แนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

แนวปฏิบัติการใช้งานสารสนเทศให้มั่นคงปลอดภัย

๑. การใช้งานรหัสผ่านและบัญชีผู้ใช้เครือข่ายนนทรี บุคลากรต้องปฏิบัติดังนี้

๑.๑ ควรเปลี่ยนรหัสผ่านประจำเครื่องคอมพิวเตอร์อย่างน้อยปีละ ๑ ครั้ง และเปลี่ยนรหัสบัญชีผู้ใช้เครือข่ายนนทรีเมื่อระบบแจ้งเตือน

๑.๒ ต้องตั้งรหัสผ่านที่ปลอดภัยให้ตรงตามข้อกำหนดการตั้งรหัสผ่านและรักษารหัสนั้นให้เป็นความลับอยู่ตลอดเวลา

๑.๓ ไม่ลักลอบใช้รหัสผ่าน หรือการกระทำอื่นใดเพื่อให้ได้มาซึ่งรหัสผ่านของผู้อื่น

๑.๔ ไม่อนุญาตให้ผู้อื่นใช้บัญชีของตน หากเกิดปัญหาจากการให้ใช้บัญชี ได้แก่ การละเมิดลิขสิทธิ์ หรือการเก็บข้อมูลที่ผิดกฎหมายเจ้าของบัญชีผู้ใช้ต้องเป็นผู้รับผิดชอบ เว้นแต่จะมีหลักฐานพิสูจน์ได้ว่าไม่ได้เป็นผู้กระทำ

๒. บุคลากรต้องป้องกันไม่ให้ผู้ไม่มีสิทธิเข้าถึงอุปกรณ์สำนักงาน เพื่อป้องกันข้อมูลสำคัญสูญหาย

๒.๑ การรักษาความลับของข้อมูลในเครื่องคอมพิวเตอร์ หรืออุปกรณ์สำนักงานจะเป็นความรับผิดชอบของผู้ใช้งานประจำเครื่องคอมพิวเตอร์ หรืออุปกรณ์สำนักงานนั้น

๒.๒ เครื่องคอมพิวเตอร์ส่วนบุคคลทุกเครื่องต้องมีรหัสผ่านประจำเครื่องสำหรับผู้ใช้งาน

๒.๓ เครื่องคอมพิวเตอร์ส่วนบุคคลทุกเครื่องต้องติดตั้งระบบ screen saver โดยกำหนดรหัสในการเข้าใช้

๓. ต้องไม่ทิ้งสินทรัพย์สารสนเทศสำคัญไว้ในที่ที่ไม่ปลอดภัย โดยต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ ได้แก่ เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์ สารสนเทศ ฯลฯ อยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ

๓.๑ ผู้พัฒนาระบบต้องกำหนดค่า Session Timeout ให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

๓.๒ ต้องล็อคอุปกรณ์ที่สำคัญเมื่อไม่ได้ใช้งานหรือปล่อยทิ้งไว้โดยไม่ได้ดูแลชั่วคราว

๓.๓ การป้องกันข้อมูลและสินทรัพย์ด้านสารสนเทศที่อยู่ในเครื่องคอมพิวเตอร์ประเภทพกพา ผู้ใช้งานต้องมีวิธีการป้องกันข้อมูลและสินทรัพย์ด้านสารสนเทศที่อยู่ในเครื่องคอมพิวเตอร์ประเภทพกพา, smart mobile device เมื่อปฏิบัติงานอยู่นอกสถานที่ ได้แก่

๑) ต้องใส่รหัสผ่านป้องกันหน้าจอทุกเครื่อง

๒) ต้องใช้กุญแจล็อคเครื่องคอมพิวเตอร์พกพา

๔. ต้องมีการกำหนดการควบคุมความมั่นคงปลอดภัยของอุปกรณ์ป้องกันการบุกรุกทางเครือข่าย โดยการกำหนดค่าต่างๆให้เหมาะสมตามความต้องการในการปฏิบัติงาน รวมทั้งมีการทบทวนการกำหนดค่าอย่างสม่ำเสมอ ทั้งนี้ ผู้ที่ควบคุมดูแลต้องเป็นผู้ดูแลระบบที่มีสิทธิ์ในการเข้าถึงการตั้งค่าของไฟร์วอลล์ตามนโยบาย

เท่านั้น เพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบเทคโนโลยีสารสนเทศและเครือข่ายภายของสำนักหอสมุด

๔.๑ กำหนดให้ฝ่ายเทคโนโลยีสารสนเทศมีหน้าที่จัดหา บริหารจัดการ การติดตั้ง และการกำหนดค่าของอุปกรณ์ป้องกันการบุกรุกทางเครือข่าย โดยการกำหนดค่าเริ่มต้นพื้นฐานของทุกเครือข่ายจะต้องเป็นปฏิเสธทั้งหมด

๔.๒ เครื่องคอมพิวเตอร์ในเครือข่ายของสำนักหอสมุดสำหรับการปฏิบัติงาน ต้องอยู่ภายใต้นโยบายการตรวจจับการบุกรุก ทุกเส้นทางเชื่อมต่ออินเทอร์เน็ตที่ไม่อนุญาตตามนโยบายจะต้องถูกปฏิเสธการรับส่งข้อมูล

๔.๓ ผู้ดูแลระบบต้องตรวจสอบการทำงานของระบบ IDS/IPS ตรวจสอบเหตุการณ์ ข้อมูลจราจร พฤติกรรมการใช้งาน กิจกรรมบนเครือข่ายและจะต้องมีการบันทึกผลการตรวจสอบอย่างสม่ำเสมอ

๔.๔ ผู้ดูแลระบบจะต้อง Update Patch/Signature ของ IDS/IPS อย่างสม่ำเสมอ

๔.๕ ค่าการเปลี่ยนแปลงทั้งหมดของอุปกรณ์ป้องกันบุกรุกทางเครือข่าย เช่น ค่าพารามิเตอร์ การกำหนดค่าใช้บริการ และการเชื่อมต่อที่อนุญาต จะต้องมีการบันทึกการเปลี่ยนแปลงทุกครั้ง

๔.๖ การเข้าถึงตัวอุปกรณ์ไฟร์วอลล์ จะต้องสามารถเข้าถึงได้เฉพาะผู้ดูแลระบบที่ได้รับมอบหมายให้ดูแลจัดการเท่านั้น

๔.๗ การกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละส่วนของเครือข่าย จะต้องกำหนดค่าอนุญาตเฉพาะพอร์ตการเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น โดยข้อนโยบายจะต้องถูกระบุให้กับเครื่องคอมพิวเตอร์แม่ข่ายเป็นรายเครื่องที่ให้บริการจริง และการกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายหรืออุปกรณ์ในเครือข่าย และต้องมีการบันทึกการกำหนดค่าการให้บริการโดยต้องระบุข้อมูลดังนี้

(๑) หมายเลข Port ที่ขอให้เปิด

(๒) หมายเลข IP Address ของปลายทางที่ต้องการติดต่อสื่อสาร

(๓) วัตถุประสงค์ หรือชื่อแอพพลิเคชั่นที่ต้องการใช้งานผ่าน Port นั้นๆ

(๔) วันที่เริ่มใช้ และวันที่สิ้นสุดการขอใช้

๔.๘ เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบงานสารสนเทศต่างๆ จะต้องไม่อนุญาตให้มีการเชื่อมต่อเพื่อใช้งานอินเทอร์เน็ต เว้นแต่มีความจำเป็น โดยจะต้องกำหนดเป็นกรณีไป เช่น Windows Update , RSS Feed เป็นต้น

