสนเทศได้ อาจส่งผลกระทบต่อจำนวนของผู้ใช้บริการของหน่วยงาน บุคลากรของหน่วยงานหรือประชาชนที่อาจได้รับอันตรายต่อชีวิต ร่างกาย อนามัย ทรัพย์สิน หรือความเสียหายอื่นใดอย่างร้ายแรงมาก

ผลการประเมิน (นำไปกรอกในตาราง ค๕)

ผลกระทบมากที่สุด **เรื่อง** ☐ ความลับ ☐ ความถูกต้อง☐ สภาพพร้อมใช้ **ระดับ** ☐ ต่ำ☐ กลาง☐ สูง

ผลกระทบด้านที่ ๓ ความสามารถในการดำเนินการตามหน้าที่ของหน่วยงาน

ตาราง ค๓ การประเมินผลกระทบต่อความสามารถในการดำเนินการตามหน้าที่ของหน่วยงาน

วัตถุประสงค์/ระดับ	การรักษาความลับ (Confidentiality)	การรักษาความถูกต้อง (Integrity)	การรักษาสภาพพร้อมใช้งาน (Availability)
ต่ำ	☐ ในกรณีที่การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตไม่ว่าทั้งหมดหรือบางส่วนอาจส่งผลกระทบต่อความสามารถในการดำเนินการตามหน้าที่ของหน่วยงานหรือบุคคลเพียงเล็กน้อยหรืออย่างจำกัด หรือ อาจเปิดเผยข้อมูลลับที่ถูกกำหนดชั้นความลับเป็นชั้นลับ	☐ ในกรณีที่การแก้ไขหรือการทำลายข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบต่อความสามารถในการดำเนินการตามหน้าที่ของหน่วยงานหรือบุคคลอย่างเล็กน้อยหรืออย่างจำกัด	☐ ในกรณีที่หน่วยงานไม่สามารถเข้าถึงและใช้งานข้อมูลหรือระบบสารสนเทศได้ อาจส่งผลกระทบต่อความสามารถในการดำเนินการตามหน้าที่ของหน่วยงานหรือบุคคลอย่างเล็กน้อยหรืออย่างจำกัด
กลาง	☐ ในกรณีที่การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตไม่ว่าทั้งหมดหรือบางส่วน อาจส่งผลกระทบต่อความสามารถในการดำเนินการตามหน้าที่ของหน่วยงานหรือบุคคลอย่างร้ายแรง หรืออาจเปิดเผยข้อมูลลับที่ถูกกำหนดชั้นความลับเป็นชั้นลับมาก	☐ ในกรณีที่การแก้ไขหรือการทำลายข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบต่อความสามารถในการดำเนินการตามหน้าที่ของหน่วยงานหรือบุคคลอย่างร้ายแรง	☐ ในกรณีที่หน่วยงานไม่สามารถเข้าถึงและใช้งานข้อมูลหรือระบบสารสนเทศได้ อาจส่งผลกระทบต่อความสามารถในการดำเนินการตามหน้าที่ของหน่วยงานหรือบุคคลอย่างร้ายแรง
สูง	☐ ในกรณีที่การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตไม่ว่าทั้งหมดหรือบางส่วน อาจส่งผลกระทบต่อความสามารถในการดำเนินการตามหน้าที่ของหน่วยงานหรือบุคคลอย่างร้ายแรงมาก หรือ อาจเปิดเผยข้อมูลลับที่ถูกกำหนดชั้นความลับเป็นชั้นลับที่สุด	☐ ในกรณีที่การแก้ไขหรือการทำลายข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบต่อความสามารถในการดำเนินการตามหน้าที่ของหน่วยงานหรือบุคคลอย่างร้ายแรงมาก	☐ ในกรณีที่หน่วยงานไม่สามารถเข้าถึงและใช้งานข้อมูลหรือระบบสารสนเทศได้ อาจส่งผลกระทบต่อความสามารถในการดำเนินการตามหน้าที่ของหน่วยงานหรือบุคคลอย่างร้ายแรงมาก

ผลการประเมิน (นำไปกรอกในตาราง ค๕)

ผลกระทบมากที่สุด **เรื่อง** ☐ ความลับ ☐ความถูกต้อง ☐สภาพพร้อมใช้ **ระดับ** ☐ต่ำ ☐ กลาง☐ สูง

ผลกระทบด้านที่ ๔ ความมั่นคงของรัฐและความสงบเรียบร้อยภายในประเทศ

ตาราง ค๔ การประเมินผลกระทบต่อความมั่นคงของรัฐและความสงบเรียบร้อยภายในประเทศ

วัตถุประสงค์/ระดับ	**การรักษาความลับ (Confidentiality)**	**การรักษาความถูกต้อง (Integrity)**	**การรักษาสภาพพร้อมใช้งาน (Availability)**
ต่ำ	☐ ในกรณีที่การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตไม่ว่าทั้งหมดหรือบางส่วน อาจส่งผลกระทบต่อความมั่นคงของรัฐและความสงบเรียบร้อยภายในประเทศเพียงเล็กน้อยหรืออย่างจำกัด หรือ อาจเปิดเผยข้อมูลลับที่ถูกกำหนดชั้นความลับเป็นชั้นลับ	☐ ในกรณีที่การแก้ไขหรือการทำลายข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบต่อการความมั่นคงของรัฐและความสงบเรียบร้อยภายในประเทศอย่างเล็กน้อยหรืออย่างจำกัด	☐ ในกรณีที่หน่วยงานไม่สามารถเข้าถึงและใช้งานข้อมูลหรือระบบสารสนเทศได้ อาจส่งผลกระทบต่อความมั่นคงของรัฐและความสงบเรียบร้อยภายในประเทศอย่างเล็กน้อยหรืออย่างจำกัด
กลาง	☐ ในกรณีที่การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตไม่ว่าทั้งหมดหรือบางส่วน อาจส่งผลกระทบต่อความมั่นคงของรัฐและความสงบเรียบร้อยภายในประเทศอย่างร้ายแรง หรือ อาจเปิดเผยข้อมูลลับที่ถูกกำหนดชั้นความลับเป็นชั้นลับมาก	☐ ในกรณีที่การแก้ไขหรือการทำลายข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบต่อความมั่นคงของรัฐและความสงบเรียบร้อยภายในประเทศอย่างร้ายแรง	☐ ในกรณีที่หน่วยงานไม่สามารถเข้าถึงและใช้งานข้อมูลหรือระบบสารสนเทศได้ อาจส่งผลกระทบต่อความมั่นคงของรัฐและความสงบเรียบร้อยภายในประเทศอย่างร้ายแรง
สูง	☐ ในกรณีที่การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตไม่ว่าทั้งหมดหรือบางส่วน อาจส่งผลกระทบต่อความมั่นคงของรัฐและความสงบเรียบร้อยภายในประเทศอย่างร้ายแรงมาก หรือ อาจเปิดเผยข้อมูลลับที่ถูกกำหนดชั้นความลับเป็นชั้นลับที่สุด	☐ ในกรณีที่การแก้ไขหรือการทำลายข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบต่อความมั่นคงของรัฐและความสงบเรียบร้อยภายในประเทศอย่างร้ายแรงมาก	☐ ในกรณีที่หน่วยงานไม่สามารถเข้าถึงและใช้งานข้อมูลหรือระบบสารสนเทศได้ อาจส่งผลกระทบต่อความมั่นคงของรัฐและความสงบเรียบร้อยภายในประเทศอย่างร้ายแรงมาก

ผลการประเมิน (นำไปกรอกในตาราง ค๕)

ผลกระทบมากที่สุด **เรื่อง** ☐ ความลับ ☐ความถูกต้อง ☐สภาพพร้อมใช้ **ระดับ** ☐ต่ำ ☐ กลาง☐ สูง

ตาราง ค๕ ตารางสรุปผลการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้กับข้อมูลหรือสารสนเทศและการประเมินระดับผลกระทบ

ผลกระทบด้าน	วัตถุประสงค์ที่มีผลกระทบมากที่สุด	ระดับผลกระทบ
มูลค่าความเสียหายทางการเงินหรือทรัพย์สินหรือต่อชื่อเสียงของหน่วยงาน	☐ ความลับ ☐ ความถูกต้อง ☐ สภาพพร้อมใช้	☐ต่ำ ☐ กลาง ☐ สูง
จำนวนของผู้ใช้บริการของหน่วยงาน บุคลากรของหน่วยงานหรือประชาชนที่อาจได้รับอันตรายต่อชีวิต ร่างกาย อนามัย ทรัพย์สิน หรือความเสียหายอื่นใด	☐ ความลับ ☐ ความถูกต้อง ☐ สภาพพร้อมใช้	☐ต่ำ ☐ กลาง ☐ สูง
ความสามารถในการดำเนินการตามหน้าที่ของหน่วยงาน	☐ ความลับ ☐ ความถูกต้อง ☐ สภาพพร้อมใช้	☐ต่ำ ☐ กลาง ☐ สูง
ความมั่นคงของรัฐและความสงบเรียบร้อยภายในประเทศ	☐ ความลับ ☐ ความถูกต้อง ☐ สภาพพร้อมใช้	☐ต่ำ ☐ กลาง ☐ สูง
ใส่ระดับผลกระทบมากที่สุด (นำผลไปใส่ในตาราง ค๖)		

ตาราง ค๖ ข้อกำหนดขั้นต่ำในการปฏิบัติตามมาตรฐานฉบับนี้ แบ่งตามผลกระทบจากการประเมิน

ผลกระทบ	เกณฑ์การดำเนินการตามข้อกำหนดขั้นต่ำ
☐ผลกระทบระดับ**สูง**	หน่วยงานจะต้องดำเนินการตามข้อกำหนดในมาตรฐานฉบับนี้ ทุกข้อ
☐ ผลกระทบระดับ**กลาง**	หน่วยงานจะต้องดำเนินการตามข้อกำหนดในมาตรฐานฉบับนี้ ดังนี้ **หัวข้อที่ ๕** ดำเนินการตามข้อกำหนดในมาตรฐานฉบับนี้ ทุกข้อ **หัวข้อที่ ๖** ดำเนินการตามข้อกำหนดในมาตรฐานฉบับนี้ โดย ยกเว้น ข้อกำหนด ข้อ ๖.๑.๑ เฉพาะส่วนของการประเมินช่องโหว่และทดสอบเจาะระบบ และการจัดการผู้ให้บริการภายนอก (Third Party Management) ข้อ ๖.๒.๑ ข้อ ๖.๒.๓ (๕) - (๗) และข้อ ๖.๒.๔ เฉพาะส่วนของการแบ่งปันข้อมูล (Information Sharing)
☐ผลกระทบระดับ**ต่ำ**	หน่วยงานจะต้องดำเนินการตามข้อกำหนดในมาตรฐานฉบับนี้ ดังนี้ **หัวข้อที่ ๕** ดำเนินการตามข้อกำหนดในมาตรฐานฉบับนี้ ทุกข้อ **หัวข้อที่ ๖** ดำเนินการตามข้อกำหนดในมาตรฐานฉบับนี้ โดย ยกเว้น ข้อกำหนด ข้อ ๖.๑.๑ ข้อ ๖.๒.๑ ข้อ ๖.๒.๓ (๔) - (๗) ข้อ ๖.๒.๔ เฉพาะส่วนการบริหารจัดการเชื่อมต่อระยะไกล (Remote Connection) สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media) และการแบ่งปันข้อมูล (Information Sharing) ข้อ ๖.๓.๑ ข้อ ๖.๔.๑ และ ข้อ ๖.๕.๑

ตาราง ค๗ การระบุหน่วยงานที่ต้องปฏิบัติตามหรือส่งเสริมให้ปฏิบัติตามมาตรฐานฉบับนี้

กลุ่ม	ลักษณะหน่วยงาน	การปฏิบัติตามข้อกำหนด
☐ กลุ่มที่ ๑	๑) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ๒) หน่วยงานควบคุมหรือกำกับดูแล ๓) หน่วยงานของรัฐ	**จะต้อง**ปฏิบัติตาม
☐ กลุ่มที่ ๒	๑) หน่วยงานเอกชน	**ส่งเสริม**ให้ปฏิบัติตาม

ส่วนที่ ๓ แบบตรวจรายการเพื่อตรวจสอบสถานะความมั่นคงปลอดภัยสำหรับเว็บไซต์

ที่	ข้อกำหนด	ข้อเสนอแนะ	การประเมิน	หลักฐาน
ข้อกำหนดการกำกับดูแลด้านความมั่นคงปลอดภัยสำหรับเว็บไซต์ (หัวข้อ ๕)				
๑	**การสำรวจบริบทของหน่วยงาน (Organization Context) (หัวข้อ ๕.๑)**			
๑.๑	หน่วยงานจะต้องมีการทำความเข้าใจสถานการณ์ต่าง ๆ ที่เกี่ยวข้องกับการตัดสินใจในการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสำหรับเว็บไซต์ของหน่วยงาน โดยหน่วยงานอาจจะพิจารณารายละเอียดการดำเนินการสำรวจบริบทของหน่วยงาน (Organization Context) ตามข้อเสนอแนะและคำอธิบายเพิ่มเติมของมาตรฐานฉบับนี้ (หัวข้อ ๕.๑.๑)	☐ ยังต้องปรับปรุง ☐ ดำเนินการแล้ว	
๒	**นโยบายด้านความมั่นคงปลอดภัยสำหรับเว็บไซต์ (Website Security Policies) (หัวข้อ ๕.๒)**			
๒.๑	หน่วยงานจะต้องมีการกำหนดนโยบายความมั่นคงปลอดภัยสำหรับเว็บไซต์ตามบริบทขององค์กรและกลยุทธ์ด้านความมั่นคงปลอดภัยเว็บไซต์ โดยมีการจัดลำดับความสำคัญ มีการสื่อสาร รวมถึงมีการบังคับใช้ (หัวข้อ ๕.๒.๑)	☐ ยังต้องปรับปรุง ☐ ดำเนินการแล้ว	
		หน่วยงานจะต้องมีการกำหนดนโยบายความมั่นคงปลอดภัยสำหรับเว็บไซต์ตามบริบทขององค์กรและกลยุทธ์ด้านความมั่นคงปลอดภัยเว็บไซต์ โดยพิจารณาแนวทางได้จากประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕ ในภาคผนวก ค ตัวอย่างการประกาศนโยบาย ข้อ ๔ หรืออาจจะพิจารณาจัดทำนโยบายตามตัวอย่างนโยบายการรักษาความมั่นคงปลอดภัยเว็บไซต์ (Website Security Policy) ของ สกมช.	☐ ดำเนินการแล้ว ☐ อยู่ในระหว่างดำเนินการ ☐ ยังไม่ได้ดำเนินการ	

ที่	ข้อกำหนด	ข้อเสนอแนะ	การประเมิน	หลักฐาน
		เฉพาะกรณีหน่วยงานมีนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ หรือนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์อยู่แล้ว หน่วยงานควรจะพิจารณาตรวจสอบและปรับปรุงให้ครอบคลุมและสอดคล้องกับมาตรฐานฉบับนี้	☐ ดำเนินการแล้ว ☐ อยู่ในระหว่างดำเนินการ ☐ ยังไม่ได้ดำเนินการ	
๒.๒	หน่วยงานจะต้องมีการทบทวน ปรับปรุง สื่อสาร และบังคับใช้นโยบายความมั่นคงปลอดภัยสำหรับเว็บไซต์เพื่อสะท้อนการเปลี่ยนแปลงความต้องการ ภัยคุกคาม เทคโนโลยี รวมถึงภารกิจของหน่วยงาน (หัวข้อ ๕.๒.๒)		☐ ยังต้องปรับปรุง ☐ ดำเนินการแล้ว	
๓	**กลยุทธ์การจัดการความเสี่ยง (Risk Management Strategy) (หัวข้อ ๕.๓)**			
๓.๑	หน่วยงานจะต้องมีการกำหนดวัตถุประสงค์การบริหารความเสี่ยงและมีการจัดทำกรอบการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสำหรับเว็บไซต์เป็นลายลักษณ์อักษร (หัวข้อ ๕.๓.๑)		☐ ยังต้องปรับปรุง ☐ ดำเนินการแล้ว	
๓.๒	เฉพาะหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานจะต้องพิจารณาดำเนินการประเมินความเสี่ยงตามคำแนะนำของ สกมช. เรื่อง แนวทางปฏิบัติในการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และมีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ (หัวข้อ ๕.๓.๒)		☐ ยังต้องปรับปรุง ☐ ดำเนินการแล้ว	
๓.๓	หน่วยงานจะต้องมีการจัดทำ สื่อสาร และมีการเก็บรักษารายการความเสี่ยงที่ระบุไว้ในทะเบียนความเสี่ยง (Risk Register) ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) และค่าเบี่ยงเบนของระดับความเสี่ยงที่ยอมรับได้ (Risk Tolerance) ให้เป็นปัจจุบัน และติดตามระดับความเสี่ยงให้อยู่ในเกณฑ์ที่ยอมรับได้ (หัวข้อ ๕.๓.๓)		☐ ยังต้องปรับปรุง ☐ ดำเนินการแล้ว	
๔	**บทบาทและความรับผิดชอบด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ (หัวข้อ ๕.๔)**			
๔.๑	หน่วยงานจะต้องมีการจัดโครงสร้างองค์กรให้มีการถ่วงดุล พร้อมกำหนดอำนาจ บทบาทหน้าที่ และความรับผิดชอบที่ชัดเจนเกี่ยวกับการบริหารจัดการความมั่นคงปลอดภัยสำหรับเว็บไซต์ โดยหน่วยงานอาจจะ ใช้แนวคิดการถ่วงดุลตามหลักการควบคุม กำกับ และตรวจสอบ (Three Lines of Defense) มาประยุกต์ใช้กับการจัดโครงสร้างองค์กรให้มีการถ่วงดุล ในการบริหารจัดการความมั่นคงปลอดภัยสำหรับเว็บไซต์ ซึ่งมี	☐ ยังต้องปรับปรุง ☐ ดำเนินการแล้ว	

