ประกาศการนิคมอุตสาหกรรมแห่งประเทศไทย

ที่ ๑๔๓ /๒๕๖๕

เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ กนอ.

ตามที่ได้มีประกาศการนิคมอุตสาหกรรมแห่งประเทศไทย ที่ ๙๗/๒๕๖๔ เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ กนอ. ลงวันที่ ๒๕ สิงหาคม ๒๕๖๔ และโดยที่พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำประกาศแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานภาครัฐ หรือโดยหน่วยงานของภาครัฐ มีความมั่นคงปลอดภัยและเชื่อถือได้ นั้น

อาศัยอำนาจตามความในมาตรา ๒๘ แห่งพระราชบัญญัติการนิคมอุตสาหกรรมแห่งประเทศไทย พ.ศ. ๒๕๒๒ ประกอบกับมาตรา ๕ และมาตรา ๗ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ การนิคมอุตสาหกรรมแห่งประเทศไทย (กนอ.) จึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศการนิคมอุตสาหกรรมแห่งประเทศไทย ที่ ๑๔๓ /๒๕๖๕ เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ กนอ.”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศเป็นต้นไป

ข้อ ๓ ให้ยกเลิกประกาศการนิคมอุตสาหกรรมแห่งประเทศไทย ที่ ๙๗/๒๕๖๔ เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ กนอ. ลงวันที่ ๒๕ สิงหาคม ๒๕๖๔

ข้อ ๔ นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ กนอ. มีวัตถุประสงค์ ดังต่อไปนี้

(๑) เพื่อจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศสำหรับการบริหารจัดการและแก้ไขปัญหาหรือความเสี่ยงที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศของ กนอ.

(๒) เพื่อเผยแพร่ให้พนักงานของ กนอ. และบุคคลภายนอกที่ปฏิบัติงานให้กับ กนอ. ได้รับทราบเพื่อสร้างความเข้าใจ ความตระหนัก และการมีส่วนร่วมในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

(๓) เพื่อใช้เป็นกรอบมาตรฐานและแนวทางปฏิบัติด้านสารสนเทศสำหรับพนักงานของ กนอ. และบุคคลภายนอกที่ปฏิบัติงานให้กับ กนอ. ถือปฏิบัติโดยเคร่งครัด

(๔) เพื่อติดตามและทบทวนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ กนอ. ให้เป็นปัจจุบัน ซึ่งสอดคล้องกับสภาพแวดล้อม มาตรฐาน และกฎหมายที่เกี่ยวข้องอย่างน้อยปีละ ๑ ครั้ง หรือตามความเหมาะสม

/ข้อ ๕ ...

ข้อ ๕ ให้ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer : CIO) เป็นผู้รับผิดชอบในการกำกับ ดูแลให้เป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ กนอ.

ข้อ ๖ ให้ดำเนินการจัดทำข้อตกลงเกี่ยวกับการรักษาความลับของข้อมูลระหว่าง กนอ. และบุคคลภายนอกที่ปฏิบัติงานให้กับ กนอ.

ข้อ ๗ นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ กนอ. ให้เป็นไปตามหลักเกณฑ์ที่กำหนดไว้ในเอกสารแนบท้ายประกาศนี้

ข้อ ๘ ให้ผู้ใช้งานที่ได้รับอนุญาตให้เข้าถึงและใช้งานระบบสารสนเทศและระบบเครือข่ายของ กนอ. ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ กนอ. ที่กำหนดไว้ในเอกสารแนบท้ายประกาศนี้โดยเคร่งครัด

ประกาศ ณ วันที่ ๒๙ สิงหาคม พ.ศ. ๒๕๖๕

(นายวีริศ อัมระปาล)
ผู้ว่าการการนิคมอุตสาหกรรมแห่งประเทศไทย

เอกสารแนบท้าย

ประกาศการนิคมอุตสาหกรรมแห่งประเทศไทย

เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ กนอ.

