



เหตุผล 3 ประการ

...ที่มหาวิทยาลัย**ต้องทำ**ระบบยืนยันตัวตน ก่อนใช้งานอินเทอร์เน็ต
เพื่อช่วยสร้างเครือข่ายที่ ปลอดภัย มีประสิทธิภาพ และตรวจสอบได้



ความรับผิดชอบและกฎหมาย



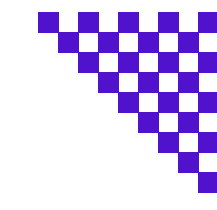
การบริหารจัดการเครือข่าย



ความปลอดภัย

ความรับผิดชอบและกฎหมาย

ACCOUNTABILITY AND LEGAL COMPLIANCE



การยืนยันตัวตน ทำให้สามารถระบุได้ว่า..
ใครทำอะไรบนเครือข่าย ซึ่งเป็น**สิ่งจำเป็น**
ตามกฎหมายและข้อบังคับ



ปฏิบัติตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

กฎหมายกำหนดให้ผู้ให้บริการอินเทอร์เน็ต (ซึ่งในที่นี้คือมหาวิทยาลัย) ต้องเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ของผู้ใช้งานไว้เป็นเวลาอย่างน้อย 90 วัน เพื่อใช้เป็นหลักฐานในกรณีที่เกิดการกระทำความผิด เช่น การหมิ่นประมาท การเผยแพร่เนื้อหาที่ผิดกฎหมาย หรือการแฮกข้อมูล



ตรวจสอบเมื่อเกิดปัญหา

หากมีการกระทำที่ผิดกฎหมายหรือผิดนโยบายของมหาวิทยาลัยเกิดขึ้นผ่านเครือข่าย การมีระบบยืนยันตัวตน จะช่วยให้สามารถติดตามและระบุตัวตนผู้กระทำผิดเพื่อรับผิดชอบได้



การบริหารจัดการเครือข่าย NETWORK MANAGEMENT



จัดสรรแบนด์วิดท์อย่างเหมาะสม

ผู้ดูแลระบบสามารถจำกัดความเร็วอินเทอร์เน็ตของผู้ใช้แต่ละคนได้ เพื่อป้องกันไม่ให้มีใครใช้งานหนักเกินไป เช่น การโหลดไฟล์ขนาดใหญ่ตลอดเวลา จนทำให้คนอื่นใช้งานอินเทอร์เน็ตช้าลงไปด้วย



บริหารสิทธิ์การเข้าถึงทรัพยากร

มหาวิทยาลัยสามารถกำหนดสิทธิ์การเข้าถึงทรัพยากรต่าง ๆ ตามประเภทของผู้ใช้งานได้ เช่น นักศึกษาสามารถเข้าถึงเว็บไซต์เพื่อการเรียนรู้และฐานข้อมูลห้องสมุดได้ ในขณะที่อาจารย์สามารถเข้าถึงระบบสร้างเนื้อหาการสอนออนไลน์ได้



วิเคราะห์และวางแผนการใช้งาน

ข้อมูลการล็อกอินช่วยให้มหาวิทยาลัยทราบว่าช่วงเวลาไหนมีคนใช้งานอินเทอร์เน็ตหนาแน่นที่สุด หรือพื้นที่ไหนในมหาวิทยาลัยมีการใช้งานสูงสุด เพื่อนำไปวางแผนขยายหรือปรับปรุงเครือข่ายในอนาคตได้

3

ความปลอดภัย: Security



ป้องกันการเข้าถึงจากบุคคลภายนอก

มหาวิทยาลัยมีข้อมูลสำคัญมากมาย เช่น งานวิจัยของคณาจารย์ ข้อมูลส่วนตัวของนักศึกษาและบุคลากร การยืนยันตัวตนจะช่วยป้องกันไม่ให้ผู้ที่ไม่เกี่ยวข้องเข้ามาในเครือข่ายเพื่องโมยข้อมูลหรือสร้างความเสียหายได้