ที่	ข้อกำหนด	ข้อเสนอแนะ	การประเมิน	หลักฐาน
		รายละเอียดตามข้อเสนอแนะและคำอธิบายเพิ่มเติมของมาตรฐานฉบับนี้ (หัวข้อ ๕.๔.๑)		
๔.๒		หน่วยงานจะต้องกำหนดให้มีผู้รับผิดชอบในการจัดทำและบริหารจัดการเว็บไซต์ของหน่วยงาน รวมถึงดำเนินการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ ซึ่งต้องเป็นนิติบุคคลหรือเป็นส่วนหนึ่งของนิติบุคคลที่สามารถรับผิดตามกฎหมายได้ และการมอบหมายหน้าที่จะต้องทำโดยไม่ขาดช่วง (หัวข้อ ๕.๔.๒)	☐ ยังต้องปรับปรุง ☐ ดำเนินการแล้ว	
๔.๓		หน่วยงานจะต้องกำหนด สื่อสาร ทำความเข้าใจและบังคับใช้บทบาท ความรับผิดชอบ และอำนาจที่เกี่ยวข้องกับการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสำหรับเว็บไซต์ รวมถึงจัดสรรทรัพยากรให้เพียงพอ (หัวข้อ ๕.๔.๓)	☐ ยังต้องปรับปรุง ☐ ดำเนินการแล้ว	
๕	**การวางแผนกำหนดความต้องการด้านความมั่นคงปลอดภัยของเว็บไซต์ (หัวข้อ ๕.๕)**			
๕.๑		หน่วยงานจะต้องมีการกำหนดวัตถุประสงค์และความต้องการในการจัดทำเว็บไซต์ ด้านฟังก์ชัน ด้านประสิทธิภาพ และที่สำคัญความต้องการด้านความมั่นคงปลอดภัย โดยหน่วยงานควรจะมีการวางแผนกำหนดความต้องการด้านความมั่นคงปลอดภัยของเว็บไซต์ โดยพิจารณาให้เป็นไปตามข้อเสนอแนะและคำอธิบายเพิ่มเติมของมาตรฐานฉบับนี้ (หัวข้อ ๕.๕.๑)	☐ ยังต้องปรับปรุง ☐ ดำเนินการแล้ว	
๖	**การกำหนดแนวทางด้านความมั่นคงปลอดภัยสำหรับเว็บไซต์ (หัวข้อ ๕.๖)**			
๖.๑		หน่วยงานจะต้องมีแนวทางด้านความมั่นคงปลอดภัยในระดับพื้นฐานตามคุณลักษณะด้านความมั่นคงปลอดภัยพื้นฐาน ๓ ด้าน คือ การรักษาความลับ (Confidentiality) การรักษาความครบถ้วนสมบูรณ์ (Integrity) และการเตรียมความพร้อมใช้งาน (Availability) โดยหน่วยงานควรจะดำเนินการตามแนวทางด้านความมั่นคงปลอดภัยในระดับพื้นฐาน ซึ่งมีรายละเอียดตามข้อเสนอแนะและคำอธิบายเพิ่มเติมของมาตรฐานฉบับนี้ (หัวข้อ ๕.๖.๑)	☐ ยังต้องปรับปรุง ☐ ดำเนินการแล้ว	
๖.๒		หน่วยงานจะต้องมีการกำหนดคุณลักษณะความมั่นคงปลอดภัยให้กับข้อมูลหรือสารสนเทศของเว็บไซต์ ตามคุณลักษณะด้านความมั่นคงปลอดภัยพื้นฐาน ๓ ระดับให้เป็นไปตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. ๒๕๖๖ (หัวข้อ ๕.๖.๒)	☐ ยังต้องปรับปรุง ☐ ดำเนินการแล้ว	

ที่	ข้อกำหนด	ข้อเสนอแนะ	การประเมิน	หลักฐาน
๖.๓		<u>เฉพาะหน่วยงานมีการดำเนินการธุรกรรมทางอิเล็กทรอนิกส์</u> หน่วยงานจะต้องดำเนินการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ ตามข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับโปรแกรมประยุกต์บนเว็บ รวมถึงประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕ (หัวข้อ ๕.๖.๓)	☐ ยังต้องปรับปรุง ☐ ดำเนินการแล้ว	
๖.๔		<u>เฉพาะหน่วยงานภาครัฐ</u> หน่วยงาน<u>จะต้อง</u>ดำเนินการตามมาตรฐานเว็บไซต์ภาครัฐ (Government Website Standard) Version ๓.๐ หัวข้อที่ ๗ ความมั่นคงปลอดภัยสำหรับเว็บไซต์ (หัวข้อ ๕.๖.๔)	☐ ยังต้องปรับปรุง ☐ ดำเนินการแล้ว	
๖.๕		<u>เฉพาะหน่วยงานที่มีเว็บไซต์ใช้บริการคลาวด์</u> หน่วยงาน<u>จะต้อง</u>มีการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับเว็บไซต์ที่ใช้บริการคลาวด์ ให้เป็นไปตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. ๒๕๖๗ (หัวข้อ ๕.๖.๕)	☐ ยังต้องปรับปรุง ☐ ดำเนินการแล้ว	
๖.๖		หน่วยงาน<u>จะต้อง</u>พิจารณาเลือกผู้ให้บริการด้านความมั่นคงปลอดภัยไซเบอร์สำหรับเว็บไซต์ เช่น การดำเนินการประเมินช่องโหว่ (Vulnerability Assessment) การทดสอบเจาะระบบ (Penetration Testing) ของเว็บไซต์ ที่ได้รับการรับรองและได้รับประกาศนียบัตร (Accreditations and Certifications) ที่เป็นที่ยอมรับในอุตสาหกรรม (หัวข้อ ๕.๖.๖)	☐ ยังต้องปรับปรุง ☐ ดำเนินการแล้ว	
๖.๗		<u>เฉพาะหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ</u> หน่วยงาน<u>จะต้อง</u>ปฏิบัติตามแนวปฏิบัติการรักษาความมั่นคงปลอดภัยเว็บไซต์ (Website Security Guideline) ของ สกมช. (หัวข้อ ๕.๖.๗)	☐ ยังต้องปรับปรุง ☐ ดำเนินการแล้ว	

ที่	ข้อกำหนด	ข้อเสนอแนะ	การประเมิน	หลักฐาน
๖.๘	หน่วยงานจะต้องมีการกำหนดแนวทางในการสำรองข้อมูลเพื่อลดผลกระทบที่เกิดขึ้นหากเว็บไซต์ของหน่วยงานโดนโจมตีจากภัยคุกคามทางไซเบอร์ โดยหน่วยงานอาจจะพิจารณาองค์ประกอบในการสำรองข้อมูล ซึ่งมีรายละเอียดตามข้อเสนอแนะและคำอธิบายเพิ่มเติมของมาตรฐานฉบับนี้ (หัวข้อ ๕.๖.๘)		☐ ยังต้องปรับปรุง ☐ ดำเนินการแล้ว	
๖.๙	หน่วยงานจะต้องมีการจัดการข้อมูลจราจรทางคอมพิวเตอร์ (Log Management) ให้เป็นไปตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และที่แก้ไขเพิ่มเติม (หัวข้อ ๕.๖.๙)		☐ ยังต้องปรับปรุง ☐ ดำเนินการแล้ว	
๖.๑๐	หน่วยงานจะต้องกำหนดหลักปฏิบัติในการเลิกใช้งานเว็บไซต์ เพื่อป้องกันภัยคุกคามไซเบอร์ที่อาจจะเกิดกับผู้ใช้บริการเว็บไซต์ ผู้ใช้งานอินเทอร์เน็ตทั่วไป ผู้ให้บริการ โดยหน่วยงานควรจะกำหนดหลักปฏิบัติในการเลิกใช้งานเว็บไซต์ซึ่งมีรายละเอียดตามข้อเสนอแนะและคำอธิบายเพิ่มเติมของมาตรฐานฉบับนี้ หรือหน่วยงานอาจจะพิจารณาการทำลายข้อมูลตามข้อเสนอแนะให้เป็นไปตาม NIST Special Publication 800-88 และขั้นตอนหลักของการทำลายข้อมูล (หัวข้อ ๕.๖.๑๐)		☐ ยังต้องปรับปรุง ☐ ดำเนินการแล้ว	
ข้อกำหนดการดำเนินการและการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ (Security and Operation Requirement) (หัวข้อ ๖)				
๗	**การระบุความเสี่ยงที่จะเกิดขึ้นกับเว็บไซต์ (Website Security Identification) (หัวข้อ ๖.๑)**			
๗.๑	หน่วยงานจะต้องมีการจัดการทรัพย์สิน (Asset Management) การประเมินความเสี่ยง (Risk Assessment) การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing) และการจัดการผู้ให้บริการภายนอก (Third Party Management) ให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (หัวข้อ ๖.๑.๑)		☐ ยังต้องปรับปรุง ☐ ดำเนินการแล้ว	
		หน่วยงานจะต้องจัดทำทะเบียนทรัพย์สิน และตรวจสอบทะเบียนทรัพย์สิน อย่างน้อยปี ละ ๑ ครั้ง รวมถึงปรับปรุงทะเบียนทรัพย์สินทุกครั้ง หากมีการเปลี่ยนแปลงใดๆ ให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัย	☐ ดำเนินการแล้ว ☐ อยู่ในระหว่างดำเนินการ ☐ ยังไม่ได้ดำเนินการ	

ที่	ข้อกำหนด	ข้อเสนอแนะ	การประเมิน	หลักฐาน
		ไซเบอร์ โดยอาจจะพิจารณาดำเนินการจัดการทรัพย์สิน ตามรายละเอียดข้อเสนอแนะและคำอธิบายเพิ่มเติมของมาตรฐานฉบับนี้		
		หน่วยงานจะต้องมีการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปี ละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญและปรับปรุงทะเบียนความเสี่ยงทุกครั้งหลังการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับเว็บไซต์ ให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยอาจจะพิจารณาการประเมินความเสี่ยง (Risk Assessment) ใน ๒ รูปแบบ ได้แก่ การประเมินความเสี่ยงเชิงปริมาณและการประเมินความเสี่ยงเชิงคุณภาพ และอาจจะพิจารณาขั้นตอนหลักในการประเมินความเสี่ยง ซึ่งมีรายละเอียดตามข้อเสนอแนะและคำอธิบายเพิ่มเติมของมาตรฐานฉบับนี้	☐ ดำเนินการแล้ว ☐ อยู่ในระหว่างดำเนินการ ☐ ยังไม่ได้ดำเนินการ	
		หน่วยงานจะต้องมีแนวทางจัดการ ควบคุม และป้องกันความเสี่ยงที่เหมาะสมสอดคล้องกับผลการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้ความเสี่ยงที่เหลืออยู่ (Residual Risk) อยู่ในระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับเว็บไซต์ที่ยอมรับได้	☐ ดำเนินการแล้ว ☐ อยู่ในระหว่างดำเนินการ ☐ ยังไม่ได้ดำเนินการ	
		หน่วยงานจะต้องมีการประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment) โดยอ้างอิงตามหลักการบริหารความเสี่ยงของหน่วยงาน โดยครอบคลุมการให้บริการเว็บไซต์ ให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อาจจะพิจารณาขอบเขตของการประเมินช่องโหว่ของบริการที่สำคัญครอบคลุมความมั่นคงปลอดภัยของระบบคอมพิวเตอร์ โครงสร้างเครือข่ายสื่อสารข้อมูล เครื่องบริการเว็บ และเว็บแอปพลิเคชัน และอาจจะพิจารณาดำเนินการ	☐ ดำเนินการแล้ว ☐ อยู่ในระหว่างดำเนินการ ☐ ยังไม่ได้ดำเนินการ	

ที่	ข้อกำหนด	ข้อเสนอแนะ	การประเมิน	หลักฐาน
		ตามแนวทางในการประเมินช่องโหว่ ซึ่งมีรายละเอียดตามข้อเสนอแนะและคำอธิบายเพิ่มเติมของมาตรฐานฉบับนี้		
		หน่วยงานควรจะดำเนินการทดสอบเจาะระบบ (Penetration Testing) โดยพิจารณาดำเนินการอย่างน้อยปีละ ๑ ครั้ง ตามความจำเป็น ให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และอาจจะพิจารณาปัจจัยในการดำเนินการทดสอบการเจาะระบบเว็บไซต์ รวมถึงเลือกผู้ให้บริการทดสอบเจาะระบบ โดยพิจารณาตามรายละเอียดข้อเสนอแนะและคำอธิบายเพิ่มเติมของมาตรฐานฉบับนี้	☐ ดำเนินการแล้ว ☐ อยู่ในระหว่างดำเนินการ ☐ ยังไม่ได้ดำเนินการ	
		หน่วยงานควรจะมีการตรวจสอบผู้ให้บริการภายนอก (Third Party Management) จะต้องรับผิดชอบ (Responsible) และมีภาระรับผิดชอบ (Accountable) ในการดูแลรักษาความมั่นคงปลอดภัยไซเบอร์ในการดำเนินงานให้บริการเว็บไซต์ ให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	☐ ดำเนินการแล้ว ☐ อยู่ในระหว่างดำเนินการ ☐ ยังไม่ได้ดำเนินการ	
		หน่วยงานควรจะมีข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการภายนอกในข้อตกลงระดับการให้บริการ (Service Level Agreement) หรือเงื่อนไขของสัญญากับผู้ให้บริการภายนอก ให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	☐ ดำเนินการแล้ว ☐ อยู่ในระหว่างดำเนินการ ☐ ยังไม่ได้ดำเนินการ	
		หน่วยงานควรจะพิจารณาสร้างกระบวนการตรวจสอบความถูกต้องของผู้ให้บริการภายนอกว่าสอดคล้องกับข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์สำหรับเว็บไซต์ในเงื่อนไขของสัญญา และควรจะพิจารณาดำเนินการเจรจาต่อรองเงื่อนไขของสัญญาจ้างให้สอดคล้องกับกรณีที่มีข้อกำหนดทางกฎหมายหรือข้อบังคับใหม่ ให้เป็นไปตาม	☐ ดำเนินการแล้ว ☐ อยู่ในระหว่างดำเนินการ ☐ ยังไม่ได้ดำเนินการ	

ที่	ข้อกำหนด	ข้อเสนอแนะ	การประเมิน	หลักฐาน
		ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์		
๘	**การป้องกันความเสี่ยงที่อาจจะเกิดขึ้นกับเว็บไซต์ (Website Security Protection) (หัวข้อ ๖.๒)**			
๘.๑		หน่วยงานจะต้องกำหนดแนวทางในการพัฒนาโปรแกรมประยุกต์บนเว็บ (Web Application) อย่างมั่นคงปลอดภัย เช่น พิจารณาใช้หลักการ DevSecOps ตั้งแต่ขั้นตอนการพัฒนาจนถึงการใช้งานจริงโดยมีการคำนึงถึงสิ่งสำคัญในการรักษาความมั่นคงปลอดภัยในการพัฒนาโปรแกรมประยุกต์บนเว็บ โดยหน่วยงานควรจะพิจารณาปรับใช้ตัวอย่างในการปรับใช้หลักการ DevSecOps และอาจจะพิจารณาสิ่งสำคัญในการรักษาความมั่นคงปลอดภัยของการพัฒนาโปรแกรมประยุกต์บนเว็บ รวมถึงอาจจะพิจารณาประยุกต์ใช้หลักการ DevSecOps โดยใช้หลักการ DSOMM ของมูลนิธิ OWASP ซึ่งมีรายละเอียดตามข้อเสนอแนะและคำอธิบายเพิ่มเติมของมาตรฐานฉบับนี้ (หัวข้อ ๖.๒.๑)	☐ ยังต้องปรับปรุง ☐ ดำเนินการแล้ว	
๘.๒		หน่วยงานจะต้องพิจารณาถึงปัจจัยเสี่ยงด้านความมั่นคงปลอดภัยของเว็บไซต์ที่พบได้บ่อยของมูลนิธิ OWASP ในการพัฒนาโปรแกรมประยุกต์บนเว็บ (Web Application) (หัวข้อ ๖.๒.๒)	☐ ยังต้องปรับปรุง ☐ ดำเนินการแล้ว	
๘.๓		หน่วยงานจะต้องพิจารณาการออกแบบสถาปัตยกรรมเว็บไซต์อย่างมั่นคงปลอดภัย ในส่วนของโครงสร้างของเว็บไซต์หรือโปรแกรมประยุกต์บนเว็บ โดยอาจจะพิจารณาส่วนประกอบของการออกแบบที่คำนึงถึงการแบ่งส่วนเครือข่าย (Network segmentation) มีการจัดวางเครื่องบริการเว็บ (Web Server) และเครื่องบริการฐานข้อมูล (Database Server) ร่วมกับอุปกรณ์รักษาความมั่นคงปลอดภัย (หัวข้อ ๖.๒.๓)	☐ ยังต้องปรับปรุง ☐ ดำเนินการแล้ว	

ที่	ข้อกำหนด	ข้อเสนอแนะ	การประเมิน	หลักฐาน
		หน่วยงานควรจะพิจารณาวางเครื่องบริการเว็บ (Web Server) ร่วมกับอุปกรณ์และบริการการรักษาความมั่งคงปลอดภัยพื้นฐาน เป็นอย่างน้อย หรืออาจจะพิจารณาวางเครื่องบริการเว็บ (Web Server) ร่วมกับการให้บริการป้องกัน Web Application (WAF) หรือหน่วยงานอาจจะพิจารณาวางเครื่องบริการเว็บ (Web Server) ร่วมกับผลิตภัณฑ์การรักษาความมั่นคงปลอดภัยเพิ่มเติม ซึ่งมีรายละเอียดตามข้อเสนอแนะและคำอธิบายเพิ่มเติมของมาตรฐานฉบับนี้	☐ ดำเนินการแล้ว ☐ อยู่ในระหว่างดำเนินการ ☐ ยังไม่ได้ดำเนินการ	
		หน่วยงานควรจะพิจารณาออกแบบโครงสร้างเว็บไซต์ออกเป็น ๔ ส่วน ให้เป็นไปตามข้อเสนอแนะและคำอธิบายเพิ่มเติมของมาตรฐานฉบับนี้	☐ ดำเนินการแล้ว ☐ อยู่ในระหว่างดำเนินการ ☐ ยังไม่ได้ดำเนินการ	
๘.๔	หน่วยงานจะต้องมีการควบคุมการเข้าถึง (Access Control) และทำให้ระบบมีความแข็งแกร่ง (System Hardening) มีการบริหารจัดการเชื่อมต่อระยะไกล (Remote Connection) สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media) และการแบ่งปันข้อมูล (Information Sharing) รวมถึงมีการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์สำหรับเว็บไซต์ (Website Security Awareness) ให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (หัวข้อ ๖.๒.๔)	☐ ยังต้องปรับปรุง ☐ ดำเนินการแล้ว	
		หน่วยงานจะต้องมีการควบคุมการเข้าถึง (Access Control) ให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	☐ ดำเนินการแล้ว ☐ อยู่ในระหว่างดำเนินการ ☐ ยังไม่ได้ดำเนินการ	
		หน่วยงานจะต้องมีการทำให้ระบบมีความแข็งแกร่ง (System Hardening) ให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	☐ ดำเนินการแล้ว ☐ อยู่ในระหว่างดำเนินการ ☐ ยังไม่ได้ดำเนินการ	

