ประกาศ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สำนักหอสมุด มหาวิทยาลัยเกษตรศาสตร์

เพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์ผ่านเครือข่ายคอมพิวเตอร์ของสำนักหอสมุด มหาวิทยาลัยเกษตรศาสตร์เป็นไปตาม มาตรา ๕ และมาตรา ๗ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ ซึ่งกำหนดให้หน่วยงานของรัฐจัดทำประกาศแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สำนักหอสมุดจึงกำหนดแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคง โดยมีวัตถุประสงค์เพื่อ

๑. คงไว้ซึ่งการใช้งานเครือข่ายคอมพิวเตอร์สำนักหอสมุดได้อย่างมีประสิทธิภาพและเสถียรภาพ

๒. ปกป้องข้อมูลส่วนบุคคลและความเป็นส่วนตัวของผู้ใช้

๓. ปกป้องและรักษาซึ่งเอกภาพของข้อมูลและทรัพยากรสารสนเทศของสำนักหอสมุด

๔. ให้ผู้มีส่วนเกี่ยวข้องเข้าใจถึงหลักปฏิบัติในการใช้เครือข่ายตามหลักจริยธรรมและหลักกฎหมาย

อาศัยอำนาจตามความในมาตรา ๑๙ และ ๒๒ แห่งพระราชบัญญัติมหาวิทยาลัยเกษตรศาสตร์ พ.ศ. ๒๕๔๑ อธิการบดีมหาวิทยาลัยเกษตรศาสตร์จึงกำหนดแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศไว้ดังนี้

ข้อ ๑. ประกาศนี้เรียกว่า "ประกาศสำนักหอสมุด มหาวิทยาลัยเกษตรศาสตร์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๕๙"

ข้อ ๒. ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศเป็นต้นไป

ข้อ ๓. การรักษาความมั่นคงปลอดภัยด้านสารสนเทศในการทำธุรกรรมทางอิเล็กทรอนิกส์ตามประกาศนี้มี ๒ ส่วน ดังนี้

๓.๑ ส่วนที่ว่าด้วยการจัดทำนโยบาย

(๑) ผู้บริหาร เจ้าหน้าที่ปฏิบัติการด้านคอมพิวเตอร์ และผู้ใช้งานได้มีส่วนร่วมในการทำนโยบาย

(๒) นโยบายได้รับการจัดทำเป็นลายลักษณ์อักษร โดยประกาศให้ผู้ใช้งานทราบและสามารถเข้าถึงได้อย่างสะดวกผ่านทางเว็บไซต์ของสำนักหอสมุด

(๓) กำหนดผู้รับผิดชอบตามนโยบายและแนวปฏิบัติดังกล่าวให้ชัดเจน

๓.๒ ส่วนที่ว่าด้วยรายละเอียดของนโยบายประกอบด้วย ๓ ส่วน คือ

ส่วนที่ ๑ ความหมายและคำจำกัดความ

ส่วนที่๒ นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศสำนักหอสมุด มหาวิทยาลัยเกษตรศาสตร์ พ.ศ.๒๕๕๙ ซึ่งกำหนดผู้รับผิดชอบตามนโยบาย ซึ่งมีสาระสำคัญสอดคล้องตามมาตรา ๕ และมาตรา ๗ พระราชกฎษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.๒๕๔๙

ส่วนที่ ๓ แนวปฏิบัติและข้อกำหนดการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อกำกับดูแลการดำเนินงาน การบริหารจัดการระบบสารสนเทศให้มีความมั่นคงปลอดภัย ได้กำหนดแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศที่มีความสอดคล้องกับนโยบายความมั่นคงปลอดภัยด้านสารสนเทศ

ข้อ ๔ กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใดๆ แก่หน่วยงานหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่องละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กำหนดให้ "ผู้บริหารระดับสูงสุด" เป็นผู้รับผิดชอบต่อความเสี่ยง และเสียหายหรืออันตรายที่เกิดขึ้น

ข้อ ๕ สำนักหอสมุดมีนโยบายไม่ตรวจตราการใช้เครือข่ายของผู้ใช้รายใดรายหนึ่งในกรณีปกติ แต่มหาวิทยาลัยสงวนสิทธิในการติดตั้งเครื่องมือฮาร์ดแวร์หรือซอฟต์แวร์เพื่อบันทึกและเฝ้าระวังการใช้คอมพิวเตอร์และเครือข่ายเพื่อคงไว้ซึ่งการให้บริการอย่างปลอดภัย มีประสิทธิภาพและเป็นไปตามกฎหมายบัญญัติ ทั้งนี้มหาวิทยาลัยคงไว้ซึ่งอำนาจในการจำกัด ระงับ หรือเพิกถอนสิทธิการใช้ระบบสารสนเทศ และดำเนินการสืบสวนเมื่อได้รับรายงาน การแจ้งเตือน หรือตรวจพบการกระทำใดที่อาจก่อให้เกิดปัญหาความมั่นคงปลอดภัย ปัญหาเสถียรภาพ หรือการกระทำที่ขัดต่อนโยบายหรือพระราชบัญญัติมหาวิทยาลัย หรือกฎหมายของรัฐ

ข้อ ๖ สำนักหอสมุดและสำนักบริการคอมพิวเตอร์มีหน้าที่ออกระเบียบปฏิบัติในการจำกัด ระงับ หรือเพิกถอนสิทธิการใช้เครือข่ายของผู้ฝ่าฝืนระเบียบ ตลอดจนระงับหรือจำกัดการเข้าถึงคอมพิวเตอร์ที่มีข้อมูลขัดต่อระเบียบ นโยบาย พระราชบัญญัติมหาวิทยาลัย หรือกฎหมายของรัฐ ในกรณีสำคัญให้สำนักบริการคอมพิวเตอร์รายงานการฝ่าฝืนระเบียบให้หน่วยงานต้นสังกัดและ/หรือมหาวิทยาลัยเพื่อพิจารณาลงโทษ

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

ประกาศ ณ วันที่ เมษายน พ.ศ. ๒๕๕๙

(นางอารีย์ ธัญกิจจานุกิจ)

ผู้อำนวยการสำนักหอสมุด

คำสั่งสำนักหอสมุด มหาวิทยาลัยเกษตรศาสตร์

ที่ /๒๕๕๙

เรื่อง แต่งตั้งคณะทำงานรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ด้วยมาตรา ๕ และมาตรา ๗ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ ซึ่งกำหนดให้หน่วยงานของรัฐจัดทำประกาศแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศนั้น เพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์ผ่านเครือข่ายคอมพิวเตอร์ของสำนักหอสมุด มหาวิทยาลัยเกษตรศาสตร์เป็นไปด้วยความเรียบร้อยและการมีส่วนร่วม จึงขอแต่งตั้งคณะทำงาน ดังนี้

๑.	ผู้อำนวยการ	ที่ปรึกษา
๒.	รองผู้อำนวยการ	ที่ปรึกษา
๓.	ผู้ช่วยผู้อำนวยการ	ที่ปรึกษา
๔.	หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ	ประธานคณะทำงาน
๕.	หัวหน้าฝ่าย	กรรมการ
๖.	คณะกรรมการเพิ่มขีดความสามารถในการใช้เทคโนโลยีสารสนเทศเพื่อการพัฒนางานห้องสมุด	กรรมการ
๗.	นางสาวดลนภา แว่วศรี	กรรมการ
๘.	นางสาวรุ่งอรุณ ผาสุกสกุล	กรรมการ
๙.	นายชาญณรงค์ เผือกพูลผล	กรรมการ
๑๐.	นายประจักษ์ สุขอร่าม	กรรมการ
๑๑.	นายอภิยศ เหรียญวิพัฒน์	กรรมการและเลขานุการ

ทั้งนี้ ให้คณะทำงานชุดนี้ ดำเนินการจัดทำ ทบทวน ตรวจสอบและเผยแพร่ เอกสาร แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้กับผู้ใช้งาน หน่วยงานภายนอก และผู้ที่เกี่ยวข้องในขอบเขตรับทราบ

สั่ง ณ วันที่ พ.ศ. ๒๕๕๙

(นางอารีย์ ธัญกิจจานุกิจ)

ผู้อำนวยการสำนักหอสมุด

คำนำ

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้ระบบเทคโนโลยีสารสนเทศของสำนักหอสมุดเป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่องรวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่างๆ สำนักหอสมุดจึงเห็นสมควรกำหนดนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยกำหนดให้มีมาตรฐาน (Standard) แนวปฏิบัติ (Guideline) ขั้นตอนปฏิบัติ (Procedure) ให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและป้องกันภัยคุกคามต่างๆ

วัตถุประสงค์

๑. การจัดทำนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์ของสำนักหอสมุดให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล

๒. กำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศอ้างอิงตามมาตรฐาน ISO/IEC 27001 และมีการปรับปรุงอย่างต่อเนื่อง

๓. นโยบายนี้จะต้องทำการเผยแพร่ให้เจ้าหน้าที่ทุกระดับในสำนักหอสมุดได้รับทราบและเจ้าหน้าที่ทุกคนจะต้องลงนามยอมรับและปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

๔. เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและขั้นตอนปฏิบัติ ให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับสำนักหอสมุด ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้ระบบเทคโนโลยีสารสนเทศในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด

๕. นโยบายนี้ต้องมีการดำเนินการทบทวน ตรวจสอบและประเมินนโยบายตามระยะเวลาอย่างน้อย ๑ ครั้ง ต่อปี

นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๑. ส่งเสริมและสนับสนุนการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้ตอบสนองต่อ พันธกิจและนโยบายขององค์กร

๒. มุ่งกำหนดแนวปฏิบัติ แนวทางแก้ไข หรือบทลงโทษตามความเหมาะสมหากมีการละเมิดหรือ ฝ่าฝืนแนวนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ รวมทั้งติดตามและตรวจสอบการดำเนินงานอย่างสม่ำเสมอ เพื่อให้เป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

๓. เน้นกำกับดูแลการดำเนินงานเพื่อบริหารจัดการให้ระบบเทคโนโลยีสารสนเทศมีความถูกต้องสมบูรณ์ และพร้อมใช้งานอยู่เสมอ

๔. เผยแพร่ความรู้ ความเข้าใจเพื่อสร้างความตระหนักให้บุคลากรที่เกี่ยวข้องทั้งของหน่วยงานเองและของหน่วยงานที่เกี่ยวข้อง ตลอดจนส่งเสริมให้มีการศึกษาอย่างต่อเนื่อง

