รายงานผลการเข้าร่วมโครงการ

เรื่อง

"โครงการพัฒนาเครือข่ายผู้ตรวจสอบภายในมหาวิทยาลัยเทคโนโลยีราชมงคล (๙ มทร.)"

ระหว่างวันที่ ๙ – ๑๑ สิงหาคม ๒๕๖๕

ณ มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์

วิทยาลัยเขตวังไกลกังวล อาคารปฏิบัติการโรงแรมและการท่องเที่ยว

(บ้านชมคลื่น) อำเภอหัวหิน จังหวัดประจวบคีรีขันธ์

สำนักงานตรวจสอบภายใน

มหาวิทยาลัยเทคโนโลยีราชมงคลล้านนา

รายงานผลการเข้าร่วมโครงการ

เรื่อง "โครงการพัฒนาเครือข่ายผู้ตรวจสอบภายในมหาวิทยาลัยเทคโนโลยีราชมงคล (๙ มทร.)"

ข้อมูลผู้เข้าร่วมอบรม

๑. นางสาวโสภา	เภสัชพิพัฒน์กุล	ตำแหน่ง รักษาราชการแทน หัวหน้าสำนักงานตรวจสอบภายใน
๒. นางสาวประศิภรณ์	ทิพย์อุทัย	ตำแหน่ง นักตรวจสอบภายใน มทร.ล้านนา
๓. นางนงคราญ	สีไชย	ตำแหน่ง นักตรวจสอบภายใน มทร.ล้านนา
๔. นายเอกชัย	ต๊ะบุญธง	ตำแหน่ง นักตรวจสอบภายใน มทร.ล้านนา
๕. นางสาวศรัญญา	ศรีสัตนา	ตำแหน่ง นักตรวจสอบภายใน มทร.ล้านนา พิษณุโลก
๖. นางชื่นหทัย	เมฆขยาย	ตำแหน่ง นักตรวจสอบภายใน มทร.ล้านนา เชียงราย
๗. นางสาวสุพรรษา	คุณาพันธ์	ตำแหน่ง นักตรวจสอบภายใน มทร.ล้านนา ลำปาง
๘. ว่าที่ร้อยตรีหญิงมนสิชา	นารีรักษ์	ตำแหน่ง นักตรวจสอบภายใน สวก.

ข้อมูลรายละเอียดการอบรม

ชื่อโครงการ "การพัฒนาเครือข่ายผู้ตรวจสอบภายในมหาวิทยาลัยเทคโนโลยีราชมงคล (๙ มทร.)"

วิทยากร ๑. รศ.ดร.อุดมวิทย์ ไชยสกุลเกียรติ อธิการบดี มทร.รัตนโกสินทร์ บรรยายเรื่อง งานตรวจสอบภายในกับการสร้างมูลค่าเพิ่มให้กับองค์กร

๒. ผู้ตรวจสอบภายในกระทรวงศึกษาธิการ บรรยายเรื่อง การตรวจสอบระบบรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๓. วิทยากรจากภายนอกเอกชน และภายนอกราชการ เป็นผู้ให้ความรู้ในการฝึกปฏิบัติ เรื่องแนวปฏิบัติการตรวจสอบนโยบายและแนวปฏิบัติด้านสารสนเทศ (Engagement Plan)

หัวข้อวิชา

๑. ความสำคัญของงานตรวจสอบภายใน เพื่อเพิ่มคุณค่าให้แก่องค์กร ในการตรวจสอบการรักษาความ มั่นคงปลอดภัยด้านสารสนเทศ

๒. การตรวจสอบระบบรักษาความมั่นคงปลอดภัย

๓. แนวปฏิบัติการตรวจสอบนโยบายและแนวปฏิบัติด้านสารสนเทศ (Engagement Plan) และการตรวจสอบโครงการด้านเทคโนโลยีสารสนเทศ

๔. การจัดทำรายงานผลการดำเนินงานของคณะกรรมการตรวจสอบภายในประจำมหาวิทยาลัยตามหลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานการตรวจสอบภายในสำหรับหน่วยงานของรัฐ พ.ศ. ๒๕๖๑ และที่แก้ไขเพิ่มเติม