สารบัญ

คำนิยาม

๑. **“ความมั่นคงปลอดภัยด้านสารสนเทศ” (Information Seucurity)** หมายถึง การธำรงไว้ซึ่งความลับ (Confidentiality) ความครบถ้วนและถูกต้อง (Integity) และความพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งความถูกต้องแท้จริง (Authenticity) ความรับผิดชอบ (Accountability) การห้ามปฏิเสธความรับผิด (Non-repudiation) และความน่าเชื่อถือ (Reliability)

๒. **“ระบบเทคโนโลยีสารสนเทศ” (Information Technology System)** หมายถึง ระบบงานที่นำเทคโนโลยีสารสนเทศมาช่วยในการสร้างสารสนเทศที่สามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนา และควบคุมการติดต่อสื่อสาร ซึ่งประกอบด้วยเทคโนโลยีคอมพิวเตอร์และเทคโนโลยีการสื่อสารโทรคมนาคม ได้แก่ ระบบคอมพิวเตอร์ (Computer System) ระบบเครือข่าย (Network System) ซอฟต์แวร์ (Software) ข้อมูล (Data) และสารสนเทศ (Information) เป็นต้น

๓. **“ผู้ดูแลระบบ” (System administrator)** หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมาย ให้มีหน้าที่รับผิดชอบในการบริหารจัดการการเข้าถึงและการใช้งานระบบเทคโนโลยีสารสนเทศของ กนอ. ได้แก่ การกำหนดบัญชีรายชื่อผู้ใช้งานการกำหนดสิทธิ์หรือการจำกัดสิทธิ์ให้กับผู้ใช้งานรวมทั้งการดูแลและบำรุงรักษาระบบเทคโนโลยีสารสนเทศของ กนอ. ให้สามารถใช้งานได้อย่างต่อเนื่อง

๔. **“เจ้าของระบบงาน” (System owner)** หมายถึง ผู้ซึ่งรับผิดชอบในการดูแลและบำรุงรักษา หรือปรับปรุงระบบงานที่ใช้ใน กนอ.

๕. **“เจ้าของข้อมูล” (Information owner)** หมายถึง ผู้ซึ่งรับผิดชอบข้อมูลของ กนอ. ซึ่งรวมถึงผู้บังคับบัญชาของเจ้าของข้อมูลนั้นด้วย โดยเจ้าของข้อมูลเป็นผู้ที่รับผิดชอบข้อมูลนั้นๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย

๖. **“ผู้ใช้งาน” (User)** หมายถึง เจ้าหน้าที่ของ กนอ. หรือบุคคลภายนอกที่ปฏิบัติงานให้กับ กนอ. รวมทั้งบุคคลภายนอกที่ได้รับอนุญาต (Authorized user) ให้เข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศของ กนอ. โดยมีสิทธิและหน้าที่ในการใช้งานตามที่ กนอ. กำหนด

๗. **“หน่วยงานภายนอก/ผู้ให้บริการภายนอก/บุคคลภายนอก” (Outside Agency/Service Provider/Third Party)** หมายถึง ลูกค้าหรือผู้ให้บริการภายนอก (Third Party/IT Outsourcing) หรือบุคคลภายนอก ที่ใช้งานระบบเทคโนโลยีสารสนเทศของ กนอ. ได้เป็นครั้งคราวหรือตามสัญญา

๘. **“สิทธิ์ของผู้ใช้งาน” (User Right)** หมายถึง สิทธิ์ทั่วไป สิทธิ์จำเพาะ สิทธิ์พิเศษ และสิทธิ์อื่นใดที่เกี่ยวข้องกับการเข้าถึงและการใช้งานระบบเทคโนโลยีสารสนเทศของ กนอ.

๙. **“สินทรัพย์” (Asset)** หมายถึง สิ่งที่มีคุณค่า มีมูลค่า และเป็นทรัพย์สินที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศที่ กนอ. เป็นเจ้าของ เช่า ว่าจ้าง พัฒนา หรือจัดซื้อ โดยแบ่งออกเป็นประเภทต่างๆ ได้ดังนี้ ฮาร์ดแวร์ (Hardware) ซอฟต์แวร์ (Software) สารสนเทศ (Information) สื่อบันทึกประเภทพกพา (Removeable media) บริการสาธารณูปโภคพื้นฐาน (Service) และบุคลากร (People)

๙.๑ **“ฮาร์ดแวร์” (Hardware)** หมายถึง อุปกรณ์ต่างๆ ที่ประกอบขึ้นเป็นเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ รวมทั้งอุปกรณ์ต่อพ่วงต่างๆ ที่สามารถมองเห็นและสัมผัสได้