๕. ติดตาม ตรวจสอบการดำเนินงาน และปรับปรุงแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้สอดคล้องตามการเปลี่ยนแปลงของเทคโนโลยี

นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขององค์กร แต่ละส่วนที่กล่าวข้างต้นจะประกอบด้วย วัตถุประสงค์ แนวทางปฏิบัติ (Guideline) และขั้นตอนวิธีการปฏิบัติ (Procedure) ในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศขององค์กร เพื่อที่จะทำให้องค์กรมีมาตรการในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศอยู่ในระดับที่ปลอดภัย ช่วยลดความเสียหายต่อการดำเนินงาน ทรัพย์สิน บุคลากร ขององค์กร ทำให้สามารถดำเนินงานได้อย่างมั่นคงปลอดภัย

นโยบายการเข้าใช้งานระบบเทคโนโลยีสารสนเทศขององค์กรนี้ จัดเป็นมาตรฐานด้านความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศขององค์กร ซึ่งบุคลากรและหน่วยงานภายนอกจะต้องปฏิบัติตามอย่างเคร่งครัด

สารบัญ

หน้า

ส่วนที่ ๓ แนวปฏิบัติและข้อกำหนดการรักษาความมั่นคงปลอดภัยสารสนเทศ

- แนวปฏิบัติการใช้งานสารสนเทศให้มั่นคงปลอดภัย
- แนวปฏิบัติในการควบคุมการเข้าถึงสารสนเทศ
- แนวปฏิบัติการควบคุมการเข้าถึงเครือข่าย
- แนวปฏิบัติการจัดการการเข้าถึงของผู้ใช้งาน
- แนวปฏิบัติการควบคุมการเข้าถึงระบบปฏิบัติการ
- แนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางกายภาพห้องควบคุมระบบ
- แนวปฏิบัติการควบคุมหน่วยงานภายนอกเข้าถึงระบบสารสนเทศ
- แนวปฏิบัติการสำรองและการกู้คืนข้อมูล
- แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสำหรับการดำเนินงาน
- แนวปฏิบัติการดำเนินการตอบสนองเหตุการณ์มั่นคงปลอดภัยระบบสารสนเทศ
- แนวปฏิบัติการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

ส่วนที่ ๑

ความหมายและคำจำกัดความ

---

๑. **หน่วยงานภายนอก** หมายความว่า องค์กร หรือหน่วยงานภายนอกที่ได้รับอนุญาตให้มีสิทธิในการเข้าถึงและการใช้งานข้อมูลหรือสินทรัพย์ต่าง ๆ ของสำนักหอสมุด โดยจะได้รับสิทธิในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับข้อมูล

๒. **ผู้บริหารระดับสูงสุด (Chief Executive Officer : CEO)** หมายความว่า ผู้อำนวยการสำนักหอสมุด

๓. **ผู้บริหารด้านไอที** หมายความว่า ผู้ที่ผู้อำนวยการสำนักหอสมุด มอบหมายให้กำกับดูแลรับผิดชอบงานด้านเทคโนโลยีสารสนเทศของสำนักหอสมุด มหาวิทยาลัยเกษตรศาสตร์

๔. **ผู้บริหาร** หมายความว่า ผู้อำนวยการ รองผู้อำนวยการ ผู้ช่วยผู้อำนวยการ หัวหน้าฝ่ายที่ได้รับมอบหมายให้ดูแลด้านไอที

๕. **ผู้บังคับบัญชา** หมายความว่า ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของสำนักหอสมุด

๖. **ผู้ดูแลระบบ** (System administrator) หมายความว่า ผู้ซึ่งได้รับมอบหมายจากผู้บังคับบัญชาให้ทำหน้าที่ดูแลเซิร์ฟเวอร์ ระบบสารสนเทศ และระบบเครือข่ายคอมพิวเตอร์ให้บริการได้อย่างมีเสถียรภาพ

๗. **ผู้พัฒนาระบบ** หมายความว่า ผู้ซึ่งได้รับมอบหมายให้รับผิดชอบในการพัฒนาระบบสารสนเทศ

๘. **เจ้าหน้าที่** หมายความว่า บุคลากรทุกประเภทของสำนักหอสมุด

๙. **ผู้ใช้งาน** (user) หมายความว่า นักเรียนโรงเรียนสาธิตแห่งมหาวิทยาลัยเกษตรศาสตร์ นิสิต บุคลากร ของมหาวิทยาลัยเกษตรศาสตร์ หรือบุคคลภายนอกที่มีบัญชีรายชื่อที่ออกโดยสำนักบริการคอมพิวเตอร์ และ/หรือหน่วยงานภายนอกที่ได้รับอนุญาตให้ใช้สินทรัพย์สารสนเทศของสำนักหอสมุด

๑๐. **การรักษาความมั่นคงปลอดภัย** หมายความว่า การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศ และการสื่อสาร

๑๑. **มาตรฐาน** (Standard) หมายความว่า บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริง เพื่อให้ได้ตามวัตถุประสงค์หรือเป้าหมาย

๑๒. **วิธีการปฏิบัติ** (Procedure) หมายความว่า รายละเอียดที่บอกขั้นตอนเป็นข้อ ๆ ที่ต้องนำมาปฏิบัติเพื่อให้ได้มาซึ่งมาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์

๑๓. **แนวปฏิบัติ** (Guideline) หมายความว่า แนวทางที่ไม่ได้บังคับให้ปฏิบัติแต่แนะนำให้ปฏิบัติตาม เพื่อให้สามารถบรรลุเป้าหมายได้ง่ายขึ้น

๑๔. **สิทธิของผู้ใช้งาน** หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของสำนักหอสมุด

๑๕. **เจ้าของข้อมูล** หมายความว่า ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงานโดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น ๆ หรือ ได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย

๑๖. **สินทรัพย์** หมายความว่า ข้อมูล ระบบข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน ได้แก่ บุคลากร ฮาร์ดแวร์ ซอฟต์แวร์ คอมพิวเตอร์ เซิร์ฟเวอร์ ระบบสารสนเทศ ระบบเครือข่าย อุปกรณ์เครือข่าย เลขที่อยู่ไอพี โดเมนเนม รวมถึงซอฟต์แวร์ที่มีลิขสิทธิ หรือสิ่งใดก็ตามที่มีคุณค่าต่อหน่วยงาน

๑๗. **ห้องควบคุม** หมายถึง ห้องที่ติดตั้งและจัดวางระบบเซิร์ฟเวอร์ อุปกรณ์เชื่อมต่อ และอุปกรณ์เครือข่ายของสำนักหอสมุด

๑๘. **ระบบอินเทอร์เน็ต** (Internet) หมายความว่า ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่างๆ ของสำนักหอสมุดเข้ากับเครือข่ายอินเทอร์เน็ต

๑๙. **ระบบสารสนเทศ** หมายความว่า ระบบงานของสำนักหอสมุดที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่าย ที่นำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนให้การบริการการพัฒนาและควบคุม การติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย ระบบปฏิบัติการ โปรแกรมประยุกต์ ข้อมูลสารสนเทศ ฯลฯ

๒๐. **ระบบเครือข่ายคอมพิวเตอร์** (Computer Network System) หมายความว่า ระบบที่เชื่อมต่อคอมพิวเตอร์ เซิร์ฟเวอร์ อุปกรณ์เครือข่ายต่าง ๆ ของสำนักหอสมุด

๒๑. **จดหมายอิเล็กทรอนิกส์** (e-mail) หมายความว่า ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และระบบเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิกภาพเคลื่อนไหว ที่ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับผ่านโพรโทคอล ต่างๆ เช่น SMTP, POP3, IMAP ฯลฯ

๒๒. **สื่อบันทึกพกพา** (portable media) หมายความว่า สื่ออิเล็กทรอนิกส์ที่ใช้ในการบันทึกหรือจัดเก็บข้อมูล เช่น CD , DVD , flash drive, external hard disk ฯลฯ

๒๓. **ชื่อผู้ใช้** (username) หมายความว่า ชุดของตัวอักษรหรือตัวเลขที่ถูกกำหนดขึ้นเพื่อใช้ในการเข้าใช้งานระบบคอมพิวเตอร์และระบบเครือข่ายที่กำหนดสิทธิการใช้งานไว้

๒๔. **รหัสผ่าน** (password) หมายความว่า ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคลเพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศ

๒๕. **การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ** หมายความว่า การอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งาน และหน่วยงานภายนอก เข้าถึงหรือใช้งานระบบสารสนเทศ อุปกรณ์ประมวลผลสารสนเทศ และระบบเครือข่าย ทั้งทางอิเล็กทรอนิกส์ และทางกายภาพ

๒๖. **ความมั่นคงปลอดภัยด้านสารสนเทศ** หมายความว่า การรักษาไว้ซึ่งความลับ (confidentiality) ความครบถ้วนถูกต้อง (integrity) และความพร้อมใช้ (availability) ของสารสนเทศ และระบบเครือข่าย รวมทั้งคุณสมบัติอื่น ได้แก่ความถูกต้องแท้จริง (authenticity) ความรับผิด (accountability) การห้ามปฏิเสธความรับผิด (non-repudiation) และความน่าเชื่อถือ (reliability)

๒๗. **เหตุการณ์ด้านความปลอดภัย** หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่งคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

๒๘. **สถานการณ์ด้านความปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด** หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ซึ่งอาจทำให้ระบบถูกบุกรุกโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

๒๙. **การพิสูจน์ยืนยันตัวตน** (authentication) หมายความว่า ขั้นตอนการรักษาความปลอดภัยในการเข้าใช้ระบบ เป็นขั้นตอนในการพิสูจน์ยืนยันตัวตนของผู้ใช้บริการระบบ ทั่วไปแล้วจะเป็นการพิสูจน์โดยใช้ชื่อผู้ใช้และรหัสผ่าน

๓๐. **VPN** (virtual private network) หมายความว่า เครือข่ายคอมพิวเตอร์เสมือนส่วนตัว โดยในการรับส่งข้อมูลจริงจะทำโดยการเข้ารหัสเฉพาะแล้วรับ-ส่งผ่านเครือข่ายอินเทอร์เน็ต ทำให้บุคคลอื่นไม่สามารถอ่านได้และมองไม่เห็นข้อมูลนั้นไปจนถึงปลายทาง