จัดโดย มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์

วันที่ ๙ - ๑๑ สิงหาคม ๒๕๖๕

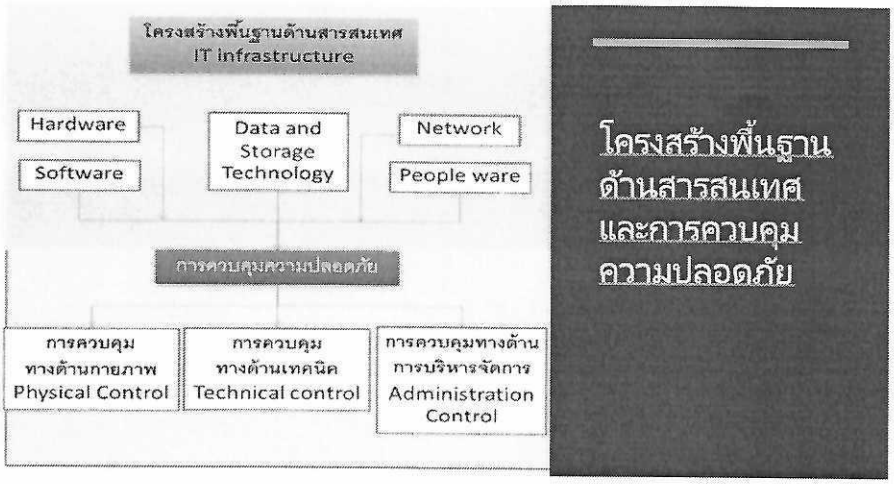
ค่าใช้จ่าย ๔๐,๒๑๒ บาท

<u>สรุปภาพรวมของการเข้าร่วมอบรม</u>

๑. ความสำคัญของงานตรวจสอบภายใน เพื่อเพิ่มคุณค่าให้แก่องค์กร ในการตรวจสอบการรักษาความ มั่นคงปลอดภัยด้านสารสนเทศ

การตรวจสอบภายใน หมายถึง กิจกรรมการให้หลักประกันอย่างเที่ยงธรรมและการให้ คำปรึกษาอย่างเป็นอิสระ ซึ่งจัดให้มีขึ้นเพื่อเพิ่มคุณค่าและปรับปรุงการปฏิบัติงานขององค์กรให้ดีขึ้น การตรวจสอบภายในช่วยให้องค์กรบรรลุถึงเป้าหมายที่วางไว้ ด้วยการประเมินและปรับปรุงประสิทธิภาพของกระบวนการบริหารความเสี่ยง การควบคุม และการกำกับดูแลอย่างเป็นระบบและเป็นระเบียบ

๒. การตรวจสอบระบบรักษาความมั่นคงปลอดภัย



การควบคุมทางด้านกายภาพ (Physical Control)

การตรวจสอบด้านกายภาพ (Physical Control) ได้แก่ ระบบควบคุมการเข้า-ออก ศูนย์คอมพิวเตอร์, Hardware ระบบ Backup/Restore และ ระบบไฟสำรอง เช่น มี UPS เพียงพอหรือไม่ และอุปกรณ์เฝ้าระวัง เช่น กล้องวงจรปิด (CCTV) เป็นต้น

การควบคุมทางด้านเทคนิค (Technical Control)

การควบคุมระบบปฏิบัติการ(operational system) อุปกรณ์เครือข่าย (network devices) อุปกรณ์รักษาความปลอดภัย (security devices) โปรแกรมฐานข้อมูล โปรแกรมประยุกต์และโปรแกรมที่ให้บริการในลักษณะ server

การควบคุมด้านการบริหารจัดการ (Administrative Control)

การควบคุมการบริหารจัดการควบคุมด้านสารสนเทศ (Administrative Control) ได้แก่ การตรวจสอบ Policy, Standard, Guideline และ Procedure ที่องค์กรมีอยู่ว่า ครอบคลุม และมีการปฏิบัติ มีการจัดฝึกอบรมด้านการรักษาความปลอดภัย (Security Awareness Training) โครงสร้างหน่วยงานที่เหมาะสม การแบ่งแยกหน้าที่ต่าง ๆ ที่ชัดเจน การจัดทำแผนสำรองฉุกเฉิน และแผนรับเหตุการณ์ (Business Continuity Planning , Disaster Recovery Planning and Incident Response Procedure) ตลอดจนการควบคุมการเปลี่ยนแปลงระบบงาน (Change Control Management)

