ประกาศมหาวิทยาลัยราชภัฏสวนสุนันทา

เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Policy)

ของมหาวิทยาลัยราชภัฏสวนสุนันทา

เพื่อให้การดำเนินการเกี่ยวกับการรักษาความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศของมหาวิทยาลัยราชภัฏสวนสุนันทาเป็นไปตามกฎหมายและมาตรฐานสากล

อาศัยอำนาจตามความในมาตรา ๓๑(๑) แห่งพระราชบัญญัติมหาวิทยาลัยราชภัฏ พ.ศ. ๒๕๔๗ ประกอบ มาตรา ๔๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์พ.ศ. ๒๕๖๒ กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้การดำเนินกิจกรรมหรือการให้บริการต่างๆ มีความมั่นคงปลอดภัยเชื่อถือได้

มหาวิทยาลัยราชภัฏสวนสุนันทาจึงได้กำหนดแนวนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ขึ้นเพื่อกำหนดทิศทาง หลักการ และกรอบของข้อกำหนดในการป้องกันทรัพย์สินที่เกี่ยวข้องกับสารสนเทศให้ปลอดภัยจากภัยคุกคามที่อาจก่อให้เกิดความเสียหายต่อการรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้ (Availability) ของข้อมูลและระบบงานสารสนเทศ เพื่อผลักดันให้มีการควบคุมภายในมหาวิทยาลัยด้านสารสนเทศที่รัดกุมตามแนวความเสี่ยง (Risk Based Approach) ที่สอดคล้องกับมาตรฐานสากล และเพื่อสนับสนุนให้ผู้ใช้งานตระหนักถึงความสำคัญของความมั่นคงปลอดภัยด้านไซเบอร์ รวมถึงความสำคัญในการบริหารจัดการความเสี่ยงด้านไซเบอร์และสารสนเทศ ดังนี้

๑. วัตถุประสงค์

๑.๑. เพื่อกำหนดมาตรฐานแนวทางปฏิบัติของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัยราชภัฏสวนสุนันทาเป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

๑.๒. เพื่อให้เกิดความเชื่อมั่นด้านความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัยราชภัฏสวนสุนันทาและทำให้ดำเนินงานต่างๆเป็นไปอย่างมีประสิทธิภาพและประสิทธิผล

๑.๓. เพื่อเผยแพร่นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้ผู้บริหาร เจ้าหน้าที่ทุกระดับ นักศึกษา นักเรียน และบุคคลภายนอกที่ปฏิบัติงานให้กับองค์กรมีความรู้ความเข้าใจและตระหนักถึงความสำคัญและถือปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

๑.๔. เพื่อให้มีระบบตรวจสอบและประเมินความเสี่ยงในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศอย่างสม่ำเสมอทุกปี

๑.๕ เพื่อใช้บังคับกับผู้บริหาร พนักงาน ลูกจ้าง นักศึกษา นักเรียน และผู้ที่ทำงานหรือปฏิบัติงานให้กับมหาวิทยาลัย

๒. คำนิยาม

ผู้บริหาร บุคลากร และผู้รับบริการ (Employee) หมายถึง ผู้บริหาร บุคลากร และ ผู้รับบริการที่ได้รับการว่าจ้างให้ทำงานเป็นผู้บริหาร บุคลากร และผู้รับบริการทดลองงาน ผู้บริหาร บุคลากร และผู้รับบริการประจำ ผู้บริหาร บุคลากร และผู้รับบริการสัญญาจ้างพิเศษ และผู้บริหารทุกระดับที่อยู่ภายใต้ การจ้างงานของมหาวิทยาลัย

ผู้ใช้งาน (User) หมายถึง ผู้บริหาร บุคลากร และผู้รับบริการของมหาวิทยาลัย รวมไปถึงบุคคลภายนอกหน่วยงานที่ได้รับอนุญาตให้มีรหัสเข้าใช้งานในบัญชีรายชื่อผู้สามารถเข้าใช้งาน หรือ/ และ มีรหัสผ่านเพื่อเข้าใช้งานอุปกรณ์ประมวลผลสารสนเทศของมหาวิทยาลัย

ผู้บังคับบัญชา หมายถึง ผู้บริหาร บุคลากร และผู้รับบริการซึ่งเป็นผู้บังคับบัญชาของหน่วยงานภายในตามโครงสร้างของมหาวิทยาลัย

ระบบคอมพิวเตอร์ (Computer System) หมายถึง เครื่องมือ หรืออุปกรณ์คอมพิวเตอร์ ทุกชนิดทั้ง Hardware และ Software ทุกขนาด อุปกรณ์เครือข่ายเชื่อมโยงข้อมูลทั้งชนิดมีสายและไร้สาย วัสดุ อุปกรณ์การเก็บรักษา และการถ่ายโอนข้อมูลชนิดต่าง ๆ ระบบ Internet และระบบ Intranet รวมถึง อุปกรณ์ไฟฟ้าและสื่อสารโทรคมนาคมต่าง ๆ ที่สามารถทำงาน หรือใช้งานได้ในลักษณะเช่นเดียวกัน หรือ คล้ายคลึงกับคอมพิวเตอร์ ทั้งที่เป็นทรัพย์สินของมหาวิทยาลัยของ คู่ค้าของมหาวิทยาลัยของ และ หน่วยงานอื่นที่อยู่ระหว่างการติดตั้ง และยังไม่ได้ส่งมอบ หรือของผู้บริหาร บุคลากร และผู้รับบริการที่นำเข้ามาติดตั้ง หรือใช้งานภายในเครือข่ายของมหาวิทยาลัย