๓๑. **แผนผังระบบเครือข่าย** (network diagram) หมายความว่า แผนผังซึ่งแสดงถึงการเชื่อมต่อของระบบเครือข่ายของสำนักหอสมุด

ส่วนที่ ๒

นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

หมวดที่ ๑ นโยบายความมั่นคงปลอดภัยขององค์กร (Security Policy)

1.1 นโยบายการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy)

วัตถุประสงค์ เพื่อกำหนดทิศทางและสนับสนุนการดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศ โดยให้สอดคล้องตามภารกิจขององค์กร และไม่ขัดต่อกฎหมายและระเบียบข้อบังคับที่เกี่ยวข้อง

นโยบาย

1.1.1 เอกสารนโยบายความมั่นคงปลอดภัยสารสนเทศที่เป็นลายลักษณ์อักษร (Information Security Policy Document)

๑) คณะทำงานด้านความมั่นคงปลอดภัยสารสนเทศ ต้องจัดทำนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ เป็นลายลักษณ์อักษรเพื่อให้เกิดความเชื่อมั่นและมีความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและระบบเครือข่ายสื่อสารข้อมูล โดยนโยบายฯ ดังกล่าวจะต้องได้รับการอนุมัติจากอธิการบดีเพื่อการนำไปใช้

๒) คณะทำงานด้านความมั่นคงปลอดภัยสารสนเทศ ต้องจัดให้เผยแพร่ เอกสาร นโยบายระบบบริหารการรักษาความมั่นคงปลอดภัยสารสนเทศ ให้กับผู้ใช้งาน หน่วยงานภายนอก และผู้ที่เกี่ยวข้องในขอบเขตรับทราบ

1.1.2 การทบทวนการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

๑) คณะทำงานด้านความมั่นคงปลอดภัยสารสนเทศ ต้องดำเนินการตรวจสอบ ทบทวน และประเมินนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศตามระยะเวลาที่กำหนดไว้ หรืออย่างน้อย ๑ ครั้งต่อปี หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญต่อองค์กร

หมวดที่ ๒ โครงสร้างความมั่นคงปลอดภัยสารสนเทศ (organization of Information Security)

๒.๑ โครงสร้างความมั่นคงปลอดภัยสารสนเทศภายในองค์กร (Internal organization)

วัตถุประสงค์ เพื่อกำหนดกรอบการบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศภายในองค์กร

นโยบาย

๒.๑.๑ การกำหนดบทบาทและหน้าที่ด้านการจัดการความมั่นคงปลอดภัยสารสนเทศ (Information security roles and responsibilities)

๑) ผู้บริหารระดับสูงสุดต้องแต่งตั้งกลุ่มหรือคณะทำงานด้านความมั่นคงปลอดภัยสารสนเทศ และมอบหมายหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ

๒.๑.๒ การแบ่งแยกหน้าที่ความรับผิดชอบ (Segregation of duties)

๑) ผู้บริหารด้านไอทีต้องกำหนดตำแหน่งหน้าที่และความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศให้เหมาะสม พร้อมทั้งควบคุมการปฏิบัติงานเพื่อให้คงไว้ซึ่งนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศขององค์กร

๒) ผู้บริหารด้านไอทีเป็นผู้รับผิดชอบการบริหารจัดการ กำกับดูแล ติดตาม และทบทวนภาพรวมของนโยบายความมั่นคงปลอดภัยด้านสารสนเทศขององค์กร

๓) ผู้บริหารต้องรับผิดชอบกำกับดูแลความมั่นคงปลอดภัยให้เป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศขององค์กร

๔) ผู้ใช้งาน และหน่วยงานภายนอกต้องรับผิดชอบในการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศขององค์กร

๒.๑.๓ การติดต่อกับหน่วยงานผู้มีอำนาจ (Contact with authorities)

๑) ต้องกำหนดรายชื่อ และข้อมูลสำหรับติดต่อกับหน่วยงานอื่นๆ เช่น สำนักบริการคอมพิวเตอร์ มหาวิทยาลัยเกษตรศาสตร์ การรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ประเทศไทย (ThaiCERT) การไฟฟ้า เพื่อใช้สำหรับติดต่อประสานงานด้านความมั่นคงปลอดภัย

๒.๑.๔ การติดต่อกับกลุ่มที่มีความสนใจเป็นพิเศษเรื่องเดียวกัน (Contact with special interest groups)

๑) ต้องกำหนดรายชื่อ และข้อมูลสำหรับติดต่อกลุ่มที่มีความสนใจเป็นพิเศษเรื่องเดียวกัน

๒.๑.๕ ความมั่นคงปลอดภัยสารสนเทศกับการบริหารจัดการโครงการ (Information security in project management)

๑) ต้องระบุความมั่นคงปลอดภัยสารสนเทศสำหรับโครงการที่เกี่ยวข้องกับสารสนเทศ

หมวดที่ ๓ ความมั่นคงปลอดภัยสำหรับทรัพยากรบุคคล (Human Resource Security)

๓.๑ การสรรหาบุคลากรก่อนการทำงาน (Prior to employment)

วัตถุประสงค์ เพื่อคัดสรรพนักงานที่ตรงกับความต้องการ และเพื่อให้พนักงานเข้าใจในหน้าที่และความรับผิดชอบ

นโยบาย

๓.๑.๑ ข้อตกลงและเงื่อนไขการจ้างงาน (Terms and conditions of employment)

๑) เพื่อให้การบริหารจัดการบัญชีผู้ใช้ เป็นไปอย่างถูกต้องและเป็นปัจจุบันที่สุด เจ้าหน้าที่บุคคลที่ดูแลทรัพยากรบุคคลขององค์กรต้องแจ้งให้ ผู้ดูแลระบบทราบทันทีเมื่อมีเหตุดังนี้

(๑) การว่าจ้างงาน

(๒) การเปลี่ยนแปลงสภาพการว่าจ้างงาน

(๓) การลาออกจากงาน หรือการสิ้นสุดการเป็นผู้บริหาร พนักงาน และลูกจ้างหรือการถึงแก่กรรม

(๔) การโยกย้ายหน่วยงาน

(๕) การพักงาน การลงโทษทางวินัย หรือระงับการปฏิบัติหน้าที่

๓.๒ ระหว่างการจ้างงาน (During employment)

วัตถุประสงค์ เพื่อให้พนักงานและผู้ที่ทำสัญญาจ้างตระหนักและปฏิบัติตามหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศของตนเอง

นโยบาย

๓.๒.๑ การสร้างความตระหนัก การให้ความรู้ และการฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศ (Information security awareness, education and training)

๑) เจ้าหน้าที่ใหม่ต้องได้รับการอบรมเกี่ยวกับเรื่องนโยบายการรักษาความมั่นคงปลอดภัย โดยควรเป็นส่วนหนึ่งของการปฐมนิเทศพนักงาน

๓.๓ การสิ้นสุดหรือการเปลี่ยนการจ้างงาน (Termination and change of employment)

วัตถุประสงค์ เพื่อให้ยกเลิกหรือเปลี่ยนแปลงสิทธิกับเจ้าหน้าที่ หรือเจ้าหน้าที่จากหน่วยงานภายนอกที่ถูกยกเลิกหรือเปลี่ยนแปลงการจ้างงาน เพื่อรักษาไว้ซึ่งความมั่นคงปลอดภัยสารสนเทศ

นโยบาย

๓.๓.๑ การสิ้นสุดหรือการเปลี่ยนหน้าที่ความรับผิดชอบของการจ้างงาน (Termination or change of employment responsibilities)

๑) หลังจากเปลี่ยนแปลงหรือยกเลิกการจ้างงาน หรือสิ้นสุดโครงการ ต้องยกเลิกสิทธิการเข้าถึงข้อมูลในระบบสารสนเทศทันที

หมวดที่ ๔ การบริหารจัดการสินทรัพย์ (Asset Management)

๔.๑ หน้าที่ความรับผิดชอบต่อสินทรัพย์ (Responsibility for Assets)

วัตถุประสงค์ เพื่อให้ระบุสินทรัพย์ขององค์กรและกำหนดหน้าที่ความรับผิดชอบในการป้องกันสินทรัพย์อย่างเหมาะสม

นโยบาย

๔.๑.๑ บัญชีสินทรัพย์ (Inventory of assets)

๑) ต้องจัดทำและเก็บทะเบียนสินทรัพย์สารสนเทศ เพื่อเป็นข้อมูลสำหรับการนำไปวิเคราะห์และประเมินความเสี่ยง และบริหารจัดการความเสี่ยงได้อย่างเหมาะสม

๒) ต้องตรวจสอบสินทรัพย์ตามระยะเวลาที่กำหนด เช่น ปีละ ๑ ครั้ง หรือ เมื่อมีการเปลี่ยนแปลงที่สำคัญ

๔.๑.๒ ผู้ถือครองสินทรัพย์ (Ownership of assets)

๑) สินทรัพย์ในทะเบียนสินทรัพย์ต้องกำหนดผู้รับผิดชอบให้ชัดเจน

๔.๑.๓ การคืนสินทรัพย์ (Return of assets)

๑) พนักงานที่สิ้นสุดการจ้างงาน หรือสิ้นสุดโครงการต้องคืนสินทรัพย์สารสนเทศที่รับผิดชอบทั้งหมด รวมทั้งกุญแจ บัตรประจำตัวพนักงาน บัตรผ่านเข้าออก คอมพิวเตอร์และอุปกรณ์ต่อพ่วง คู่มือและอุปกรณ์ต่าง ๆ

๔.๒ การจัดชั้นความลับของสารสนเทศ (Information classification)

วัตถุประสงค์ เพื่อให้สินทรัพย์สารสนเทศได้รับการป้องกันที่เหมาะสมโดยสอดคล้องกับระดับความสำคัญของสารสนเทศที่มี

นโยบาย

๔.๒.๑ ชั้นความลับของสารสนเทศ (Classification of information)

๑) ต้องทำการจัดหมวดหมู่สินทรัพย์ กำหนดระดับความสำคัญ และกำหนดชั้นความลับ เพื่อป้องกันสารสนเทศให้มีความปลอดภัย โดยให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความลับของราชการ พ.ศ. ๒๕๔๔

