นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มหาวิทยาลัยเทคโนโลยีราชมงคลอีสาน พ.ศ. ๒๕๖๕

คำนำ

ตามที่พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ ในมาตรา ๕ มาตรา ๗ และมาตรา ๘ ซึ่งออกโดยอาศัยอำนาจตามความในมาตรา ๓๕ แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.๒๕๔๔ ได้กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินกิจกรรมหรือการให้บริการต่างๆ มีความมั่นคงปลอดภัยและเชื่อถือได้ ตลอดจนมีมาตรฐานเป็นที่ยอมรับในระดับสากลและตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ.๒๕๕๓ และฉบับที่ ๒ พ.ศ.๒๕๕๖ กำหนดให้หน่วยงานของรัฐต้องจัดให้มีนโยบายในการรักษาความปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร

มหาวิทยาลัยเทคโนโลยีราชมงคลอีสาน จึงได้จัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ขึ้นเพื่อเป็นแนวทางปฏิบัติในการควบคุมการปฏิบัติงานและรักษาความปลอดภัยด้านระบบสารสนเทศ พ.ศ.๒๕๖๑ และได้ทบทวน ปรับปรุงในปี พ.ศ.๒๕๖๕ เพื่อให้สอดคล้องตามพระราชกฤษฎีกาดังกล่าว ซึ่งเป็นสิ่งสำคัญที่ผู้ปฏิบัติงานต้องถือปฏิบัติเพื่อให้เกิดความมั่นคงปลอดภัยในการขับเคลื่อนพันธกิจและการให้บริการของมหาวิทยาลัย อีกทั้งยังเป็นการสร้างความเชื่อมั่นให้กับผู้ใช้บริการและผู้มีส่วนเกี่ยวข้องในทุกภาคส่วนและเพื่อสร้างความน่าเชื่อถือให้กับมหาวิทยาลัยเทคโนโลยีราชมงคลอีสานต่อไป

สารบัญ

หน้า

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
มหาวิทยาลัยเทคโนโลยีราชมงคลอีสาน พ.ศ. ๒๕๖๕

หลักการและเหตุผล

พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินธุรกรรมด้วยวิธีการทางอิเล็กทรอนิกส์มีความมั่นคงปลอดภัยและเชื่อถือได้ ดังนั้น มหาวิทยาลัยเทคโนโลยีราชมงคลอีสาน จึงได้จัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้บุคลากรและผู้ที่เกี่ยวข้องนำไปปฏิบัติ

วัตถุประสงค์

๑. เพื่อให้มีนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัยเทคโนโลยีราชมงคลอีสานเป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง
๒. เพื่อกำหนดแนวทางและวิธีการปฏิบัติ สำหรับบุคลากรและบุคคลที่ปฏิบัติงานให้กับมหาวิทยาลัยเทคโนโลยีราชมงคลอีสานในการยืนยันตัวบุคคล การเข้าถึงและการควบคุมการใช้งานระบบเทคโนโลยีสารสนเทศ
๓. เพื่อให้มีการสำรองข้อมูลสารสนเทศ อย่างสม่ำเสมอ เพื่อรักษาความถูกต้อง สมบูรณ์ในการพร้อมใช้งาน สามารถกู้ระบบกลับคืนมาได้ในระยะเวลาที่เหมาะสม มีแผนการสำรองข้อมูล และแผนเตรียมความพร้อมกรณีฉุกเฉินที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ได้ตามปกติ
๔. เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ
๕. เพื่อสร้างความตระหนักและส่งเสริมให้เกิดความรู้ ความเข้าใจและการให้การอบรมทางด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศให้แก่ บุคลากรและบุคคลที่เกี่ยวข้อง

นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
มหาวิทยาลัยเทคโนโลยีราชมงคลอีสาน พ.ศ. ๒๕๖๕

๑. ส่งเสริมและสนับสนุนการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้ตอบสนองต่อพันธกิจและนโยบายของมหาวิทยาลัยเทคโนโลยีราชมงคลอีสาน

๒. มุ่งกำหนดแนวปฏิบัติ แนวทางแก้ไข หรือบทลงโทษตามความเหมาะสมหากมีการละเมิดหรือฝ่าฝืนแนวนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ รวมทั้งติดตามและตรวจสอบการดำเนินงานอย่างสม่ำเสมอ เพื่อให้เป็นไปตามกฎหมายที่เกี่ยวข้อง

๓. เน้นกำกับดูแลการดำเนินงานเพื่อบริหารจัดการให้ระบบเทคโนโลยีสารสนเทศมีความถูกต้องสมบูรณ์ และพร้อมใช้งานอยู่เสมอ

๔. เผยแพร่ความรู้ ความเข้าใจเพื่อสร้างความตระหนักให้บุคลากรของมหาวิทยาลัย และบุคคลที่เกี่ยวข้อง ตลอดจนส่งเสริมให้มีการศึกษาอย่างต่อเนื่อง

๕. ติดตาม ตรวจสอบการดำเนินงาน และปรับปรุงแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้สอดคล้องตามการเปลี่ยนแปลงของเทคโนโลยี

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
มหาวิทยาลัยเทคโนโลยีราชมงคลอีสาน พ.ศ. ๒๕๖๕

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มหาวิทยาลัยเทคโนโลยีราชมงคลอีสานจัดทำขึ้นเพื่อกำหนด วิธีปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้สอดคล้องและเป็นไปตามนโยบายที่กำหนดไว้ โดยแบ่งนโยบายออกเป็นส่วน ๆ ดังต่อไปนี้

ส่วนที่ ๑. แนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

ส่วนที่ ๒. แนวปฏิบัติการใช้ระบบคอมพิวเตอร์และระบบเครือข่าย

ส่วนที่ ๓. แนวปฏิบัติการเข้าถึงหรือควบคุมการใช้ระบบสารสนเทศ

ส่วนที่ ๔. แนวปฏิบัติการควบคุมการเข้าถึงระบบเครือข่าย

ส่วนที่ ๕. แนวปฏิบัติการควบคุมการเข้าถึงระบบปฏิบัติการ

ส่วนที่ ๖. แนวปฏิบัติการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ

ส่วนที่ ๗. แนวปฏิบัติของผู้ดูแลระบบ

ส่วนที่ ๘. แนวปฏิบัติการจัดทำระบบสำรองระบบสารสนเทศและแผนเตรียมความพร้อมกรณีฉุกเฉิน

ส่วนที่ ๙. แนวปฏิบัติการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

ส่วนที่ ๑๐. แนวปฏิบัติการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

ส่วนที่ ๑๑. การกำหนดผู้รับผิดชอบ

คำนิยาม

คำนิยามของแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มหาวิทยาลัยเทคโนโลยีราชมงคลอีสาน มีดังนี้

“มหาวิทยาลัย” หมายความว่า มหาวิทยาลัยเทคโนโลยีราชมงคลอีสาน

“คณะกรรมการบริหารเทคโนโลยีสารสนเทศ” หมายความว่า ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตาม กำกับ ดูแล ควบคุมตรวจสอบเจ้าหน้าที่ในระดับปฏิบัติการทบทวนปรับปรุงนโยบายและข้อปฏิบัติให้เป็นปัจจุบัน

“ระบบคอมพิวเตอร์และเครือข่าย” หมายความว่า ระบบคอมพิวเตอร์และเครือข่ายที่อยู่ภายใต้การดูแลและรับผิดชอบของมหาวิทยาลัย

“ระบบสารสนเทศ” หมายความว่า ระบบงานของมหาวิทยาลัย ที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์และระบบเครือข่าย มาช่วยในการสร้างสารสนเทศที่สามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร

“สินทรัพย์” หมายความว่า ฮาร์ดแวร์ ซอฟต์แวร์ และข้อมูลภายใต้การดูแลของมหาวิทยาลัย

“ผู้บังคับบัญชา” หมายความว่า ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของมหาวิทยาลัย

“ผู้ใช้งาน” หมายความว่า บุคลากรและนักศึกษาของมหาวิทยาลัย หรือ บุคคลภายนอกจากหน่วยงานภายนอกที่ได้รับอนุญาตให้ใช้ระบบคอมพิวเตอร์และเครือข่ายของมหาวิทยาลัย

“ผู้ดูแลระบบ” หมายความว่า ข้าราชการพลเรือนในสถาบันอุดมศึกษา พนักงานในสถาบันอุดมศึกษา พนักงานราชการ ลูกจ้างประจำ หรือลูกจ้างเงินรายได้ ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบเครือข่ายซึ่งสามารถเข้าถึงโปรแกรมเครือข่าย เพื่อจัดการฐานข้อมูลของระบบเครือข่าย

“บุคคลภายนอก” หมายความว่า บุคคลภายนอกมหาวิทยาลัยแต่ได้รับอนุญาตให้มีสิทธิ์ในการเข้าถึงและใช้งานข้อมูลหรือสินทรัพย์ต่าง ๆ ของมหาวิทยาลัย โดยจะได้รับสิทธิ์ในการใช้ระบบตามหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล

“จดหมายอิเล็กทรอนิกส์” หมายความว่า ระบบการรับส่งจดหมายข้อความระหว่างกันผ่านเครื่องคอมพิวเตอร์ ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว และเสียง โดยผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ตามมาตรฐานที่ใช้ในการรับส่งข้อมูลได้แก่ SMTP, POP3 และ IMAP

“แบนด์วิดท์” หมายความว่า ปริมาณข้อมูลที่ไหลเข้าหรือออกจากจุดใดจุดหนึ่งของระบบ เป็นการแสดงให้เห็นถึงปริมาณข้อมูลที่ สามารถถ่ายโอนได้ในช่วงเวลาหนึ่ง และเป็นการบอกถึงความเร็วในการรับส่งข้อมูล

“รหัสผ่าน” หมายความว่า ตัวอักษรหรืออักขระหรือตัวเลขที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศ

“บัญชีผู้ใช้งาน หรือ บัญชีสมาชิกอินเทอร์เน็ต” หมายความว่า รายชื่อผู้มีสิทธิ์ใช้งานเครื่องคอมพิวเตอร์ และบริการในระบบเครือข่ายของมหาวิทยาลัย

“เวลาอ้างอิงสากล” หมายความว่า การเปรียบเทียบเวลาของเครื่องคอมพิวเตอร์แม่ข่ายที่ใช้ในการเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) กับเวลามาตรฐานสากลในประเทศไทยนั้นอ้างอิงกับหน่วยงานมาตรฐาน ได้แก่ กรมอุทกศาสตร์ กองทัพเรือ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ เพื่อให้สอดคล้องกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

“ข้อมูลจราจรทางคอมพิวเตอร์” หมายความว่า ข้อมูลที่เกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง วันที่ ปริมาณ ระยะเวลา และชนิดของบริการอื่น ๆ ที่เกี่ยวข้องในการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

“เลขที่อยู่ไอพี” หมายความว่า ตัวเลขประจำเครื่องคอมพิวเตอร์ที่ต่ออยู่ในระบบเครือข่าย ซึ่งเลขนี้ของแต่ละเครื่องจะต้องไม่ซ้ำกัน โดยประกอบด้วยชุดของตัวเลข ๔ ส่วนหรือ ๖ ส่วน ที่คั่นด้วยเครื่องหมายจุด (.)

“เลขที่อยู่ไอพีสาธารณะ” หมายความว่า เลขที่อยู่ไอพีที่มีไว้สำหรับให้แต่ละหน่วยงาน หรือแต่ละบุคคลสามารถเชื่อมต่อเข้าหากัน หรือรับส่งข้อมูลระหว่างกันผ่านเครือข่ายสาธารณะได้

“ลงบันทึกเข้า” หมายความว่า กระบวนการที่ผู้ใช้งานต้องทำให้เสร็จสิ้นตามเงื่อนไขที่ตั้งไว้เพื่อเข้าใช้งานระบบคอมพิวเตอร์และระบบเครือข่าย ซึ่งปกติแล้วจะอยู่ในรูปแบบของการกรอกชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ให้ถูกต้อง

“ลงบันทึกออก” หมายความว่า กระบวนการที่ผู้ใช้งานทำเพื่อสิ้นสุดการใช้งานระบบคอมพิวเตอร์และระบบเครือข่าย

“สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด” หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจไม่คาดคิด (unwanted or unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตีและความมั่นคงปลอดภัยถูกคุกคาม

“อุปกรณ์จัดเส้นทาง” หมายความว่า อุปกรณ์ที่ใช้ในระบบเครือข่ายคอมพิวเตอร์ที่ทำหน้าที่จัดเส้นทางและค้นหาเส้นทางเพื่อส่งข้อมูลต่อไปยังระบบเครือข่ายอื่น

“อุปกรณ์กระจายสัญญาณข้อมูล” หมายความว่า อุปกรณ์ที่ใช้ในระบบเครือข่ายคอมพิวเตอร์ที่ทำหน้าที่รับ-ส่งข้อมูล

“การพิสูจน์ยืนยันตัวตน” หมายความว่า ขั้นตอนการรักษาความปลอดภัยในการเข้าใช้ระบบ เป็นขั้นตอนในการพิสูจน์ตัวตนของผู้ใช้งานระบบทั่วไปแล้วจะเป็นการพิสูจน์โดยใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password)

“สิทธิ์” หมายความว่า สิทธิ์ผู้ใช้ สิทธิ์ทั่วไป สิทธิ์จำเพาะ สิทธิ์พิเศษ และสิทธิ์อื่นใดที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงานความมั่นคงและความปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน โดยธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non-Repudiation) และ ความน่าเชื่อถือ (Reliability)

“การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ” หมายความว่า การอนุญาต การกำหนดสิทธิ์ หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึง หรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

“แผนผังระบบเครือข่าย” หมายความว่า แผนผังซึ่งแสดงถึงการเชื่อมต่อของระบบเครือข่ายของมหาวิทยาลัย

“เหตุการณ์ด้านความมั่นคงปลอดภัย” หมายความว่า การเกิดเหตุการณ์ สภาพของบริการ หรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัย หรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

ส่วนที่ ๑
แนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม
(Physical and Environmental Control)

๑. วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการในการควบคุมและป้องกันการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยพิจารณาตามความสำคัญของอุปกรณ์ ระบบเทคโนโลยีสารสนเทศและข้อมูล ซึ่งเป็นสินทรัพย์ที่มีค่าและอาจจำเป็นต้องรักษาความลับโดยมาตรการนี้จะมีผลบังคับใช้กับผู้ใช้งานที่เป็นบุคลากรของมหาวิทยาลัย และบุคคลภายนอก ซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัย

๒. แนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environmental Control)

๒.๑. สำนักวิทยบริการและเทคโนโลยีสารสนเทศเป็นผู้กำหนดพื้นที่ผู้ใช้งาน พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารให้ชัดเจนและจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้รับทราบทั่วกัน โดยการกำหนดพื้นที่ดังกล่าวแบ่งออกได้เป็นพื้นที่ทำงาน พื้นที่ติดตั้งและจัดเก็บอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย พื้นที่ใช้งานระบบเครือข่ายไร้สาย เป็นต้น

๒.๒. สำนักวิทยบริการและเทคโนโลยีสารสนเทศ เป็นผู้กำหนดสิทธิ์ กำหนดมาตรการควบคุมการเข้า-ออกพื้นที่ในการเข้าถึงพื้นที่บริการเครือข่ายคอมพิวเตอร์

๒.๓. บุคคลภายนอกที่นำเครื่องคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานระบบเครือข่ายภายในมหาวิทยาลัย จะต้องขออนุญาตใช้งานอุปกรณ์ และต้องมีเจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาลงนาม

๓. พื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัย (Secure areas)

๓.๑. ขอบเขตหรือบริเวณโดยรอบทางกายภาพ (Physical security perimeter) ต้องแบ่งพื้นที่อย่างชัดเจน และกำหนดระดับการควบคุมเพื่อป้องกันการเข้าถึงสินทรัพย์สารสนเทศที่มีความสำคัญ และจัดทำแผนผังแสดงตำแหน่งและพื้นที่แต่ละชนิดและประกาศให้ผู้เกี่ยวข้องทราบ

๓.๒. การควบคุมการเข้าออกทางกายภาพ (Physical entry controls) ควบคุมให้เฉพาะผู้ที่มีสิทธิ หรือผู้ที่ได้รับอนุญาตสามารถเข้าออกในพื้นที่ กำหนดสิทธิและช่วงเวลาในการผ่านเข้า-ออกพื้นที่ บันทึกการผ่านเข้า-ออกในพื้นที่ที่สำคัญ และไม่เปิดประตูสำนักงานทิ้งไว้ หรือยินยอมให้บุคคลอื่นติดตามเข้าภายในพื้นที่สำนักงานโดยเด็ดขาด เว้นแต่บุคคลอื่นนั้นสามารถแสดงบัตรประจำตัว หรือบัตรผู้มาติดต่อได้ เพื่อเป็นการป้องกันการเข้าถึงพื้นที่สำนักงาน และพื้นที่ควบคุมความมั่นคงปลอดภัยโดยบุคคลที่ไม่ได้รับอนุญาต

๓.๓. การรักษาความมั่นคงปลอดภัยสำหรับสำนักงาน ห้องทำงาน และอุปกรณ์ (Securing office, room and facilities) ให้ปฏิบัติดังนี้

๓.๑. ต้องจัดให้มีมาตรการในการรักษาความมั่นคงปลอดภัยอื่น ๆ ให้กับสำนักงาน ห้องทำงานและเครื่องมือต่าง ๆ เช่น เครื่องคอมพิวเตอร์หรือระบบที่มีความสำคัญสูงต้องไม่ตั้งอยู่ในบริเวณที่มีการผ่านเข้า-ออกของบุคคลเป็นจำนวนมาก

๓.๒. เจ้าหน้าที่ควรตรวจสอบความมั่นคงปลอดภัยของพื้นที่ทำงานของตนเป็นประจำทุกวันหลังเลิกงานเพื่อให้มั่นใจว่าตู้เซฟ ตู้เอกสาร ลิ้นชัก และอุปกรณ์ต่าง ๆ ได้รับการปลดล็อค อย่างเหมาะสม และกุญแจถูกเก็บรักษาไว้อย่างปลอดภัย

๓.๓. ข้อมูล สื่อบันทึก วัสดุ และอุปกรณ์ที่จัดเก็บข้อมูลลับต้องไม่ถูกทิ้งไว้โดยลำพังบนโต๊ะทำงาน ในห้องประชุม หรือในตู้ที่ไม่ได้ล็อคกุญแจโดยเด็ดขาด