๔.๙ สำนักหอสมุดมีสิทธิ์ที่จะระงับหรือบล็อกการใช้งานของเครื่องคอมพิวเตอร์ลูกข่ายที่มีพฤติกรรมการใช้งานที่ขัดต่อนโยบาย ประกาศ ระเบียบของสำนักหอสมุดหรือกฎหมาย หรืออาจทำให้เกิดการทำงานของโปรแกรม ที่มีความเสี่ยงต่อความปลอดภัยของระบบเทคโนโลยีสารสนเทศ จนกว่าจะได้รับการแก้ไข

๔.๑๐ การเชื่อมต่อในลักษณะของการ Remote Login จากภายนอกมายังเครื่องแม่ข่าย หรืออุปกรณ์เครือข่ายภายใน จะต้องได้รับความเห็นชอบจากหัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

๔.๑๑ พฤติกรรมการใช้งาน กิจกรรม หรือเหตุการณ์ทั้งหมดที่มีความเสี่ยงต่อการบุกรุก การโจมตีระบบ พฤติกรรมน่าสงสัย หรือพยายามเข้าระบบทั้งที่ประสบความสำเร็จและไม่ประสบความสำเร็จจะต้องมีตรวจสอบและแก้ไขทันที

๔.๑๒ การตรวจสอบการบุกรุกทั้งหมดจะต้องเก็บบันทึกข้อมูลไว้ไม่น้อยกว่า ๙๐ วัน

๔.๑๓ มีรูปแบบการตอบสนองต่อเหตุการณ์ที่เกิดขึ้น ได้แก่ รายงานผลการตรวจพบของเหตุการณ์ต่างๆ ดำเนินการตามขั้นตอนเพื่อลดความเสียหาย ลบซอฟต์แวร์มุ่งร้ายที่ตรวจพบ ป้องกันเหตุการณ์ที่อาจเกิดอีกในอนาคต และดำเนินการตามแผน

๔.๑๔ ผู้ที่ถูกตรวจสอบว่าพยายามกระทำการอันใดที่เป็นการละเมิดนโยบายของสำนักหอสมุดการพยายามเข้าถึงระบบโดยมิชอบ การโจมตีระบบ หรือมีพฤติกรรมเสี่ยงต่อการทำงานของระบบเทคโนโลยีสารสนเทศ จะถูกระงับการใช้เครือข่ายทันที หากการกระทำดังกล่าวเป็นการกระทำความผิดที่สอดคล้องกับ พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ หรือเป็นการกระทำที่ส่งผลให้เกิดความเสียหายต่อข้อมูล และทรัพยากรระบบของสำนักหอสมุดจะต้องถูกดำเนินคดีตามขั้นตอนของกฎหมาย

แนวปฏิบัติในการควบคุมการเข้าถึงสารสนเทศ

๑. ผู้ดูแลระบบ ต้องกำหนดสิทธิการเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการใช้งานของผู้ใช้งาน และหน้าที่ความรับผิดชอบในการปฏิบัติงานของผู้ใช้งานระบบสารสนเทศ รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ดังนี้

๑.๑ กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ ที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิหรือการมอบอำนาจ ดังนี้

๑) กำหนดสิทธิของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง ได้แก่

- สิทธิอ่านอย่างเดียว
- สิทธิการเพิ่มข้อมูล
- สิทธิการแก้ไขข้อมูล
- สิทธิการลบข้อมูล
- สิทธิการอนุมัติ/อนุญาต
- ไม่มีสิทธิ

๑.๒ กำหนดการระงับสิทธิ มอบอำนาจ ให้เป็นไปตามแนวปฏิบัติการจัดการการเข้าถึงของผู้ใช้งาน ที่ได้กำหนดไว้

๑.๓ ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศจะต้องได้รับการพิจารณาจากผู้ดูแลระบบที่ได้รับมอบหมาย

๑.๔ การแบ่งประเภทของข้อมูลและการจัดลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล ใช้แนวทางตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ ซึ่งระเบียบดังกล่าวเป็นมาตรการที่ละเอียด รอบคอบ ถือเป็นแนวทางที่เหมาะสมในการจัดการเอกสารอิเล็กทรอนิกส์ และการรักษาความปลอดภัยของเอกสารอิเล็กทรอนิกส์ โดยได้กำหนดกระบวนการ และกรรมวิธีต่อเอกสารที่สำคัญไว้ ดังนี้

๑.๔.๑ จัดแบ่งประเภทข้อมูลออกเป็น

๑.๔.๑.๑ ข้อมูลทั่วไปที่เปิดเผยได้ ได้แก่ ข้อมูลด้านการให้บริการ ข้อมูลรับสมัครงาน ข่าวสารประชาสัมพันธ์ เป็นต้น

๑.๔.๑.๒ ข้อมูลเฉพาะที่ต้องกำหนดสิทธิ ได้แก่

๑) ข้อมูลสารสนเทศด้านการบริหาร ได้แก่ ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์ และคำร้อง ข้อมูลบุคลากร ข้อมูลงบประมาณการเงินและบัญชี เป็นต้น

๒) ข้อมูลสารสนเทศตามพันธกิจ ได้แก่ ข้อมูลด้านการวิจัย เป็นต้น

๓) ข้อมูลสารสนเทศด้านการให้บริการ ได้แก่ ระบบฐานข้อมูลออนไลน์

๑.๔.๒ จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น ๔ ระดับ

๑.๔.๖.๑ ข้อมูลที่มีระดับความสำคัญมากที่สุด ได้แก่ ข้อมูลงบประมาณการเงินและบัญชี ข้อมูลด้านการวิจัย

๑.๔.๖.๒ ข้อมูลที่มีระดับความสำคัญมาก ได้แก่ ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์ ข้อมูลส่วนบุคคล ข้อมูลบุคลากร

๑.๔.๖.๓ ข้อมูลที่มีระดับความสำคัญปานกลาง

๑.๔.๖.๔ ข้อมูลที่มีระดับความสำคัญน้อย

หากข้อมูลที่นอกเหนือจากที่กำหนด การจัดระดับความสำคัญของข้อมูล ให้พิจารณาในระดับฐานข้อมูล ด้วยการประเมินมูลค่าความเสียหายต่อหน่วยงานหากข้อมูลมีปัญหา ไม่สมบูรณ์ แนวปฏิบัติในการพิจารณาจัดลำดับความสำคัญของข้อมูลมีดังนี้

ระดับความสำคัญของข้อมูล	**การประเมินมูลค่าความเสียหายหากข้อมูลมีปัญหา หรือไม่สมบูรณ์**
ความสำคัญมากที่สุด	มีผลกระทบรุนแรงต่อการดำรงอยู่ของหน่วยงาน หรือปิดหน่วยงาน
ความสำคัญมาก	มีผลกระทบในระดับที่ยังไม่มีนัยสำคัญต่อการดำเนินงานขององค์กร
ความสำคัญปานกลาง	มีผลกระทบในระดับที่มีนัยสำคัญเล็กน้อย
ความสำคัญน้อย	ไม่มีผลกระทบใด ๆ ต่อการดำเนินภารกิจ