ที่	ข้อกำหนด	ข้อเสนอแนะ	การประเมิน	หลักฐาน
		หน่วยงานจะต้องมีการบริหารจัดการเชื่อมต่อระยะไกล (Remote Connection) ให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	☐ ดำเนินการแล้ว ☐ อยู่ในระหว่างดำเนินการ ☐ ยังไม่ได้ดำเนินการ	
		หน่วยงานจะต้องมีการบริหารจัดการสื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media) ให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	☐ ดำเนินการแล้ว ☐ อยู่ในระหว่างดำเนินการ ☐ ยังไม่ได้ดำเนินการ	
		หน่วยงานจะต้องมีการแบ่งปันข้อมูล (Information Sharing) ให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	☐ ดำเนินการแล้ว ☐ อยู่ในระหว่างดำเนินการ ☐ ยังไม่ได้ดำเนินการ	
		หน่วยงานจะต้องมีการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์สำหรับเว็บไซต์ (Website Security Awareness) ให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	☐ ดำเนินการแล้ว ☐ อยู่ในระหว่างดำเนินการ ☐ ยังไม่ได้ดำเนินการ	
๘.๕	หน่วยงานจะต้องพิจารณาการพิสูจน์ตัวตนแบบหลายปัจจัย (Multi-Factor Authentication: MFA) หรือพิจารณาการพิสูจน์ตัวตนจากระบบเชื่อมโยงข้อมูลเพื่อการพิสูจน์และยืนยันตัวตนทางดิจิทัล (Digital ID) ตามข้อเสนอแนะของ สพร. นอกเหนือจากการควบคุมการเข้าถึง (Access Control) ข้อ ๖.๒.๔ โดยหน่วยงานควรจะพิจารณาตรวจสอบตัวตนของผู้ใช้งานโดยใช้ปัจจัยที่แตกต่างกันมากกว่าหนึ่งปัจจัย และอาจจะพิจารณาตัวอย่างการใช้งาน MFA ให้เป็นไปตามรายละเอียดข้อเสนอแนะและคำอธิบายเพิ่มเติมของมาตรฐานฉบับนี้ (หัวข้อ ๖.๒.๕)	☐ ยังต้องปรับปรุง ☐ ดำเนินการแล้ว	

ที่	ข้อกำหนด	ข้อเสนอแนะ	การประเมิน	หลักฐาน
๘.๖	หน่วยงานจะต้องตั้งค่าเพื่อความมั่นคงปลอดภัยพื้นฐานของโปรแกรมสำหรับให้บริการเว็บ (Web Server Software) โปรแกรมประยุกต์บนเว็บ (Web Application) ระบบบริหารจัดการเว็บไซต์ (CMS) ระบบปฏิบัติการ (Operating System) และการตั้งค่าฐานข้อมูล (หัวข้อ ๖.๒.๖)		☐ ยังต้องปรับปรุง ☐ ดำเนินการแล้ว	
		หน่วยงานควรจะมีการตั้งค่าเพื่อความมั่นคงปลอดภัยพื้นฐานของโปรแกรมสำหรับให้บริการเว็บ (Web Server Software) โดยอาจจะพิจารณาการตั้งค่าเพื่อความมั่นคงปลอดภัยพื้นฐานตาม CIS Benchmark ให้เป็นไปตามข้อเสนอแนะและคำอธิบายเพิ่มเติมของมาตรฐานฉบับนี้	☐ ดำเนินการแล้ว ☐ อยู่ในระหว่างดำเนินการ ☐ ยังไม่ได้ดำเนินการ	
		หน่วยงานควรจะพิจารณาให้มีการตั้งค่าเพื่อความมั่นคงปลอดภัยพื้นฐานของโปรแกรมประยุกต์บนเว็บ (Web Application) ตามหัวข้อที่ ๔ ของเอกสารข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ว่าด้วยมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับโปรแกรมประยุกต์บนเว็บ โดยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ โดยอาจจะพิจารณาใช้รายการตรวจสอบ Web Application ของโครงการ OWASP ซึ่งมีรายละเอียดตามข้อเสนอแนะและคำอธิบายเพิ่มเติมของมาตรฐานฉบับนี้	☐ ดำเนินการแล้ว ☐ อยู่ในระหว่างดำเนินการ ☐ ยังไม่ได้ดำเนินการ	
		หน่วยงานควรจะพิจารณาหลักการที่สำคัญที่ต้องตั้งค่าระบบ CMS ให้เป็นไปตามข้อเสนอแนะและคำอธิบายเพิ่มเติมของมาตรฐานฉบับนี้	☐ ดำเนินการแล้ว ☐ อยู่ในระหว่างดำเนินการ ☐ ยังไม่ได้ดำเนินการ	
		หน่วยงานควรจะพิจารณาการตั้งค่าเพื่อเพิ่มความมั่นคงปลอดภัยของระบบปฏิบัติการเบื้องต้นตาม NIST SP 800-123 ซึ่งนำไปประยุกต์ใช้กับระบบปฏิบัติการทุกประเภท	☐ ดำเนินการแล้ว ☐ อยู่ในระหว่างดำเนินการ ☐ ยังไม่ได้ดำเนินการ	

ที่	ข้อกำหนด	ข้อเสนอแนะ	การประเมิน	หลักฐาน
		หน่วยงานควรจะพิจารณารายละเอียดในการตั้งค่าฐานข้อมูลเพื่อให้มีความมั่นคงปลอดภัย ให้เป็นไปตามข้อเสนอแนะและคำอธิบายเพิ่มเติมของมาตรฐานฉบับนี้	☐ ดำเนินการแล้ว ☐ อยู่ในระหว่างดำเนินการ ☐ ยังไม่ได้ดำเนินการ	
๘.๗	หน่วยงานจะต้องกำหนดแนวทางและการเลือกบริการที่เกี่ยวข้องกับเว็บไซต์ ประกอบด้วย เครื่องบริการเว็บ (Web Server) ระบบบริหารจัดการเว็บไซต์ (CMS) เลือกบริการโดเมนและชื่อโดเมน และขั้นตอนวิธีการเข้ารหัส Cipher Suite ของ TLS Certificate (หัวข้อ ๖.๒.๗)		☐ ยังต้องปรับปรุง ☐ ดำเนินการแล้ว	
		หน่วยงานจะต้องกำหนดแนวทางและการเลือกบริการเครื่องบริการเว็บ โดยอาจจะพิจารณาแนวทางและการเลือกบริการ ซึ่งมีรายละเอียดตามข้อเสนอแนะและคำอธิบายเพิ่มเติมของมาตรฐานฉบับนี้	☐ ดำเนินการแล้ว ☐ อยู่ในระหว่างดำเนินการ ☐ ยังไม่ได้ดำเนินการ	
		หน่วยงานจะต้องกำหนดแนวทางและการเลือก CMS ที่มีความมั่นคงปลอดภัย โดยอาจจะพิจารณาแนวทางและการเลือก CMS ซึ่งมีรายละเอียดตามข้อเสนอแนะและคำอธิบายเพิ่มเติมของมาตรฐานฉบับนี้	☐ ดำเนินการแล้ว ☐ อยู่ในระหว่างดำเนินการ ☐ ยังไม่ได้ดำเนินการ	
		หน่วยงานจะต้องกำหนดแนวทางและการเลือกผู้รับจดทะเบียนชื่อโดเมน โดยอาจจะพิจารณาแนวทางและการเลือก ซึ่งรายละเอียดตามข้อเสนอแนะและคำอธิบายเพิ่มเติมของมาตรฐานฉบับนี้	☐ ดำเนินการแล้ว ☐ อยู่ในระหว่างดำเนินการ ☐ ยังไม่ได้ดำเนินการ	
		หน่วยงานจะต้องกำหนดแนวทางและการเลือกขั้นตอนวิธีการเข้ารหัส Cipher Suite ของ TLS Certificate โดยอาจจะพิจารณาแนวทางและการเลือก รวมถึงรายละเอียดในการเลือกระดับการรับรอง ซึ่งรายละเอียดตามข้อเสนอแนะและคำอธิบายเพิ่มเติมของมาตรฐานฉบับนี้	☐ ดำเนินการแล้ว ☐ อยู่ในระหว่างดำเนินการ ☐ ยังไม่ได้ดำเนินการ	
๘.๘	หน่วยงานจะต้องตั้งค่าไฟร์วอลล์เพื่อควบคุมและป้องกันการบุกรุกต่าง ๆ ที่เกิดขึ้นกับเว็บไซต์ โดยควรจะพิจารณาหลักการตั้งค่าอย่างน้อย ดังนี้ การกำหนดนโยบายความมั่นคงปลอดภัย (Define Security Policies) การตั้งค่ากฎการกรอง (Configure Filtering Rules) การจำกัด		☐ ยังต้องปรับปรุง ☐ ดำเนินการแล้ว	

ที่	ข้อกำหนด	ข้อเสนอแนะ	การประเมิน	หลักฐาน
	การเข้าถึงโดยภูมิศาสตร์ (Geographic Restrictions) การป้องกันการโจมตี (Protect Against Attacks) การตรวจสอบและบันทึก (Monitoring and Logging) และการปรับปรุงและอัปเดตเป็นประจำ (Regular Updates) โดยอาจจะพิจารณาหลักการตั้งค่าไฟร์วอลล์ให้เป็นไปตามข้อเสนอแนะและคำอธิบายเพิ่มเติมของมาตรฐานฉบับนี้ (หัวข้อ ๖.๒.๘)			
๙	**มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์สำหรับเว็บไซต์ (Website Security Detection) (หัวข้อ ๖.๓)**			
๙.๑	หน่วยงานจะต้องมีการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring) ให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (หัวข้อ ๖.๓.๑)		☐ ยังต้องปรับปรุง ☐ ดำเนินการแล้ว	
		หน่วยงานจะต้องมีการสร้างกลไกและกระบวนการ เพื่อตรวจจับ จัดประเภท วิเคราะห์ และระบุว่ามีภัยคุกคามหรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องเว็บไซต์ให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	☐ ดำเนินการแล้ว ☐ อยู่ในระหว่างดำเนินการ ☐ ยังไม่ได้ดำเนินการ	
		หน่วยงานจะต้องมีการทบทวนกลไกและกระบวนการอย่างน้อย ปีละ ๑ (หนึ่ง) ครั้ง ตามความเหมาะสม ให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	☐ ดำเนินการแล้ว ☐ อยู่ในระหว่างดำเนินการ ☐ ยังไม่ได้ดำเนินการ	
๑๐	**การเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์สำหรับเว็บไซต์ (Website Incident Response) (หัวข้อ ๖.๔)**			
๑๐.๑	หน่วยงานจะต้องจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์สำหรับเว็บไซต์ (Website Security Incident Response Plan) ให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ มีการสื่อสาร ฝึกซ้อม ทบทวน และปรับปรุง แผนการรับมือภัยคุกคามทางไซเบอร์ของเว็บไซต์ รวมถึงแผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan) และการฝึกซ้อมความมั่นคงปลอดภัย ไซเบอร์สำหรับเว็บไซต์ (Website		☐ ยังต้องปรับปรุง ☐ ดำเนินการแล้ว	

ที่	ข้อกำหนด	ข้อเสนอแนะ	การประเมิน	หลักฐาน
	Security Exercise) ให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (หัวข้อ ๖.๔.๑)			
		หน่วยงานจะต้องจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์สำหรับเว็บไซต์ (Website security Incident Response Plan) ให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยอาจจะพิจารณาคำแนะนำและข้อควรพิจารณาในการตอบสนองต่อเหตุการณ์สำหรับการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์ของ NIST ตามข้อเสนอแนะและคำอธิบายเพิ่มเติมของมาตรฐานฉบับนี้	☐ ดำเนินการแล้ว ☐ อยู่ในระหว่างดำเนินการ ☐ ยังไม่ได้ดำเนินการ	
		หน่วยงานจะต้องมีการสื่อสาร ทบทวน และปรับปรุง แผนการรับมือภัยคุกคามทางไซเบอร์ของเว็บไซต์ และมีการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์สำหรับเว็บไซต์ (Website Security Exercise) โดยพิจารณาฝึกซ้อมอย่างน้อยปีละ ๑ ครั้ง ให้เป็นไปตามความเหมาะสม ให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	☐ ดำเนินการแล้ว ☐ อยู่ในระหว่างดำเนินการ ☐ ยังไม่ได้ดำเนินการ	
		หน่วยงานจะต้องมีการจัดทำแผนการสื่อสารในภาวะวิกฤตเพื่อตอบสนองต่อวิกฤตที่เกิดจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์สำหรับเว็บไซต์ ให้เป็นไปตามความเหมาะสม ให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยหน่วยงานอาจจะพิจารณาระบุรายละเอียด ให้เป็นไปตามข้อเสนอแนะและคำอธิบายเพิ่มเติมของมาตรฐานฉบับนี้	☐ ดำเนินการแล้ว ☐ อยู่ในระหว่างดำเนินการ ☐ ยังไม่ได้ดำเนินการ	
		หน่วยงานจะต้องมีส่วนร่วมในการฝึกซ้อมรับมือกับภัยคุกคามทางไซเบอร์สำหรับเว็บไซต์ทั้งในระดับชาติหรือระดับภาคส่วน เช่น ฝึกซ้อมกับ สกมช. หรือหน่วยงานควบคุม	☐ ดำเนินการแล้ว ☐ อยู่ในระหว่างดำเนินการ ☐ ยังไม่ได้ดำเนินการ	

ที่	ข้อกำหนด	ข้อเสนอแนะ	การประเมิน	หลักฐาน
		หรือกำกับดูแล รวมถึงตรวจสอบให้แน่ใจว่าบุคลากรที่เกี่ยวข้องที่ระบุไว้ในแผนการรับมือภัยคุกคามทางไซเบอร์สำหรับเว็บไซต์ มีส่วนร่วมในการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ให้เป็นไปตามความเหมาะสม ให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์		
๑๑	**การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์สำหรับเว็บไซต์ (Website Recovery) (หัวข้อ ๖.๕)**			
๑๑.๑	หน่วยงานจะต้องมีการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์สำหรับเว็บไซต์ (Website Security Resilience and Recovery) โดยจะต้องจัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP) และจะต้องจัดให้มีการฝึกซ้อมให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (หัวข้อ ๖.๕.๑)	☐ ยังต้องปรับปรุง ☐ ดำเนินการแล้ว	
		หน่วยงานจะต้องมีจัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP) ให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยอาจจะพิจารณาให้มีรายละเอียดของแผนตามการบริหารความพร้อมต่อสภาวะวิกฤติ (การทำแผน BCP) ของสำนักงานคณะกรรมการพัฒนาระบบราชการ	☐ ดำเนินการแล้ว ☐ อยู่ในระหว่างดำเนินการ ☐ ยังไม่ได้ดำเนินการ	
		หน่วยงานจะต้องมีการฝึกซ้อม BCP อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง หรืออาจจะพิจารณาตามความเหมาะสมตามสภาพของหน่วยงาน ให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	☐ ดำเนินการแล้ว ☐ อยู่ในระหว่างดำเนินการ ☐ ยังไม่ได้ดำเนินการ	

แบบฟอร์ม ค๒ แบบรายงานรายการที่ยังต้องปรับปรุง

สำหรับหน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานของรัฐ และหน่วยงานเอกชน

<u>คำแนะนำ</u> เมื่อหน่วยงานพบรายการที่ไม่เป็นไปตามข้อกำหนด ที่มีสถานะ “ยังต้องปรับปรุง” ตามผลการประเมินตามแบบฟอร์ม ค๑ ให้ระบุรายการที่ยังต้องปรับปรุงลงในแบบฟอร์มนี้

วันที่ประเมินตนเอง (Self-Assessment).....หน่วยงานเจ้าของเว็บไซต์.....

ชื่อเว็บไซต์.....การเข้าถึงเว็บไซต์ หรือ URL.....

ลำดับ	ข้อกำหนดที่ยังต้องปรับปรุง	สาเหตุ	การปรับปรุงแก้ไขในเบื้องต้น	สิ่งที่ต้องการปรับปรุงแก้ไข		
				รายการแก้ไข	ผู้รับผิดชอบดำเนินการ	กำหนดวันที่แล้วเสร็จ

ผู้กรอกแบบรายงาน.....ตำแหน่ง.....

สังกัดหน่วยงาน (ภายใน).....เบอร์โทร.....อีเมล.....

บรรณานุกรม

๑. Mark Curphey JS, Erik Olson Improving Web Application Security: Threats and Countermeasures. Microsoft.

๒. National Institute of Standards and Technology. The NIST Cybersecurity Framework (CSF) 2.0 2024 [updated 26/02/2024: [Available from: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf.

๓. คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์. ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ.

๔. สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ. สถิติภัยคุกคามทางไซเบอร์ ๒๕๖๖ [Available from: https://www.ncsa.or.th/service-statistics.html.

๕. คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ. พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ ๒๕๖๒ [Available from: https://www.ratchakitcha.soc.go.th/DATA/PDF/2562/A/069/T_0020.PDF.

๖. วิไลลักษณ์ ก. คอมพิวเตอร์เบื้องต้น (ฉบับปรับปรุงครั้งที่ ๒). กรุงเทพฯ: มหาวิทยาลัยสุโขทัยธรรมาธิราช; ๒๕๖๖.

๗. สมาคมผู้ดูแลเว็บและสื่อออนไลน์ไทย. เว็บไซต์ (Website) คืออะไร? date unknown [Available from: https://www.webmaster.or.th/website.

๘. Cambridge University Press & Assessment. Cambridge English Dictionary date unknown [Available from: https://dictionary.cambridge.org/dictionary/english/.

๙. สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์. Website D.I.Y. ๒๕๖๗. Available from: https://www.etda.or.th/th/Useful-Resource/documents-for-download/Website-D-I-Y.aspx.