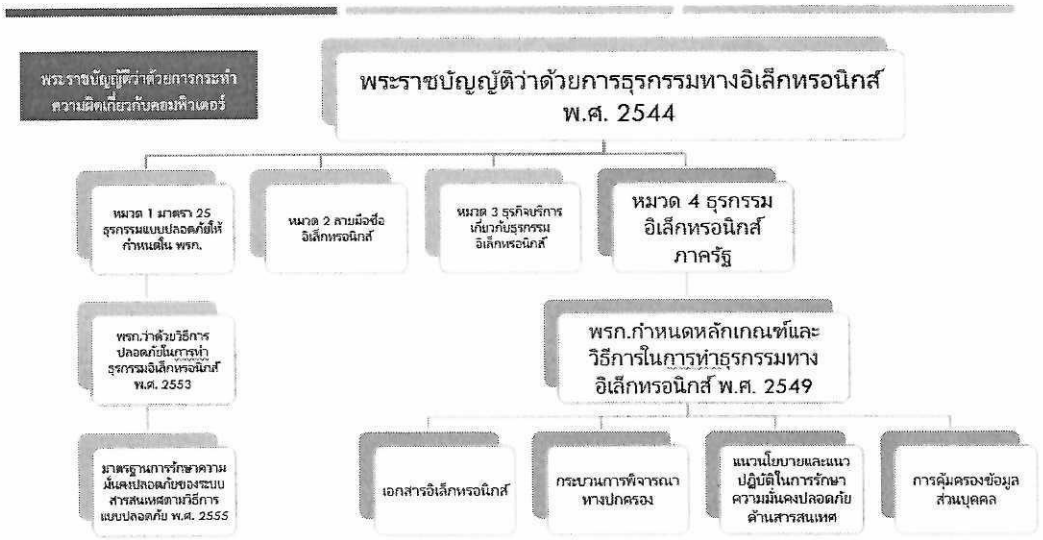
กฎหมายและประกาศ ที่เกี่ยวข้อง

- พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
- พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

- พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ
- แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
- แนวนโยบายและแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล
- มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการปลอดภัย

ความมั่นคงปลอดภัยด้านสารสนเทศ (information security)

หมายถึง การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของสารสนเทศ รวมถึงคุณสมบัติอื่น ได้แก่ ความถูกต้องที่แท้จริง (authenticity) ความรับผิด (accountability) การห้ามปฏิเสธความรับผิด (non-repudiation) และความน่าเชื่อถือ



๓. แนวปฏิบัติการตรวจสอบนโยบายและแนวปฏิบัติด้านสารสนเทศ (Engagement Plan) และการ ตรวจสอบโครงการด้านเทคโนโลยีสารสนเทศ

จัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐ หรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ การจัดทำแนวนโยบาย และแนวปฏิบัติ อย่างน้อยต้องประกอบด้วย เนื้อหา ดังต่อไปนี้

๑. การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

๒. การจัดให้มีระบบสารสนเทศและระบบสำรองของสารสนเทศ ซึ่งอยู่ในสภาพพร้อมใช้งานและจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อให้สามารถใช้งานสารสนเทศได้อย่างปกติต่อเนื่อง

๓. การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ

๓.๑ มาตรา ๗ แนวนโยบายและแนวปฏิบัติ ให้หน่วยงานของรัฐจัดทำเป็นประกาศและต้องได้รับความเห็นชอบจากคณะกรรมการหรือหน่วยงานที่คณะกรรมการมอบหมาย

หน่วยงานของรัฐต้องปฏิบัติตามแนวนโยบายและแนวปฏิบัติที่ได้แสดงไว้ และจัดให้มีการตรวจสอบการปฏิบัติตามแนวนโยบายและแนวปฏิบัติที่กำหนดไว้อย่างสม่ำเสมอ

๓.๒ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ต้องจัดทำเป็นลายลักษณ์อักษร