๓.๔. ข้อมูล สื่อบันทึก วัสดุ และอุปกรณ์ที่จัดเก็บข้อมูลลับต้องไม่ถูกทิ้งลงในถังขยะโดยไม่ได้รับการทำลายอย่างเหมาะสม

๓.๕. เจ้าหน้าที่ต้องไม่ยินยอมให้ผู้ใดทำการเคลื่อนย้ายเครื่องคอมพิวเตอร์หรือสื่อบันทึกข้อมูลออกจากพื้นที่ทำงานของตนโดยเด็ดขาด เว้นแต่ บุคคลผู้นั้นเป็นเจ้าหน้าที่ ที่ได้รับอนุญาตให้ดำเนินการและเป็นการดำเนินการที่มีคำสั่งอย่างถูกต้องของหน่วยงานเท่านั้น

๓.๔. การป้องกันต่อภัยคุกคามจากภายนอกและสภาพแวดล้อม (Protecting against external end environmental threats) ต้องมีวิธีป้องกันจากการทำลายของธรรมชาติหรือคนที่อาจจะเกิดขึ้น

๓.๕. การปฏิบัติงานในพื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัย (Working in secure areas) หากพบสิ่งผิดปรกติ หรือการละเมิดความมั่นคงปลอดภัย จะต้องแจ้งให้ผู้บังคับบัญชาทราบ ในบริเวณที่ต้องการรักษาความมั่นคงปลอดภัยต้องติดประกาศแจ้งเตือน เช่น ”ห้ามเข้าก่อนได้รับอนุญาต”

๓.๖. พื้นที่สำหรับรับส่งของสิ่งของ (Delivery and loading areas) ต้องแยกจุดที่รับส่งสิ่งของ ออกจากพื้นที่ที่มีอุปกรณ์ประมวลผลสารสนเทศ และดำเนินการแกะหีบห่อหรือตรวจสอบให้เสร็จสิ้น ก่อนนำเข้าสู่พื้นที่ที่ต้องการรักษาความมั่นคงปลอดภัย

๔. อุปกรณ์ (Equipment)

๔.๑. ต้องป้องกันหรือกำหนดสิทธิการเข้าใช้งานอุปกรณ์ (Equipment siting and protection) และการจัดตั้งหรือการจัดวางอุปกรณ์ สินทรัพย์สารสนเทศ อุปกรณ์ใดที่มีความสำคัญสูงต้องจัดวางในที่ที่เข้าถึงได้ยาก รวมถึงในขณะที่อุปกรณ์ไม่มีผู้ใช้งาน

๔.๒. ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting utilities) อุปกรณ์ที่มีความสำคัญสูงควรติดตั้งระบบป้องกันความล้มเหลวของอุปกรณ์ เช่น ระบบสำรองไฟฟ้า ระบบปรับอากาศ เป็นต้น

๔.๓. ความมั่นคงปลอดภัยของการเดินสายสัญญาณและสายสื่อสาร (Cabling security) การเดินสายสัญญาณต้องแยกท่อเพื่อป้องกันสัญญาณรบกวนต้องมีการทำป้ายสายสัญญาณชัดเจน และเมื่อมีการเปลี่ยนแปลงต้องมีการปรับปรุงป้ายสายสัญญาณให้ถูกต้อง

๔.๔. การบำรุงรักษาอุปกรณ์ (Equipment maintenance) ต้องจัดให้มีการบำรุงรักษาอุปกรณ์เพื่อให้มีสภาพพร้อมใช้งานอย่างน้อยปีละ 1 ครั้ง หรือมากกว่าตามระดับความสำคัญ

๔.๕. การนำสินทรัพย์ขององค์กรออกนอกสำนักงาน (Removal of assets) ห้ามนำสินทรัพย์สารสนเทศออกนอกพื้นที่ก่อนได้รับอนุญาตจากผู้รับผิดชอบ และต้องมีขั้นตอนในการตรวจสอบและติดตาม

๔.๖. ความมั่นคงปลอดภัยของอุปกรณ์และสินทรัพย์ที่ใช้งานอยู่ภายนอกสำนักงาน (Security of equipment and assets off-premises) สินทรัพย์ที่ใช้งานอยู่ภายนอกสำนักงานต้องมีการรักษาความมั่นคงปลอดภัยตามความเสี่ยง

๔.๗. ความมั่นคงปลอดภัยสำหรับการกำจัดหรือทำลายอุปกรณ์ หรือการนำอุปกรณ์ไปใช้งานอย่างอื่น (Secure disposal or re-use of equipment) ข้อมูลที่เก็บอยู่บนสื่อบันทึกข้อมูล หากไม่มีการใช้งานแล้วต้องทำลายให้สิ้นซาก โดยให้ปฏิบัติดังนี้

๔.๗.๑. เมื่อต้องทำลายข้อมูลอิเล็กทรอนิกส์ ผู้รับผิดชอบข้อมูลอิเล็กทรอนิกส์ต้องเป็นผู้ทำลายข้อมูล

๔.๗.๒. กำหนดวิธีการทำลายข้อมูลอิเล็กทรอนิกส์บนสื่อบันทึกข้อมูล ดังนี้หรือใช้มาตรฐาน DoD 5220.22 M ของกระทรวงกลาโหมสหรัฐอเมริกา

ประเภทสื่อบันทึกข้อมูล	**วิธีการทำลายใช้ใหม่ได้**	**วิธีทำลาย**	**ระยะเวลาทำลาย**
กระดาษ	-	ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร	เก็บรักษาไว้อย่างน้อย ๑ ปีหรือตามที่กฎหมายกำหนด
Flash Drive	ใช้วิธีการ Format	ทำลายข้อมูลบน Flash Drive ตามมาตรฐาน DoD 5220.22 M ของกระทรวงกลาโหมสหรัฐอเมริกา ซึ่งเป็นมาตรฐานการทำลายข้อมูลโดยการเขียนทับข้อมูลเดิมหลายรอบ และใช้วิธีการทุบหรือบดให้เสียหาย	เก็บรักษาไว้อย่างน้อย ๑ ปีหรือตามที่กฎหมายกำหนด
แผ่น CD/DVD	ใช้วิธีการ Format	ใช้การหั่น ตัด เผา ให้สิ้นสภาพการใช้งาน	เก็บรักษาไว้อย่างน้อย ๑ ปีหรือตามที่กฎหมายกำหนด
เทป		ใช้วิธีการทุบหรือบดให้เสียหาย หรือเผาทำลาย	เก็บรักษาไว้อย่างน้อย ๑ ปีหรือตามที่กำหนด
ฮาร์ดดิสก์	ใช้วิธีการ Format	ทำลายข้อมูลบน Flash Drive ตามมาตรฐาน DoD 5220.22-M ของกระทรวงกลาโหมสหรัฐอเมริกา ซึ่งเป็นมาตรฐานการทำลายข้อมูล โดยการเขียนทับข้อมูลเดิมหลายรอบ และใช้วิธีการทุบหรือบดให้เสียหาย	เก็บรักษาไว้อย่างน้อย ๑ ปีหรือตามที่กำหนด

๔.๘. อุปกรณ์ของผู้ใช้งานที่ทิ้งไว้โดยไม่มีผู้ดูแล (Unattended user equipment) ต้องป้องกันให้ผู้ไม่มีสิทธิเข้าถึงอุปกรณ์สินทรัพย์สารสนเทศที่ไม่มีผู้ดูแล

๔.๙. ต้องไม่ทิ้งสินทรัพย์สารสนเทศสำคัญไว้ในที่ที่ไม่ปลอดภัย โดยต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ ได้แก่ เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์ สารสนเทศ ฯลฯ ให้อยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และให้ปฏิบัติดังนี้

๔.๙.๑. ต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

๔.๙.๒. เครื่องคอมพิวเตอร์ส่วนบุคคลทุกเครื่องต้องมีรหัสผ่านประจำเครื่องสำหรับผู้ใช้งานและรหัสผ่านของผู้ดูแลระบบ

๔.๙.๓. ผู้ใช้งานต้องล็อคอุปกรณ์ที่สำคัญเมื่อไม่ได้ใช้งานหรือปล่อยทิ้งไว้โดยไม่ได้ดูแลชั่วคราว

๔.๙.๔. การป้องกันข้อมูลและสินทรัพย์ด้านสารสนเทศที่อยู่ในเครื่องคอมพิวเตอร์ประเภทพกพา ผู้ใช้งานต้องมีวิธีการป้องกันข้อมูลและสินทรัพย์ด้านสารสนเทศที่อยู่ในเครื่องคอมพิวเตอร์ประเภทพกพา smart mobile device เมื่อปฏิบัติงานอยู่นอกสถานที่ ได้แก่ ต้องใส่รหัสผ่านป้องกันหน้าจอทุกเครื่อง ใช้กุญแจล็อคเครื่องคอมพิวเตอร์พกพา และเข้ารหัสข้อมูลที่สำคัญไว้

ส่วนที่ ๒
แนวปฏิบัติการใช้ระบบคอมพิวเตอร์และระบบเครือข่าย
(Computer Systems and Networking)

๑. วัตถุประสงค์

เพื่อช่วยให้ผู้ใช้งานที่เป็นบุคลากรของมหาวิทยาลัยและบุคคลภายนอก ได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้ระบบคอมพิวเตอร์และระบบเครือข่ายคอมพิวเตอร์ รวมทั้งทำความเข้าใจตลอดจนปฏิบัติตามอย่างเคร่งครัด อันจะเป็นการป้องกันทรัพยากรและข้อมูล ให้เป็นความลับมีความถูกต้องและมีความพร้อมใช้งานอยู่เสมอ

๒. แนวปฏิบัติการใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่าย (Computer and Network)

๒.๑.ผู้ใช้งานจะต้องไม่ใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายโดยมีวัตถุประสงค์ ดังต่อไปนี้

๒.๑.๑. เผยแพร่ซึ่งข้อมูลคอมพิวเตอร์ที่อาจกระทบกระเทือนต่อความมั่นคงแห่งราชอาณาจักร หรือที่มีลักษณะขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชนสู่ระบบคอมพิวเตอร์

๒.๑.๒. นำข้อมูลคอมพิวเตอร์ปลอมไม่ว่าทั้งหมดหรือบางส่วนหรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยกระทำการที่น่าจะเกิดความเสียหายแก่ผู้อื่นเข้าสู่ระบบคอมพิวเตอร์

๒.๑.๓. นำข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยกระทำการที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศหรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน เข้าสู่ระบบคอมพิวเตอร์

๒.๑.๔. นำข้อมูลคอมพิวเตอร์ใด ๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญาเข้าสู่ระบบคอมพิวเตอร์

๒.๑.๕. นำข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันลามกและข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้ เข้าสู่ระบบคอมพิวเตอร์

๒.๑.๖. นำข้อมูลคอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อเติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ทั้งนี้ โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียงถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย เข้าสู่ระบบคอมพิวเตอร์

๒.๑.๗. เผยแพร่ หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์โดยรู้อยู่แล้วว่าเป็น ข้อมูลคอมพิวเตอร์ตาม ๒.๑.๑ ถึง ๒.๑.๖

๒.๒.ผู้ใช้งานจะต้องไม่สนับสนุนหรือยินยอมให้มีการกระทำความผิดตามข้อ ๒.๑ ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน

๒.๓.ผู้ใช้งานจะต้องไม่กระทำการ ดังต่อไปนี้

๒.๓.๑. เข้าใช้ระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตนโดยมิชอบ

๒.๓.๒. นำมาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ ผู้อื่นจัดทำขึ้นเป็นการเฉพาะไปเปิดเผยโดยมิชอบในการกระทำที่น่าจะเกิดความเสียหายแก่ผู้อื่น

๒.๓.๓. เข้าถึงซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตนโดยมิชอบ

๒.๓.๔. กระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่ อยู่ระหว่างการส่งในระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้

๒.๓.๕. ทำให้ข้อมูลคอมพิวเตอร์ของผู้อื่นเสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วนโดยมิชอบ

๒.๓.๖. กระทำด้วยประการใดโดยมิชอบ เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทำงานได้ตามปกติ

๒.๓.๗. ส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์ (e-mail) แก่บุคคลอื่นโดยปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าว อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่น

๒.๓.๘. กระทำให้เกิดความเสียหายต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือการบริการสาธารณะ หรือเป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีไว้เพื่อประโยชน์สาธารณะ

๒.๓.๙. มหาวิทยาลัยเป็นผู้มีหน้าที่ จัดคอมพิวเตอร์แบบตั้งโต๊ะและพกพา พร้อมโปรแกรมคอมพิวเตอร์ที่จำเป็นต่อการใช้งานและถูกต้องตามกฎหมาย หากบุคคลใดมีความประสงค์ต้องการใช้งานโปรแกรมคอมพิวเตอร์อื่นนอกเหนือจากที่ ทางมหาวิทยาลัยจัดไว้ ให้แจ้งความประสงค์มายังสำนักวิทยบริการและเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษรเพื่อพิจารณาจัดหาต่อไป

๒.๓.๑๐. จำหน่ายหรือเผยแพร่โปรแกรมที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตาม ข้อ ๒.๓.๑ ถึงข้อ ๒.๓.๘

๒.๓.๑๑. ผู้ใช้งานจะต้องรับผิดชอบลิขสิทธิ์โปรแกรมคอมพิวเตอร์และการกระทำใด ๆ อันเกิดจากการใช้คอมพิวเตอร์แบบพกพา (Notebook) อันเป็นทรัพย์สินส่วนตัวของผู้ใช้งาน

๒.๓.๑๒. ห้ามมิให้ผู้ใช้งานทำการแก้ไขเปลี่ยนแปลงการตั้งค่าพารามิเตอร์ต่าง ๆ ของคอมพิวเตอร์ ได้แก่ Computer Name, System Configuration และ Program Configuration เว้นแต่เป็นผู้มีหน้าที่ดูแลระบบคอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์

๒.๓.๑๓. ห้ามมิให้ผู้ใช้ติดตั้งโปรแกรมคอมพิวเตอร์ด้วยตนเอง เว้นแต่เป็นผู้มีหน้าที่ดูแลระบบคอมพิวเตอร์ หรือระบบเครือข่ายคอมพิวเตอร์

๒.๓.๑๔. ห้ามมิให้ใช้ระบบคอมพิวเตอร์และเครือข่ายของมหาวิทยาลัย เพื่อการพาณิชย์หรือการอื่นใดที่ไม่เกี่ยวข้องกับหน้าที่ที่ได้รับมอบหมาย

๒.๔.การใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายผู้ใช้งานต้องปฏิบัติดังต่อไปนี้

๒.๔.๑. ใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายของมหาวิทยาลัย อย่างมีประสิทธิภาพและเกิดประโยชน์สูงสุด

๒.๔.๒. ไม่คัดลอกโปรแกรมต่าง ๆ ที่มหาวิทยาลัยได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมายนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งาน โดยไม่ได้รับอนุญาต

๒.๔.๓. ไม่ทำการปรับแต่งไบออส (BIOS) หรือการตั้งค่าระบบ (Configuration) อื่นใดที่อาจส่งผลกระทบต่อระบบการทำงานของคอมพิวเตอร์ อันเป็นเหตุให้ไม่สามารถเปิดเครื่องใช้งานได้เป็นปกติ

๒.๔.๔. ไม่ทำการเปลี่ยนแปลงเลขที่อยู่ไอพี (IP Address) ของเครื่องคอมพิวเตอร์ภายในมหาวิทยาลัย

๒.๔.๕. หากผู้ใช้งานที่มีความประสงค์จะขอใช้เลขที่อยู่ไอพีสาธารณะ (Public IP Address) จะต้องทำหนังสือขออนุญาตเป็นลายลักษณ์อักษรต่อผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ

๒.๔.๖. ไม่ติดตั้งโปรแกรมคอมพิวเตอร์ที่สามารถใช้ในการตรวจสอบข้อมูลบนระบบเครือข่าย เว้นแต่จะได้รับอนุญาตจากผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ

๒.๔.๗. ไม่ติดตั้งโปรแกรมคอมพิวเตอร์หรืออุปกรณ์คอมพิวเตอร์อื่นใดเพิ่มเติมในเครื่องคอมพิวเตอร์ หรือเครื่องคอมพิวเตอร์แม่ข่าย (Server) ของมหาวิทยาลัยเพื่อให้บุคคลอื่นสามารถใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายได้ เว้นแต่จะได้รับอนุญาตจากผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ

๒.๔.๘. ไม่ใช้บริการบนระบบเครือข่ายและอินเทอร์เน็ตที่มีการครอบครองแบนด์วิดท์ (Bandwidth) จำนวนมากหรือเป็นเวลานานในระหว่างเวลาทำงาน

๒.๕.ผู้ใช้จะต้องลงทะเบียนเพื่อขอรับ ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบเครือข่ายคอมพิวเตอร์และระบบสารสนเทศของมหาวิทยาลัย ผ่านการลงทะเบียนผู้ใช้งานระบบจัดการข้อมูลและบริการอินเทอร์เน็ต โดยใช้รหัสประจำตัวนักศึกษาในการลงทะเบียนขอใช้รหัสผู้ใช้งาน เพื่อใช้สำหรับยืนยันตัวตนของผู้ใช้งานในการเข้าใช้ระบบเครือข่ายคอมพิวเตอร์และระบบสารสนเทศของมหาวิทยาลัย

๒.๖. กำหนดหลักเกณฑ์ในการยกเลิกเพิกถอนการอนุญาตให้เข้าถึงระบบสารสนเทศ ได้แก่

๒.๖.๑. การตัดออกจากทะเบียน การโยกย้ายหน่วยงาน การระงับการปฏิบัติงาน หรือเมื่อสิ้นสุดสถานภาพการเป็นผู้ใช้งาน

๒.๖.๒. การใช้งานที่ขัดต่อข้อกำหนดการใช้งานเครือข่าย

๒.๗.การบริหารจัดการรหัสผ่าน (Password Managers)

๒.๗.๑. กำหนดให้รหัสผ่านต้องมีมากกว่าหรือเท่ากับ ๘ ตัวอักษรหรือมากกว่านั้น โดยผสมกันระหว่างตัวอักษร (a-z, A-Z) ตัวเลข (0-9) เครื่องหมายหรืออักขระพิเศษ (! @ # $ % ^ & * ( ) _ + | ~- = \ ` { } [ ] : ” ; ' < > ? , . /) เข้าด้วยกัน

