ประกาศสถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๘

.....

โดยที่พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ มาตรา ๕ กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐ หรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ กำหนดให้หน่วยงานของรัฐต้องจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร ประกอบกับตามมาตรา ๔๔ มาตรา ๔๕ แห่งพระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดให้หน่วยงานของรัฐจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ สถาบันจึงเห็นสมควรกำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อเป็นเครื่องมือให้กับผู้ใช้งาน ผู้ดูแลระบบงาน และผู้เกี่ยวข้องกับระบบเครือข่ายคอมพิวเตอร์ใช้เป็นแนวทางในการดูแลรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสถาบัน

อาศัยอำนาจตามความในมาตรา ๓๔ แห่งพระราชบัญญัติสถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง พ.ศ. ๒๕๕๑ ประกอบมาตรา ๕ และมาตรา ๗ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ จึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศสถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๘”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศเป็นต้นไป

ข้อ ๓ บรรดาประกาศ คำสั่ง หรือมติอื่นใดของสถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบังในส่วนที่ได้กำหนดไว้แล้วในประกาศนี้ หรือซึ่งขัดหรือแย้งกับประกาศนี้ ให้ใช้ประกาศนี้แทน

ข้อ ๔ นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ประกอบด้วย

นโยบายที่ ๑ นโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ

นโยบายที่ ๒ นโยบายและแนวปฏิบัติการจัดโครงสร้างความมั่นคงปลอดภัยของระบบสารสนเทศ

นโยบายที่ ๓ นโยบายและแนวปฏิบัติการบริหารจัดการสินทรัพย์สารสนเทศ

นโยบายที่ ๔ นโยบายและแนวปฏิบัติการสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร

นโยบายที่ ๕ นโยบายและแนวปฏิบัติการสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม

นโยบายที่ ๖ นโยบายและแนวปฏิบัติการบริหารจัดการระบบเครือข่ายคอมพิวเตอร์และการดำเนินการ

นโยบายที่ ๗ นโยบายและแนวปฏิบัติการเข้าถึงและควบคุมการใช้งานสารสนเทศ

นโยบายที่ ๘ นโยบายและแนวปฏิบัติการจัดหา พัฒนา และดูแลรักษาระบบสารสนเทศ

นโยบายที่ ๙ นโยบายและแนวปฏิบัติการบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ

นโยบายที่ ๑๐ นโยบายและแนวปฏิบัติการบริหารความต่อเนื่องทางธุรกิจในด้านความมั่นคงปลอดภัยของระบบสารสนเทศ

นโยบายที่ ๑๑ นโยบายและแนวปฏิบัติการควบคุมกระบวนการทำงานให้เป็นไปตามข้อกำหนด

นโยบายที่ ๑๒ นโยบายและแนวปฏิบัติการใช้งานระบบสารสนเทศอย่างปลอดภัย

นโยบายที่ ๑๓ นโยบายและแนวปฏิบัติการใช้งานระบบคลาวด์

นโยบายที่ ๑๔ นโยบายและแนวปฏิบัติการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

ข้อ ๕ ให้สถาบันมีนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศตามเอกสารแนบท้ายประกาศนี้

ข้อ ๖ ส่วนงานภายในสถาบันต้องจัดทำ **"แผนการรับมือภัยคุกคามทางไซเบอร์"** ให้เป็นไปตามกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และสอดคล้องกับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสถาบัน

ข้อ ๗ การกำหนดหน้าที่และความรับผิดชอบ

๗.๑ ผู้บริหารระดับสูงสุด (Chief Executive Officer : CEO) ผู้ปฏิบัติหน้าที่อธิการบดีสถาบัน เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นกรณีระบบคอมพิวเตอร์ หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๗.๒ ผู้ที่ปฏิบัติหน้าที่เป็นผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer : CIO) ของสถาบันเป็นผู้รับผิดชอบในการสั่งการ กำกับนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตามกำกับ ดูแลและควบคุมตรวจสอบการดำเนินงานด้านเทคโนโลยีสารสนเทศให้สอดคล้องกับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๗.๓ ผู้ที่ปฏิบัติหน้าที่เป็นผู้บริหารด้านความมั่นคงปลอดภัยสารสนเทศ (Chief Information Security Officer : CISO) เป็นผู้รับผิดชอบในการดำเนินการให้เป็นไปตามประกาศนี้ รวมถึงกำหนดให้มีการปฏิบัติที่ชัดเจนและให้มีการทบทวนนโยบายและแนวปฏิบัติให้เป็นปัจจุบันอย่างน้อยปีละ ๑ ครั้ง ทั้งนี้หากมีความเสี่ยงที่เกิดขึ้นอย่างเด่นชัด เช่น กรณีมีการนำระบบสารสนเทศใหม่เข้ามาใช้งาน หรือมีกรณีที่ต้องปฏิบัติตามกฎหมายฉบับใหม่ อันมีผลกระทบกับการดำเนินการของสถาบัน หากแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศไม่เป็นปัจจุบันยังไม่ตอบสนองต่อภารกิจและความเสี่ยงอย่างเหมาะสม ต้องทบทวนปรับปรุงนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศภายใน ๙๐ วันหลังจากรับทราบ เพื่อปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย และรับมือกับความเสี่ยงได้อย่างเหมาะสมและทันเหตุการณ์

๗.๔ ผู้อำนวยการสำนักบริหารข้อมูลดิจิทัลพระจอมเกล้าเจ้าคุณทหารลาดกระบังเป็นผู้รับผิดชอบ ติดตาม กำกับ ดูแล ควบคุม ตรวจสอบ รวมทั้งให้ข้อเสนอแนะ วิธีการ และแนวทางแก้ไขปัญหาแก่เจ้าหน้าที่ระดับปฏิบัติการหรือผู้ที่ได้รับมอบหมาย ให้เป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๗.๕ เพื่อให้การปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสถาบันเป็นไปอย่างมีประสิทธิภาพ กำหนดให้สำนักบริหารข้อมูลดิจิทัลพระจอมเกล้าเจ้าคุณทหารลาดกระบัง ผู้ดูแลระบบ ผู้รับผิดชอบระบบสารสนเทศ และผู้ที่ได้รับมอบหมาย เป็นผู้รับผิดชอบในการดำเนินการให้เป็นไปตามประกาศนี้ และร่วมดำเนินงาน ทบทวน ปรับปรุงนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และหากมีการเปลี่ยนแปลงนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสถาบัน ให้ประกาศให้เจ้าหน้าที่ทุกระดับรับทราบทุกครั้ง

ข้อ ๘ ให้อธิการบดีเป็นผู้รักษาการตามประกาศนี้ และมีอำนาจวินิจฉัยปัญหาเกี่ยวกับการปฏิบัติตามประกาศนี้

ประกาศ ณ วันที่ ๒๐ พฤษภาคม พ.ศ. ๒๕๖๘

(รองศาสตราจารย์คมสัน มาลีสี)
อธิการบดีสถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

เอกสารแนบท้าย

ประกาศสถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
พ.ศ. ๒๕๖๘

คำนำ

ระบบเทคโนโลยีสารสนเทศเป็นสิ่งสำคัญสำหรับสถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบังในปัจจุบัน และมีบทบาทในการช่วยอำนวยความสะดวกให้กับการดำเนินงาน ทำให้การเข้าถึงข้อมูลมีความรวดเร็ว การติดต่อสื่อสารมีประสิทธิภาพ และช่วยประหยัดต้นทุนในการดำเนินงานด้านต่าง ๆ ของสถาบัน แต่ในขณะเดียวกัน ทำให้สถาบันมีความเสี่ยงเพิ่มขึ้นจากภัยคุกคามของระบบเทคโนโลยีสารสนเทศ ซึ่งอาจสร้างความเสียหายต่อการปฏิบัติงานได้เนื่องจากระบบเทคโนโลยีสารสนเทศมีการเชื่อมโยงข้อมูลไปยังส่วนงานต่าง ๆ ส่งผลให้ช่องทางในการถูกบุกรุกเปิดกว้างขึ้นและอาจก่อให้เกิดเหตุอาชญากรรมทางคอมพิวเตอร์กับสถาบันได้หลายรูปแบบ เช่น ชุดคำสั่งไม่พึงประสงค์ หรือการบุกรุกโจมตีผ่านระบบเครือข่ายอินเทอร์เน็ต เพื่อก่อกวนให้ระบบใช้การไม่ได้ รวมถึงการขโมยข้อมูลหรือความลับทางราชการ ส่งผลให้สถาบันสูญเสียชื่อเสียงหรือภาพลักษณ์ ดังนั้นผู้ใช้บริการและผู้ดูแลระบบงานด้านเทคโนโลยีสารสนเทศ จึงมีความจำเป็นต้องตระหนักถึงการดูแล บำรุงรักษา และการควบคุมรักษาความมั่นคงปลอดภัยด้านสารสนเทศเป็นอย่างยิ่ง

ดังนั้น สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง จึงจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสถาบัน เพื่อให้การดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์มีความมั่นคงปลอดภัยและเชื่อถือได้ และเพื่อให้มีมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ตลอดจนมีมาตรฐานเป็นที่ยอมรับในระดับสากล และให้การดำเนินการของส่วนงานภายในเป็นไปในทิศทางเดียวกัน สอดคล้องกับกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

ทั้งนี้ นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสถาบันนั้นต้องได้รับความร่วมมือในการปฏิบัติตามอย่างเคร่งครัดและต้องทำอย่างต่อเนื่อง มีการตรวจสอบอย่างสม่ำเสมอ และปรับปรุงเพื่อให้สอดคล้องกับการพัฒนาของเทคโนโลยีที่เปลี่ยนแปลงไปอย่างรวดเร็ว จึงหวังเป็นอย่างยิ่งว่านโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้ จะเป็นเครื่องมือให้กับผู้ใช้งาน ผู้ดูแลระบบ และผู้ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศของสถาบัน ในการดูแลรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของสถาบันต่อไป

สารบัญ

สารบัญ

สารบัญ

คำนิยาม

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสถาบัน ประกอบด้วยคำนิยาม ดังนี้

(๑) "สถาบัน" หมายความว่า สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

(๒) "สำนักบริหารข้อมูลดิจิทัล" หมายความว่า สำนักบริหารข้อมูลดิจิทัลพระจอมเกล้าเจ้าคุณทหารลาดกระบัง สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง เป็นส่วนงานภายในสถาบันที่ให้บริการเทคโนโลยีต่าง ๆ เพื่อส่งเสริมให้เกิด Digital University มุ่งพัฒนาสถาบันให้เป็นองค์กรที่ขับเคลื่อนด้วยข้อมูล (Data Driven Organization) และบูรณาการข้อมูลต่าง ๆ ของสถาบันให้มีการรวมศูนย์เป็นไปตามหลัก Single Source of Trust รวมถึงจัดทำระบบสารสนเทศต่าง ๆ เพื่อรองรับการทำงานของแต่ละส่วนงานในสถาบัน และการดูแลรักษาระบบเครือข่าย โครงสร้างพื้นฐานต่าง ๆ รวมถึงความปลอดภัยทางไซเบอร์ของสถาบัน

(๓) "ผู้บริหารระดับสูงสุด" (Chief Executive Officer : CEO) หมายความว่า อธิการบดีสถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

(๔) "ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง" (Chief Information Officer : CIO) หมายความว่า รองอธิการบดี ที่ได้รับมอบหมายให้ดูแลรับผิดชอบงานด้านเทคโนโลยีสารสนเทศของสถาบัน

(๕) "ผู้บริหารด้านความมั่นคงปลอดภัยสารสนเทศ" (Chief Information Security Officer : CISO) หมายความว่า ผู้ช่วยอธิการบดีฝ่ายสารสนเทศและความปลอดภัยทางไซเบอร์ หรือผู้ที่ได้รับมอบหมาย

(๖) "ผู้บังคับบัญชา" หมายความว่า ผู้บังคับบัญชาของส่วนงานภายในสถาบัน หรือผู้มีอำนาจสั่งการตามโครงสร้างการบริหารงานของสถาบัน

(๗) "ผู้อำนวยการสำนักบริหารข้อมูลดิจิทัล" หมายความว่า ผู้อำนวยการสำนักบริหารข้อมูลดิจิทัลพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

(๘) "ผู้บริหาร" หมายความว่า อธิการบดี รองอธิการบดี ผู้ช่วยอธิการบดี หัวหน้าส่วนงานวิชาการ หัวหน้าส่วนงานอื่น ผู้อำนวยการสำนัก ผู้อำนวยการสำนักงาน หัวหน้าสำนักงานสภาสถาบัน หัวหน้าศูนย์ หัวหน้าภาควิชา

(๙) "ผู้ใช้งาน" หรือ "ผู้ใช้บริการ" หมายความว่า บุคลากรสถาบัน นักศึกษา ศิษย์เก่า และบุคคลอื่นที่ได้รับอนุญาต

(๙.๑) "บุคลากรสถาบัน" หมายความว่า ข้าราชการ พนักงานสถาบันทุกประเภท และลูกจ้างสถาบันทุกประเภท สามารถเข้าใช้งานบริหารหรือดูแลรักษาระบบสารสนเทศของสถาบัน โดยมีสิทธิและหน้าที่ขึ้นอยู่กับบทบาท (Role)

(๙.๒) "นักศึกษา" หมายความว่า ผู้ที่กำลังศึกษาอยู่ในสถาบันระดับปริญญาตรี โท เอก และมีข้อมูลอยู่ในระบบฐานข้อมูลของสำนักทะเบียนและบริการการศึกษา

(๙.๓) "ศิษย์เก่า" หมายความว่า บุคคลผู้สำเร็จการศึกษาจากสถาบัน (ระดับปริญญาตรี โท เอก) และมีข้อมูลสำเร็จการศึกษาอยู่ในระบบฐานข้อมูลของสำนักทะเบียนและบริการการศึกษา

(๙.๔) "บุคคลอื่นที่ได้รับอนุญาต" (Authorized user) หมายความว่า บุคคลที่สถาบันอนุญาตให้เข้ามาใช้ระบบสารสนเทศของสถาบันได้ชั่วคราวเพื่อประโยชน์ในการดำเนินงานของสถาบัน ได้แก่ บุคลากรแลกเปลี่ยนตามความร่วมมือของสถาบัน พนักงาน หรือลูกจ้างบริษัทภายนอกที่เข้ามาติดต่อ หรือดูแลรักษาระบบให้กับสถาบัน หรือที่ปรึกษา หรือผู้ปฏิบัติงานตามสัญญาจ้าง

(๑๐) "ผู้ดูแลระบบ" (System Administrator) หมายความว่า เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชา ให้มีหน้าที่รับผิดชอบในการดูแลรักษาหรือจัดการระบบคอมพิวเตอร์และระบบเครือข่าย ซึ่งสามารถเข้าถึงระบบเครือข่ายคอมพิวเตอร์ เพื่อการบริหารจัดการเครือข่ายสถาบัน

(๑๑) "ผู้พัฒนาระบบ" หมายความว่า เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชา ให้มีหน้าที่รับผิดชอบในการพัฒนาระบบหรือแอปพลิเคชัน

(๑๒) "ส่วนงานภายในสถาบัน" หรือ "ส่วนงาน" หมายความว่า สำนักงานสภาสถาบัน สำนักงานอธิการบดี ส่วนงานวิชาการ และส่วนงานอื่น

(๑๓) "หน่วยงานภายนอก" หรือ "ผู้ให้บริการภายนอก" หมายความว่า หน่วยงานภายนอก หรือผู้ให้บริการภายนอกที่สถาบันอนุญาตให้มีสิทธิในการเข้าถึงและใช้งานข้อมูลหรือสินทรัพย์ต่าง ๆ ของสถาบัน โดยจะได้รับสิทธิในการใช้งานตามอำนาจหน้าที่ และต้องรับผิดชอบในการรักษาความลับของข้อมูลของสถาบัน

(๑๔) "ความมั่นคงปลอดภัยด้านสารสนเทศ" (Information Security) หมายความว่า การรักษาความมั่นคงปลอดภัยสำหรับระบบสารสนเทศของสถาบัน เพื่อการธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศรวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non-Repudiation) และความน่าเชื่อถือ (Reliability) และหมายความรวมถึง การป้องกันสินทรัพย์สารสนเทศจากการเข้าถึง ใช้ เปิดเผย ขัดขวาง เปลี่ยนแปลงแก้ไข ทำสูญหาย ทำให้เสียหาย ถูกทำลาย หรือล่วงรู้โดยมิชอบ

(๑๕) "มาตรฐาน" (Standard) หมายความว่า บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริง เพื่อให้ได้ตามวัตถุประสงค์หรือเป้าหมาย

(๑๖) "วิธีปฏิบัติ" (Procedure) หมายความว่า รายละเอียดที่บอกขั้นตอนเป็นข้อ ๆ ที่ต้องนำมาปฏิบัติเพื่อให้ได้มาซึ่งมาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์

(๑๗) "แนวทางปฏิบัติ" (Guideline) หมายความว่า แนวทางที่ไม่ได้บังคับให้ปฏิบัติ แต่แนะนำให้ปฏิบัติตามเพื่อให้สามารถบรรลุเป้าหมายได้ง่ายขึ้น

(๑๘) "ข้อมูลคอมพิวเตอร์" หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์ ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์

(๑๙) "เจ้าของข้อมูล" (Data Owner) หมายความว่า ส่วนงานภายในสถาบันที่ได้รับมอบหมายจากผู้บังคับบัญชา ให้ปฏิบัติงานรับผิดชอบข้อมูลที่ระบุไว้ โดยทำหน้าที่กำกับดูแลตามธรรมาภิบาลข้อมูลตลอดวงจรชีวิตของข้อมูลนั้น ๆ รวมทั้งทำหน้าที่กำหนดสิทธิในการเข้าถึงข้อมูลและจัดชั้นความลับของข้อมูลของเจ้าของข้อมูลส่วนบุคคล (Data Subject)

(๒๐) "ระบบสารสนเทศ" (Information System) หมายความว่า ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูล ซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่ายและสามารถนำไปใช้ประโยชน์ในการบริหารจัดการ การวางแผน การตัดสินใจ และอื่น ๆ นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

(๒๑) "ระบบคอมพิวเตอร์" หมายความว่า อุปกรณ์หรือชุดอุปกรณ์คอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันโดยมีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่เป็นแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

(๒๒) "ระบบเครือข่าย" (Network System) หมายความว่า ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบสารสนเทศต่าง ๆ ของสถาบันได้ เช่น ระบบแลน (LAN) ระบบอินทราเน็ต (Intranet) ระบบอินเทอร์เน็ต (Internet) เป็นต้น

(๒๓) "ระบบแลน" (Local Area Network : LAN) และ **"ระบบอินทราเน็ต"** (Intranet) หมายความว่า ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่าง ๆ ภายในสถาบันเข้าด้วยกันเป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในสถาบัน

(๒๔) "ระบบอินเทอร์เน็ต" (Internet) หมายความว่า ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่าง ๆ ของสถาบัน เข้ากับเครือข่ายอินเทอร์เน็ตทั่วโลก

(๒๕) "VPN" (Virtual Private Network) หมายความว่า เครือข่ายคอมพิวเตอร์เสมือนส่วนตัว โดยในการรับส่งข้อมูลจริงจะทำการเข้ารหัสเฉพาะแล้วรับส่งผ่านเครือข่ายอินเทอร์เน็ต ทำให้บุคคลอื่นไม่สามารถอ่านได้ และมองไม่เห็นข้อมูลนั้นไปจนถึงปลายทาง

(๒๖) "ไฟร์วอลล์" (Firewall) หมายความว่า เทคโนโลยีป้องกันการบุกรุกจากบุคคลภายนอกเพื่อไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้ามาใช้ข้อมูลและทรัพยากรในเครือข่าย โดยอาจใช้ทั้งอุปกรณ์ที่เป็นฮาร์ดแวร์และซอฟต์แวร์ที่พัฒนาสำหรับป้องกันการรักษาความปลอดภัย

(๒๗) "MAC Address" (Media Access Control Address) หมายความว่า หมายเลขเฉพาะที่ใช้อ้างถึงอุปกรณ์ที่ต่อกับระบบเครือข่าย หมายเลขนี้จะมากับอีเทอร์เน็ตการ์ด โดยแต่ละการ์ดจะมีหมายเลขที่ไม่ซ้ำกัน ตัวเลขจะอยู่ในรูปของเลขฐาน ๑๖ จำนวน ๖ คู่ ตัวเลขเหล่านี้จะมีประโยชน์ไว้ใช้สำหรับการส่งผ่านข้อมูลไปยังต้นทางและปลายทางได้อย่างถูกต้อง

(๒๘) "เลขที่อยู่ไอพี" (IP Address) หมายความว่า ตัวเลขประจำเครื่องคอมพิวเตอร์ที่ต่ออยู่ในระบบเครือข่ายซึ่งเลขที่อยู่ไอพีของแต่ละเครื่องจะต้องไม่ซ้ำกัน โดยประกอบด้วยชุดของตัวเลข ๔ ส่วน หรือ ๖ ส่วน ที่คั่นด้วยเครื่องหมายจุด (.)