๑.๔.๓ จัดแบ่งลำดับชั้นความลับของข้อมูล

๑.๔.๓.๑ ข้อมูลลับที่สุด หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด

๑.๔.๓.๒ ข้อมูลลับมาก หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรง

๑.๔.๓.๓ ข้อมูลลับ หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย

๑.๔.๓.๔ ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

๑.๔.๔ จัดแบ่งระดับชั้นการเข้าถึง ดังนี้

๑.๔.๔.๑ เข้าถึงได้ทุกกลุ่มผู้ใช้งาน ได้แก่ ข้อมูลทั่วไปที่เปิดเผยได้

๑.๔.๔.๒ เข้าถึงได้เฉพาะกลุ่มผู้ใช้งานที่ได้รับสิทธิ ได้แก่ ข้อมูลเฉพาะที่ต้องกำหนดสิทธิ ข้อมูลลับ

๑.๔.๔.๓ เข้าถึงได้เฉพาะผู้มีสิทธิในการบริหารจัดการระบบสารสนเทศ ได้แก่ ข้อมูลระบบ

๑.๔.๕ กำหนดช่องทางในการเข้าถึงข้อมูล

๑.๔.๕.๑ ผู้ใช้งานเข้าใช้บริการผ่านทางระบบเครือข่ายภายใน ได้ตลอด ๒๔ ชั่วโมง

๑.๔.๕.๒ ผู้ใช้งานเข้าใช้บริการผ่านทางระบบเครือข่ายอินเตอร์เน็ตที่อยู่ภายนอก ผ่านระบบ VPN ได้ตลอด ๒๔ ชั่วโมง

๑.๔.๖ กำหนดเวลาและจำนวนระยะเวลาในการเข้าถึงข้อมูล

๑.๔.๖.๑ ระบบงานบริการสำหรับผู้ใช้งานทั่วไปเข้าถึงได้ตลอดเวลา

๑.๔.๖.๒ 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

๑.๕ มีข้อกำหนดการใช้งานตามภารกิจ เพื่อควบคุมการเข้าถึงสารสนเทศ โดยแบ่งการจัดทำข้อปฏิบัติเป็นสองส่วน คือ

๑.๔.๑ มีการควบคุมการเข้าถึงสารสนเทศ โดยให้กำหนดแนวทางการควบคุมการเข้าถึงระบบสารสนเทศ และสิทธิที่เกี่ยวข้องกับระบบสารสนเทศ

๑.๔.๒ มีการปรับปรุงให้สอดคล้องกับข้อมูลกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย

๑.๖ ต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบสารสนเทศและแก้ไขเปลี่ยนแปลงสิทธิต่าง ๆ เพื่อเป็นหลักฐานในการตรวจสอบ

๑.๗ ต้องจัดให้มีการบันทึกการผ่านเข้า-ออกสถานที่ตั้งของระบบสารสนเทศเพื่อเป็นหลักฐานในการตรวจสอบ

แนวปฏิบัติการควบคุมการเข้าถึงเครือข่าย

เพื่อควบคุมการใช้บริการบนระบบเครือข่ายคอมพิวเตอร์

๑. ผู้ดูแลระบบต้องออกแบบและแบ่งแยกระบบเครือข่าย ตามกลุ่มของบริการระบบเทคโนโลยีสารสนเทศ กลุ่มของผู้ใช้งาน และกลุ่มของระบบสารสนเทศ โดยประกอบด้วย โซนภายใน (Internal Zone) โซนภายนอก (External Zone) เพื่อให้การบริหารจัดการและควบคุมเป็นระบบ และป้องกันการบุกรุกได้อย่างมีประสิทธิภาพ

๒. การพิสูจน์ตัวตนสำหรับผู้ใช้งานที่อยู่ภายนอกสำนักหอสมุดผู้ดูแลระบบต้องกำหนดให้พิสูจน์ตัวตน ก่อนที่จะอนุญาตเข้าใช้งานเครือข่าย และระบบสารสนเทศของสำนักหอสมุด ได้แก่

๒.๑ การแสดงตัวตน ด้วยชื่อผู้ใช้งาน (Username)

๒.๒ การพิสูจน์ยืนยันตัวตน ด้วยการใช้รหัสผ่าน (Password)

๒.๓ การเข้าสู่ระบบสารสนเทศของสำนักหอสมุด จะต้องมีการตรวจสอบผู้ใช้งานอีกครั้ง

๒.๔ การเข้าสู่ระบบจากระยะไกล เพื่อเพิ่มความปลอดภัยของการรับส่งข้อมูล ต้องมีการใช้การเข้ารหัสข้อมูล ได้แก่ SSL

๓. การใช้งานเครือข่ายจากแหล่ง หรือสถานที่ที่ได้รับอนุญาต ผู้ดูแลระบบต้องจัดทำกระบวนการพิสูจน์ตัวตนในการเชื่อมต่อระหว่างเครือข่ายของสำนักหอสมุดและเครือข่ายภายนอกว่ามาจากแหล่งหรือสถานที่ที่ได้รับอนุญาตเท่านั้น

๔. การควบคุมผู้ใช้งานในการใช้งานเครือข่าย ผู้ดูแลระบบต้องมีวิธีการจำกัดสิทธิการใช้งาน เพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น ได้แก่

๕.๑ ใช้ Monitoring Tool เพื่อตรวจสอบการเชื่อมต่อทางระบบเครือข่าย

๕.๒ มีระบบการตรวจจับผู้บุกรุกทั้งในระดับเครือข่าย และระดับเครื่องแม่ข่าย

๕.๓ ควบคุมไม่ให้มีการเปิดให้บริการบนระบบเครือข่ายโดยไม่ได้รับอนุญาต

๕. การจำกัดเส้นทางการเข้าถึงเครือข่ายที่ใช้งานร่วมกัน ผู้ดูแลระบบต้องกำหนดตารางของการใช้เส้นทางบนระบบเครือข่าย (Network routing Control) บนอุปกรณ์จัดเส้นทาง (Router) หรืออุปกรณ์กระจายสัญญาณ เพื่อควบคุมผู้ใช้งานเฉพาะเส้นทางที่ได้รับอนุญาตเท่านั้น

๖. ผู้ดูแลระบบต้องกำหนด IP Address ให้กับอุปกรณ์ที่เชื่อมต่อเครือข่ายเพื่อให้สามารถระบุถึงอุปกรณ์เครือข่ายได้อย่างถูกต้อง ในกรณีที่ไม่สามารถใช้ IP Address ระบุถึงอุปกรณ์ได้ กำหนดให้ผู้ใช้งานต้องลงทะเบียน MAC Address อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่าย เพื่อให้สามารถระบุอุปกรณ์เครือข่ายตัวนั้นได้อย่างถูกต้อง

๗. ผู้ดูแลระบบจะต้องทำการป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ ทั้งการเข้าถึงทางกายภาพและผ่านทางเครือข่าย ได้แก่

๗.๑ ต้องตรวจสอบ และปิดพอร์ตที่ไม่มีการใช้งานอยู่เสมอ

๗.๒ ต้องควบคุมการเข้าถึงระบบผ่านอุปกรณ์ป้องกันการบุกรุก (Firewall) ของระบบเครือข่าย