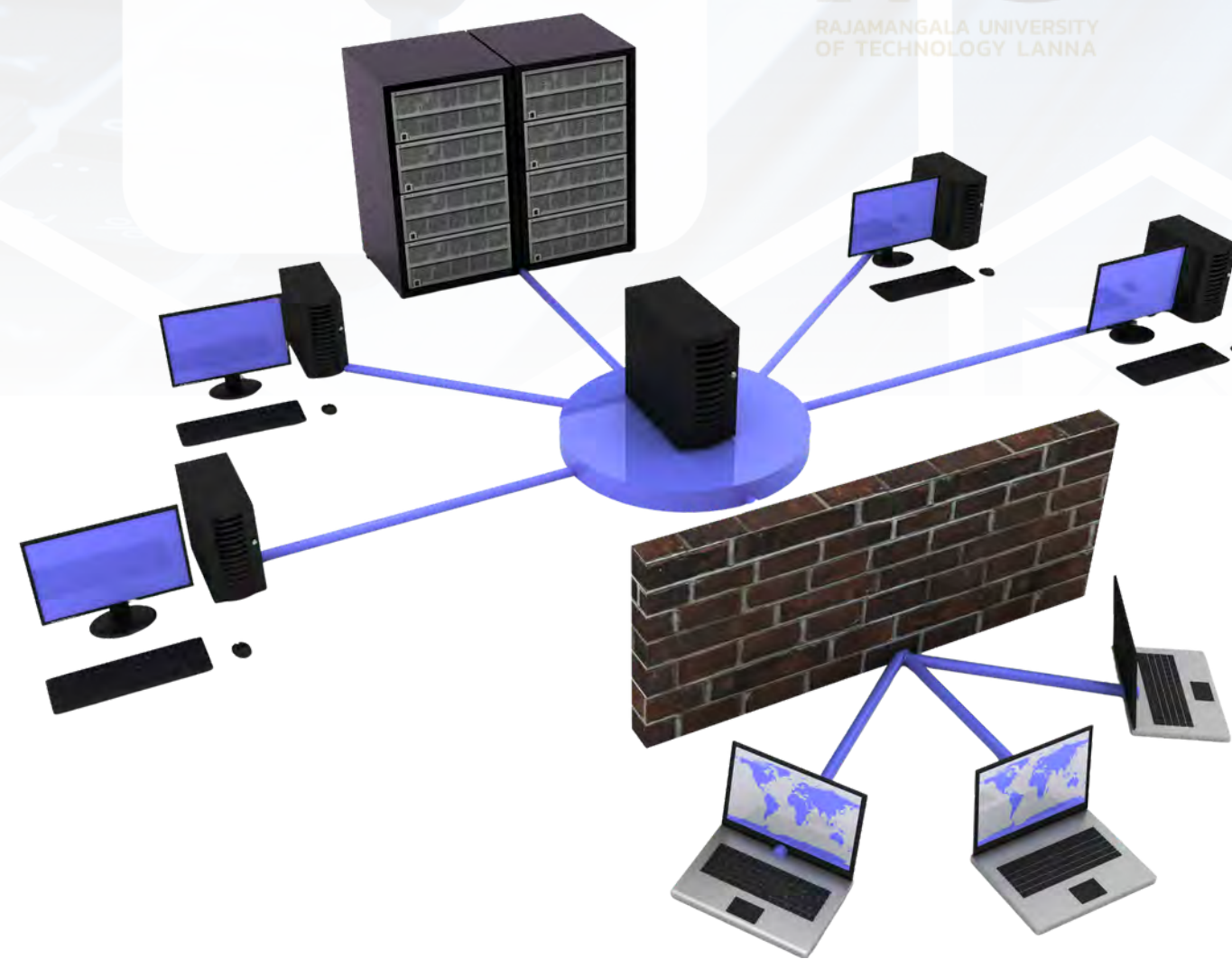
ลดความเสี่ยงการแพร่กระจายมัลแวร์

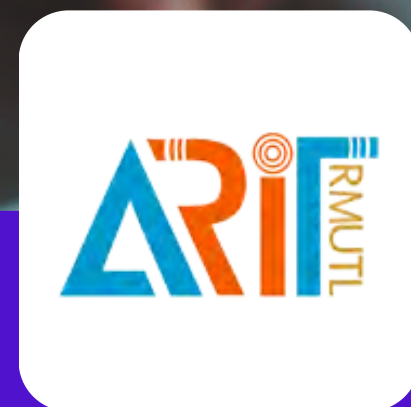
หากมีอุปกรณ์ที่ติดไวรัสหรือมัลแวร์เชื่อมต่อเข้ามาในระบบ การที่ทราบว่าใครเป็นเจ้าของจะช่วยให้ผู้ดูแลระบบสามารถแจ้งเตือนและตัดการเชื่อมต่อของอุปกรณ์นั้นออกจากเครือข่ายได้อย่างรวดเร็ว เพื่อไม่ให้แพร่กระจายไปยังคอมพิวเตอร์เครื่องอื่น ๆ



ป้องกันการโจมตีจากภายในเครือข่าย

การยืนยันตัวตนช่วยลดความเสี่ยงจากการที่บุคคลใดบุคคลหนึ่งใช้เครือข่ายของมหาวิทยาลัยเป็นฐานในการโจมตีระบบอื่น ๆ ทั้งภายในและภายนอก





ระบบยืนยันตัวตน =  ความรับผิดชอบและกฎหมาย +  การบริหารจัดการเครือข่าย +  ความปลอดภัย

ช่วยสร้างเครือข่ายที่ ปลอดภัย มีประสิทธิภาพ และตรวจสอบได้