๒) สินทรัพย์สารสนเทศ ซึ่งทำซ้ำมาจากต้นฉบับซึ่งมีการกำหนดชั้นความลับไว้ ให้ถือว่ามีชั้นความลับเดียวกับต้นฉบับ

๔.๒.๒ การบ่งชี้สารสนเทศ (Labeling of information)

๑) ต้องจัดให้มีวิธีการจัดทำ และจัดการป้ายชื่อสินทรัพย์

๔.๒.๓ การจัดการสินทรัพย์ (Handling of assets)

๑) ข้อมูลลับต้องไม่ถูกเปิดเผยกับผู้อื่น เว้นแต่มีความจำเป็นในการปฏิบัติงาน

๒) ข้อมูลที่เป็นข้อมูลลับต้องไม่เปิดเผยต่อบุคคลภายนอก ยกเว้นในกรณีที่การเปิดเผยนั้นครอบคลุมโดยข้อตกลงการไม่เปิดเผยข้อมูล

๓) ข้อมูลสำคัญที่เกี่ยวข้องกับการดำเนินงานขององค์กรทั้งหมด ทั้งที่เก็บรักษาอยู่ในเครื่องคอมพิวเตอร์ของผู้ใช้งานหรือเครื่องคอมพิวเตอร์แม่ข่ายที่ดูแลโดยผู้ใช้งาน ต้องได้รับการสำรองข้อมูลอย่างสม่ำเสมอ เพื่อประโยชน์ในการกู้คืนข้อมูลเมื่อมีปัญหาใด ๆ เกิดขึ้น ตัวอย่างเช่น การติดไวรัส ฮาร์ดดิสก์เสีย เป็นต้น

๔.๓ การจัดการสื่อบันทึกข้อมูล (Media Handling)

วัตถุประสงค์ เพื่อป้องกันการเปิดเผยโดยไม่ได้รับอนุญาต การเปลี่ยนแปลง การขนย้ายการลบ หรือการทำลายสารสนเทศที่จัดเก็บอยู่บนสื่อบันทึกข้อมูล

นโยบาย

๔.๓.๑ การบริหารจัดการสื่อบันทึกข้อมูลที่ถอดแยกได้ (Management of removable media)

๑) สื่อบันทึกข้อมูล และอุปกรณ์คอมพิวเตอร์พกพาต่าง ๆ (เช่น PDA, Thumb- Drive, CD -Rom เป็นต้น) ที่มีข้อมูลลับขององค์กรบันทึกอยู่ ต้องได้รับการดูแลรักษาและใช้งานอย่างระมัดระวัง

๔.๓.๒ การทำลายสื่อบันทึกข้อมูล (Disposal of media)

๑) ข้อมูลลับขององค์กรที่สำเนามาเก็บอยู่บนสื่อบันทึกข้อมูล หากไม่ใช้งานแล้วต้องทำลายให้ไม่สามารถนำข้อมูลไปใช้งานต่อได้ ตามแนวปฏิบัติการทำลายข้อมูลหรือกำจัดสื่อบันทึกข้อมูล

๔.๓.๓ การขนย้ายสื่อบันทึกข้อมูล (Physical media transfer)

๑) หากต้องขนย้ายสื่อบันทึกข้อมูลจะต้องป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต เช่น การล็อกกุญแจ การปิดผนึก การเข้ารหัส เป็นต้น

หมวดที่ ๕ การควบคุมการเข้าถึง (Access Control)

๕.๑ ความต้องการทางธุรกิจสำหรับการควบคุมการเข้าถึง (Business requirements of access control)

วัตถุประสงค์ เพื่อจำกัดการเข้าถึงสารสนเทศ และอุปกรณ์ประมวลผลสารสนเทศเฉพาะผู้ที่ได้รับอนุญาต

นโยบาย

๕.๑.๑ นโยบายควบคุมการเข้าถึง (Access control policy)

๑) กำหนดนโยบายควบคุมการเข้าถึง เป็นการกำหนดมาตรฐานแนวทางปฏิบัติที่มีความสอดคล้องกับนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศสำหรับผู้ใช้งาน เจ้าหน้าที่ รวมถึงบุคคลภายนอกเพื่อควบคุมให้เข้าถึงเฉพาะผู้ที่ได้รับอนุญาต โดยมีมาตรการควบคุมการเข้าถึง ตามแนวปฏิบัติดังต่อไปนี้

๑) แนวปฏิบัติในการควบคุมการเข้าถึงสารสนเทศ

๒) แนวปฏิบัติการควบคุมการเข้าถึงเครือข่ายและบริการเครือข่าย

๓) แนวปฏิบัติการควบคุมการเข้าถึงระบบปฏิบัติการ

๔) แนวปฏิบัติการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ

๕.๑.๒ การเข้าถึงเครือข่ายและบริการเครือข่าย (Access to networks and network services)

๑) กำหนดการป้องกันทางเครือข่ายให้มีความมั่นคงปลอดภัย ตามแนวปฏิบัติการควบคุมการเข้าถึงเครือข่ายและบริการเครือข่าย

๕.๒ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User access management)

วัตถุประสงค์ เพื่อป้องกันไม่ให้ผู้ที่ไม่มีสิทธิใช้งานสามารถเข้าถึงระบบสารสนเทศได้ เช่น เขียน app โดยป้องกัน ip , mac address , decaptcha

นโยบาย

๕.๒.๑ การลงทะเบียนและการถอดถอนสิทธิผู้ใช้งาน (User registration and de-registration)

๑) การลงทะเบียนผู้ใช้งานใหม่ ต้องกำหนดให้มีระเบียบปฏิบัติอย่างเป็นทางการเพื่อให้สามารถใช้งานระบบสารสนเทศ และระบบเครือข่ายคอมพิวเตอร์ ในกรณีที่ผู้ใช้งานสิ้นสุดสถานภาพต้องยกเลิกออกจากระบบทันทีตาม แนวปฏิบัติการจัดการการเข้าถึงของผู้ใช้งาน

๕.๒.๒ การจัดการสิทธิการเข้าถึงของผู้ใช้งาน (User access Provisioning)

๑) ผู้ดูแลระบบต้องมีกระบวนการกำหนดสิทธิให้ครอบคลุมผู้ใช้งานให้ครบทุกประเภทและทุกบริการ

๕.๒.๓ การบริหารจัดการสิทธิการเข้าถึงตามระดับสิทธิ (Management of privileged access right)

๑) ผู้ดูแลระบบต้องกำหนดสิทธิผู้ใช้งานในการเข้าถึงระบบสารสนเทศแต่ละระบบ รวมทั้งกำหนดสิทธิแยกตามหน้าที่รับผิดชอบด้วย โดยให้เป็นไปตามแนวปฏิบัติการจัดการการเข้าถึงของผู้ใช้งาน

๕.๒.๔ การบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้งาน (Management of privileged access right)

๑) การส่งมอบข้อมูลการพิสูจน์ตัวตนซึ่งเป็นข้อมูลลับ ดังนั้นต้องมีกระบวนการป้องกันและการปกปิด โดยให้เป็นไปตามแนวปฏิบัติการจัดการการเข้าถึงของผู้ใช้งาน

๕.๒.๕ การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of user access rights)

๑) ผู้ดูแลระบบต้องทบทวนสิทธิในการเข้าถึงระบบสารสนเทศอย่างสม่ำเสมอ

๕.๒.๖ การถอดถอนหรือปรับปรุงสิทธิการเข้าถึง (Removal or adjustment of access rights)

๑) เมื่อเจ้าหน้าที่ลาออก เปลี่ยนแปลงข้อตกลงหรือหรือสัญญา ผู้ดูแลระบบต้องทำการถอดถอนหรือปรับปรุงสิทธิให้ถูกต้อง

๕.๓ หน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities)

วัตถุประสงค์ เพื่อให้ผู้ใช้งานมีความรับผิดชอบในการป้องกันข้อมูลการพิสูจน์ตัวตน

นโยบาย

๕.๓.๑ การใช้ข้อมูลการพิสูจน์ตัวตนซึ่งเป็นข้อมูลลับ (Use of secret authentication information)

๑) ผู้ใช้งานต้องปฏิบัติตามการควบคุมการเข้าถึงสารสนเทศองค์กร การกำหนด การเปลี่ยนแปลงและการยกเลิกรหัสผ่าน และการจัดการควบคุมการใช้รหัสผ่านตามแนวปฏิบัติการใช้งานสารสนเทศให้มั่นคงปลอดภัย หัวข้อ การใช้งานรหัสผ่าน

๒) รหัสผ่านถือเป็นข้อมูลลับ และเป็นหน้าที่ของผู้ใช้งานทุกคนที่ต้องเก็บรักษารหัสผ่านอย่างมั่นคงปลอดภัย

๓) ผู้ใช้งานต้องรับผิดชอบต่อการกระทำใด ๆ ที่กระทำผ่านบัญชีผู้ใช้งานและรหัสผ่านของตนทั้งหมด

๔) รหัสผ่านต้องได้รับการเปลี่ยนเมื่อเข้าใช้งานครั้งแรก และเปลี่ยนอย่างสม่ำเสมอตามช่วงระยะเวลาที่กำหนดไว้

๕.๔ การควบคุมการเข้าถึงระบบ (System and application access control)

วัตถุประสงค์ เพื่อป้องกันการเข้าถึงระบบสารสนเทศและข้อมูลบนระบบสารสนเทศโดยไม่ได้รับอนุญาต

นโยบาย

๕.๔.๑ การจำกัดการเข้าถึงสารสนเทศ (Information access restriction)

๑) ต้องควบคุมการใช้งานสารสนเทศในระบบสารสนเทศ ได้แก่ กำหนดสิทธิในการใช้งาน ได้แก่ เขียน อ่าน ลบ ได้ เป็นต้น กำหนดกลุ่มของผู้ใช้งาน ที่สามารถใช้งานได้ ตรวจสอบว่า สารสนเทศที่อนุญาตให้ใช้งานนั้นมี เฉพาะข้อมูลที่จำเป็นต้องใช้งาน โดยให้เป็นไปตามแนวปฏิบัติการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ

๒) บัญชีผู้ใช้งานที่มีสิทธิการเข้าถึงระบบสารสนเทศในระดับพิเศษ เช่น Root หรือ Administrator ต้องได้รับการพิจารณามอบหมายให้แก่ผู้ใช้งานตามความจำเป็น และกำหนดระยะเวลาในการเข้าถึงอย่างเหมาะสมกับการทำงานเท่านั้น