๗.๓ ต้องเก็บอุปกรณ์ที่เชื่อมต่อเครือข่ายไว้ในห้องที่มีการควบคุมการเข้าถึง และจะเข้าได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น หรือล็อกกุญแจเพื่อป้องกันการเชื่อมต่อโดยไม่ได้รับอนุญาต

๘. ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

แนวปฏิบัติการจัดการการเข้าถึงของผู้ใช้งาน

เพื่อป้องกันไม่ให้ผู้ที่ไม่มีสิทธิใช้งานสามารถเข้าถึงระบบสารสนเทศได้ และควบคุมการเข้าถึงระบบสารสนเทศ อุปกรณ์ประมวลผลสารสนเทศ ให้เข้าถึงเฉพาะผู้ที่ได้รับอนุญาต

๑. กำหนดขั้นตอนปฏิบัติในการลงทะเบียนผู้ใช้งาน (User registration) ครอบคลุมในเรื่องต่อไปนี้

๑.๑ จัดทำแบบฟอร์มลงทะเบียนผู้ใช้งานระบบสารสนเทศเพื่อตรวจสอบสิทธิ และดำเนินการตามขั้นตอนการลงทะเบียนผู้ใช้งาน

๑.๒ ต้องจัดทำเอกสารแสดงถึงสิทธิ และความรับผิดชอบของผู้ใช้งานซึ่งต้องลงนามรับทราบด้วย

๑.๓ ต้องบันทึกและจัดเก็บข้อมูลการขออนุมัติเข้าใช้ระบบสารสนเทศ

๑.๔ กำหนดหลักเกณฑ์ในการอนุญาตให้เข้าถึงระบบสารสนเทศ ได้แก่

๑) ต้องเป็นบุคคลที่มีบัญชีรายชื่อที่ออกโดยสำนักบริการคอมพิวเตอร์ และยังไม่สิ้นสุดสถานภาพการเป็นนักเรียน นิสิต บุคลากรของมหาวิทยาลัยเกษตรศาสตร์

๒) ผู้ใช้งานต้องได้รับอนุญาตจากเจ้าของข้อมูล และได้รับมอบหมายจากผู้บังคับบัญชา

๓) ได้รับการอนุมัติจากผู้อำนวยการสำนักหอสมุด หรือผู้ดูแลระบบที่ได้รับมอบหมาย

๔) กำหนดหลักเกณฑ์ในการยกเลิกเพิกถอนการอนุญาตให้เข้าถึงระบบสารสนเทศ การตัดออกจากทะเบียน การโยกย้ายหน่วยงาน การระงับการปฏิบัติงาน หรือเมื่อสิ้นสุดสถานภาพการเป็นผู้ใช้งาน

๒. การบริหารจัดการสิทธิของผู้ใช้งาน (Privileges Management) โดยแสดงรายละเอียดที่เกี่ยวกับการควบคุมและจำกัดสิทธิเพื่อให้สามารถเข้าถึง และใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นๆ ที่เกี่ยวข้องกับการเข้าถึง ดังนี้

๒.๑ ต้องมอบหมายหรือกำหนดสิทธิการใช้งานให้แก่ผู้ใช้งานที่เหมาะสมต่อสถานภาพหรือหน้าที่ความรับผิดชอบ

๒.๒ ต้องกำหนดระดับสิทธิในการเข้าถึงระบบสารสนเทศที่เหมาะสมตามหน้าที่ความรับผิดชอบ และตามความจำเป็นในการใช้งาน

๒.๓ ต้องมอบหมายสิทธิ ต้องสอดคล้องกับนโยบายควบคุมการเข้าถึง

๒.๔ ต้องบันทึกและจัดเก็บข้อมูลการมอบหมายสิทธิให้แก่ผู้ใช้งาน

๓. การบริหารจัดการรหัสผ่านต้องเป็นไปตามข้อกำหนดการตั้งรหัสผ่าน

๔. การทบทวนสิทธิในการเข้าถึงระบบของผู้ใช้งาน ผู้ดูแลระบบต้องทบทวนสิทธิในการเข้าถึงระบบสารสนเทศตามระยะเวลาที่กำหนดไว้ อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อเปลี่ยนแปลงสถานภาพ

แนวปฏิบัติการควบคุมการเข้าถึงระบบปฏิบัติการ

๑. กำหนดขั้นตอนการปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัยสำหรับระบบที่มีความความสำคัญสูงหรือมีความเสี่ยงสูง การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยแสดงวิธียืนยันตัวสำหรับระบบสารสนเทศ ดังนี้

๑.๑ ระบบสามารถยุติการเชื่อมต่อจากเครื่องปลายทางได้ เมื่อพบว่ามีการพยายามคาดเดารหัสผ่านจากเครื่องปลายทาง

๑.๒ ต้องกำหนดระยะเวลาสำหรับการป้อนรหัสผ่าน

๑.๓ จำกัดเข้าถึงระบบปฏิบัติการเฉพาะอินทราเน็ต

๒. การพิสูจน์ตัวตนสำหรับผู้ใช้งาน ผู้ดูแลระบบต้องกำหนดให้พิสูจน์ตัวตนสำหรับผู้ใช้งานเป็นรายบุคคลก่อนที่จะอนุญาตให้เข้าใช้งานระบบสารสนเทศ ได้แก่

๒.๑ ผู้ใช้งานต้องลงบันทึกเข้า (Login) โดยใช้ชื่อผู้ใช้ (Username) ของตนเอง และทำการลงบันทึกออก (Logout) ทุกครั้งเมื่อสิ้นสุดการใช้งานหรือหยุดการใช้งานชั่วคราว

๒.๒ ผู้ใช้งานที่เป็นเจ้าของบัญชีผู้ใช้บริการ ต้องเป็นผู้รับผิดชอบในผลต่าง ๆ อันเกิดจากการใช้ชื่อผู้ใช้ (Username) เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

๓. การบริหารจัดการรหัสผ่าน ผู้ดูแลระบบต้องจัดให้มีระบบหรือวิธีการในการตรวจสอบคุณภาพของรหัสผ่านและมีวิธีการควบคุมดูแลให้ผู้ใช้เปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนด ได้แก่

๓.๑ กำหนดให้รหัสผ่านต้องมีมากกว่าหรือเท่ากับ ๘ ตัวอักษร โดยผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวพิมพ์ใหญ่ ตัวเลข และสัญลักษณ์เข้าด้วยกัน

๓.๒ ต้องให้ผู้ใช้งานลงนามเพื่อเก็บรักษารหัสผ่านทั้งของตนเองและของกลุ่มไว้เป็นความลับ และไม่เปิดเผยให้ผู้อื่นทราบ

๓.๓ กำหนดรหัสผ่านเริ่มต้นให้กับผู้ใช้ให้ยากต่อการเดา

๓.๔ ส่งมอบรหัสผ่านชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย หลีกเลี่ยงการใช้บุคคลอื่น หรือการส่งจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน

๓.๕ ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันทีหลังจากได้รับรหัสผ่านชั่วคราว

๓.๖ ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชาของหน่วยงานเจ้าของระบบ โดยต้องกำหนดระยะเวลาใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาสิทธิพิเศษที่ได้รับ