(๒๙) "แผนผังระบบเครือข่าย" (Network Diagram) หมายความว่า แผนผังซึ่งแสดงถึงการเชื่อมต่อของระบบเครือข่ายของสถาบัน

(๓๐) "อุปกรณ์จัดเส้นทาง" (Router) หมายความว่า อุปกรณ์ที่ใช้ในระบบเครือข่ายคอมพิวเตอร์ทำหน้าที่จัดเส้นทางและค้นหาเส้นทาง เพื่อส่งข้อมูลต่อไปยังระบบเครือข่ายอื่น

(๓๑) "ชุดคำสั่งไม่พึงประสงค์" (Malicious Software หรือ Malware) หมายความว่า ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไข เปลี่ยนแปลง หรือเพิ่มเติม นำมาซึ่งการขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้ เว้นแต่ เป็นชุดคำสั่งไม่พึงประสงค์ที่อาจนำมาใช้เพื่อป้องกันหรือแก้ไขชุดคำสั่งดังกล่าวข้างต้น

(๓๒) "ระบบเทคโนโลยีสารสนเทศ" (Information Technology System) หมายความว่า ระบบงานของสถาบันที่นำเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่สถาบันสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ ได้แก่ ระบบคอมพิวเตอร์ ระบบเครือข่าย ระบบปฏิบัติการ โปรแกรมประยุกต์ ข้อมูล และสารสนเทศ เป็นต้น

(๓๓) "พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ" (Information System Workspace) หมายความว่า พื้นที่ที่สถาบันอนุญาตให้มีการใช้งานระบบเทคโนโลยีสารสนเทศ โดยแบ่งเป็น

(๓๓.๑) "พื้นที่ทำงานทั่วไป" (General Working Area) หมายความว่า พื้นที่ที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคล และคอมพิวเตอร์พกพาที่ประจำโต๊ะทำงาน

(๓๓.๒) "พื้นที่ทำงานของผู้ดูแลระบบ" (System Administrator Area) หมายความว่า พื้นที่ที่เจ้าหน้าที่ผู้ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาหรือจัดการระบบคอมพิวเตอร์และระบบเครือข่ายปฏิบัติงาน

(๓๓.๓) "พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย" (IT Equipment or Network Area) หมายความว่า พื้นที่ติดตั้งและจัดเก็บอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย และให้หมายความรวมถึงพื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data Storage Area)

(๓๔) "สินทรัพย์" หมายความว่า สิ่งใดก็ตามทั้งที่มีตัวตนและไม่มีตัวตน ที่มีคุณค่าสำหรับสถาบัน อันได้แก่ ข้อมูล ระบบข้อมูล ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ ข้อมูลคอมพิวเตอร์และสินทรัพย์ด้านเทคโนโลยีสารสนเทศของสถาบัน เช่น อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ ระบบสารสนเทศ ตัวเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ เครื่องบันทึกข้อมูล อุปกรณ์ต่อพ่วง เป็นต้น

(๓๕) "จดหมายอิเล็กทรอนิกส์" (E-mail) หมายความว่า ระบบที่บุคคลใช้ในการรับส่งข้อมูลระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่ายภาพกราฟิกภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ มาตรฐานที่ใช้ในการรับส่งข้อมูลชนิดนี้ ได้แก่ SMTP, POP3, IMAP และ Exchange เป็นต้น

(๓๖) "ชื่อบัญชีผู้ใช้งาน" หรือ "บัญชีผู้ใช้บริการ" (Account Name) หมายความว่า ชุดของตัวอักษรหรือตัวเลขที่ถูกกำหนดขึ้นเพื่อใช้ในการลงชื่อเข้า (Login) เพื่อใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายที่มีการกำหนดสิทธิการใช้งานไว้

(๓๗) "รหัสผ่าน" (Password) หมายความว่า ชุดของตัวอักษรหรืออักขระหรือตัวเลขที่ถูกกำหนดขึ้นเพื่อใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคลที่มีการกำหนดสิทธิการใช้งานไว้ เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

(๓๘) "การพิสูจน์ยืนยันตัวตน" (Authentication) หมายความว่า ขั้นตอนการรักษาความปลอดภัยในการเข้าใช้งานระบบ เป็นขั้นตอนในการพิสูจน์ตัวตนของผู้ใช้งาน ซึ่งทั่วไปแล้วจะเป็นการพิสูจน์โดยใช้ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password)

(๓๙) "ลงชื่อเข้า" (Login) หมายความว่า กระบวนการที่ผู้ใช้งานต้องทำให้เสร็จสิ้นตามเงื่อนไขที่ตั้งไว้เพื่อเข้าใช้งานระบบคอมพิวเตอร์และระบบเครือข่าย ซึ่งปกติแล้วจะอยู่ในรูปแบบของการป้อนข้อมูลชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ให้ถูกต้อง

(๔๐) "ลงชื่อออก" (Logout) หมายความว่า กระบวนการที่ผู้ใช้งานทำเพื่อสิ้นสุดการใช้งานระบบคอมพิวเตอร์และระบบเครือข่าย

(๔๑) "การเข้ารหัส" (Encryption) หมายความว่า การนำข้อมูลมาเข้ารหัสลับ เพื่อป้องกันการลักลอบเข้ามาใช้ข้อมูล ผู้ที่สามารถเปิดไฟล์ข้อมูลที่เข้ารหัสลับไว้ จะต้องมีโปรแกรมถอดรหัสลับ (Decryption) เพื่อให้ข้อมูลกลับมาใช้งานได้ตามปกติ

(๔๒) "สิทธิของผู้ใช้งาน" หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของสถาบัน

(๔๓) "การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ" (Access Control) หมายความว่า การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานระบบเครือข่ายหรือระบบสารสนเทศทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

(๔๔) "เหตุการณ์ด้านความมั่นคงปลอดภัย" (Information Security Event) หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

(๔๕) "สถานการณ์ความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด" (Information Security Incident) หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or Unexpected) ซึ่งอาจทำให้ระบบของสถาบันถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

(๔๖) "การรักษาความมั่นคงปลอดภัยไซเบอร์" หมายความว่า มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ทั้งจากภายในและภายนอกประเทศ อันกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ

(๔๗) "ภัยคุกคามทางไซเบอร์" หมายความว่า การกระทำหรือการดำเนินการใด ๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งไม่พึงประสงค์ โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

(๔๘) "ไซเบอร์" หมายความว่า ข้อมูลและการสื่อสารที่เกิดจากการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต หรือโครงข่ายโทรคมนาคม รวมทั้งการให้บริการโดยปกติของดาวเทียมและระบบเครือข่ายที่คล้ายคลึงกัน ที่เชื่อมต่อกันเป็นการทั่วไป

(๔๙) "ประมวลแนวทางปฏิบัติ" หมายความว่า ระเบียบหรือหลักเกณฑ์ที่คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์กำหนด

(๕๐) "เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์" หมายความว่า เหตุการณ์ที่เกิดจากการกระทำหรือการดำเนินการใด ๆ ที่มิชอบ ซึ่งกระทำการผ่านทางคอมพิวเตอร์หรือระบบคอมพิวเตอร์ ซึ่งอาจเกิดความเสียหายหรือผลกระทบต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือความมั่นคงปลอดภัยไซเบอร์ของคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์

นโยบายที่ ๑
นโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ
(Information Security Policy)

วัตถุประสงค์

เพื่อให้ผู้ใช้งานและบุคคลที่เกี่ยวข้องตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ และได้รับทราบถึงหน้าที่ความรับผิดชอบและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ

นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มี ๒ ส่วน

<u>ส่วนที่ ๑.</u> การจัดทำนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๑.๑ การจัดทำนโยบาย

(๑) ผู้บริหาร และผู้ใช้งาน ได้มีส่วนร่วมในการจัดทำข้อปฏิบัติที่สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสถาบัน

(๒) นโยบายได้ทำเป็นลายลักษณ์อักษร โดยประกาศให้ผู้ใช้งานทราบ และสามารถเข้าถึงได้อย่างสะดวกผ่านทางเว็บไซต์ของสถาบัน

(๓) กำหนดผู้รับผิดชอบตามนโยบายและแนวปฏิบัติดังกล่าวให้ชัดเจน

(๔) ทบทวนและปรับปรุงนโยบายอย่างน้อยปีละ ๑ ครั้ง

๑.๒ รายละเอียดของนโยบาย

(๑) การกำหนดการเข้าถึงหรือควบคุมการใช้งานสารสนเทศตามเป้าหมายครอบคลุมอย่างน้อย ๔ เรื่อง ดังนี้

(๑.๑) การเข้าถึงสารสนเทศ

ต้องมีนโยบายในการบริหารจัดการระบบสารสนเทศที่ได้มาตรฐาน โดยมีการแยกประเภทและจัดเก็บเทคโนโลยีสารสนเทศเป็นหมวดหมู่ มีระบบสำรองระบบสารสนเทศและระบบคอมพิวเตอร์ที่สมบูรณ์พร้อมใช้งาน รวมทั้งมีแผนฉุกเฉินในการใช้งาน เพื่อให้สามารถทำงานได้อย่างต่อเนื่อง

(๑.๒) การเข้าถึงระบบเครือข่าย

ต้องมีการควบคุมการเข้าถึงระบบเครือข่าย การแบ่งแยกระบบเครือข่ายคอมพิวเตอร์โดยสอดคล้องเหมาะสมกับระดับความต้องการด้านการรักษาความมั่นคงปลอดภัยของแต่ละขอบเขตที่ถูกจัดแบ่งการใช้บริการระบบเครือข่าย ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

(๑.๓) การเข้าถึงระบบปฏิบัติการ

ต้องมีการควบคุมการเข้าถึงระบบปฏิบัติการ เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต การกำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการที่จะต้องควบคุมโดยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย

(๑.๔) การเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ

ต้องมีการกำหนดมาตรการจำกัดหรือควบคุมบุคคลที่ไม่ได้รับอนุญาตเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศของสถาบัน โดยให้สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้

(๒) การจัดระบบสารสนเทศและระบบสำรองของสารสนเทศ ต้องมีนโยบายในการบริหารจัดการระบบสารสนเทศที่ได้มาตรฐาน อยู่ในสภาพพร้อมใช้งาน และจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

(๓) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ ต้องมีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ โดยกำหนดให้มีการตรวจสอบ และควบคุมคุณภาพระบบงานเทคโนโลยีสารสนเทศ และตรวจประเมินระบบรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของสถาบันอย่างน้อยปีละ ๑ ครั้ง ด้วยผู้ตรวจสอบภายในของสถาบัน หรือ ผู้ตรวจสอบอิสระด้านความมั่งคงปลอดภัยจากภายนอก

(๔) การกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจ ต้องมีแนวปฏิบัติในการบริหารจัดการสิทธิในแต่ละกลุ่ม รวมถึงการระงับสิทธิ

<u>ส่วนที่ ๒.</u> แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

วัตถุประสงค์และขอบเขต

เพื่อให้ระบบเทคโนโลยีสารสนเทศของสถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง หรือต่อไปนี้เรียกว่า “สถาบัน” เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่าง ๆ สถาบันจึงเห็นสมควรกำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยกำหนดให้มีมาตรฐาน (Standard) แนวปฏิบัติ (Guideline) ขั้นตอนปฏิบัติ (Procedure) ให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและป้องกันภัยคุกคามต่าง ๆ โดยมีวัตถุประสงค์ ดังต่อไปนี้

๒.๑ การจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศหรือเครือข่ายคอมพิวเตอร์ของสถาบัน ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล

๒.๒ กำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร อ้างอิงตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ และประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยของรัฐ (ฉบับที่ ๒) พ.ศ. ๒๕๕๖ ที่มีการปรับปรุงอย่างต่อเนื่อง และมาตรฐาน ISO/IEC ๒๗๐๐๑

๒.๓ นโยบายและแนวปฏิบัตินี้จะต้องทำการเผยแพร่ให้บุคลากรเจ้าหน้าที่ทุกระดับในสถาบันได้รับทราบและปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

๒.๔ เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติ และวิธีปฏิบัติ ให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับสถาบันตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศของสถาบันในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด

องค์ประกอบของนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

นโยบายที่ ๑ นโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ (Information Security Policy)

นโยบายที่ ๒ นโยบายและแนวปฏิบัติการจัดโครงสร้างความมั่นคงปลอดภัยของระบบสารสนเทศ (Organization of Information Security)

นโยบายที่ ๓ นโยบายและแนวปฏิบัติการบริหารจัดการสินทรัพย์สารสนเทศ (Asset Management)

นโยบายที่ ๔ นโยบายและแนวปฏิบัติการสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร (Human Resource Security)

นโยบายที่ ๕ นโยบายและแนวปฏิบัติการสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม (Physical and Environmental Control)

นโยบายที่ ๖ นโยบายและแนวปฏิบัติการบริหารจัดการระบบเครือข่ายคอมพิวเตอร์และการดำเนินการ (Communications and Operations Management)

นโยบายที่ ๗ นโยบายและแนวปฏิบัติการเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control)

นโยบายที่ ๘ นโยบายและแนวปฏิบัติการจัดหา พัฒนา และดูแลรักษาระบบสารสนเทศ (System Acquisition, Development and Maintenance)

นโยบายที่ ๙ นโยบายและแนวปฏิบัติการบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security Incident Management)

นโยบายที่ ๑๐ นโยบายและแนวปฏิบัติการบริหารความต่อเนื่องทางธุรกิจในด้านความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security Aspects of Business Continuity Management)

นโยบายที่ ๑๑ นโยบายและแนวปฏิบัติการควบคุมกระบวนการทำงานให้เป็นไปตามข้อกำหนด (Compliance)

นโยบายที่ ๑๒ นโยบายและแนวปฏิบัติการใช้งานระบบสารสนเทศอย่างปลอดภัย (Information System Secure Usage)

นโยบายที่ ๑๓ นโยบายและแนวปฏิบัติการใช้งานระบบคลาวด์
(Cloud Computing Usage)

นโยบายที่ ๑๔ นโยบายและแนวปฏิบัติการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ
(Risk Management)

แนวทางปฏิบัติ

๑.๑ ดำเนินการกำหนดนโยบายความมั่นคงปลอดภัยสารสนเทศ โดยจัดทำเป็นลายลักษณ์อักษรตามวัตถุประสงค์ของขอบเขตงานที่ได้รับการอนุมัติจากผู้บริหารระดับสูงสุด (CEO) หรือผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) เพื่อประกาศใช้และถือปฏิบัติในสถาบัน โดยให้มีผลบังคับใช้กับบุคลากรในทุกระดับของสถาบัน ตลอดจนบุคคลภายนอกที่เกี่ยวข้องกับการใช้ข้อมูลและสินทรัพย์สารสนเทศของสถาบัน

๑.๒ ทำความเข้าใจ และให้การสนับสนุนการปฏิบัติตามนโยบายความมั่นคงปลอดภัยสารสนเทศ โดยจัดให้มีการทำรายงานการประชุมผู้บริหาร และแจ้งเป็นแนวปฏิบัติให้เจ้าหน้าที่ผู้เกี่ยวข้องรับทราบและปฏิบัติตามอย่างเคร่งครัด

๑.๓ จัดให้มีการทบทวนปรับปรุงนโยบายและข้อปฏิบัติให้เป็นปัจจุบันอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง เพื่อให้สอดคล้องกับการเปลี่ยนแปลงและแนวโน้มของความเสี่ยงในอนาคตที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยทางด้านสารสนเทศของสถาบัน

๑.๔ จัดให้มีการประเมินแนวปฏิบัติความมั่นคงปลอดภัยสารสนเทศ เพื่อนำไปปรับปรุงให้มีประสิทธิภาพในปีถัดไป

นโยบายที่ ๒
นโยบายและแนวปฏิบัติการจัดโครงสร้างความมั่นคงปลอดภัยของระบบสารสนเทศ
(Organization of Information Security)

วัตถุประสงค์

เพื่อกำหนดโครงสร้างองค์กรให้มีผู้รับผิดชอบดูแลด้านความมั่นคงปลอดภัยของระบบสารสนเทศ และกำหนดมาตรการควบคุมการปฏิบัติหน้าที่ด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศสำหรับส่วนงานต่าง ๆ ภายในองค์กร ให้เป็นไปตามนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

แนวทางปฏิบัติ

๒.๑ การจัดการโครงสร้างความมั่นคงปลอดภัยของระบบสารสนเทศ

๒.๑.๑ ผู้บริหารระดับสูงสุด (Chief Executive Office : CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใด ๆ แก่สถาบัน หรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๒.๑.๒ จัดให้มีการประชุมคณะกรรมการพัฒนาบริหารจัดการระบบสารสนเทศ โดยผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO)/ผู้ช่วยอธิการบดี/คณบดี/ผู้อำนวยการสำนัก/ผู้อำนวยการสำนักงาน เพื่อทำการทบทวนและทราบถึงนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างน้อยปีละ ๑ ครั้ง ส่วนผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) เป็นผู้กำกับดูแลรับผิดชอบด้านสารสนเทศของสถาบัน

๒.๑.๓ จัดให้มีทรัพยากรด้านบุคลากร งบประมาณ การบริหารจัดการ และวัตถุดิบที่พอเพียงต่อการบริหารจัดการด้านความมั่นคงปลอดภัยในแต่ละปีงบประมาณ ซึ่งรวมถึงแผนความมั่นคงปลอดภัยสารสนเทศที่จะดำเนินการในปีงบประมาณนั้นด้วย

๒.๑.๔ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) ต้องจัดให้มีการแบ่งแยกหน้าที่ในการปฏิบัติงานด้านต่าง ๆ ที่เกี่ยวกับความมั่นคงปลอดภัยของระบบสารสนเทศออกจากกันอย่างชัดเจน เพื่อให้มีการสอบทานระหว่างกัน และป้องกันความเสี่ยงในการปฏิบัติงานที่อาจเกิดขึ้น เช่น การแบ่งแยกบุคลากรที่ปฏิบัติหน้าที่ในส่วนการพัฒนาระบบงาน (Developer) ออกจากบุคลากรที่ทำหน้าที่บริหารระบบ (System Administrator) ซึ่งปฏิบัติงานอยู่ในส่วนระบบคอมพิวเตอร์ที่ใช้งานจริง (Production Environment)

นโยบายที่ ๓

นโยบายและแนวปฏิบัติการบริหารจัดการสินทรัพย์สารสนเทศ

(Asset Management)

วัตถุประสงค์

๑. เพื่อให้สินทรัพย์สารสนเทศที่มีความสำคัญได้รับการป้องกันอย่างเหมาะสม ต้องจัดให้มีการระบุและกำหนดหน้าที่ความรับผิดชอบในการรักษาความมั่นคงปลอดภัยของสินทรัพย์สารสนเทศ

๒. เพื่อให้ข้อมูลและสินทรัพย์สารสนเทศที่มีความสำคัญต่อสถาบันได้รับการปกป้องในระดับที่เหมาะสมตามระดับความสำคัญ

๓. เพื่อป้องกันการเปิดเผย เปลี่ยนแปลงแก้ไข หรือสร้างความเสียหายต่อข้อมูลสารสนเทศสำคัญที่ถูกจัดเก็บในสื่อบันทึกข้อมูล

แนวทางปฏิบัติ

๓.๑ การบริหารจัดการสินทรัพย์สารสนเทศ

๓.๑.๑ มีการเก็บบันทึกข้อมูลสินทรัพย์สารสนเทศ โดยข้อมูลที่จัดเก็บต้องประกอบด้วยข้อมูลที่จำเป็นในการค้นหาเพื่อการใช้งานในภายหลัง

๓.๑.๒ ต้องกำหนดผู้รับผิดชอบสินทรัพย์สารสนเทศแต่ละประเภท เพื่อดูแลความมั่นคงปลอดภัยตลอดอายุการใช้งานของสินทรัพย์

๓.๑.๓ ตรวจสอบและทบทวนรายการสินทรัพย์อย่างสม่ำเสมอ เพื่อให้เกิดความถูกต้องเป็นปัจจุบัน โดยต้องดำเนินการดังกล่าวอย่างน้อยปีละ ๑ ครั้งและเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ

๓.๑.๔ ต้องจัดให้มีข้อกำหนดในการใช้งานสินทรัพย์สารสนเทศอย่างเหมาะสม เพื่อให้มั่นใจได้ว่าผู้ใช้งานสินทรัพย์สารสนเทศมีการเข้าถึงและใช้งานอย่างถูกต้องปลอดภัย

๓.๑.๕ ต้องควบคุมให้พนักงานและผู้ให้บริการภายนอก คืนสินทรัพย์สารสนเทศของสถาบัน ในกรณีที่ลาออก เลิกสัญญาว่าจ้าง หรือเปลี่ยนแปลงหน้าที่ปฏิบัติงาน

๓.๑.๖ จำแนกประเภทสินทรัพย์สารสนเทศตามระดับชั้นความลับ และความสำคัญต่อสถาบันและทบทวนการจำแนกประเภทดังกล่าวอย่างสม่ำเสมอ

๓.๑.๗ จัดทำป้ายชื่อสินทรัพย์สารสนเทศ (Labeling) ให้ชัดเจน ทั้งสินทรัพย์ประเภทอุปกรณ์คอมพิวเตอร์และสินทรัพย์ที่เป็นข้อมูลสารสนเทศ (Information Labeling) เพื่อให้ทราบถึงผู้รับผิดชอบรายละเอียดและระดับความสำคัญของสินทรัพย์สารสนเทศ พร้อมทั้งจัดให้มีมาตรการดูแลรักษาความมั่นคงปลอดภัยที่สอดคล้องเหมาะสมกับแต่ละกลุ่มประเภทของสินทรัพย์สารสนเทศ เช่น การควบคุมการเข้าถึง การจัดให้มีการเข้ารหัสข้อมูลที่เป็นความลับหรือต้องการความถูกต้องในระดับสูง เป็นต้น

นโยบายที่ ๔
นโยบายและแนวปฏิบัติการสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร
(Human Resource Security)

วัตถุประสงค์

เพื่อให้ผู้ใช้งานระบบสารสนเทศทั้งหมดที่ปฏิบัติงานภายในสถาบัน มีความตระหนักรู้และปฏิบัติงานโดยคำนึงถึงการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ

แนวทางปฏิบัติ

๔.๑ การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร

๔.๑.๑ ต้องประชาสัมพันธ์เผยแพร่ความรู้ให้กับผู้ใช้งานที่ปฏิบัติงานในสถาบันระมัดระวัง และละเว้นการใช้งานระบบสารสนเทศในลักษณะที่อาจก่อให้เกิดความเสียหายกับพันธกิจของสถาบันหรือความมั่นคงของประเทศ เช่น การหมิ่นประมาท การข่มขู่ การปลอมแปลงเป็นบุคคลอื่น การส่งจดหมายอิเล็กทรอนิกส์แบบลูกโซ่ และการเปิดเผยข้อมูลที่เป็นความลับของสถาบัน เป็นต้น

๔.๑.๒ ต้องประชาสัมพันธ์เผยแพร่ความรู้ให้ผู้ใช้งานที่ปฏิบัติงานภายในสถาบันตระหนัก และสังเกตถึงความผิดปกติใด ๆ ที่อาจส่งผลต่อความมั่นคงปลอดภัยของระบบสารสนเทศ (Security Weaknesses) และรายงานบุคคลหรือส่วนงานที่ทำหน้าที่รับแจ้งสถานการณ์ (Point of Contact) ทันที เมื่อพบความผิดปกติดังกล่าวทุกครั้ง