๒.๗.๒. ต้องให้ผู้ใช้งานลงนามเพื่อเก็บรักษารหัสผ่านทั้งของตนเองและของกลุ่มไว้เป็นความลับ และไม่เปิดเผย ให้ผู้อื่นทราบ

๒.๗.๓. กำหนดรหัสผ่านเริ่มต้นให้กับผู้ใช้ให้ยากต่อการเดา

๒.๗.๔. ส่งมอบรหัสผ่านชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย หลีกเลี่ยงการใช้บุคคลอื่น หรือการส่งจดหมายอิเล็กทรอนิกส์ (e-mail) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน

๒.๗.๕. ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันทีหลังจากได้รับรหัสผ่านชั่วคราว

๒.๗.๖. ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชาของหน่วยงานเจ้าของระบบ โดยต้องกำหนดระยะเวลาใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาสิทธิพิเศษที่ได้รับ

๒.๘. การทบทวนสิทธิในการเข้าถึงระบบของผู้ใช้งาน ผู้ดูแลระบบต้องทบทวนสิทธิในการเข้าถึงระบบสารสนเทศตามระยะเวลาที่กำหนดไว้ อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อเปลี่ยนแปลงสถานภาพ

๓. แนวปฏิบัติการควบคุมการเข้าถึงหรือใช้ระบบปฏิบัติการ (Operating System)

๓.๑. ผู้ใช้งานเครื่องคอมพิวเตอร์จะต้องสร้าง ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ในการเข้าใช้งาน ระบบปฏิบัติการของเครื่องคอมพิวเตอร์

๓.๒. ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ของมหาวิทยาลัย

๓.๓. ผู้ใช้งานต้องทำการลงบันทึกออก (Logout) ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานานกว่า 30 นาที

๓.๔. มีการกำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดย วิธีการยืนยันตัวตนที่มั่นคงปลอดภัย โดยการระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and authentication) โดยจะทำการเก็บข้อมูลการทางจราจรคอมพิวเตอร์ (Log) ในกรณีนี้ มหาวิทยาลัยได้ใช้ระบบ Authentication Firewall เป็นตัวควบคุม

๓.๕. เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (session time-out)

๔. แนวปฏิบัติการใช้งานบัญชีผู้ใช้งาน (Account)

๔.๑. ผู้ใช้งานที่เป็นเจ้าของบัญชี ผู้ใช้งาน (Account) ต้องเป็นผู้รับผิดชอบในผลต่าง ๆ อันจะเกิดขึ้นจากการใช้บัญชี ผู้ใช้งาน (Account) ของเครื่องคอมพิวเตอร์และระบบเครือข่าย เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

๔.๒. ผู้ใช้งานจะต้องเก็บรักษาบัญชีผู้ใช้งาน (Account) ไว้เป็นความลับและห้ามเปิดเผยต่อบุคคลอื่น ห้ามโอน จำหน่าย หรือจ่ายแจกให้ผู้อื่น โดยไม่ได้รับอนุญาต

๔.๓. ผู้ใช้งานจะต้องลงบันทึกเข้า (Login) โดยใช้บัญชีผู้ใช้งาน (Account) ของตนเองและทำการลงบันทึกออก (Logout) ทุกครั้ง เมื่อสิ้นสุดการใช้งานหรือหยุดการใช้งานชั่วคราว

๕. ให้มีการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตและผ่านการฝึกอบรม หลักสูตร การสร้างความตระหนักเรื่องความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Awareness Training) เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต มีรายละเอียด ดังนี้

๕.๑. สร้างความรู้ ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงต้องใช้มาตรการเชิงป้องกันตามความเหมาะสมโดยผู้เชี่ยวชาญเฉพาะด้าน

๕.๒. การบริหารจัดการสิทธิ์ของผู้ใช้งาน (User Management) จัดให้มีการควบคุมและจำกัดสิทธิ์เพื่อเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิ์จำเพาะ สิทธิ์พิเศษ และสิทธิ์อื่น ๆ ที่เกี่ยวข้องกับการเข้าถึง

๕.๓. การทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน (Review of User Access Rights) ให้มีกระบวนการทบทวนสิทธิ์การเข้าถึงของผู้ใช้งานระบบสารสนเทศตามระยะเวลาที่กำหนดไว้ เมื่อมีเจ้าหน้าที่หรือพนักงานของมหาวิทยาลัยลาออกจากงานไปแล้วโดยปกติ จะต้องทำการเก็บข้อมูลไว้ระยะหนึ่งตามความเหมาะสมและความเห็นของผู้มีอำนาจตามสายงานนั้น ๆ ซึ่งเมื่อถึงระยะรอบเวลาดังกล่าว สำนักวิทยบริการและเทคโนโลยีสารสนเทศ สอบถามไปยังผู้มีอำนาจตามสายงาน โดยวิธีการส่งจดหมายอิเล็กทรอนิกส์ (e-mail) หรือ บันทึกข้อความ ทั้งนี้ขึ้นอยู่กับความเหมาะสม ของแต่ละครั้งไป

๖. แนวปฏิบัติการใช้รหัสผ่าน (Password)

๖.๑. รหัสผ่าน (Password) ต้องมีมากกว่าหรือเท่ากับ ๘ ตัวอักษร โดยผสมกันระหว่างตัวอักษร (a-z, A-Z) ตัวเลข (0-9) เครื่องหมายหรืออักขระพิเศษ (! @ # $ % ^ & * ( ) _ + | ~- = \ ` { } [ ] : ” ; ' < > ? , . /) เข้าด้วยกัน

๖.๒. ไม่กำหนดรหัสผ่าน (Password) จากชื่อหรือชื่อสกุลของผู้ใช้งาน ชื่อบุคคลในครอบครัว บุคคลที่มีความสัมพันธ์กับตนหรือคำศัพท์ที่ใช้ในพจนานุกรมหรือจากหมายเลขโทรศัพท์ และไม่กำหนดรหัสผ่านอย่างเป็นแบบแผนซึ่งง่ายต่อการคาดเดา

๖.๓. ทำการเปลี่ยนรหัสผ่าน (Password) เพื่อใช้งานเครื่องคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ของมหาวิทยาลัยทุก ๓-๖ เดือน หรือเปลี่ยนรหัสผ่าน (Password) ทุกครั้งที่มีสัญญาณบอกเหตุว่าอาจรั่วไหล

๖.๔. ในการเปลี่ยนรหัสผ่านแต่ละครั้งไม่กำหนดรหัสผ่านใหม่ให้ซ้ำของเดิมครั้งสุดท้าย

๖.๕. ผู้ใช้งานที่ได้รับรหัสผ่านในครั้งแรก (Default Password) หรือได้ รับรหัสผ่านใหม่และให้เปลี่ยนรหัสผ่านนั้นโดยทันที

๖.๖. ผู้ใช้งานเก็บรักษารหัสผ่าน (Password) สำหรับการใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายคอมพิวเตอร์ที่ได้มา โดยถือว่าเป็นความลับเฉพาะบุคคล และจะต้องไม่เปิดเผยหรือกระทำการใดให้ผู้อื่นทราบ

๖.๗. หากมีการนำอุปกรณ์สื่อสารสนเทศอื่น ๆ เข้ามาต่อพ่วงได้แก่ แฟลชไดร์ฟ, สมาร์ทโฟน, กล้องดิจิตอล ผู้ใช้งานจะต้องแน่ใจว่าอุปกรณ์เหล่านั้นไม่ก่อให้เกิดความเสียหายต่ออุปกรณ์คอมพิวเตอร์ภายในมหาวิทยาลัย หากจำเป็นต้องมีการเชื่อมต่อให้แจ้งเจ้าหน้าที่ งานเทคโนโลยีสารสนเทศ สำนักวิทยบริการและเทคโนโลยีสารสนเทศ เพื่อทำการตรวจสอบก่อนการใช้งาน

๖.๘. การนำวิธีการเข้ารหัสข้อมูลมาใช้กับข้อมูลที่เป็นความลับ ผู้ใช้งานจะต้องปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ และต้องใช้วิธีการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล

๗. แนวปฏิบัติการใช้งานระบบอินเทอร์เน็ตและเครือข่ายสังคมออนไลน์ (Internet and Social Networking)

๗.๑. ผู้ใช้งานต้องเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานระบบอินเทอร์เน็ต (Internet) ผ่านระบบรักษาความปลอดภัยที่มหาวิทยาลัยจัดสรรไว้เท่านั้น และห้ามผู้ใช้งานทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น ยกเว้นแต่ว่ามีเหตุผลความจำเป็นและได้รับอนุญาตจากอธิการบดีเป็นลายลักษณ์อักษรแล้ว

๗.๒. ผู้ใช้งาน ต้องเข้าถึงระบบเทคโนโลยีสารสนเทศตามสิทธิ์ที่ได้รับตามหน้าที่ความรับผิดชอบเท่านั้น และเพื่อประสิทธิภาพของระบบเครือข่ายและความปลอดภัยทางข้อมูลของมหาวิทยาลัย ต้องไม่ใช้ระบบอินเทอร์เน็ต (Internet) ของมหาวิทยาลัยเพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม ได้แก่ เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับมหาวิทยาลัย

๗.๓. ห้ามผู้ใช้งานเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของมหาวิทยาลัย ที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต (Internet)

๗.๔. ผู้ใช้งาน ต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากระบบอินเทอร์เน็ต (Internet) ซึ่งรวมถึงการดาวน์โหลดการอัพเดท (Update) โปรแกรมต่าง ๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์ หรือทรัพย์สินทางปัญญา

๗.๕. ในการใช้งานเครือข่ายสังคมออนไลน์ กระดานสนทนาอิเล็กทรอนิกส์ (Web board) ผู้ใช้งานต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของมหาวิทยาลัย

๗.๖. ในการใช้งานเครือข่ายสังคมออนไลน์ กระดานสนทนาอิเล็กทรอนิกส์ (Web board) ผู้ใช้งานต้องไม่เสนอความคิดเห็น ใช้ข้อความที่ยั่วยุ ให้ร้าย อันจะก่อให้เกิดความเสื่อมเสียต่อชื่อเสียงของมหาวิทยาลัยหรือการทำลายความสัมพันธ์กับบุคลากรของมหาวิทยาลัย

๗.๗. การใช้งานหรือใช้บริการเว็บไซต์เครือข่ายสังคมออนไลน์ ต้องใช้งานเพื่อประโยชน์ของทางราชการเป็นสำคัญ

๗.๘. ในการใช้งาน เครือข่ายสังคมออน ไลน์ผู้ใช้งาน ต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของมหาวิทยาลัย

๗.๙. หากผู้ใช้งานทราบหรือคาดการณ์ในภายหลังว่าการใช้งานเครือข่ายสังคมออนไลน์ของท่าน อาจมีผลกระทบกับมหาวิทยาลัย ผู้ใช้งานต้องแจ้งงานเทคโนโลยีสารสนเทศ สำนักวิทยบริการและเทคโนโลยีสารสนเทศโดยเร็วที่สุด เพื่อดำเนินการ ตามความเหมาะสม

๗.๑๐. หลังจากใช้งานระบบอินเทอร์เน็ต (Internet) เสร็จแล้ว ให้ผู้ใช้งานทำการปิดเว็บเบราเซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น

๘. แนวปฏิบัติการใช้งานและการควบคุมการใช้งานจดหมายอิเล็กทรอนิกส์ (e-mail)

๘.๑. แนวปฏิบัติการใช้งานสำหรับผู้ใช้งาน (User)

๘.๑.๑. ผู้ใช้ต้องมีบัญชีผู้ใช้ (User) และรหัสผ่าน (Password) บัญชีสมาชิกอินเทอร์เน็ตของมหาวิทยาลัย

๘.๑.๒. ผู้ใช้งานไม่ควรบันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

๘.๑.๓. ผู้ใช้งานต้องมีการเปลี่ยนรหัสผ่าน (Password) ทุก ๓-๖ เดือนหรือตามระยะเวลาที่เหมาะสม

๘.๑.๔. ผู้ใช้งานต้องไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (e-mail address) ของผู้อื่นเพื่ออ่าน รับส่งข้อความ เว้นแต่จะได้รับความยินยอมจากเจ้าของผู้ใช้งานและให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์ (e-mail) เป็นผู้รับผิดชอบต่อการใช้งานต่าง ๆ ในจดหมายอิเล็กทรอนิกส์ (e-mail) ของตน

๘.๑.๕. หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (e-mail) เสร็จสิ้นผู้ใช้งานให้ทำการลงบันทึกออก (Logout) ทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้ามาสวมสิทธิ์การใช้งาน

๘.๑.๖. ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับ ผู้ใช้งานต้องไม่ระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์ (e-mail)

๘.๑.๗. ผู้ใช้งานมีหน้าที่ จะต้องรักษาชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เป็นความลับไม่ให้รั่วไหลไปถึงบุคคลที่ไม่เกี่ยวข้อง

๘.๒. แนวทางการควบคุมการใช้งานสำหรับผู้ดูแลระบบ

๘.๒.๑. ผู้ดูแลระบบได้ กำหนดสิทธิ์ การเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ (e-mail) ของมหาวิทยาลัย ให้เหมาะสมกับการเข้าใช้บริการของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของผู้ใช้งาน รวมทั้งมีการทบทวนสิทธิ์ การเข้าใช้งานอย่างสม่ำเสมอ ได้แก่ การลาออก การโอนย้าย โดยจะต้องได้รับหนังสือจากต้นสังกัดของผู้ใช้งานเพื่อยืนยันการเพิ่ม ลดสิทธิ์รวมไปถึงการทำลายข้อมูล เป็นต้น

๙. แนวปฏิบัติ ให้มีการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application and Information Access Control) โดยมีรายละเอียด ดังนี้

๙.๑. การจำกัดการเข้าถึงสารสนเทศ (Information access restriction)

๙.๑.๑. ผู้ดูแลระบบต้องจัดให้มีการลงทะเบียนผู้ใช้งาน พร้อมทั้งกำหนดสิทธิตามอำนาจหน้าที่ที่ได้รับ จะต้องมีการทบทวนสิทธิการใช้งาน

๙.๑.๒. ผู้ดูแลระบบต้องกำหนดระยะเวลาในการเชื่อมต่อกับระบบงาน (Session Time Out) หากมีการเว้นว่างจากการใช้งานเกินระยะเวลา ๑๕ นาที ต้องทำการยุติการใช้งานทันที

๙.๑.๓. ผู้ดูแลระบบ ต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

๙.๒. การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก (Outsourced software development)

๙.๒.๑. จัดให้มีการควบคุมโครงการพัฒนาซอฟต์แวร์โดยผู้รับจ้างให้บริการจากภายนอก

๙.๒.๒. พิจารณาระบุว่าใครจะเป็นผู้มีสิทธิ์ในทรัพย์สินทางปัญญาสำหรับซอร์สโค้ด ในการพัฒนาซอฟต์แวร์

๙.๒.๓. พิจารณากำหนดเรื่องการสงวนสิทธิ์ที่จะตรวจสอบด้านคุณภาพและความถูกต้องของซอฟต์แวร์โดยระบุไว้ในสัญญาจ้าง

๙.๒.๔. หลังจากการส่งมอบการพัฒนาซอฟต์แวร์จากหน่วยงานภายนอก หน่วยงานต้องดำเนินการเปลี่ยนรหัสผ่านต่าง ๆ

๙.๓. ระบบซึ่งไวต่อการรบกวนมีผลกระทบและมีความสำคัญสูงต่อองค์กร จะได้รับการแยกออกจากระบบอื่น ๆ

๙.๓.๑. การแยกระบบสารสนเทศที่มีความสำคัญสูงและจำเป็นต้องได้รับการดูแลเป็นพิเศษ ต้องแยกระบบซึ่งไวต่อการรบกวนดังกล่าวออกจากระบบอื่น ๆ ให้ทำงานอยู่บนเครื่องเซิฟเวอร์ หรือคอมพิวเตอร์ไม่ใช้ปะปนกับระบบอื่น เพื่อป้องกันความผิดพลาดอันอาจจะเกิดจากระบบอื่นซึ่งทำงานอยู่บนเครื่องเดียวกัน ซึ่งต้องติดติดตั้งห้องคอมพิวเตอร์แม่ข่ายที่มีสภาพแวดล้อมเหมาะสม

๙.๓.๒. ให้มีการควบคุมสภาพแวดล้อมของระบบโดยเฉพาะ ได้แก่ ห้องคอมพิวเตอร์แม่ข่าย ระบบไฟฟ้า ระบบสำรองไฟฟ้า ระบบควบคุมการเข้า-ออกห้องคอมพิวเตอร์แม่ข่าย และอื่น ๆ เพื่อป้องกันการหยุดชะงักการทำงานของระบบ

๙.๓.๓. ควบคุมการเข้ามาใช้งานจากเครือข่ายภายในและเครือข่ายภายนอก กำหนดสิทธิการเข้าใช้งาน โดยกำหนดค่าที่ Firewall

๙.๔. การควบคุมคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ได้กำหนดข้อปฏิบัติและมาตรการที่เหมาะสมเพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และสื่อสาร มีการควบคุมหรือป้องกันอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกหน่วยงาน (Mobile computing and teleworking) ที่เกี่ยวข้องกับระบบดังกล่าว

๙.๕. การควบคุมการปฏิบัติงานจากภายนอกมหาวิทยาลัย (Teleworking) หรือ การควบคุมระยะไกล (Remote Desktop) กำหนดข้อปฏิบัติแผนงานและขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานภายนอกมหาวิทยาลัย ทั้งนี้จะให้บริการในส่วนนี้ผ่านทางหน้าเว็บไซต์ ซึ่งจะมีระบบไฟร์วอลล์ (Firewall) เป็นตัวควบคุมและบริหารจัดการการส่ง-รับข้อมูลผ่านการทำงานประเภทการปฏิบัติงานจากภายนอกมหาวิทยาลัย (Teleworking) หรือการควบคุมระยะไกล (Remote Desktop)

๙.๕.๑. ผู้ดูแลระบบต้องควบคุมการปฏิบัติงานของผู้ใช้งานจากระยะไกลตามแนวปฏิบัติการควบคุมการเข้าใช้งานระบบจากภายนอก รวมถึงการเตรียมการระบบเทคโนโลยีสารสนเทศที่เกี่ยวข้องเพื่อให้มีความมั่นคงปลอดภัย