๑๐. Amazon Web Services I. What is Cloud Hosting? [Available from: https://aws.amazon.com/what-is/cloud-hosting/.

๑๑. National Institute of Standards and Technology. Web Server date unknown [Available from: https://csrc.nist.gov/glossary/term/web_server.

๑๒. Sciencedirect. Web Server Software 2016 [Available from: https://www.sciencedirect.com/topics/computer-science/web-server-software.

๑๓. National Institute of Standards and Technology. NIST Special Publication 800-152 A Profile for U.S. Federal Cryptographic Key Management Systems. 2015.

๑๔. National Institute of Standards and Technology. Secure Sockets Layer (SSL) date unknown [Available from: https://csrc.nist.gov/glossary/term/secure_sockets_layer.

๑๕. National Institute of Standards and Technology. NIST Special Publication 1800-15 Securing Small-Business and Home Internet of Things (IoT) Devices: Mitigating Network-Based Attacks Using Manufacturer Usage Description (MUD). 2021.

๑๖. Raghu Ramakrishnan JG. Database management systems. Boston: Mcgraw-Hill; 2003.

๑๗. National Institute of Standards and Technology. NIST Special Publication 1800-16 Securing Web Transactions: TLS Server Certificate Management. 2020.

๑๘. Kaufman DECW. Domain Name System Security Extensions 1997 [Available from: https://datatracker.ietf.org/doc/html/rfc2065.

๑๙. merriam-webster. fire wall 2024 [Available from: https://www.merriam-webster.com/dictionary/firewall.

๒๐. OWASP. Web Application Firewall 2024 [Available from: https://owasp.org/www-community/Web_Application_Firewall.

๒๑. Gartner. Endpoint Detection and Response (EDR) Solutions Reviews 2020 [Available from: https://www.gartner.com/reviews/market/endpoint-detection-and-response-solutions.

๒๒. Gartner Research. Innovation Insight for Extended Detection and Response 2020 [updated 19 March 2020. Available from: https://www.gartner.com/en/documents/3982247.

๒๓. ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ. ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ. ๒๕๖๖.

๒๔. คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ. ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานขั้นต่ำของข้อมูลหรือระบบสารสนเทศ ๒๕๖๖ [Available from: https://www.ncsa.or.th/.

๒๕. คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ. ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์. ๒๕๖๗.

๒๖. สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ. คำแนะนำของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง แนวปฏิบัติการรักษาความมั่นคงปลอดภัยเว็บไซต์ (Website Security Guideline) สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ. ๒๕๖๖.

๒๗. สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์. ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับโปรแกรมประยุกต์บนเว็บ. ๒๕๖๐.

๒๘. สำนักงานพัฒนารัฐบาลดิจิทัล. มาตรฐานเว็บไซต์ภาครัฐ (Government Website Standard Version 3.0) ๒๕๕๖.

๒๙. คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย. ๒๕๕๕.

๓๐. สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช). คำแนะนำ สกมช. เรื่อง แนวทางปฏิบัติในการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ๒๕๖๖.

๓๑. National Institute of Standards and Technology. NIST SP 800-88 Rev. 1 Guidelines for Media Sanitization 2014 [Available from: https://csrc.nist.gov/pubs/sp/800/88/r1/final.

๓๒. OWASP. Welcome to the OWASP Top 10 2021 [Available from: https://owasp.org/Top10/.

๓๓. สำนักงานคณะกรรมการพัฒนาระบบราชการ. การบริหารความพร้อมต่อสภาวะวิกฤติ (การทำแผน BCP) ๒๕๖๓ [Available from: https://www.opdc.go.th/content/NjE3Mg.

๓๔. สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ. นโยบายการรักษาความมั่นคงปลอดภัยเว็บไซต์ ๒๕๖๘ [Available from: https://www.ncsa.or.th/policy/WebsiteSecurityPolicy.

๓๕. สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน). นโยบายและคู่มือบริหารความเสี่ยง (Enterprise Risk Management Manual) ๒๕๖๔ Available from: https://www.dga.or.th

๓๖. บริษัท ปตท. จำกัด (มหาชน). มาตรการตรวจสอบการใช้ดุลยพินิจ ๒๕๖๕ [Available from: https://www.pttplc.com/.

๓๗. Ho A. Roles of Three Lines of Defense for Information Security and Governance 2018 [Available from: https://www.isaca.org/resources/isaca-journal/issues/2018/volume-4/roles-of-three-lines-of-defense-for-information-security-and-governance.

๓๘. สำนักงานเลขาธิการคณะรัฐมนตรี. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล. ๒๕๖๒ [Available from: https://www.ratchakitcha.soc.go.th/DATA/PDF/2562/A/069/T_0052.PDF.

๓๙. กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม. ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ ๒๕๖๔ [Available from: https://www.ratchakitcha.soc.go.th/DATA/PDF/2564/E/188/T_0009.PDF.

๔๐. National Institute of Standards and Technology (NIST). FIPS PUB 200 Minimum Security Requirements for Federal Information and Information Systems 2006 [Available from: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf

๔๑. U.S. Department of Homeland Security. CVE Program 1999 [Available from: https://cve.mitre.org/.

๔๒. Abbasi S. 2023 Threat Landscape Year in Review: If Everything Is Critical, Nothing Is 2023 [Available from: https://blog.qualys.com/vulnerabilities-threat-research/2023/12/19/2023-threat-landscape-year-in-review-part-one.

๔๓. OWASP. Matrix DSOMM. 2024. [Available from: https://dsomm.owasp.org/

๔๔. National Institute of Standards and Technology. NIST Special Publication 800-63B Digital Identity Guidelines Authentication and Lifecycle Management 2024 [Available from: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-63b.pdf.

๔๕. Center for Internet Security. CIS Password Policy Guide 2021 [Available from: https://www.cisecurity.org/insights/white-papers/cis-password-policy-guide.

๔๖. NIST. NIST SP 800-123 Guide to General Server Security 2008 [Available from: https://csrc.nist.gov/pubs/sp/800/123/final.

๔๗. Defense Information Systems Agency (DISA). STIGs Document Library 2025 [Available from: https://public.cyber.mil/stigs/downloads/.

๔๘. Center for Internet Security. CIS Benchmarks List 2025 [Available from: https://www.cisecurity.org/cis-benchmarks.

๔๙. OWASP. Web Application Checklist 2025 [Available from: https://owasp.org/www-project-developer-guide/draft/06-design/02-web-app-checklist/00-toc#checklist-define-security-requirements.

๕๐. Byers K. Domain Extensions: .com vs .org, .net, .io & 4 Other TLDs 2022 [updated 30/1/2022. Available from: https://growthbadger.com/top-level-domains/.

๕๑. National Institute of Standards and Technology (NIST). Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile 2024 [Available from: https://csrc.nist.gov/pubs/sp/800/61/r3/final.

ฉบับภาษาอังกฤษ
English Version

อยู่ระหว่างดำเนินการแปลเอกสารเป็นฉบับภาษาอังกฤษ

The translation of the document into English is underway.

19 อภิธานศัพท์
Glossary

ชื่อหน่วยงาน

Name of the Organization

คำภาษาไทย Thai words	**คำภาษาอังกฤษ** English words	**คำอ่าน** Pronunciation
กรมการขนส่งทางราง	Department of Rail Transport	dɪˈpɑrtmənt ʌv reɪl ˈtrænspɔr
กรมการปกครอง	Department of Provincial Administration	dɪˈpɑrtmənt ʌv prəˈvɪnʃəl ædˌmɪnɪˈstreɪʃən
กรมชลประทาน	Royal Irrigation Department	ˈrɔɪəl ˌɪrəˈgeɪʃən dɪˈpɑrtmənt
กรมศุลกากร	Thai Customs	taɪ ˈkʌstəmz
กระทรวงการคลัง	Ministry of Finance	ˈmɪnəstri ʌv fəˈnæns
กระทรวงพลังงาน	Ministry of Energy	ˈmɪnəstri ʌv ˈɛnərʤi
การประปาส่วนภูมิภาค (เฉพาะบริการส่วนภูมิภาค)	Provincial Waterworks Authority (Provincial services only)	prəˈvɪnʃəl ˈwɔtərˌwɜrks əˈθɔrəti (prəˈvɪnʃəl ˈsɜrvəsəz ˈoʊnli)
ทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์	Cyber Incident Response Team (CIRT)	ˈsaɪbər ˈɪnsədənt rɪˈspɑns tim (si-aɪ-ɑr-ti)
ธนาคารแห่งประเทศไทย	Bank of Thailand	bæŋk ʌv ˈtaɪˌlænd
ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ	Computer Emergency Response Team (CERT) for Organizations of Critical Information Infrastructure	kəmˈpjutər ɪˈmɜrʤənsi rɪˈspɑns tim (si-i-ɑr-ti) fɔr ˌɔrgənəˈzeɪʃənz ʌv ˈkrɪtɪkəl ˌɪnfərˈmeɪʃən ˌɪnfrəˈstrʌktʃər
ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ	Thailand Computer Emergency Response Team (ThaiCERT)	ˈtaɪˌlænd kəmˈpjutər ɪˈmɜrʤənsi rɪˈspɑns tim (ˈtī /sɜːt/)
สำนักงานการบินพลเรือนแห่งประเทศไทย	The Civil Aviation Authority of Thailand	ðə ˈsɪvəl ˌeɪviˈeɪʃən əˈθɔrəti ʌv ˈtaɪˌlænd
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ	National Cyber Security Agency (NCSA)	ˈnæʃənəl ˈsaɪbər sɪˈkjʊrəti ˈeɪʤənsi (ɛn-si-ɛs-eɪ)

คำภาษาไทย Thai words	**คำภาษาอังกฤษ** English words	**คำอ่าน** Pronunciation
สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์	The Securities and Exchange Commission	ðə sɪˈkjʊrətiz ænd ɪksˈtʃeɪndʒ kəˈmɪʃən
สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ	Office of The National Broadcasting and Telecommunications Commission	ˈɔfəs ʌv ðə ˈnæʃənəl ˈbrɔdˌkæstɪŋ ænd ˌtɛləkəmˌjunəˈkeɪʃənz kəˈmɪʃən
สำนักงานตำรวจแห่งชาติ	Royal Thai Police	ˈrɔɪəl taɪ pəˈlis
สำนักงานปลัดกระทรวงกลาโหม	Office of the Permanent Secretary for Defense	ˈɔfəs ʌv ðə ˈpɜrmənənt ˈsɛkrəˌtɛri fɔr dɪˈfɛns
สำนักงานปลัดกระทรวงคมนาคม	Office of the Permanent Secretary of the Ministry of Transport	ˈɔfəs ʌv ðə ˈpɜrmənənt ˈsɛkrəˌtɛri ʌv ðə ˈmɪnəstri ʌv ˈtrænspɔrt
สำนักงานปลัดกระทรวงสาธารณสุข	Office of the Permanent Secretary of the Ministry of Public Health	ˈɔfəs ʌv ðə ˈpɜrmənənt ˈsɛkrəˌtɛri ʌv ðə ˈmɪnəstri ʌv ˈpʌblɪk ˈhɛlθ
สำนักงานคณะกรรมการอาหารและยา	Food and Drug Administration	fud ænd drʌg ædˌmɪnɪˈstreɪʃən
สำนักงานปรมาณูเพื่อสันติ	Office of Atomic Energy for Peace	ˈɔfəs ʌv əˈtɑmɪk ˈɛnərdʒi fɔr piːs
สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)	Digital Government Development Agency (Public Organization)	ˈdɪdʒətəl ˈgʌvərmənt dɪˈvɛləpmənt ˈeɪdʒənsi (ˈpʌblɪk ˌɔrgənəˈzeɪʃən)
สำนักงานสภาความมั่นคงแห่งชาติ	Office of the National Security Council	ˈɔfəs ʌv ðə ˈnæʃənəl sɪˈkjʊrəti ˈkaʊnsəl
หน่วยงาน	agency	ˈeɪdʒənsi
หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ	Organization of Critical Information Infrastructure	ˌɔrgənəˈzeɪʃən ʌv ˈkrɪtɪkəl ˌɪnfərˈmeɪʃən ˌɪnfrəˈstrʌktʃər

ชื่อคณะกรรมการและตำแหน่ง

Names of the Committee and Positions

คำภาษาไทย Thai words	**คำภาษาอังกฤษ** English words	**คำอ่าน** Pronunciation
คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.)	National Cyber Security Committee (NCSC)	ˈnæʃənəl ˈsaɪbər sɪˈkjʊrəti kəˈmɪti (ɛn-si-ɛs-si)
คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.)	Cybersecurity Regulating Committee (CRC)	ˈsaɪbərsɪˈkjʊrəti ˈrɛgjəˌleɪtɪŋ kəˈmɪti (si-ɑr-si)
คณะกรรมการบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ (กบส)	Committee Managing the National Cyber Security Agency (CMSA)	kəˈmɪti ˈmænəʤɪŋ ði ˈɔfəs ʌv ðə ˈnæʃənəl ˈsaɪbərsɪˈkjʊrəti kəˈmɪti (si-ɛm-oʊ)
คณะกรรมการรับมือกับภัยคุกคามทางไซเบอร์ในระดับร้ายแรง (ครร.)	Critical Incident Response Committee (CIRC)	ˈkrɪtɪkəl ˈɪnsədənt rɪˈspɑns kəˈmɪti (si-aɪ-ɑr-si)
ประธานกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ	Chairman of the National Cyber Security Committee	ˈʧɛrmən ʌv ðə ˈnæʃənəl ˈsaɪbər sɪˈkjʊrəti kəˈmɪti
ประธานกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์	Chairperson of the Cybersecurity Regulating Committee	ˈʧɛrˌpɜrsən ʌv ðə ˈsaɪbərsɪˈkjʊrəti ˈrɛgjəˌleɪtɪŋ kəˈmɪti
พนักงานเจ้าหน้าที่	Competent Official	ˈkɑmpətɪnt əˈfɪʃəl
เลขาธิการ	Secretary-General	ˈsɛkrəˌtɛri-ˈʤɛnərəl
เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ	Secretary-General of the National Cybersecurity Committee	ˈsɛkrəˌtɛri-ˈʤɛnərəl ʌv ðə ˈnæʃənəl ˈsaɪbərsɪˈkjʊrəti kəˈmɪti
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ	National Cyber Security Agency (NCSA)	ˈnæʃənəl ˈsaɪbər sɪˈkjʊrəti ˈeɪʤənsi (ɛn-si-ɛs-eɪ)

ชื่อด้านของโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

Names of the Sectors of Critical Information Infrastructure

คำภาษาไทย Thai words	**คำภาษาอังกฤษ** English words	**คำอ่าน** Pronunciation
ด้านความมั่นคงของรัฐ	National Security Sector	ˈnæʃənəl sɪˈkjʊrəti ˈsɛktər
ด้านบริการภาครัฐที่สำคัญ	Critical Government Service Sector	ˈkrɪtɪkəl ˈgʌvərmənt ˈsɜrvəs ˈsɛktər
ด้านการเงินการธนาคาร	Banking and Financial Sector	ˈbæŋkɪŋ ænd fəˈnænʃəl ˈsɛktər
ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม	Information Technology and Telecommunication Sector	ˌɪnfərˈmeɪʃən tɛkˈnɑlədʒi ænd ˌtɛləkəmˌjunɪˈkeɪʃən ˈsɛktər
ด้านการขนส่งและโลจิสติกส์	Transportation and Logistics Sector	ˌtrænspərˈteɪʃən ænd ləˈdʒɪstɪks ˈsɛktər
ด้านพลังงานและสาธารณูปโภค	Energy and Public Utilities Sector	ˈɛnərdʒi ænd ˈpʌblɪk juˈtɪlətiz ˈsɛktər
ด้านสาธารณสุข	Public Health Sector	ˈpʌblɪk hɛlθ ˈsɛktər
ที่มีภารกิจเกี่ยวข้องกับการป้องกันประเทศ	Perform missions related to national defense	pərˈfɔrm ˈmɪʃənz rɪˈleɪtɪd tu ˈnæʃənəl dɪˈfɛns
ที่มีภารกิจเกี่ยวข้องกับการบังคับใช้กฎหมาย	Perform missions concerning law enforcement	pərˈfɔrm ˈmɪʃənz kənˈsɜrnɪŋ lɔ ɛnˈfɔrsmənt
ที่มีภารกิจเกี่ยวข้องกับความมั่นคงอื่น ๆ	Perform missions in other securities	pərˈfɔrm ˈmɪʃənz ɪn ˈʌðər sɪˈkjʊrətiz
ที่มีบริการด้านการเงิน	Provide financial services	prəˈvaɪd fəˈnænʃəl ˈsɜrvəsəz
ที่มีการให้บริการโดยตรงแก่ประชาชน	Provide services directly to the public	prəˈvaɪd ˈsɜrvəsəz dəˈrɛktli tu ðə ˈpʌblɪk
ที่มีการให้บริการที่เกี่ยวข้องกับการแจ้งเตือน	Provide services related to alerting	prəˈvaɪd ˈsɜrvəsəz rɪˈleɪtɪd tu əˈlɜrtɪŋ
ที่มีการให้บริการทางการเงิน	Provide financial services	prəˈvaɪd fəˈnænʃəl ˈsɜrvəsəz
ที่มีการให้บริการที่เกี่ยวข้องกับตลาดทุน	Provide services related to capital market	prəˈvaɪd ˈsɜrvəsəz rɪˈleɪtɪd tu ˈkæpətəl ˈmɑrkət
ที่มีการให้บริการโทรคมนาคม	Provide telecommunication services	prəˈvaɪd ˌtɛləkəmˌjunɪˈkeɪʃən ˈsɜrvəsəz
ที่มีการให้บริการขนส่งทางราง	Provide rail transport services	prəˈvaɪd reɪl ˈtrænspɔrt ˈsɜrvəsəz
ที่มีการให้บริการขนส่งทางน้ำ	Provide water transportation services	prəˈvaɪd ˈwɔtər ˌtrænspərˈteɪʃən ˈsɜrvəsəz
ที่มีการให้บริการขนส่งทางอากาศ	Provide air transportation services	prəˈvaɪd ɛr ˌtrænspərˈteɪʃən ˈsɜrvəsəz
ที่มีการให้บริการด้านไฟฟ้า	Provide electricity services	prəˈvaɪd ɪˌlɛkˈtrɪsəti ˈsɜrvəsəz
ที่มีการให้บริการด้านปิโตรเลียมและก๊าซ	Provide services related to petroleum and gas	prəˈvaɪd ˈsɜrvəsəz rɪˈleɪtɪd tu pəˈtroʊliəm ænd gæs