ข้อมูลสารสนเทศ (Information Technology) หมายถึง ข้อมูล ข่าวสาร บันทึก ประวัติ ข้อความในเอกสาร โปรแกรมคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์รูปภาพ เสียง เครื่องหมาย และสัญลักษณ์ต่าง ๆ ไม่ว่าจะเก็บไว้ในรูปแบบที่สามารถสื่อความหมายให้บุคคลสามารถเข้าใจได้โดยตรง หรือผ่านเครื่องมือ หรือ อุปกรณ์ใด ๆ

ข้อมูลสำคัญ หรือ ข้อมูลที่เป็นความลับ (Sensitive Information) หมายถึง ข้อมูล สารสนเทศที่มีความสำคัญต่อภาระกิจและการดำเนินงานของมหาวิทยาลัย หรือที่หน่วยงาน มีพันธะ ผูกพันตามข้อกำหนดของกฎหมาย จรรยาบรรณในการประกอบวิชาชีพ หรือสัญญาซึ่งหน่วยงาน ไม่อาจนำไปเปิดเผยต่อบุคคลอื่นหรือนำไปใช้ประโยชน์อย่างอื่น นอกเหนือจากวัตถุประสงค์ในการดำเนินงานของของมหาวิทยาลัย การรั่วไหลของข้อมูลสำคัญ หรือข้อมูลที่เป็นความลับดังกล่าวอาจเป็นเหตุให้การดำเนินงานของมหาวิทยาลัย ต้องหยุดชะงัก ขาดประสิทธิภาพ หรือหน่วยงานเสื่อมเสียชื่อเสียง

ระบบที่มีความสำคัญ (Important System) หมายถึง ระบบคอมพิวเตอร์ที่หน่วยงานใช้ประโยชน์ เพื่อให้บริการงานทะเบียนนักศึกษาทั้งระบบ รวมถึงระบบอิเล็กทรอนิกส์อื่นใดที่ช่วยในการดำเนินงาน ทะเบียนนักศึกษาของมหาวิทยาลัยให้เป็นปกติ และระบบที่ได้รับการกำหนดโดยหน่วยงานด้านความปลอดภัยข้อมูลและระบบสารสนเทศของมหาวิทยาลัย ทั้งนี้หากระบบที่มีความสำคัญ ดังกล่าวหยุดการทำงาน หรือมีความสามารถในการทำงานที่ลดถอยลงจะทำให้การดำเนินงานทะเบียนนักศึกษาของมหาวิทยาลัย การทะเบียนต้องหยุดชะงัก หรือด้อยประสิทธิภาพ

ทรัพย์สินสารสนเทศ(Asset) ทรัพย์สินสารสนเทศของมหาวิทยาลัย ประกอบด้วยทรัพย์สินสารสนเทศในหมวดหมู่ต่าง ๆ เช่น ข้อมูล (Information) ฮาร์ดแวร์ (Hardware) ซอฟต์แวร์ (Software) เป็นต้น

เจ้าของระบบ (System Owner) หมายถึง หน่วยงานภายในซึ่งเป็นเจ้าของระบบคอมพิวเตอร์ และมีความรับผิดชอบในระบบคอมพิวเตอร์นั้น ๆ

เจ้าของทรัพย์สิน (Asset Owner) หมายถึง ผู้ที่ได้รับมอบหมายจากเจ้าของระบบคอมพิวเตอร์หรือ ข้อมูลสารสนเทศในการสนับสนุนงานการดูแล จัดการ และควบคุมการเข้าใช้ข้อมูลสารสนเทศให้เป็นไปตามข้อกำหนดหรือระดับสิทธิที่เจ้าของระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศกำหนด

ผู้ดูแลระบบ (Administrator) หมายถึง ผู้ที่ได้รับมอบหมายให้ดูแลใช้งาน และบำรุงรักษา ระบบคอมพิวเตอร์ทั้งอุปกรณ์ Hardware Software และอุปกรณ์ต่อพ่วงที่ประกอบกันขึ้นเป็นระบบคอมพิวเตอร์ ผู้ดูแลระบบจะเป็นผู้ที่ได้รับอนุญาตให้มีอำนาจในการปรับเปลี่ยน เพิ่มเติม แก้ไข ปรับปรุงให้ระบบคอมพิวเตอร์ของมหาวิทยาลัย ทำงานได้อย่างถูกต้อง มีประสิทธิภาพสอดคล้องกับความต้องการดำเนินงานด้านทะเบียนนักศึกษา และมีความปลอดภัย

การรักษาความมั่นคงปลอดภัยหรือ ความมั่นคงปลอดภัย (Security) หมายถึง กระบวนการและการกระทำใด ๆ เช่น การป้องกัน การเข้มงวดกวดขัน การระมัดระวัง การเอาใจใส่ในการใช้งาน และการดูแลรักษาระบบคอมพิวเตอร์ และข้อมูลสารสนเทศที่เป็นระบบและข้อมูลสำคัญให้พ้นจากความพยายามใด ๆ ทั้งจากผู้บริหาร บุคลากร และผู้รับบริการภายใน และจากบุคคลภายนอกในการเข้าถึง เพื่อโจรกรรมทำลาย หรือแทรกแซงการทำงาน จนเป็นเหตุให้การดำเนินงานของมหาวิทยาลัยได้รับความเสียหาย