๙.๕.๒. ผู้ดูแลระบบเตรียมการป้องกันทางกายภาพสำหรับระบบสื่อสารข้อมูลจากระยะไกลและระบบงานต่าง ๆ ภายในมหาวิทยาลัย ก่อนที่จะอนุญาตให้เริ่มปฏิบัติงานจากระยะไกลตามแนวปฏิบัติการควบคุมการเข้าถึงระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย

ส่วนที่ ๓
แนวปฏิบัติการควบคุมการเข้าถึงระบบสารสนเทศ
(Access Control)

๑. วัตถุประสงค์

เพื่อจำกัดการเข้าถึงสารสนเทศ และอุปกรณ์ประมวลผลสารสนเทศเฉพาะผู้ที่ไดรับอนุญาต ควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล ให้คำนึงถึงการใช้งานและความมั่งคงปลอดภัย กำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึง การกำหนดสิทธิ์ การมอบอำนาจ และให้ผู้ใช้งานได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ โดยให้มีการการปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัยของมหาวิทยาลัย

๒. การควบคุมการเข้าถึงระบบสารสนเทศ (Access Control)

๒.๑. ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศจะต้องขออนุญาตเป็นลายลักษณ์อักษร และได้รับการพิจารณาจากหัวหน้าหน่วยงาน/ผู้รับผิดชอบ/เจ้าของข้อมูล/เจ้าของระบบ หรือผู้ดูแลระบบที่ได้รับมอบหมาย โดยผ่านการลงทะเบียนในระบบบัญชีสมาชิกอินเทอร์เน็ต และบุคคลภายนอกให้ลงทะเบียนผ่านระบบบัญชีสมาชิกชั่วคราว

๒.๒. การระงับสิทธิ มอบอำนาจ ให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) ที่ได้กำหนดไว้

๒.๓. ผู้ดูแลระบบสารสนเทศ ต้องทำการติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศของมหาวิทยาลัย และตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบข้อมูล

๒.๔. ผู้ดูแลระบบสารสนเทศ ได้จัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบการแก้ไขเปลี่ยนแปลงสิทธิ์ต่าง ๆ และการผ่านเข้า-ออกสถานที่ตั้งของระบบของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาตเพื่อเป็นหลักฐานในการตรวจสอบ

๒.๕. ผู้ดูแลระบบได้ บริหารจัดการสิทธิ์ ของผู้ใช้งาน ดังต่อไปนี้

๒.๕.๑. กำหนดจำแนกประเภทสิทธิ์ตามหน้าที่และความรับผิดชอบ โดยจัดเก็บและมอบหมายสิทธิ์ ให้แก่ผู้ใช้งานระบบสารสนเทศซึ่งจะมีสิทธิ์ตามลำดับชั้นการเข้าถึงข้อมูล ดังนี้

(๑) สิทธิอ่านอย่างเดียว

(๒) สิทธิการเพิ่มข้อมูล

(๓) สิทธิการแก้ไขข้อมูล

(๔) สิทธิการลบข้อมูล

(๕) สิทธิการอนุมัติ/อนุญาต

(๖) ไม่มีสิทธิ

๒.๕.๒. ในกรณี ผู้ใช้งานมีความจำเป็นต้องใช้สิทธิ์สูงกว่าปกติ ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้น

ระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิ์พิเศษที่ได้รับว่าเข้าถึงข้อมูลระดับใดได้บ้างโดยกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติเพื่อผู้ดูแลระบบจะได้ดำเนินการปรับค่าหรือแก้ไขต่อไป

๒.๕.๓. ทำการยกเลิกรหัสผ่าน (Password) เมื่อได้รับการแจ้งจากส่วนบริหารงานบุคคลหรือผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ เมื่อผู้ใช้งานระบบลาออก หรือพ้นจากตำแหน่งหรือยกเลิกอำนาจหน้าที่

๒.๖. การกำหนดเวลาใช้งานระบบสารสนเทศ (Session time-out)

๒.๖.๑. กำหนดให้ระบบสารสนเทศมีการตัดและหมดเวลาการใช้งาน รวมทั้งปิดการใช้งานด้วย หลังจากที่ไม่มีกิจกรรมการใช้งานช่วงระยะเวลา ๑๕ นาที

๒.๖.๒. กำหนดให้ระบบสารสนเทศมีการตัดและหมดเวลาการใช้งานที่สั้นขึ้นสำหรับระบบสารสนเทศที่มีความเสี่ยงสูง

๒.๗. การจำกัดระยะเวลาการเชื่อมต่อระบบเทคโนโลยีสารสนเทศ (Limitation of connection time)

๒.๗.๑. ผู้ดูแลระบบต้องจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection Time) ของผู้ใช้งานไปยังเครื่องปลายทาง เพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศหรือแอพพลิเคชั่นที่มีความเสี่ยงหรือมีความสำคัญสูง ได้แก่ ระบบบัญชีเงินเดือน ระบบฐานข้อมูลบุคคล โดยสามารถเข้าใช้งานระบบในช่วงวันเวลาราชการตั้งแต่เวลา ๘.๓๐-๑๖.๓๐ น. โดยการเชื่อมต่อ ๑ ครั้งอนุญาตให้ใช้งานได้ไม่เกิน ๒ ชั่วโมง ในกรณีมีความจำเป็นเร่งด่วนให้ทำการขออนุมัติจากผู้บังคับบัญชาหรือผู้ที่ได้รับมอบหมายเพื่ออนุมัติให้เข้าใช้งานระบบเป็นครั้งคราว

๒.๗.๒. กำหนดให้ระบบเทคโนโลยีสารสนเทศ ที่มีความสำคัญสูง ระบบงานที่มีการใช้งานในสถานที่ที่มีความเสี่ยง (ในที่สาธารณะหรือพื้นที่ภายนอกหน่วยงาน) มีการจำกัดช่วงระยะเวลาการเชื่อมต่อหลังจากที่ไม่มีกิจกรรมการใช้งานเกิน ๓๐ นาที

๒.๘. จัดแบ่งประเภทของข้อมูล ออกเป็น

๒.๘.๑. ข้อมูลสารสนเทศด้านการบริหาร ได้แก่ ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์ ข้อมูลบุคลากร ข้อมูลงบประมาณการเงินและบัญชี ระบบสารสนเทศเพื่อบริการศึกษา (ESS) ระบบสารสนเทศเพื่อบริหารทรัพยากรองค์กร (ERP) เป็นต้น

๒.๘.๒. ข้อมูลสารสนเทศด้านบริการวิชาการ ได้แก่ ฐานข้อมูลอิเล็กทรอนิกส์ ข้อมูลสื่อการเรียนการสอนออนไลน์ ฐานข้อมูลบัญชีสมาชิกอินเทอร์เน็ต เป็นต้น

๒.๙. จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น ๓ ระดับ คือ

๒.๙.๑. ข้อมูลที่มีระดับความสำคัญมากที่สุด หมายถึง มีผลกระทบรุนแรงต่อการดำรงอยู่ของหน่วยงานหรือปิดหน่วยงาน

๒.๙.๒. ข้อมูลที่มีระดับความสำคัญปานกลาง หมายถึง มีผลกระทบในระดับที่มีนัยสำคัญเล็กน้อย

๒.๙.๓. ข้อมูลที่มีระดับความสำคัญน้อย หมายถึง ไม่มีผลกระทบใด ๆ ต่อการดำเนินภารกิจ

๒.๑๐. จัดแบ่งลำดับชั้นความลับของข้อมูล

๒.๑๐.๑. ข้อมูลลับมาก หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรง

๒.๑๐.๒. ข้อมูลลับ หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย

๒.๑๐.๓. ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

๒.๑๑. จัดแบ่งระดับชั้นประเภทผู้ใช้งาน

๒.๑๑.๑. ระดับชั้นสำหรับผู้บริหาร

๒.๑๑.๒. ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย

๒.๑๑.๓. ระดับชั้นสำหรับผู้ใช้งานทั่วไป

๒.๑๒. จัดแบ่งระดับชั้นการเข้าถึง

๒.๑๒.๑. เข้าถึงได้ทุกกลุ่มผู้ใช้งาน ได้แก่ ข้อมูลทั่วไปที่เปิดเผยได้

๒.๑๒.๒. เข้าถึงได้เฉพาะกลุ่มผู้ใช้งานที่ได้รับสิทธิ์ ได้แก่ ข้อมูลเฉพาะที่ต้องกำหนดสิทธิ์ ข้อมูลลับ

๒.๑๒.๓. เข้าถึงได้เฉพาะผู้มีสิทธิ์ในการบริหารจัดการระบบสารสนเทศ ได้แก่ ข้อมูลระบบ

๒.๑๓. กำหนดช่องทางในการเข้าถึงข้อมูล

๒.๑๓.๑. ผู้ใช้งานเข้าใช้บริการผ่านทางระบบเครือข่ายภายใน ได้ตลอด ๒๔ ชั่วโมง

๒.๑๓.๒. ผู้ใช้งานเข้าใช้บริการผ่านทางระบบเครือข่ายอินเตอร์เน็ตภายนอกมหาวิทยาลัย ผ่านระบบเครือข่ายส่วนตัวเสมือน (VPN) ได้ตลอด ๒๔ ชั่วโมง

๒.๑๔. กำหนดเวลาและจำนวนระยะเวลาในการเข้าถึงข้อมูล

๒.๑๔.๑. ระบบงานบริการสำหรับผู้ใช้งานทั่วไปเข้าถึงได้ตลอดเวลา

๒.๑๔.๒. ระบบงานภายในสำหรับผู้ใช้งานสามารถเข้าถึงระบบตามช่วงเวลา ดังนี้

(๑) เวลาราชการ (๘.๓๐ – ๑๖.๓๐ น.)

(๒) นอกเวลาราชการ (นอกช่วงเวลา ๘.๓๐ – ๑๖.๓๐ น.)

(๓) ช่วงเวลาวันหยุดราชการ (วันหยุดราชการ และวันหยุดนักขัตฤกษ์)

(๔) ช่วงเวลาพิเศษเป็นรายครั้ง โดยระบุช่วงเวลา ระยะเวลาการเข้าถึง

๒.๑๕. มีข้อกำหนดการใช้งานตามภารกิจ เพื่อควบคุมการเข้าถึงสารสนเทศ โดยแบ่งการจัดทำข้อปฏิบัติเป็น ๒ สองส่วน คือ

๒.๑๕.๑. มีการควบคุมการเข้าถึงสารสนเทศ โดยให้กำหนดแนวทางการควบคุมการเข้าถึงระบบสารสนเทศและสิทธิที่เกี่ยวข้องกับระบบสารสนเทศ

๒.๑๕.๒. มีการปรับปรุงให้สอดคล้องกับข้อมูลกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย

๓. การบริหารจัดการการเข้าถึงระบบสารสนเทศของผู้ใช้งาน (User Access Management)

มหาวิทยาลัยโดยผู้ดูแลระบบได้กำหนดการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญได้แก่ ระบบคอมพิวเตอร์ โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (e-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบ

อินเทอร์เน็ต (Internet) เป็นต้น โดยให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษรรวมทั้งได้มีการทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

๓.๑. ผู้ดูแลระบบสารสนเทศ ต้องกำหนดการลงทะเบียนผู้ใช้งานใหม่ดังนี้

๓.๑.๑. จัดทำระบบลงทะเบียนผู้ใช้งานระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัย

๓.๑.๒. ผู้ดูแลระบบต้องตรวจสอบบัญชีผู้ใช้งาน เพื่อไม่ให้มีการลงทะเบียนซ้ำซ้อน

๓.๑.๓. ผู้ดูแลระบบต้องตรวจสอบและให้สิทธิ์ผู้ใช้ทั่วไป สิทธิ์จำเพาะ สิทธิพิเศษ และสิทธิอื่น ๆ ในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ

๓.๑.๔. ผู้ดูแลระบบต้องกำหนดให้มีการแสดงเป็นลายลักษณ์อักษรให้แก่ ผู้ใช้งานเพื่อแสดงถึงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งานในการเข้าถึงระบบเทคโนโลยีสารสนเทศ

๓.๒. ผู้ดูแลระบบสารสนเทศ ต้องกำหนดการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์ โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (e-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเตอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่และได้รับความเห็นชอบเป็นลายลักษณ์อักษร

๓.๓. ผู้ดูแลระบบสารสนเทศ ต้องทบทวนบัญชีผู้ใช้งาน สิทธิ์การใช้งาน อย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต โดยตรวจสอบเปรียบเทียบกับระบบบริหารงานบุคคล

๓.๔. การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management)

๓.๔.๑. การยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานลาออกหรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน

๓.๔.๒. กำหนดชื่อผู้ใช้งานหรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

๓.๔.๓. ส่งมอบรหัสผ่าน (Password) ให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัยหลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (e-mail) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน (Password)

๓.๔.๔. กำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่าน (Password) ผิดพลาดได้ไม่เกิน ๓ ครั้ง

๓.๔.๕. กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

๓.๕. ผู้ดูแลระบบสารสนเทศ ต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับ ในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ มีดังต่อไปนี้

๓.๔.๑. ควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

๓.๔.๒. กำหนดรายชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้งานข้อมูลในแต่ละชั้นความลับของข้อมูล

๓.๔.๓. การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL, VPN หรือ XML Encryption เป็นต้น

๓.๔.๔. กำหนดการเปลี่ยนรหัสผ่าน (Password) ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

๓.๔.๕. เจ้าของข้อมูลต้องมีการตรวจสอบความเหมาะสมของสิทธิ์ในการเข้าถึงข้อมูลของผู้ใช้งาน อย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิ์ต่าง ๆ ที่ให้ไว้ยังคงมีความเหมาะสม

๓.๖. ระบบงานสารสนเทศทางธุรกิจที่เชื่อมโยงกัน (Business Information Systems) ให้หัวหน้าหน่วยงานพิจารณาประเด็นต่าง ๆ ทางด้านความมั่นคงปลอดภัย และจุดอ่อนต่าง ๆ ก่อนตัดสินใจใช้ข้อมูลร่วมกันในระบบงาน หรือระบบเทคโนโลยีสารสนเทศที่จะเชื่อมโยงเข้าด้วยกัน

๔. การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

๔.๑. การใช้งานรหัสผ่าน ผู้ใช้งานต้องปฏิบัติ ดังนี้

๔.๑.๑. กำหนดรหัสผ่าน (Password) ต้องมีมากกว่าหรือเท่ากับ ๘ ตัวอักษร โดยผสมกันระหว่างตัวอักษร (a-z, A-Z) ตัวเลข (0-9) เครื่องหมายหรืออักขระพิเศษ (! @ # $ % ^ & * ( ) _ + | ~- = \ ` { } [ ] : ” ; ' < > ? , . /) เข้าด้วยกัน

๔.๑.๒. ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

๔.๑.๓. ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่ผู้ใช้งานครอบครองอยู่

๔.๑.๔. ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

๔.๑.๕. กำหนดรหัสผ่านเริ่มต้นให้กับผู้ใช้งานให้ยากต่อการเดา และการส่งมอบรหัสผ่านให้กับผู้ใช้งานต้องเป็นไปอย่างปลอดภัย

๔.๒. การนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ ผู้ใช้งานจะต้องปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ และต้องใช้วิธีการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล

๔.๓. การกระทำใด ๆ ที่เกิดจากการใช้บัญชีของผู้ใช้งาน (Username) อันมีกฎหมายกำหนดให้เป็นความผิด ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม ให้ถือว่าเป็นความรับผิดชอบส่วนบุคคลซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

๔.๔. ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนที่จะใช้สินทรัพย์หรือระบบสารสนเทศของหน่วยงาน และหากการพิสูจน์ตัวตนนั้นมีปัญหา ไม่ว่าจะเกิดจากรหัสผ่านล็อกก็ดีหรือเกิดจากความผิดพลาดใด ๆ ก็ดีผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบทันทีโดยปฏิบัติตามแนวทาง ดังนี้

๔.๑.๑. คอมพิวเตอร์ทุกประเภท ก่อนการเข้าถึงระบบปฏิบัติการต้องทำการพิสูจน์ตัวตนทุกครั้ง

๔.๑.๒. การใช้งานระบบคอมพิวเตอร์อื่นในเครือข่ายจะต้องทำการพิสูจน์ตัวตนทุกครั้ง

๔.๑.๓. การใช้งานอินเตอร์เน็ต (Internet) ต้องทำการพิสูจน์ตัวตน และต้องมีการบันทึกข้อมูลซึ่งสามารถบ่งบอกตัวตนบุคคลผู้ใช้งานได้

๔.๑.๔. เมื่อผู้ใช้งานไม่อยู่ที่เครื่องคอมพิวเตอร์ต้องทำการล็อกหน้าจอทุกครั้ง และต้องทำการพิสูจน์ตัวตนก่อนการใช้งานทุกครั้ง

๔.๑.๕. เครื่องคอมพิวเตอร์ทุกเครื่องต้องทำการตั้งเวลาพักหน้าจอ (Screen Saver) โดยตั้งเวลาอย่างน้อย ๑๕ นาที

๔.๕. ข้อมูลที่เป็นความลับหรือมีระดับความสำคัญ ที่อยู่ในการครอบครอง/ดูแลของหน่วยงาน ห้ามไม่ให้ทำการเผยแพร่ เปลี่ยนแปลง ทำซ้ำ หรือทำลาย โดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงาน

๔.๖. ผู้ใช้งานมีส่วนร่วมในการดูแลรักษาและรับผิดชอบต่อข้อมูลของมหาวิทยาลัย และข้อมูลของผู้รับบริการ หากเกิดการสูญหาย โดยนำไปใช้ในทางที่ผิด การเผยแพร่โดยไม่ได้รับอนุญาต ผู้ใช้งานต้องมีส่วนร่วมในการรับผิดชอบต่อความเสียหายนั้นด้วย

๔.๗. ผู้ใช้งานต้องป้องกัน ดูแล รักษาไว้ซึ่งความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูลตลอดจนเอกสาร สื่อบันทึกข้อมูลคอมพิวเตอร์ หรือสารสนเทศต่าง ๆ ที่เสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ์