๓) บุคคลภายนอก ต้องแสดงความยินยอมปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างเคร่งครัด ก่อนที่จะได้รับอนุญาตให้เข้าถึงระบบสารสนเทศ ตามแนวปฏิบัติการควบคุมหน่วยงานภายนอกเข้าถึงระบบสารสนเทศ

๕.๔.๒ ขั้นตอนปฏิบัติสำหรับการล็อกอินเข้าระบบที่มีความมั่นคงปลอดภัย (Secure log-on procedures)

๑) การเข้าถึงระบบปฏิบัติการจะต้องผ่านการล็อกอินเข้าระบบที่มีความมั่นคงปลอดภัยตาม แนวปฏิบัติการควบคุมการเข้าถึงระบบปฏิบัติการ

๕.๔.๓ การใช้โปรแกรมอรรถประโยชน์ (Use of privileged utility programs)

๑) ต้องกำหนดให้ควบคุมการใช้โปรแกรมยูทิลิตี้สำหรับระบบ เพื่อป้องกันการเข้าถึงโดยผู้ที่ไม่ได้รับอนุญาต ได้แก่

(๑) ก่อนใช้ต้องทำการพิสูจน์ตัวตนก่อน

(๒) ให้ทำการแยกโปรแกรมยูทิลิตี้ออกจากโปรแกรมระบบงาน

(๓) จำกัดการใช้งานโปรแกรมยูทิลิตี้ให้เฉพาะผู้ที่ได้รับมอบหมายแล้วเท่านั้น

(๔) ให้บันทึกรายละเอียดการเข้าใช้งานโปรแกรมยูทิลิตี้

๕.๔.๔ การควบคุมการเข้าถึงซอร์สโค้ดของโปรแกรม (Access control to program source code)

๑) อนุญาตเฉพาะผู้รับผิดชอบสามารถเข้าถึงซอร์สโค้ดของโปรแกรม

หมวดที่ ๖ ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and environmental Security)

๖.๑ พื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัย (Secure areas)

วัตถุประสงค์ เพื่อป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต ความเสียหาย และการแทรกแซงการทำงาน ที่มีต่อระบบสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศขององค์กร

นโยบาย

๖.๑.๑ ขอบเขตหรือบริเวณโดยรอบทางกายภาพ (Physical security perimeter)

๑) ต้องแบ่งพื้นที่อย่างชัดเจน และกำหนดระดับการควบคุมเพื่อป้องกันการเข้าถึงสินทรัพย์สารสนเทศที่มีความสำคัญ
๒) ต้องจัดทำแผนผังแสดงตำแหน่งและพื้นที่แต่ละชนิดและประกาศให้ผู้เกี่ยวข้องทราบ
๓) ต้องดูแลรักษาสภาพแวดล้อมของพื้นที่ให้เป็นไปตาม แนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางกายภาพห้องควบคุมระบบ

๖.๑.๒ การควบคุมการเข้าออกทางกายภาพ (Physical entry controls)

๑) ต้องควบคุมให้เฉพาะผู้ที่มีสิทธิ หรือผู้ที่ได้รับอนุญาตสามารถเข้าออกในพื้นที่
๒) ต้องกำหนดสิทธิ และช่วงเวลาในการผ่านเข้าออกพื้นที่
๓) ต้องบันทึกการผ่านเข้าออกในพื้นที่ที่สำคัญ
๔) ต้องไม่เปิดประตูสำนักงานทิ้งไว้ หรือยินยอมให้บุคคลอื่นติดตามเข้าภายในพื้นที่สำนักงานโดยเด็ดขาด เว้นแต่บุคคลอื่นนั้นสามารถแสดงบัตรประจำตัว หรือบัตรผู้มาติดต่อได้ เพื่อเป็นการป้องกันการเข้าถึงพื้นที่สำนักงาน และพื้นที่ควบคุมความมั่นคงปลอดภัยโดยบุคคลที่ไม่ได้รับอนุญาต

๖.๑.๓ การรักษาความมั่นคงปลอดภัยสำหรับสำนักงาน ห้องทำงาน และอุปกรณ์ (Securing office, room and facilities)

๑) ต้องจัดให้มีมาตรการในการรักษาความมั่นคงปลอดภัยอื่นๆ ให้กับสำนักงาน ห้องทำงานและเครื่องมือต่างๆ เช่น เครื่องคอมพิวเตอร์หรือระบบที่มีความสำคัญสูงต้องไม่ตั้งอยู่ในบริเวณที่มีการผ่านเข้าออกของบุคคลเป็นจำนวนมาก
๒) เจ้าหน้าที่ควรตรวจสอบความมั่นคงปลอดภัยของพื้นที่ทำงานของตนเป็นประจำทุกวันหลังเลิกงาน เพื่อให้มั่นใจว่าตู้เซฟ ตู้เอกสาร ลิ้นชัก และอุปกรณ์ต่างๆ ได้รับการปิดล็อค อย่างเหมาะสม และกุญแจถูกเก็บรักษาไว้อย่างปลอดภัย
๓) ข้อมูล สื่อบันทึก วัสดุ และอุปกรณ์ที่จัดเก็บข้อมูลลับต้องไม่ถูกทิ้งไว้โดยลำพังบนโต๊ะทำงาน ในห้องประชุม หรือในตู้ที่ไม่ได้ล็อคกุญแจโดยเด็ดขาด
๔) ข้อมูล สื่อบันทึก วัสดุ และอุปกรณ์ที่จัดเก็บข้อมูลลับต้องไม่ถูกทิ้งลงในถังขยะโดยไม่ได้รับการทำลายอย่างเหมาะสม โดยให้เป็นไปตามแนวปฏิบัติการทำลายข้อมูลหรือกำจัดสื่อบันทึกข้อมูล
๕) เจ้าหน้าที่ต้องไม่ยินยอมให้ผู้ใดทำการเคลื่อนย้ายเครื่องคอมพิวเตอร์หรือสื่อบันทึกข้อมูลออกจากพื้นที่ทำงานของตนโดยเด็ดขาด เว้นแต่ บุคคลผู้นั้นเป็นเจ้าหน้าที่ ที่ได้รับอนุญาตให้ดำเนินการ และเป็นการดำเนินการที่มีคำสั่งอย่างถูกต้องของหน่วยงานเท่านั้น

๖.๑.๔ การป้องกันต่อภัยคุกคามจากภายนอกและสภาพแวดล้อม (Protecting against external end environmental threats)

๑) ต้องมีวิธีป้องกันจากการทำลายของธรรมชาติหรือคนที่อาจจะเกิดขึ้น

๖.๑.๕ การปฏิบัติงานในพื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัย (Working in secure areas)

๑) หากพบสิ่งผิดปรกติ หรือการละเมิดความมั่นคงปลอดภัย จะต้องแจ้งให้ผู้บังคับบัญชาทราบ
๒) ในบริเวณที่ต้องการรักษาความมั่นคงปลอดภัยต้องติดประกาศแจ้งเตือน เช่น ”ห้ามเข้าก่อนได้รับอนุญาต”

๖.๑.๖ พื้นที่สำหรับรับส่งของสิ่งของ (Delivery and loading areas)

๑) ต้องแยกจุดที่รับส่งสิ่งของ ออกจากพื้นที่ที่มีอุปกรณ์ประมวลผลสารสนเทศ และดำเนินการแกะหีบห่อหรือตรวจสอบให้เสร็จสิ้น ก่อนนำเข้าสู่พื้นที่ที่ต้องการรักษาความมั่นคงปลอดภัย

๖.๒ อุปกรณ์ (Equipment)

วัตถุประสงค์ เพื่อป้องกันการสูญหาย การเสียหาย การขโมย หรือการเป็นอันตรายต่อสินทรัพย์และป้องกันการหยุดชะงักต่อการดำเนินงานขององค์กร

นโยบาย

๖.๒.๑ การจัดตั้งและป้องกันอุปกรณ์ (Equipment setting and protection)

๑) การจัดตั้ง หรือการจัดวางอุปกรณ์สินทรัพย์สารสนเทศ อุปกรณ์ใดที่มีความสำคัญสูงต้องจัดวางในที่ที่เข้าถึงได้ยาก

๖.๒.๒ ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting utilities)

๑) อุปกรณ์ที่มีความสำคัญสูงควรติดตั้งระบบป้องกันความล้มเหลวของอุปกรณ์ เช่น ระบบสำรองไฟฟ้า ระบบปรับอากาศ เป็นต้น

๖.๒.๓ ความมั่นคงปลอดภัยของการเดินสายสัญญาณและสายสื่อสาร (Cabling security)

๑) การเดินสายสัญญาณต้องแยกท่อเพื่อป้องกันสัญญาณรบกวนตามข้อกำหนดการเดินสายสัญญาณเครือข่าย

๒) ต้องมีการทำป้ายสายสัญญาณชัดเจน และเมื่อมีการเปลี่ยนแปลงต้องมีการปรับปรุงป้ายสายสัญญาณให้ถูกต้อง

๖.๒.๔ การบำรุงรักษาอุปกรณ์ (Equipment maintenance)

๑) ต้องจัดให้มีการบำรุงรักษาอุปกรณ์เพื่อให้มีสภาพพร้อมใช้งานอย่างน้อยปีละ ๑ ครั้ง หรือมากกว่าตามระดับความสำคัญ

๖.๒.๕ การนำสินทรัพย์ขององค์กรออกนอกสำนักงาน (Removal of assets)

๑) ห้ามนำสินทรัพย์สารสนเทศออกนอกพื้นที่ก่อนได้รับอนุญาตจากผู้รับผิดชอบ และต้องมีขั้นตอนในการตรวจสอบและติดตามโดยให้เป็นไปตามแนวปฏิบัติการนำทรัพย์สินสารสนเทศออกนอกพื้นที่

๖.๒.๖ ความมั่นคงปลอดภัยของอุปกรณ์และสินทรัพย์ที่ใช้งานอยู่ภายนอกสำนักงาน (Security of equipment and assets off- premises)

๑) สินทรัพย์ที่ใช้งานอยู่ภายนอกสำนักงานต้องมีการรักษาความมั่นคงปลอดภัยตามความเสี่ยง

๖.๒.๗ ความมั่นคงปลอดภัยสำหรับการกำจัดหรือทำลายอุปกรณ์ หรือการนำอุปกรณ์ไปใช้งานอย่างอื่น (Secure disposal or re-use of equipment)