๓. หลักการปฏิบัติในการรักษาความมั่นคงปลอดภัย (Security Principles)

หลักการปฏิบัติในการรักษาความมั่นคงปลอดภัยนี้ มีหลักการเพื่อให้บรรลุผลตามวัตถุประสงค์ ดังต่อไปนี้

๓.๑. ความลับ (Confidentiality) การปกป้องความลับของข้อมูล โดยป้องกันการเข้าถึง และการเปิดเผยข้อมูลจากผู้ที่ไม่ได้รับอนุญาต รวมไปถึงข้อมูลส่วนบุคคลหรือข้อมูลที่เป็นกรรมสิทธิ์ของมหาวิทยาลัย

๓.๒. ความถูกต้อง (Integrity) การทำให้มั่นใจว่าข้อมูลของมหาวิทยาลัย ไม่ถูกแก้ไข ดัดแปลง หรือโดนทำลายโดยผู้ที่ไม่ได้รับอนุญาต

๓.๓. ความพร้อมใช้งาน (Availability) การทำให้มั่นใจว่าผู้ใช้งานที่ได้รับอนุญาตสามารถเข้าถึง ข้อมูลและบริการได้อย่างรวดเร็วและเชื่อถือได้

๓.๔. ความรับผิดชอบ (Accountability) การระบุหน้าที่ความรับผิดชอบของแต่ละบุคคล รวมถึงการรับ ผิดและรับชอบในผลของกระทำตามบทบาทหน้าที่นั้นๆ

๓.๕. การพิสูจน์ตัวตน (Authentication) การทำให้มั่นใจว่าสิทธิการเข้าใช้งานระบบคอมพิวเตอร์และ ข้อมูลสารสนเทศต้องผ่านกระบวนการยืนยันตัวตนที่สมบูรณ์แล้วเท่านั้น

๓.๖. การกำหนดสิทธิ (Authorization) การทำให้มั่นใจว่าการให้สิทธิเข้าใช้งานระบบคอมพิวเตอร์และข้อมูลสารสนเทศเป็นไปตามความจำเป็น (Least Privilege) และสอดคล้องกับความต้องการพื้นฐาน (Need to Know Basis) ตามที่ได้รับอนุญาต

๓.๗. การห้ามปฏิเสธความรับผิดชอบ (Non-repudiation) การทำให้มั่นใจว่าผู้มีส่วนร่วม (parties) ที่เกี่ยวข้องในการทำธุรกรรมไม่สามารถปฏิเสธได้ว่าไม่มีส่วนเกี่ยวข้องกับการทำธุรกรรมที่เกิดขึ้น การรักษาความมั่นคงปลอดภัยอย่างได้ผล จำเป็นต้องมีข้อตกลงร่วมกันและได้รับความเอาใจใส่อย่างจริงจังในทุกเรื่องที่เกี่ยวข้อง อันประกอบไปด้วย

๑) การรักษาความปลอดภัยถือว่าเป็นหน้าที่ของผู้บริหาร บุคลากร และผู้รับบริการ และบุคคลภายนอกที่เกี่ยวข้องทุกคน

๒) การบริหารและการปฏิบัติในด้านการรักษาความมั่นคงปลอดภัยเป็นกระบวนการที่ต้องกระทำอย่างต่อเนื่องอยู่ตลอดเวลา

๓) การมีจิตสำนึก รู้จักหน้าที่ มีความรับผิดชอบ และใส่ใจที่จะกระทำตามข้อปฏิบัติ ที่กำหนดไว้ในนโยบาย มาตรฐาน กรอบการดำเนินงาน ขั้นตอนการปฏิบัติงาน คำแนะนำ และกระบวนการต่างๆ ถือเป็นสิ่งสำคัญที่สุดในกระบวนการรักษาความมั่นคงปลอดภัย การอธิบายให้ผู้บริหาร บุคลากร และ ผู้รับบริการและบุคคลภายนอกทราบอย่างชัดเจนเพื่อให้มีความเข้าใจในหน้าที่และความรับผิดชอบในการ รักษาความปลอดภัยที่ตนเองรับผิดชอบเป็นสิ่งที่จะทำให้การรักษาความมั่นคงปลอดภัยดำเนินไปอย่างมีประสิทธิผล

๔. บทบาทหน้าที่และความรับผิดชอบ (Information security roles and responsibilities)

เพื่อขับเคลื่อนและดำเนินการให้เป็นไปตามเป้าหมาย มหาวิทยาลัยได้กำหนดบทบาทหน้าที่และความรับผิดชอบ ไว้ดังนี้

๔.๑. ผู้บังคับบัญชา มีบทบาทหน้าที่และความรับผิดชอบ ดังต่อไปนี้

๑) ชี้แจงให้ผู้บริหาร บุคลากร และผู้รับบริการทราบถึงนโยบาย มาตรฐาน กรอบการดำเนินงาน ขั้นตอนการปฏิบัติงาน วิธีการปฏิบัติ คำแนะนำ และกระบวนการต่าง ๆ ของมหาวิทยาลัยที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์

๒) ดูแล แนะนำและตักเตือน กรณีที่พบเห็นการปฏิบัติที่ไม่ถูกต้องหรือไม่เหมาะสม
๓) พิจารณาลงโทษทางวินัยแก่ผู้กระทำผิดอย่างเสมอภาค และเป็นธรรม