๙.๑.๑ **“คอมพิวเตอร์แม่ข่าย” (Server)** หมายถึง เครื่องคอมพิวเตอร์ที่ทำหน้าที่เป็นศูนย์กลางของการทำงานในระบบคอมพิวเตอร์ ซึ่งให้บริการแก่เครื่องคอมพิวเตอร์ตามที่ร้องขอ ได้แก่ การประมวลผลข้อมูล การจัดเก็บข้อมูล การป้องกันไวรัส

๙.๑.๒ **“เครื่องคอมพิวเตอร์หรือเครื่องคอมพิวเตอร์ลูกข่าย” (Computer or Client Computer)** หมายถึง อุปกรณ์ที่ใช้ในการประมวลผลข้อมูลผ่านซอฟต์แวร์หรือซอฟต์แวร์ประยุกต์ เพื่อให้ได้ผลลัพธ์ตามที่ต้องการ ได้แก่ คอมพิวเตอร์ส่วนบุคคล (Personal computer) หรือคอมพิวเตอร์แบบพกพาได้ (Notebook computer) รวมทั้งอุปกรณ์อัจฉริยะ (Smart device) หรืออุปกรณ์พกพา (Mobile device)

๙.๑.๓ **“อุปกรณ์ต่อพ่วง” (Peripheral device)** หมายถึง อุปกรณ์อิเล็กทรอนิกส์ที่ใช้งานร่วมกับเครื่องคอมพิวเตอร์ เพื่อสนับสนุนให้เครื่องคอมพิวเตอร์สามารถทำงานได้ตามต้องการ ได้แก่ การนำเข้าข้อมูล หรือการแสดงผล

๙.๑.๔ **“สื่อสัญญาณ” (Signal)** หมายถึง สื่อกลางใดๆ ได้แก่ สายทองแดง สายใยแก้วนำแสง หรือระบบเครือข่ายไร้สาย ทำหน้าที่เชื่อมต่อระหว่างเครื่องคอมพิวเตอร์หรืออุปกรณ์อื่นๆ ในระบบเครือข่าย

๙.๑.๕ **“ระบบเครือข่าย” (Network)** หมายถึง ระบบที่เชื่อมโยงเครื่องคอมพิวเตอร์หรือระบบเครือข่ายอื่นๆ เข้าด้วยกัน เพื่อการติดต่อสื่อสารหรือการแลกเปลี่ยนข้อมูล

๙.๑.๕.๑ **“ระบบอินเทอร์เน็ต” (Internet)** หมายถึง ระบบเครือข่ายที่เชื่อมโยงคอมพิวเตอร์หรือระบบเครือข่ายของ กนอ. เข้ากับระบบเครือข่ายภายนอกทั่วโลก

๙.๑.๕.๒ **“ระบบอินทราเน็ต” (Intranet)** หมายถึง ระบบเครือข่ายที่เชื่อมโยงเครื่องคอมพิวเตอร์หรือระบบเครือข่ายภายในของ กนอ. เข้าด้วยกัน

๙.๑.๖ **“ระบบป้องกันการบุกรุก” (Intrusion protection system)** หมายถึง ระบบรักษาความปลอดภัย ประกอบด้วย ฮาร์ดแวร์หรือซอฟต์แวร์ทำหน้าที่ป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้าถึงหรือใช้งานระบบเทคโนโลยีสารสนเทศได้ และจำกัดการเข้าถึงและการใช้งานระบบเทคโนโลยีสารสนเทศของผู้ใช้งานภายในให้เป็นไปตามที่กำหนด

๙.๒ **“ซอฟต์แวร์” (Software)** หมายถึง โปรแกรมประเภทหนึ่งที่ถูกสร้างขึ้นสำหรับใช้งานเฉพาะทาง เช่น ระบบ EPP ระบบ ERP ระบบ E-mail ระบบ Workflow เป็นต้น

๙.๓ **“สารสนเทศ” (Information)** หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัดระเบียบข้อมูล ซึ่งอาจจะอยู่ในรูปของตัวเลข ข้อความหรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้งานสามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่นๆ

๑๐. **“การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ” (Accessing or Controlling for use of information)** หมายถึง การอนุมัติ การกำหนดสิทธิ์ การตรวจสอบหรือการมอบอำนาจให้ผู้ใช้งานภายในและบุคคลภายนอกให้สามารถเข้าถึงหรือใช้งานระบบเทคโนโลยีสารสนเทศของ กนอ.