๔.๘. ผู้ใช้งานมีสิทธิ์โดยชอบธรรมที่จะเก็บรักษา ใช้งาน และป้องกันข้อมูลส่วนบุคคลตามเห็นสมควร มหาวิทยาลัยจะให้การสนับสนุนและเคารพต่อสิทธิส่วนบุคคล และไม่อนุญาตให้บุคคลหนึ่งบุคคลใดทำการละเมิดต่อข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตจากผู้ใช้งานที่ครอบครองข้อมูลนั้น ยกเว้นในกรณีที่มหาวิทยาลัยต้องการตรวจสอบข้อมูล หรือคาดว่าข้อมูลนั้นเกี่ยวข้องกับมหาวิทยาลัยซึ่งมหาวิทยาลัยอาจแต่งตั้งให้ผู้ทำหน้าที่ตรวจสอบ ทำการตรวจสอบข้อมูลเหล่านั้นได้ตลอดเวลา โดยไม่ต้องแจ้งให้ผู้ใช้งานทราบ

๔.๙. ห้ามใช้สินทรัพย์ของหน่วยงาน ที่จัดเตรียมให้เพื่อการเผยแพร่ ข้อมูล ข้อความ รูปภาพหรือสิ่งอื่นใด ที่มีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมาย หรือกระทบต่อภารกิจของมหาวิทยาลัย

๔.๑๐. ห้ามใช้สินทรัพย์ของหน่วยงาน เพื่อการรบกวน ก่อให้เกิดความเสียหาย หรือใช้ในการโจรกรรมข้อมูล หรือสิ่งอื่นใดอันเป็นการขัดต่อกฎหมายและศีลธรรม หรือกระทบต่อภารกิจของมหาวิทยาลัย

๔.๑๑. ห้ามใช้สินทรัพย์ของมหาวิทยาลัยเพื่อประโยชน์ทางการค้า

๔.๑๒. ห้ามกระทำการใด ๆ เพื่อการดักข้อมูล ไม่ว่าจะเป็นข้อความ ภาพ เสียง หรือสิ่งอื่นใดในเครือข่ายระบบสารสนเทศของมหาวิทยาลัย โดยเด็ดขาด ไม่ว่าจะด้วยวิธีการใด ๆ ก็ตาม

๔.๑๓. ห้ามกระทำการรบกวน ทำลาย หรือทำให้ระบบสารสนเทศของหน่วยงานต้องหยุดชะงัก

๔.๑๔. ห้ามใช้ระบบสารสนเทศของมหาวิทยาลัย เพื่อการควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอก โดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบที่ได้รับมอบหมาย

๔.๑๕. ห้ามกระทำการใด ๆ อันมีลักษณะเป็นการลักลอบใช้งานหรือรับรู้รหัสส่วนบุคคลของผู้อื่นไม่ว่าจะเป็นกรณีใด ๆ เพื่อประโยชน์ในการเข้าถึงข้อมูล หรือเพื่อการใช้ทรัพยากรก็ตามห้ามติดตั้งอุปกรณ์หรือกระทำการใด ๆ เพื่อเข้าถึงระบบสารสนเทศของมหาวิทยาลัย โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบที่ได้รับมอบหมาย

๔.๑๖. การป้องกันอุปกรณ์ที่ไม่มีผู้ดูแล ผู้ใช้งานต้องมีวิธีเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิเข้าถึงอุปกรณ์สำนักงานที่ไม่มีผู้ใช้ดูแล เพื่อป้องกันข้อมูลสำคัญสูญหาย

๔.๑๖.๑. ผู้ดูแลระบบมีอำนาจที่จะยุติหรือเพิกถอนสิทธิการใช้คอมพิวเตอร์และเครือข่ายโดยทันที หากตรวจพบผู้ใช้ที่ฝ่าฝืนระเบียบหรือกระทำการใดที่อาจสร้างความเสียหายให้กับระบบ

๔.๑๖.๒. เครื่องคอมพิวเตอร์ส่วนบุคคลทุกเครื่องต้องติดตั้งระบบ Screen Saver โดยกำหนดรหัสในการเข้าใช้

๔.๑๖.๓. การรักษาความลับของข้อมูลในเครื่องคอมพิวเตอร์ หรืออุปกรณ์สำนักงานจะเป็นความรับผิดชอบของผู้ใช้งานประจำเครื่องคอมพิวเตอร์ หรืออุปกรณ์สำนักงานนั้น

ส่วนที่ ๔
แนวปฏิบัติการควบคุมการเข้าถึงระบบเครือข่าย
(Network Access Control)

๑. วัตถุประสงค์

เพื่อควบคุมการเข้าถึงระบบเครือข่ายของมหาวิทยาลัย โดยคำนึงถึงการใช้งานและความมั่งคงปลอดภัย กำหนดกฎเกณฑ์ที่เกี่ยวกับการเข้าถึงระบบเครือข่าย ระบบเครือข่ายไร้สาย อุปกรณ์เชื่อมต่อเครือข่าย การป้องกันพอร์ต การแบ่งแยกเครือข่าย และการบริหารจัดการคอมพิวเตอร์แม่ข่าย

๒. การเข้าใช้งานระบบเครือข่าย (Network Access)

๒.๑. การพิสูจน์ตัวตน (Authentication) สำหรับผู้ใช้งานระบบเครือข่ายของมหาวิทยาลัยจะต้องพิสูจน์ตัวตนด้วยบัญชีผู้ใช้ที่มหาวิทยาลัยออกให้ ซึ่งผู้ใช้สามารถสมัครใช้งานได้ที่ระบบจัดการข้อมูลและบริการอินเทอร์เน็ต*

๒.๒. ผู้ใช้งานที่ได้รับอนุญาตเข้าถึงระบบเครือข่าย สามารถเข้าใช้ได้เฉพาะบริการในระบบเครือข่ายตามสิทธิ์ที่ได้รับอนุญาตเท่านั้น

๒.๓. การพิสูจน์ตัวตนสำหรับผู้ใช้งานที่อยู่ภายนอกมหาวิทยาลัย ต้องใช้ “บัตรประจำตัวประชาชน” เป็นหลักฐานสำหรับขออนุญาตใช้งาน ระบบเครือข่ายและระบบสารสนเทศของมหาวิทยาลัย ซึ่งจะเข้าถึงได้ตามสิทธิ์ที่ได้รับอนุญาต

๒.๔. ช่องทางในการเข้าถึงระบบเครือข่ายจากภายนอกองค์กร (User authentication for external connections) ให้เข้าใช้งานผ่านระบบ VPN และต้องใช้รหัสบัญชีผู้ใช้ของมหาวิทยาลัยยืนยันตัวตนก่อนเข้าใช้เท่านั้น

๒.๕. กำหนดเวลาและจำนวนระยะเวลาในการเข้าถึงข้อมูล ระบบงานบริการสำหรับผู้ใช้งานทั่วไปเข้าถึงได้ตลอดเวลา ระบบงานภายในสำหรับผู้ใช้งานสามารถเข้าถึงระบบตามช่วงเวลา ดังนี้

๖.๔.๑. เวลาราชการ (๘.๓๐-๑๖.๓๐ น.)

๖.๔.๒. นอกเวลาราชการ (นอกช่วงเวลา ๘.๓๐-๑๖.๓๐ น.)

๖.๔.๓. ช่วงเวลาวันหยุดราชการ (วันหยุดราชการ และวันหยุดนักขัตฤกษ์)

๖.๔.๔. ช่วงเวลาพิเศษเป็นรายครั้ง โดยระบุช่วงเวลา ระยะเวลาการเข้าถึง

๓. การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (WLAN : Wireless Local Area Network)

๓.๑. ผู้ดูแลระบบเครือข่าย ดำเนินการควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (Access-Point) ให้รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายน้อยที่สุด

๓.๒. ผู้ดูแลระบบเครือข่าย ดำเนินการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าโดยปริยาย (Default) มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณ (Access Point) มาใช้งาน

* ระบบจัดการข้อมูลและบริการอินเทอร์เน็ต หมายถึง ระบบข้อมูลบัญชีสมาชิกที่นำไปใช้กับบริการทางด้านระบบเครือข่ายที่มหาวิทยาลัยฯ เปิดให้บริการ ประกอบด้วย บริการอิเล็กทรอนิกส์เมล์ (e-mail), โฮมเพจส่วนบุคคล (Personal Homepage), ระบบประชาสัมพันธ์ข่าว, เครือข่ายไร้สาย (Wireless Network) และบริการอื่น

๓.๓. ผู้ดูแลระบบเครือข่าย ดำเนินการกำหนดค่า WEP (Wired Equivalent Privacy) หรือ WPA (Wi-Fi Protected Access) ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และ อุปกรณ์กระจายสัญญาณ (Access Point) และกำหนดค่าให้ไม่แสดงชื่อระบบเครือข่ายไร้สายตามความเหมาะสมในกรณีต่าง ๆ

๓.๔. ผู้ดูแลระบบเครือข่าย ใช้วิธีการควบคุมผ่านระบบ Firewall Authentication โดยกำหนดชื่อผู้ใช้ (Username) รหัสผ่าน (Password) สำหรับบุคคลากรภายในมหาวิทยาลัย

๓.๕. ผู้ดูแลระบบเครือข่าย ติดตั้งไฟร์วอลล์ (Firewall) ระหว่างระบบเครือข่ายไร้สายกับระบบเครือข่ายภายในมหาวิทยาลัย

๓.๖. ผู้ดูแลระบบเครือข่าย ใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายเพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย และจัดส่งรายงานผลการตรวจสอบทุก ๓ เดือน และในกรณีที่ตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติ ให้ผู้ดูแลระบบ (System Administrator) รายงานต่อผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศทราบทันที

๓.๗. ผู้ดูแลระบบเครือข่าย ควบคุมดูแลไม่ให้บุคคลภายนอกที่ไม่ได้รับอนุญาตใช้งานระบบเครือข่ายไร้สายในการเข้าสู่ระบบอินทราเน็ต (Intranet) และฐานข้อมูลภายในต่าง ๆ ของมหาวิทยาลัย

๔. การระบุอุปกรณ์ที่นำมาเชื่อมต่อบนเครือข่าย

๔.๑. อุปกรณ์ที่นำมาเชื่อมต่อได้รับหมายเลขไอพีแอดเดรสตามที่กำหนดโดยผู้ดูแลระบบเครือข่าย

๔.๒. เก็บข้อมูลการใช้ MAC Address จากเครื่องบริการกำหนดค่าหมายเลขไอพีแอดเดรส (DHCP Server) หรือจาก ARP Table บนสวิทช์ L3

๕. การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ

๕.๑. ต้องควบคุมพอร์ตและหมายเลขไอพีแอดเดรสที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้เข้าถึงอุปกรณ์เครือข่ายอย่างรัดกุม

๕.๒. ต้องกำหนดรหัสผ่านสำหรับตรวจสอบและปรับแต่งอุปกรณ์เครือข่าย เมื่อใช้การเชื่อมต่อโดยตรงบนตัวอุปกรณ์

๕.๓. ไม่อนุญาตให้เชื่อมต่อพอร์ตโดยตรงจากเครือข่ายภายนอกมหาวิทยาลัย แต่ให้เชื่อมต่อผ่านช่องทางที่ปลอดภัยที่มหาวิทยาลัยกำหนด เช่น VPN เป็นต้น

๕.๔. อุปกรณ์เครือข่ายคอมพิวเตอร์ที่สำคัญต้องจัดเก็บในห้องอุปกรณ์เครือข่ายที่ควบคุมความปลอดภัย

๕.๕. ต้องปิดพอร์ตหรือปิดบริการ บนอุปกรณ์เครือข่ายที่ไม่มีความจำเป็นในการใช้งาน

๕.๖. ต้องตรวจสอบและปิดพอร์ตของระบบหรืออุปกรณ์ที่ไม่มีความจำเป็นในการเข้าใช้งานอย่างสม่ำเสมออย่างน้อยสัปดาห์ละ ๑ ครั้ง

๖. การควบคุมการเข้าถึงระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Network and Servers Connection Control)

๖.๑. มหาวิทยาลัย ได้กำหนดมาตรการควบคุมการ เข้า – ออก ห้องควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server) ที่ไม่ใช่เจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศเพื่องานวิชาการ โดยต้องลงทะเบียนขออนุญาต ระบุวัน-เวลาเข้า-ออกและเหตุผลความจำเป็น

๖.๒. ผู้ใช้งานภายนอกที่จะนำเครื่องคอมพิวเตอร์และอุปกรณ์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์และระบบเครือข่ายของ มหาวิทยาลัย ต้องได้รับอนุญาตจาก ผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ และต้องปฏิบัติตามนโยบายนี้โดยเคร่งครัด

๖.๓. ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใด ๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลักโดยไม่ได้รับอนุญาตจากผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ

๖.๔. ผู้ดูแลระบบเครือข่าย ควบคุมการเข้าถึงระบบเครือข่าย เพื่อบริหารจัดการระบบเครือข่ายได้อย่างมีประสิทธิภาพ ดังต่อไปนี้

๖.๔.๑. ใช้วิธีการจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น

๖.๔.๒. มีวิธีการจำกัดเส้นทางการเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน

๖.๔.๓. มีการกำหนดให้ จำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ของผู้ใช้งานไปยังเครื่องคอมพิวเตอร์แม่ข่าย

๖.๔.๔. ระบบเครือข่ายทั้งหมดของมหาวิทยาลัย ที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกมหาวิทยาลัย ได้ถูกเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก และมีความสามารถในการตรวจจับโปรแกรมประสงค์ร้าย (Malware)

๖.๔.๕. การเข้าสู่ระบบเครือข่ายภายในมหาวิทยาลัย ผ่านทางระบบอินเทอร์เน็ตได้กำหนดให้ ลงบันทึกเข้า (Login) โดยระบุชื่อผู้ใช้งานและรหัสผ่านผู้ใช้งานผ่านระบบพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้องของผู้ใช้งาน

๖.๔.๖. เลขที่อยู่ไอพี (IP Address) ของระบบเครือข่ายภายในมหาวิทยาลัยได้มีการป้องกันหน่วยงานภายนอกที่เชื่อมต่อไม่สามารถมองเห็นได้

๖.๔.๗. จัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอก ที่สามารถระบุบนระบบเครือข่ายและอุปกรณ์บนเครือข่าย พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ และการระบุอุปกรณ์บนเครือข่าย (Equipment Identification in Networks) มีวิธีการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ และใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยัน

๖.๔.๘. การใช้เครื่องมือต่าง ๆ เพื่อการตรวจสอบระบบเครือข่ายจะต้องได้รับการอนุมัติจากผู้ดูแลระบบ (System Administrator) และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

๖.๔.๙. มีการป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection) ควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย ได้แก่

(๑) ต้องตรวจสอบ และปิดพอร์ตที่ไม่มีการใช้งานอยู่เสมอ

(๒) ต้องควบคุมการเข้าถึงระบบผ่านอุปกรณ์ป้องกันการบุกรุก (firewall) ของระบบเครือข่าย

(๓) การขอใช้งานพอร์ตดังกล่าวต้องได้รับอนุญาตจากผู้อำนวยการสำนักบริการและเทคโนโลยีสารสนเทศ หรือผ่านช่องทางที่จัดเตรียมไว้ให้

(๔) ต้องเก็บอุปกรณ์ที่เชื่อมต่อเครือข่ายไว้ในห้องที่มีการควบคุมการเข้าถึง และจะเข้าได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น หรือล็อกกุญแจเพื่อป้องกันการเชื่อมต่อโดยไม่ได้รับอนุญาต

๖.๔.๑๐. มีการควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control) ควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างหน่วยงานให้สอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึง

๖.๔.๑๑. มีการควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control) ควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการ ส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ

๖.๔.๑๒. ผู้ดูแลระบบต้องหนด IP Address ให้กับอุปกรณ์ที่เชื่อมต่อเครือข่ายเพื่อให้สามารถระบุถึงอุปกรณ์เครือข่ายได้อย่างถูกต้อง ในกรณีที่ไม่สามารถใช้ IP Address ระบุถึงอุปกรณ์ได้ กำหนดให้ผู้ใช้งานต้องลงทะเบียน MAC Address อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่าย เพื่อให้สามารถระบุอุปกรณ์เครือข่ายตัวนั้นได้อย่างถูกต้อง

๖.๕. ผู้ดูแลระบบเครือข่าย ทำหน้าที่บริหารควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server) และรับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนดแก้ไขหรือเปลี่ยนแปลงค่าต่าง ๆ ของซอฟต์แวร์ระบบ (Systems Software)

๖.๖. ผู้ดูแลระบบจะต้องทำการป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ ทั้งการเข้าถึงทางกายภาพและผ่านทางเครือข่าย ได้แก่

๖.๖.๑. ต้องตรวจสอบ และปิดพอร์ตที่ไม่มีการใช้งานอยู่เสมอ

๖.๖.๒. ต้องควบคุมการเข้าถึงระบบผ่านอุปกรณ์ป้องกันการบุกรุก (firewall) ของระบบเครือข่าย

๖.๖.๓. การขอใช้งานพอร์ตดังกล่าวต้องได้รับอนุญาตจากผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ หรือผ่านช่องทางที่สำนักวิทยบริการและเทคโนโลยีสารสนเทศ จัดเตรียมไว้ให้

๖.๖.๔. ต้องเก็บอุปกรณ์ที่เชื่อมต่อเครือข่ายไว้ในห้องที่มีการควบคุมการเข้าถึง และจะเข้าได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น หรือล็อกกุญแจเพื่อป้องกันการเชื่อมต่อโดยไม่ได้รับอนุญาต

๖.๗. มหาวิทยาลัยได้กำหนดมาตรการควบคุมการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์ (Log) มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้ตามแนวทาง ดังต่อไปนี้

๖.๗.๑. ความครบถ้วน ถูกต้อง แท้จริง และระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้และข้อมูลที่ใช้ในการจัดเก็บ กำหนดชั้นความลับในการเข้าถึงข้อมูล ซึ่งผู้ดูแลระบบไม่ได้รับอนุญาตให้ แก้ไขข้อมูลที่เก็บรักษาไว้ ยกเว้นผู้ตรวจสอบระบบสารสนเทศของมหาวิทยาลัย (Internal IT Auditor) หรือบุคคลที่มหาวิทยาลัยมอบหมาย

๖.๗.๒. บันทึกการทำงานของระบบบันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุกได้แก่ การบันทึกการเข้า-ออกระบบ การบันทึกการพยายามเข้าสู่ระบบ การบันทึกการใช้งาน Command Line และ Firewall Log เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย ๙๐ วัน นับตั้งแต่การใช้บริการสิ้นสุดลง