๔.๒. หน้าที่ของผู้บริหาร บุคลากร ผู้ปฏิบัติงาน และผู้รับบริการ มีบทบาทหน้าที่และความรับผิดชอบดังต่อไปนี้

๑) ต้องเรียนรู้ ทำความเข้าใจ และปฏิบัติตามนโยบาย มาตรฐาน กรอบการดำเนินงาน ขั้นตอนการปฏิบัติงาน วิธีการปฏิบัติ คำแนะนำ และกระบวนการต่าง ๆ ของมหาวิทยาลัยที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเคร่งครัด
๒) ให้ความร่วมมือกับหน่วยงานอย่างเต็มที่ในการป้องกันระบบคอมพิวเตอร์และข้อมูลสารสนเทศของมหาวิทยาลัย
๓) แจ้งให้หน่วยงานทราบทันที เมื่อพบเห็นการปฏิบัติที่ไม่พบเห็นการบุกรุกโจรกรรม ทำลาย แทรกแซงการทำงาน หรือจารกรรมที่อาจสร้างความเสียหายต่อหน่วยงาน

๔.๓. ผู้บริหาร บุคลากร ผู้ปฏิบัติงาน และผู้รับบริการที่ได้รับมอบหมายให้ใช้งานเครื่อง คอมพิวเตอร์ต้องปฏิบัติดังต่อไปนี้

๑) ต้องออกจากระบบ (Log-out, Log-off) ทุกระบบเมื่อไม่ได้ใช้งานเป็นเวลานาน และปิดเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงอื่นทันทีหลังเลิกงาน
๒) ต้องล็อคหน้าจอ (Lock Screen) แบบกำหนดรหัสผ่าน (Password) หากไม่ใช้งาน หรือไปทำกิจกรรมอย่างอื่นเป็นระยะเวลาสั้นๆ เพื่อป้องกันมิให้บุคคลอื่นลักลอบเข้าไปใช้งาน
๓) ต้องตรวจสอบข้อมูลที่นำมาลงในเครื่องคอมพิวเตอร์ของตนเองทุกครั้ง โดยใช้โปรแกรมป้องกันไวรัส (Anti-virus) ที่มีข้อมูลไวรัสที่ทันสมัย
๔) ต้องเก็บรักษารหัสผ่าน (Password) และรหัสอื่นใดที่หน่วยงานกำหนด เพื่อใช้ในการเข้าถึงระบบคอมพิวเตอร์ ข้อมูลสารสนเทศ หรือข้อมูลของมหาวิทยาลัย เป็นความลับส่วนตัว ผู้บริหาร บุคลากร และผู้รับบริการ ซึ่งจะต้องเก็บรักษาไว้มิให้ผู้อื่นล่วงรู้ และห้ามใช้ร่วมกันกับบุคคลอื่น ทั้งนี้ ผู้บริหาร บุคลากร และผู้รับบริการต้องเปลี่ยนรหัสผ่านและรหัสอื่นใดเมื่อรหัสเก่าหมดอายุตามระยะเวลาที่กำหนดหรือเมื่อผู้บริหาร บุคลากร และผู้รับบริการเห็นสมควรต้องทำการเปลี่ยนรหัสผ่าน
๕) ผู้บริหาร บุคลากร ผู้ปฏิบัติงาน และผู้รับบริการที่มีหน้าที่เกี่ยวข้องกับบุคคลภายนอกต้องจัดให้มีการควบคุมดูแลบุคคลภายนอกให้ปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ของมหาวิทยาลัย

๕. การบริหารจัดการความความเสี่ยงด้านความปลอดภัยไซเบอร์ (Cyber Security Risk Management)

กำหนดให้มหาวิทยาลัยต้องมีการบริหารจัดการความความเสี่ยงด้านความปลอดภัยไซเบอร์ เพื่อแสดงถึงการยอมรับความเสี่ยงและลดความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ โดยใช้วิธีการที่สอดคล้องกันในการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัย (Security Risk Management) รวมถึงมีมาตรการรักษาความมั่นคงปลอดภัยเพื่อปกป้องข้อมูลซึ่งสอดคล้องกับกระบวนการในการระบุและประเมินความเสี่ยง (Risk Identification and Assessment)

๖. การบริหารจัดการระบบ (System Management)

เพื่อให้มีมาตรการในการปกป้องทรัพย์สินของมหาวิทยาลัยอย่างเหมาะสม มหาวิทยาลัยจึงกำหนดแนวปฏิบัติไว้ ดังนี้

๖.๑. จัดทำนโยบายหรือกระบวนการจัดการทรัพย์สินสารสนเทศ และข้อกำหนดการใช้งานทรัพย์สินสารสนเทศและการปรับปรุงให้สอดคล้องกับมาตรฐาน

๖.๒. ทรัพย์สินทั้งหมดจะต้องกำหนดให้มีผู้ดูแลและเจ้าของอย่างชัดเจน โดยผู้เป็นเจ้าของทรัพย์สินดังกล่าวอาจระบุเป็นชื่อบุคคล หรือชื่อหน่วยงานได้

๖.๓. เจ้าของหรือผู้มีหน้าที่ดูแลทรัพย์สินสารสนเทศจัดทำรายการทรัพย์สินสารสนเทศโดยการระบุข้อมูลสารสนเทศและทรัพย์สินระบบสารสนเทศ และทบทวนรายการทรัพย์สินสารสนเทศอย่างสม่ำเสมอ