๑) ข้อมูลที่เก็บอยู่บนสื่อบันทึกข้อมูล หากไม่มีการใช้งานแล้วต้องทำลายไม่ให้สามารถนำข้อมูลไปใช้งานต่อได้ โดยให้เป็นไปตามแนวปฏิบัติการทำลายข้อมูลหรือกำจัดสื่อบันทึกข้อมูล

๖.๒.๘ อุปกรณ์ของผู้ใช้งานที่ทิ้งไว้โดยไม่มีผู้ดูแล (Unattended user equipment)

๑) ต้องป้องกันให้ผู้ไม่มีสิทธิเข้าถึงอุปกรณ์สินทรัพย์สารสนเทศที่ไม่มีผู้ดูแล

๖.๒.๙ การควบคุมการไม่ทิ้งสินทรัพย์สารสนเทศที่สำคัญไว้ในที่ไม่ปลอดภัย (Clear desk and clear screen policy)

๑) เจ้าหน้าที่ต้องควบคุมเอกสาร ข้อมูล หรือสื่อต่างๆ ที่มีข้อมูลสำคัญจัดเก็บ หรือบันทึกอยู่ ไม่ให้วางทิ้งไว้บนโต๊ะทำงานหรือในสถานที่ไม่ปลอดภัยในขณะไม่ได้นำมาใช้งาน ตลอดจนการควบคุมหน้าจอ

คอมพิวเตอร์ (Desktop) ไม่ให้มีข้อมูลสำคัญปรากฏในขณะไม่ได้ใช้งาน โดยให้เป็นไปตามแนวปฏิบัติการใช้งานสารสนเทศให้มั่นคงปลอดภัย

หมวดที่ ๗ ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operations Security)

8.๑ ขั้นตอนการปฏิบัติงานและหน้าที่ความรับผิดชอบ (Operational Procedures and Responsibilities)

วัตถุประสงค์ เพื่อให้การปฏิบัติงานกับอุปกรณ์ประมวลผลสารสนเทศเป็นไปอย่างถูกต้องและมั่นคงปลอดภัย

นโยบาย

8.1.1 ขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษร (Documented operating procedures)

1) ต้องจัดทำคู่มือหรือขั้นตอนปฏิบัติงานที่เกี่ยวกับสารสนเทศที่สำคัญของหน่วยงาน เพื่อป้องกันการปฏิบัติงานด้านสารสนเทศที่ผิดพลาด

8.1.2 การบริหารจัดการการเปลี่ยนแปลง (Change management)

1) กำหนดให้มีการควบคุมการเปลี่ยนแปลงสารสนเทศ เช่น ต้องมีการขออนุมัติจากผู้บังคับบัญชาก่อนดำเนินการ
2) ต้องมีการสำรองข้อมูลสารสนเทศก่อนการเปลี่ยนแปลงสารสนเทศ

8.1.3 การบริหารจัดการขีดความสามารถของระบบ (Capacity management)

1) ควรติดตั้งระบบเพื่อตรวจสอบติดตามทรัพยากรของระบบ เช่น CPU Memory Harddisk ว่าเพียงพอหรือไม่ และนำข้อมูลการตรวจสอบติดตามมาวางแผนการเพิ่มหรือลดทรัพยากรในอนาคต

8.1.4 การแยกสภาพแวดล้อมสำหรับการพัฒนา การทดสอบ และการให้บริการออกจากกัน (Separation of development, testing and operational environments)

1) ในระบบที่มีความสำคัญสูงควรแยกระบบการพัฒนา ออกจากระบบการให้บริการจริง เพื่อป้องกันการเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต

8.๒ การป้องกันโปรแกรมไม่ประสงค์ดี (Protection from Malware)

วัตถุประสงค์ เพื่อให้สารสนเทศและอุปกรณ์ประมวลผลสารสนเทศได้รับการป้องกันจากโปรแกรมไม่ประสงค์ดี

นโยบาย

8.2.1 มาตรการป้องกันโปรแกรมไม่ประสงค์ดี (Controls against malware)

1) เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา ก่อนเชื่อมต่ออินเทอร์เน็ตผ่านเว็บเบราเซอร์ (Web browser) ต้องติดตั้งโปรแกรมป้องกันไวรัสและอุดช่องโหว่ของระบบปฏิบัติการและเว็บเบราเซอร์
2) ผู้ใช้ต้องปรับปรุง Patch และ HotFix อย่างสม่ำเสมอ โดยสามารถดาวน์โหลด Patch และ HotFix ต่างๆ จากเว็บไซต์เจ้าของผลิตภัณฑ์เพื่อแก้ปัญหาช่องโหว่ เป็นต้น
3) ในการรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเทอร์เน็ตจะต้องทดสอบไวรัส (Virus Scanning) โดยโปรแกรมป้องกันไวรัสก่อนการรับส่งข้อมูลทุกครั้ง

8.๓ การสำรองข้อมูล (Backup)

วัตถุประสงค์ เพื่อป้องกันการสูญหายของข้อมูล และให้มั่นใจว่าระบบสารสนเทศอยู่ในสภาพพร้อมใช้งาน

นโยบาย

8.3.1 นโยบายการสำรองและกู้คืนข้อมูล (Information backup and recovery policy)

(๑) หน่วยงานที่มีเครื่องคอมพิวเตอร์แม่ข่ายให้บริการให้ดำเนินการสำรองข้อมูลตามแนวปฏิบัติการสำรองและการกู้คืนข้อมูล

(๒) ต้องสำรวจข้อมูล และจัดระดับความสำคัญ กำหนดข้อมูลที่ต้องการสำรอง และความถี่ในการสำรองข้อมูล

(๓) ข้อมูลที่มีความสำคัญสูงต้องจัดให้มีความถี่การสำรองมาก และควรจัดให้มีการสำรองข้อมูลภายนอกสำนักงาน

(๔) ต้องมีการควบคุมการเข้าถึงทางกายภาพ (Physical Access Control) ของสถานที่ที่เก็บข้อมูลสำรอง สื่อเก็บข้อมูลต้องได้รับการป้องกันสอดคล้องกับระดับความสำคัญของระบบสารสนเทศ

(๕) ต้องทดสอบข้อมูลที่สำรองอย่างสม่ำเสมอ

(๖) ต้องทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง อย่างน้อยปีละ ๑ ครั้ง

(๗) หากต้องมีการกู้คืนข้อมูลให้ดำเนินการกู้คืนข้อมูลตามแนวปฏิบัติการสำรองและการกู้คืนข้อมูล

8.๔ การบันทึกข้อมูลล็อกและการเฝ้าระวัง (Logging and Monitoring)

วัตถุประสงค์ เพื่อให้มีการบันทึกเหตุการณ์และจัดทำหลักฐาน

นโยบาย

8.4.1 การบันทึกข้อมูลล็อกแสดงเหตุการณ์ (Event logging)

1) อุปกรณ์ประมวลผลระบบสารสนเทศต้องมีการจัดเก็บข้อมูลล็อกและบันทึกกิจกรรมของผู้ใช้งาน เพื่อใช้ติดตามกรณีเกิดเหตุความมั่นคงปลอดภัย

8.4.2 การป้องกันข้อมูลล็อก (Protection of log information)

1) อุปกรณ์บันทึกล็อกและข้อมูลการล็อกสามารถเข้าถึงได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น

8.4.3 ข้อมูลล็อกกิจกรรมของผู้ดูแลระบบและเจ้าหน้าที่ปฏิบัติการระบบ (Administrator and operator logs)

1) ต้องมีการบันทึกกิจกรรมการดำเนินงานของผู้ดูแลระบบ และมีการทบทวนอยู่เสมอ

8.4.4 การตั้งนาฬิกาให้ถูกต้อง (Clock Synchronization)

1) เครื่องคอมพิวเตอร์แม่ข่ายทุกเครื่องต้องตั้งเวลาให้ตรงกันโดยเทียบเวลาจากเซิร์ฟเวอร์ประสานจังหวะเวลาโดยกรมอุทกศาสตร์ กองทัพเรือ

8.๕ การควบคุมการติดตั้งซอฟต์แวร์บนระบบให้บริการ (Control of operational software)

วัตถุประสงค์ เพื่อให้ระบบให้บริการมีการทำงานที่ถูกต้อง

นโยบาย

8.5.1 การติดตั้งซอฟต์แวร์บนระบบให้บริการ (Installation of software on operational systems)

1) ต้องติดตั้งเฉพาะที่ซอฟต์แวร์ที่จำเป็นในการให้บริการเท่านั้น

8.๖ การบริหารจัดการช่องโหว่ทางเทคนิค (Technical Vulnerability Management)

วัตถุประสงค์ เพื่อป้องกันการใช้ประโยชน์จากช่องโหว่ทางเทคนิค

นโยบาย

8.6.1 การจำกัดการติดตั้งซอฟต์แวร์บนระบบให้บริการ (Restrictions on software installation)

1) ระบบที่ให้บริการต้องทำการ Patch ซอฟต์แวร์อย่างสม่ำเสมอ
2) ต้องทำการลบ User ที่ไม่จำเป็นออกจากระบบ เช่น Test
3) ต้องปิด Service ที่ไม่ได้ใช้งาน
4) ซอฟต์แวร์ใดไม่ได้ใช้งานต้องลบออก

8.6.2 การบริหารจัดการช่องโหว่ทางเทคนิค (Management of technical vulnerabilities)

1) ต้องติดตามข้อมูลทางด้านเทคนิคของช่องโหว่อย่างสม่ำเสมอ

หมวดที่ ๘ ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications security)

๘.๑ การบริหารจัดการความมั่นคงปลอดภัยของเครือข่าย (Network Security Management)

วัตถุประสงค์ เพื่อให้มีการป้องกันสารสนเทศในเครือข่าย และอุปกรณ์ประมวลผลสารสนเทศ

นโยบาย

๘.๑.๑ มาตรการเครือข่าย (Network controls)

๑) กำหนดนโยบายการควบคุมการเข้าถึงเครือข่าย และบริการเครือข่ายให้มีความมั่นคงปลอดภัยโดยให้เป็นไปตามแนวปฏิบัติการควบคุมการเข้าถึงเครือข่ายและบริการเครือข่าย

๘.๑.๒ ความมั่นคงปลอดภัยสำหรับบริการเครือข่าย (Security of network services)