ชื่อลักษณะหน่วยงาน

Name of the Organization's Characteristics

คำภาษาไทย Thai words	คำภาษาอังกฤษ English words	คำอ่าน Pronunciation
ที่มีภารกิจเกี่ยวข้องกับการป้องกันประเทศ	Perform missions related to national defense	pərˈfɔrm ˈmɪʃənz rɪˈleɪtɪd tu ˈnæʃənəl dɪˈfɛns
ที่มีภารกิจเกี่ยวข้องกับการบังคับใช้กฎหมาย	Perform missions concerning law enforcement	pərˈfɔrm ˈmɪʃənz kənˈsɜrnɪŋ lɔ ɛnˈfɔrsmənt
ที่มีภารกิจเกี่ยวข้องกับความมั่นคงอื่น ๆ	Perform missions in other securities	pərˈfɔrm ˈmɪʃənz ɪn ˈʌðər sɪˈkjʊrətiz
ที่มีบริการด้านการเงิน	Provide financial services	prəˈvaɪd fəˈnænʃəl ˈsɜrvəsəz
ที่มีการให้บริการโดยตรงแก่ประชาชน	Provide services directly to the public	prəˈvaɪd ˈsɜrvəsəz dəˈrɛktli tu ðə ˈpʌblɪk
ที่มีการให้บริการที่เกี่ยวข้องกับการแจ้งเตือน	Provide services related to alerting	prəˈvaɪd ˈsɜrvəsəz rɪˈleɪtɪd tu əˈlɜrtɪŋ
ที่มีการให้บริการทางการเงิน	Provide financial services	prəˈvaɪd fəˈnænʃəl ˈsɜrvəsəz
ที่มีการให้บริการที่เกี่ยวข้องกับตลาดทุน	Provide services related to capital market	prəˈvaɪd ˈsɜrvəsəz rɪˈleɪtɪd tu ˈkæpətəl ˈmɑrkət
ที่มีการให้บริการโทรคมนาคม	Provide telecommunication services	prəˈvaɪd ˌtɛləkəmˌjunɪˈkeɪʃən ˈsɜrvəsəz
ที่มีการให้บริการขนส่งทางบก	Provide land transportation services	prəˈvaɪd lænd ˌtrænspərˈteɪʃən ˈsɜrvəsəz
ที่มีการให้บริการขนส่งทางราง	Provide rail transport services	prəˈvaɪd reɪl ˈtrænspɔrt ˈsɜrvəsəz
ที่มีการให้บริการขนส่งทางน้ำ	Provide water transportation services	prəˈvaɪd ˈwɔtər ˌtrænspərˈteɪʃən ˈsɜrvəsəz
ที่มีการให้บริการขนส่งทางอากาศ	Provide air transportation services	prəˈvaɪd ɛr ˌtrænspərˈteɪʃən ˈsɜrvəsəz
ที่มีการให้บริการด้านไฟฟ้า	Provide electricity services	prəˈvaɪd ɪˌlɛkˈtrɪsəti ˈsɜrvəsəz
ที่มีการให้บริการด้านปิโตรเลียมและก๊าซ	Provide services related to petroleum and gas	prəˈvaɪd ˈsɜrvəsəz rɪˈleɪtɪd tu pəˈtroʊliəm ænd gæs
ที่มีการให้บริการด้านประปา	Provide water services	prəˈvaɪd ˈwɔtər ˈsɜrvəsəz
ที่มีการให้บริการสุขภาพในโรงพยาบาล	Provide healthcare services in hospitals	prəˈvaɪd ˈhɛlθˌkɛr ˈsɜrvəsəz ɪn ˈhɑˌspɪtəlz

คำภาษาไทย Thai words	**คำภาษาอังกฤษ** English words	**คำอ่าน** Pronunciation
ที่มีการให้บริการสุขภาพระหว่างโรงพยาบาล	Provide health services between hospitals	prəˈvaɪd hɛlθ ˈsɜrvəsəz bɪˈtwin ˈhɑˌspɪtəlz
ที่มีการให้บริการด้านยาเวชภัณฑ์ และเครื่องมือแพทย์	Provide services related to medicines, medical supplies, and medical equipment	prəˈvaɪd ˈsɜrvəsəz rɪˈleɪtɪd tu ˈ mɛdəsənz, ˈmɛdəkəl səˈplaɪz, ænd ˈmɛdəkəl ɪˈkwɪpmənt
ที่มีการให้บริการตรวจวิเคราะห์ทางการแพทย์และรังสีวิทยา	Provide medical analysis and radiology services	prəˈvaɪd ˈmɛdəkəl əˈnæləsəs ænd ˌreɪdiˈɑlədʒi ˈsɜrvəsəz
ที่มีการให้บริการข้อมูลสุขภาพดิจิทัล	Provide digital health data services	prəˈvaɪd ˈdɪdʒətəl hɛlθ ˈdeɪtə ˈs ɜrvəsəz

ชื่อบริการที่สำคัญ

Name of the Critical Services

คำภาษาไทย Thai words	**คำภาษาอังกฤษ** English words	**คำอ่าน** Pronunciation
ภารกิจด้านการพัฒนาศักยภาพการป้องกันประเทศ	Missions in national defense capability development	ˈmɪʃənz ɪn ˈnæʃənəl dɪˈfɛns ˌkeɪp əˈbɪləti dɪˈvɛləpmənt
ภารกิจด้านการบังคับใช้กฎหมายและอำนวยความยุติธรรมทางอาญา	Missions in law enforcement and administration of criminal justice	ˈmɪʃənz ɪn lɔ ɛnˈfɔrsmənt ænd æd ˌmɪnɪˈstreɪʃən ʌv ˈkrɪmənəl ˈʤʌstəs
ภารกิจด้านการเฝ้าระวังและการแจ้งเตือนภัยคุกคามที่กระทบต่อความมั่นคง	Missions related to threat monitoring and alarming that impact the security	ˈmɪʃənz rɪˈleɪtɪd tu θrɛt ˈmɑnətə rɪŋ ænd əˈlɑrmɪŋ ðæt ˈɪmpækt ðə sɪˈkjʊrəti
ภารกิจด้านการป้องกันและแก้ไขปัญหาที่กระทบต่อความมั่นคง	Missions related to preventing mitigate problems that impact the security	ˈmɪʃənz rɪˈleɪtɪd tu prɪˈvɛntɪŋ ˈmɪtəˌgeɪt ˈprɑbləmz ðæt ˈɪmpækt ðə sɪˈkjʊrəti
บริการที่เกี่ยวข้องกับการบริหารการเงินการคลังภาครัฐ (GFMIS)	Services related to management Government Fiscal Management Information System (GFMIS)	ˈsɜrvəsəz rɪˈleɪtɪd tu ˈmænəʤmənt ˈgʌvərmənt ˈfɪskəl ˈmænəʤmənt
บริการที่เกี่ยวข้องกับการเชื่อมโยงข้อมูลหน่วยงานภาครัฐ และภาคธุรกิจสำหรับการนำเข้า - ส่งออกและโลจิสติกส์	Services related to information exchange among government agencies and business sectors in import-export and logistics	ˌɪnfərˈmeɪʃən ˈsɪstəm (ʤi-ɛf-ɛm-aɪ-ɛs)
บริการที่เกี่ยวข้องกับการทะเบียนราษฎร	Services related to civil registration	ˈsɜrvəsəz rɪˈleɪtɪd tu ˌɪnfərˈmeɪʃən ɪksˈʧeɪnʤ əˈmʌŋ ˈgʌvərmənt ˈeɪʤənsiz ænd ˈbɪznəs ˈsɛktərz ɪn ˈɪmpɔrt- ˈɛkspɔrt ænd ləˈʤɪstɪks
บริการที่เกี่ยวข้องกับบัตรประจำตัวประชาชน	Services related to identification cards	ˈsɜrvəsəz rɪˈleɪtɪd tu ˈsɪvəl ˌrɛʤɪˈstreɪʃən
บริการ Linkage Center	Linkage center services	ˈsɜrvəsəz rɪˈleɪtɪd tu ˈfæməli ˌrɛʤɪˈstreɪʃən
บริการที่เกี่ยวข้องกับการพิสูจน์และยืนยันตัวตนทางดิจิทัล	Services related to digital identity verification and authentication	ˈlɪŋkəʤ ˈsɛntər ˈsɜrvəsəz
บริการที่เกี่ยวข้องกับการตรวจสอบคนเข้าเมือง	Services related to immigration inspection	ˈsɜrvəsəz rɪˈleɪtɪd tu ˈdɪʤətəl aɪˈdɛntəti ˌvɛrəfəˈkeɪʃən ænd ɔˌθɛntəˈkeɪʃən

คำภาษาไทย Thai words	**คำภาษาอังกฤษ** English words	**คำอ่าน** Pronunciation
บริการที่เกี่ยวข้องกับการรับแจ้งเหตุฉุกเฉิน	Services related to emergency call handling	ˈsɜrvəsəz rɪˈleɪtɪd tu ˌɪməˈgreɪʃən ɪnˈspɛkʃən
บริการที่เกี่ยวข้องกับการพิสูจน์และยืนยันตัวตนทางดิจิทัล	Services related to digital identity verification and authentication	ˈsɜrvəsəz rɪˈleɪtɪd tu ɪˈmɜrʤənsi kɔl ˈhændlɪŋ
บริการที่เกี่ยวข้องกับการแลกเปลี่ยนข้อมูลกลางภาครัฐ	Services related to government data exchange	ˈsɜrvəsəz rɪˈleɪtɪd tu ˈdɪʤətəl aɪˈdɛntəti ˌvɛrəfəˈkeɪʃən ænd ɔˌθɛntəˈkeɪʃən
บริการที่เกี่ยวข้องกับการคาดการณ์คุณภาพน้ำและการเตือนภัย	Services related to water quality forecasting and warning	ˈsɜrvəsəz rɪˈleɪtɪd tu ˈgʌvərmənt ˈdeɪtə ɪksˈtʃeɪnʤ
บริการที่เกี่ยวข้องกับการชลประทาน	Services related to irrigation	ˈsɜrvəsəz rɪˈleɪtɪd tu ˈwɔtər ˈkwɑləti ˈfɔrˌkæstɪŋ ænd ˈwɔrnɪŋ
บริการที่เกี่ยวข้องกับการแพร่ภาพและกระจายเสียงแบบดิจิทัล	Services related to digital broadcasting	ˈsɜrvəsəz rɪˈleɪtɪd tu ˌɪrəˈgeɪʃən
บริการฝาก-ถอนเงินรายย่อย	Deposit and withdrawal services for retail banking	ˈsɜrvəsəz rɪˈleɪtɪd tu ˈdɪʤətəl ˈbrɔdˌkæstɪŋ
บริการระบบชำระเงินรายใหญ่ระหว่างสถาบันการเงินผ่านระบบบาทเนต (BAHTNET)	Bulk payment system services between financial institutions via Bank of Thailand Automated High-value Transfer Network (BAHTNET)	dəˈpɑzɪt ænd wɪðˈdrɔəl ˈsɜrvəsəz fɔr ˈriˌteɪl ˈbæŋkɪŋ
บริการระบบชำระเงินรายย่อยผ่านระบบพร้อมเพย์ (PromptPay)	Retail payment system services via the PromptPay system (PromptPay)	ˈriˌteɪl ˈpeɪmənt ˈsɪstəm ˈsɜrvəsəz bɪˈtwin fəˈnænʃəl ˌɪnstɪˈtuʃənz ˈvaɪə ˈɪməʤd Cheque ˈklɪrɪŋ ænd ˈɑrˌkaɪv ˈsɪstəm (aɪ-si-eɪ-ɛs)
บริการระบบชำระเงินรายย่อยผ่านระบบการโอนเงินทีละรายการ (Single Payment System)	Retail payment system services via a Single Payment System	ˈriˌteɪl ˈpeɪmənt ˈsɪstəm ˈsɜrvəsəz ˈvaɪə ðə PromptPay ˈsɪstəm (PromptPay)

คำภาษาไทย Thai words	**คำภาษาอังกฤษ** English words	**คำอ่าน** Pronunciation
บริการศูนย์กลางจับคู่คำสั่งซื้อขาย	Order matching center services	ˈriˌteɪl ˈpeɪmənt ˈsɪstəm ˈsɜrvəsəz ˈvaɪə ə ˈsɪŋgəl ˈpeɪmənt ˈsɪstəm
บริการศูนย์กลางชำระราคาและส่งมอบหลักทรัพย์	Clearing and settlement center services	ˈɔrdər ˈmætʃɪŋ ˈsɛntər ˈsɜrvəsəz
บริการศูนย์กลางรับฝากหลักทรัพย์	Securities depository center services	ˈklɪrɪŋ ænd ˈsɛtəlmənt ˈsɛntər ˈsɜrvəsəz
บริการโทรศัพท์ประจำที่ภายในประเทศ (Fixed-line)	Fixed-line telephone services	sɪˈkjʊrətiz dɪˈpɑzəˌtɔri ˈsɛntər ˈsɜrvəsəz
บริการโทรศัพท์เคลื่อนที่ภายในประเทศ (Mobile)	Mobile phone services	fɪkst-laɪn ˈtɛləˌfoʊn ˈsɜrvəsəz
บริการอินเทอร์เน็ตบรอดแบนด์ประจำที่ (Internet)	Fixed Broadband Internet services	ˈmoʊbəl foʊn ˈsɜrvəsəz
บริการที่เกี่ยวข้องกับการควบคุมการจราจรในพื้นที่กรุงเทพมหานคร	Services related to traffic control in the Bangkok area	fɪkst ˈbrɔdˌbænd ˈɪntərˌnɛt ˈsɜrvəsəz
บริการที่เกี่ยวข้องกับการควบคุมการเดินรถจากศูนย์กลาง	Services related to centralized traffic control	ˈsɜrvəsəz rɪˈleɪtɪd tu ˈtræfɪk kənˈtroʊl ɪn ðə bæŋˈkɑk ˈɛriə
บริการขายตั๋วและสำรองที่นั่ง	Ticketing and reservation services	ˈsɜrvəsəz rɪˈleɪtɪd tu ˈsɪgnəl trænˈsmɪʃən, kəmˌjunəˈkeɪʃən, ænd ˈdeɪtə trænˈsmɪʃən
บริการที่เกี่ยวข้องกับการควบคุม กำกับดูแลและเก็บข้อมูล	Services related to data control, supervision and collection	ˈtɪkətɪŋ ænd ˌrɛzərˈveɪʃən ˈsɜrvəsəz
บริการที่เกี่ยวข้องกับการบริหารจัดการท่าเรือ	Services related to port management	ˈsɜrvəsəz rɪˈleɪtɪd tu ˈdeɪtə kənˈtroʊl, ˌsupərˈvɪʒən ænd kəˈlɛkʃən
บริการด้านเรือ สินค้า คลังสินค้า เครื่องมือทุ่นแรง และใบแจ้งหนี้ค่าภาระต่าง ๆ	Services related to ships, cargo, warehouses, labor-saving tools, and invoices for expenses	ˈsɜrvəsəz rɪˈleɪtɪd tu pɔrt ˈmænədʒmənt

คำภาษาไทย Thai words	**คำภาษาอังกฤษ** English words	**คำอ่าน** Pronunciation
บริการที่เกี่ยวข้องกับการจัดการท่าเทียบเรือตู้สินค้า	Services related to container terminal management	ˈsɜrvəsəz rɪˈleɪtɪd tu ʃɪps, ˈkɑrˌgoʊ, ˈwɛrˌhaʊzɪz, ˈleɪbər-ˈseɪvɪŋ tulz, ænd ˈɪnvɔɪsɪz fɔr ɪkˈspɛnsəz
บริการที่เกี่ยวข้องกับการควบคุมและลากจูง	Services related to control and towing	ˈsɜrvəsəz rɪˈleɪtɪd tu kənˈteɪnər ˈtɜrmənəl ˈmænədʒmənt
บริการจราจรทางอากาศ	Air traffic services	ˈsɜrvəsəz rɪˈleɪtɪd tu kənˈtroʊl ænd ˈtoʊɪŋ
บริการข่าวสารการบิน	Aeronautical information services	ɛr ˈtræfɪk ˈsɜrvəsəz
บริการที่เกี่ยวข้องกับการปฏิบัติการท่าอากาศยาน	Services related to airport operation	ˌɛroʊˈnɑtəkəl ˌɪnfərˈmeɪʃən ˈsɜrvəsəz
บริการเครื่องอำนวยความสะดวกการเดินอากาศ	Air navigation facility services	ˈsɜrvəsəz rɪˈleɪtɪd tu ˈɛrˌpɔrt ˌɑpəˈreɪʃən
บริการที่เกี่ยวข้องกับบริการสิ่งอำนวยความสะดวกและรักษาความปลอดภัยกิจการการบิน	Services related to facilities and security services concerning aeronautical business	ɛr ˈnævəˈgeɪʃən fəˈsɪlɪti ˈsɜrvəsəz
บริการสายการบิน	Airline services	ˈsɜrvəsəz rɪˈleɪtɪd tu ˌeroʊˈnɑtəkəl ˌmitiəˈrɑlədʒi
บริการที่เกี่ยวข้องกับการป้องกันคลื่นวิทยุ (สนามบิน)	Services related to radio wave protection (airport)	ˈɛrˌlaɪn ˈsɜrvəsəz
บริการที่เกี่ยวข้องกับการขนถ่ายสินค้า	Services related to goods transfer	ˈsɜrvəsəz rɪˈleɪtɪd tu ˈreɪdiˌoʊ weɪv prəˈtɛkʃən (ˈɛrˌpɔrt)
บริการครัวการบินและสิ่งอำนวยความสะดวกสำหรับผู้โดยสารบนอากาศยาน	In-flight catering services and onboard passenger facilities	ˈsɜrvəsəz rɪˈleɪtɪd tu gʊdz ˈtrænsfər
บริการลานจอด ตรวจสอบและบำรุงรักษาอากาศยาน	Apron, inspection, and aircraft maintenance services	ɪn-flaɪt ˈkeɪtərɪŋ ˈsɜrvəsəz ænd ˈɑnˌbɔrd ˈpæsəndʒər fəˈsɪlətiz
บริการผลิตไฟฟ้า	Electricity generating services	ˈeɪprən, ɪnˈspɛkʃən, ænd ˈɛrˌkræft ˈmeɪntənəns ˈsɜrvəsəz