๔.๑.๓ ต้องกำหนดมาตรการดำเนินการทางวินัยต่อผู้ฝ่าฝืนนโยบายและหลักปฏิบัติเกี่ยวกับการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ

๔.๑.๔ กำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารนเทศ และการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ ให้ปฏิบัติดังนี้

๔.๑.๔.๑ การใช้งานรหัสผ่าน (Password Use)

ผู้ใช้งานระบบสารสนเทศต้องปฏิบัติตามข้อกำหนดในการใช้งานรหัสผ่าน

(๑) ผู้ใช้งานควรตั้งรหัสผ่านที่ตรวจสอบโดยระบบบริหารจัดการรหัสผ่าน (Password Management System) และมีความปลอดภัยในระดับสูงขึ้นไป

(๒) ผู้ใช้งานไม่เปิดเผยรหัสผ่านของตนเอง

(๓) ผู้ใช้งานควรจัดเก็บรหัสผ่านไว้ในสถานที่ที่มีความปลอดภัย

(๔) ผู้ใช้งานควรเปลี่ยนรหัสผ่านโดยทันทีเมื่อทราบว่ารหัสผ่านของตนอาจถูกเปิดเผยหรือล่วงรู้โดยผู้อื่น

(๕) ผู้ใช้งานควรตั้งรหัสผ่านที่ยากต่อการคาดเดา

(๖) ผู้ใช้งานควรเปลี่ยนรหัสผ่านตามรอบระยะเวลาที่กำหนด โดยไม่ใช้รหัสผ่านเดิมที่ใช้ตั้งมาแล้ว

(๗) ผู้ใช้งานควรเปลี่ยนรหัสผ่านชั่วคราวที่ได้รับโดยทันทีครั้งแรกที่ทำการลงชื่อเข้าสู่ระบบงาน

(๘) ผู้ใช้งานไม่ควรทำการบันทึกรหัสผ่านหรือจดจำรหัสผ่านของตนเองไว้บนอุปกรณ์ต่าง ๆ เช่น คอมพิวเตอร์ โน้ตบุ๊ก

(๙) ผู้ใช้งานไม่ควรใช้รหัสผ่านของตนร่วมกับผู้อื่น

(๑๐) ผู้ใช้งานไม่ควรใช้รหัสผ่านเดียวกันสำหรับระบบงานภายในองค์กร กับภายนอกองค์กร

(๑๑) ผู้ดูแลระบบควรเปลี่ยนรหัสผ่านด้วยความถี่ที่มากกว่าผู้ใช้งานทั่วไป เช่น ทุก ๓ เดือน

๔.๑.๔.๒ การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์

(๑) ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศโดยทันทีเมื่อเสร็จสิ้นงาน เช่น ระบบงาน เครื่องคอมพิวเตอร์ที่ใช้งาน หรือเครื่องคอมพิวเตอร์แบบพกพา

(๒) ผู้ใช้งานควรล็อกหน้าจออุปกรณ์ที่สำคัญเมื่อไม่ได้ใช้งานหรือปล่อยทิ้งไว้โดยไม่ได้ดูแลชั่วคราว

(๓) ผู้ดูแลระบบควรกำหนดให้พนักงานป้องกันผู้อื่นเข้าใช้เครื่องคอมพิวเตอร์หรือระบบสารสนเทศของตนโดยใส่รหัสผ่านได้ถูกต้องก่อนเข้าใช้งานเครื่องคอมพิวเตอร์

๔.๑.๔.๓ การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear Desk and Clear Screen Policy) ต้องกำหนดการควบคุมเอกสาร ข้อมูล หรือสื่อบันทึกข้อมูลต่าง ๆ เช่น USB Drive และ External Hard Disk ที่มีข้อมูลสารสนเทศที่จัดเก็บหรือบันทึกอยู่ไม่ให้วางทิ้งไว้บนโต๊ะทำงานหรือสถานที่ไม่ปลอดภัยในขณะที่ไม่ได้ใช้งาน (Clear Desk) ตลอดจนการควบคุมหน้าจอคอมพิวเตอร์ไม่ให้มีข้อมูลสำคัญปรากฏในขณะที่ไม่ได้ใช้งาน (Clear Screen) เช่น การตัดออกจากระบบ (Session Time Out) และการล็อกหน้าจอ (Lock Screen) อัตโนมัติ เป็นต้น

๔.๑.๔.๔ ผู้ใช้งานอาจนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ ดังนี้

(๑) ต้องแสดงหลักฐานในการกำหนดเครื่องข้อมูลลับ หรือข้อมูลที่สำคัญยิ่งยวด

(๒) ต้องแสดงข้อปฏิบัติสำหรับการเข้าถึงข้อมูลลับ หรือข้อมูลที่สำคัญยิ่งยวด

นโยบายที่ ๕
นโยบายและแนวปฏิบัติการสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม
(Physical and Environmental Control)

วัตถุประสงค์

เพื่อป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าถึงพื้นที่หวงห้าม เช่น ศูนย์ข้อมูลคอมพิวเตอร์ (Data Center) ศูนย์คอมพิวเตอร์สำรอง (Backup Site) และพื้นที่ที่ตั้งอุปกรณ์ระบบเครือข่ายคอมพิวเตอร์ ได้แก่ Floor Switch, Building Switch, Router Switch ซึ่งอาจก่อให้เกิดความเสียหายต่ออุปกรณ์สารสนเทศหรือมีผลกระทบต่อข้อมูลที่เป็นความลับหรือมีความสำคัญ

แนวทางปฏิบัติ

๕.๑ การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม

๕.๑.๑ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) ต้องกำหนดและแบ่งแยกบริเวณพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศให้ชัดเจน โดยการกำหนดพื้นที่ดังกล่าวอาจแบ่งออกได้เป็น พื้นที่ทำงานทั่วไป (General Working Area) พื้นที่ทำงานของผู้ดูแลระบบ (System Administrator Area) พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศ (IT Equipment Area) พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data Storage Area) เป็นต้น

๕.๑.๒ ภายในสถาบันมีการติดตั้งระบบควบคุมการเข้าออกอัตโนมัติ (Access Control System) เพื่อควบคุมการเข้าออกห้องควบคุมเครื่องคอมพิวเตอร์แม่ข่าย มีการกำหนดสิทธิในการเข้าออกให้กับบุคคลที่เกี่ยวข้องหรือได้รับอนุญาต เพื่อป้องกันการบุกรุก ที่สามารถบริหารจัดการได้อย่างมีระบบ เช่น การกำหนดช่วงเวลาที่อนุญาตให้เข้าออกของแต่ละบุคคล หรือการกำหนดสิทธิในการเข้าออก โดยจำแนกและกำหนดพื้นที่การติดตั้งระบบควบคุมการเข้าออกอัตโนมัติ (Access Control System) เป็น ๓ ส่วน ดังนี้

ส่วนที่ ๑ บริเวณทางเข้าสำนักบริหารข้อมูลดิจิทัล

ส่วนที่ ๒ บริเวณศูนย์ควบคุมเครื่องแม่ข่ายคอมพิวเตอร์และอุปกรณ์ระบบเครือข่ายสถาบัน (Data Center)

ส่วนที่ ๓ บริเวณ Facility อื่น ๆ ภายในสถาบัน

๕.๑.๓ ภายในสถาบันมีการติดตั้งระบบกล้องวงจรปิดและบำรุงรักษาอย่างสม่ำเสมอ เพื่อจุดประสงค์ในการเฝ้าระวังควบคุมการรักษาความมั่นคงปลอดภัย จากผู้ที่ไม่ได้รับอนุญาตรวมทั้งป้องกันความเสียหายอื่น ๆ ที่อาจเกิดขึ้นได้

๕.๑.๔ ต้องกำหนดสิทธิการเข้าถึงพื้นที่ของบุคลากร เพื่อปฏิบัติหน้าที่ตามที่ได้รับมอบหมาย

๕.๑.๕ บุคคลภายนอกที่ขอเข้าพื้นที่ บุคลากรที่ได้รับมอบหมายให้ดูแลพื้นที่นั้น ๆ ต้องตรวจสอบเหตุผลและความจำเป็นก่อนที่จะอนุญาต

๕.๑.๖ สถานที่ตั้งของระบบเทคโนโลยีสารสนเทศที่สำคัญต้องมีการควบคุมการเข้าออกที่รัดกุม และอนุญาตให้เฉพาะบุคคลที่ได้รับสิทธิและมีความจำเป็นผ่านเข้าใช้งานได้เท่านั้น

นโยบายที่ ๖
นโยบายและแนวปฏิบัติการบริหารจัดการระบบเครือข่ายคอมพิวเตอร์และการดำเนินการ
(Communications and Operations Management)

วัตถุประสงค์

๑. เพื่อป้องกันไม่ให้มีการกระทำที่มีความเสี่ยงต่อข้อมูลสารสนเทศในระบบเครือข่ายคอมพิวเตอร์

๒. เพื่อรักษาความมั่นคงปลอดภัยในการรับส่งข้อมูลสารสนเทศผ่านระบบเครือข่ายภายในองค์กรและระหว่างระบบเครือข่ายภายในองค์กรกับระบบเครือข่ายภายนอก

๓. เพื่อให้มั่นใจว่าการปฏิบัติงานด้านระบบสารสนเทศเป็นไปอย่างถูกต้องและมั่นคงปลอดภัย

๔. เพื่อให้มั่นใจว่าระบบสารสนเทศได้รับการป้องกันภัยคุกคามจากชุดคำสั่งไม่พึงประสงค์

๕. เพื่อป้องกันการสูญหายของข้อมูล

๖. เพื่อบันทึกและจัดเก็บหลักฐานการใช้งานเกี่ยวกับระบบสารสนเทศอย่างครบถ้วนและเพียงพอเพื่อการสอบทานการใช้งานข้อมูลระบบสารสนเทศ และป้องกันการใช้งานระบบสารสนเทศที่มีความผิดปกติหรือไม่เป็นไปตามที่กฎหมายกำหนด รวมทั้งเพื่อให้มีการติดตามและวิเคราะห์หลักฐานที่จัดเก็บ

๗. เพื่อควบคุมให้ระบบการทำงานให้มีความถูกต้อง ครบถ้วน และน่าเชื่อถือ (Integrity of Operational System)

๘. เพื่อป้องกันภัยคุกคามจากช่องโหว่ทางเทคนิค

๙. เพื่อจัดให้มีการวางแผนการตรวจสอบระบบสารสนเทศอย่างเพียงพอเหมาะสม โดยการตรวจสอบดังกล่าวต้องส่งผลกระทบต่อการปฏิบัติงานน้อยที่สุด

แนวทางปฏิบัติ

๖.๑ การบริหารจัดการระบบเครือข่ายคอมพิวเตอร์ให้ปลอดภัย

๖.๑.๑ มีการบริหารจัดการและควบคุมระบบเครือข่ายคอมพิวเตอร์อย่างมั่นคงปลอดภัย โดยขั้นต่ำควรมีการดำเนินการ ดังนี้

(๑) แบ่งแยกหน้าที่ความรับผิดชอบระหว่างผู้ดูแลระบบเครือข่ายและผู้ดูแลระบบคอมพิวเตอร์ออกจากกัน พร้อมทั้งกำหนดหน้าที่ความรับผิดชอบและขั้นตอนในการบริหารจัดการระบบ และอุปกรณ์เครือข่ายให้ชัดเจน

(๒) เปิดใช้งาน Service Port ที่เชื่อมต่อตามความจำเป็น พร้อมทั้งมีวิธีการเพื่อระบุถึงอุปกรณ์ที่เชื่อมต่ออย่างชัดเจน เช่น IP Address เป็นต้น ทั้งนี้ หากบริการที่จำเป็นต้องใช้มีความเสี่ยงต่อระบบรักษาความปลอดภัยแล้วต้องมีมาตรการเพิ่มเติมด้วย

(๓) มีการควบคุมการเชื่อมต่อกับระบบเครือข่ายสาธารณะ (Public Network) และระบบเครือข่ายไร้สาย (Wireless Network) อย่างรัดกุม เพื่อป้องกันการรั่วไหลหรือเปลี่ยนแปลงแก้ไขข้อมูลที่ส่งผ่านระบบเครือข่ายดังกล่าวเช่น การเข้ารหัสข้อมูลก่อนส่งผ่านเครือข่าย

(๔) มีการควบคุมเป็นพิเศษเพื่อให้ระบบเครือข่ายอยู่ในสภาพที่พร้อมใช้งานอยู่เสมอ เช่น จัดให้มีระบบเครือข่ายคอมพิวเตอร์ที่ใช้งานทดแทนกันได้ (Network Load Balance) เป็นต้น

(๕) มีการบันทึกและจัดเก็บหลักฐาน (Logs) เพื่อติดตามตรวจสอบการทำงานที่เกี่ยวข้องหรืออาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบเครือข่ายคอมพิวเตอร์

๖.๑.๒ จัดทำข้อตกลงการใช้บริการระบบเครือข่ายคอมพิวเตอร์ (Network Services Agreements) กับผู้ให้บริการภายนอก โดยมีเนื้อหาครอบคลุมถึงวิธีการบริหารจัดการ คุณภาพการให้บริการ รวมทั้งกระบวนการรักษาความมั่นคงปลอดภัยของระบบเครือข่ายคอมพิวเตอร์

๖.๑.๓ จัดให้มีการแบ่งแยกระบบเครือข่ายคอมพิวเตอร์ตามความเหมาะสม โดยระบุขอบเขต (Domain) ของระบบเครือข่ายย่อยอย่างชัดเจน และจัดให้มีกระบวนการควบคุมการเข้าถึงขอบเขตดังกล่าว โดยสอดคล้องเหมาะสมกับระดับความต้องการด้านการรักษาความมั่นคงปลอดภัยของแต่ละขอบเขตที่ถูกจัดแบ่ง

๖.๑.๔ จัดให้มีนโยบายและหลักปฏิบัติเพื่อปกป้องข้อมูลสารสนเทศที่รับส่งผ่านระบบและอุปกรณ์ในการสื่อสารทุกประเภท โดยมีเนื้อหาขั้นต่ำครอบคลุมถึงถึงรายละเอียด ดังนี้

(๑) แนวปฏิบัติที่ดีในการรับส่งข้อมูลสารสนเทศผ่านช่องทางการสื่อสารอิเล็กทรอนิกส์ประเภทต่าง ๆ

(๒) กระบวนการป้องกันการรับส่งข้อมูลสารสนเทศนอกเส้นทางที่ได้กำหนดไว้ (Mis-Routing) การดักรับสัญญาณ การเปลี่ยนแปลงแก้ไขหรือทำความเสียหายกับข้อมูล และชุดคำสั่งไม่พึงประสงค์ที่ถูกส่งผ่านช่องทางการสื่อสาร

(๓) กระบวนการป้องกันข้อมูลที่เป็นความลับหรือมีความสำคัญที่รับส่งในรูปแบบของไฟล์แนบ (Attachment Files) และการส่งต่อจดหมายอิเล็กทรอนิกส์แบบอัตโนมัติออกสู่ภายนอกองค์กร

(๔) การนำเทคนิคการเข้ารหัสข้อมูลมาใช้ในการรับส่งข้อมูลสารสนเทศผ่านช่องทางการสื่อสารบางประเภทที่ต้องการการรักษาความมั่นคงปลอดภัย เช่น การใช้งานระบบ Cloud Computing

๖.๑.๕ การใช้งานระบบรับส่งข้อความผ่านทางอิเล็กทรอนิกส์ (Electronic Messaging) ต้องคำนึงถึงความมั่นคงปลอดภัยของข้อมูลสารสนเทศที่รับส่งผ่านช่องทางดังกล่าว โดยต้องจัดให้มีมาตรการป้องกันการเปลี่ยนแปลงแก้ไข ทำความเสียหาย หรือเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต และมีกระบวนการตรวจสอบผู้ใช้งานอย่างเข้มงวดในกรณีที่ใช้งานผ่านเครือข่ายสาธารณะรวมทั้งต้องจัดการและควบคุมให้ระบบทำงานรับส่งข้อมูลได้อย่างถูกต้องและพร้อมใช้งานอยู่เสมอ ทั้งนี้ การใช้งานระบบส่งข้อความผ่านทางอิเล็กทรอนิกส์ที่ให้บริการโดยบุคคลภายนอก เช่น โปรแกรมสนทนาผ่านระบบอิเล็กทรอนิกส์ (Instant Messaging) ระบบเครือข่ายสังคมออนไลน์ (Social Networking) หรือโปรแกรมเรียกใช้แฟ้มข้อมูลร่วมกัน (File Sharing) ต้องจัดให้มีการควบคุมดูแลอย่างเหมาะสมเพียงพอ เช่น มีการขออนุมัติก่อนการใช้งาน รวมทั้งต้องปฏิบัติตามกฎหมายและหลักเกณฑ์ของทางการอย่างเคร่งครัด

๖.๑.๖ ต้องมีการทำสัญญารักษาความลับหรือไม่เปิดเผยข้อมูลที่มีความสำคัญกับเจ้าหน้าที่และผู้ให้บริการภายนอก โดยขั้นต่ำต้องมีเนื้อหาครอบคลุมถึงรายละเอียด ดังนี้

(๑) การระบุความเป็นเจ้าของข้อมูล (Data Owner) ข้อมูลสำคัญ ทรัพย์สินทางปัญญา และวิธีป้องกันการรั่วไหลของข้อมูล

(๒) ป้องกันการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต

(๓) การกำหนดขั้นตอนการขออนุญาตเข้าถึงข้อมูลหรือกำหนดสิทธิการเข้าถึงข้อมูลตามที่ได้ลงนาม

(๔) การกำหนดสิทธิการเข้าถึงข้อมูลเพื่อตรวจสอบหรือติดตามการใช้งานข้อมูลที่มีความสำคัญ

(๕) การกำหนดกระบวนการแจ้งเตือนและรายงานผู้เกี่ยวข้องหากพบการรั่วไหลหรือเปิดเผยข้อมูล โดยไม่ได้รับอนุญาต

(๖) การกำหนดมาตรการดำเนินการกรณีละเมิดหรือยกเลิกสัญญา รวมทั้งข้อกำหนดในการคืนหรือ ทำลายข้อมูลที่มีความสำคัญเมื่อสิ้นสุดสัญญา

(๗) ต้องจัดให้มีการลงนามโดยผู้รับผิดชอบ

๖.๒ การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ

๖.๒.๑ สถาบันต้องจัดให้มีวิธีปฏิบัติงานด้านระบบสารสนเทศที่สำคัญให้เป็นลายลักษณ์อักษรเพื่อให้เจ้าหน้าที่ปฏิบัติงานได้อย่างถูกต้องและเป็นไปตามนโยบายด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ เช่น ขั้นตอนในการเปิด - ปิดระบบ การประมวลผล การตรวจสอบประสิทธิภาพการทำงานของระบบ และตารางเวลาในการปฏิบัติงาน เป็นต้น และต้องทบทวนวิธีปฏิบัติดังกล่าวให้เป็นปัจจุบันอยู่เสมอ รวมทั้งจัดให้วิธีปฏิบัติงานดังกล่าวอยู่ในสภาพที่พร้อมใช้งานและเข้าถึงได้

๖.๒.๒ สถาบันต้องมีการควบคุมการปฏิบัติงานอย่างเคร่งครัด โดยเฉพาะในกรณีที่มีการเปลี่ยนแปลงโครงสร้างองค์กร ขั้นตอนการปฏิบัติงาน หรือการทำงานของระบบงานต่าง ๆ ซึ่งอาจกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ โดยต้องดำเนินการควบคุมตามวิธีการดังต่อไปนี้

(๑) กำหนดขั้นตอนหรือวิธีปฏิบัติที่เป็นลายลักษณ์อักษร ในกรณีการเปลี่ยนแปลงที่มีนัยสำคัญ

(๒) มีแผนรองรับ และดำเนินการทดสอบภายหลังการเปลี่ยนแปลง

(๓) มีการประเมินผลกระทบที่อาจเกิดขึ้นจากการเปลี่ยนแปลง

(๔) มีขั้นตอนการขออนุมัติจากผู้มีอำนาจ

(๕) มีขั้นตอนการตรวจสอบเพื่อให้มั่นใจว่ากระบวนการเปลี่ยนแปลงดังกล่าวเป็นไปตามนโยบายด้านความมั่นคงปลอดภัยของระบบสารสนเทศ

(๖) มีการสื่อสารให้บุคคลที่เกี่ยวข้องได้รับทราบเพื่อให้สามารถปฏิบัติงานได้อย่างถูกต้อง

(๗) มีกระบวนการถอยกลับสู่สภาพเดิม (Roll-Back) ของระบบงาน หากเกิดข้อผิดพลาดระหว่างการเปลี่ยนแปลง

๖.๒.๓ สถาบันต้องติดตามประสิทธิภาพการทำงานของระบบงานและอุปกรณ์สารสนเทศที่สำคัญให้ทำงานได้อย่างต่อเนื่องและมีประสิทธิภาพ เพื่อใช้เป็นข้อมูลในการประเมินสมรรถภาพและความเพียงพอ (Capacity) ของระบบงาน อุปกรณ์สารสนเทศ และบุคลากร เพื่อให้สามารถรองรับแผนการปฏิบัติงานในอนาคตได้อย่างมีประสิทธิภาพด้วย

๖.๒.๔ สถาบันต้องแบ่งแยกส่วนคอมพิวเตอร์ที่มีไว้สำหรับการพัฒนาระบบงาน (User Acceptance Testing : UAT) และใช้งานจริง (Production Environment) ออกจากกัน และควบคุมให้มีการเข้าถึงเฉพาะผู้ที่เกี่ยวข้องในแต่ละส่วนเท่านั้น ทั้งนี้ การแบ่งแยกส่วนดังกล่าวอาจแบ่งโดยใช้เครื่องคอมพิวเตอร์คนละเครื่องหรือแบ่งโดยการจัดเนื้อที่แยกไว้ต่างหากภายในเครื่องคอมพิวเตอร์เดียวกันก็ได้