๔. กระบวนการในการเข้าสู่ระบบให้บริการอย่างมั่นคงปลอดภัย ผู้ดูแลระบบต้องกำหนดกระบวนการในการเข้าสู่ระบบให้บริการเพื่อใช้งานเครื่องให้บริการที่มีความมั่นคงปลอดภัย เช่น กำหนดให้ระบบให้บริการปฏิเสธการใช้งาน หากผู้ใช้พิมพ์รหัสผ่านผิดพลาดเกิน ๓ ครั้ง เป็นต้น

๕. การพิสูจน์ตัวตนสำหรับเครื่องคอมพิวเตอร์ ผู้ดูแลระบบต้องมีวิธีการพิสูจน์ตัวตนสำหรับเครื่องคอมพิวเตอร์ก่อนที่จะอนุญาตให้เข้ามาใช้งานระบบเครือข่ายคอมพิวเตอร์

๖. การตัดเวลาการใช้งานเครื่องคอมพิวเตอร์ ผู้ดูแลระบบต้องมีวิธีการตัดเวลาการใช้งานเครื่องคอมพิวเตอร์ เมื่อเครื่องคอมพิวเตอร์ นั้นไม่ได้ใช้งานเป็นระยะเวลาหนึ่ง เช่น กลไกการล็อคหน้าจอ และต้องใช้รหัสผ่านในการเข้าสู่ระบบ เป็นต้น

๗. การควบคุมการใช้งานโปรแกรมยูทิลิตี้ ผู้ดูแลระบบต้องกำหนดให้ควบคุมการใช้โปรแกรมยูทิลิตี้สำหรับระบบเพื่อป้องกันการเข้าถึงโดยผู้ที่ไม่ได้รับอนุญาต ได้แก่

๗.๑ จำกัดการใช้งานโปรแกรมยูทิลิตี้ให้เฉพาะผู้ที่ได้รับมอบหมายแล้วเท่านั้น

๗.๒ ให้แยกโปรแกรมยูทิลิตี้ออกจากโปรแกรมระบบงาน

๗.๓ โปรแกรมยูทิลิตี้ที่นำมาใช้งานต้องไม่ละเมิดลิขสิทธิ

๘. การติดตั้งระบบเตือนภัยสำหรับระบบที่มีความสำคัญสูง ผู้บริหารต้องจัดให้ติดตั้งระบบเตือนภัยให้กับผู้ใช้ที่ปฏิบัติงานกับระบบที่มีความสำคัญสูง

๙. การใช้งานระบบเทคโนโลยีสารสนเทศต้องกำหนดให้ตัด และหมดเวลาการใช้งานหลังจากที่ไม่มีกิจกรรมการใช้งานเกิน ๓๐ นาที

แนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางกายภาพห้องควบคุมระบบ

ความมั่นคงทางกายภาพถือเป็นส่วนสำคัญอันหนึ่งของระบบรักษาความปลอดภัย ความมั่นคงทางกายภาพรวมถึงการป้องกันสถานที่และอุปกรณ์ ให้ปลอดภัยจากการปล้น การโจรกรรม อุบัติภัยทางธรรมชาติ เช่นแผ่นดินไหว น้ำท่วมเป็นต้น การป้องกันอุบัติเหตุอันก่อให้เกิดความเสียหายเนื่องจากกระแสไฟฟ้าลัดวงจร อุณหภูมิ หรือความชื้น ในห้องควบคุมที่สูงเกินขีดจำกัด หรือการทำกระทำโดยประมาท เช่น การทำน้ำหกรดโดนเครื่องคอมพิวเตอร์ เซิร์ฟเวอร์ ดังนั้นจึงมีความจำเป็นในการป้องกันอาคารและอุปกรณ์โดยกำหนดเป็นนโยบายเพื่อถือปฏิบัติ ในเรื่องการสร้างห้องควบคุมระบบคอมพิวเตอร์และเครือข่ายรวมถึงมาตรการในการใช้ห้องควบคุมระบบคอมพิวเตอร์แม่ข่ายและเครือข่าย

๑. การเข้าไปในพื้นที่จำกัดการเข้าถึงห้องควบคุมระบบคอมพิวเตอร์แม่ข่ายและเครือข่าย
   ๑.๑ ไม่อนุญาตให้บุคคลใดเข้าไปในพื้นที่จำกัดการเข้าถึง ยกเว้นเจ้าหน้าที่ห้องควบคุมระบบหรือในกรณีที่บุคคลอื่นที่มีความจำเป็นเข้าไปปฏิบัติงานต้องได้รับอนุญาตจากผู้ดูแลระบบที่ได้รับมอบหมาย และต้องมีผู้ดูแลระบบที่ได้รับมอบหมายอย่างน้อย ๑ คนเข้าไปร่วมปฏิบัติงานและประสานงานด้วยทุกครั้ง และให้บันทึกกิจกรรมการปฏิบัติงานทุกครั้ง
   ๑.๒ ไม่อนุญาตให้บุคคลที่มีอายุต่ำกว่า ๑๕ ปี เข้าไปในพื้นที่จำกัดการเข้าถึง
   ๑.๓ ไม่อนุญาตให้นำอาหารหรือเครื่องดื่มเข้าไปในพื้นที่จำกัดการเข้าถึง
   ๑.๔ ไม่อนุญาตให้นำวัตถุไวไฟ วัตถุอันตราย และวัตถุติดไฟง่าย เช่น เศษกระดาษ เศษถุงพลาสติก เป็นต้น เข้าไปในเขตพื้นที่จำกัดการเข้าถึงเว้นแต่รับความเห็นชอบจากผู้ดูแลระบบที่ได้รับมอบหมาย
   ๑.๕ ในกรณีที่มีความจำเป็นเร่งด่วนหรือเหตุการณ์ฉุกเฉินอันอาจเป็นผลทำให้เกิดความเสียหายต่อ สินทรัพย์ จะอนุญาตให้เข้าไปในพื้นที่จำกัดการเข้าถึงได้โดยได้รับความเห็นชอบจากผู้ดูแลระบบที่ได้รับมอบหมาย
๒. ด้านกายภาพของห้องควบคุมระบบ
   ๒.๑ แยกอุปกรณ์ที่มีความสำคัญมากออกจากอุปกรณ์ที่ใช้งานทั่วไป โดยกำหนดลำดับความสำคัญของอุปกรณ์แต่ละชนิดไว้เช่น router, switch, server, UPS เป็นต้น
   ๒.๒ มี rack ในการจัดเก็บอุปกรณ์ต่างๆที่เหมาะสมเพื่อสะดวกในการบำรุงรักษา
   ๒.๓ ตำแหน่งของการวางอุปกรณ์ต่างๆ ไม่ควรวางใกล้ประตู หน้าต่างเพื่อป้องกันอุบัติเหตุที่อาจเกิดขึ้น ไม่ควรวางอุปกรณ์ให้เครื่องปรับอากาศเป่าถูกโดยตรงเพื่อหลีกเลี่ยงความชื้น
   ๒.๔ การจัดวางสาย cable network สายไฟฟ้าควรติดป้ายชื่อสายต้นทางปลายทาง และเก็บสายให้เรียบร้อยเพื่อป้องการการเดินสะดุด
   ๒.๕ ติดประกาศบันทึกการบำรุงรักษา ชื่อและหมายเลขโทรศัพท์ของผู้ดูแลรับผิดชอบอุปกรณ์แต่ละชนิด
   ๒.๖ มีระบบรักษาความปลอดภัยในห้องเช่น กล้อง CCTV ระบบการเข้าออกห้อง
   ๒.๗ มีระบบสังเกตการณ์อุณหภูมิภายใน Rack ระบบแจ้งเตือนและป้องกันอัคคีภัย
   ๒.๘ มีระบบสำรองไฟฟ้าเพื่อป้องกันไฟฟ้าดับ เช่น ติดตั้งระบบเครื่องกำเนิดไฟฟ้าอัตโนมัติ และระบบสำรองไฟฟ้าอัตโนมัติ เป็นต้น