คำภาษาไทย Thai words	**คำภาษาอังกฤษ** English words	**คำอ่าน** Pronunciation
บริการสายส่งไฟฟ้า	Electricity transmission line services	ɪˌlɛkˈtrɪsəti ˈʤɛnəˌreɪtɪŋ ˈsɜrvəsəz
บริการจำหน่ายไฟฟ้า	Electricity distribution services	ɪˌlɛkˈtrɪsəti trænˈsmɪʃən laɪn ˈsɜrvəsəz
บริการควบคุมไฟฟ้า	Electrical control services	ɪˌlɛkˈtrɪsəti ˌdɪstrəˈbjuʃən ˈsɜrvəsəz
บริการที่เกี่ยวข้องกับการบริหารจัดการพลังงานไฟฟ้า	Services related to electrical energy management services	ɪˈlɛktrɪkəl kənˈtroʊl ˈsɜrvəsəz
บริการผลิตปิโตรเลียม	Petroleum production services	ˈsɜrvəsəz rɪˈleɪtɪd tu ɪˈlɛktrɪkəl ˈɛnərʤi ˈmænəʤmənt ˈsɜrvəsəz
บริการขนส่งก๊าซ และน้ำมัน	Gas and oil transportation services	pəˈtroʊliəm prəˈdʌkʃən ˈsɜrvəsəz
บริการเก็บรักษาและแปรสภาพก๊าซ	Gas storage and gasification services	gæs ænd ɔɪl ˌtrænspərˈteɪʃən ˈsɜrvəsəz
บริการที่เกี่ยวข้องกับงานควบคุมคุณภาพน้ำประปา	Services related to water quality control services	gæs ˈstɔrəʤ ænd ˌgæsəfəˈkeɪʃən ˈsɜrvəsəz
บริการที่เกี่ยวข้องกับการผลิตน้ำ	Services related to water production	ˈsɜrvəsəz rɪˈleɪtɪd tu ˈwɔtər ˈkwɑləti kənˈtroʊl ˈsɜrvəsəz
บริการจำหน่ายน้ำ	Water distribution services	ˈsɜrvəsəz rɪˈleɪtɪd tu ˈwɔtər prəˈdʌkʃən
บริการทางการแพทย์ในสถานพยาบาล และบริการที่เกี่ยวข้องกับงานสนับสนุน	Medical services in healthcare facilities and services related to support work	ˈwɔtər ˌdɪstrəˈbjuʃən ˈsɜrvəsəz
บริการที่เกี่ยวข้องกับการควบคุมการแพร่กระจายเชื้อโรคในสถานพยาบาล	Services related to disease control in healthcare facilities	ˈmɛdəkəl ˈsɜrvəsəz ɪn ˈhɛlθˌkɛr fəˈsɪlətiz ænd ˈsɜrvəsəz rɪˈleɪtɪd tu səˈpɔrt wɜrk
บริการทางการแพทย์ฉุกเฉินนอกสถานพยาบาล	Emergency medical services outside healthcare facilities	ˈsɜrvəsəz rɪˈleɪtɪd tu dɪˈziz kənˈtroʊl ɪn ˈhɛlθˌkɛr fəˈsɪlətiz
บริการทางห้องปฏิบัติการ	Laboratory services	ɪˈmɜrʤənsi ˈmɛdəkəl ˈsɜrvəsəz ˈaʊtˈsaɪd ˈhɛlθˌkɛr fəˈsɪlətiz
บริการทางรังสีวิทยา	Radiology services	ˈlæbrəˌtɔri ˈsɜrvəsəz
บริการโลหิตและคลังเลือด	Blood and blood bank services	ˌreɪdiˈɑləʤi ˈsɜrvəsəz

คำภาษาไทย Thai words	**คำภาษาอังกฤษ** English words	**คำอ่าน** Pronunciation
บริการที่เกี่ยวข้องกับการควบคุมโรคติดต่อ	Services related to infectious disease control	blʌd ænd blʌd bæŋk ˈsɜrvəsəz
บริการที่เกี่ยวข้องกับการผลิตยา	Services related to pharmaceutical manufacturing	ˈsɜrvəsəz rɪˈleɪtɪd tu ɪnˈfɛkʃəs dɪˈziz kənˈtroʊl
บริการที่เกี่ยวข้องกับการผลิตเวชภัณฑ์	Services related to medical supplies production	ˈsɜrvəsəz rɪˈleɪtɪd tu ˌfɑrməˈsutɪkəl ˌmænjəˈfæktʃərɪŋ
บริการที่เกี่ยวข้องกับการผลิตเครื่องมือแพทย์	Services related to medical equipment production	ˈsɜrvəsəz rɪˈleɪtɪd tu ˈmɛdəkəl səˈplaɪz prəˈdʌkʃən
บริการนำเข้า กระจาย และจำหน่ายยา	Pharmaceutical import, distribution, and sales services	ˈsɜrvəsəz rɪˈleɪtɪd tu ˈmɛdəkəl ɪˈkwɪpmənt prəˈdʌkʃən
บริการนำเข้า กระจาย และจำหน่ายเวชภัณฑ์	Medical supply import, distribution, and sales services	ˌfɑrməˈsutɪkəl ˈɪmpɔrt, ˌdɪstrəˈbjuʃən, ænd seɪlz ˈsɜrvəsəz
บริการนำเข้า กระจาย และจำหน่ายเครื่องมือแพทย์	Medical equipment imports, distribution, and sales services	ˈmɛdəkəl səˈplaɪ ˈɪmpɔrt, ˌdɪstrəˈbjuʃən, ænd seɪlz ˈsɜrvəsəz
บริการที่เกี่ยวข้องกับการตรวจวิเคราะห์ทางการแพทย์	Services related to medical analysis	ˈmɛdəkəl ɪˈkwɪpmənt ɪmˈpɔrts, ˌdɪstrəˈbjuʃən, ænd seɪlz ˈsɜrvəsəz
บริการทางรังสีวิทยา	Radiology services	ˈsɜrvəsəz rɪˈleɪtɪd tu ˈmɛdəkəl əˈnæləsəs
บริการทางกัมมันตรังสี	Radioactive services	ˌreɪdiˈɑlədʒi ˈsɜrvəsəz
บริการด้านการเงินการคลังสุขภาพ	Health financing services	ˌreɪdioʊˈæktɪv ˈsɜrvəsəz
บริการคลังข้อมูลสุขภาพ	Health Data Center	hɛlθ fəˈnænsɪŋ ˈsɜrvəsəz
บริการคลังข้อมูลสุขภาพ	Services related to digital health system	hɛlθ ˈdeɪtə ˈsɛntər
บริการที่เกี่ยวข้องกับระบบสุขภาพดิจิทัล	Medical services in healthcare facilities and services related to support work	ˈsɜrvəsəz rɪˈleɪtɪd tu ˈdɪdʒətəl hɛlθ ˈsɪstəm

อภิธานศัพท์ทั่วไป

General Glossary

คำภาษาไทย Thai words	คำภาษาอังกฤษ English words	คำอ่าน Pronunciation
การควบคุมการเข้าถึง	Access Control	ˈækˌsɛs kənˈtroʊl
การบริหารจัดการคีย์สำหรับการเข้าถึงระบบต่าง ๆ	access key managements	ˈækˌsɛs ki ˈmænɪʤmənts
การรับรองระบบงาน	Accreditations	əˌkrɛdəˈdeɪʃənz ænd
การวินิจฉัยชี้ขาด	adjudicate	əˈʤudɪˌkeɪt
อำนวยความยุติธรรมทางอาญา	administration of criminal justice	ædˌmɪnɪˈstreɪʃən ʌv ˈkrɪmənəl ˈʤʌstəs
กระบวนการทบทวนหลังการดำเนินการ	After-Action Review Process	ˈæftər-ˈækʃən ˌriˈvju ˈproˌsɛs
ภาคี	alliances	əˈlaɪənsəz
อาการหรือสิ่งผิดปกติ	anomalies	əˈnɑməliz
การตรวจสอบความมั่นคงปลอดภัยของสถาปัตยกรรม	Architecture Security Review	ˈɑrkəˌtɛktʃər sɪˈkjʊrəti ˌriˈvju
ทะเบียนทรัพย์สิน	asset inventory	ˈæˌsɛt ˌɪnvənˈtɔri
การจัดการทรัพย์สิน	Asset Management	ˈæˌsɛt ˈmænəʤmənt
แหล่งที่มาของการโจมตี	attacking host	əˈtækɪŋ hoʊst
เทคนิคการพิสูจน์ตัวตน	Authentication Techniques	ɔˌθɛntəˈkeɪʃən tɛkˈniks
เทคนิคการตรวจสอบสิทธิ์	authorization checking techniques	ˌɔθərəˈzeɪʃən ˈtʃɛkɪŋ tɛkˈniks
ความพร้อมในการใช้งาน	availability	əˌveɪləˈbɪləti
แนวปฏิบัติพื้นฐาน	baseline	ˈbeɪˌslaɪn
แนวทางปฏิบัติที่ดี	best practice	bɛst ˈpræktəs
แผนความต่อเนื่องทางธุรกิจ	Business Continuity Plan (BCP)	ˈbɪznəs ˌkɑntəˈnuəti plæn (bi-si-pi)
การวิเคราะห์ผลกระทบทางธุรกิจ	Business Impact Analysis (BIA)	ˈbɪznəs ˈɪmpækt əˈnæləsəs (bi-aɪ-eɪ)
โมเดลการวัดระดับขีดความสามารถขององค์กร	Capability Maturity Model	ˌkeɪpəˈbɪləti məˈtʃʊrəti ˈmɑdəl

คำภาษาไทย Thai words	**คำภาษาอังกฤษ** English words	**คำอ่าน** Pronunciation
ราชการส่วนกลาง	central government	ˈsɛntrəl ˈgʌvərmənt
การรับรอง	Certifications	sɜrtəfəˈkeɪʃənz
กระบวนการจัดการเปลี่ยนแปลง	Change Management Process	ʧeɪnʤ ˈmænəʤmənt ˈprɑˌsɛs
ประมวลแนวทางปฏิบัติ	code of practice	koʊd ʌv ˈpræktəs
กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	cybersecurity standard frameworks	ˈsaɪbərsɪˈkjʊrəti ˈstændərd ˈfreɪmˌwɜrks
เขตอำนาจ	Competent Court	ˈkɑmpətɪnt kɔrt
นิติวิทยาศาสตร์ทางคอมพิวเตอร์	computer forensics science	kəmˈpjutər fəˈrɛnsɪks ˈsaɪəns
ข้อมูลจราจรทางคอมพิวเตอร์	computer logs	kəmˈpjutər lɔgz
การรักษาความลับ	confidentiality	ˌkɑnfəˌdɛnʃiˈæləti
แผนการบริหารจัดการการตั้งค่าหรือการเปลี่ยนแปลงค่าของอุปกรณ์	configuration management plan	kənˌfɪgjəˈreɪʃən ˈmænəʤmənt plæn
การระงับ	containment	kənˈteɪnmənt
แผนการดำเนินการแก้ไข	corrective action plan	kəˈrɛktɪv ˈækʃən plæn
แผนการสื่อสารในภาวะวิกฤต	Crisis Communication Plan	ˈkraɪsəs kəmˌjunəˈkeɪʃən plæn
ทีมสื่อสารในภาวะวิกฤต	crisis communication team	ˈkraɪsəs kəmˌjunəˈkeɪʃən tim
ระดับวิกฤติ	crisis level	ˈkraɪsəs ˈlɛvəl
ภาวะคับขัน	crisis situations	ˈkraɪsəs ˌsɪtʃuˈeɪʃənz
โครงสร้างพื้นฐานสำคัญทางสารสนเทศ	critical information infrastructure	ˈkrɪtɪkəl ˌɪnfərˈmeɪʃən ˌɪnfrəˈstrʌktʃər
แผนการป้องกันโครงสร้างพื้นฐานสำคัญทางสารสนเทศ	critical information infrastructure protection plan	ˈkrɪtɪkəl ˌɪnfərˈmeɪʃən ˌɪnfrəˈstrʌktʃər prəˈtɛkʃən plæn
ทรัพย์สินสำคัญทางสารสนเทศ	critical IT assets	ˈkrɪtɪkəl ɪt ˈæˌsɛts
ระดับร้ายแรง	critical level	ˈkrɪtɪkəl ˈlɛvəl
บริการที่สำคัญ	Critical Service	ˈkrɪtɪkəl ˈsɜrvəs
ระบบงานที่มีความสำคัญ	critical system	ˈkrɪtɪkəl ˈsɪstəm
วิทยาการเข้ารหัสลับ	cryptography	krɪpˈtɑː.grə.fi

คำภาษาไทย Thai words	**คำภาษาอังกฤษ** English words	**คำอ่าน** Pronunciation
หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์	Cyber Incident Reporting Criteria and Procedure	ˈsaɪbər ˈɪnsədənt rɪˈpɔrtɪŋ kraɪˈtɪriə ænd prəˈsiʤər
การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์	Cyber Threat Detection and Monitoring	ˈsaɪbər θrɛt dɪˈtɛkʃən ænd ˈmɑnətərɪŋ
ลักษณะภัยคุกคามทางไซเบอร์	cyber incident characteristics	ˈsaɪbər θrɛt ˈɪmpækt ˌkɛrəktə ˈrɪstɪks
มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์	cyber threat monitoring and detection measure	ˈsaɪbər θrɛt ˈmɑnətərɪŋ ænd dɪˈtɛkʃən ˈmɛʒər
ความมั่นคงปลอดภัยไซเบอร์	cybersecurity	ˈsaɪbərsɪˈkjʊrəti
พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒	Cybersecurity Act B.E. 2562 (2019)	ˈsaɪbərsɪˈkjʊrəti ækt bi.i. 2562 (2019)
การตรวจสอบความมั่นคงปลอดภัย	cybersecurity assessment	ˈsaɪbərsɪˈkjʊrəti əˈsɛsmənt
แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	Cybersecurity Audit Plan	ˈsaɪbərsɪˈkjʊrəti ˈɔdɪt plæn
การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์	Cybersecurity Awareness Raising	ˈsaɪbərsɪˈkjʊrəti əˈwɛrnəs ˈreɪzɪŋ
การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์	Cybersecurity Exercise	ˈsaɪbərsɪˈkjʊrəti ˈɛksərˌsaɪz
การจำแนกลักษณะของภัยคุกคามทางไซเบอร์	cybersecurity incident characterization	ˈsaɪbərsɪˈkjʊrəti ˈɪnsədənt ˌkɛrəktərɪˈzeɪʃən
การดำเนินมาตรการที่เกี่ยวข้องเพื่อจัดการภัยคุกคามทางไซเบอร์	cybersecurity incident handling	ˈsaɪbərsɪˈkjʊrəti ˈɪnsədənt ˈhændlɪŋ
แผนการรับมือภัยคุกคามทางไซเบอร์	Cybersecurity Incident Response Plan	ˈsaɪbərsɪˈkjʊrəti ˈɪnsədənt rɪˈspɑns plæn
สถานการณ์จำลองเหตุการณ์	cybersecurity incident scenarios	ˈsaɪbərsɪˈkjʊrəti ˈɪnsədənt sɪˈnɛrioʊz
ภัยคุกคามทางไซเบอร์	cyber incidents	ˈsaɪbərsɪˈkjʊrəti ˈɪnsədənts

คำภาษาไทย Thai words	**คำภาษาอังกฤษ** English words	**คำอ่าน** Pronunciation
ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้	Cybersecurity Risk Appetite	ˈsaɪbərsɪˈkjʊrəti rɪsk ˈæpəˌtaɪt
การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	Cybersecurity Risk Assessment	ˈsaɪbərsɪˈkjʊrəti rɪsk əˈsɛsmənt
โปรไฟล์ความเสี่ยง	cybersecurity risk profile	ˈsaɪbərsɪˈkjʊrəti rɪsk ˈproʊˌfaɪl
การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้	Denial of Service	dɪˈnaɪəl ʌv ˈsɜrvəs
การตรวจจับและวิเคราะห์	detection and analysis	dɪˈtɛkʃən ænd əˈnæləsəs
การตรวจจับการบุกรุก	detection of intrusion	dɪˈtɛkʃən ʌv ɪnˈtruʒən
การพิสูจน์หลักฐานทางดิจิทัล	Digital Forensics	ˈdɪdʒətəl fəˈrɛnsɪks
การพิสูจน์และยืนยันตัวตนทางดิจิทัล	digital identity verification and authentication	ˈdɪdʒətəl aɪˈdɛntəti ˌvɛrəfəˈkeɪʃən ænd ɔˌθɛntəˈkeɪʃən
แผนฟื้นฟู	disaster recovery plan	dɪˈzæstər rɪˈkʌvri plæn
หยุดชะงัก	disrupt	dɪsˈrʌpt
ความมั่นคงทางเศรษฐกิจ	economic security	ˌɛkəˈnɑmɪk sɪˈkjʊrəti
สร้างความตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	Education Training and Awareness (ETA)	ˌɛdʒəˈkeɪʃən ˈtreɪnɪŋ ænd əˈwɛrnəs (i-ti-eɪ)
การประชุมผ่านสื่ออิเล็กทรอนิกส์	electronic meeting	ɪˌlɛkˈtrɑnɪk ˈmitɪŋ
การรับแจ้งเหตุฉุกเฉิน	emergency call handling	ɪˈmɜrdʒənsi kɔl ˈhændlɪŋ
ไต่สวนคำร้องฉุกเฉิน	emergency hearing motion	ɪˈmɜrdʒənsi ˈhirɪŋ ˈmoʊʃən
เอกสารแนบท้ายประกาศ	Enclosure	ɛnˈkloʊʒər
การปราบปราม	eradication	ɪˌrædəˈkeɪʃən
ถูกจู่โจม	exploited	ˈɛkˌsplɔɪtəd
ผู้ให้บริการภายนอก	external service provider	ɪkˈstɜrnəl ˈsɜrvəs prəˈvaɪdər
นิติวิทยาศาสตร์	forensic science	ˌsaɪənˈtɪfɪk ˈdɪdʒətəl fəˈrɛnsɪk