๖.๒.๕ สถาบันต้องมีการป้องกันและตรวจสอบชุดคำสั่งไม่พึงประสงค์ รวมทั้งแก้ไขเพื่อให้ระบบกลับมาใช้งานได้ตามปกติ (Recovery) โดยขั้นต่ำต้องกำหนดมาตรการ ดังนี้

(๑) กำหนดนโยบายห้ามใช้ซอฟต์แวร์ที่ไม่ได้รับอนุญาต

(๒) มีกระบวนการป้องกันและตรวจสอบการใช้ซอฟต์แวร์ที่ไม่ได้รับอนุญาต และการใช้งานเว็บไซต์ ที่อาจมีชุดคำสั่งไม่พึงประสงค์

(๓) ติดตั้งซอฟต์แวร์ตรวจสอบชุดคำสั่งไม่พึงประสงค์ และปรับปรุงให้เป็นปัจจุบันอย่างสม่ำเสมอ พร้อมทั้งกำหนดผู้มีหน้าที่รับผิดชอบให้รายงานและแก้ไขปัญหากรณีพบภัยคุกคาม

(๔) ตรวจสอบซอฟต์แวร์ระบบงานที่มีความสำคัญอย่างสม่ำเสมอ หากพบการติดตั้งหรือเปลี่ยนแปลงที่ไม่ได้รับอนุญาต ต้องมีการตรวจสอบ

(๕) จัดให้มีการติดตามและกลั่นกรองข่าวสารเกี่ยวกับภัยคุกคาม เพื่อให้ทราบข้อเท็จจริง รวมทั้งแจ้งให้ผู้ที่เกี่ยวข้องได้ตระหนักถึงภัยคุกคามดังกล่าว

(๖) ในกรณีที่จำเป็นต้องจัดเก็บข้อมูลเป็นระยะเวลานาน ต้องคำนึงถึงวิธีการนำข้อมูลกลับมาใช้งานในอนาคตด้วย เช่น กรณีที่จัดเก็บข้อมูลในสื่อบันทึกประเภทใด ต้องมีการเก็บอุปกรณ์และโปรแกรมที่เกี่ยวข้องสำหรับใช้อ่านสื่อบันทึกประเภทนั้นไว้ด้วยเช่นกัน เป็นต้น

๖.๒.๖ สถาบันต้องจัดให้มีการบันทึกและจัดเก็บหลักฐาน (Logs) ของระบบงานที่มีความสำคัญประเภทต่าง ๆ ดังต่อไปนี้

(๑) หลักฐานการเข้าถึงพื้นที่หวงห้าม (Physical Access Log) โดยขั้นต่ำต้องมีรายละเอียดเกี่ยวกับบุคคลที่เข้าถึง ความพยายามในการเข้าถึง (ถ้ามี) วันและเวลาที่ผ่านเข้าออก โดยจัดเก็บเป็นระยะเวลาไม่น้อยกว่า ๖ เดือน

(๒) หลักฐานการเข้าถึงระบบปฏิบัติการ ฐานข้อมูล ระบบเครือข่ายคอมพิวเตอร์ (Authentication Log) โดยขั้นต่ำต้องมีรายละเอียดเกี่ยวกับบัญชีผู้ใช้งาน วันและเวลาที่เข้าใช้งาน และความพยายามในการเข้าใช้งาน โดยจัดเก็บเป็นระยะเวลาไม่น้อยกว่า ๖ เดือน

(๓) หลักฐานการเข้าถึงและใช้งานระบบสารสนเทศ (Application log) โดยขั้นต่ำต้องมีรายละเอียดเกี่ยวกับบัญชีผู้ใช้งาน หมายเลขประจำเครื่องที่ใช้งาน (Client IP Address) (ถ้ามี) วันและเวลาที่มีการใช้งาน Order ID และ Account ID โดยจัดเก็บเป็นระยะเวลาไม่น้อยกว่า ๖ เดือน ทั้งนี้ หากสถาบัน

ใช้หมายเลขประจำเครื่องแบบพลวัต (Dynamic IP Address) สถาบันต้องมีข้อมูลที่สามารถระบุผู้ใช้งานและหมายเลข IP Address ในช่วงเวลาที่ใช้งานดังกล่าวได้ด้วย

(๔) หลักฐานการบริหารระบบปฏิบัติการ (Event Log) หลักฐานบันทึกข้อมูลจราจรคอมพิวเตอร์ (Traffic Log) ของอุปกรณ์เครือข่ายที่สำคัญและหลักฐานการจัดการบริหารข้อมูล (Database Log) โดยให้เป็นไปตามการประเมินความเสี่ยงขององค์กรและเพียงพอต่อการตรวจสอบ

(๕) หลักฐานการใช้งานแฟ้มข้อมูล (Audit Log) เช่น Read, Write, Copy และ Delete เป็นต้น โดยจัดเก็บเป็นระยะเวลาไม่น้อยกว่า ๖ เดือน

(๖) หลักฐานการใช้งานอินเทอร์เน็ตที่เกิดขึ้นจากการใช้งานผ่านเครือข่ายสารสนเทศของสถาบัน (Internet Access Log) โดยขั้นต่ำต้องมีรายละเอียดเกี่ยวกับบัญชีผู้ใช้งาน หมายเลขประจำเครื่องที่ใช้งาน (IP Address) หมายเลขอินเทอร์เน็ตของสถาบัน (Organization IP Address) วันเวลาที่มีการใช้งาน และที่อยู่ของเว็บไซต์ปลายทาง (full URL) โดยจัดเก็บเป็นระยะเวลาไม่น้อยกว่า ๖ เดือน ทั้งนี้ หากใช้หมายเลขประจำเครื่องแบบพลวัต (Dynamic IP Address) สถาบันต้องมีข้อมูลที่สามารถระบุผู้ใช้งานและหมายเลข IP Address ในช่วงเวลาที่ใช้งานดังกล่าวได้ด้วย

๖.๒.๗ สถาบันต้องจัดเก็บข้อมูลการติดต่อสนทนาผ่านช่องทางอิเล็กทรอนิกส์ (Electronic Messaging) โดยให้จัดเก็บเป็นระยะเวลาไม่น้อยกว่า ๖ เดือน จัดเก็บข้อความในจดหมายอิเล็กทรอนิกส์ (Email Archive)

๖.๒.๘ สถาบันต้องจัดให้มีการป้องกันข้อมูลและระบบการบันทึกและจัดเก็บหลักฐานการใช้งานเกี่ยวกับระบบสารสนเทศจากการถูกเปลี่ยนแปลงแก้ไข ทำความเสียหาย หรือเข้าถึงโดยไม่ได้รับอนุญาต และมีการตรวจสอบอย่างสม่ำเสมอทั้งกรณีของ System Administrator Logs และ System Operator Logs

๖.๒.๙ สถาบันต้องกำหนดระบบเวลาของอุปกรณ์และระบบสารสนเทศที่มีความสำคัญให้ตรงกับเวลาอ้างอิงสากล (Stratum 0) โดยผิดพลาดไม่เกิน ๑๐๐ มิลลิวินาที

๖.๒.๑๐ สถาบันต้องจัดให้มีการติดตามและวิเคราะห์หลักฐานที่ถูกจัดเก็บสำหรับการใช้งานระบบสารสนเทศที่มีความสำคัญ โดยให้สอดคล้องกับการประเมินความเสี่ยงของสถาบัน

๖.๒.๑๑ สถาบันต้องจัดให้มีขั้นตอนเพื่อควบคุมการติดตั้งซอฟต์แวร์บนระบบงาน รวมทั้งจัดให้มีมาตรการเพื่อจำกัดการติดตั้งซอฟต์แวร์โดยผู้ใช้งาน

๖.๒.๑๒ ต้องมีขั้นตอนหรือวิธีปฏิบัติในการตรวจสอบระบบคอมพิวเตอร์แม่ข่ายและในกรณีที่พบว่ามีการใช้งาน หรือเปลี่ยนแปลงค่าในลักษณะผิดปกติ จะต้องดำเนินการแก้ไขรวมทั้งมีการรายงานโดยทันที

๖.๒.๑๓ สถาบันต้องจัดให้มีการติดตามข้อมูลข่าวสารเกี่ยวกับช่องโหว่ทางเทคนิคที่อาจเป็นความเสี่ยงต่อระบบสารสนเทศของสถาบันอย่างทันต่อเหตุการณ์ รวมทั้งต้องจัดให้มีการตรวจสอบหาช่องโหว่ดังกล่าวและมีมาตรการดำเนินการเพื่อปิดช่องโหว่หรือกำหนดแผนรองรับกรณีที่ระบบถูกบุกรุกผ่านช่องโหว่ดังกล่าว โดยขั้นต่ำต้องกำหนดแนวทางดำเนินการ ดังนี้

(๑) กำหนดผู้มีหน้าที่รับผิดชอบในการจัดการเกี่ยวกับช่องโหว่ทางเทคนิค โดยครอบคลุมถึงการประเมินความเสี่ยงของสินทรัพย์สารสนเทศที่เกี่ยวข้องซึ่งอาจได้รับผลกระทบจากช่องโหว่ดังกล่าว โดยเฉพาะ

สินทรัพย์สารสนเทศที่มีความเสี่ยงสูง การดำเนินการเพื่อปิดช่องโหว่ (Patching) และการประสานงานกับบุคคลที่เกี่ยวข้อง

(๒) มีการประเมินความเสี่ยงของโปรแกรมเพื่อปิดช่องโหว่ (Patches) โดยก่อนการติดตั้งโปรแกรม ต้องมีการทดสอบและประเมินผลกระทบที่อาจเกิดจากการติดตั้งโปรแกรมดังกล่าว ทั้งนี้ กรณีที่ไม่มีโปรแกรมเพื่อปิดช่องโหว่ ให้ปฏิบัติตามคำแนะนำของบริษัทผู้ผลิตสินทรัพย์สารสนเทศที่เกี่ยวข้อง

(๓) มีการทดสอบการบุกรุกระบบ (Penetration Test) กับระบบงานที่มีความสำคัญทุกระบบ โดยสถาบันอาจพิจารณาเลือกจัดทำการทดสอบกับบางระบบงานตามการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis) ได้ โดยต้องจัดทำการทดสอบอย่างน้อยทุก ๒ ปี และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ อย่างไรก็ดี สถาบันยังคงต้องจัดให้มีการทดสอบกับระบบงานที่มีความสำคัญอื่น ๆ ให้ครบถ้วน อย่างน้อยทุก ๔ ปี

(๔) กระบวนการจัดการช่องโหว่ด้านเทคนิคต้องสอดคล้องกับกระบวนการจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ (Incident Management) เพื่อเตรียมความพร้อมรองรับกรณีที่ระบบถูกบุกรุกผ่านช่องโหว่ ทั้งนี้ ให้รวมถึงกรณีที่ตรวจพบช่องโหว่แต่ยังไม่สามารถหาวิธีปิดช่องโหว่ได้

(๕) มีการบันทึกและจัดเก็บหลักฐานเพื่อการตรวจสอบในการดำเนินการต่าง ๆ ที่เกี่ยวข้องกับการจัดการช่องโหว่ทางเทคนิค

๖.๒.๑๔ สถาบันต้องจัดให้มีการวางแผนการตรวจสอบระบบสารสนเทศให้สอดคล้องกับความเสี่ยงที่ได้ประเมินไว้

๖.๒.๑๕ สถาบันต้องกำหนดขอบเขตการตรวจสอบทางเทคนิค (Technical Audit Test) ให้ครอบคลุมจุดเสี่ยงที่สำคัญและต้องควบคุมการตรวจสอบดังกล่าวไม่ให้กระทบต่อการปฏิบัติงานตามปกติ

๖.๒.๑๖ ในกรณีที่การตรวจสอบระบบสารสนเทศมีโอกาสกระทบต่อความพร้อมใช้งานของระบบ (System Availability) สถาบันต้องจัดให้มีการทดสอบนอกเวลาทำการ

๖.๒.๑๗ การติดตั้งและการเชื่อมต่อระบบคอมพิวเตอร์แม่ข่ายจะต้องดำเนินการหรืออยู่ในความดูแลของผู้อำนวยการสำนักบริหารข้อมูลดิจิทัลเท่านั้น

๖.๒.๑๘ ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่าง ๆ และจำกัดสิทธิการเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

นโยบายที่ ๗
นโยบายและแนวปฏิบัติการเข้าถึงและควบคุมการใช้งานสารสนเทศ
(Access Control)

วัตถุประสงค์

๑. เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้รับอนุญาตให้เข้าถึงระบบสารสนเทศของสถาบัน และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก หรือจากชุดคำสั่งไม่พึงประสงค์ที่จะสร้างความเสียหายแก่ข้อมูลหรือการทำงานของระบบสารสนเทศให้หยุดชะงักและทำให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบสารสนเทศของสถาบันได้อย่างถูกต้อง

๒. เพื่อกำหนดเป็นมาตรการการเข้าถึงระบบสารสนเทศของผู้ใช้งานมิให้บุคคลที่ไม่มีหน้าที่เกี่ยวข้องในการทำงานเข้าถึงระบบสารสนเทศและเครือข่ายภายในโดยไม่ได้รับอนุญาต รวมทั้งจำกัดสิทธิในการใช้งานระบบสารสนเทศ เพื่อให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบสารสนเทศของสถาบัน

๓. เพื่อกำหนดมาตรการควบคุมป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องในการปฏิบัติหน้าที่เข้าถึงล่วงรู้ แก้ไขเปลี่ยนแปลงระบบเครือข่ายและการสื่อสารที่สำคัญซึ่งจะทำให้เกิดความเสียหายต่อข้อมูลและระบบสารสนเทศของสถาบัน โดยมีการกำหนดกระบวนการควบคุมการเข้าใช้งานเครือข่ายที่แตกต่างกันของกลุ่มเครือข่ายต่าง ๆ ตามการแบ่งแยกเครือข่ายเป็น VLAN

๔. เพื่อให้ผู้ใช้งานได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้ระบบปฏิบัติการ รวมทั้งทำความเข้าใจตลอดจนปฏิบัติตามอย่างเคร่งครัดอันจะเป็นการป้องกันทรัพยากรและข้อมูลของส่วนงาน

แนวทางปฏิบัติ

๗.๑ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

เพื่อกำหนดเป็นมาตรการการเข้าถึงระบบสารสนเทศของผู้ใช้งาน มิให้บุคคลที่ไม่มีหน้าที่เกี่ยวข้องในการทำงานเข้าถึงระบบสารสนเทศและเครือข่ายภายในโดยไม่ได้รับอนุญาต รวมทั้งจำกัดสิทธิในการใช้งานระบบสารสนเทศ เพื่อให้สามารถตรวจสอบ ติดตาม พิสูจน์ตัวบุคคลที่เข้าใช้งานระบบสารสนเทศของสถาบัน โดยกำหนดแนวปฏิบัติในการควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตและผ่านการฝึกอบรมหลักสูตรการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ เพื่อป้องกันการเข้าถึงจากผู้ที่ไม่ได้รับอนุญาต

๗.๒ การควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ

๗.๒.๑ กำหนดประเภทของข้อมูล ดังนี้

(๑) ข้อมูลทั่วไป

(๒) ข้อมูลสำหรับการบริหาร

(๓) ข้อมูลสำหรับการปฏิบัติการ

๗.๒.๒ จัดแบ่งระดับความสำคัญของข้อมูลแต่ละประเภทออกเป็น ๓ ระดับ

(๑) ข้อมูลที่มีระดับความสำคัญมากที่สุด

(๒) ข้อมูลที่มีระดับความสำคัญปานกลาง

(๓) ข้อมูลที่มีระดับความสำคัญน้อย

๗.๒.๓ จัดแบ่งระดับชั้นความลับของข้อมูล

(๑) ข้อมูลลับที่สุด คือ หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด

(๒) ข้อมูลลับมาก คือ หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรง

(๓) ข้อมูลลับ คือ หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย

(๔) ข้อมูลทั่วไป คือ ข้อมูลที่สามารถเปิดเผยหรือแพร่ทั่วไปได้

๗.๒.๔ จัดแบ่งระดับชั้นการเข้าถึงข้อมูล

(๑) ระดับชั้นสำหรับผู้บริหาร

(๒) ระดับชั้นสำหรับผู้ใช้งานทั่วไป

(๓) ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมาย

๗.๒.๕ การอนุญาตการกำหนดสิทธิ หรือการมอบอำนาจดังนี้

(๑) อ่านอย่างเดียว

(๒) สร้างข้อมูล

(๓) ป้อนข้อมูล

(๔) แก้ไข

(๕) ลบ

(๖) อนุมัติ

(๗) ไม่มีสิทธิ

๗.๒.๖ การกำหนดเวลาที่เข้าถึงข้อมูลและระบบสารสนเทศ

(๑) ผู้ใช้งานเข้าถึงข้อมูลและระบบสารสนเทศได้ตลอดเวลา โดยผ่านระบบพิสูจน์ตัวตนก่อนเข้าใช้งาน

(๒) การใช้งานระบบสารสนเทศในแต่ละครั้ง กำหนดระยะเวลาใช้งาน ๘ ชั่วโมงต่อครั้ง

๗.๒.๗ มีการกำหนดช่องทางการเข้าถึงข้อมูล โดยช่องทางที่สามารถเข้าถึงได้ แบ่งออกเป็น

(๑) อินทราเน็ต (Intranet)

(๒) อินเทอร์เน็ต (Internet)

(๓) จดหมายอิเล็กทรอนิกส์ (E-Mail)

๗.๒.๘ มีข้อกำหนดการใช้งานตามภารกิจ เพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control) โดยกำหนดแนวทางการเข้าถึงระบบสารสนเทศและสิทธิที่เกี่ยวข้องโดยมีแนวปฏิบัติแบ่งเป็น ๒ ส่วน คือ

(๑) มีการควบคุมการเข้าถึงสารสนเทศ โดยให้กำหนดแนวทางการควบคุมการเข้าถึงระบบสารสนเทศ และสิทธิที่เกี่ยวข้องกับระบบสารสนเทศ

(๒) มีการปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย

๗.๒.๙ ผู้ดูแลระบบต้องกำหนดสิทธิการเข้าถึงข้อมูลและระบบข้อมูลให้สอดคล้องกับนโยบายที่เกี่ยวข้องกับการอนุญาตการกำหนดสิทธิ หรือการมอบหมาย/มอบอำนาจของสถาบันให้เหมาะสมกับการเข้าใช้งานของผู้ใช้ระบบ และหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบสารสนเทศรวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ ผู้ใช้ระบบจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

๗.๒.๑๐ ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายเท่านั้นที่สามารถแก้ไขเปลี่ยนแปลงสิทธิการเข้าถึงข้อมูลและระบบสารสนเทศ

๗.๒.๑๑ ผู้ดูแลระบบควรจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศของสถาบัน และตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบข้อมูลสำคัญ

๗.๒.๑๒ ผู้ดูแลระบบต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิต่าง ๆ และการผ่านเข้าออกสถานที่ตั้งระบบของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาต เพื่อเป็นหลักฐานในการตรวจสอบหากมีปัญหาเกิดขึ้น

๗.๓ การลงทะเบียนผู้ใช้งาน (User Registration)

๗.๓.๑ จัดทำแบบฟอร์มการลงทะเบียนผู้ใช้งาน สำหรับระบบสารสนเทศของสถาบัน

๗.๓.๒ ผู้ดูแลระบบต้องตรวจสอบบัญชีผู้ใช้งาน โดยเฉพาะผู้ที่ไม่มีการลงทะเบียนผู้ใช้งานมาก่อน

๗.๓.๓ ผู้ดูแลระบบต้องตรวจสอบและให้สิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบของผู้ใช้งาน

๗.๓.๔ ผู้ดูแลระบบต้องกำหนดให้มีการแจกเอกสารหรือสิ่งที่แสดงเป็นลายลักษณ์อักษรให้แก่ผู้ใช้งานเพื่อแสดงถึงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งานในการเข้าถึงระบบสารสนเทศ รวมทั้งกำหนดให้ผู้ใช้งานทำการลงนามในเอกสารดังกล่าวหลังจากที่ได้ทำความเข้าใจแล้ว

๗.๓.๕ ผู้ดูแลระบบต้องกำหนดให้มีการถอดถอนสิทธิการเข้าถึงระบบสารสนเทศโดยทันทีเมื่อผู้ใช้งานนั้นเปลี่ยนตำแหน่งงาน หรือพ้นสภาพการเป็นบุคลากรสถาบัน

๗.๓.๖ การลงทะเบียนผู้ใช้งาน ผู้ดูแลระบบต้องทำการตรวจสอบหรือทบทวนบัญชีผู้ใช้งานทั้งหมดเพื่อป้องกันการเข้าถึงระบบสารสนเทศโดยไม่ได้รับอนุญาต

๗.๔ การบริหารจัดการสิทธิของผู้ใช้งาน (User Management)

๗.๔.๑ ผู้ดูแลระบบต้องกำหนดสิทธิการใช้ระบบสารสนเทศ โดยให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

๗.๔.๒ ผู้ดูแลระบบต้องกำหนดระดับสิทธิในการเข้าถึงที่เหมาะสมสำหรับระบบสารสนเทศ

๗.๔.๓ ผู้ดูแลระบบต้องมอบหมายสิทธิที่มีความสอดคล้องกับนโยบายควบคุมการเข้าถึง

๗.๔.๔ ผู้ดูแลระบบต้องจัดเก็บการมอบหมายสิทธิให้แก่ผู้ใช้งาน

๗.๔.๕ กรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิพิเศษที่ได้รับว่าสามารถเข้าถึงในระดับใดได้บ้าง และต้องกำหนดให้ใช้ชื่อบัญชีผู้ใช้งาน (Account Name) และรหัสผ่าน (Password) ที่มีความแตกต่างกับชื่อบัญชีผู้ใช้งานและรหัสผ่านตามปกติ รวมถึงชื่อบัญชีผู้ใช้งานและรหัสผ่าน ต้องมีความแตกต่างกันในแต่ละระบบ

๗.๕ การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management)

๗.๕.๑ ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานลงนามเพื่อป้องกันการเปิดเผยข้อมูลรหัสผ่านของตน เช่น ลงนามในเอกสารเพื่อแสดงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งานในการเข้าถึงระบบสารสนเทศของสถาบัน

๗.๕.๒ ผู้ดูแลระบบต้องกำหนดขั้นตอนปฏิบัติสำหรับการตั้งหรือเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัย

๗.๕.๓ ผู้ดูแลระบบต้องให้ผู้ใช้งานเปลี่ยนรหัสผ่านโดยทันที ภายหลังจากที่ได้รับรหัสผ่านชั่วคราว และควรเปลี่ยนรหัสผ่านที่มีความยากต่อการเดาโดยผู้อื่น

๗.๕.๔ ผู้ดูแลระบบต้องกำหนดรหัสผ่านชั่วคราว โดยกำหนดรหัสผ่านให้มีความยากต่อการเดาโดยผู้อื่น และควรกำหนดรหัสผ่านที่แตกต่างกัน

๗.๕.๕ ผู้ดูแลระบบต้องจัดส่งรหัสผ่านให้ผู้ใช้งาน โดยมีการป้องกันการเข้าถึงจากผู้ไม่มีสิทธิ และควรกำหนดให้ผู้ใช้งานตอบกลับหลังจากที่ได้รับรหัสผ่านแล้ว

๗.๖ การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Rights)

๗.๖.๑ ผู้ดูแลระบบดำเนินการทบทวนสิทธิการเข้าถึงของผู้ใช้งานอย่างน้อย ๑ ครั้งต่อปี

๗.๖.๒ ผู้ดูแลระบบทบทวนสิทธิสำหรับผู้ที่มีสิทธิในระดับสูง ด้วยความถี่ที่มากกว่าผู้ใช้งานทั่วไป

๗.๖.๓ ผู้ดูแลระบบทบทวนสิทธิตามรอบระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงใด ๆ เช่น การเลื่อนตำแหน่ง ลดตำแหน่ง ย้ายส่วนงาน หรือสิ้นสุดการจ้างงาน

๗.๖.๔ ผู้ดูแลระบบต้องกำหนดให้มีการบันทึกการเปลี่ยนแปลงต่อบัญชีผู้ใช้งานที่มีสิทธิในระดับสูงเพื่อใช้ในการทบทวนในภายหลัง

๗.๗ การฝึกอบรมเพื่อสร้างความตระหนักเรื่องการรักษาความปลอดภัยระบบสารสนเทศ

๗.๗.๑ มีการกำหนดกิจกรรมเพื่อสร้างความตระหนักรู้ (Awareness) เกี่ยวกับการรักษาความมั่นคงปลอดภัยระบบสารสนเทศแก่ผู้ใช้งานระบบสารสนเทศที่ปฏิบัติงานภายในสถาบันอย่างสม่ำเสมออย่างน้อยปีละ ๑ ครั้ง โดยเนื้อหาต้องสอดคล้องกับนโยบายด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ และหน้าที่ความรับผิดชอบของบุคลากร

๗.๗.๒ ฝึกอบรมให้ความรู้ความเข้าใจกับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

๗.๘ กระบวนการควบคุมการเข้าถึงและใช้บริการระบบเครือข่าย

๗.๘.๑ การควบคุมการเข้าถึงเครือข่ายภายในสถาบัน (Network Access Control)

เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

(๑) มีการกำหนดระบบสารสนเทศที่ต้องมีการควบคุมการเข้าถึง โดยระบุเครือข่ายหรือบริการที่อนุญาตให้มีการใช้งานได้

(๒) มีข้อปฏิบัติสำหรับผู้ใช้งานให้สามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

(๓) มีการยืนยันตัวบุคคลสำหรับผู้ใช้ที่อยู่ภายในสถาบัน (User Authentication for External Connections) โดยต้องยืนยันตัวบุคคลก่อนอนุญาตให้เข้าใช้งานเครือข่ายและระบบสารสนเทศของสถาบัน

๗.๘.๒ การควบคุมการเข้าใช้งานระบบจากภายนอกสถาบัน

ต้องกำหนดให้มีการควบคุมการใช้งานระบบที่ผู้ดูแลระบบได้ติดตั้งไว้ภายในองค์กร เพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอก โดยมีแนวทางปฏิบัติดังนี้

(๑) การเข้าสู่ระบบระยะไกล (Remote Access) สู่ระบบเครือข่ายของสถาบัน ต้องควบคุมบุคคลที่จะเข้าสู่ระบบของสถาบันจากระยะไกล โดยกำหนดมาตรการการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน โดยต้องมีการลงชื่อเข้าใช้และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้อง

(๒) วิธีการใดก็ตามที่สามารถเข้าถึงข้อมูลหรือระบบสารสนเทศจากระยะไกล ต้องได้รับการอนุมัติจากสำนักบริหารข้อมูลดิจิทัลก่อน และมีการควบคุมอย่างเข้มงวดก่อนนำมาใช้ และผู้ใช้ต้องปฏิบัติตามข้อกำหนดของสถาบันในการเข้าสู่ข้อมูลหรือระบบสารสนเทศอย่างเคร่งครัด

(๓) การทำการให้สิทธิในการเข้าสู่ระบบจากระยะไกล ผู้ใช้ต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับองค์กรอย่างเพียงพอและต้องได้รับอนุมัติจากผู้มีอำนาจอย่างเป็นทางการ

(๔) ต้องมีการควบคุมพอร์ท (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

(๕) การอนุญาตให้ผู้ใช้เข้าสู่ระบบข้อมูลจากระยะไกล ต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น และไม่ควรเปิดพอร์ตทิ้งไว้โดยไม่จำเป็น ช่องทางดังกล่าวควรตัดการเชื่อมต่อเมื่อไม่ได้งานแล้ว และจะเปิดให้ใช้ได้เมื่อมีการร้องขอที่จำเป็นเท่านั้น

(๖) การพิสูจน์ตัวตนสำหรับผู้ใช้งานที่อยู่ภายนอก ผู้ใช้ระบบทุกคนเมื่อจะเข้าใช้งานระบบต้องผ่านการพิสูจน์ตัวตนจากระบบขององค์กรโดยแสดงชื่อผู้ใช้งาน (Username) และ รหัสผ่าน (Password) เป็นอย่างน้อย

๗.๘.๓ การระบุอุปกรณ์บนเครือข่าย (Equipment Identification in Networks)

ต้องมีวิธีการหรือกระบวนการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ โดยสามารถใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยันการเข้าถึง ดังนี้

(๑) ให้กำหนดวิธีการพิสูจน์ตัวตนทุกครั้งที่ใช้อุปกรณ์

(๒) มีการควบคุมการใช้งานอย่างเหมาะสม

(๓) จำกัดผู้ใช้งานที่สามารถเข้าใช้อุปกรณ์ได้

๗.๘.๔ การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection)

ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย ดังนี้

(๑) แสดงขั้นตอนหรือหลักเกณฑ์ในการควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบสำหรับการเข้าถึงทางกายภาพและทางเครือข่าย

(๒) กำหนดวิธีการป้องกันช่องทางที่ใช้บำรุงรักษาระบบผ่านเครือข่าย

(๓) ปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้ใช้งานได้อย่างจำกัดระยะเวลาเท่าที่จำเป็น โดยต้องได้รับการอนุญาตจากผู้รับผิดชอบเป็นลายลักษณ์อักษร

๗.๘.๕ การแบ่งแยกเครือข่าย (Segregation in Network)

ผู้ดูแลระบบต้องมีการออกแบบระบบเครือข่ายตามกลุ่มของบริการระบบสารสนเทศที่มีการใช้งาน กลุ่มของผู้ใช้ และกลุ่มของระบบสารสนเทศ เพื่อทำให้การควบคุมและป้องกันการบุกรุกได้อย่างเป็นระบบ ดังนี้

(๑) โซนภายใน (Internal Zone)

(๒) โซนภายนอก (External Zone)

๗.๘.๖ การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control)

ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างกันให้สอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึง ดังนี้

(๑) มีการตรวจสอบการเชื่อมต่อเครือข่าย

(๒) จำกัดสิทธิ และความสามารถของผู้ใช้ในการเชื่อมต่อเข้าสู่เครือข่าย

(๓) ระบุอุปกรณ์ เครื่องมือที่ใช้ควบคุมการเชื่อมต่อเครือข่าย

(๔) มีระบบการตรวจจับผู้บุกรุกทั้งในระดับเครือข่าย และระดับเครื่องคอมพิวเตอร์แม่ข่าย

(๕) ควบคุมไม่ให้มีการเปิดให้บริการบนเครือข่ายโดยไม่ได้รับอนุญาต

๗.๘.๗ การควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control)

ต้องควบคุมการจัดเส้นทางบนเครือข่าย เพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ ดังนี้

(๑) ควบคุมไม่ให้มีการเปิดเผยแผนการใช้หมายเลขเครือข่าย (IP Address)

(๒) กำหนดให้มีการแปลงหมายเลขเครือข่าย เพื่อแยกเครือข่ายย่อย

(๓) กำหนดมาตรการการบังคับใช้เส้นทางเครือข่าย ให้สามารถเชื่อมเครือข่ายปลายทางผ่านช่องทางที่กำหนดไว้ หรือจำกัดสิทธิในการใช้บริการเครือข่าย

๗.๘.๘ ผู้ดูแลระบบควรจัดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่าย (Enforced Path)

กำหนดเส้นทางให้เครื่องลูกข่ายใช้ไปยังเครื่องแม่ข่าย เพื่อไม่ให้ผู้ใช้สามารถใช้เส้นทางอื่น ๆ ได้ และกำหนดบุคคลที่รับผิดชอบในการกำหนดแก้ไขหรือเปลี่ยนแปลงค่าพารามิเตอร์ (Parameter) ต่าง ๆ ของระบบ

๗.๘.๙ ป้องกันเครือข่ายและอุปกรณ์

การเชื่อมต่อกับระบบเครือข่ายควรทบทวนการกำหนดค่าพารามิเตอร์ (Parameter) อย่างน้อยปีละหนึ่งครั้ง นอกจากนี้การกำหนดแก้ไขหรือเปลี่ยนแปลงค่าพารามิเตอร์ (Parameter) ควรแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

๗.๘.๑๐ ระบบเครือข่ายทั้งหมดของสถาบันที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นภายนอกสถาบัน

กำหนดการเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือโปรแกรมในการทำ Packet filtering เช่น การใช้ไฟร์วอลล์ (Firewall) หรือฮาร์ดแวร์อื่น เป็นต้น รวมทั้งต้องมีความสามารถในการตรวจจับมัลแวร์ (Malware) ด้วย

๗.๘.๑๑ ต้องมีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS)

เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของสถาบันในลักษณะที่ผิดปกติผ่านระบบเครือข่าย โดยมีการตรวจสอบการบุกรุกผ่านระบบเครือข่ายการใช้งานในลักษณะที่ผิดปกติ และการแก้ไขเปลี่ยนแปลงระบบเครือข่ายโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

๗.๘.๑๒ เลขที่อยู่ไอพี (IP address) ภายในของระบบงานเครือข่ายภายในของสถาบัน

ต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายได้โดยง่าย

๗.๘.๑๓ จัดทำแผนผังระบบเครือข่าย (Network Diagram)

จัดทำแผนผังรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายใน เครือข่ายภายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๗.๘.๑๔ การใช้เครื่องมือ (Tools)

เพื่อการตรวจสอบระบบเครือข่ายควรได้รับการอนุมัติจากผู้ดูแลระบบ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

๗.๘.๑๕ การติดตั้งและการเชื่อมต่ออุปกรณ์เครือข่าย

ต้องดำเนินการโดยสำนักบริหารข้อมูลดิจิทัลเท่านั้น

๗.๙ การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

๗.๙.๑ กำหนดขั้นตอนการปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย

การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยแสดงวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย โดยมีแนวปฏิบัติ ดังนี้

(๑) ผู้ใช้งานควรกำหนดรหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ที่รับผิดชอบ

(๒) ผู้ใช้งานควรตั้งค่าล็อกหน้าจอภาพเมื่อไม่มีการใช้งาน (Screen lock) หลังจากนั้นเมื่อต้องการใช้งาน ผู้ใช้งานต้องใส่รหัสผ่าน (Password) เพื่อเข้าใช้งาน

(๓) ก่อนการเข้าใช้ระบบปฏิบัติการต้องใส่ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ทุกครั้ง

(๔) ผู้ใช้งานไม่ควรอนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ของส่วนงานร่วมกัน

(๕) ผู้ใช้งานควรทำการลงชื่อออก (Logout) ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

๗.๙.๒ มีการระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication)

กำหนดให้มีการระบุตัวตนของผู้ใช้งานและเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสมดังนี้

(๑) ผู้ใช้งานต้องทำการพิสูจน์ตัวตนโดยระบุบัญชีผู้ใช้บริการ (Account Name) และรหัสผ่านทุกครั้งก่อนใช้ระบบสารสนเทศ เพื่อป้องกันผู้ไม่มีสิทธิเข้าใช้งานระบบสารสนเทศ หากการระบุและยืนยันตัวตนของผู้ใช้งานมีปัญหาหรือเกิดความผิดพลาด ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทำการแก้ไข

(๒) ผู้ใช้งานที่เป็นเจ้าของบัญชีผู้ใช้บริการ (Account Name) ต้องเป็นผู้รับผิดชอบในความเสียหายต่าง ๆ อันจะเกิดขึ้นจากการใช้บัญชีผู้ใช้บริการ (Account Name) ของเครื่องคอมพิวเตอร์และระบบเครือข่าย เว้นแต่จะพิสูจน์ได้ว่าความเสียหายนั้นเกิดจากการกระทำของผู้อื่น

(๓) ผู้ใช้งานจะต้องเก็บรักษาบัญชีผู้ใช้บริการ (Account Name) ไว้เป็นความลับและห้ามเปิดเผยต่อบุคคลอื่น ห้ามโอน จำหน่าย หรือจ่ายแจกให้ผู้อื่น โดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

(๔) ผู้ใช้งานจะต้องลงชื่อเข้าใช้ (Login) โดยใช้บัญชีผู้ใช้บริการ (Account Name) ของตนเองและทำการลงชื่อออก (Logout) ทุกครั้ง เมื่อสิ้นสุดการใช้งานหรือหยุดการใช้งานชั่วคราว

๗.๙.๓ การบริหารจัดการรหัสผ่าน (Password Management System)

ต้องมีระบบบริหารจัดการรหัสผ่านอัตโนมัติ โดยในการกำหนดรหัสผ่าน (Password) ของผู้ใช้งานจะมีระบบอัตโนมัติในการตรวจสอบว่ารหัสผ่านดังกล่าวมีความปลอดภัยมากน้อยเพียงใด โดยผู้ใช้งานระบบจะใช้รหัสผ่านที่ตรวจสอบแล้วว่ามีความปลอดภัยในระดับสูงเท่านั้น

๗.๙.๔ การใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities)

ควรจำกัดและควบคุมการใช้งานโปรแกรมอรรถประโยชน์สำหรับโปรแกรมคอมพิวเตอร์ที่สำคัญ เนื่องจากการใช้งานโปรแกรมอรรถประโยชน์บางชนิดสามารถทำให้ผู้ใช้งานหลีกเลี่ยงมาตรการป้องกันทางด้านความมั่นคงปลอดภัยของระบบได้ และเพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว ให้ดำเนินการดังนี้

(๑) จำกัดสิทธิการเข้าถึง และกำหนดสิทธิอย่างรัดกุมในการอนุญาตให้ใช้โปรแกรมอรรถประโยชน์

(๒) กำหนดให้อนุญาตใช้งานโปรแกรมอรรถประโยชน์เป็นรายครั้ง

(๓) จัดเก็บโปรแกรมอรรถประโยชน์ไว้ในสื่อภายนอก หากไม่ต้องใช้งานเป็นประจำ

(๔) มีการเก็บบันทึกการเรียกใช้งานโปรแกรมเหล่านี้

(๕) กำหนดให้มีการถอดถอนโปรแกรมอรรถประโยชน์ที่ไม่จำเป็นออกจากระบบ

๗.๙.๕ เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (Session Time – Out)

โดยดำเนินการตามหลักปฏิบัติดังนี้

(๑) ให้กำหนดหลักเกณฑ์การยุติการใช้งานระบบสารสนเทศ เมื่อว่างเว้นจากการใช้งานเป็นเวลา ๑๕ นาทีเป็นอย่างน้อย หากเป็นระบบที่มีความเสี่ยงหรือความสำคัญสูง ให้กำหนดระยะเวลายุติการใช้งานระบบเมื่อว่างเว้นจากการใช้งานให้สั้นขึ้นหรือเป็นเวลา ๕ นาที ตามความเหมาะสม เพื่อป้องกันการเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต

(๒) ถ้าไม่มีการใช้งานระบบ ต้องทำการยกเลิกการใช้โปรแกรมประยุกต์และการเชื่อมต่อเข้าสู่ระบบโดยอัตโนมัติ

(๓) เครื่องปลายทางที่ตั้งอยู่ในพื้นที่ที่มีความเสี่ยงสูงต้องมีการกำหนดระยะเวลาให้ทำการปิดเครื่องโดยอัตโนมัติหลังจากที่ไม่มีการใช้งานเป็นระยะเวลาตามที่กำหนด

๗.๙.๖ การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection time)

ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศหรือโปรแกรมที่มีความเสี่ยงหรือมีความสำคัญสูง โดยมีข้อกำหนดดังนี้

(๑) กำหนดหลักเกณฑ์ในการจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ สำหรับระบบสารสนเทศหรือแอปพลิเคชันที่มีความเสี่ยงหรือมีความสำคัญสูง เพื่อให้ผู้ใช้งานสามารถใช้งานได้นานที่สุดภายในระยะเวลาที่กำหนดเท่านั้น เช่น กำหนดให้ใช้งานได้ ๓ ชั่วโมง ต่อการเชื่อมต่อหนึ่งครั้ง กำหนดให้ใช้งานได้เฉพาะในช่วงเวลาการทำงานของส่วนงานตามปกติเท่านั้น

(๒) การกำหนดช่วงเวลาสำหรับการเชื่อมต่อระบบเครือข่ายจากเครื่องปลายทาง จะต้องพิจารณาถึงระดับความเสี่ยงของที่ตั้งของเครื่องปลายทางด้วย

(๓) กำหนดให้ระบบสารสนเทศ เช่น ระบบงานที่มีความสำคัญสูง ระบบงานที่มีการใช้งานในสถานที่ที่มีความเสี่ยง (ในที่สาธารณะหรือพื้นที่ภายนอกสำนักงาน) เป็นต้น มีการจำกัดช่วงระยะเวลาการเชื่อมต่อ

๗.๑๐ การควบคุมการเข้าถึงโปรแกรมประยุกต์ หรือแอปพลิเคชันและสารสนเทศ (Application and Information Access Control)

๗.๑๐.๑ การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction)

ต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานและบุคลากรสถาบัน ในการเข้าถึงสารสนเทศและฟังก์ชัน (Functions) ต่าง ๆ ของโปรแกรมประยุกต์หรือแอปพลิเคชัน โดยให้กำหนดหลักเกณฑ์ในการจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานที่สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้ดังนี้

(๑) ผู้ดูแลระบบต้องกำหนดการลงทะเบียนประจำส่วนงานภายในสถาบัน ตามข้อกำหนดการลงทะเบียนผู้ใช้งานและการบริหารจัดการสิทธิของผู้ใช้งาน เพื่อควบคุมและจำกัดสิทธิการเข้าถึงระบบสารสนเทศและข้อมูลต่าง ๆ

(๒) ต้องจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศต่าง ๆ และหากไม่มีการใช้งานนานเกินระยะเวลาที่กำหนด ต้องยกเลิกการเชื่อมต่อระบบ

(๓) ผู้ให้บริการภายนอก (Outsource) ต้องลงนามในสัญญาการไม่เปิดเผยข้อมูลของส่วนงานภายในสถาบัน

(๔) ผู้ดูแลระบบต้องดำเนินการเพิกถอนหรือเปลี่ยนสิทธิการเข้าถึงระบบสารสนเทศของผู้ให้บริการภายนอก (Outsource) ที่สิ้นสุดการว่าจ้างโดยทันที

(๕) ผู้ดูแลระบบต้องควบคุมการเข้าถึงข้อมูลของผู้ให้บริการภายนอก (Outsource) ให้มีสิทธิเข้าถึงเฉพาะข้อมูลที่เกี่ยวข้อง และตรวจสอบการนำข้อมูลเข้าและออกจากระบบสารสนเทศของผู้ให้บริการภายนอก (Outsource) ทุกครั้ง

๗.๑๐.๒ ระบบที่ไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อสถาบัน

ต้องดำเนินการดังนี้

(๑) ต้องแยกระบบซึ่งไวต่อการรบกวนดังกล่าวออกจากระบบอื่น ๆ และแสดงให้เห็นถึงผลกระทบและระดับความสำคัญต่อส่วนงานภายในสถาบัน

(๒) ต้องประเมินความเสี่ยงสำหรับการใช้งานทรัพยากรร่วมกัน ระหว่างระบบงานอื่นที่มีความสำคัญน้อยกว่า

(๓) มีการควบคุมสภาพแวดล้อมของระบบดังกล่าวโดยเฉพาะ

(๔) มีการควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่จากการปฏิบัติงานภายนอกสถาบัน (Mobile Computing and Teleworking) ที่เกี่ยวข้องกับระบบดังกล่าว

๗.๑๐.๓ การควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ (Mobile Computing)

ต้องดำเนินการดังนี้

(๑) ต้องกำหนดรหัสผ่านที่มีความมั่นคงปลอดภัยสำหรับผู้ใช้งานอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่

(๒) ไม่อนุญาตให้บุคคลภายนอกสามารถเข้าถึงข้อมูลสำคัญหรือข้อมูลลับในอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่

(๓) เมื่อพบชุดคำสั่งไม่พึงประสงค์ในอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ให้ปฏิบัติตามข้อปฏิบัติในการป้องกันชุดคำสั่งไม่พึงประสงค์และที่เกี่ยวข้อง

(๔) ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ มิให้ถูกขโมยหรือสูญหาย โดยการล็อกเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะหรือในบริเวณที่มีความเสี่ยงต่อการสูญหายโดยทำการล็อกอุปกรณ์ไว้กับโต๊ะ หรือนำไปเก็บไว้ในตู้ที่สามารถล็อกได้ หรือวิธีการอื่นใดที่เหมาะสม