๑๑. **“เหตุการณ์ด้านความมั่นคงปลอดภัย” (Information security event)** หมายถึง เหตุการณ์ที่แสดงให้เห็นถึงความเป็นไปได้ที่เกิดขึ้นกับระบบเทคโนโลยีสารสนเทศของ กนอ. จากการละเมิดหรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ หรือความประมาท

๑๒. **“สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด” (Information security incedent)** หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ (Unwanted) หรือไม่อาจคาดคิด (Unexpected) ซึ่งมีแนวโน้มทำให้ระบบเทคโนโลยีสารสนเทศของ กนอ. ถูกบุกรุก ถูกโจมตี หรือถูกคุกคาม

๑๓. **“ซอฟต์แวร์ประสงค์ร้าย” (Malicious Software)** หมายถึง ซอฟต์แวร์ที่ตั้งใจใส่เข้าไปในระบบเทคโนโลยีสารสนเทศโดยไม่ได้รับอนุญาต เพื่อให้ทำงานตามความความต้องการของผู้ประสงค์ร้าย ส่งผลให้ระบบเทคโนโลยีสารสนเทศได้รับความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือเพิ่มเติม จนเกิดความขัดข้องหรือไม่สามารถปฏิบัติงานได้

๑๔. **“บัญชีรายชื่อ” (User account)** หมายถึง รายชื่อของผู้ใช้งานที่ได้รับอนุญาตหรือไม่ได้ รับอนุญาตให้เข้าถึงหรือใช้งานระบบเทคโนโลยีสารสนเทศของ กนอ.

๑๔.๑ **“บัญชีรายชื่อผู้ดูแลระบบ” (Administrator account)** หมายถึง รายชื่อของผู้ดูแลระบบ (Username) ของผู้ดูแลระบบที่ได้รับอนุญาตหรือไม่ได้รับอนุญาตให้เข้าถึงหรือใช้งานระบบเทคโนโลยีสารสนเทศของ กนอ.

๑๔.๒ **“บัญชีรายชื่อผู้ใช้งาน” (User account)** หมายถึง รายชื่อของผู้ใช้งานภายในและบุคคลภายนอก (Username) ที่ได้รับอนุญาตหรือไม่ได้รับอนุญาตให้เข้าถึงหรือใช้งานระบบเทคโนโลยีสารสนเทศของ กนอ.

๑๔.๓ **“รหัสผ่าน” (Password)** หมายถึง ตัวอักษร อักขระหรือตัวเลขที่ใช้เป็นสำหรับตรวจสอบการพิสูจน์ตัวตนหรือการยืนยันตัวตนของผู้ใช้งาน

๑๕. **“การพิสูจน์ตัวตนหรือการยืนยันตัวตน” (Authentication)** หมายถึง ขั้นตอนในการพิสูจน์ตัวตนของผู้ใช้งานเพื่อควบคุมการเข้าถึงหรือการใช้งานระบบเทคโนโลยีสารสนเทศของ กนอ. โดยทั่วไปแล้วจะตรวจสอบรายชื่อผู้ใช้งาน(Username) ร่วมกับรหัสผ่าน (Password) เป็นอย่างน้อย

๑๖. **“พื้นที่ใช้งาน” (Information system workspace)** หมายถึง พื้นที่ที่อนุญาตให้มีการเข้าถึงและการใช้งานระบบเทคโนโลยีสารสนเทศของ กนอ. ได้แก่

๑๖.๑ **“พื้นที่ทำงานทั่วไป” (General working area)** หมายถึง พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคล และคอมพิวเตอร์แบบพกพาที่ประจำโต๊ะทำงาน

๑๖.๒ **“พื้นที่ทำงานของผู้ดูแลระบบ” (System administrator area)** หมายถึง พื้นที่ควบคุมที่อนุญาตให้เฉพาะผู้ดูแลระบบที่มีสิทธิ์เท่านั้น

๑๖.๓ **“พื้นที่ติดตั้งอุปกรณ์ของระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย” (IT equipment or network area)** หมายถึง พื้นที่สำหรับติดตั้งอุปกรณ์ที่เกี่ยวกับระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย

๑๖.๔ **“การเข้าถึงระบบเครือข่ายจากระยะไกล” (Remote Access)** หมายถึง การเชื่อมต่อเครื่องคอมพิวเตอร์หรือระบบเครือข่ายอื่นๆ เข้ากับระบบเครือข่ายของ กนอ. ผ่านอุปกรณ์สื่อสารหรือสื่อสัญญาณอื่นๆ ได้แก่ VPN (Vitual Private Network)