คำภาษาไทย Thai words	**คำภาษาอังกฤษ** English words	**คำอ่าน** Pronunciation
ผลกระทบต่อการทำงานของระบบ	functional impact	ˈfʌŋkʃənəl ˈɪmpækt
ราชกิจจานุเบกษา	Royal Thai Government Gazette	ˈgʌvərmənt gəˈzɛt
แนวทางปฏิบัติ	guideline	ˈgaɪˌdlaɪn
เผชิญเหตุ	handle the incident	ˈhændəl ði ˈɪnsədənt
การประทุษร้ายต่อข้อมูล	harm to data	hɑrm tu ˈdeɪtə
การประเมินความมั่นคงปลอดภัยของโฮสต์	Host Security Assessment	hoʊst sɪˈkjʊrəti əˈsɛsmənt
ภัยคุกคามทางไซเบอร์ในระดับวิกฤติ	incident at a crisis level	ˈɪnsədənt æt ə ˈkraɪsəs ˈlɛvəl
ภัยคุกคามทางไซเบอร์ระดับร้ายแรง	Incident at a Critical Level	ˈɪnsədənt æt ə ˈkrɪtɪkəl ˈlɛvəl
ภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง	incident at a non-critical level	ˈɪnsədənt æt ə nɑn-ˈkrɪtɪkəl ˈlɛvəl
หมวดหมู่ภัยคุกคาม	Incident Category	ˈɪnsədənt ˈkætəˌgɔri
รายงานปิดเหตุการณ์ภัยคุกคาม	incident closure report	ˈɪnsədənt ˈkloʊʒər rɪˈpɔrt
สิ่งบอกเหตุการณ์	incident indicators	ˈɪnsədənt ˈɪndəˌkeɪtərz
โครงสร้างการรายงานเหตุการณ์	Incident Reporting Structure	ˈɪnsədənt rɪˈpɔrtɪŋ ˈstrʌktʃər
การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์	Incident Resilience and Recovery	ˈɪnsədənt rɪˈzɪliəns ænd rɪˈkʌvri
การทดสอบความสามารถในการตอบสนองต่อภัยคุกคามทางไซเบอร์	incident respond capability testing	ˈɪnsədənt rɪˈspɑnd ˌkeɪpəˈbɪləti ˈtɛstɪŋ
องค์กรอิสระ	independent institution	ˌɪndɪˈpɛndənt ˌɪnstɪˈtuʃən
ระบบที่ใช้ควบคุมเครื่องจักรในอุตสาหกรรม	Industrial Control System (ICS)	ɪnˈdʌstriəl kənˈtroʊl ˈsɪstəm (aɪ-si-ɛs)
ผลกระทบต่อข้อมูล	information impact	ˌɪnfərˈmeɪʃən ˈɪmpækt
ความมั่นคงปลอดภัยสารสนเทศ	Information Security	ˌɪnfərˈmeɪʃən sɪˈkjʊrəti
การแบ่งปันข้อมูล	Information Sharing	ˌɪnfərˈmeɪʃən ˈʃɛrɪŋ

คำภาษาไทย Thai words	**คำภาษาอังกฤษ** English words	**คำอ่าน** Pronunciation
ศูนย์กลางเครือข่ายข้อมูล	information sharing hub	ˌɪnfərˈmeɪʃən ˈʃɛrɪŋ hʌb
ความครบถ้วนถูกต้อง	integrity	ɪnˈtɛgrəti
การบุกรุก	intrusion	ɪnˈtruʒən
การสืบสวนสอบสวน	investigation	ɪnˌvɛstəˈgeɪʃən
การใช้คำสั่งระบบ	Issuing System Commands	ˈɪʃuɪŋ ˈsɪstəm kəˈmændz
องค์กรฝ่ายตุลาการ	judicial institution	ʤuˈdɪʃəl ˌɪnstɪˈtuʃən
นิติบุคคล	juristic person	jü-ˈrɪstɪks ˈpɜrsən
ดัชนีชี้วัดความเสี่ยงที่สำคัญ	Key Risk Indicator (KRI)	ki rɪsk ˈɪndəˌkeɪtər (keɪ-ɑr-aɪ)
การปฏิบัติตามกฎหมาย	lawfulness	ˈlɔfəlnəs
สิทธิพิเศษในการเข้าถึงน้อยที่สุด	Least Access Privilege	list ˈækˌsɛs ˈprɪvləʤ
องค์กรฝ่ายนิติบัญญัติ	legislative institution	ˈlɛʤəˌsleɪtɪv ˌɪnstɪˈtuʃən
ผู้บริหารท้องถิ่น	local administer	ˈloʊkəl ədˈmɪnəstər
สมาชิกสภาท้องถิ่น	local councilor	ˈloʊkəl ˈkaʊnsələr
ราชการส่วนท้องถิ่น	local government	ˈloʊkəl ˈgʌvərmənt
ข้อมูลจราจร	Log	lɔg
สิ่งที่ไม่พึงประสงค์	malicious code	məˈlɪʃəs koʊd
การบุกรุกโดยการใช้มัลแวร์	Malicious Logic	məˈlɪʃəs ˈlɑʤɪk
ระยะเวลาสูงสุดที่ยอมให้ธุรกิจหยุดชะงัก	Maximum Tolerance Period of Disruption (MTPD)	ˈmæksəməm ˈtɑlərəns ˈpɪriəd ʌv dɪsˈrʌpʃən (ɛm-ti-pi-di)
มาตรการ	measure	ˈmɛʒər
ความสมบูรณ์ของข้อความ	Message Integrity	ˈmɛsəʤ ɪnˈtɛgrəti
บรรเทา	mitigate	ˈmɪtəˌgeɪt
มาตรการเยียวยา	mitigation measures	ˌmɪtɪˈgeɪʃən ˈmɛʒərz
เฝ้าระวัง	monitor	ˈmɑnətər
คำร้อง	motion	ˈmoʊʃən
ผลประโยชน์ของชาติ	national interests	ˈnæʃənəl ˈɪntrəsts
แผนผังโครงสร้างเครือข่าย	Network diagrams	ˈnɛˌtwɜrk ˈdaɪəˌgræmz
ขอบเขตเครือข่าย	network perimeter	ˈnɛˌtwɜrk pəˈrɪmətər

คำภาษาไทย Thai words	**คำภาษาอังกฤษ** English words	**คำอ่าน** Pronunciation
การประเมินความมั่นคงปลอดภัยของเครือข่าย	Network Security Assessment	ˈnɛˌtwɜrk sɪˈkjʊrəti əˈsɛsmənt
การไม่ปฏิบัติตาม	non-compliance	nɑn-kəmˈplaɪəns
ระดับไม่ร้ายแรง	non-critical level	nɑn-ˈkrɪtɪkəl ˈlɛvəl
ประกาศ	Notification	ˌnoʊtəfəˈkeɪʃən
การกระทำความผิด	offense	əˈfɛns
เจ้าหน้าที่ของพรรคการเมือง	officer of a political party	ˈɔfəsər ʌv ə pəˈlɪtəkəl ˈpɑrti
สภาพแวดล้อมการปฏิบัติการทางไซเบอร์	operational environment	ˌɑpəˈreɪʃənəl ɪnˈvaɪrənmənt
ผู้ดำเนินการ	operator	ˈɑpəˌreɪtər
หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ	Organization of Critical Information Infrastructure	ˌɔrgənəˈzeɪʃən ʌv ˈkrɪtɪkəl ˌɪnfərˈmeɪʃən ˌɪnfrəˈstrʌktʃər
กฎหมายอาญา	Penal Code	ˈpinəl koʊd
การทดสอบเจาะระบบ	Penetration Test	ˌpɛnəˈtreɪʃən tɛst
บัญชีช่องทางการติดต่อ	point of contact	pɔɪnt ʌv ˈkɑnˌtækt
การดำเนินกิจกรรมที่เกี่ยวข้องภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์	post-incident activity	poʊst-ˈɪnsədənt ækˈtɪvəti
แนวปฏิบัติ	Practice	ˈpræktəs
การเตรียมการและป้องกัน	Preparation and Protection	ˌprɛpəˈreɪʃən ænd prəˈtɛkʃən
การจัดลำดับความสำคัญ	prioritization	prī-ˈȯr-ə-ˌtīz
มาตรการเชิงรุก	proactive measure	ˈproʊˈæktɪv ˈmɛʒər
การเข้ามาลาดตระเวน	Probing	ˈproʊbɪŋ
องค์การมหาชน	public organization	ˈpʌblɪk ˌɔrgənəˈzeɪʃənz
ความปลอดภัยสาธารณะ	public safety	ˈpʌblɪk ˈseɪfti
การให้บริการของรัฐ	public service	ˈpʌblɪk ˈsɜrvəs
การบริหารจัดการคุณภาพ	quality management	ˈkwɑləti ˈmænədʒmənt
มาตรการเชิงรับ	reactive measure	riˈæktɪv ˈmɛʒər
กลไกที่สามารถแจ้งเตือนได้ทันที	real-time alerts	riəl-taɪm əˈlɜrts

คำภาษาไทย Thai words	**คำภาษาอังกฤษ** English words	**คำอ่าน** Pronunciation
การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี	Reconnaissance	riˈkɑnəsəns
ความสามารถในการกู้คืน	recoverability effort	rɪˌkʌvərəˈbɪləti ˈɛfərt
แผนการกู้คืน	recovery plan	rɪˈkʌvri plæn
ระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย	Recovery Point Objective (RPO)	rɪˈkʌvri pɔɪnt əbˈʤɛktɪv (ɑr-pi-oʊ)
กระบวนการกู้คืน	Recovery Process	rɪˈkʌvri ˈprɑˌsɛs
ระยะเวลาในการกู้คืนระบบ	Recovery Time Objective (RTO)	rɪˈkʌvri taɪm əbˈʤɛktɪv (ɑr-ti-oʊ)
ราชการส่วนภูมิภาค	regional government	ˈriʤənəl ˈgʌvərmənt
การมอบหมายการควบคุมและกำกับดูแล	Regulation Assignment	ˌrɛgjəˈleɪʃən əˈsaɪnmənt
หน่วยงานควบคุมหรือกำกับดูแล	Regulator	ˈrɛgjəˌleɪtər
การเชื่อมต่อระยะไกล	Remote Connection	rɪˈmoʊt kəˈnɛkʃən
สื่อบันทึกข้อมูลแบบถอดได้	Removable Media	rɪˈmuvəbəl ˈmidiə
ความเสี่ยงที่เหลืออยู่	Residual Risk	rɪˈzɪʤuəl rɪsk
มติ	resolution	ˌrɛzəˈluʃən
รับมือ	respond	rɪˈspɑnd
การกู้คืนระบบให้กลับมาดำเนินการได้ตามปกติ	restoring system integrity	rɪˈstɔrɪŋ ˈsɪstəm ɪnˈtɛgrəti
การวิเคราะห์ความเสี่ยง	Risk Analysis	rɪsk əˈnæləsəs
การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง	Risk Assessment and Risk Management Strategy	rɪsk əˈsɛsmənt ænd rɪsk ˈmænəʤmənt ˈstrætəʤi
การประเมินค่าความเสี่ยง	Risk Evaluation	rɪsk ɪˌvæljuˈeɪʃən
การระบุความเสี่ยง	Risk Identification	rɪsk aɪˌdɛntəfəˈkeɪʃən
การบริหารความเสี่ยง	Risk Management	rɪsk ˈmænəʤmənt
การติดตามและทบทวนความเสี่ยง	Risk Monitoring and Review	rɪsk ˈmɑnətərɪŋ ænd ˌriˈvju
การรายงานความเสี่ยง	Risk Reporting	rɪsk rɪˈpɔrtɪŋ
การจัดการความเสี่ยง	Risk Treatment	rɪsk ˈtritmənt

คำภาษาไทย Thai words	**คำภาษาอังกฤษ** English words	**คำอ่าน** Pronunciation
การบุกรุกในระดับผู้ควบคุมระบบ	Root Level Intrusion	rut ˈlɛvəl ɪnˈtruʒən
เลขาธิการ	Secretary-General	ˈsɛkrəˌtɛri-ˈʤɛnərəl
มาตรา	section	ˈsɛkʃən
มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย	Security Baseline Configuration Standards	sɪˈkjʊrəti ˈbeɪˌslaɪn kənˌfɪgjəˈreɪʃən ˈstændərdz
แนวปฏิบัติพื้นฐาน	security control baseline	sɪˈkjʊrəti kənˈtroʊl ˈbeɪˌslaɪn
ข้อตกลงระดับการให้บริการ	Service Level Agreement	ˈsɜrvəs ˈlɛvəl əˈgrimənt
การจู่โจมด้วยวิศวกรรมสังคม	Social Engineering	ˈsoʊʃəl ˈɛnʤəˈnɪrɪŋ
กรอบมาตรฐาน	standard framework	ˈstændərd ˈfreɪmˌwɜrk
รัฐวิสาหกิจ	state enterprise	steɪt ˈɛntərˌpraɪz
เครือข่ายย่อย	subnet	ˈsəbˈnet
การทำให้ระบบมีความแข็งแกร่ง	System Hardening	ˈsɪstəm ˈhɑrdənɪŋ
ข้อมูลสถานะของระบบ	system snapshot	ˈsɪstəm ˈsnæpˌʃɑt
วาระการดำรงตำแหน่ง	term	tɜrm
การจัดการผู้ให้บริการภายนอก	Third Party Management	θɜrd ˈpɑrti ˈmænəʤmənt
ความผิดพลาดจากคนนอกองค์กร	third-party failures	θɜrd-ˈpɑrti ˈfeɪljərz
ผู้ให้บริการภายนอก	third-party service provider	θɜrd- ˈpɑrti ˈsɜrvəs prəˈvaɪdər
ข่าวกรองเกี่ยวกับภัยคุกคามทางไซเบอร์	threat intelligence	θrɛt ɪnˈtɛləʤəns
การเฝ้าระวังและการแจ้งเตือนภัยคุกคาม	threat monitoring and alarming	θrɛt ˈmɑnətərɪŋ ænd əˈlɑrmɪŋ
การติดตามและตรวจสอบ	track and review	træk ænd ˌriˈvju
การควบคุมการจราจร	traffic control	ˈtræfɪk kənˈtroʊl
ความมั่นคงปลอดภัยในการส่ง	Transmission Security	trænˈsmɪʃən sɪˈkjʊrəti
มาตรการเร่งด่วน	urgent measure	ˈɜrʤənt ˈmɛʒər
การบุกรุกในระดับผู้ใช้งาน	User Level Intrusion	ˈjuzər ˈlɛvəl ɪnˈtruʒən
จุดอ่อน	vulnerability	ˌvʌlnərəˈbɪlɪti

คำภาษาไทย Thai words	**คำภาษาอังกฤษ** English words	**คำอ่าน** Pronunciation
การประเมินช่องโหว่และการทดสอบเจาะระบบ	Vulnerability Assessment and Penetration Testing	ˌvʌlnərəˈbɪlɪti əˈsɛsmənt ænd ˌpɛnəˈtreɪʃən ˈtɛstɪŋ
ระบบบริหารจัดการงานต่าง ๆ	workflow management system	wɜrkfloʊ ˈmænədʒmənt ˈsɪstəm

20 อินโฟกราฟิกส์
Infographic



ฉบับภาษาไทย
Thai Version

กฎหมายลำดับรองที่สำคัญ

ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

1 ประกาศ กมช. เรื่อง การจัดตั้ง หน้าที่และอำนาจของ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ พ.ศ. 2564

มีผลใช้บังคับตั้งแต่วันที่ 24 ส.ค. 64 เป็นต้นไป

ThaiCERT
Thailand Computer Emergency Response Team
By NCSA Thailand

มีหน้าที่
เฝ้าระวัง ติดตาม วิเคราะห์ และประมวลผลข้อมูล
เกี่ยวกับภัยคุกคามทางไซเบอร์และการแจ้งเตือน
เกี่ยวกับภัยคุกคามทางไซเบอร์

2 ประกาศ กมช. เรื่อง ลักษณะ หน้าที่และความรับผิดชอบของ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและภารกิจหรือให้บริการที่เกี่ยวข้อง พ.ศ. 2564

มีผลใช้บังคับตั้งแต่วันที่ 23 ส.ค. 65 เป็นต้นไป

สาระสำคัญ **เพื่อกำหนดลักษณะ หน้าที่ และความรับผิดชอบของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ (Sectoral CERT)** สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เพื่อประสานงาน เฝ้าระวัง รับมือ และแก้ไขภัยคุกคามทางไซเบอร์

Sectoral CERT 18 แห่ง ในประเทศไทย

3 ประกาศ กมช. เรื่อง การกำหนดหลักเกณฑ์ ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการมอบหมายการควบคุมและกำกับดูแล พ.ศ. 2568

มีผลใช้บังคับตั้งแต่วันที่ 17 ก.ย. 68 เป็นต้นไป

สาระสำคัญ **เพื่อเป็นการประกาศกำหนดภารกิจหรือบริการของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศทั้งสิ้น 7 ด้าน** ปัจจุบันประกาศฯ ดังกล่าวมี

REGULATOR 19 หน่วย | CII 76 หน่วย

ด้านความมั่นคงของรัฐ | ด้านบริการภาครัฐที่สำคัญ | ด้านการเงินการธนาคาร | ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม | ด้านการขนส่งและโลจิสติกส์ | ด้านพลังงานและสาธารณูปโภค | ด้านสาธารณสุข

4 ประกาศ กกม. เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐาน ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564

มีผลใช้บังคับตั้งแต่วันที่ 6 ก.ย. 65 เป็นต้นไป

สาระสำคัญ กำหนดให้หน่วยของรัฐ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ **มีหน้าที่ในการจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์** อันเป็นข้อกำหนดขั้นต่ำ

ประมวลแนวทางปฏิบัติ มีองค์ประกอบ 3 ฉบับ/ประกอบ
- แผนการตรวจสอบฯ
- การประเมินความเสี่ยงฯ
- แผนการรับมือภัยคุกคามทางไซเบอร์

กรอบมาตรฐาน มีองค์ประกอบ 5 ฉบับ/ประกอบ
- การระบุความเสี่ยง | Identify
- มาตรการป้องกัน | Protect
- มาตรการตรวจสอบและเฝ้าระวัง | Detect
- มาตรการเผชิญเหตุ | Respond
- มาตรการรักษาและฟื้นฟูความเสียหาย | Recover

5 ประกาศ กมช. เรื่อง การกำหนดระดับความรู้ความชำนาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อแต่งตั้งเป็นพนักงานเจ้าหน้าที่ พ.ศ. 2564

มีผลใช้บังคับตั้งแต่วันที่ 8 ธ.ค. 64 เป็นต้นไป

สาระสำคัญ **เพื่อกำหนดคุณสมบัติและความรู้ความชำนาญ** ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ **ของบุคคลที่จะได้รับการแต่งตั้งเป็นพนักงานเจ้าหน้าที่**