๓.๓ ข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

อย่างน้อยต้องประกอบด้วยกระบวนการ ดังต่อไปนี้

๑) ต้องจัดทำข้อปฏิบัติที่สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน

๒) ต้องประกาศนโยบายและข้อปฏิบัติ ให้ผู้ที่เกี่ยวข้องทราบ เพื่อให้สามารถเข้าถึง เข้าใจ และปฏิบัติตามได้

๓) ต้องกำหนดผู้รับผิดชอบตามนโยบายและข้อปฏิบัติ ให้ชัดเจน

๔) ต้องทบทวนปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๓.๔ ข้อกำหนดในการรักษาความมั่นคงปลอดภัย

ต้องมีอย่างน้อย ๑๐ ข้อ

๑) การเข้าถึงและควบคุมการใช้งานสารสนเทศ (access control)

๒) การใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (business requirements for access control)

๓) การบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management)

๔) การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities)

๕) การควบคุมการเข้าถึงเครือข่าย (network access control)

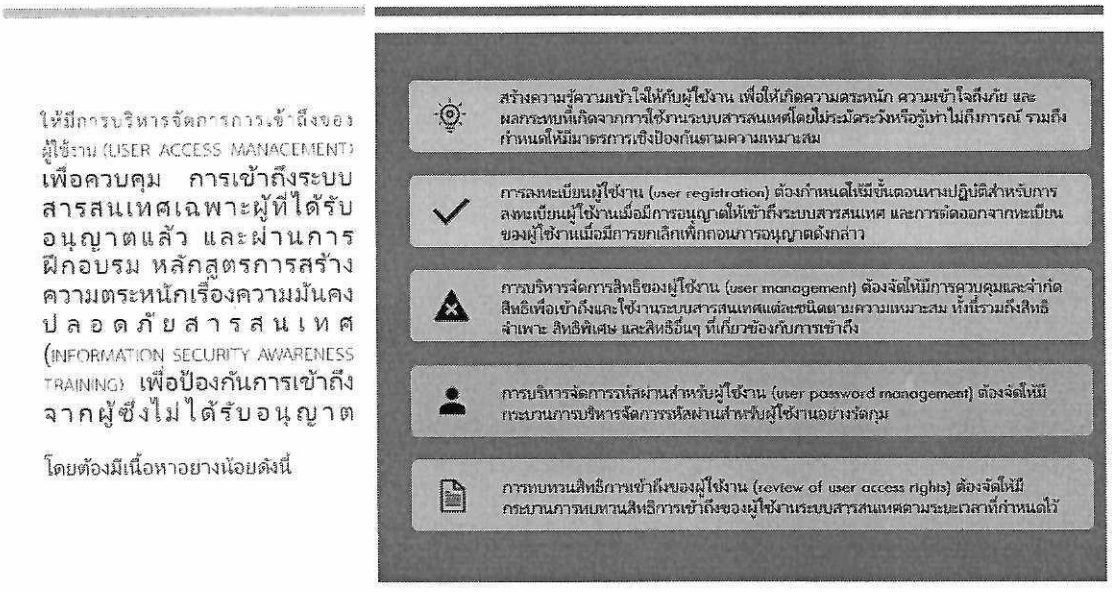
๖) การควบคุมการเข้าถึงระบบปฏิบัติการ (operating system access control)

๗) การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (application and information access control)

๘) การจัดทำระบบสำรอง

๙) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

๑๐) การกำหนดความรับผิดชอบที่ชัดเจน กรณีเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กร หรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติ



๑. การใช้งานแต่รหัสผ่าน (password use) ต้องกำหนดแนวปฏิบัติที่ดีสำหรับผู้ใช้งานในการกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ

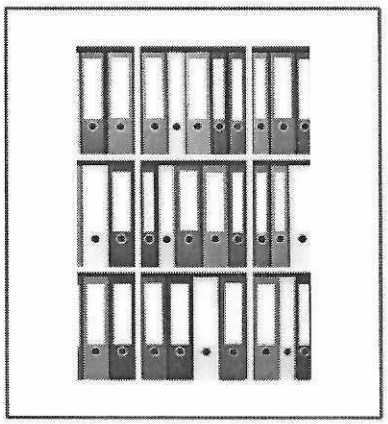
๒. การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ ต้องกำหนดข้อปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล

๓. การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (clear desk and clear screen policy) ต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูลคอมพิวเตอร์ หรือสารสนเทศอยู่ในภาวะซึ่งเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

๔. ผู้ใช้งานอาจนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔

หน่วยงานของรัฐที่มีระบบสารสนเทศต้องจัดทำระบบสำรอง ตามแนวทางต่อไปนี้

- จัดหาอุปกรณ์ที่จำเป็นและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานที่เหมาะสม
- จัดจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามประเภทอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินอย่างสม่ำเสมอ ให้สามารถนำไปใช้ได้อย่างเหมาะสม และสอดคล้องกับการใช้งานตามภารกิจ
- ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลเกี่ยวข้องกับระบบสารสนเทศระบบสำรอง และการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์
- ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และแผนเตรียมความพร้อมกรณีฉุกเฉินอย่างสม่ำเสมอ
- สำหรับความถี่ของการปฏิบัติในแต่ละข้อ หากมีการปฏิบัติที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน



ต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยต้องมีเนื้อหาอย่างน้อย ดังนี้

ต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (information security audit and assessment) อย่างน้อยปีละหนึ่งครั้ง

ในการตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการโดยผู้ตรวจสอบภายในหน่วยงานของรัฐ (internal auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (external auditor)เพื่อให้หน่วยงานของรัฐได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศของหน่วยงาน

การจัดทำแผนการปฏิบัติงานตรวจสอบการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

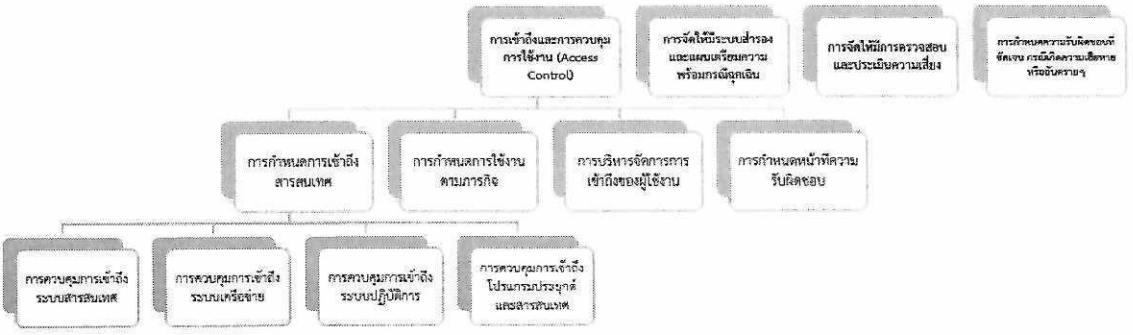
ประเด็นการตรวจสอบ

ประเด็นที่ 1 นโยบายและข้อปฏิบัติของหน่วยงานเป็นไปตามกฎหมายและประกาศคณะกรรมการธุรกรรมฯ

1	2	3	4
การจัดทำนโยบายการรักษาความมั่นคงปลอดภัยและข้อปฏิบัติคลอบคลุมข้อกำหนดตามกฎหมายและประกาศคณะกรรมการธุรกรรมฯ	การเผยแพร่นโยบายและข้อปฏิบัติ ให้ผู้ที่เกี่ยวข้องทราบสามารถเข้าถึงเข้าใจและปฏิบัติตามได้	กำหนดผู้รับผิดชอบตามนโยบายและข้อปฏิบัติที่ชัดเจน	ทบทวนนโยบายและข้อปฏิบัติให้เป็นปัจจุบันอยู่เสมอ

ประเด็นการตรวจสอบ

ประเด็นที่ 2 หน่วยงานมีการปฏิบัติเป็นไปตามประกาศคณะกรรมการธุรกรรมฯ



โจทย์การฝึกปฏิบัติ

๑. การจัดทำแนวนโยบายและแนวปฏิบัติของหน่วยงานของท่านว่า เป็นไปตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๙ มาตรา ๕ และมาตรา ๗ รวมถึงประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ และที่แก้ไขเพิ่มเติม ฉบับที่ ๒ พ.ศ. ๒๕๕๖