(๕) ต้องสำรองข้อมูลสำคัญที่อยู่ในอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่อย่างสม่ำเสมอ

(๖) ต้องมีการป้องกันการเชื่อมต่อของอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่เข้ากับเครือข่ายของส่วนงานโดยไม่ได้รับอนุญาต

๗.๑๐.๔ การปฏิบัติงานจากภายนอกสถาบัน (Teleworking)

ต้องดำเนินการดังนี้

(๑) ต้องเข้ารหัส (Encryption) ด้วย SSL, VPN, XML Encryption หรือวิธีการอื่นใดที่เป็นมาตรฐานสากล ในการสื่อสารข้อมูลระหว่างสถานที่ ที่จะมีการปฏิบัติงานจากภายนอกสถาบันและระบบงานต่าง ๆ ของส่วนงานภายในสถาบัน ทั้งนี้ให้มีความเหมาะสมกับรูปแบบการสื่อสารของข้อมูล

(๒) การเข้าถึงระบบสารสนเทศของส่วนงานจากระยะไกลด้วยอุปกรณ์ที่เป็นของส่วนตัวต้องได้รับอนุญาตจากสำนักบริหารข้อมูลดิจิทัล

(๓) การเปิดใช้งานระบบสารสนเทศให้สามารถปฏิบัติงานจากภายนอกสถาบันได้ ต้องมีหนังสือเป็นลายลักษณ์อักษรและมีความเห็นของผู้บังคับบัญชาตามลำดับชั้น และได้รับความเห็นชอบจากผู้อำนวยการสำนักบริหารข้อมูลดิจิทัล โดยต้องระบุรายละเอียด ดังต่อไปนี้

(๓.๑) เหตุผลความจำเป็นที่ต้องการให้สามารถปฏิบัติงานจากภายนอกสถาบัน

(๓.๒) รายละเอียด หรือลักษณะของระบบงาน

(๓.๓) ช่องทางที่ใช้ในการปฏิบัติงานจากภายนอก

(๓.๔) รายชื่อผู้ใช้งาน หรือกลุ่มผู้ใช้งาน

(๓.๕) ช่วงเวลาและระยะเวลาในการใช้ปฏิบัติงานจากภายนอกสถาบัน

(๔) ไม่อนุญาตให้ปฏิบัติงานจากภายนอกสถาบัน สำหรับระบบงานที่มีความลับชั้นลับชั้นลับมาก และชั้นลับมากที่สุด

(๕) การเข้าสู่ระบบสารสนเทศภายในสถาบันจากระยะไกล ต้องมีการลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน (Username) และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication)

ด้วยการใช้รหัสผ่าน (Password) หรือวิธีอื่นที่ส่วนงานกำหนด เพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนทุกครั้ง

(๖) ผู้ได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงระบบสารสนเทศและข้อมูลของสถาบันได้ โดยห้ามมิให้สมาชิกในครอบครัวหรือบุคคลใด ๆ ที่ไม่ได้รับอนุญาตเข้าถึงระบบสารสนเทศและข้อมูลของสถาบัน และสถาบันสงวนสิทธิในการระงับหรือยกเลิกสิทธิ หากพบว่าไม่ปฏิบัติตามนโยบายและระเบียบปฏิบัติที่เกี่ยวข้อง

(๗) ผู้ดูแลระบบต้องควบคุมช่องทาง (Port) ที่ใช้เข้าสู่ระบบอย่างรัดกุม และมีการเฝ้าระวังสม่ำเสมอเมื่อพบเหตุการณ์ผิดปกติต้องระงับการให้บริการทันที

(๘) การยกเลิกสิทธิในการปฏิบัติงานภายนอกสถาบัน ต้องมีหนังสือเป็นลายลักษณ์อักษรขอยกเลิกต่อผู้อำนวยการสำนักบริหารข้อมูลดิจิทัล ทันทีที่ครบระยะเวลา หรือเมื่อหมดความจำเป็นในการปฏิบัติงานจากภายนอกสถาบัน

(๙) ต้องทบทวนปรับปรุงสิทธิการอนุญาตให้ใช้ปฏิบัติงานจากภายนอกสถาบัน อย่างน้อยปีละ ๑ ครั้ง

๗.๑๐.๕ ผู้ดูแลระบบ (System Administrator)

ต้องดำเนินการดังต่อไปนี้

(๑) กำหนดการลงทะเบียนบุคลากรใหม่ของสถาบัน ควรกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการเพื่อให้มีสิทธิต่าง ๆ ในการใช้งานตามความจำเป็นรวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน เช่น การลาออก หรือการเปลี่ยนตำแหน่งงานภายในสถาบัน เป็นต้น

(๒) ต้องกำหนดสิทธิการใช้งานระบบสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

(๓) ต้องบริหารจัดการสิทธิการใช้งานระบบและรหัสผ่านของบุคลากรสถาบันดังต่อไปนี้

(๓.๑) กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบลาออก หรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน

(๓.๒) ส่งมอบรหัสผ่าน (Password) ชั่วคราวให้กับผู้ใช้บริการด้วยวิธีการที่ปลอดภัย ควรหลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (E-mail) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน (Password)

(๓.๓) กำหนดให้ผู้ใช้บริการตอบยืนยันการได้รับรหัสผ่าน (Password)

(๓.๔) กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

(๓.๕) กำหนดชื่อบัญชีผู้ใช้งาน (Account Name) และรหัสผ่าน (Password) ต้องไม่ซ้ำกัน

(๓.๖) ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิพิเศษที่ได้รับว่าสามารถเข้าถึงในระดับใดได้บ้าง และต้องกำหนดให้ชื่อบัญชีผู้ใช้งาน (Account Name) และรหัสผ่าน (Password) ที่มีความแตกต่างกันจากชื่อบัญชีผู้ใช้งาน (Account Name) และรหัสผ่าน (Password) ตามปกติ

(๔) ต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับ ในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้

(๔.๑) ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

(๔.๒) ต้องกำหนดรายชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล

(๔.๓) กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

(๔.๔) การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL VPN หรือ XML Encryption เป็นต้น

(๔.๕) กำหนดการเปลี่ยนรหัสผ่าน (Password) ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

(๔.๖) กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของส่วนงานภายในสถาบัน เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

นโยบายที่ ๘
นโยบายและแนวปฏิบัติการจัดหา พัฒนา และดูแลรักษาระบบสารสนเทศ
(System Acquisition, Development and Maintenance)

วัตถุประสงค์

๑. เพื่อให้กระบวนการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเป็นส่วนหนึ่งของระบบสารสนเทศตลอดช่วงอายุการใช้งานระบบสารสนเทศ (Entire Life Cycle) ได้แก่ กระบวนการจัดหา กระบวนการพัฒนาระบบ (System Development Life Cycle) การใช้งาน และการดูแลรักษา

๒. เพื่อให้มีการรักษาความมั่นคงปลอดภัยระบบสารสนเทศตลอดช่วงการพัฒนาระบบสารสนเทศ (System Development Life Cycle)

แนวทางปฏิบัติ

๘.๑ ต้องระบุข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสารสนเทศไว้เป็นส่วนหนึ่งของข้อกำหนดคุณสมบัติของระบบ เมื่อจัดให้มีระบบสารสนเทศใหม่หรือเมื่อปรับปรุงระบบเก่า

๘.๒ ต้องจัดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศที่ผ่านระบบให้บริการ การใช้งาน (Application Service) ทั้งในกรณีทั่วไปและกรณีที่ผ่านเครือข่ายสาธารณะ เพื่อป้องกัน การกระทำผิดในลักษณะทุจริต (Fraudulent Activities) การทำธุรกรรมที่ไม่สมบูรณ์หรือผิดพลาด (Incomplete Transmission or Mis-routing) หรือการเปิดเผย คัดลอก หรือเปลี่ยนแปลงแก้ไขข้อมูล โดยไม่ได้รับอนุญาต

๘.๓ ต้องจัดให้มีการควบคุมการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบสารสนเทศตลอดทุกขั้นตอนตามการควบคุมที่ได้กำหนดไว้ ได้แก่

(๑) มีการประเมินผลกระทบที่อาจเกิดขึ้นจากการเปลี่ยนแปลง

(๒) มีการกำหนดวิธีปฏิบัติให้คำขอให้แก้ไขหรือพัฒนาต้องมาจากผู้ที่มีสิทธิและอนุมัติคำขอ โดยผู้มีอำนาจต้องควบคุมผลข้างเคียงที่อาจเกิดขึ้นเนื่องจากมีการแก้ไข มีการตรวจรับจากผู้มีอำนาจภายหลังการแก้ไขหรือพัฒนาแล้วเสร็จก่อนโอนย้ายระบบงาน รวมทั้งมีการจัดเก็บรายละเอียดของคำขอไว้ เป็นต้น

๘.๔ กำหนดวิธีปฏิบัติในกรณีที่มีการแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ในกรณีฉุกเฉิน และบันทึกเหตุผลความจำเป็นและขออนุมัติจากผู้มีอำนาจทุกครั้ง

๘.๕ ปรับปรุงเอกสารประกอบระบบงานทั้งหมดหลังจากที่ได้มีการแก้ไขเปลี่ยนแปลง เพื่อให้ทันสมัยอยู่เสมอ เช่น เอกสารประกอบรายละเอียดโครงสร้างข้อมูล คู่มือระบบงาน ทะเบียนรายชื่อผู้มีสิทธิใช้งาน ขั้นตอนการทำงานของโปรแกรม และต้องจัดเก็บเอกสารดังกล่าวในที่ปลอดภัยและสะดวกต่อการใช้งาน เป็นต้น

๘.๖ จัดเก็บโปรแกรม Version ก่อนการเปลี่ยนแปลงไว้ใช้งาน หรือมีกระบวนการถอยกลับสู่สภาพเดิม (Roll-Back) ของระบบงาน ในกรณีระบบงานผิดพลาดหรือไม่สามารถใช้งานได้

๘.๗ มีการสื่อสารให้กับบุคคลที่เกี่ยวข้องได้รับทราบและสามารถปฏิบัติงานได้อย่างถูกต้อง

๘.๘ บันทึกและจัดเก็บหลักฐานทั้งหมด (Audit Trail) ที่เกี่ยวข้องกับการเปลี่ยนแปลง เพื่อใช้ประกอบในกรณีที่มีการตรวจสอบ

๘.๙ ต้องจัดให้มีการทดสอบระบบสารสนเทศที่ได้รับการพัฒนาหรือแก้ไขเปลี่ยนแปลง เพื่อให้มั่นใจว่าการทำงานมีประสิทธิภาพ การประมวลผลถูกต้องครบถ้วน และเป็นไปตามความต้องการของผู้ใช้งาน พร้อมทั้งปรับปรุงแผนบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Plan) ให้สอดคล้องกับการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบสารสนเทศดังกล่าว

๘.๑๐ ต้องควบคุมสภาพแวดล้อมของการพัฒนาระบบสารสนเทศ (Development Environment) ซึ่งได้แก่ บุคลากรผู้พัฒนาระบบ ขั้นตอนการพัฒนาระบบ และเทคโนโลยีสำหรับการพัฒนาระบบให้มีความมั่นคงปลอดภัยตลอดขั้นตอนการพัฒนาระบบ โดยคำนึงถึงรายละเอียดต่อไปนี้

(๑) การรักษาความลับของข้อมูลที่นำมาประมวลผล จัดเก็บ และส่งผ่านระบบ และการควบคุมการนำข้อมูลเข้าและออกจากระบบที่อยู่ระหว่างการพัฒนา

(๒) การควบคุมการเข้าถึงสภาพแวดล้อมของการพัฒนาระบบสารสนเทศอย่างรัดกุมเหมาะสม

(๓) การติดตามหากมีการเปลี่ยนแปลงสภาพแวดล้อมของการพัฒนาระบบสารสนเทศ

(๔) มีการจัดเก็บข้อมูลสำรองในพื้นที่นอกองค์กรที่มีความมั่นคงปลอดภัย

(๕) ต้องจัดให้มีการดูแล ติดตาม และควบคุมการปฏิบัติงานของผู้ให้บริการพัฒนาระบบงานสารสนเทศจากภายนอก (Outsourced System Development) ให้เป็นไปตามนโยบายการพัฒนาระบบงานสารสนเทศภายใต้ข้อตกลงที่ให้สิทธิกับสถาบันให้สามารถเข้าตรวจสอบการปฏิบัติงานดังกล่าวได้

(๖) ต้องจัดให้มีการทดสอบการทำงานของระบบที่ได้รับการพัฒนาโดยผู้ใช้งาน หรือผู้ทดสอบอื่นที่เป็นอิสระจากผู้พัฒนาระบบสารสนเทศดังกล่าว เพื่อให้มั่นใจได้ว่าระบบที่ได้รับการพัฒนาดังกล่าวสามารถทำงานได้ถูกต้องตรงความต้องการของผู้ใช้งาน และเป็นไปตามนโยบายด้านความมั่นคงปลอดภัยของระบบสารสนเทศ ทั้งนี้ ควรระมัดระวังโดยจัดให้มีแนวทางควบคุมและป้องกันการรั่วไหลของข้อมูลที่ใช้ในการทดสอบหากข้อมูลดังกล่าวเป็นความลับหรือมีความสำคัญ

(๗) ควรมีการทดสอบโปรแกรมระบบ (System Software) เกี่ยวกับการรักษาความปลอดภัยและประสิทธิภาพ การใช้งานโดยทั่วไปก่อนติดตั้งและหลังจากการแก้ไขหรือบำรุงรักษา

นโยบายที่ ๙
นโยบายและแนวปฏิบัติการบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ
(Information Security Incident Management)

วัตถุประสงค์

เพื่อให้เหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยของระบบสารสนเทศได้รับการดำเนินการอย่างถูกต้อง มีประสิทธิภาพในช่วงระยะเวลาที่เหมาะสม

แนวทางปฏิบัติ

๙.๑ สถาบันต้องจัดให้มีขั้นตอนและกระบวนการบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ รวมทั้งกำหนดผู้มีหน้าที่รับผิดชอบซึ่งมีความรู้ความสามารถและประสบการณ์ โดยขั้นต่ำต้องมีการกำหนดขั้นตอนและกระบวนการดังต่อไปนี้

(๑) การกำหนดแผนรองรับในกรณีที่เกิดเหตุการณ์อย่างเป็นลายลักษณ์อักษร

(๒) การประเมินเหตุการณ์หรือจุดอ่อนของมาตรการรักษาความมั่นคงปลอดภัยระบบสารสนเทศและพิจารณาว่าควรจัดเป็นเหตุการณ์ที่มีระดับความรุนแรง ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ

(๓) จัดให้มีบุคคลหรือส่วนงานเพื่อทำหน้าที่รับแจ้งเหตุการณ์ (Point of Contact) และรายงานเหตุการณ์ต่อคณะผู้บริหารหรือผู้เกี่ยวข้องให้ทราบและดำเนินการต่อไป (Escalation)

(๔) การดำเนินการเพื่อตอบสนองต่อเหตุการณ์ที่เกิดขึ้นอย่างมีประสิทธิภาพ เพื่อทำให้เหตุการณ์คลี่คลายหรือกลับสู่ภาวะปกติอย่างรวดเร็ว

(๕) การรวบรวมและจัดเก็บหลักฐานทันทีที่เกิดเหตุการณ์ที่ส่งผลกระทบต่อระบบสารสนเทศที่มีความสำคัญอย่างมีนัยสำคัญ อาจก่อให้เกิดความเสียหายกับข้อมูลหรือสินทรัพย์ของผู้ใช้งาน ผู้ใช้บริการหรือเจ้าของข้อมูล (Data Owner) โดยต้องคำนึงถึงประเด็นสำคัญต่าง ๆ เช่น กระบวนการการจัดเก็บอย่างมั่นคงปลอดภัย การกำหนดหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้อง การคัดเลือกบุคคลที่มีความรู้ความสามารถหรือมีประสบการณ์ด้านการรวบรวมและจัดเก็บหลักฐาน เพื่อวิเคราะห์ตรวจสอบและจัดทำเอกสารสรุปนำเสนอต่อบุคคลที่มีหน้าที่รับผิดชอบ เป็นต้น ทั้งนี้ การรวบรวม จัดเก็บ และนำเสนอหลักฐานต้องสอดคล้องกับหลักเกณฑ์ของกฎหมายที่ใช้บังคับ

(๖) การบันทึกและจัดเก็บหลักฐานการบริหารจัดการทุกขั้นตอน

(๗) การรายงานให้ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงรับทราบถึงสถานการณ์และผลการบริหารจัดการ

(๘) การตรวจหา ติดตาม วิเคราะห์ และรายงานเหตุการณ์ ทั้งนี้ ให้รวมถึงการวิเคราะห์ภายหลังเหตุการณ์ยุติแล้ว เพื่อระบุถึงสาเหตุของเหตุการณ์และเพื่อใช้ประโยชน์จากผลการวิเคราะห์ในการเตรียมความพร้อมรองรับเหตุการณ์ที่อาจเกิดขึ้นได้อีกในอนาคต

๙.๒ สถาบันต้องจัดให้มีการรายงานสถานการณ์ที่เกิดขึ้นอย่างรวดเร็วและทันต่อเหตุการณ์ผ่านบุคคลหรือส่วนงานที่ทำหน้าที่รับแจ้งเหตุการณ์ (Point of Contact) โดยให้ดำเนินการดังนี้

(๑) จัดทำแบบฟอร์มที่เป็นมาตรฐานเพื่อรองรับการรายงานสถานการณ์ และสร้างความเข้าใจให้กับผู้รายงานเกี่ยวกับการดำเนินการต่าง ๆ ที่จำเป็นในกรณีที่เกิดเหตุการณ์ ทั้งนี้ เนื้อหาขั้นต่ำต้องประกอบด้วย วันเวลา เหตุการณ์ ผลกระทบที่คาดว่าจะเกิดขึ้น การดำเนินการแก้ไข ผลการแก้ไข ระยะเวลาในการแก้ไข สาเหตุที่เกิดปัญหา และแนวทางการป้องกันในอนาคต

(๒) รายงานผู้บริหารเทคโนโลยีสารสนเทศระดับสูงเมื่อทราบเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัย เช่น พบช่องโหว่ในการควบคุมความมั่นคงปลอดภัย (Ineffective Security Control) เกิดเหตุการณ์ ที่อาจส่งผลกระทบต่อการรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของระบบสารสนเทศ ข้อผิดพลาดจากการปฏิบัติงาน (Human Errors) การบุกรุกด้านกายภาพ (Breaches of Physical Security Arrangements) การปฏิบัติงานที่ไม่เป็นไปตามนโยบายด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ (Non-Compliances with Policies) การเปลี่ยนแปลงระบบปฏิบัติการหรือชุดคำสั่งที่ควบคุมระบบงานโดยไม่ได้รับอนุญาต (Uncontrolled System Changes) การทำงานผิดพลาดของโปรแกรมและอุปกรณ์คอมพิวเตอร์ (Malfunctions of Software or Hardware) และการเข้าถึงโดยไม่ได้รับอนุญาต (Access Violations)

(๓) รายงานผู้บริหารเทคโนโลยีสารสนเทศระดับสูงเมื่อเกิดเหตุการณ์ที่ส่งผลกระทบต่อระบบสารสนเทศที่มีความสำคัญ ประเภทดังต่อไปนี้

(๓.๑) ระบบหยุดชะงัก (System Disruption)

(๓.๒) มีการบุกรุก เข้าถึง หรือใช้งานระบบโดยไม่ได้รับอนุญาต (System Compromised)

(๓.๓) ส่งผลกระทบต่อชื่อเสียงของสถาบัน (Harm to Reputation) เช่น ถูกปลอมแปลงหน้าเว็บไซต์ของสถาบัน (Website Defacement) เป็นต้น

(๔) รายงานทันทีเมื่อทราบเหตุการณ์ โดยมีเนื้อหาครอบคลุมถึง วันเวลา ประเภทเหตุการณ์ เหตุการณ์และผลกระทบที่คาดว่าจะเกิดขึ้น ทั้งนี้ อาจแจ้งโดยวาจาหรือแจ้งผ่านระบบรับส่งข้อความผ่านทางอิเล็กทรอนิกส์ (Electronic Messaging) ตามความเหมาะสม

(๕) รายงานภายในวันทำการถัดไปหลังทราบเหตุการณ์เป็นลายลักษณ์อักษร โดยมีเนื้อหาครอบคลุมถึงวันเวลา ประเภทเหตุการณ์ เหตุการณ์และผลกระทบที่เกิดขึ้น การดำเนินการแก้ไขปัญหาและความคืบหน้าในการแก้ไขปัญหา

(๖) รายงานเมื่อเหตุการณ์ยุติหรือแก้ไขปัญหาแล้วเสร็จเป็นลายลักษณ์อักษร โดยมีเนื้อหาครอบคลุมถึงวันเวลา ประเภทเหตุการณ์ เหตุการณ์และผลกระทบที่เกิดขึ้น การดำเนินการแก้ไขปัญหา ผลการแก้ไขปัญหา ระยะเวลาในการแก้ไข สาเหตุที่เกิดปัญหา และแนวทางป้องกันในอนาคต

(๗) แจ้งบุคคลที่เกี่ยวข้องรับทราบโดยไม่ชักช้า ในกรณีที่เหตุการณ์ส่งผลกระทบต่อบุคคล

นโยบายที่ ๑๐

นโยบายและแนวปฏิบัติการบริหารความต่อเนื่องทางธุรกิจในด้านความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security Aspects of Business Continuity Management)

วัตถุประสงค์

เพื่อให้การรักษาความมั่นคงปลอดภัยระบบสารสนเทศเป็นส่วนหนึ่งของการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management) ของสถาบัน ทั้งนี้ เพื่อให้ระบบสารสนเทศอยู่ในสภาพที่พร้อมใช้งานอยู่เสมอ

แนวทางปฏิบัติ

๑๐.๑ การบริหารความต่อเนื่องทางธุรกิจ

๑๐.๑.๑ เจ้าหน้าที่ทุกคนต้องคำนึงถึงความมั่นคงปลอดภัยของระบบสารสนเทศเมื่อเกิดสถานการณ์ที่ไม่พึงประสงค์หรือไม่คาดคิด