ปัจจุบันมีการแต่งตั้งพนักงานเจ้าหน้าที่ จำนวน **152** ราย ซึ่งครอบคลุมทุก Sector

6 ประกาศ กมช. เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคาม ทางไซเบอร์แต่ละระดับ พ.ศ. 2564

มีผลใช้บังคับตั้งแต่วันที่ 12 ธ.ค. 64 เป็นต้นไป

สาระสำคัญ **เพื่อประโยชน์ในการจำแนกลักษณะของภัยคุกคามทางไซเบอร์แต่ละระดับ** รวมทั้งประเมินจากระดับผลกระทบที่อาจเกิดขึ้น หากโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หรือระบบงานที่มีความสำคัญอื่น ๆ ถูกโจมตีจากภัยคุกคามทางไซเบอร์



7 ระเบียบ กกม. ว่าด้วย การมอบอำนาจให้ปฏิบัติการแทน คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2565

มีผลใช้บังคับตั้งแต่วันที่ 27 ธ.ค. 65 เป็นต้นไป

สาระสำคัญ **เพื่อให้การดูแลและดำเนินการเพื่อรับมือกับภัยคุกคามทางไซเบอร์ในระดับร้ายแรงได้ทันท่วงที** กกม. จึงมีการมอบอำนาจให้ **คณะกรรมการรับมือกับภัยคุกคามทางไซเบอร์ในระดับร้ายแรง (คกร.)** เพื่อทำหน้าที่พิจารณาสั่งการกรณีเกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ในระดับร้ายแรงหรือระดับวิกฤติ



8 ประกาศ กมช. เรื่อง นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 – 2570)

มีผลใช้บังคับตั้งแต่วันที่ 10 ธ.ค. 65 เป็นต้นไป

สาระสำคัญ **เพื่อเป็นแผนแม่บทในการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย**



9 ประกาศ กกม. เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ. 2566

มีผลใช้บังคับตั้งแต่วันที่ 10 พ.ค. 66 เป็นต้นไป

สาระสำคัญ **เพื่อกำหนดแนวทางในการแจ้งและรายงานกรณีที่เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ต่อระบบสารสนเทศ** ของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ



10 ประกาศ สกมช. เรื่อง หลักเกณฑ์และอัตราค่าธรรมเนียม ค่าบำรุง ค่าตอบแทน และค่าบริการในการดำเนินงาน พ.ศ. 2566

มีผลใช้บังคับตั้งแต่วันที่ 6 ก.ย. 66 เป็นต้นไป

สาระสำคัญ **เพื่อให้ สกมช. มีแนวทางในการเรียกเก็บค่าธรรมเนียม และ/หรือค่าบริการจากผู้รับบริการ** สำหรับกรณี ดังต่อไปนี้

1. **การใช้ระบบหรือบริการสารสนเทศ เครื่องมือ หรืออุปกรณ์** หรือสิ่งอำนวยความสะดวกและพื้นที่หรือสถานที่
2. **การใช้บริการสำรวจ การวางแผน การจัดการ หรือการวิจัย** ในลักษณะการว่าจ้าง
3. **การใช้บริการจัดฝึกอบรม** สัมมนา หรือประชุม เชิงปฏิบัติการ
4. **การรับรองมาตรฐานผู้ให้บริการ** เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์
5. **การใช้บริการดำเนินโครงการ** หรือบริการอื่นที่เกี่ยวกับหรือเกี่ยวเนื่องกับการรักษาความมั่นคงปลอดภัยไซเบอร์

11 ประกาศ กมช. เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. 2566

มีผลใช้บังคับตั้งแต่วันที่ 18 ม.ค. 68 เป็นต้นไป

สาระสำคัญ เพื่อให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ **มีการกำหนดคุณลักษณะและการจัดระดับผลกระทบของข้อมูลหรือระบบสารสนเทศ**

การกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ **พิจารณาจากวัตถุประสงค์ด้านความมั่นคงปลอดภัยไซเบอร์ (Security objectives)**
- Confidentiality การรักษาความลับ
- Integrity การรักษาความถูกต้องครบถ้วน
- Availability การรักษาสภาพพร้อมใช้งาน

การประเมินและจัดระดับผลกระทบ แบ่งเป็น 3 ระดับ

ระดับต่ำ | ระดับกลาง | ระดับสูง

12 ประกาศ กมช. เรื่อง มาตรฐานขั้นต่ำ ของข้อมูลหรือระบบสารสนเทศ พ.ศ. 2566

มีผลใช้บังคับตั้งแต่วันที่ 18 ม.ค. 68 เป็นต้นไป

สาระสำคัญ กรณีหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ได้กำหนดคุณลักษณะและการจัดระดับผลกระทบของข้อมูลหรือระบบสารสนเทศของตนว่ามีลักษณะ สูง กลาง หรือต่ำแล้ว **มีหน้าที่ต้องกำหนดมาตรการควบคุมความมั่นคงปลอดภัยไซเบอร์ขั้นต่ำ สำหรับข้อมูลหรือระบบสารสนเทศนั้นในแต่ละระดับ**



13 ประกาศ กมช. เรื่อง มาตรฐานและแนวทางส่งเสริมพัฒนาระบบการให้บริการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2566

มีผลใช้บังคับตั้งแต่วันที่ 6 ก.ย. 66 เป็นต้นไป

สาระสำคัญ **เพื่อให้มีกระบวนการตรวจสอบและรับรองการดำเนินงานของผู้ให้บริการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์** ไม่ว่าจะเป็นกระบวนการดำเนินงานระบบหรือเครื่องมือที่ใช้ในการดำเนินงาน หรือบุคลากรที่เกี่ยวข้องในการดำเนินงานว่ามีคุณภาพเป็นไปตามมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์

การรับรองคุณภาพของผู้ให้บริการฯ มี 3 ระดับ



14 ประกาศ กมช. เรื่อง มาตรการและแนวทางในการยกระดับทักษะความรู้และความเชี่ยวชาญ ในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2567

มีผลใช้บังคับตั้งแต่วันที่ 10 ก.ย. 68 เป็นต้นไป

สาระสำคัญ **เพื่อกำหนดมาตรการและแนวทางในการยกระดับทักษะความรู้และความเชี่ยวชาญในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของพนักงานเจ้าหน้าที่และเจ้าหน้าที่ของหน่วยงาน** โครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานเอกชนที่เกี่ยวข้อง **โดยมีองค์ประกอบดังนี้**



15 ประกาศ กกม. เรื่อง หน้าที่ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและหน่วยงานควบคุมหรือกำกับดูแล พ.ศ. 2567

มีผลใช้บังคับตั้งแต่วันที่ 21 มิ.ย. 68 เป็นต้นไป

สาระสำคัญ **เพื่อกำหนดหน้าที่ให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน่วยงานควบคุมหรือกำกับดูแลให้มีความชัดเจนและมีมาตรฐานที่เหมาะสม** เพื่อให้การรับมือภัยคุกคามทางไซเบอร์ของแต่ละหน่วยงานเป็นไปอย่างเหมาะสมและมีประสิทธิภาพ



16 ประกาศ กมช. เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567

มีผลใช้บังคับตั้งแต่วันที่ 10 ก.ย. 69 เป็นต้นไป

สาระสำคัญ **เพื่อกำหนดมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์** ให้แก่หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ **เพื่อลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่มีต่อการใช้บริการคลาวด์สาธารณะ**



17 ประกาศ กมช. เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ พ.ศ. 2568

มีผลใช้บังคับตั้งแต่วันที่ 16 ก.ย. 69 เป็นต้นไป

สาระสำคัญ **เพื่อเป็นการกำหนดและส่งเสริมให้** หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมถึงหน่วยงานเอกชน **มีมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ของตน เป็นไปอย่างมีประสิทธิภาพ ปลอดภัย และให้บริการได้อย่างต่อเนื่อง**

WEBSITE

จัดทำโดย
สำนักกฎหมาย สกมช.
crc@ncsa.or.th
0 2142 6887



ท่านสามารถศึกษาข้อมูลเพิ่มเติมได้ที่
https://ncsa.or.th/standards/laws





ฉบับภาษาอังกฤษ
English Version

IMPORTANT SUBORDINATE LAWS

UNDER THE CYBERSECURITY ACT B.E. 2562 (2019)

1

NOTIFICATION OF NCSC RE :
ESTABLISHMENT, DUTIES, AND POWERS OF
THAILAND COMPUTER EMERGENCY RESPONSE TEAM (THAICERT)
B.E. 2564 (2021)

EFFECTIVE FROM AUGUST 24, 2021, ONWARDS.

ThaiCERT
Thailand Computer Emergency Response Team
By NCSA Thailand

Has the duty to monitor, track, analyze, and process data related to cyber threats and provide alerts regarding cyber threats.

2

NOTIFICATION OF NCSC RE :
CHARACTERISTICS, DUTIES, AND RESPONSIBILITIES OF
THE COMPUTER EMERGENCY RESPONSE TEAM FOR CRITICAL INFORMATION INFRASTRUCTURE ORGANIZATIONS,
RELATED MISSIONS AND SERVICES B.E. 2564 (2021)

EFFECTIVE FROM AUGUST 23, 2022, ONWARDS.

Essence To define the roles, duties, and responsibilities of the Computer Security Incident Response Team (Sectoral CERT) for critical information infrastructure organizations, in order to coordinate, monitor, respond to, and resolve cyber threats.

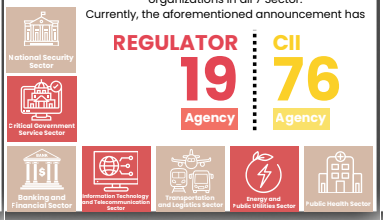
Sectoral CERT 15 units in Thailand

3

NOTIFICATION OF NCSC RE :
CRITERIA AND CHARACTERISTICS FOR DESIGNATING AGENCIES WITH MISSIONS OR SERVICES AS CRITICAL INFORMATION INFRASTRUCTURE ORGANIZATIONS
AND THE REGULATION ASSIGNMENT, B.E. 2568 (2025)

EFFECTIVE FROM SEPTEMBER 17, 2025, ONWARDS.

Essence To announce the determination of the missions or services of critical information infrastructure organizations in all 7 Sector.
Currently, the aforementioned announcement has



REGULATOR 19 Agency | **CII** 76 Agency

4

NOTIFICATION OF CRC RE :
CODES OF PRACTICE AND STANDARD FRAMEWORKS
FOR GOVERNMENT AGENCIES AND CRITICAL INFORMATION INFRASTRUCTURE ORGANIZATIONS
B.E. 2564 (2021)

EFFECTIVE FROM SEPTEMBER 6, 2022, ONWARDS.

Essence It is specified that government agencies and critical information infrastructure organizations are responsible for developing a compilation of guidelines and standards for cybersecurity, which serve as the minimum requirements.

Codes of Practice consist of 3 elements
- Audit Plan
- Risk Assessment
- Incident Response Plan

Standard Frameworks consist of 5 elements
- Identify
- Protect
- Detect
- Respond
- Recover

5

NOTIFICATION OF NCSC RE :
CYBERSECURITY KNOWLEDGE AND EXPERTISE REQUIREMENTS
FOR COMPETENT OFFICIAL APPOINTMENT
B.E. 2564 (2021)

EFFECTIVE FROM DECEMBER 8, 2021, ONWARDS.

Essence To define the qualifications and expertise in cybersecurity of individuals who will be appointed as competent Official.



Currently 152 Competent Officials have been appointed.

6

NOTIFICATION OF NCSC RE :
CHARACTERISTICS AND MEASURES FOR PREVENTION, RESPONSE, ASSESSMENT, ERADICATION,AND CONTAINMENT
OF CYBER INCIDENTS AT EACH LEVEL, B.E. 2564 (2021)

EFFECTIVE FROM DECEMBER 12, 2021, ONWARDS.

Essence To categorize the characteristics of each level of cyber threats, and assess the potential impact that may occur if critical information infrastructure or other important systems are attacked by cyber threats.



Levels of cyber threats

7

REGULATION OF CRC
ON THE ASSIGNMENT OF POWERS TO PERFORM TASKS
ON BEHALF OF THE CYBERSECURITY REGULATING COMMITTEE B.E. 2565 (2022)

EFFECTIVE FROM DECEMBER 27, 2022, ONWARDS.

Essence To ensure timely management and response to severe cyber threats, CRC has delegated authority to the Critical Incident Response Committee (CIRC) to consider and issue directives in the event of or in anticipation of severe or critical cyber threats.



8

NOTIFICATION OF THE NCSC RE:
POLICY AND PLAN ON CYBER SECURITY B.E. 2565 - 2570 (2022-2027)

EFFECTIVE FROM DECEMBER 10, 2022 ONWARDS.

Essence to act as the master plan for the cyber security of Thailand



9

NOTIFICATION OF CRC RE :
CYBER INCIDENT
REPORTING CRITERIA AND PROCEDURE
B.E.2566 (2023)

EFFECTIVE FROM MAY 10, 2023, ONWARDS.

Essence To define the guidelines for notifying and reporting incidents in cases of actual or anticipated cyber threats to the information systems of government agencies and CII.

If there is an occurrence or a potential occurrence of a cyber incident
- **promptly notify the NCSA**
- **report to NCSA within 24 hours**

10

NOTIFICATION OF NCSA RE:
CRITERIA AND RATES OF FEES,
MAINTENANCE FEES, COMPENSATION FEES, AND SERVICE FEES FOR OPERATIONS
B.E. 2566 (2023)

EFFECTIVE FROM SEPTEMBER 6, 2023, ONWARDS.

Essence To provide the NCSA with guidelines for charging fees and/or service charges from users in the following cases :

1. The use of information systems or services, tools, equipment, or facilities, and spaces or locations.
2. The use of surveying, planning, management, or research services in the form of contracting.
3. The use of training, seminar, or workshop services.
4. Certification of service providers for cybersecurity standards.
5. The use of project implementation services or other services related to or associated with cybersecurity.

11

NOTIFICATION OF THE NCSC RE:
STANDARDS FOR DEFINING CYBERSECURITY CHARACTERISTICS
FOR DATA OR INFORMATION SYSTEMS
B.E. 2566 (2023)

EFFECTIVE FROM JANUARY 18, 2025, ONWARDS.

Essence To ensure that government agencies, regulatory, and CII define the characteristics and impact levels of information or information systems.

Defining the characteristics of cybersecurity is based on the **security objectives**.
- **C**onfidentiality
- **I**ntegrity
- **A**vailability

Impact assessment and classification are divided into 3 levels.

Low	Medium	High

12

NOTIFICATION OF THE NCSC RE:
STANDARDS FOR DATA OR INFORMATION SYSTEMS
B.E. 2566 (2023)

EFFECTIVE FROM JANUARY 18, 2025, ONWARDS.

Essence In cases where government agencies, regulatory authorities, and critical information infrastructure organizations have defined the characteristics and impact levels of their information or information systems as high, medium, or low, they are required to establish minimum cybersecurity control measures for that information or information system at each level.



13

NOTIFICATION OF THE NCSC RE:
STANDARDS AND GUIDELINES FOR PROMOTING THE DEVELOPMENT
OF CYBERSECURITY SERVICE DELIVERY SYSTEMS
B.E. 2566 (2023)

EFFECTIVE FROM SEPTEMBER 6, 2023, ONWARDS.

Essence To establish a process for auditing and certifying the operations of cybersecurity service providers, whether it involves the operational processes, systems or tools used, or personnel involved in the operations, ensuring that they meet the quality standards for cybersecurity.

Quality certification of service providers has **3** Levels.



14

NOTIFICATION OF THE NCSC RE:
MEASURES AND GUIDELINES TO ENHANCE THE KNOWLEDGE AND EXPERTISE
IN CYBERSECURITY
B.E. 2567 (2024)

EFFECTIVE FROM SEPTEMBER 10, 2025, ONWARDS.

Essence To define measures and guidelines for enhancing the skills, knowledge, and expertise in cybersecurity of officials and personal from critical information infrastructure organizations, government agencies, regulatory authorities, and relevant private sector organizations, with the following components:

1. Scope of development
2. Consideration of budget allocation and staffing levels
3. Steps for developing the skills of officials or personnel of the organization
4. Staff skill development plan

15

NOTIFICATION OF THE CRC RE :
THE DUTIES OF CRITICAL INFORMATION INFRASTRUCTURE ORGANIZATIONS AND DUTIES OF REGULATORS
B.E. 2567 (2024)

EFFECTIVE FROM JUNE 21, 2025, ONWARDS.

Essence To define the duties of critical information infrastructure organizations and regulatory authorities with clarity and appropriate standards, ensuring that each organization's response to cyber threats is conducted appropriately and effectively.

TEAM THAILAND FOR CYBERSECURITY

16

NOTIFICATION OF THE NCSC RE:
CYBERSECURITY STANDARDS FOR CLOUD SYSTEMS
B.E. 2567 (2024)

EFFECTIVE FROM SEPTEMBER 10, 2026, ONWARDS.

Essence To establish cybersecurity standards for cloud systems for government agencies, regulatory authorities, and critical information infrastructure organizations, in order to reduce the risks from cyber threats associated with the use of public cloud services.

17

NOTIFICATION OF THE NCSC RE:
WEBSITE SECURITY STANDARDS
B.E. 2568 (2025)

EFFECTIVE FROM SEPTEMBER 16, 2026, ONWARDS.

Essence To establish and promote website security standards for government agencies, regulator cii, and private sector entities, in order to ensure that their websites operate efficiently, securely, and with service continuity.

WEBSITE

Made by
Legal Office, NCSA
crc@ncsa.or.th
0 2142 6887



More information at
https://ncsa.or.th/standards/laws





สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

120 อาคารซี ชั้น 7 ศูนย์ราชการเฉลิมพระเกียรติ 80 พรรษา
5 ธันวาคม 2550 ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ 10210
โทรศัพท์ 02 142 6888 (ติดต่อเวลาทำการ) อีเมล : saraban@ncsa.or.th
เว็บไซต์ : www.ncsa.or.th

National Cyber Security Agency (NCSA)

120 , Building C, 7th Floor, Government Complex Commemorating His Majesty the King's 80th Birthday Anniversary, Chaeng Watthana Road, Thung Song Hong, Laksi, Bangkok 10210, Thailand
Phone: +66 2 142 6888 (Office Hours) Email : saraban@ncsa.or.th
Website : www.ncsa.or.th