๖.๗.๓. ตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานระบบอย่างสม่ำเสมอ

๖.๗.๔. วิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่าง ๆ และจำกัดสิทธิ์การเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

๖.๘. กำหนดมาตรการควบคุมการใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) เพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอกตามแนวทาง ดังต่อไปนี้

๒.๓.๑. บุคคลจาก หน่วยงาน ภายนอกที่ ต้องการสิทธิ์ในการเข้าใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) ของมหาวิทยาลัยจะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษรเพื่อขออนุญาตจากผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ

๒.๓.๒. ผู้ดูแลระบบได้ ควบคุมช่องทาง (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

๒.๓.๓. วิธีการใด ๆ ที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้จากระยะไกลต้องได้รับการอนุญาตจากผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ

๒.๓.๔. การเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องแสดงหลักฐาน ระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ

๒.๓.๕. การเข้าใช้งานต้องผ่านระบบการพิสูจน์ตัวตนจากระบบของมหาวิทยาลัย

๗. การแบ่งแยกเครือข่าย (DMZ : Demilitarized Zone)

๗.๑. ต้องจัดทำแผนผังระบบเครือข่าย ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๗.๒. แบ่งแยกเครือข่ายตามกลุ่มของบริการ กลุ่มผู้ใช้ และระบบงานต่าง ๆ ของมหาวิทยาลัย

๗.๓. ต้องใช้ไฟร์วอลล์กั้นหรือแบ่งเครือข่ายภายในออกเป็นเครือข่ายย่อย ๆ

๗.๔. ต้องใช้เกตเวย์เพื่อควบคุมการเข้าถึงเครือข่ายทั้งจากภายในและภายนอกหน่วยงานซึ่งสอดคล้องกับนโยบายควบคุมการเข้าถึงและนโยบายการใช้งานบริการเครือข่ายของหน่วยงาน

๘. การควบคุมการเชื่อมต่อทางเครือข่ายและการควบคุมการจัดเส้นทางบนเครือข่าย

๘.๑. อนุญาตการเชื่อมต่อเฉพาะหมายเลขไอพีแอดเดรสที่กำหนดให้เท่านั้น

๘.๒. ระบบเครือข่ายที่เชื่อมต่อไปยังเครือข่ายอื่น ๆ ภายนอกมหาวิทยาลัย ต้องติดตั้งระบบตรวจจับการบุกรุก และต้องมีความสามารถในการตรวจจับโปรแกรมไม่ประสงค์ดี

๘.๓. อนุญาตเส้นทางเครือข่ายเฉพาะกลุ่มหมายเลขไอพีแอดเดรสที่กำหนด

๘.๔. มีเกตเวย์เพื่อกรองข้อมูลที่ไหลเวียนในเครือข่าย

๘.๕. ต้องตรวจสอบหมายเลขไอพีแอดเดรสของต้นทางและปลายทาง

๘.๖. ต้องควบคุมการไหลของข้อมูลผ่านเครือข่าย

๘.๗. ต้องกำหนดเส้นทางการไหลของข้อมูลบนเครือข่ายที่สอดคล้องกับการควบคุมการเข้าถึงและการใช้งานบริการเครือข่าย

๘.๘. ต้องจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่ายเพื่อระงับการใช้จากเส้นทางอื่น

๙. การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกมหาวิทยาลัย

๙.๑. ผู้ใช้งานที่จะเข้าใช้งานระบบต้องแสดงตัวตนด้วยชื่อผู้ใช้งานทุกครั้ง

๙.๒. ผู้ใช้งานที่อยู่ภายนอกหน่วยงาน ต้องเป็นผู้ที่ได้รับสิทธิ์ในการเข้าใช้บริการแล้วเท่านั้น

๙.๓. ต้องมีระบบตรวจสอบผู้ใช้งานทุกครั้งก่อนที่จะอนุญาตให้เข้าถึงระบบสารสนเทศของมหาวิทยาลัย โดยจะต้องมีวิธีการยืนยันตัวตนด้วยการป้อนชื่อผู้ใช้งานและรหัสผ่าน เพื่อแสดงว่าเป็นผู้ใช้งานตัวจริง

ส่วนที่ ๕
แนวปฏิบัติการควบคุมการเข้าถึงระบบปฏิบัติการ
(Operating System Access Contron)

๑. วัตถุประสงค์

เพื่อกำหนดการควบคุมการเข้าถึงระบบปฏิบัติการ โดยกำหนดหน้าที่และแนวปฏิบัติ ขั้นตอน การบริหารจัดการรหัสผ่าน การใช้งานโปรแกรมอรรถประโยชน์ ของผู้ดูแลและผู้ใช้งาน

๒. ผู้ดูแลระบบ (System Administrator)

๒.๑. ต้องกำหนดชื่อผู้ใช้งานและรหัสผ่านให้กับระบบปฏิบัติการของเครื่องแม่ข่ายคอมพิวเตอร์ สำหรับบริการงานด้านเทคโนโลยีสารสนเทศของมหาวิทยาลัย

๓. กำหนดขั้นตอนการปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย

๓.๑. ต้องไม่ให้ระบบแสดงรายละเอียดสำคัญของระบบก่อนที่การเข้าสู่ระบบจะเสร็จสมบูรณ์

๓.๒. ระบบสามารถยุติการเชื่อมต่อเครื่องปลายทางได้เมื่อพบว่ามีการพยายามคาดเดารหัสผ่านจากเครื่องปลายทาง

๓.๓. จำกัดระยะเวลาสำหรับใช้ในการป้องกันรหัสผ่าน

๓.๔. จำกัดการเชื่อมต่อโดยตรงสู่ระบบปฏิบัติการผ่านทาง Command Line เนื่องจากอาจสร้างความเสียหายให้กับระบบได้

๔. ระบุและยืนยันตัวตนของผู้ใช้งาน (Authentication)

๔.๑. ผู้ใช้งานต้องมีบัญชีผู้ใช้และรหัสผ่าน สำหรับเข้าใช้งานระบบสารสนเทศของมหาวิทยาลัย

๔.๒. สามารถใช้อุปกรณ์ควบคุมความปลอดภัยเพิ่มเติม หรือวิธีการอื่นที่มีความปลอดภัย

๕. การบริหารจัดการรหัสผ่าน (Password)

๕.๑. ต้องจำกัดระยะเวลาในการป้อนรหัสผ่าน หากผู้ใช้งานป้อนรหัสผ่านผิดเกินจำนวนครั้งที่กำหนด ระบบจะทำการ ระงับสิทธิ์การเข้าถึงของผู้ใช้งาน ทำให้ไม่สามารถใช้งานได้จนกว่าผู้ดูแลระบบจะปลดล็อกให้

๕.๒. ระบบสามารถยุติการเชื่อมต่อจากเครื่องปลายทางได้ เมื่อพบว่ามีความพยายามในการเดารหัสผ่านจากเครื่องปลายทาง

๕.๓. ระบบต้องให้ผู้ใช้งานสามารถเปลี่ยนและยืนยันรหัสผ่านได้ด้วยตนเอง

๕.๔. ต้องจัดเก็บไฟล์ข้อมูลรหัสผ่านของผู้ใช้งานแยกต่างหากจากข้อมูลของระบบงาน

๕.๕. ไม่แสดงข้อมูลรหัสผ่านในหน้าจอของผู้ใช้งานระหว่างที่ผู้ใช้งานกำลังใส่ข้อมูลรหัสผ่านของตนเอง แต่แสดงเป็นเครื่องหมายจุดหรือดอกจันบนหน้าจอแทน

๕.๖. เมื่อได้ดำเนินการติดตั้งระบบแล้ว ให้ยกเลิกชื่อผู้ใช้งานหรือเปลี่ยนรหัสผ่านของทุกชื่อผู้ใช้ที่ได้ถูกกำหนดไว้เริ่มต้นที่มาพร้อมกับการติดตั้งระบบโดยทันที

๖. การใช้งานโปรแกรมอรรถประโยชน์ (Utility Program)

๖.๑. จำกัดสิทธิ์การเข้าถึง และกำหนดสิทธิ์อย่างรัดกุมในการอนุญาตให้ใช้โปรแกรมอรรถประโยชน์

๖.๒. จัดเก็บโปรแกรมอรรถประโยชน์ไว้ในสื่อภายนอก ถ้าไม่ต้องใช้งานเป็นประจำ

๖.๓. ต้องจัดเก็บบันทึกการเรียกใช้งานโปรแกรมเหล่านี้

๖.๔. ต้องถอดถอนโปรแกรมอรรถประโยชน์ที่ไม่จำเป็นออกจากระบบ

๖.๕. โปรแกรมที่ติดตั้ง ต้องเป็นโปรแกรมที่องค์กรได้ซื้อลิขสิทธิ์ถูกต้องตามกฎหมาย

๖.๖. ห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ แล้วนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๗. การหมดเวลาใช้งานระบบสารสนเทศ (Session Time-Out)

๗.๑. ให้กำหนดหลักเกณฑ์การยุติการใช้งานระบบสารสนเทศเมื่อว่างเว้นจากการใช้งานเป็นเวลาไม่เกิน ๓๐ นาที หากเป็นระบบที่มีความเสี่ยงหรือความสำคัญสูง ให้กำหนดระยะเวลายุติการใช้งานระบบเมื่อว่างเว้นจากการใช้งานให้สั้นลงหรือเป็นเวลาไม่เกิน ๑๕ นาทีตามความเหมาะสม เพื่อป้องกันการเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต

๗.๒. ถ้าไม่มีการใช้งานระบบ ต้องทำการยกเลิกการใช้โปรแกรมประยุกต์และการเชื่อมต่อเข้าสู่ระบบโดยอัตโนมัติ

๗.๓. เครื่องปลายทางที่ตั้งอยู่ในพื้นที่ที่มีความเสี่ยงสูงต้องกำหนดระยะเวลาให้ทำการปิด เครื่องโดยอัตโนมัติหลังจากที่ไม่มีการใช้งานเป็นระยะเวลาตามที่กำหนด

๘. การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection Time)

๘.๑. กำหนดหลักเกณฑ์ในการจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ สำหรับระบบสารสนเทศหรือแอปพลิเคชันที่มีความเสี่ยงหรือมีความสำคัญสูง เพื่อให้ผู้ใช้งานสามารถใช้งานได้นานที่สุดภายในระยะเวลาที่กำหนดเท่านั้น ได้แก่ กำหนดให้ใช้งานได้ ๓ ชั่วโมง ต่อการเชื่อมต่อหนึ่งครั้ง เป็นต้น และกำหนดให้ใช้งานได้เฉพาะในช่วงเวลาการทำงานตามปกติของมหาวิทยาลัยเท่านั้น

๘.๒. การกำหนดช่วงเวลาสำหรับการเชื่อมต่อระบบเครือข่ายจากเครื่องปลายทางจะต้องพิจารณาถึงระดับความเสี่ยงของที่ตั้งของเครื่องปลายทางด้วย

๘.๓. กำหนดให้ระบบสารสนเทศ ได้แก่ ระบบงานที่มีความสำคัญสูง และ/หรือระบบงานที่มีการใช้งานในสถานที่ที่มีความเสี่ยงในที่สาธารณะ หรือพื้นที่ภายนอกสำนักงาน มีการจำกัดช่วงระยะเวลาการเชื่อมต่อ

๙. ผู้ใช้งานอาจนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔

ส่วนที่ ๖

แนวปฏิบัติของการเข้าถึงโปรแกรมประยุกต์และระบบสารสนเทศหรือแอพพลิเคชันและสารสนเทศ (Application and Information Access Control)

๑. วัตถุประสงค์

เพื่อควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งาน และสามารถพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัยได้อย่างถูกต้อง ในการเข้าใช้งาน ในการเข้าถึงสารสนเทศและฟังก์ชันต่าง ๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชัน และป้องกันผู้บุรุกในการเข้าถึง โปรแกรมชุดคำสั่งไม่พึงประสงค์ที่จะสร้างความเสียหายกับระบบสารสนเทศหรือข้อมูลของมหาวิทยาลัย หรือทำให้การสื่อสารเสียหาย หยุดชะงัก

๒. การจำกัดการเข้าถึงสารสนเทศ (Information Access Control)

ต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานในการเข้าใช้งานในการเข้าถึงสารสนเทศและฟังก์ชันต่าง ๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชัน โดยให้กำหนดหลักเกณฑ์ในการจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานที่สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้

๒.๑. การจำกัดการเข้าถึงของผู้ใช้งาน ได้แก่ เข้าได้ตามสิทธิ์ที่ได้รับอนุญาตเท่านั้น กำหนดสิทธิ์การเข้าถึงข้อมูลส่วนบุคคล และ ต้องบันทึกการออกจากระบบงานโดยทันทีที่ใช้งานเสร็จ เป็นต้น

๒.๒. แบ่งกลุ่มบุคลากรที่ปฏิบัติงานด้านสารสนเทศของมหาวิทยาลัย ออกเป็น ๓ กลุ่ม คือ ผู้ดูแลระบบ ผู้พัฒนาระบบงาน และผู้ใช้งานระบบ โดยกำหนดหน้าที่รับผิดชอบอย่างชัดเจนเป็นลายลักษณ์อักษร

๒.๓. การบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศ ต้องบันทึกข้อมูลพฤติกรรมการใช้งาน การเข้าถึงระบบสารสนเทศที่สำคัญ ดังนี้

- ๒.๓.๑. ชื่อบัญชีผู้ใช้
- ๒.๓.๒. วันเวลาที่เข้าถึงระบบ
- ๒.๓.๓. วันเวลาที่ออกจากระบบ
- ๒.๓.๔. เหตุการณ์สำคัญที่เกิดขึ้น
- ๒.๓.๕. บันทึกการเข้าใช้ทั้งที่สำเร็จและไม่สำเร็จ
- ๒.๓.๖. ความพยายามในการเข้าถึงทรัพยากรทั้งที่สำเร็จและไม่สำเร็จ
- ๒.๓.๗. แสดงการใช้สิทธิ์ เช่น สิทธิ์ของผู้ดูแลระบบ
- ๒.๓.๘. แสดงการเข้าถึงไฟล์และการกระทำกับไฟล์ เช่น เปิด ปิด เขียน อ่านไฟล์เป็นต้น
- ๒.๓.๙. หมายเลขไอพีแอดเดรสที่เข้าถึง
- ๒.๓.๑๐. แสดงการหยุดการทำงานของระบบป้องกันการบุกรุก
- ๒.๓.๑๑. แสดงการหยุดการทำงานของระบบงานที่สำคัญ ๆ

๒.๔. การควบคุมผู้รับเหมาช่วง (outsource) กรณีมีการจ้างเหมาบำรุงรักษา ดูแล และพัฒนาระบบสารสนเทศ

- ๒.๓.๑. มีกระบวนการคัดเลือกผู้รับเหมาช่วงโดยเฉพาะ และต้องกำหนดคุณสมบัติของผู้รับเหมาช่วงที่ชัดเจน เช่น ต้องมีประสบการณ์มีลูกค้าอ้างอิงน่าเชื่อถือ หรือใบรับรองทางด้านทักษะวิชาชีพตาม

มาตรฐานสากล มีความพร้อมด้านเทคโนโลยีของการรับเหมาช่วงทั้งในส่วนของ ฮาร์ดแวร์และซอฟท์แวร์รวมถึงระบบสนับสนุนอื่น ๆ เพื่อให้ได้ผู้รับเหมาช่วงที่มีคุณสมบัติตรงตามมาตรฐานที่หน่วยงานต้องการ

๒.๓.๒. มีข้อตกลงหรือสัญญาอย่างชัดเจนในการว่าจ้างผู้รับเหมาช่วง และต้องกำหนดขอบเขตและระดับการรับเหมาช่วงอย่างชัดเจน และผู้รับเหมาช่วงต้องนำเสนอรายละเอียดงานขอบเขตงานอย่างครบถ้วน

๒.๓.๓. หน่วยงานต้องเข้าไปตรวจสอบรายละเอียดของการปฏิบัติงานของผู้รับเหมาช่วงได้เช่น ร่วมกำหนดวิธีการทำงาน การตรวจติดตามคุณภาพของผู้รับเหมาช่วงเป็นระยะ ๆ ตามที่กำหนดไว้หรือการสุ่มตรวจสอบการปฏิบัติงานในจุดที่สำคัญ เพื่อพิจารณากระบวนการที่ผู้รับเหมาช่วงใช้ในการปฏิบัติงาน และเพื่อประเมินความสม่ำเสมอของผู้รับเหมาช่วงในการกระทำตามข้อกำหนดของหน่วยงาน

๒.๓.๔. ต้องควบคุมการเข้าถึงของข้อมูลที่ชัดเจน มีระบบบันทึกการเข้าถึงข้อมูล และการสำรองข้อมูลทุกขั้นตอน จำกัดการเข้าถึงข้อมูลสำคัญหรือให้ใช้ข้อมูลจากชุดจำลองแทนข้อมูลจริง

๒.๓.๕. มีหลักเกณฑ์และกระบวนการในการตรวจรับงานที่ส่งมอบโดยผู้รับเหมาช่วงที่ชัดเจน เพื่อให้ได้งานตรงตามมาตรฐานที่กำหนด

๓. ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อมหาวิทยาลัย

ต้องปฏิบัติหรือดำเนินการดังนี้

๓.๑. ต้องแยกระบบซึ่งไวต่อการรบกวนดังกล่าวออกจากระบบอื่น ๆ และแสดงให้เห็นถึงผลกระทบและระดับความสำคัญต่อมหาวิทยาลัย

๓.๒. มีการควบคุมสภาพแวดล้อมของระบบดังกล่าวโดยเฉพาะ

๓.๓. มีการควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ และการปฏิบัติงานจากภายนอกมหาวิทยาลัย (Mobile Computing and Teleworking) ที่เกี่ยวข้องกับระบบดังกล่าว อนุญาตให้ปฏิบัติงานจากภายนอกหน่วยงานโดยต้องใช้งานผ่านช่องทางที่จัดเตรียมไว้ และต้องตรวจสอบตัวตนก่อนการใช้งาน โดยให้เป็นไปตาม แนวปฏิบัติการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ และห้ามนำข้อมูลลับขององค์กรไว้บนอุปกรณ์ส่วนตัว หรือหากมีความจำเป็นต้องใช้งาน เมื่อใช้เสร็จแล้วควรลบทิ้งไป