๑๐.๑.๒ การจัดทำแผนบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management) มอบหมายให้บุคลากรที่เกี่ยวข้องดำเนินการดังต่อไปนี้

(๑) กำหนดกระบวนการในการวางแผนรับมือกับเหตุภัยพิบัติสำหรับระบบที่มีความสำคัญสูง

(๒) กำหนดชนิดของภัยพิบัติที่มีผลต่อระบบที่มีความสำคัญสูงและจำเป็นต้องวางแผนรับมือ

(๓) ทำการประเมินความเสี่ยงที่มีผลทำให้ระบบที่มีความสำคัญสูงติดขัด หรือไม่สามารถใช้งานได้อันเป็นผลจากภัยพิบัติที่กำหนดไว้

(๔) จัดทำแผนรับมือกับเหตุภัยพิบัติสำหรับระบบที่มีความสำคัญสูง

(๕) ทดสอบ ประเมิน และปรับปรุงแผนรับมือกับเหตุภัยพิบัติสำหรับระบบที่มีความสำคัญสูงอย่างน้อยปีละ ๑ ครั้ง

(๖) จัดให้มีการอบรมให้ความรู้และซักซ้อมแผนฉุกเฉินภัยพิบัติของระบบสารสนเทศ (IT Contingence Plan) อย่างน้อยปีละ ๑ ครั้ง

๑๐.๑.๓ สถาบันต้องจัดให้มีขั้นตอน กระบวนการดำเนินการ และการควบคุมด้านความมั่นคงปลอดภัยของระบบสารสนเทศ เพื่อให้มั่นใจได้ว่ามีความสอดคล้องกับแผนบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management)

๑๐.๑.๔ สถาบันต้องจัดให้มีระบบสารสนเทศและระบบสำรองของสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งาน

๑๐.๑.๕ จัดให้มีรายชื่อบุคคลและช่องทางสำหรับติดต่อ (Contact Person) ของผู้ดูแลรับผิดชอบประจำส่วนงานภายในสถาบัน และหน่วยงานภายนอกผู้ให้บริการที่สนับสนุนการทำงานระบบสารสนเทศของสถาบัน เพื่อให้สามารถติดต่อประสานงาน หรือขอความช่วยเหลือในกรณีเกิดเหตุการณ์ที่ส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ พร้อมทั้งปรับปรุงรายชื่อและช่องทางสำหรับติดต่อดังกล่าวให้เป็นปัจจุบัน

๑๐.๒ การสำรองข้อมูลและสารสนเทศ

๑๐.๒.๑ ต้องพิจารณาคัดเลือกระบบสารสนเทศที่สำคัญและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน ตามแนวทางต่อไปนี้

๑๐.๒.๒ มีการจัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของส่วนงานพร้อมทั้งกำหนดระบบสารสนเทศที่จะจัดทำระบบสำรอง และจัดทำระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง

๑๐.๒.๓ กำหนดให้มีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบ และกำหนดความถี่ในการสำรองข้อมูล หากระบบใดที่มีการเปลี่ยนแปลงบ่อยควรกำหนดให้มีความถี่ในการสำรองข้อมูลมากขึ้น โดยให้มีวิธีการสำรองข้อมูล ดังนี้

(๑) สถาบันต้องกำหนดระยะเวลาในการกลับคืนสู่สภาพการดำเนินงานปกติของระบบสารสนเทศ (Recovery Time Objectives : RTO) พร้อมทั้งจัดลำดับการกู้คืนระบบงานสารสนเทศที่มีความสำคัญทุกระบบให้เหมาะสมกับผลกระทบที่อาจเกิดขึ้น ทั้งนี้ ระยะเวลาในการกู้คืนดังกล่าวต้องปฏิบัติได้อย่างมีประสิทธิภาพ

(๒) สถาบันต้องกำหนดเป้าหมายในการกู้คืนข้อมูล เช่น กำหนดประเภทของข้อมูล และชุดข้อมูลล่าสุดที่จะกู้คืนได้ (Recovery Point Objective : RPO) และจัดให้มีแผนการการสำรองข้อมูลและระบบสารสนเทศเพื่อให้อยู่ในสภาพพร้อมใช้งานหรือสอดคล้องกับ RTO

(๓) ผู้ดูแลระบบคอมพิวเตอร์ต้องจัดให้มีการสำรองและทดสอบข้อมูลที่สำรองเก็บไว้อย่างสม่ำเสมอ

(๔) การจัดทำบันทึกการสำรองข้อมูล (Operator Logs) ผู้ดูแลระบบคอมพิวเตอร์ต้องทำบันทึกรายละเอียดการสำรองข้อมูล ได้แก่ เวลาเริ่มต้นและสิ้นสุด ชื่อผู้สำรอง ชนิดของข้อมูลที่บันทึก

(๕) การรายงานข้อผิดพลาด (Fault Logging) ผู้ดูแลระบบคอมพิวเตอร์ต้องทำรายงานข้อผิดพลาดจากการสำรองข้อมูลที่เกิดขึ้น รวมทั้งวิธีการที่ใช้แก้ไขด้วย

(๖) ให้ผู้ดูแลระบบคอมพิวเตอร์มอบหมายหน้าที่การสำรองข้อมูลแก่เจ้าหน้าที่คนอื่นไว้สำรองในกรณีที่ผู้ดูแลระบบคอมพิวเตอร์ หรือผู้ดูแลระบบเครือข่ายไม่สามารถปฏิบัติงานได้

(๗) ในกรณีที่พบปัญหาในการสำรองข้อมูลจนเป็นเหตุไม่สามารถดำเนินการอย่างสมบูรณ์ได้ ให้ดำเนินการแก้ไขปัญหาและสรุปผลการแก้ไขปัญหา และรายงานต่อหัวหน้ากลุ่มเทคโนโลยีสารสนเทศ

(๘) ให้ผู้ดูแลระบบคอมพิวเตอร์และผู้ดูแลระบบเครือข่ายกำหนดชนิดและช่วงเวลาการสำรองข้อมูลตามความเหมาะสม พร้อมทั้งกำหนดสื่อที่ใช้เก็บข้อมูล โดยรูปแบบการสำรองข้อมูลมีสองชนิด คือ การสำรองข้อมูลแบบเต็ม (Full Backup) และการสำรองข้อมูลแบบส่วนต่าง (Incremental Backup)

(๙) การเข้ารหัสข้อมูลสำคัญในการสำรองข้อมูล (Encrypted Backup) ผู้ดูแลระบบคอมพิวเตอร์ต้องจัดให้มีการเข้ารหัสข้อมูลสำรองที่สำคัญ โดยการใช้เทคโนโลยีการเข้ารหัสที่เหมาะสมเพื่อป้องกันมิให้ข้อมูลสำรองเหล่านั้นถูกเปิดเผย

๑๐.๓ การกู้คืนระบบ

ต้องมีขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ ดังนี้

๑๐.๓.๑ ผู้ดูแลระบบต้องบันทึกการกู้คืนระบบทุกครั้งที่มีการกู้คืนระบบ และรายงานให้ผู้บังคับบัญชาทราบ โดยมีรายละเอียดดังนี้

(๑) มีการกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ

(๒) มีการกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูล และทดสอบกู้คืนข้อมูลที่สำรองไว้

๑๐.๓.๒ ผู้ดูแลระบบต้องทำการแก้ไขหากเกิดปัญหารวมถึงรายงานผู้บังคับบัญชาถึงปัญหาและวิธีการแก้ไขการกู้คืนระบบ

๑๐.๓.๓ ผู้ดูแลระบบต้องทำการกู้คืนระบบโดยใช้ข้อมูลสำรองที่ทันสมัยที่สุด (Last update) ที่ได้สำรองไว้

๑๐.๓.๔ จัดเก็บสื่อบันทึกข้อมูลสำรอง พร้อมทั้งสำเนาขั้นตอนหรือวิธีปฏิบัติต่าง ๆ ไว้นอกสถานที่เพื่อความปลอดภัยในกรณีที่สถานที่ปฏิบัติงานได้รับความเสียหาย โดยสถานที่ดังกล่าวต้องจัดให้มีระบบควบคุมการเข้าออกและระบบป้องกันความเสียหายตามที่กล่าวในหัวข้อการสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อมด้วย

๑๐.๓.๕ จัดให้มีการทดสอบข้อมูลสำรองและกระบวนการกู้คืนข้อมูล อย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าข้อมูลรวมทั้งโปรแกรมระบบทั้งหมดที่ได้สำรองไว้ มีความถูกต้องครบถ้วนและสามารถใช้งานได้ภายในระยะเวลาที่กำหนด

๑๐.๓.๖ ต้องมีการซักซ้อมการกู้คืนระบบ อย่างน้อยระบบละ ๑ ครั้งต่อปี

๑๐.๔ การจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน

ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง และต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสม และสอดคล้องกับการใช้งานตามภารกิจ โดยมีรายละเอียดอย่างน้อยดังนี้

๑๐.๔.๑ มีการกำหนดหน้าที่และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด

๑๐.๔.๒ มีการประเมินสถานการณ์ความเสี่ยงสำหรับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบสารสนเทศที่มีความสำคัญ และกำหนดมาตรการเพื่อลดความเสี่ยงเหล่านั้น

๑๐.๔.๓ มีการกำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอกเมื่อเกิดเหตุจำเป็นฉุกเฉิน เช่น ผู้ให้บริการเครือข่าย ฮาร์ดแวร์ ซอฟต์แวร์ เป็นต้น

๑๐.๔.๔ ต้องมีการทดสอบสภาพความพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมความพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง

๑๐.๔.๕ มีการทบทวนระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมความพร้อมกรณีฉุกเฉินที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละส่วนงาน อย่างน้อยปีละ ๑ ครั้ง

๑๐.๔.๖ สร้างความตระหนักและให้ความรู้แก่เจ้าหน้าที่ผู้ที่เกี่ยวข้องเพื่อให้ทราบขั้นตอนการปฏิบัติสิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน หรือความรู้อื่นใดในการเตรียมความพร้อมกรณีฉุกเฉิน

นโยบายที่ ๑๑
นโยบายและแนวปฏิบัติการควบคุมกระบวนการทำงานให้เป็นไปตามข้อกำหนด (Compliance)

วัตถุประสงค์

๑. เพื่อป้องกันการละเมิดกฎหมาย หลักเกณฑ์ของทางการ และข้อกำหนดตามสัญญาต่าง ๆ ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ

๒. เพื่อให้การบริหารจัดการความมั่นคงปลอดภัยของระบบสารสนเทศเป็นไปตามนโยบายและหลักปฏิบัติของสถาบัน รวมทั้งมาตรฐานสากลด้านความมั่นคงปลอดภัยของระบบสารสนเทศ

แนวทางปฏิบัติ

๑๑.๑ สถาบันต้องระบุกฎหมาย หลักเกณฑ์ของภาครัฐและข้อกำหนดตามสัญญาต่าง ๆ ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ โดยจัดทำเป็นเอกสารและปรับปรุงให้เป็นปัจจุบันอย่างสม่ำเสมอ

๑๑.๒ สถาบันต้องกำหนดขั้นตอนปฏิบัติงาน เพื่อให้มั่นใจว่าในการใช้งานข้อมูลสารสนเทศที่อาจถือเป็นทรัพย์สินทางปัญญา หรือการใช้งานซอฟต์แวร์ที่พัฒนาโดยสถาบันมีความสอดคล้องกับกฎหมายและข้อกำหนดตามสัญญาต่าง ๆ

๑๑.๓ สถาบันต้องป้องกันมิให้ข้อมูลบันทึกหลักฐาน (Logs) ต่าง ๆ เกิดความเสียหาย สูญหาย เปลี่ยนแปลงแก้ไข เข้าถึงหรือเผยแพร่โดยไม่ได้รับอนุญาต โดยให้สอดคล้องกับกฎหมาย ข้อกำหนดตามสัญญาต่าง ๆ และความต้องการทางธุรกิจ

๑๑.๔ สถาบันต้องจัดให้มีการคุ้มครองข้อมูลส่วนบุคคล (PDPA) โดยต้องได้รับความยินยอมจากเจ้าของข้อมูล (Data Owner) รวมทั้งให้มีความสอดคล้องกับกฎหมาย หลักเกณฑ์ของภาครัฐและข้อกำหนดตามสัญญาต่าง ๆ

๑๑.๕ สถาบันต้องควบคุมการเข้ารหัสข้อมูลให้สอดคล้องกับกฎหมาย หลักเกณฑ์ของภาครัฐและข้อกำหนดตามสัญญาต่าง ๆ

๑๑.๖ สถาบันต้องจัดให้มีการตรวจสอบขั้นตอนและการปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศให้เป็นไปตามนโยบายด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ โดยผู้ตรวจสอบที่เป็นอิสระจากการบริหารจัดการความมั่นคงปลอดภัยของระบบสารสนเทศ ซึ่งอาจเป็นส่วนงานตรวจสอบภายในของสถาบัน หรือผู้ตรวจสอบภายนอก อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีเหตุการณ์ที่มีนัยสำคัญ

๑๑.๗ สถาบันต้องจัดให้มีการทบทวนและปรับปรุงขั้นตอนและการปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศให้เป็นไปตามนโยบายด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศและสอดคล้องกับมาตรฐานสากลด้านความมั่นคงปลอดภัยของระบบสารสนเทศ

๑๑.๘ สถาบันต้องจัดให้มีการทบทวนระบบสารสนเทศในด้านเทคนิค เช่น การทดสอบการบุกรุกระบบ (Penetration Test) อย่างสม่ำเสมอ เพื่อให้สอดคล้องกับนโยบายด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ และมาตรฐานสากลด้านความมั่นคงปลอดภัยของระบบสารสนเทศ เป็นต้น

นโยบายที่ ๑๒
นโยบายและแนวปฏิบัติการใช้งานระบบสารสนเทศอย่างปลอดภัย
(Information System Secure Usage)

วัตถุประสงค์

๑. เพื่อให้มั่นใจว่าการใช้งานของผู้ใช้งานจะไม่ส่งผลกระทบต่อระบบสารสนเทศ

๒. เพื่อให้มั่นใจว่าระบบสารสนเทศได้รับการป้องกันภัยคุกคามจากชุดคำสั่งไม่พึงประสงค์

๓. เพื่อกำหนดมาตรการรักษาความมั่นคงปลอดภัยสำหรับการปฏิบัติงานขององค์กรจากระยะไกล รวมทั้งการใช้งานอุปกรณ์คอมพิวเตอร์ประเภทพกพา

แนวทางปฏิบัติ

๑๒.๑ ข้อกำหนดในการใช้งานระบบสารสนเทศอย่างปลอดภัย ให้ปฏิบัติดังนี้

๑๒.๑.๑ กำหนดให้เครื่องคอมพิวเตอร์ทุกเครื่องที่มีการใช้งานภายในสถาบันต้องติดตั้งโปรแกรมช่วยตรวจสอบชุดคำสั่งไม่พึงประสงค์ และตั้งค่าให้มีการ Update อย่างสม่ำเสมอ โดยโปรแกรมช่วยตรวจสอบชุดคำสั่งไม่พึงประสงค์ที่ใช้งานอาจเป็นซอฟต์แวร์ที่สามารถใช้งานฟรี หรือมีการจัดหาในรูปแบบอื่น ๆ ได้

๑๒.๑.๒ กำหนดให้มีการฝึกอบรมให้ผู้ใช้งานมีความรู้พื้นฐานในการใช้ระบบสารสนเทศอย่างปลอดภัย และตระหนักรู้ถึงการใช้งานระบบสารสนเทศอย่างปลอดภัยอย่างสม่ำเสมอ

๑๒.๑.๓ ผู้ใช้งานต้องไม่ติดตั้งซอฟต์แวร์อื่น ๆ ภายในเครื่องคอมพิวเตอร์โดยไม่มีการตรวจสอบและได้รับอนุญาตจากผู้ดูแลระบบ

๑๒.๑.๔ การใช้งานอุปกรณ์จัดเก็บข้อมูลแบบพกพาเพื่อการจัดเก็บและถ่ายโอนข้อมูลจากเครื่องหนึ่งไปยังอีกเครื่องหนึ่งต้องตรวจสอบให้มั่นใจว่าอุปกรณ์จัดเก็บข้อมูลแบบพกพานั้นปลอดภัยจากชุดคำสั่งไม่พึงประสงค์ก่อน

๑๒.๑.๕ กำหนดให้ผู้ใช้งานจะต้องสำรองข้อมูลของตนเองอย่างสม่ำเสมอ

๑๒.๑.๖ ผู้ใช้งานจะต้องไม่กระทำความผิดตามลักษณะการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

๑๒.๒ ข้อกำหนดในการป้องกันชุดคำสั่งไม่พึงประสงค์ ให้ปฏิบัติดังนี้

๑๒.๒.๑ สถาบันต้องมีกลไกในการป้องกันและตรวจสอบชุดคำสั่งไม่พึงประสงค์ รวมทั้งแก้ไขเพื่อให้ระบบกลับมาใช้งานได้ตามปกติ (Recovery) โดยขั้นต่ำต้องกำหนดมาตรการ ดังนี้

(๑) กำหนดนโยบายห้ามใช้ซอฟต์แวร์ที่ไม่ได้รับอนุญาต

(๒) มีกระบวนการป้องกันและตรวจสอบการใช้ซอฟต์แวร์ที่ไม่ได้รับอนุญาต และการใช้งานเว็บไซต์ที่อาจมีชุดคำสั่งไม่พึงประสงค์

(๓) ติดตั้งซอฟต์แวร์ตรวจสอบชุดคำสั่งไม่พึงประสงค์และปรับปรุงให้เป็นปัจจุบันอย่างสม่ำเสมอ พร้อมทั้งกำหนดผู้มีหน้าที่รับผิดชอบให้รายงานและแก้ไขปัญหากรณีพบภัยคุกคาม

(๔) ตรวจสอบซอฟต์แวร์ระบบงานที่มีความสำคัญอย่างสม่ำเสมอ หากพบการติดตั้งหรือเปลี่ยนแปลงที่ไม่ได้รับอนุญาตต้องมีการตรวจสอบโดยผู้ดูแลระบบงาน

(๕) จัดให้มีการติดตามและกลั่นกรองข่าวสารเกี่ยวกับภัยคุกคาม เพื่อให้ทราบข้อเท็จจริง รวมทั้งแจ้งให้ผู้ที่เกี่ยวข้องได้ตระหนักถึงภัยคุกคามดังกล่าว

๑๒.๓ ข้อกำหนดในการปฏิบัติงานขององค์กรในระยะไกล ให้ปฏิบัติดังนี้

๑๒.๓.๑ ในกรณีการใช้อุปกรณ์คอมพิวเตอร์ประเภทพกพาสำหรับการปฏิบัติงานที่มีการเชื่อมต่อกับระบบงานภายในองค์กร สถาบันต้องมีมาตรการป้องกันข้อมูลสารสนเทศที่สำคัญ โดยพิจารณาถึงแนวทางดังต่อไปนี้

(๑) กำหนดให้มีการลงทะเบียนอุปกรณ์คอมพิวเตอร์ประเภทพกพา เช่น ยี่ห้อ รุ่นระบบปฏิบัติการ รหัสประจำเครื่อง (Serial Number) หมายเลขอ้างอิงอุปกรณ์เครือข่าย (MAC Address) เป็นต้น อย่างน้อยปีละ ๑ ครั้ง และเมื่อมีการเปลี่ยนอุปกรณ์เพื่อให้มั่นใจได้ว่าการใช้งานอุปกรณ์ดังกล่าว มีความสอดคล้องเป็นไปตามนโยบายด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ

(๒) มีมาตรการป้องกันข้อมูลที่เป็นความลับหรือมีความสำคัญ (Sensitive Data) กรณีที่อุปกรณ์คอมพิวเตอร์ประเภทพกพาสูญหาย เช่น การกำหนดให้ใส่รหัสผ่านก่อนใช้งานอุปกรณ์ (Lock Screen) หรือการลบข้อมูลจากระยะไกล (Remote Wipe-Out) เป็นต้น

(๓) กำหนดประเภทบริการการใช้งาน (Application Service) ที่อนุญาตให้ใช้งานผ่านอุปกรณ์คอมพิวเตอร์ประเภทพกพา และกำหนดมาตรการควบคุมการเข้าถึงบริการการใช้งานดังกล่าวโดยคำนึงถึงความปลอดภัยของการเชื่อมต่อกับเครือข่าย เช่น จำกัดให้เข้าถึงบริการการใช้งานบางประเภทหากเป็นการเชื่อมต่อกับเครือข่ายภายนอก เป็นต้น

(๔) จัดให้มีการเข้ารหัสข้อมูลสารสนเทศที่สำคัญบนอุปกรณ์พกพาและที่รับส่งผ่านระบบเครือข่ายคอมพิวเตอร์

(๕) จัดให้มีการอบรมผู้ใช้งานเพื่อตระหนักและทราบถึงความเสี่ยงจากการใช้งาน และแนวทางการควบคุมความเสี่ยงดังกล่าว

(๖) ควบคุมให้มีการติดตั้งเฉพาะซอฟต์แวร์ที่ถูกต้องตามลิขสิทธิ์ และโปรแกรมเพื่อปิดช่องโหว่ (Patches) ที่เหมาะสม

(๗) กำหนดมาตรการป้องกันชุดคำสั่งไม่พึงประสงค์ (Malware)

(๘) จัดให้มีการดำเนินการเพื่อลดผลกระทบเมื่อเกิดเหตุการณ์ที่ส่งผลกระทบต่อความมั่นคงปลอดภัยของข้อมูลสารสนเทศ เช่น ตัดการเชื่อมต่อโดยทันทีที่ทราบเหตุ เป็นต้น

๑๒.๓.๒ ในกรณีที่มีการปฏิบัติงานขององค์กรจากระยะไกล (Teleworking Site) สถาบันต้องกำหนดมาตรการรักษาความมั่นคงปลอดภัยที่รัดกุมเพียงพอสำหรับข้อมูลสารสนเทศที่ถูกเข้าถึง ประมวลผล และจัดเก็บในพื้นที่ปฏิบัติงาน โดยพิจารณาถึงรายละเอียดดังนี้

(๑) การกำหนดมาตรการรักษาความมั่นคงปลอดภัยด้านกายภาพที่เหมาะสม รัดกุมเพียงพอสำหรับพื้นที่ปฏิบัติงานนอกองค์กร