๖.๔. ทะเบียนทรัพย์สินด้านสารสนเทศ ต้องระบุผู้มีหน้าที่ดูแลควบคุมการใช้งาน และรับผิดชอบทรัพย์สินดังกล่าว พร้อมทั้งปรับปรุงแก้ไขข้อมูลให้มีความถูกต้องอยู่เสมอ

๖.๕. ผู้ที่เป็นเจ้าของทรัพย์สินจะต้องพิจารณากำหนด ทบทวนระดับชั้นความลับของข้อมูลในทรัพย์สินที่ตนเองเป็นเจ้าของ และต้องปฏิบัติตามการจัดการระดับชั้นความลับของข้อมูล

๖.๖. ต้องมีการประเมินความเสี่ยงตามแนวทางการจัดการความเสี่ยงของทรัพย์สิน เมื่อมีทรัพย์สินใหม่หรือทรัพย์สินที่มีการเปลี่ยนแปลงที่สำคัญเกิดขึ้น

๗. การบริหารจัดการหน่วยงานและบุคลากร (Human Resource Management)

เพื่อให้ผู้บริหาร บุคลากร ผู้รับบริการและบุคคลภายนอกที่ทำสัญญากับหน่วยงาน เข้าใจในหน้าที่ความรับผิดชอบของตนเอง รวมถึงตระหนักถึงการรักษาความมั่นคงปลอดภัยในการปฏิบัติ มหาวิทยาลัยจึงกำหนดแนวปฏิบัติไว้ ดังนี้

๗.๑. มาตรการก่อนการจ้างงาน (Screening) ในการพิจารณารับพนักงานเข้าทำงาน หรือการว่าจ้าง หน่วยงานหรือบุคคลภายนอก ให้มีการตรวจสอบประวัติหรือคุณสมบัติเพื่อให้เป็นไปตามกฎหมาย กฎระเบียบและจริยธรรมที่เกี่ยวข้อง โดยให้คำนึงถึงระดับชั้นความลับของข้อมูลสารสนเทศที่จะให้เข้าถึง

๗.๒. ส่งเสริมและสนับสนุนการให้ความรู้ความเข้าใจด้านความมั่นคงปลอดภัยสารสนเทศแก่พนักงานและผู้ให้บริการภายนอกที่เกี่ยวข้อง และคณะผู้บริหารฯ จะต้องให้ความร่วมมือและสนับสนุน เพื่อให้สามารถดำเนินการตามนโยบายและวิธีปฏิบัติที่กำหนด รวมถึงการลงโทษหากพบว่ามีการละเมิดนโยบายหรือวิธีปฏิบัติที่กำหนดไว้

๗.๓. ต้องจัดให้มีการอบรมให้ความรู้เกี่ยวกับการรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศและด้านความปลอดภัยไซเบอร์ แก่ผู้ใช้งาน อย่างน้อยปีละ ๑ ครั้ง

๗.๔. ต้องมีการจัดทำข้อตกลงการรักษาความลับ หรือสัญญาไม่เปิดเผยข้อมูล (Non-Disclosure Agreement) และเงื่อนไขการจ้างงานอย่างเป็นลายลักษณ์อักษรกับพนักงาน ลูกจ้างชั่วคราว ผู้ให้บริการภายนอกที่เกี่ยวข้องและปฏิบัติตามอย่างเคร่งครัด

๗.๕. ผู้ดูแลระบบ จะต้องยกเลิกสิทธิของผู้ใช้งานหรือบุคคลภายนอกในการเข้าใช้งานสารสนเทศ เมื่อสิ้นสุดสถานะการเป็นพนักงาน หรือสิ้นสุดสัญญาหรือข้อตกลงการปฏิบัติงาน และให้ปรับเปลี่ยนระดับสิทธิในการเข้าใช้งานระบบสารสนเทศให้เหมาะสมเมื่อมีการเปลี่ยนแปลงหน้าที่ความรับผิดชอบใด ๆ เกิดขึ้น

๘. การรักษาความมั่นคงปลอดภัยสถานที่และอุปกรณ์ (Physical and Equipment Security)

เพื่อป้องกันการเข้าถึงสถานที่และอุปกรณ์โดยไม่ได้รับอนุญาต ซึ่งอาจทำให้เกิดความ เสียหายและการแทรกแซงการทำงานต่อระบบคอมพิวเตอร์ของมหาวิทยาลัย มหาวิทยาลัยจึงกำหนดแนวปฏิบัติไว้ ดังนี้

๘.๑. ต้องมีการจำแนก และกำหนดบริเวณพื้นที่ใช้งานระบบสารสนเทศ รวมทั้งจัดทำแผนผังแสดงตำแหน่งและชนิดของพื้นที่ใช้งานระบบสารสนเทศ เพื่อการเฝ้าระวัง การควบคุม และรักษาความมั่นคงปลอดภัยจากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่น ๆ ที่อาจเกิดขึ้นได้

๘.๒. ควบคุมพื้นที่การทำงานให้ความมั่นคงปลอดภัยสารสนเทศ และมาตรการป้องกันที่เหมาะสมตามระดับความเสี่ยงของพื้นที่ เพื่อป้องกันการเข้าถึงพื้นที่โดยไม่ได้รับอนุญาต รวมถึงความเสียหายที่เกิดขึ้นในพื้นที่และการแทรกแซงข้อมูลของมหาวิทลัย และการทำงานของอุปกรณ์ประมวลผลข้อมูลต่าง ๆ