๒.๙ ระบบปรับอากาศแบบควบคุมอุณหภูมิ (๒๐-๒๔°C) และความชื้น (๒๐- ๘๐%)

๓. การบำรุงรักษาห้องควบคุมระบบคอมพิวเตอร์แม่ข่ายและเครือข่าย

๓.๑ กรณีติดตั้งเซิร์ฟเวอร์หรืออุปกรณ์ต่างๆ ให้แกะหีบห่อและประกอบให้แล้วเสร็จจากภายนอกห้องควบคุมระบบคอมพิวเตอร์แม่ข่ายและเครือข่ายก่อนนำไปติดตั้ง เว้นแต่รับความเห็นชอบจากผู้ดูแลระบบที่ได้รับมอบหมาย

๓.๒ กรณีที่จำเป็นต้องทำงานก่อสร้าง แก้ไข และติดตั้ง ในพื้นที่ควบคุมและพื้นที่จำกัดการเข้าถึงต้องมีอุปกรณ์ควบคุม ฝุ่น ความร้อน เพื่อป้องกันความเสียหาย โดยผ่านความเห็นชอบจากผู้ดูแลระบบที่ได้รับมอบหมายก่อนการปฏิบัติงาน

๓.๓ ตรวจสอบความพร้อมของระบบรักษาความปลอดภัยทุกปี

๓.๔ จัดทำขั้นตอนแผนการดำเนินงานเมื่อเกิดกรณีฉุกเฉิน เช่น ไฟฟ้าลัดวงจร ไฟไหม้ แผ่นดินไหว น้ำท่วม หรือมีผู้บุกรุก เป็นต้น

๓.๕ ซ้อมการปฏิบัติงานตามแผนการดำเนินงานเมื่อเกิดกรณีฉุกเฉินทุกปี

๓.๖ มีตารางการเข้าบำรุงรักษาอุปกรณ์ชัดเจน

แนวปฏิบัติการควบคุมหน่วยงานภายนอกเข้าถึงระบบสารสนเทศ

การใช้บริการด้านไอซีทีจากหน่วยงานภายนอก บางครั้งหน่วยงานภายนอกอาจเข้าถึงระบบสารสนเทศ แก้ไข เปลี่ยนแปลง และประมวลผลระบบงานโดยไม่ได้รับอนุญาต ดังนั้น จึงต้องกำหนดแนวทางในการปฏิบัติงานของหน่วยงานภายนอกเพื่อความมั่นคง ปลอดภัย ของระบบสารสนเทศของสำนักหอสมุด โดยนโยบายและแนวปฏิบัตินี้ต้องตรวจสอบ และประเมินตามระยะเวลา ๑ ครั้งต่อปี

๑. หน่วยงานภายนอก ที่ต้องการสิทธิในการเข้าใช้งานระบบสารสนเทศและการสื่อสารของสำนักหอสมุด จะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษรเพื่อขออนุมัติจากผู้บริหารของหน่วยงาน

๒. จัดทำเอกสารแบบฟอร์มสำหรับหน่วยงานภายนอก โดยต้องมีรายละเอียดในการเข้าระบบสารสนเทศอย่างน้อย ดังนี้

๒.๑ เหตุผลในการขอใช้งาน

๒.๒ ระยะเวลาในการใช้งาน

๒.๓ การกำหนดการป้องกันในเรื่องการเปิดเผยข้อมูล

๓. หน่วยงานภายนอกที่ทำงานให้กับสำนักหอสมุดทุกหน่วยงาน จำเป็นต้องลงนามในสัญญาการไม่เปิดเผยข้อมูลของสำนักหอสมุด โดยสัญญาต้องทำให้เสร็จก่อนให้สิทธิในการเข้าสู่ระบบสารสนเทศ

๔. เจ้าของโครงการซึ่งรับผิดชอบต่อโครงการที่มีการเข้าถึงข้อมูลโดยหน่วยงานภายนอก ต้องกำหนดการเข้าใช้งานเฉพาะบุคคลที่จำเป็นเท่านั้น และให้หน่วยงานภายนอกลงนามในสัญญาไม่เปิดเผยข้อมูล และผู้ดูแลระบบ

ต้องควบคุมการปฏิบัติงานนั้น ๆ ให้มีความปลอดภัยทั้ง ๓ ด้าน คือ การรักษาความลับ (Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)

๕. สำนักหอสมุดมีสิทธิในการตรวจสอบตามสัญญาการใช้บริการด้านไอซีทีเพื่อให้มั่นใจว่าสามารถควบคุมการใช้งานอย่างทั่วถึงตามข้อกำหนด

๖. ในการจ้างเหมาพัฒนา บำรุงรักษาระบบผู้ดูแลระบบต้องกำหนดการเข้าถึงระบบสารสนเทศสำหรับผู้ปฏิบัติงานจากภายนอก ได้แก่

๖.๑ ต้องจัดให้มีการควบคุมการใช้งาน ได้แก่ กำหนดสิทธิในการใช้งานเฉพาะที่จำเป็นขั้นต่ำ ตรวจสอบว่าระบบสารสนเทศที่อนุญาตให้ใช้งานนั้นมีเฉพาะข้อมูลที่จำเป็นต้องใช้งาน

๖.๒ ต้องมีวิธีการพิสูจน์ตัวตนสำหรับผู้ใช้งานภายนอก ก่อนที่จะอนุญาตให้เข้ามาใช้งานระบบสารสนเทศ ได้แก่ การกำหนดชื่อผู้ใช้ และรหัสผ่าน สำหรับเข้าใช้งานระบบสารสนเทศ

๖.๓ ต้องบันทึกกิจกรรมการใช้งานข้อมูลเก็บเป็น Log File

๖.๔ ในระบบที่มีความสำคัญสูงไม่อนุญาตให้ทดสอบบนระบบจริง (Production) แต่ต้องทดสอบบนระบบทดสอบ (Test) ให้เสร็จสิ้นก่อนจึงจะนำมาติดตั้งบนระบบจริง และก่อนการติดตั้งระบบจริงต้องได้รับอนุญาตจากผู้บริหารก่อน

แนวปฏิบัติการสำรองและการกู้คืนข้อมูล

๑. การสำรองข้อมูล หน่วยงานที่มีเครื่องคอมพิวเตอร์แม่ข่ายให้บริการให้ดำเนินการคัดเลือกและจัดทำระบบสำรองข้อมูล ดังนี้

๑.๑ ผู้ดูและระบบมีหน้าที่

๑.๑.๑ ต้องสำรวจเครื่องคอมพิวเตอร์แม่ข่ายที่อยู่ในความดูแล และจัดระดับความสำคัญของข้อมูล