๒. การบันทึกข้อมูลในกระดาษทำการที่เกี่ยวข้องให้สมบูรณ์ หากผลการตรวจสอบพบว่า

๒.๑ หน่วยงานของท่านไม่มีการจัดทำแผนการตรวจสอบและบำรุงรักษาสายไฟฟ้าและสายเคเบิลต่าง ๆ ภายในงานสารสนเทศ อย่างสม่ำเสมอ แต่จะทำการซ่อมแซมเมื่อเกิดความเสียหาย

๒.๒ เมื่อนักศึกษาจบการศึกษาหรือบุคลากรของหน่วยงานลาออก ไม่มีการทบทวนตัดสิทธิ์ในการเข้าใช้ระบบสารสนเทศของหน่วยงาน

๒.๓ กรณีที่เกิดความเสียหายอันเกิดจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ หน่วยงานท่านกำหนดให้เป็นความรับผิดชอบของ CIO ของหน่วยงานของท่าน

๒.๔ กรณีหน่วยงาน Outsource มาพัฒนาโปรแกรม พบว่า หลังดำเนินการเสร็จ ผู้พัฒนาโปรแกรมไม่ส่ง source code และได้นำโปรแกรมที่พัฒนาไปปรับปรุงขายให้กับหน่วยงานอื่น นอกจากยังสามารถเข้าใช้งานในฐานะ admin ของโปรแกรมจากนอกสำนักงานได้ด้วย และยังพบว่า การกำหนดรหัสผ่านของผู้ใช้งานยังไม่เป็นตามแนวปฏิบัติในการกำหนดรหัสผ่านตามข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยของมหาวิทยาลัยด้วย

โดยแบ่งกลุ่มจัดทำกระดาษทำการ เพื่อสรุปผลการตรวจสอบที่ตรวจพบ ตามข้อตรวจพบจำนวน ๔ ข้อ

๓. การจัดทำรายงานผลการดำเนินงานของคณะกรรมการตรวจสอบภายในประจำมหาวิทยาลัยตามหลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานการตรวจสอบภายในสำหรับหน่วยงานของรัฐ พ.ศ. ๒๕๖๑ และที่แก้ไข

การจัดทำรายงานผลการดำเนินงานของคณะกรรมการตรวจสอบภายในประจำมหาวิทยาลัยตามหลักเกณฑ์ฯ ควรมีการรายงานงบกระแสเงินสดไว้ในรายงานด้วย เพื่อให้ผู้บริหารได้รับทราบถึงการหมุนเวียนของงบกระแสเงินสด

<u>เอกสารที่ได้รับจากการเข้าร่วมอบรม</u>

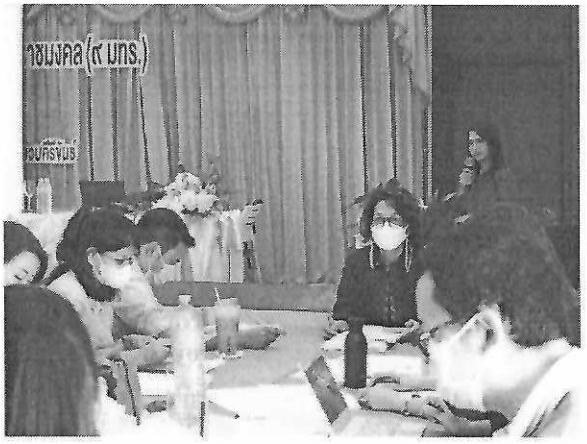
๑. พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙

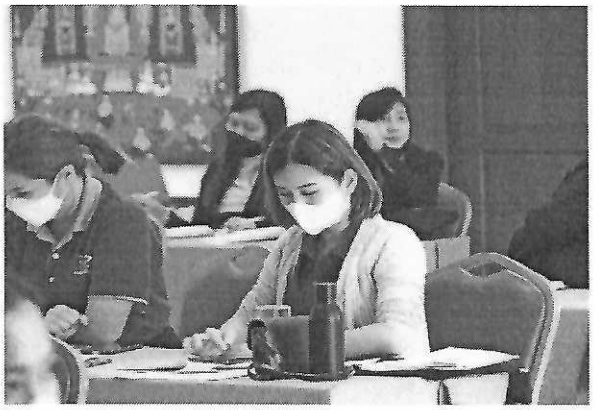
๒. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓

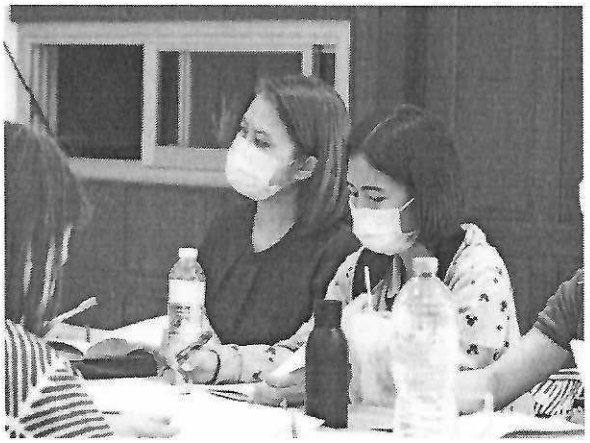
๓. เอกสารบรรยายการตรวจสอบการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๔. แผนการปฏิบัติงานตรวจสอบ การตรวจสอบการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

รูปภาพ


ราชมงคล(๙ มทร.)





ผู้จัดทำ

๑. นางสาวโสภา	เภสัชพิพัฒน์กุล	ตำแหน่ง รักษาราชการแทน หัวหน้าสำนักงานตรวจสอบภายใน
๒. นางสาวประศิภรณ์	ทิพย์อุทัย	ตำแหน่ง นักตรวจสอบภายใน มทร.ล้านนา
๓. นางนงคราญ	สีไชย	ตำแหน่ง นักตรวจสอบภายใน มทร.ล้านนา
๔. นายเอกชัย	ต๊ะบุญธง	ตำแหน่ง นักตรวจสอบภายใน มทร.ล้านนา
๕. นางสาวศรัญญา	ศรีสัตนา	ตำแหน่ง นักตรวจสอบภายใน มทร.ล้านนา พิษณุโลก
๖. นางชื่นหทัย	เมฆขยาย	ตำแหน่ง นักตรวจสอบภายใน มทร.ล้านนา เชียงราย
๗. นางสาวสุพรรษา	คุณาพันธ์	ตำแหน่ง นักตรวจสอบภายใน มทร.ล้านนา ลำปาง
๘. ว่าที่ร้อยตรีหญิงมนสิชา	นารีรักษ์	ตำแหน่ง นักตรวจสอบภายใน สวก.

ความคิดเห็นของหัวหน้าสำนักงานตรวจสอบภายใน

๑. การนำองค์ความรู้ที่ได้รับมาประยุกต์ใช้โครงสร้าง บทบาท หน้าที่ และความรับผิดชอบ ในการรักษาความมั่นคงปลอดภัย สารสนเทศของ มทร.ล้านนา มีดังนี้

๑) มทร.ล้านนา ต้องมีการปฏิบัติตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.๒๕๔๙ มาตรา ๗ แนวนโยบายและแนวปฏิบัติตามมาตรา ๕ และมาตรา ๖ ให้หน่วยงานของรัฐจัดทำเป็นประกาศ และต้องได้รับความเห็นชอบจากคณะกรรมการหรือหน่วยงานที่คณะกรรมการมอบหมาย จึงมีผลใช้บังคับได้ หน่วยงานของรัฐต้องปฏิบัติตามแนวนโยบายและแนวปฏิบัติที่ได้แสดงไว้ และให้จัดให้มีการตรวจสอบการปฏิบัติตามแนวนโยบายและแนวปฏิบัติที่กำหนดไว้อย่างสม่ำเสมอ

๒) กรณีหากมทร.ล้านนา ยังไม่ได้มีการปฏิบัติตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.๒๕๔๙ มาตรา ๗ มทร.ล้านนา ควรดำเนินการดังนี้