๘.๓. จัดหาอุปกรณ์ป้องกันภัยจากสภาพแวดล้อมต่าง ๆ เช่น อุปกรณ์ตรวจจับไฟไหม้ อุปกรณ์ดับเพลิงอัตโนมัติ อุปกรณ์ตรวจจับน้ำรั่วซึม อุปกรณ์ควบคุมอุณหภูมิ เป็นต้น

๘.๔ ให้มีมาตรการควบคุมการเข้า-ออกในบริเวณหรือพื้นที่ควบคุมความมั่นคงปลอดภัยภายใต้ขอบเขตระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ และอนุญาตให้ผ่านเข้า-ออกเฉพาะผู้ที่ได้รับอนุญาตเท่านั้น

๘.๕. กำหนดให้มีการล็อคหน้าจอคอมพิวเตอร์เมื่อไม่ได้ใช้งานหรือไม่มีผู้ดูแล

๘.๖. ต้องควบคุมทรัพย์สินสารสนเทศ ได้แก่ เอกสาร สื่อบันทึกข้อมูล อุปกรณ์คอมพิวเตอร์ ฯลฯ ให้ปลอดภัยจากการเข้าถึงโดยผู้ไม่มีสิทธิ

๙. ความมั่นคงปลอดภัยสำหรับบริการเครือข่าย (Security of network services)

เพื่อตรวจสอบให้มั่นใจว่าการใช้บริการบนเครือข่ายมีการรักษาความปลอดภัยอย่างหมาะสม มหาวิทยาลัยจึงกำหนดแนวปฏิบัติไว้ ดังนี้

๙.๑. กำหนดให้มีการบริหารจัดการการควบคุมเครือข่ายคอมพิวเตอร์ และกำหนดสิทธิผู้ใช้งานผ่านเครือข่ายโดยอนุญาตเฉพาะผู้ที่มีสิทธิเท่านั้น เพื่อป้องกันภัยคุกคาม และมีการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ และแอปพลิเคชันที่ทำงานบนเครือข่ายคอมพิวเตอร์ รวมทั้งข้อมูลสารสนเทศที่มีการแลกเปลี่ยนบนเครือข่ายดังกล่าว

๙.๒. ต้องออกแบบระบบเครือข่ายตามกลุ่มของการบริการระบบ และการสื่อสารที่มีการใช้งาน โดยแบ่งตามกลุ่มของผู้ใช้ และกลุ่มของระบบสารสนเทศ โดยแบ่งเป็นโซนภายใน (Internal Zone) และ โซนภายนอก (External Zone) เพื่อทำให้การควบคุมและป้องกันการบุกรุกได้อย่างเป็นระบบ

๙.๓. ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) โดยมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๙.๔. ต้องกำหนดให้มีการจัดทำข้อตกลง และควบคุมดูแลให้บุคคลหรือหน่วยงานภายนอกที่ให้บริการเครือข่ายคอมพิวเตอร์แก่หน่วยงาน หรือที่ต้องปฏิบัติงานระยะไกล ตามที่ว่าจ้างปฏิบัติตามสัญญาหรือข้อตกลงให้บริการที่ระบุไว้ ซึ่งต้องครอบคลุมถึงงานด้านความมั่นคงปลอดภัย ลักษณะการให้บริการ และระดับการให้บริการ และมีการติดตามตรวจสอบรายงานหรือบันทึกการให้บริการของบุคคลหรือหน่วยงานภายนอกที่ให้บริการแก่หน่วยงานตามที่ว่าจ้างอย่างสม่ำเสมอ

๙.๕. ให้กำหนดมาตรการความปลอดภัยให้เหมาะสมสำหรับเครือข่ายแบบไร้สาย โดยให้เชื่อมต่อภายนอกเพื่อแยกการเข้าถึงออกจากเครือข่ายภายใน หากมีความจำเป็นต้องเข้าถึงเครือข่ายภายในต้องได้รับอนุญาตจากผู้รับผิดชอบเท่านั้น

๙.๖. กำหนดให้ไม่เข้าใช้งานเว็บไซต์ที่มีความเสี่ยงต่อองค์กร เช่น เว็บไซต์ที่มีโอกาสในการติดมัลแวร์ เว็บไซต์ที่ผิดกฎหมาย และเฝ้าติดตามอัพเดท ข้อมูลเว็บไซต์ที่มีความเสี่ยงอยู่สม่ำเสมอ

๙.๗. กำหนดให้มีการสื่อสารการใช้งานจากแหล่งข้อมูลออนไลน์ให้มีความปลอดภัย รวมถึงข้อจำกัดและความเสี่ยงสำหรับการใช้งานเว็บไซต์และแอปพลิเคชั่นที่ไม่พึงประสงค์

๙.๘. ห้ามใช้งานระบบอินเทอร์เน็ตของมหาวิทยาลัย เพื่อใช้หาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือน

หรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิของผู้อื่นหรือข้อมูลที่อาจก่อให้เกิดความเสียหายให้กับมหาวิทยาลัย

๑๐. การบริหารจัดการการควบคุมการเข้าถึง (Access Control Management)

เพื่อควบคุมการเข้าถึงข้อมูลและระบบคอมพิวเตอร์เฉพาะผู้ที่ได้รับอนุญาต และป้องกันการ เข้าถึงระบบและบริการโดยไม่ได้รับอนุญาต มหาวิทยาลัยจึงกำหนดแนวปฏิบัติไว้ ดังนี้