๑.๑.๒ สำรวจข้อมูล และ จัดระดับความสำคัญในการสำรองข้อมูล ดังนี้

ระดับ	ความหมาย	คำอธิบายความหมายเพิ่มเติม
๐	ไม่มีผลกระทบ	ไม่มีผลกระทบใด ๆ ต่อการดำเนินภารกิจ
๑	กระทบเล็กน้อย	มีผลกระทบในระดับที่ยังไม่มีนัยสำคัญต่อการดำเนินงานขององค์กร
๒	กระทบค่อนข้างน้อย	มีผลกระทบในระดับที่มีนัยสำคัญเล็กน้อย
๓	กระทบค่อนข้างรุนแรง	มีผลกระทบอย่างมีนัยสำคัญต่อการดำเนินภารกิจ
๔	กระทบรุนแรง	มีผลกระทบรุนแรงต่อความสามารถในการดำเนินงานต่อไปได้
๕	ปิดหน่วยงาน	มีผลกระทบรุนแรงต่อการดำรงอยู่ขององค์กร

๑.๑.๓ ต้องจัดให้มีความถี่ในการสำรองให้พอเพียง ในระบบที่มีความสำคัญสูง เครื่องที่มีความสำคัญสูงควรเพิ่มความถี่การสำรองให้มากขึ้น

๑.๑.๔ ต้องจัดทำผังการเชื่อมต่อระบบหรือขั้นตอนการสำรองข้อมูล

๑.๑.๕ ต้องทดสอบข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

๑.๑.๖ ต้องจัดทำบันทึกการสำรองข้อมูล และตรวจสอบว่าการสำรองข้อมูลสำเร็จหรือไม่ แก้ไขและรายงานต่อผู้บังคับบัญชา

๑.๑.๗ ต้องจัดให้มีการสำรองข้อมูลภายนอกหน่วยงานในระบบที่มีความสำคัญระดับสูง

๑.๑.๘ ต้องดำเนินการแก้ไขปัญหาและสรุปผลการแก้ไขปัญหาและรายงานต่อผู้บังคับบัญชา หรือในกรณีที่พบปัญหาในการสำรองข้อมูลจนเป็นเหตุไม่สามารถดำเนินการอย่างสมบูรณ์ได้

๑.๑.๙ เป็นผู้กำหนดชนิด เช่น Full หรือ Incremental และช่วงเวลาการสำรองข้อมูลตามความเหมาะสม พร้อมทั้งกำหนดสื่อที่ใช้เก็บข้อมูล

๑.๑.๑๐ ต้องทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง อย่างน้อยปีละ ๑ ครั้ง

๒. การกู้คืนข้อมูล ในกรณีที่พบปัญหาที่อาจสร้างความเสียหายต่อระบบคอมพิวเตอร์จนเป็นเหตุทำให้ต้องดำเนินการกู้คืนระบบ ผู้ดูแลระบบมีหน้าที่ดำเนินการแก้ไข รายงานผลการแก้ไขพร้อมทั้งบันทึกและรายงานสรุปผลการปฏิบัติงาน ต่อผู้บังคับบัญชา ดังนี้

๒.๑ ให้ใช้ข้อมูลทันสมัยที่สุด (Latest Update) ที่ได้สำรองไว้หรือตามความเหมาะสมเพื่อกู้คืนระบบ

๒.๒ หากความเสียหายที่เกิดขึ้นกับระบบคอมพิวเตอร์ หรือระบบเครือข่ายกระทบต่อการให้บริการ หรือการใช้งานของผู้ใช้ระบบ ให้แจ้งผู้ใช้งานทราบทันที พร้อมทั้งรายงาน ความคืบหน้าการกู้คืนระบบเป็นระยะจนกว่าจะดำเนินการเสร็จสิ้นอย่างสมบูรณ์

๒.๓ สาเหตุและวิธีการกู้คืน

สาเหตุ	วิธีการ
กรณีที่ ๑ เกิดความเสียหายขึ้นกับโปรแกรมต้นฉบับ (Source code)	ดำเนินการติดตั้งโปรแกรมต้นฉบับ (Source code) ที่มีการใช้งานอยู่ ณ ปัจจุบัน หรือล่าสุด
กรณีที่ ๒ เกิดความเสียหายขึ้นกับฐานข้อมูล (Database)	ดำเนินการกู้คืนฐานข้อมูลที่เก็บไว้ล่าสุด เพื่อให้ใช้งานได้ต่อเนื่องโดยที่ข้อมูลสูญหายน้อยที่สุด
กรณีที่ ๓ เกิดความเสียหายขึ้นกับระบบปฏิบัติการ (OS) โดยที่ฮาร์ดแวร์ยังคงทำงานปกติ	ดำเนินการติดตั้งระบบปฏิบัติการใหม่และติดตั้งระบบงานจากโปรแกรมต้นฉบับที่มีการใช้งานอยู่ ณ ปัจจุบัน หรือล่าสุด รวมถึงกู้คืนข้อมูลจากฐานข้อมูลที่เก็บไว้ล่าสุด
กรณีที่ ๔ เกิดความเสียหายขึ้นกับฮาร์ดแวร์	ให้บริษัทผู้ดูแลแก้ไขเบื้องต้นให้ฮาร์ดแวร์สามารถทำงานได้ตามปกติ และหากเกิดความเสียหายกับระบบปฏิบัติการและระบบงาน ให้บริษัทหรือผู้ได้รับมอบหมายดำเนินการติดตั้งระบบปฏิบัติการและระบบงานนั้นใหม่ โดยใช้โปรแกรมต้นฉบับ ที่มีการใช้งานอยู่ ณ ปัจจุบันหรือล่าสุด และกู้คืนข้อมูลจากฐานข้อมูลที่เก็บไว้ล่าสุด

๓. การจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ ที่อาจเกิดขึ้นกับระบบสารสนเทศ (IT Contingency Plan) หน่วยงานที่รับผิดชอบระบบสารสนเทศมีหน้าที่

๓.๑ ต้องจัดทำแผนความพร้อมกรณีฉุกเฉิน โดยแผนความพร้อมกรณีฉุกเฉินต้องได้รับการเห็นชอบจากผู้บริหารประกอบด้วย

๓.๑.๑ การกำหนดชนิดของภัยพิบัติ

๓.๑.๒ ประเมินความเสี่ยงที่มีผลทำให้ระบบที่มีระดับความสำคัญสูง ติดขัดหรือไม่สามารถใช้งานได้

๓.๑.๓ กำหนดขั้นตอนรับมือภัยพิบัติ

๓.๒ ต้องทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมความพร้อมกรณีฉุกเฉินอย่างสม่ำเสมออย่างน้อยปีละ ๑ ครั้ง

๓.๓ ทบทวนแผนเตรียมความพร้อมกรณีฉุกเฉินความพร้อมอย่างน้อยปีละ ๑ ครั้ง

แนวปฏิบัติการดำเนินการตอบสนองเหตุการณ์มั่นคงปลอดภัยระบบสารสนเทศ

หากเกิดเหตุการณ์ด้านความมั่นคงปลอดภัย จำเป็นต้องตอบสนองต่อเหตุการณ์อย่างทันท่วงที ดังนั้น จึงต้องมีแนวปฏิบัติเมื่อเกิดเหตุการณ์ที่มีผลต่อความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