๑) ผู้บริหารต้องมีการกำหนดระดับความต้องการสำหรับบริการเครือข่าย

๘.๑.๓ การแบ่งแยกเครือข่าย (Segregation in networks)

๑) ผู้ดูแลระบบต้องจัดแบ่งเครือข่ายระหว่างการใช้งานภายในและผู้ใช้ภายนอกโดยพิจารณาจากบริการเครือข่าย ระบบสารสนเทศ กลุ่มของผู้ใช้งานของทั้งสองฝ่าย

๘.๒ การถ่ายโอนสารสนเทศ (Information transfer)

วัตถุประสงค์ เพื่อให้มีการรักษาความมั่นคงปลอดภัยของสารสนเทศที่มีการถ่ายโอนภายในองค์กรและถ่ายโอนกับหน่วยงานภายนอก

นโยบาย

๘.๒.๑ นโยบายและขั้นตอนปฏิบัติสำหรับการถ่ายโอนสารสนเทศ (Information transfer policies and procedures)

๑) การใช้บริการสารสนเทศจากหน่วยงานภายนอก ให้เป็นไปตามแนวปฏิบัติการควบคุมหน่วยงานภายนอกเข้าถึงระบบสารสนเทศ

๘.๒.๒ ข้อตกลงสำหรับการถ่ายโอนสารสนเทศ (Agreements on information transfer)

๑) การทำข้อตกลงต้องคำนึงถึงความมั่นคงปลอดภัยสารสนเทศ และผู้ดูแลระบบต้องควบคุมการปฏิบัติงานนั้น ๆ ให้มีความปลอดภัยทั้ง ๓ ด้าน คือ การรักษาความลับ (Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)

หมวดที่ ๙ การจัดหา การพัฒนา และการบำรุงรักษาระบบ (System acquisition, development and maintenance)

๙.๑ ความต้องการด้านความมั่นคงปลอดภัยของระบบ (Security requirements of information systems)

วัตถุประสงค์ เพื่อให้ความมั่นคงปลอดภัยสารสนเทศเป็นองค์ประกอบสำคัญหนึ่งของระบบตลอดวงจรของการพัฒนาระบบ ซึ่งรวมถึงความต้องการด้านระบบที่มีการให้บริการผ่านเครือข่ายสาธารณะด้วย

นโยบาย

๙.๑.๑ การวิเคราะห์และกำหนดความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ (Information security requirements analysis and specification)

๑) ต้องกำหนดความต้องการด้านความมั่นคงปลอดภัยก่อนจะพัฒนาขึ้นมาใช้งานหรือซื้อมาใช้งาน

๙.๑.๒ ความมั่นคงปลอดภัยของบริการสารสนเทศบนเครือข่ายสาธารณะ (Securing application services on public networks)

๑) สารสนเทศที่เกี่ยวข้องกับบริการสารสนเทศซึ่งมีการส่งผ่านเครือข่ายสาธารณะต้องได้รับการป้องกันจากการฉ้อโกง การโต้เถียง การเปิดเผยและการเปลี่ยนแปลงสารสนเทศโดยไม่ได้รับอนุญาต

๙.๒ ความมั่นคงปลอดภัยสำหรับกระบวนการพัฒนาและสนับสนุน (Security in development and support processes)

วัตถุประสงค์ เพื่อให้ความมั่นคงปลอดภัยสารสนเทศมีการออกแบบและดำเนินการตลอดวงจรชีวิตของการพัฒนาระบบ

นโยบาย

๙.๒.๑ นโยบายการพัฒนาระบบให้มีความมั่นคงปลอดภัย (Secure development policy)

๑) ผู้พัฒนาระบบสารสนเทศต้องมีกระบวนการเพื่อควบคุมการเปลี่ยนแปลงแก้ไขซอฟต์แวร์สำหรับระบบสารสนเทศที่ใช้งานจริง

๙.๒.๒ ขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงระบบ (System change control procedures)

๑) ผู้พัฒนาระบบสารสนเทศต้องจัดทำแนวปฏิบัติการควบคุมการเปลี่ยนแปลงระบบสารสนเทศ

๙.๒.๓ การทบทวนทางเทคนิคต่อระบบหลังจากเปลี่ยนแปลงโครงสร้างพื้นฐานของระบบ (Technical review of applications after operating platform changes)

๑) เมื่อระบบปฏิบัติการมีการแก้ไขหรือเปลี่ยนแปลงซอฟต์แวร์ต่างๆ ผู้พัฒนาระบบสารสนเทศจะต้องตรวจสอบและทดสอบว่าไม่มีผลกระทบต่อการทำงานและความมั่นคงปลอดภัย

๙.๒.๔ การจำกัดการเปลี่ยนแปลงซอฟต์แวร์สำเร็จรูป (Restrictions on changes to software packages)

๑) เมื่อมีการใช้งานซอฟต์แวร์สำเร็จรูปต้องมีการควบคุมการเปลี่ยนแปลงเท่าที่จำเป็น และการเปลี่ยนแปลงทั้งหมดจะต้องถูกทดสอบและจัดทำเป็นเอกสารเพื่อให้สามารถนำมาใช้งานได้เมื่อมีการปรับปรุงซอฟต์แวร์ในอนาคต

๙.๒.๕ หลักการวิศวะกรรมระบบด้านความมั่นคงปลอดภัย (Secure system engineering principles)

๑) ควรนำหลักการวิศวกรรมระบบมาประยุกต์ใช้กับงานการพัฒนาระบบ เช่น

(๑) ควรนำระบบงานที่สำคัญไปอยู่หลัง Firewall

(๒) ปิดช่องโหว่ของระบบให้เหลือน้อยที่สุด

๙.๒.๖ สภาพแวดล้อมของการพัฒนาระบบที่มีความมั่นคง (Secure development environment)

๑) หากมีความจำเป็นต้องให้หน่วยงานภายนอกเข้ามาพัฒนาระบบภายในหน่วยงาน ต้องกำหนดสภาพแวดล้อมที่มีความมั่นคงปลอดภัย เช่น ตัดการเชื่อมต่อเครือข่ายออกสู่ภายนอกเพื่อป้องกันการนำข้อมูลลับออกสู่ภายนอก

๒) มีการแบ่งสิทธิตามหน้าที่การทำงานอย่างชัดเจน เช่น ผู้พัฒนาระบบ ผู้ดูแลฐานข้อมูล

๓) ต้องตรวจสอบประวัติของหน่วยงานภายนอกที่มารับจ้าง

๔) หน่วยงานภายนอกต้องปฏิบัติตามนโยบายความมั่นคงปลอดภัยของหน่วยงาน

๙.๒.๗ การจ้างหน่วยงานภายนอกพัฒนาระบบ (Outsourced development)

๑) ต้องมีการประชุมติดตาม และบันทึกการประชุมกิจกรรมการพัฒนาระบบอย่างสม่ำเสมอ

๒) หากพบการละเมิดความมั่นคงปลอดภัยต้องแจ้งให้ผู้บังคับบัญชาทราบ

๙.๒.๘ การทดสอบด้านความมั่นคงปลอดภัยของระบบ (System security testing)

๑) การทดสอบด้านความมั่นคงปลอดภัยต้องทำการทดสอบการใช้งานในช่วงของการพัฒนา หากไม่ผ่านการทดสอบต้องแก้ไขให้แล้วเสร็จก่อนการส่งมอบ

๙.๒.๙ การทดสอบเพื่อรับรองระบบ (System acceptance testing)

๑) การทำงานของฟังก์ชันทุกฟังก์ชันการทำงาน ต้องทำงานถูกต้อง และสามารถทำงานได้

๙.๓ ข้อมูลสำหรับการทดสอบ (Test data)

วัตถุประสงค์ เพื่อให้มีการป้องกันข้อมูลที่นำมาใช้ในการทดสอบระบบสารสนเทศ

นโยบาย

๙.๓.๑ การป้องกันข้อมูลสำหรับการทดสอบ

๑) ข้อมูลจริงที่จะนำไปใช้ในการทดสอบระบบจะต้องได้รับอนุญาตจากผู้รับผิดชอบในการรักษาข้อมูลและเจ้าของข้อมูลนั้นๆ ก่อน เมื่อใช้งานเสร็จจะต้องทำการลบข้อมูลจริงออกจากระบบทดสอบทันทีและทำการบันทึกไว้เป็นหลักฐานว่า ได้นำข้อมูลจริงไปใช้ในการทดสอบอะไรบ้าง รวมถึงวัน เวลา และหน่วยงานที่ทดสอบ

หมวด ๑๐ ความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier relationships)

๑๐.๑ ความมั่นคงปลอดภัยสารสนเทศกับความสัมพันธ์กับผู้ให้บริการภายนอก (Information security in supplier relationship)

วัตถุประสงค์ เพื่อให้มีการป้องกันสินทรัพย์ขององค์กรที่มีการเข้าถึงโดยผู้ให้บริการภายนอก

นโยบาย

๑๐.๑.๑ นโยบายความมั่นคงปลอดภัยสารสนเทศด้านความสัมพันธ์กับผู้ให้บริการภายนอก (Information security policy for supplier relationships)

๑) ต้องจัดทำข้อกำหนดทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร เมื่อมีความจำเป็นต้องให้ผู้ใช้บริการเข้าถึงสารสนเทศหรือสินทรัพย์สารสนเทศขององค์กร

๑๐.๑.๒ การระบุความมั่นคงปลอดภัยในข้อตกลงการให้บริการของผู้ให้บริการภายนอก (Addressing security within supplier agreements)

๑) ต้องระบุและบังคับใช้ข้อกำหนดทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร เมื่อมีความจำเป็นต้องให้ผู้ใช้งานเข้าถึงสารสนเทศหรือสินทรัพย์สารสนเทศขององค์กร ก่อนที่ จะอนุญาตให้สามารถเข้าถึงได้

๑๐.๑.๓ ห่วงโซ่การให้บริการเทคโนโลยีสารสนเทศและการสื่อสารโดยผู้ให้บริการภายนอก (Information and communication technology supply chain)

๑) ข้อกำหนดทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร ต้องสื่อสารถึงห่วงโซ่ผู้ให้บริการภายนอกทั้งหมดที่เข้าถึงสารสนเทศหรือสินทรัพย์สารสนเทศขององค์กร

๑๐.๒ การบริหารจัดการการให้บริการโดยผู้ให้บริการภายนอก (Supplier service delivery management)