๑๐.๑. กำหนดและประกาศใช้นโยบายการควบคุมการเข้าถึงระบบสารสนเทศ เพื่อให้เจ้าของพื้นที่/ระบบสารสนเทศ ระบบเครือข่าย ข้อมูลสารสนเทศ ได้ดำเนินการควบคุมการเข้าใช้งานระบบสารสนเทศอย่างปลอดภัย

๑๐.๒. จัดให้มีการควบคุมบัญชีผู้ใช้งานระบบสารสนเทศ ซึ่งจะต้องมีการลงทะเบียนบัญชีและยกเลิกผู้ใช้อย่างเป็นทางการ เพื่อควบคุมและจำกัดการให้สิทธิ และการยกเลิกสิทธิให้สอดคล้องกับบทบาทหน้าที่ความรับผิดชอบของผู้เข้าใช้งานระบบสารสนเทศ

๑๐.๓. กำหนดให้ผู้ใช้งานมีบัญชีผู้ใช้งานเป็นของตัวเองและไม่ซ้ำกับผู้อื่น และจะต้องมีการพิสูจน์ตัวตนที่ปลอดภัย ยกเว้นระบบที่มีข้อจำกัดในการบริหารจัดการบัญชีรายชื่อผู้ใช้ ซึ่งจำเป็นต้องใช้บัญชีร่วม จะต้องทำทะเบียนบัญชีร่วม ซึ่งต้องกำหนดผู้ใช้งานที่ใช้บัญชีร่วมนั้น

๑๐.๔. การควบคุมการเข้าถึงของผู้ใช้งานเฉพาะผู้ที่ได้รับอนุญาตตามสิทธิที่ได้รับเท่านั้น เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

๑๐.๕. กำหนดวิธีการปฏิบัติในการเข้าถึงระบบปฏิบัติการรวมทั้งการใช้งานโปรแกรมอรรถประโยชน์รวมถึงการควบคุมการเข้าออกระบบและแอปพลิเคชัน

๑๐.๖. ข้อมูลการพิสูจน์ตัวตนของผู้ใช้งานต้องจัดเก็บเป็นความลับและดูแลข้อมูลนั้นอย่างเหมาะสม

๑๐.๗. จำกัดสิทธิในการเข้าถึงระบบสารสนเทศ ระบบเครือข่าย ข้อมูลสารสนเทศและฟังก์ชันต่าง ๆ ในแอพพลิเคชั่น ตามความเหมาะสมต่อการใช้งาน

๑๐.๘. จัดให้มีการบริหารจัดการเรื่องการกำหนดรหัสผ่าน (password) สำหรับผู้ใช้งานระบบ ผู้ดูแลระบบและกำหนดให้มีการพิสูจน์ตัวตนก่อนที่จะอนุญาตให้ผู้ใช้ที่อยู่ภายนอกองค์กรสามารถเข้าใช้งานเครือข่ายคอมพิวเตอร์และระบบสารสนเทศ

๑๐.๙. ผู้ดูแลระบบ ต้องทบทวนสิทธิ ตรวจสอบ บัญชีรายชื่อผู้ใช้งานระบบสารสนเทศ อย่างสม่ำเสมอ หรือเมื่อมีการเปลี่ยนแปลงผู้ใช้งาน

๑๑. การตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Response to information security incidents)

เพื่อให้เหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยต่อระบบสารสนเทศได้รับการตอบสนองที่ถูกต้องในช่วงระยะเวลาที่เหมาะสม มหาวิทยาลัยจึงกำหนดแนวปฏิบัติไว้ ดังนี้

๑๑.๑. หากพบเห็นเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศหรือการทำงานที่บกพร่องหรือการทำงานผิดปกติ ต้องรายงานสิ่งที่เกิดขึ้นให้แก่หน่วยงานเจ้าของกิจกรรมทราบโดยทันที

๑๑.๒. กรณีเกิดเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ ผู้ดูแลระบบต้องร่วมกับหน่วยงานเจ้าของกิจกรรม ประเมินขอบเขต (Scope) และความรุนแรง (Severity) ของปัญหา หากพบว่าเป็นปัญหาที่จะมีผลกระทบรุนแรง หรือมีผลต่อชื่อเสียงของบริษัท จะต้องรายงานให้กับผู้ที่เกี่ยวข้องทราบโดยด่วน เพื่อหาแนวทางแก้ไขและป้องกันต่อไป

๑๑.๓. ผู้ดูแลระบบหรือผู้รับผิดชอบในส่วนงานที่เกี่ยวข้อง ให้ตอบสนองต่อสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดคิด อย่างรวดเร็ว มีระเบียบและมีประสิทธิผล โดยปฏิบัติตามเอกสารวิธีปฏิบัติงานเรื่องการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ และให้มีการบันทึกเหตุการณ์ต่าง ๆ ที่เข้าข่ายการละเมิดความมั่นคงปลอดภัย เพื่อรับทราบและเรียนรู้จากเหตุการณ์ที่เกิดขึ้น พร้อมเตรียมการป้องกันที่จำเป็นไว้ล่วงหน้า

๑๑.๔. ภายหลังจากเกิดสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดคิด เกี่ยวข้องกับการดำเนินการทางกฎหมาย ให้มีการรวบรวม จัดเก็บ และนำเสนอหลักฐานให้สอดคล้องกับหลักเกณฑ์ของกฎหมายที่ใช้บังคับ