๑. ระบบไฟร์วอลล์

๑.๑. ดำเนินการตรวจสอบกฎ (Rule) ของระบบป้องกันการบุกรุก อย่างน้อยเดือนละครั้ง

๑.๒. ดำเนินการตรวจสอบบันทึกของไฟล์ล็อก (Log File) และรายงานของไฟล์วอลล์ สิ่งที่ต้องตรวจสอบมีดังต่อไปนี้

๑.๒.๑ กลุ่มข้อมูล (Packet) ที่ไฟล์วอลล์ได้ปิดกั้น

๑.๒.๒ ลักษณะของกลุ่มข้อมูล (Packet) ที่ถูกปิดกั้น

๑.๒.๓ หมายเลขไอพี ของเครือข่ายใดที่ถูกปิดกั้น เป็นจำนวนมาก

๑.๓. หากตรวจสอบพบการโจมตี หรือเหตุการณ์ละเมิดความมั่นคงปลอดภัยระบบสารสนเทศให้แจ้งผู้บังคับบัญชาเพื่อตัดสินใจดำเนินการแก้ไขปัญหา หากไม่สามารถแก้ไขปัญหาได้ให้รายงานต่อผู้อำนวยการสำนักหอสมุด

๑.๔. กรณีที่ตรวจพบเหตุละเมิดความมั่นคงปลอดภัยที่มีผลกระทบค่อนข้างรุนแรง ที่อาจส่งผลต่อเครือข่ายโดยรวม ให้ระงับการเชื่อมต่อเครือข่าย และให้แก้ไขเครื่องนั้นทันที

๒. เครื่องคอมพิวเตอร์แม่ข่าย

๒.๑ ต้องตรวจสอบความปลอดภัยเครื่องคอมพิวเตอร์แม่ข่ายก่อนเปิดให้บริการ โดยอย่างน้อยต้องดำเนินการดังต่อไปนี้

๒.๑.๑ ติดตั้งไฟล์วอลล์ที่เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ เปิดเฉพาะ port ที่ใช้งาน

๒.๑.๒ ปิด Service ที่ไม่ได้ใช้งาน

๒.๑.๓ ติดตั้ง NTP เพื่อเทียบเวลาให้ถูกต้อง

๒.๒ ต้องสำรวจเครื่องคอมพิวเตอร์ที่อยู่ในความดูแล และกำหนดผู้ดูแลรับผิดชอบหลัก และผู้รับผิดชอบสำรอง

๒.๓ ต้องตรวจสอบความมั่นคงปลอดภัย ต้องจดบันทึก ตรวจสอบ แก้ไข และรายงาน เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยต่อผู้บังคับบัญชา

๒.๔ ต้องตรวจสอบ แก้ไข และรายงานช่องโหว่ของเครื่องคอมพิวเตอร์แม่ข่ายต่อผู้บังคับบัญชา

๒.๕ กรณีที่ตรวจพบเหตุละเมิดความมั่นคงปลอดภัยที่มีผลกระทบค่อนข้างรุนแรง ต้องดำเนินการแจ้งไปยังผู้รับผิดชอบหน่วยงาน หรือผู้มีอำนาจที่ได้รับมอบหมาย ระงับการเชื่อมต่อเครือข่าย และให้แก้ไขเครื่องนั้นทันที

๓. ภัยคุกคามทางอินเทอร์เน็ต ประกอบด้วย ไวรัส หนอนอินเทอร์เน็ต โทรจัน รวมถึงสปายแวร์

๓.๑ ต้องดำเนินการจัดหาซอฟต์แวร์เพื่อป้องกัน

๓.๒ ต้องดำเนินการติดตั้งโปรแกรมป้องกันภัยคุกคามทางอินเทอร์เน็ต และต้องตั้งให้ Update อย่างน้อยสัปดาห์ละครั้ง

๓.๓ ดำเนินการตรวจสอบบันทึกของไฟล์ล็อก (Log File) และรายงานของของอุปกรณ์ สิ่งที่ต้องตรวจสอบมีดังต่อไปนี้

๓.๓.๑ การคุกคามทางอินเทอร์เน็ตใดที่มีเป็นจำนวนมาก

๓.๓.๒ ถูกส่งมาจากที่ใด และถูกส่งไปยังที่ใด

๓.๔ ต้องศึกษาหาวิธีแก้ไขเครื่องคอมพิวเตอร์ที่มีภัยคุกคามทางอินเทอร์เน็ต โดยเฉพาะที่ตรวจพบว่ามีการกระจายภายในเครือข่าย

๓.๕ กรณีที่ตรวจพบเหตุละเมิดความมั่นคงปลอดภัยที่มีผลกระทบค่อนข้างรุนแรง ที่อาจส่งผลต่อเครือข่ายโดยรวม ให้ระงับการเชื่อมต่อเครือข่าย และให้แก้ไขเครื่องนั้นทันที

ระดับความรุนแรงของเหตุการณ์

ระดับ	ความหมาย	คำอธิบายความหมายเพิ่มเติม
๐	ไม่มีผลกระทบ	ไม่มีผลกระทบใด ๆ ต่อการดำเนินภารกิจ
๑	กระทบเล็กน้อย	มีผลกระทบในระดับที่ยังไม่มีนัยสำคัญต่อการดำเนินงานขององค์กร
๒	กระทบค่อนข้างน้อย	มีผลกระทบในระดับที่มีนัยสำคัญเล็กน้อย
๓	กระทบค่อนข้างรุนแรง	มีผลกระทบอย่างมีนัยสำคัญต่อการดำเนินภารกิจ
๔	กระทบรุนแรง	มีผลกระทบรุนแรงต่อความสามารถในการดำเนินงานต่อไปได้
๕	ปิดหน่วยงาน	มีผลกระทบรุนแรงต่อการดำรงอยู่ขององค์กร

แนวปฏิบัติการทำลายข้อมูลหรือกำจัดสื่อบันทึกข้อมูล

๑. เมื่อต้องทำลายข้อมูลอิเล็กทรอนิกส์ ผู้รับผิดชอบข้อมูลอิเล็กทรอนิกส์ต้องเป็นผู้ทำลายข้อมูล

๒. กำหนดวิธีการทำลายข้อมูลอิเล็กทรอนิกส์บนสื่อบันทึกข้อมูล ดังนี้ หรือใช้มาตรฐาน 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	เก็บรักษาไว้อย่างน้อย ๑ ปีหรือตามที่กฎหมายกำหนด
แผ่น CD/DVD	ใช้วิธีการ Format	- ใช้การตัดให้สิ้นสภาพการใช้งาน	เก็บรักษาไว้อย่างน้อย ๑ ปีหรือตามที่กฎหมายกำหนด
เทป	-	- ใช้วิธีการทุบให้เสียหาย	เก็บรักษาไว้อย่างน้อย ๑ ปีหรือตามที่กฎหมายกำหนด
ฮาร์ดดิสก์	ใช้วิธีการ Format	- ทำลายข้อมูลบน Flash Drive ตามมาตรฐาน DoD 5220.22-M ของกระทรวงกลาโหมสหรัฐอเมริกา ซึ่งเป็นมาตรฐานการทำลายข้อมูลโดยการเขียนทับข้อมูลเดิมหลายรอบ - ใช้วิธีการทุบให้เสียหาย	เก็บรักษาไว้อย่างน้อย ๑ ปีหรือตามที่กฎหมายกำหนด