(๒) การควบคุมสิทธิการใช้งานและการเข้าถึงข้อมูลสารสนเทศของผู้ใช้งานอย่างเหมาะสม

(๓) การรักษาความมั่นคงปลอดภัยกรณีมีการเชื่อมต่อระบบงานที่สำคัญ หรือรับส่งข้อมูลที่เป็นความลับหรือมีความสำคัญจากระยะไกล (Remote Access)

(๔) การป้องกันการรั่วไหลของข้อมูลสารสนเทศในกรณีใช้เทคโนโลยี Virtual Desktop

(๕) การป้องกันการเข้าถึงข้อมูลสารสนเทศจากบุคคลที่ไม่มีสิทธิในการใช้งาน เช่น ญาติพี่น้องและเพื่อน เป็นต้น

(๖) มีวิธีการในการตรวจสอบความมั่นคงปลอดภัยของอุปกรณ์คอมพิวเตอร์ส่วนตัวของพนักงานในพื้นที่ปฏิบัติงานนอกองค์กร

(๗) การป้องกันชุดคำสั่งไม่พึงประสงค์

นโยบายที่ ๑๓
นโยบายและแนวปฏิบัติการใช้งานระบบคลาวด์
(Cloud Computing Usage)

วัตถุประสงค์

เพื่อเสริมสร้างความมั่นคงปลอดภัยในระบบสารสนเทศเมื่อมีการติดตั้ง และใช้งานระบบสารสนเทศโดยมีการเช่าใช้งานระบบ Cloud Computing จากผู้ให้บริการจากภายนอก

แนวทางปฏิบัติ

๑๓.๑ การใช้งานระบบ Cloud Computing

๑๓.๑.๑ มีการประเมินความเสี่ยงเกี่ยวกับการใช้บริการ Cloud Computing อย่างสม่ำเสมอ

๑๓.๑.๒ ต้องมีการกำหนดประเภทงานที่จะใช้บริการ Cloud Computing อย่างชัดเจน

๑๓.๑.๓ กำหนดรูปแบบของการใช้บริการ เช่น Software as a Service (SaaS), Platform as a Service (PaaS) และ Infrastructure as a Service (IaaS) เป็นต้น

๑๓.๑.๔ ในการคัดเลือกและประเมินผู้ให้บริการ (Due Diligence) ผู้ให้บริการต้องมีมาตรฐานการรับรองความมั่นคงปลอดภัยด้านสารสนเทศในระดับสากล เช่น ได้รับมาตรฐาน ISO ๒๗๐๐๑ เป็นอย่างน้อย เป็นต้น

๑๓.๑.๕ มีการทบทวนคุณสมบัติของผู้ให้บริการอย่างสม่ำเสมอเพื่อประเมินความพร้อมในการให้บริการโดยคุณสมบัติที่ต้องมีการทบทวน เช่น ฐานะทางการเงิน ความเพียงพอของการให้บริการ (Capacity Planning) เพื่อให้มั่นใจได้ว่าผู้ให้บริการจะสามารถให้บริการได้อย่างต่อเนื่องและเพียงพอกับความต้องการของสถาบัน เป็นต้น

๑๓.๑.๖ ข้อมูลแต่ละประเภทที่มีการใช้งานใน Cloud จะต้องมีการกำหนดความปลอดภัย โดยแบ่งชั้นความลับของข้อมูล และกำหนดวิธีปฏิบัติแต่ละระดับชั้นความลับของข้อมูล

๑๓.๑.๗ กำหนดเงื่อนไขสำหรับผู้ให้บริการในการเข้าถึงและเปิดเผยข้อมูลของสถาบัน

๑๓.๑.๘ กำหนดบทบาทหน้าที่ความรับผิดชอบของผู้ให้บริการอย่างชัดเจน เช่น การสำรองข้อมูล การรับเรื่องแก้ไขปัญหา ขั้นตอนและกระบวนการแก้ไขปัญหา รายชื่อและช่องทางสำหรับติดต่อ เป็นต้น

๑๓.๑.๙ จัดให้มีการเผยแพร่นโยบายเกี่ยวกับการใช้บริการและจัดอบรมให้ความรู้แก่บุคลากรสถาบันเพื่อให้ตระหนักถึงความมั่นคงปลอดภัยจากการใช้บริการ Cloud Computing

๑๓.๑.๑๐ กำหนดมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมตามการใช้งานแต่ละประเภทเพื่อป้องกันภัยคุกคามและการเข้าถึงข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต

๑๓.๑.๑๑ กำหนดให้มีการตรวจสอบบันทึกหลักฐานต่าง ๆ และติดตามปัญหาที่อาจส่งผลต่อการใช้บริการ

๑๓.๒ การกำหนดข้อตกลงระหว่างผู้ให้บริการและสถาบัน

๑๓.๒.๑ ข้อมูลสารสนเทศบนระบบ Cloud ถือว่าเป็นข้อมูลที่สถาบันเป็นเจ้าของ

๑๓.๒.๒ สถาบันจะกำหนดประเภทบริการที่จะใช้ Cloud

๑๓.๒.๓ ต้องกำหนดมาตรฐานความปลอดภัยด้านเครือข่ายขั้นต่ำของระบบ Cloud ที่จะใช้งาน เช่น การเข้ารหัสข้อมูลที่รับส่งผ่านระบบเครือข่ายคอมพิวเตอร์ การป้องกันการโจมตีในลักษณะ DDoS Distributed Denial of Service) การป้องกันการบุกรุกจากชุดคำสั่งไม่พึงประสงค์ (Malware) การป้องกันภัยคุกคามในรูปแบบใหม่ (Advanced Persistent Threat) การแบ่งแยกเครือข่าย การเข้ารหัสระหว่างแอปพลิเคชัน (Application) การป้องกันการบุกรุกแบบลำดับชั้น (Defense-in-Depth) และการสร้างความมั่นคงปลอดภัยให้กับระบบสารสนเทศ (Hardening) เป็นต้น

๑๓.๒.๔ ต้องระบุข้อตกลงในการควบคุมการเข้าถึงข้อมูล เช่น วิธีการเข้าใช้งานระบบ วิธีการกำหนดสิทธิการใช้งาน การติดตามการแก้ปัญหา การรายงานข้อผิดพลาด ประสิทธิภาพและสภาพโดยรวมของระบบอย่างชัดเจน เป็นต้น

๑๓.๒.๕ กำหนดบทบาทหน้าที่ความรับผิดชอบของผู้ให้บริการในด้านการสำรองข้อมูล กระบวนการแก้ไขปัญหาระดับการให้บริการ (Service Level Agreement) ระยะเวลาในการกลับคืนสู่สภาพการดำเนินงานปกติของระบบสารสนเทศ (Recovery Time Objectives : RTO) และกำหนดเป้าหมายในการกู้คืนข้อมูล เช่น กำหนดประเภทของข้อมูลและชุดข้อมูลล่าสุดที่จะกู้คืนได้ (Recovery Point Objective : RPO) อย่างชัดเจน

๑๓.๒.๖ กำหนดเงื่อนไขความรับผิดชอบในกรณีที่ผู้ให้บริการไม่สามารถให้บริการตามสัญญาที่กำหนด

๑๓.๒.๗ กำหนดให้มีการลงนามในสัญญาที่เกี่ยวกับนโยบายการป้องกันการรั่วไหลของข้อมูลที่อาจเกิดขึ้นจากผู้ให้บริการ

๑๓.๒.๘ ผู้ให้บริการไม่มีสิทธิเข้าถึงและเปิดเผยข้อมูลของสถาบัน เว้นแต่จะแจ้งและได้รับความยินยอมจากสถาบัน

๑๓.๒.๙ สถาบันต้องมีมาตรการเพื่อให้มั่นใจได้ว่าผู้ให้บริการจัดให้มีการตรวจสอบขั้นตอนการปฏิบัติงานอย่างน้อยปีละ ๑ ครั้ง จากผู้ตรวจสอบอิสระ

๑๓.๒.๑๐ มีข้อกำหนดเมื่อสิ้นสุดการใช้บริการ (Exit Plan) เช่น กำหนดระยะเวลารักษาข้อมูลและวิธีการทำลายข้อมูลเพื่อให้มั่นใจว่าไม่สามารถกู้คืนข้อมูลกลับมาได้ เป็นต้น

๑๓.๒.๑๑ ต้องมีการเปิดเผยขั้นตอนปฏิบัติงานและเงื่อนไขการใช้บริการ Cloud Computing ต่อจากผู้ให้บริการรายอื่น (Sub Cloud) อย่างชัดเจน

๑๓.๓ การใช้บริการ Cloud Computing ต่อจากผู้ให้บริการรายอื่น (Sub cloud)

๑๓.๓.๑ ต้องแจ้งส่วนที่ Sub Cloud ให้สถาบันทราบ และให้ถือว่าบริการดังกล่าวเป็นส่วนหนึ่งของบริการของผู้ให้บริการด้วย โดยต้องมีคุณสมบัติด้านความปลอดภัยเทียบเท่ากับผู้ให้บริการ

๑๓.๓.๒ ต้องมีการเข้ารหัสในกรณีที่มีการรับส่งข้อมูลระหว่าง Cloud Provider กับ Sub Cloud Provider

๑๓.๓.๓ ต้องมีการกำหนดขั้นตอนปฏิบัติงานและเงื่อนไขการ Sub Cloud อย่างชัดเจน

๑๓.๔ การติดตาม ประเมิน และทบทวนการให้บริการของผู้ให้บริการ

๑๓.๔.๑ ต้องติดตามตรวจสอบประสิทธิภาพของการให้บริการ รวมทั้งมาตรการด้านความมั่นคงปลอดภัยให้สอดคล้องกับข้อกำหนดตามสัญญาต่าง ๆ หรือข้อตกลงในการให้บริการ

๑๓.๔.๒ ต้องประเมินความเพียงพอของระบบงานของผู้ให้บริการ (Capacity Planning) อย่างสม่ำเสมอ

๑๓.๔.๓ ต้องทบทวนเงื่อนไขการบริการในกรณีที่มีการเปลี่ยนแปลง เพื่อให้มั่นใจได้ว่าการให้บริการยังคงสอดคล้องกับการใช้งานและนโยบายด้านความมั่นคงปลอดภัยของระบบสารสนเทศของสถาบัน

๑๓.๔.๔ ต้องทบทวนคุณสมบัติของผู้ให้บริการอย่างต่อเนื่อง เช่น การตรวจสอบความมั่นคงในฐานะทางการเงิน กระบวนการปฏิบัติงาน และประสิทธิภาพการปฏิบัติงาน เป็นต้น

๑๓.๕ การโอนย้ายข้อมูล (Data Migration)

๑๓.๕.๑ สถาบันต้องกำหนดขั้นตอนการโอนย้ายข้อมูล (Data Migration) ไปยังผู้ให้บริการรายใหม่อย่างชัดเจนในกรณีที่มีการเปลี่ยนผู้ให้บริการ ทั้งนี้ เพื่อให้มั่นใจได้ว่าข้อมูลสารสนเทศยังคงมีความครบถ้วนถูกต้องและพร้อมใช้งานอยู่เสมอ

นโยบายที่ ๑๔
นโยบายและแนวปฏิบัติการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ
(Risk Management)

วัตถุประสงค์

๑. เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศ

๒. เพื่อเป็นการป้องกันและลดระดับความเสี่ยงที่อาจจะเกิดขึ้นกับระบบสารสนเทศ

แนวทางปฏิบัติ

๑๔.๑ การประเมินผลกระทบ

๑๔.๑.๑ ผลกระทบด้านมูลค่าความเสียหายทางการเงิน

การประเมินมูลค่าความเสียหายทางการเงินให้คำนวณจากความเสียหายที่จะเกิดขึ้นในหนึ่งวัน และคำนวณความเสียหายโดยตรงเท่านั้น โดยมีเกณฑ์ในการประเมินดังนี้

(๑) ในกรณีมูลค่าความเสียหายทางการเงินไม่เกินหนึ่งล้านบาทให้จัดเป็นผลกระทบระดับต่ำ

(๒) ในกรณีมูลค่าความเสียหายทางการเงินเกินกว่าหนึ่งล้านบาทแต่ไม่เกินหนึ่งร้อยล้านบาท ให้จัดเป็นผลกระทบระดับกลาง

(๓) ในกรณีมูลค่าความเสียหายทางการเงินเกินกว่าหนึ่งร้อยล้านบาทขึ้นไป ให้จัดเป็นผลกระทบระดับสูง

๑๔.๑.๒ ผลกระทบต่อจำนวนผู้ใช้บริการหรือผู้มีส่วนได้ส่วนเสียที่อาจได้รับอันตรายต่อชีวิต ร่างกาย หรืออนามัย

การประเมินผลกระทบต่อจำนวนผู้ใช้บริการหรือผู้มีส่วนได้ส่วนเสียที่อาจได้รับอันตรายต่อชีวิต ร่างกาย หรืออนามัย ให้คำนวณจากจำนวนของบุคคลดังกล่าวที่ได้รับผลกระทบในหนึ่งวัน โดยมีเกณฑ์ในการประเมินดังนี้

(๑) ในกรณีที่ไม่มีผู้ใช้บริการหรือผู้มีส่วนได้ส่วนเสียได้รับผลกระทบต่อร่างกาย หรืออนามัย ให้จัดเป็นผลกระทบระดับต่ำ

(๒) ในกรณีจำนวนผู้ใช้บริการหรือผู้มีส่วนได้ส่วนเสียได้รับผลกระทบต่อร่างกาย หรืออนามัย ตั้งแต่หนึ่งคน แต่ไม่เกินหนึ่งพันคน ให้จัดเป็นผลกระทบระดับกลาง

(๓) ในกรณีจำนวนผู้ใช้บริการหรือผู้มีส่วนได้ส่วนเสียได้รับผลกระทบต่อร่างกาย หรืออนามัย เกินกว่าหนึ่งพันคน หรือต่อชีวิตตั้งแต่หนึ่งคน ให้จัดเป็นผลกระทบระดับสูง

๑๔.๑.๓ ผลกระทบต่อจำนวนผู้ใช้บริการหรือผู้มีส่วนได้ส่วนเสียที่อาจได้รับความเสียหายอื่นใดนอกจากผลกระทบในข้อ ๑๔.๑.๒

การประเมินผลกระทบต่อจำนวนผู้ใช้บริการหรือผู้มีส่วนได้ส่วนเสียที่อาจได้รับความเสียหาย ให้คำนวณจากจำนวนของบุคคลดังกล่าวที่ได้รับผลกระทบในหนึ่งวัน และคำนวณความเสียหายโดยตรงเท่านั้น

(นอกจากข้อ ๑๔.๑.๔ (๒) ในกรณีมีผลกระทบต่อความมั่นคงของรัฐ ให้จัดเป็นผลกระทบระดับสูง) โดยมีเกณฑ์ในการประเมินดังนี้

(๑) ในกรณีจำนวนผู้ใช้บริการหรือผู้มีส่วนได้ส่วนเสียที่อาจได้รับผลกระทบไม่เกินหนึ่งหมื่นคน ให้จัดเป็นผลกระทบระดับต่ำ

(๒) ในกรณีจำนวนผู้ใช้บริการหรือผู้มีส่วนได้ส่วนเสียที่อาจได้รับผลกระทบเกินกว่าหนึ่งหมื่นคน แต่ไม่เกินหนึ่งแสนคน ให้จัดเป็นผลกระทบระดับกลาง

(๓) ในกรณีจำนวนผู้ใช้บริการหรือผู้มีส่วนได้ส่วนเสียที่อาจได้รับผลกระทบเกินกว่าหนึ่งแสนคน ให้จัดเป็นผลกระทบระดับสูง

๑๔.๑.๔ ผลกระทบด้านความมั่นคงของรัฐให้จัดเป็นสองระดับ โดยมีเกณฑ์ในการประเมินดังนี้

(๑) ในกรณีที่ไม่มีผลกระทบต่อความมั่นคงของรัฐ ให้จัดเป็นผลกระทบระดับต่ำ

(๒) ในกรณีมีผลกระทบต่อความมั่นคงของรัฐ ให้จัดเป็นผลกระทบระดับสูง

๑๔.๒ การประเมินความเสี่ยงระบบสารสนเทศ

๑๔.๒.๑ มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยมีเนื้อหาอย่างน้อยดังนี้

(๑) ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (Information Security Audit and Assessment) อย่างน้อยปีละ ๑ ครั้ง

(๒) ตรวจสอบและประเมินความเสี่ยงที่ดำเนินการโดยผู้ตรวจสอบภายในของสถาบัน (Internal Auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) เพื่อให้ส่วนงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

๑๔.๒.๒ มีแนวทางในตรวจสอบและประเมินความเสี่ยงที่ต้องคำนึงถึงอย่างน้อย ดังนี้

(๑) มีการทบทวนกระบวนการบริหารจัดการความเสี่ยง อย่างน้อยปีละ ๑ ครั้ง

(๒) มีการทบทวนนโยบายและมาตรการในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง

(๓) มีการตรวจสอบและประเมินความเสี่ยงและให้จัดทำรายงานพร้อมข้อเสนอแนะ

๑๔.๒.๓ มีมาตรการในการตรวจประเมินระบบสารสนเทศ อย่างน้อย ดังนี้

(๑) ควรกำหนดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้แบบอ่านได้อย่างเดียว

(๒) ในกรณีที่จำเป็นต้องเข้าถึงข้อมูลในแบบอื่น ๆ ให้สร้างสำเนาสำหรับข้อมูลนั้น เพื่อให้ผู้ตรวจสอบใช้งาน รวมทั้งควรทำลายหรือลบโดยทันทีที่ตรวจสอบเสร็จ หรือต้องจัดเก็บไว้โดยมีการป้องกันเป็นอย่างดี

๑๔.๒.๔ ควรกำหนดให้มีการระบุและจัดสรรทรัพยากรที่จำเป็นต้องใช้ในการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย

๑๔.๒.๕ ควรกำหนดให้มีการเฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้งบันทึกข้อมูล (Log) แสดงการเข้าถึงนั้น ซึ่งรวมถึงวันและเวลาที่เข้าถึงระบบงานที่สำคัญ

๑๔.๒.๖ ในกรณีที่มีเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ ควรกำหนดให้แยกการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบออกจากระบบให้บริการจริงหรือระบบที่ใช้ในการพัฒนา และมีการจัดเก็บป้องกันเครื่องมือนั้นจากการเข้าถึงโดยไม่ได้รับอนุญาต

๑๔.๒.๗ มีการรายงานผลการประเมินความเสี่ยงด้านสารสนเทศ ปีละ ๑ ครั้ง และแจ้งให้คณะกรรมการบริหารความเสี่ยงของสถาบันดำเนินการต่อไป

๑๔.๒.๘ มีการแสดงผลการตรวจสอบตามนโยบายการรักษาความปลอดภัยด้านสารสนเทศ เป็นส่วนหนึ่งของการรายงานผลการติดตาม ตรวจสอบและประเมินผลงานด้านเทคโนโลยีสารสนเทศ

๑๔.๓ การประเมินสถานการณ์ความเสี่ยง

การติดตามตรวจสอบความเสี่ยงต่าง ๆ ในระบบสารสนเทศสถาบัน พบความเสี่ยงที่อาจเป็นอันตรายต่อระบบเครือข่ายคอมพิวเตอร์ ซึ่งเป็นองค์ประกอบหลักในระบบสารสนเทศของสถาบัน สามารถแยกเป็นภัยและความเสี่ยง ดังต่อไปนี้

๑๔.๓.๑ ความเสี่ยงจากอุปกรณ์โครงสร้างพื้นฐานด้านสารสนเทศที่เก่าชำรุดล้าสมัย

(๑) ตรวจสอบอุปกรณ์ เพื่อให้ใช้งานได้ตามปกติ

(๒) ทำการบำรุงรักษา ทั้งเชิงป้องกันและเชิงแก้ไข

(๓) จัดหาอุปกรณ์ทดแทนอุปกรณ์ที่เสียหายใช้การไม่ได้ หรือไม่เหมาะกับเทคโนโลยีสมัยใหม่

๑๔.๓.๒ ภัยที่เกิดจากชุดคำสั่งไม่พึงประสงค์

เป็นภัยที่สร้างความเสียหายให้แก่เครื่องคอมพิวเตอร์ หรือระบบเครือข่ายคอมพิวเตอร์ ประกอบด้วย ไวรัสคอมพิวเตอร์ (Computer Virus) หนอนอินเทอร์เน็ต (Internet Worm) ม้าโทรจัน (Trojan Horse) และข่าวไวรัสหลอกลวง (Hoax) ซึ่ง Software ประเภทนี้อาจรบกวนการทำงานและก่อให้เกิดความเสียหายให้แก่ระบบสารสนเทศของสถาบัน ถึงขั้นทำให้ระบบเครือข่ายคอมพิวเตอร์ของสถาบันใช้งานไม่ได้

๑๔.๓.๓ ภัยที่เกิดจากบุคลากรของส่วนงาน (Human Error)

บุคลากรของส่วนงานขาดความรู้ความเข้าใจในเครื่องมืออุปกรณ์คอมพิวเตอร์ทั้งด้าน Hardware และ Software ซึ่งอาจทำให้ระบบสารสนเทศเสียหายใช้งานไม่ได้ เกิดการชะงักงัน หรือ หยุดทำงานและส่งผลให้ไม่สามารถใช้งานระบบสารสนเทศได้อย่างเต็มประสิทธิภาพ

๑๔.๓.๔ ภัยจากไฟไหม้ หรือระบบไฟฟ้า

จัดเป็นภัยร้ายแรงที่ทำความเสียหายให้แก่ระบบสารสนเทศ สถาบันได้ให้ความสำคัญและระมัดระวังเป็นอย่างยิ่งที่จะไม่ให้เกิดภัยลักษณะดังกล่าวขึ้น

๑๔.๓.๕ ภัยจากน้ำท่วม (อุทกภัย)

ความเสี่ยงต่อความเสียหายจากน้ำท่วม จัดเป็นภัยร้ายแรงที่ทำความเสียหายให้แก่ระบบสารสนเทศได้ ซึ่งสถาบันได้ให้ความสำคัญและระมัดระวังเป็นอย่างยิ่งที่จะไม่ให้ภัยในลักษณะดังกล่าวเกิดขึ้น

.....