๑๑.๕. การจัดเก็บหลักฐานสามารถจัดเก็บรูปแบบของเอกสารหรือระบบอิเล็กทรอนิกส์ได้

๑๒. ความพร้อมด้านความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการเพื่อความต่อเนื่อง (ICT readiness for business continuity)

เพื่อให้มั่นใจว่าระบบสนับสนุนการประมวลผลสารสนเทศของมหาวิทยาลัย มีความพร้อมในการให้บริการตามความต้องการของการดำเนินงาน มหาวิทยาลัยจึงกำหนดแนวปฏิบัติไว้ ดังนี้

๑๒.๑ ให้มีการจัดทำแผน กำหนดแผนที่ชัดเจนในการทดสอบแผน ตั้งแต่เริ่มต้น จนสิ้นสุดกระบวนการและขั้นตอนการปฏิบัติ สำหรับการบริหารจัดการเพื่อการดำเนินงานอย่างต่อเนื่อง ที่จะใช้รับมือกับการหยุดชะงักของระบบ เพื่อรักษาไว้หรือกู้คืนการให้บริการสารสนเทศหลังเกิดเหตุการณ์ รวมถึงให้ข้อมูลสารสนเทศอยู่ในสภาพพร้อมใช้งานตามระดับที่กำหนดไว้ ภายในระยะเวลาที่กำหนดไว้

๑๒.๒. ให้มีการทดสอบ และทบทวน ปรับปรุงแผน หรือขั้นตอนการปฏิบัติ สำหรับการบริหารจัดการเพื่อการดำเนินงานอย่างต่อเนื่องในภาวะฉุกเฉินอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจว่าแผนดังกล่าวเป็นปัจจุบันและมีประสิทธิผล

๑๒.๓. ให้มีการระบุเหตุการณ์ที่ส่งผลให้การดำเนินงานหยุดชะงัก และประเมินความเสี่ยง โดยระบุความเป็นไปได้ในการเกิดผลกระทบ ตลอดจนผลต่อเนื่องจากการหยุดชะงักนั้นในแง่ของความมั่นคงปลอดภัยสารสนเทศ เพื่อป้องกันความล้มเหลวต่อระบบและสร้างความต่อเนื่องให้สามารถควบคุมระบบสารสนเทศได้

๑๒.๔. ให้จัดเตรียมความพร้อมใช้งานของอุปกรณ์ให้เพียงพอ เพื่อให้ตรงตามความต้องการของระบบ (system availability) ที่กำหนด

๑๒.๕. ต้องมีการสื่อสารให้ผู้ใช้งาน ผู้ใช้บริการ และผู้มีส่วนเกี่ยวข้องให้รับทราบถึงวัตถุประสงค์ ขั้นตอนการปฏิบัติงาน เข้าใจแผนความต่อเนื่องในการดำเนินกิจกรรม ขั้นตอนการรายงาน ระบบรักษาความปลอดภัย และหน้าที่ความรับผิดชอบตามแผนอย่างชัดเจน

๑๒.๖. ระบุขั้นตอนการปฏิบัติงานเพื่อฟื้นฟูให้เหตุการณ์กลับสู่ภาวะปกติ การควบคุมการติดตั้งการตั้งค่าและทดสอบระบบที่ถูกกู้คืนมาหรือทดแทนใหม่ การรายงานสรุปความเสียหายต่อผู้บริหาร

๑๓. ข้อกำหนดทางกฎหมาย ระเบียบข้อบังคับ และสัญญา (Legal, statutory, regulatory and contractual requirements)

เพื่อให้มั่นใจว่าการดำเนินงานสอดคล้องตามกฎหมาย กฎระเบียบข้อบังคับ หรือข้อผูกพันตามสัญญาที่เกี่ยวข้อง มหาวิทยาลัยจึงกำหนดแนวปฏิบัติไว้ ดังนี้

๑๓.๑. กำหนดให้มีการวางแผนและจัดให้มีข้อกำหนดการตรวจสอบ เพื่อให้ความสอดคล้องกับนโยบาย กฎระเบียบ และมาตรการด้านความมั่นคงปลอดภัย

๑๓.๒. หากพบว่าผู้ปฏิบัติงานไม่ปฏิบัติตามนโยบายกฎระเบียบ และมาตรฐานด้านความมั่นคงปลอดภัยให้พิจารณาบทลงโทษตามความเหมาะสม

๑๔. ช่องการการติดต่อหรือแจ้งเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

หากพบเห็นเหตุการละเมิดสามารถแจ้งเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ได้ที่ ฝ่ายระบบเครือข่ายและอินเทอร์เน็ต สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏสวนสุนันทา

สถานที่ติดต่อ: อาคาร ๓๑ ชั้น ๒ เลขที่ ๑ ถนนอู่ทองนอก เขตดุสิต กรุงเทพฯ ๑๐๓๐๐
โทรศัพท์ : ๐๒-๑๖๐-๑๒๒๙
อีเมล์ : arit@ssru.ac.th

จึงประกาศให้ทราบโดยทั่วกัน

ประกาศ ณ วันที่ ๗ ตุลาคม ๒๕๖๗

(รศ.ดร.ชุติกาญจน์ ศรีวิบูลย์)
อธิการบดีมหาวิทยาลัยราชภัฏสวนสุนันทา
07ต.ค.67 เวลา 17:19:31 Non-PKI Server Sign
Signature Code : OAA5A-DYARg-AzADI-ANQA4