๒.๑) แต่งตั้งผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer: CIO) มีหน้าที่อนุมัติการใช้งานนโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ ในกรณีพบความเสี่ยงด้านเทคโนโลยีสารสนเทศที่อยู่ในระดับที่สำนักงานยอมรับไม่ได้ และมีข้อจำกัดหรือเหตุผลทำให้ไม่สามารถแก้ไขและควบคุมความเสี่ยงนั้นได้ ให้ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงเป็นผู้พิจารณายอมรับความเสี่ยงนั้น หรือเสนอแนะแนวทางอื่นในการแก้ไข โดยคำนึงถึงผลกระทบที่อาจจะเกิดขึ้น

๒.๒) นำนโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศที่ได้กำหนดตามข้อ ๒.๑ เสนอคณะกรรมการบริหารมหาวิทยาลัย (Chief Executive Officer : CEO) เพื่อพิจารณา เนื่องจากตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ (ฉบับที่ ๒) พ.ศ.๒๕๕๖ ข้อ ๒ ได้กำหนดข้อ ๑๔ ว่า “หน่วยงานของรัฐต้องกำหนดความรับผิดชอบที่ชัดเจน กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ทั้งนี้ ให้ผู้บริหารระดับสูงของหน่วยงาน (Chief Executive Officer : CEO) เป็นผู้รับผิดชอบต่อความเสียหาย หรืออันตรายที่เกิดขึ้น”

๒.๓) นำนโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศที่ได้กำหนดตามข้อ ๒.๒ เสนอต่อสภามหาวิทยาลัยเพื่อพิจารณา

๒.๔) นำนโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศที่ได้กำหนดตามข้อ ๒.๓ ปฏิบัติตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.๒๕๔๙ มาตรา ๗ กล่าวคือ “ต้องได้รับความเห็นชอบจากคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ (อาจใช้เวลาในการให้ความเห็นชอบประมาณ ๓ ปี)”

๒.๕) เมื่อนโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศผ่านความเห็นชอบจากคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์แล้ว มทร.ล้านนา ต้องทบทวนให้มีความเป็นปัจจุบันปีละ ๑ ครั้ง และนำเสนอต่อสภามหาวิทยาลัยเพื่อทราบ

กรณีมีการปรับปรุง นโยบายและแนวประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ มทร.ล้านนา โดย CIO ต้องดำเนินการปรับปรุงแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้มีความสอดคล้อง นำเสนอ CEO และสภามหาวิทยาลัยเพื่อพิจารณา รวมถึงต้องได้รับความเห็นชอบจากคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

๒. การนำองค์ความรู้ที่ได้รับมาประยุกต์ใช้ในงานตรวจสอบภายใน ของสำนักงานตรวจสอบภายใน ดังนี้

๒.๑ ปฏิบัติตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ.๒๕๕๓ ข้อ ๑๓ หน่วยงานของรัฐต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยต้องมีเนื้อหาอย่างน้อย ดังนี้

(๑) หน่วยงานของรัฐต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง

(๒) ในการตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการ โดยผู้ตรวจสอบภายในของหน่วยงานของรัฐ หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก เพื่อให้หน่วยงานของรัฐได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศของหน่วยงาน

๒.๒ ดังนั้น ในการจัดทำแผนการตรวจสอบภายในประจำปีงบประมาณ พ.ศ.๒๕๖๖ จึงต้องกำหนดเป็นกิจกรรมการตรวจสอบ ทั้งนี้ ได้เห็นชอบร่วมกันให้มีการตรวจสอบแบบบูรณาการ และได้นำผลการฝึกปฏิบัติการบันทึกข้อมูลในกระดาษทำการที่ได้จากการเข้าร่วมโครงการ มาถ่ายทอดองค์ความรู้ให้กับผู้ตรวจสอบภายในที่ไม่ได้เข้าร่วมโครงการได้นำมาใช้ในการปฏิบัติงานต่อไป

ลงชื่อ.....โสภา.....

(นางสาวโสภา เภสัชพิพัฒน์กุล)

รักษาราชการแทน หัวหน้าสำนักงานตรวจสอบภายใน

๒๕ สิงหาคม ๒๕๖๕