๔. การควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่

ต้องปฏิบัติหรือดำเนินการดังนี้

๔.๑. ตรวจสอบความพร้อมของคอมพิวเตอร์ และอุปกรณ์ที่จะนำไปใช้งานว่าอยู่ในสภาพพร้อมใช้งานหรือไม่ และตรวจสอบโปรแกรมมาตรฐานว่าถูกต้องตามลิขสิทธิ์

๔.๒. การยืมใช้อุปกรณ์ ต้องมีการบันทึกรายละเอียดการยืมใช้งานอย่างเป็นลายลักษณ์อักษร

๔.๓. ระมัดระวังไม่ให้บุคคลภายนอกคัดลอกข้อมูลจากคอมพิวเตอร์ที่นำไปใช้ได้ เว้นแต่ข้อมูลที่ได้มีการเผยแพร่เป็นการทั่วไป

๔.๔. เมื่อหมดความจำเป็นต้องใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่แล้ว ให้รีบนำส่งคืนเจ้าหน้าที่ที่รับผิดชอบทันที

๔.๕. เจ้าหน้าที่รับผิดชอบในการรับคืนต้องตรวจสอบสภาพความพร้อมใช้งานของอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ที่รับคืนด้วย

๔.๖. หากปรากฏว่าความเสียหายที่เกิดขึ้นนั้น เกิดจากความประมาณอย่างร้ายแรงของผู้นำไปใช้ ผู้นำไปใช้ต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

ส่วนที่ ๗

แนวปฏิบัติหน้าที่และความรับผิดชอบของผู้ดูแลระบบ

(System Administrator Reponsibilities)

๑. วัตถุประสงค์

เพื่อกำหนดหน้าที่และแนวปฏิบัติของผู้ดูแลระบบเครือข่ายและระบบสารสนเทศของมหาวิทยาลัย ในการบริหารจัดการกำกับดูแลเครื่องคอมพิวเตอร์แม่ข่าย (Server) และระบบเครือข่าย (Network) ให้สามารถใช้งานได้ดีอยู่เสมอ

๒. แนวปฏิบัติของผู้ดูแลระบบ

๒.๑. ผู้ดูแลระบบมีอำนาจหน้าที่ ดังต่อไปนี้

๒.๑.๑. ตรวจสอบดูแลรักษาการใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายของมหาวิทยาลัย ให้เป็นไปด้วยความเรียบร้อยและมีประสิทธิภาพ หากตรวจพบสิ่งผิดปกติเกี่ยวกับการใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายให้รีบดำเนินการแก้ไข รวมทั้งป้องกันและบรรเทาความเสียหายที่อาจจะเกิดขึ้นในทันที ในกรณีที่สิ่งผิดปกติดังกล่าวเกิดขึ้นจากการใช้งานของผู้ใช้งานที่ไม่เป็นไปตามนโยบายนี้ ให้รีบแจ้งผู้ใช้งานผู้นั้นให้ยุติการกระทำดังกล่าวในทันที และในกรณีจำเป็นเพื่อป้องกันหรือบรรเทาความเสียหายที่ จะเกิดขึ้นแก่มหาวิทยาลัย ให้ผู้ดูแลระบบ (System Administrator) พิจารณาระงับการใช้ระบบเครือข่ายของผู้ใช้งานดังกล่าวได้ทันที

๒.๑.๒. ตรวจสอบความมั่นคงปลอดภัยในการใช้งานเครื่องคอมพิวเตอร์แม่ข่าย (Server) และระบบเครือข่ายอยู่เสมอ

๒.๑.๓. ติดตั้งและปรับปรุงโปรแกรมคอมพิวเตอร์สำหรับแก้ไขข้อบกพร่องของเครื่องคอมพิวเตอร์และระบบเครือข่าย ให้มีความมั่นคงปลอดภัยในการใช้งานและทันสมัยอยู่เสมอ

๒.๑.๔. ตรวจสอบความมั่นคงปลอดภัยในการใช้งานเครื่องคอมพิวเตอร์แม่ข่าย (Server) และระบบเครือข่าย

๒.๑.๕. เมื่อหมดความจำเป็นในการใช้งานด้วยวิธีการตามมาตรฐาน DOD 5220.22-M * ผู้ดูแลระบบ จะทำการ ลบข้อมูลคอมพิวเตอร์หรือโปรแกรมคอมพิวเตอร์แม่ข่าย (Server) อย่างถาวรหรือทำลายข้อมูลที่เกี่ยวข้องกับการปฏิบัติงานของมหาวิทยาลัย บนเครื่องคอมพิวเตอร์และระบบเครือข่าย

๒.๑.๖. ดูแลรักษาและตรวจสอบช่องทางการสื่อสารของระบบเครือข่ายอยู่เสมอและปิดช่องทางการสื่อสารของระบบเครือข่ายที่ไม่มีความจำเป็นต้องใช้งานในทันที

๒.๑.๗. ดูแลรักษาและปรับปรุงบัญชีจดหมายอิเล็กทรอนิกส์ (e-mail) ให้ถูกต้องและเป็นปัจจุบันอยู่เสมอ โดยให้ยกเลิกสิทธิ์การใช้งานของผู้ใช้งานที่พ้นสภาพการเป็นผู้ใช้งาน

๒.๑.๘. ตรวจสอบเครื่องคอมพิวเตอร์ของผู้ใช้งานให้มีการกำหนดรหัสผ่าน (Password) รวมทั้งการเก็บรักษารหัสผ่าน (Password)

๒.๑.๙. ไม่ใช้อำนาจหน้าที่ของตนในการเข้าถึงข้อมูลของผู้ใช้งานที่ใช้งานระบบคอมพิวเตอร์โดยไม่มีเหตุผลอันสมควร

* มาตรฐาน DOD 5220.22-M คือ การทำลายข้อมูลบนฮาร์ดดิสก์ด้วยการเขียนข้อมูล 1 และ 0 ทับข้อมูลเดิมจำนวน ๓ ครั้ง

๒.๑.๑๐. ไม่กระทำการอื่นใดที่มีลักษณะเป็นการละเมิดสิทธิ์หรือข้อมูลส่วนบุคคลของผู้ใช้งานที่ใช้งานระบบคอมพิวเตอร์หรือมีข้อมูลส่วนบุคคลจัดเก็บไว้ในระบบคอมพิวเตอร์ โดยไม่มีเหตุผลอันสมควร

๒.๑.๑๑. ไม่เปิดเผยข้อมูลที่ได้มาจากการปฏิบัติหน้าที่ซึ่งข้อมูลดังกล่าวเป็นข้อมูลที่ไม่เปิดเผยให้บุคคลหนึ่งบุคคลใดทราบโดยไม่มีเหตุผลอันสมควร

๒.๑.๑๒. เมื่อผู้ดูแลระบบ (System Administrator) พ้นจากหน้าที่ จะต้องคืนสินทรัพย์ของมหาวิทยาลัยที่เกี่ยวข้องกับการปฏิบัติหน้าที่ของตนในทันทีที่พ้นจากหน้าที่และให้ผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับมอบหมายตรวจสอบการคืนสินทรัพย์

๒.๒. ผู้ดูแลระบบ ทำหน้าที่เก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ (Log) โดยเก็บรักษาข้อมูลของผู้ใช้งานเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ใช้งานนับตั้งแต่เริ่มใช้บริการและเก็บรักษาไว้เป็นเวลาไม่น้อยกว่าเก้าสิบวันนับตั้งแต่การใช้บริการสิ้นสุดลง การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ (Log) ใช้วิธีการที่มั่นคงปลอดภัยดังต่อไปนี้

๒.๒.๑. เก็บในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วนถูกต้องแท้จริง และระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้

๒.๒.๒. มีระบบการเก็บรักษาความลับของข้อมูลที่จัดเก็บ และกำหนดชั้นความลับในการเข้าถึงข้อมูลดังกล่าว เพื่อรักษาความน่าเชื่อถือของข้อมูลและไม่ให้ผู้ดูแลระบบ (System Administrator) สามารถแก้ไขข้อมูลที่เก็บรักษาไว้เว้นแต่ผู้ที่กำหนดให้สามารถเข้าถึงข้อมูลดังกล่าวได้ โดยมอบหมายให้ผู้ตรวจสอบระบบสารสนเทศของมหาวิทยาลัย (Internal IT Auditor) หรือบุคคลที่มหาวิทยาลัยกำหนดเป็นผู้ดำเนินการ

๒.๒.๓. ในการเก็บข้อมูลจราจรนั้น สามารถระบุรายละเอียดผู้ใช้งานเป็นรายบุคคลได้

๒.๒.๔. เพื่อให้ข้อมูลจราจรมีความถูกต้องและนำมาใช้ประโยชน์ได้จริง ผู้ดูแลระบบได้ ตั้งนาฬิกาของอุปกรณ์บริการทุกชนิดให้ตรงกับเวลาอ้างอิงสากล (Stratum 0) โดยผิดพลาดไม่เกิน ๑๐ มิลลิวินาที

ส่วนที่ ๘

แนวปฏิบัติการจัดทำระบบสำรองระบบสารสนเทศและแผนเตรียมความพร้อมกรณีฉุกเฉิน (Data Backup and Disaster Recovery Site)

๑. วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการในการสำรองข้อมูลเครื่องคอมพิวเตอร์แม่ข่าย (Server) อุปกรณ์หลักที่ทำหน้าที่เชื่อมโยงระบบเครือข่ายและเตรียมความพร้อมในกรณีเกิดเหตุฉุกเฉินหรือไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ ให้สามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาที่เหมาะสม เพื่อให้สามารถใช้งานระบบเทคโนโลยีสารสนเทศได้ตามปกติอย่างต่อเนื่อง เหมาะสม และสอดคล้องกับการใช้งานตามภารกิจของมหาวิทยาลัย

๒. แนวทางปฏิบัติการจัดทำระบบสำรองระบบสารสนเทศและแผนเตรียมความพร้อมกรณีฉุกเฉิน (Data Backup and Disaster Recovery Site)

๒.๑. การสำรองข้อมูลและกู้คือข้อมูลในสถานการณ์ปกติเมื่อมีระบบงานใหม่หรือข้อมูลใหม่ หรือข้อมูลที่มีการเปลี่ยนแปลงใหม่กำหนดให้ใช้แนวทางปฏิบัติในการจัดทำนโยบายการสำรอง และกู้คืนข้อมูล ดังต่อไปนี้

๒.๒.๑. มีการจัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของหน่วยงาน พร้อมทั้งกำหนดระบบสารสนเทศที่จะจัดทำระบบสำรอง และจัดทำระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง

๒.๒.๒. กำหนดให้มีการสำรองข้อมูลของระบบสารสนเทศ และกำหนดความถี่ในการสำรองข้อมูล หากระบบใดที่มีการเปลี่ยนแปลงบ่อย ให้กำหนดให้มีความถี่ในการสำรองข้อมูลมากขึ้น โดยให้มีวิธีการสำรองข้อมูล ดังนี้

(๑) กำหนดประเภทของข้อมูลที่ต้องทำการสำรองเก็บไว้ และความถี่ในการสำรอง

(๒) กำหนดรูปแบบการสำรองข้อมูลให้เหมาะสมกับข้อมูลที่จะทำการสำรอง

(๓) บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วัน/เวลา ขนาดข้อมูลที่สำรอง สำเร็จ/ไม่สำเร็จ เป็นต้น

(๔) ตรวจสอบข้อมูลทั้งหมดของระบบว่ามีการสำรองข้อมูลไว้อย่างครบถ้วน ได้แก่ ระบบปฏิบัติการ ซอฟต์แวร์ต่าง ๆ ที่เกี่ยวข้องกับระบบสารสนเทศ ข้อมูลในฐานข้อมูล

(๕) จัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ ระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลสำรองกับหน่วยงานควรห่างกันเพียงพอเพื่อไม่ให้ส่งผลกระทบต่อข้อมูลที่จัดเก็บไว้นอกสถานที่นั้นในกรณีที่เกิดภัยพิบัติกับหน่วยงาน

(๖) ทดสอบบันทึกข้อมูลสำรองอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ

(๗) จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่ได้สำรองเก็บไว้

(๘) ตรวจสอบและทดสอบประสิทธิภาพและประสิทธิผลของขั้นตอนปฏิบัติในการกู้คืนข้อมูลอย่างสม่ำเสมอ

๒.๒.๓. กำหนดขั้นตอนการจัดทำสำรองข้อมูล และการกู้คืนข้อมูลอย่างถูกต้อง รวมทั้งซอฟต์แวร์

๒.๒.๔. กำหนดความถี่ในการสำรองข้อมูล ขึ้นอยู่กับความสำคัญของข้อมูลและการยอมรับความเสี่ยงที่กำหนดโดยเจ้าของข้อมูล หรือระบบ

๒.๒.๕. ต้องทำการทดสอบกู้คืนข้อมูลที่สำรองไว้ อย่างน้อยปีละ ๑ ครั้ง รวมทั้งดำเนินการทดสอบว่าระบบงานทั้งหมดสามารถใช้งานได้ เพื่อให้มั่นใจว่าข้อมูลที่สำรองไว้สามารถกู้ข้อมูลกลับมาได้อย่างสมบูรณ์

๒.๒.๖. จัดทำแผนสำรองข้อมูลและแผนเตรียมความพร้อมรองรับสถานการณ์ฉุกเฉิน ด้านระบบสารสนเทศระบบสารสนเทศให้สามารถกู้คืนระบบกลับคืนได้ภายในระยะที่กำหนด โดยมีรายละเอียดอย่างน้อย ดังนี้

(๑) มีการกำหนดหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด

(๒) มีการประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญเหล่านั้น และกำหนดมาตรการเพื่อลดความเสี่ยงเหล่านั้น ได้แก่ ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว การชุมนุมประท้วงทำให้ไม่สามารถเข้ามาใช้ระบบงานได้ เป็นต้น

(๓) มีการกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ

(๔) มีการกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูล และทดสอบกู้คืนข้อมูลที่สำรองไว้

(๕) มีการกำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอก เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อ

(๖) การสร้างความตระหนัก หรือให้ความรู้แก่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติหรือสิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน เป็นต้น

(๗) มีการทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ ๑ ครั้ง

๒.๒.๗. ต้องมีการตรวจสอบรายงานบันทึกการเก็บสื่อข้อมูลที่สถานที่เก็บข้อมูลสำรองเป็นประจำทุกปี

๒.๒.๘. กำหนดผู้รับผิดชอบในการสำรองข้อมูล ได้แก่

ผู้บริหาร เจ้าหน้าที่ สำนักวิทยบริการและเทคโนโลยีสารสนเทศ งานเทคโนโลยีสารสนเทศ

ผศ.พรภัสสร	อ่อนเกิด	ผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ ๐๘๘-๖๖๔-๙๙๖๖
นายสุเทพ	ยนต์พิมาย	รองผู้อำนวยการงานเทคโนโลยีสารสนเทศ ๐๖๓-๓๙๕-๕๔๙๔
นายสายชล	สารนอก	หัวหน้างานเทคโนโลยีสารสนเทศ ๐๙๘-๓๒๔-๖๕๑๕

นายชัยวัฒน์	แดงจันทึก	หัวหน้าแผนกวิศวกรรมเครือข่าย
		๐๘๐-๙๑๖-๕๖๔๕
นางปวีณา	นาดี	หัวหน้าแผนกงานอีเลิร์นิ่งและเทคโนโลยีการศึกษา
		๐๙๖-๖๕๙-๑๔๒๔
นายธีรธรรม์	โรจนรุ่งสถิตย์	หัวหน้าแผนกงานสารสนเทศ
		๐๙๔-๕๑๙-๕๖๑๖

๒.๒.๙. ต้องจัดทำ แผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ

๒.๒.๑๐. ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

๒.๒.๑๑. ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง

๒.๒.๑๒. มีการทบทวนระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉิน ที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน อย่างน้อยปีละ ๑ ครั้ง

๒.๒.๑๓. จัดทำขั้นตอนการปฏิบัติการ และจัดทำการสำรองข้อมูลและการกู้คืนข้อมูลอย่าง สม่ำเสมอทุกเดือนหรือตามความเหมาะสมไปยัง ศูนย์กู้คืนระบบจากความเสียหายทางภัยพิบัติ (DR-Site) ทั้งระบบซอฟต์แวร์และข้อมูลในระบบสารสนเทศ

๒.๒.๑๔. จัดเก็บฮาร์ดิสก์หรือเทปที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูลและผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน และทำการจัดเก็บเทปสำรองข้อมูลรายเดือนแยกไว้ ณ สถานที่อื่น

๒.๒.๑๕. เตรียมศูนย์คอมพิวเตอร์สำรอง (DR site) เพื่อเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินให้สามารถกู้ระบบงานตามลำดับความสำคัญคืนมาให้ใช้งานได้ภายในระยะเวลาที่เหมาะสม โดยมีการทดสอบปีละ ๒ ครั้ง

๓. ระบบสำรอง (disaster recovery site: DR site)

๓.๑. จัดทำบัญชีระบบเครือข่ายและระบบสารสนเทศที่สำคัญและจำเป็นต้องมีระบบสำรอง และทบทวนบัญชีอย่างน้อยปีละ ๑ ครั้ง โดยให้สำรองข้อมูลระบบงานอย่างน้อยดังนี้

๓.๑.๑. ระบบสารสนเทศเพื่อการบริการ (ERP)

๓.๑.๒. ระบบสารสนเทศเพื่อการศึกษา (ESS)

๓.๑.๓. ระบบค้นหาและจัดการข้อมูลเชิงลึก (e-Document)

๓.๑.๔. ระบบคลังข้อมูลสารสนเทศเพื่อการตัดสิน (BI)

๓.๑.๕. ระบบการเรียนการสอนออนไลน์ (e-learning)

๓.๒. ระบบสำรองต้องอยู่ในห้องหรือพื้นที่ที่ต่างจากระบบหลัก และมีการควบคุม ดังนี้

๓.๒.๑. มีระบบการควบคุมการเข้าถึงที่อนุญาตเฉพาะผู้มีหน้าที่เกี่ยวข้อง

๓.๒.๒. มีระบบไฟฟ้าสำรอง

๓.๒.๓. มีระบบปรับอากาศและความชื้นที่เหมาะสม

๓.๒.๔. มีระบบป้องกันอัคคีภัย

๓.๒.๕. มีระบบส่องสว่างที่เหมาะสม

๓.๒.๖. มีระบบสื่อสารหรือระบบเครือข่ายสำรอง

๓.๒.๗. มีระบบแจ้งเตือนกรณีที่ระบบสนับสนุนทำงานผิดปกติหรือหยุดการทำงาน

๓.๓. มีแผนบำรุงรักษาระบบสำรองทุกระบบอย่างต่อเนื่อง

๔. การสำรองข้อมูล (Data Backup)