วัตถุประสงค์ เพื่อให้มีการรักษาไว้ซึ่งระดับความมั่นคงปลอดภัยและระดับการให้บริการตามที่ตกลงกันไว้ในข้อตกลงการให้บริการของผู้ให้บริการภายนอก

นโยบาย

๑๐.๒.๑ การติดตามและทบทวนบริการของผู้ให้บริการภายนอก (Monitoring and review of supplier services)

๑) ในข้อตกลงการให้บริการ ต้องกำหนดให้มีการติดตาม ทบทวน และตรวจประเมินการให้บริการภายนอกอย่างสม่ำเสมอ

๑๐.๒.๒ การบริหารจัดการการเปลี่ยนแปลงบริการของผู้ให้บริการภายนอก (Managing changes to supplier services)

๑) หากมีการเปลี่ยนแปลงข้อตกลงการให้บริการสำหรับระบบที่สำคัญ จะต้องจัดทำการประเมินความเสี่ยงด้านความมั่นคงปลอดภัย

หมวด ๑๑ การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management)

๑๑.๑ การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management)

วัตถุประสงค์ เพื่อให้มีวิธีการที่สอดคล้องกันและได้ผลสำหรับการบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ ซึ่งรวมถึงการแจ้งสถานการณ์ความมั่นคงปลอดภัยสารสนเทศและจุดอ่อนความมั่นคงปลอดภัยสารสนเทศให้ได้รับทราบ

นโยบาย

๑๑.๒.๑ หน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติ (Responsibilities and procedures)

๑) ต้องกำหนดหน้าที่รับผิดชอบและขั้นตอนปฏิบัติเพื่อรับมือเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของหน่วยงาน และมีความเป็นระบบระเบียบที่ดี โดยให้เป็นไปตามแนวปฏิบัติการดำเนินการตอบสนองเหตุการณ์มั่นคงปลอดภัยระบบสารสนเทศ

๑๑.๒.๒ การรายงานสถานการณ์ความมั่นคงปลอดภัยสารสนเทศ (Reporting information security events)

๑) ต้องกำหนดช่องทางการติดต่อเพื่อรายงานสถานการณ์ความมั่นคงปลอดภัยอย่างชัดเจน

๑๑.๒.๓ การรายงานจุดอ่อนความมั่นคงปลอดภัยสารสนเทศ (Reporting information security weaknesses)

๑) หากผู้ใช้งานตรวจพบเหตุอันอาจส่งผลต่อความมั่นคงปลอดภัยของระบบสารสนเทศต้องรายงานเหตุการณ์ดังกล่าวต่อผู้รับผิดชอบ

๑๑.๒.๔ การประเมินและตัดสินใจต่อสถานการณ์ความมั่นคงปลอดภัยสารสนเทศ (Assessment of and decision on information security events)

๑) ก่อนการรายงานสถานการณ์ด้านความมั่นคงปลอดภัยต้องตรวจสอบให้ชัดเจน

๑๑.๒.๕ การตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Response to information security incidents)

๑) กำหนดให้มีการรายงานสถานการณ์ความมั่นคงปลอดภัยสารสนเทศตามระดับความรุนแรงของเหตุการณ์ หากส่งผลกระทบรุนแรงต่อผู้ใช้งานเป็นจำนวนมาก ต้องประกาศให้ทราบโดยรวดเร็ว

๑๑.๒.๖ การเรียนรู้จากเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Learning from information security incidents)

๑) ต้องมีการบันทึกเหตุการณ์ละเมิดความมั่นคงปลอดภัย โดยอย่างน้อยต้องพิจารณาถึงประเภทของเหตุการณ์ ปริมาณที่เกิดขึ้น และค่าใช้จ่ายที่เกิดจากความเสียหาย เพื่อจะได้เรียนรู้และเตรียมการป้องกัน

๑๑.๒.๗ การเก็บรวบรวมหลักฐาน (Collection of evidence)

๑) ต้องรวบรวมและจัดเก็บหลักฐานตามกฎหรือหลักเกณฑ์สำหรับอ้างอิงในกระบวนการทางศาล

หมวด ๑๒ การบริหารจัดการความมั่นคงปลอดภัยเพื่อสร้างความต่อเนื่องขององค์กร (Information security aspects of business continuity management)

๑๒.๑ การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management)

วัตถุประสงค์ เพื่อป้องกันการหยุดชะงักในการดำเนินงานขององค์กรที่เป็นผลมาจากวิกฤตหรือภัยพิบัติหนึ่ง

นโยบาย

๑๒.๑.๑ นโยบายการวางแผนความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Planning information security continuity policy)

๑) ผู้ดูแลระบบต้องมีการจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ ที่อาจเกิดขึ้นกับระบบสารสนเทศ (IT Contingency Plan) ตามแนวปฏิบัติการสำรองและการกู้คืนข้อมูล

๑๒.๑.๒ นโยบายตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ (Risk assessment information policy)

๑) ต้องดำเนินการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศอย่างน้อยปีละ ๑ ครั้ง ตามแนวปฏิบัติการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

๑๒.๑.๓ การตรวจสอบ การทบทวน และการประเมินความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Verify, review and evaluate information security continuity)

๑) ต้องทบทวนแผนเตรียมความพร้อมกรณีฉุกเฉินความพร้อมอย่างน้อยปีละ ๑ ครั้ง

๑๒.๒ การเตรียมการอุปกรณ์ประมวลผลสำรอง (Redundancies)

วัตถุประสงค์ เพื่อจัดเตรียมสภาพความพร้อมใช้ของอุปกรณ์ประมวลผลสารสนเทศ

นโยบาย

๑๒.๒.๑ สภาพความพร้อมใช้ของอุปกรณ์ประมวลผลสารสนเทศ (Availability of information processing facilities)

๑) อุปกรณ์ประมวลผลสารสนเทศต้องมีการเตรียมการสำรองไว้อย่างเพียงพอเพื่อให้ตรงตามความต้องการด้านสภาพความพร้อมใช้ที่กำหนดไว้

หมวด ๑๓ การปฏิบัติตามข้อกำหนด (Compliance)

๑๓.๑ ความสอดคล้องกับความต้องการด้านกฎหมายและในสัญญาจ้าง (Compliance with legal and contractual requirements)

วัตถุประสงค์ เพื่อหลีกเลี่ยงการละเมิดข้อผูกพันในกฎหมาย ระเบียบข้อบังคับ หรือสัญญาจ้าง ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ และที่เป็นความต้องการด้านความมั่นคงปลอดภัย

นโยบาย

๑๓.๑.๑ การระบุกฎหมายและความต้องการในสัญญาจ้างที่เกี่ยวข้อง (Identification of applicable legislation and contractual requirements)

๑) จัดทำประกาศนโยบาย และแนวปฏิบัติ คู่มือการใช้งานสารสนเทศ พร้อมทั้งเผยแพร่ทางเว็บไซต์ขององค์กร

๒) ผู้ดูแลระบบต้องจัดให้มีหลักสูตรที่สอดคล้องกับการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศเพื่อป้องกันการเข้าถึงจากผู้ใช้ซึ่งไม่ได้รับอนุญาต

๑๓.๑.๒ สิทธิในสินทรัพย์ทางปัญญา (Intellectual property rights)

๑) ต้องปฏิบัติตาม ข้อกำหนดที่ระบุไว้ใน ลิขสิทธิ์การใช้งานซอฟต์แวร์อย่างเคร่งครัด รวมทั้งต้องมีการควบคุมการใช้งานซอฟต์แวร์ตามลิขสิทธิ์ที่ได้รับด้วย ได้แก่ การลงทะเบียนเพื่อใช้งานซอฟต์แวร์ต้องเก็บหลักฐานแสดงความเป็นเจ้าของลิขสิทธิ์

๑๓.๑.๓ การป้องกันข้อมูล (Protection of records)

๑) ห้ามผู้ใช้งานทำซ้ำ เผยแพร่ ข้อมูลที่เป็นการละเมิดลิขสิทธิ์ หรือซอฟต์แวร์ที่เป็นการละเมิดลิขสิทธิ์บนระบบสารสนเทศขององค์กร

๑๓.๒ การทบทวนความมั่นคงปลอดภัยสารสนเทศ (Information security reviews)

วัตถุประสงค์ เพื่อให้มีการปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศอย่างสอดคล้องกับนโยบาย แนวปฏิบัติ ข้อกำหนดขององค์กร

นโยบาย

๑๓.๒.๑ การทบทวนอย่างอิสระด้านความมั่นคงปลอดภัยสารสนเทศ (Independent review of information security)

๑) นโยบาย แนวปฏิบัติ ข้อกำหนด มาตรการต่าง ๆ ต้องมีการทบทวนตามรอบระยะเวลาที่กำหนด

๑๓.๒.๒ ความสอดคล้องกับนโยบายและมาตรฐานด้านความมั่นคงปลอดภัย (Compliance with security policies and standards)

๑) หน่วยงานต้องคอยตรวจสอบ สอดส่อง ขั้นตอนปฏิบัติที่อยู่ภายใต้การดำเนินงานของตนเองโดยเทียบกับนโยบายมาตรฐาน

๑๓.๒.๓ การทบทวนความสอดคล้องทางเทคนิค (Technical compliance review)

๑) การตั้งค่าการทำงานของระบบต้องได้รับการทบทวนอย่าสม่ำเสมอ เพื่อมุ่งไปยังการรักษาความมั่นคงปลอดภัยสารสนเทศ

ส่วนที่ ๓

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 กำหนดให้ผู้ใช้งานต้อง

ลงทะเบียน 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 เช่น แผ่นดินไหว 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 และเก็บสายให้เรียบร้อย เพื่อป้องการการเดินสะดุด

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 จึงต้องกำหนดแนวทางในการปฏิบัติงาน

ของหน่วยงานภายนอกเพื่อความมั่นคง 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 และผู้ดูแลระบบต้องควบคุมการปฏิบัติงานนั้น 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

เอกสารอ้างอิง

- ประกาศมหาวิทยาลัยเกษตรศาสตร์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มหาวิทยาลัยเกษตรศาสตร์
- ISO27001:2013 Information technology – Security techniques – Information Security Management Systems – Requirement มาตรฐานด้านการจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ
- Control Objectives for information and related Technology 5 for Risk (COBIT 5 for Risks) การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ
- The Ultimate Guide to Service-Level Agreements (SLA) การกำหนดมาตรฐานการให้บริการ