๔.๑. จัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของหน่วยงานที่จะทำการสำรองข้อมูลและทบทวนบัญชีอย่างน้อยปีละ ๑ ครั้ง

๔.๒. กำหนดวิธีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบ

๔.๓. กำหนดความถี่ในการสำรองข้อมูล ระบบที่มีความสำคัญสูง หรือระบบที่มีการเปลี่ยนแปลงบ่อย ต้องกำหนดให้มีความถี่ในการสำรองข้อมูลมากขึ้น

๔.๔. บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วัน/เวลา ชื่อข้อมูลที่สำรอง สถานะการทำงานสำเร็จ/ไม่สำเร็จ เป็นต้น

๔.๕. ตรวจสอบข้อมูลทั้งหมดของระบบว่ามีการสำรองข้อมูลไว้อย่างครบถ้วน เช่น ซอฟต์แวร์ต่าง ๆ ที่เกี่ยวข้องกับระบบสารสนเทศ ข้อมูลในฐานข้อมูล และ ข้อมูลการตั้งค่าระบบและอุปกรณ์ต่าง ๆ เป็นต้น

๔.๖. จัดเก็บข้อมูลสำรองไว้ในระบบสำรองข้อมูล

๔.๗. ดำเนินการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรองที่ใช้จัดเก็บข้อมูลสำรอง

๔.๘. มีแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ ดังนี้

๓.๘.๑ ต้องกำหนดหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด

๓.๘.๒ ต้องประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญเหล่านั้น และกำหนดมาตรการ เพื่อลดความเสี่ยงเหล่านั้น เช่น ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว การชุมนุมประท้วงทำให้ไม่สามารถเข้ามาใช้ระบบงานได้ เป็นต้น

๓.๘.๓ ต้องกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ

๓.๘.๔ ต้องกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูล และทดสอบกู้คืนข้อมูลที่สำรองไว้

๓.๘.๕ ต้องทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ ๑ ครั้ง

ส่วนที่ ๙
แนวปฏิบัติการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ
(Verification and Information Risk Assessment)

๑. วัตถุประสงค์

เพื่อให้มีมาตรการในการควบคุมความเสี่ยงและป้องกันผลกระทบที่อาจมีต่อความมั่นคงปลอดภัยด้านสารสนเทศ รวมทั้งให้สามารถกำหนดวิธีการประเมินความเสี่ยงได้อย่างถูกต้อง ส่งผลให้ระบุความเสี่ยงได้อย่างชัดเจน และสามารถควบคุมความเสี่ยงได้อย่างมีประสิทธิภาพ

๒. แนวปฏิบัติการตรวจสอบและประเมินความเสี่ยง (Verification and Information Risk Assessment)

๒.๑. ระบุความเสี่ยงและผลกระทบของความเสี่ยงให้สอดคล้องตามแผนบริหารความเสี่ยงของมหาวิทยาลัย เพื่อการตรวจสอบและประเมินความเสี่ยงนั้น ดังต่อไปนี้

๒.๓.๑. ความเสี่ยงที่เกิดจากการลอบเข้าทางระบบปฏิบัติการเพื่อยึดครองเครื่องคอมพิวเตอร์แม่ข่ายผ่านระบบอินเทอร์เน็ต (Internet)

๒.๓.๒. ความเสี่ยงที่เกิดจากการลักลอบเข้าเชื่อมโยงกับระบบเครือข่ายไร้สายโดยไม่ได้รับอนุญาต

๒.๓.๓. ความเสี่ยงที่เกิดจากเครื่องมือด้านเทคโนโลยีสารสนเทศ หรือระบบเครือข่ายเกิดการขัดข้องระหว่างการใช้งาน

๒.๓.๔. ความเสี่ยงที่เกิดจากการลงบันทึกเข้า (Login) สารสนเทศที่สำคัญผ่านระบบเครือข่ายของผู้ใช้งานคนเดียวกันมากกว่าหนึ่งจุด

๒.๓.๕. ความเสี่ยงที่เกิดจากการลักลอบใช้รหัสผ่าน (Password) ของผู้อื่นโดยไม่ได้รับอนุญาต

๒.๓.๖. จัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (Information Security Audit and Assessment) อย่างน้อยปีละ ๑ ครั้ง โดยเป็นผู้ตรวจสอบภายในหน่วยงานของรัฐ (Internal Auditor) หากได้รับงบประมาณในการตรวจสอบและประเมินที่สามารถดำเนินการโดยละเอียด จะดำเนินการโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor)

๒.๒. กำหนดวิธีการในการตรวจสอบและประเมินความเสี่ยงและความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงนั้นโดยผู้ตรวจสอบภายในหน่วยงานของรัฐ (Internal Auditor) หากได้รับงบประมาณในการตรวจสอบและประเมินที่สามารถดำเนินการโดยละเอียด จะดำเนินการโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) เพื่อให้หน่วยงานของรัฐได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศของหน่วยงาน

๒.๓. การตรวจสอบและประเมินความเสี่ยงให้คำนึงถึงองค์ประกอบ ดังต่อไปนี้

๒.๓.๑. ความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงที่ระบุ

๒.๓.๒. ภัยคุกคามหรือสิ่งที่อาจก่อให้เกิดเหตุการณ์ที่ระบุรวมถึงความเป็นไปได้ที่จะเกิดขึ้น

๒.๓.๓. จุดอ่อนหรือช่องโหว่ที่อาจถูกใช้ในการก่อให้เกิดเหตุการณ์ที่ระบุ

๒.๓.๔. ในการตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการ โดยผู้ตรวจสอบภายในมหาวิทยาลัย เพื่อให้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัย ด้าน สารสนเทศ ความเสียหาย หรืออันตรายที่จะเกิดขึ้นของหน่วยงาน

ส่วนที่ ๑๐
แนวปฏิบัติการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ (Information Security Awareness)

๑. วัตถุประสงค์

เพื่อเผยแพร่แนวนโยบายและแนวปฏิบัติให้กับบุคลากรและบุคคลที่เกี่ยวข้อง ได้มีความรู้ความเข้าใจและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ลดการกระทำความผิดที่เกิดขึ้นจากการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์โดยไม่คาดคิด ตลอดจนสามารถนำไปปฏิบัติได้อย่างถูกต้อง

๒. แนวปฏิบัติการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Awareness)

๒.๑. มีการประกาศนโยบายเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ซึ่งลงนามโดยอธิการบดีมหาวิทยาลัย

๒.๒. จัดฝึกอบรมแนวปฏิบัติตามแนวนโยบายอย่างสม่ำเสมอ โดยการจัดฝึกอบรมอาจใช้วิธีการเสริมเนื้อหาแนวปฏิบัติตามแนวนโยบายเข้ากับหลักสูตรอบรมต่าง ๆ ตามแผนการฝึกอบรมของมหาวิทยาลัย

๒.๓. จัดเผยแพร่แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และสร้างความตระหนักถึงความสำคัญของการปฏิบัติให้กับบุคลากร โดยการจัดอบรม/สัมมนา ต้องจัดปีละไม่น้อยกว่า ๑ ครั้ง โดยอาจจัดร่วมกับกิจกรรมอื่นของมหาวิทยาลัยด้วยก็ได้ และอาจเชิญวิทยากรจากภายนอกที่มีประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มาถ่ายทอดความรู้

๒.๔. ติดประกาศประชาสัมพันธ์ให้ความรู้เกี่ยวกับแนวปฏิบัติ ในลักษณะเกร็ดความรู้หรือข้อระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย โดยมีการปรับเปลี่ยนเกร็ดความรู้อยู่เสมอ

๒.๕. ระดมการมีส่วนร่วมและลงสู่ภาคปฏิบัติด้วยการกำกับ ติดตาม ประเมินผล และสำรวจความต้องการของผู้ใช้งาน

๒.๖. ให้คณะกรรมการเทคโนโลยีสารสนเทศ (CIO) เป็นผู้รับผิดชอบดำเนินการให้เป็นไปตามประกาศนี้และทบทวนปรับปรุงนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศมหาวิทยาลัยอย่างน้อยปีละ ๑ ครั้ง

๒.๗. ให้มีการสร้างความตระหนักเกี่ยวกับโปรแกรมไม่ประสงค์ดีเพื่อให้เจ้าหน้าที่มีความรู้ความเข้าใจและสามารถป้องกันตนเองได้และให้รับทราบขั้นตอนปฏิบัติเมื่อพบเหตุโปรแกรมไม่ประสงค์ดีว่าต้องดำเนินการอย่างไร

๒.๘. สร้างความรู้ความเข้าใจให้แก่ผู้ใช้งานให้ตระหนักถึงเหตุการณ์ด้านความมั่นคงปลอดภัยที่เกิดขึ้น และสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด เพื่อให้ผู้ใช้งานปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของหน่วยงาน

๒.๙. ผู้ใช้งานต้องตระหนักและปฏิบัติตามกฎหมายใด ๆ ที่ได้ประกาศใช้ในประเทศไทยรวมทั้งกฎระเบียบของมหาวิทยาลัย และข้อตกลงระหว่างประเทศอย่างเคร่งครัด ทั้งนี้หากผู้ใช้งานไม่ปฏิบัติตามกฎหมายดังกล่าว

ถือว่าความผิดนั้นเป็นความผิดส่วนบุคคลซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง หากผู้ใช้งานฝ่าฝืนจะต้องถูกลงโทษตามระเบียบ และกฎหมายที่เกี่ยวข้องต่อไป

๓. ความสอดคล้องกับความต้องการด้านกฎหมายและในสัญญาจ้าง (Compliance with legal and contractual requirements)

๓.๑. การระบุกฎหมายและความต้องการในสัญญาจ้างที่เกี่ยวข้อง (Identification of applicable legislation and contractual requirements) ให้ปฏิบัติดังนี้

๒.๓.๑. จัดทำประกาศนโยบาย และแนวปฏิบัติคู่มือการใช้งานสารสนเทศ พร้อมทั้งเผยแพร่ทางเว็บไซต์ของมหาวิทยาลัย

๒.๓.๒. ผู้ดูแลระบบต้องจัดให้มีหลักสูตรที่สอดคล้องกับการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศเพื่อป้องกันการเข้าถึงจากผู้ใช้ซึ่งไม่ได้รับอนุญาต

๒.๓.๓. ต้องจัดสัมมนาเพื่อเผยแพร่แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ และสร้างความตระหนักถึงความสำคัญของการปฏิบัติให้กับผู้ใช้งาน

๓.๒. สิทธิในสินทรัพย์ทางปัญญา (Intellectual property rights) ต้องปฏิบัติตาม ข้อกำหนดที่ระบุไว้ใน ลิขสิทธิ์การใช้งานซอฟต์แวร์อย่างเคร่งครัด รวมทั้งต้องมีการควบคุมการใช้งานซอฟต์แวร์ตามลิขสิทธิ์ที่ได้รับด้วย ได้แก่ การลงทะเบียนเพื่อใช้งานซอฟต์แวร์ต้องเก็บหลักฐานแสดงความเป็นเจ้าของลิขสิทธิ์

๓.๓. การป้องกันข้อมูล (Protection of records) ห้ามผู้ใช้งานทำซ้ำ เผยแพร่ ข้อมูลที่เป็นการละเมิดลิขสิทธิ์หรือซอฟต์แวร์ที่เป็นการละเมิดลิขสิทธิ์บนระบบสารสนเทศขององค์กร

ส่วนที่ ๑๑
การกำหนดผู้รับผิดชอบ
(User Responsibilities)

๑. วัตถุประสงค์

เพื่อกำหนดความรับผิดชอบที่ชัดเจน กรณีระบบคอมพิวเตอร์หรือระบบสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๒. ระดับนโยบาย

ให้ผู้บริหารระดับสูงซึ่งมีหน้าที่ดูแลรับผิดชอบด้านสารสนเทศของหน่วยงาน ที่ทำหน้าที่ (Chief information officer : CIO เป็นผู้รับผิดชอบในการสั่งการตามนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มหาวิทยาลัย ติดตามและกำกับดูแลควบคุมตรวจสอบ

กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ทั้งนี้ ให้ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Officer : CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น”

๓. แนวทางปฏิบัติของผู้รับผิดชอบ (User Responsibilities)

๒.๑. ระดับนโยบาย ผู้รับผิดชอบ

๒.๑.๑. ผู้บริหารระดับสูงสุดของหน่วยงาน (CEO) มีหน้าที่

(๑) รับผิดชอบในการกำหนดนโยบาย ติดตาม กำกับ ดูแล ควบคุมตรวจสอบผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO)

(๒) รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นกรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๒.๑.๒. ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) มีหน้าที่

(๑) ให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตาม กำกับ ดูแล ควบคุมตรวจสอบเจ้าหน้าที่ในระดับปฏิบัติการ

(๒) ทบทวนปรับปรุงนโยบายและข้อปฏิบัติให้เป็นปัจจุบันทุก ๔ ปี

๒.๒. ระดับบริหาร ผู้รับผิดชอบ

ผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ หัวหน้างาน/หัวหน้าแผนก หรือเทียบเท่า ที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ มีหน้าที่

๒.๒.๑. รับผิดชอบ กำกับ ดูแลการปฏิบัติงานของผู้ปฏิบัติ ตลอดจนศึกษา ทบทวน วางแผน ติดตามการบริหารความเสี่ยง และระบบรักษาความปลอดภัยฐานข้อมูลและเทคโนโลยีสารสนเทศ

๒.๒.๒. รับผิดชอบในการควบคุม ดูแล รักษาความปลอดภัย ระบบสารสนเทศและระบบฐานข้อมูล

๒.๓. ระดับปฏิบัติการ ผู้รับผิดชอบ

ผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่จากระดับบริหาร มีหน้าที่

๒.๒.๑. ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๒.๒.๒. ประสานการปฏิบัติงานตามแผนป้องกันและแก้ไขปัญหาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ

๒.๒.๓. รับผิดชอบควบคุม ดูแล รักษาความปลอดภัย และบำรุงรักษา ระบบเครื่องคอมพิวเตอร์ระบบเครือข่าย ห้องแม่ข่ายคอมพิวเตอร์และเครื่องคอมพิวเตอร์แม่ข่าย

๒.๒.๔. ทำการสำรองข้อมูลและเรียกคืนข้อมูล (Backup and Recovery) ตามรอบระยะเวลาที่กำหนด

๒.๒.๕. ป้องกันการถูกเจาะระบบ และแก้ไขปัญหาการถูกเจาะเข้าระบบฐานข้อมูล เว็บไซต์หน่วยงาน จากบุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาต

๒.๒.๖. ควบคุมการเข้า-ออกห้อง Server ตามการกำหนดสิทธิ์การเข้าถึง Server

๒.๒.๗. กำกับดูแล ตรวจสอบ บำรุงรักษาอุปกรณ์ Server และอุปกรณ์เชื่อมโยงเครือข่าย (Network) ของระบบการเชื่อมโยงเครือข่ายฐานข้อมูลทั้งหมดให้สามารถใช้งานได้ตามปกติตลอด ๒๔ ชั่วโมง

๒.๒.๘. กำกับดูแล การติดตั้ง รื้อถอน ดูแล ตรวจสอบ การเชื่อมโยงการสื่อสารผ่านเครือข่ายทางระบบ LAN, Internet, Intranet ที่ให้บริการในมหาวิทยาลัย

๒.๒.๙. แก้ไขปัญหา อุปสรรค สถานการณ์ความเสี่ยงและความเสียหายที่เกิดขึ้นกับระบบเชื่อมโยงเครือข่ายของระบบฐานข้อมูลสารสนเทศ

๒.๒.๑๐. รายงานผลการปฏิบัติงานสถานการณ์ที่เกิดขึ้นกับระบบเครือข่ายและระบบฐานข้อมูลและสารสนเทศ ให้แก่ ผู้บังคับบัญชา ระดับสูง ทราบสม่ำเสมอ

๒.๒.๑๑. กำกับดูแล การติดตาม ตรวจสอบ (Monitor) การเข้าใช้งานและการเข้าถึงระบบการทำงานของ Server ตามสิทธิ์การเข้าถึงระบบ

๒.๒.๑๒. กำกับดูแล ตรวจสอบ บำรุงรักษาอุปกรณ์ป้องกันการถูกเจาะระบบจากบุคคลภายนอก (Firewall) และโปรแกรมปฏิบัติการทั้งหมดที่ติดตั้งอยู่ใน Server ของระบบฐานข้อมูลทั้งหมดที่ให้บริการในเว็บไซต์ ให้สามารถใช้งานได้ตามปกติ

พิจารณาเพิ่มเติม

การป้องกันโปรแกรมไม่ประสงค์ดี

- ผู้ใช้งานต้องติดตั้งและใช้งานโปรแกรมคอมพิวเตอร์สำหรับป้องกันและกำจัดโปรแกรมไม่ประสงค์ดี รวมทั้งทำการปรับปรุงให้ทันสมัยอยู่เสมอ
- ต้องทำการปรับปรุงระบบปฏิบัติการ เว็บเบราว์เซอร์ และโปรแกรมต่าง ๆ อย่างสม่ำเสมอเพื่อปิดช่องโหว่ เป็นการป้องกันการโจมตีจากภัยคุกคามต่าง ๆ
- ในการรับส่งข้อมูลคอมพิวเตอร์หรือสารสนเทศ ผ่านทางระบบเครือข่าย และ ผ่านทางสื่อบันทึกข้อมูลทุกชนิด ผู้ใช้งานต้องทำการตรวจสอบ เพื่อป้องกันและกำจัดโปรแกรมไม่ประสงค์ดี ก่อนการรับส่งทุกครั้ง
- ผู้ใช้งานต้องตรวจสอบไฟล์ โดยใช้โปรแกรมป้องกันโปรแกรมไม่ประสงค์ดี ก่อนการเปิดใช้ไฟล์ที่สามารถประมวลผลได้ (Executable file) เช่นไฟล์ที่มีนามสกุล .exe .com .bat .vbs .scr .pif .hta .txt.exe .doc.exe .xls.exe เป็นต้น