๑๖.๕ **“การควบคุมการเข้าถึง” (Access Control)** หมายถึง การควบคุมการเข้าถึงหรือการใช้งานระบบเทคโนโลยีสารสนเทศให้เป็นไปตามสิทธิ์และหน้าที่ของผู้ใช้งานที่กำหนดไว้เท่านั้น

๑๖.๖ **“การเข้ารหัส” (Encryption)** หมายถึง การนำข้อมูลมาผ่านกระบวนการเข้ารหัสเพื่อป้องกันการลักลอบเข้าถึงหรือใช้ข้อมูลโดยผู้ที่ไม่ได้รับอนุญาติ โดยผู้ที่ได้รับอนุญาตหรือมีกุญแจถอดรหัสเท่านั้นที่สามารถเข้าถึงหรือใช้ข้อมูลที่เข้ารหัสได้

๑๖.๗ **“เอกสารโครงแบบ” (Configuration Document)** หมายถึง เอกสารที่แสดงรายละเอียดการกำหนดค่าต่างๆ ในระบบเทคโนโลยีสารสนเทศ เพื่อให้สามารถทำงานได้ตามความต้องการ

๑๗. **“ความเสี่ยง” (Risk)** หมายถึง โอกาสของสินทรัพย์ของระบบเทคโนโลยีสารสนเทศที่ถูกละเมิดหรือฝ่าฝืนการรักษาความมั่นคงปลอดภัย

๑๘. **“นโยบายการบริหารความเสี่ยงระบบเทคโนโลยีสารสนเทศ” (IT Risk Management Policy)** หมายถึง แนวทางในการบริหารจัดการความเสี่ยงระบบเทคโนโลยีสารสนเทศ ให้สามารถดำเนินการประเมินความเสี่ยงได้อย่างมีประสิทธิผลและสอดคล้องกับการประเมินความเสี่ยงของ กนอ.

๑๙. **“การบริหารความต่อเนื่องทางธุรกิจระบบเทคโนโลยีสารสนเทศ” (Business Continuity for Information Technology)** หมายถึง แนวทางในการบริหารจัดการธุรกิจได้อย่างต่อเนื่องเมื่อ กนอ. อยู่ในสภาวะวิกฤติและเหตุฉุกเฉินต่างๆ ทำให้มั่นใจได้ว่า ขั้นตอนการดำเนินงานและระบบสารสนเทศต่างๆ ของ กนอ. ที่สำคัญได้รับการวางแผนความต่อเนื่องในการดำเนินงานของ กนอ. (Business Continuity Plan หรือ BCP) อย่างเหมาะสม

๒๐. **ผอ.ฝดจ.** หมายถึง ผู้อำนวยการฝ่ายดิจิทัล

๒๑. **ผอ.กพจ** หมายถึง ผู้อำนวยการกองพัฒนาระบบงานดิจิทัล

๒๒. **ผอ.กปจ.** หมายถึง ผู้อำนวยการกองปฏิบัติการดิจิทัล

๒๓. **ผอ.ศขจ.** หมายถึง ผู้อำนวยการศูนย์ข้อมูลดิจิทัล

ส่วนที่ ๑
การบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ
(IT Asset Management)

วัตถุประสงค์

๑. เพื่อให้ กนอ. มีแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศสำหรับการบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศของ กนอ.

๒. เพื่อให้ผู้รับผิดชอบและผู้มีส่วนเกี่ยวข้อง ได้แก่ ผู้บริหารระดับสูง ผู้บริหาร ผู้ดูแลระบบ เจ้าหน้าที่หน่วยงาน เจ้าของข้อมูล บุคคลภายนอกที่ปฏิบัติงานให้กับ กนอ. และบุคคลภายนอกที่ได้รับอนุญาตให้เข้าถึงและใช้งานสารสนเทศของ กนอ. รับทราบและทำความเข้าใจ รวมทั้งปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างเคร่งครัด

ขอบเขต

บังคับใช้กับทุกหน่วยงานใน กนอ.

อ้างอิงมาตรฐาน

๑. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศตามวิธีแบบปลอดภัย พ.ศ. ๒๕๕๕

๒. มาตรฐาน ISO/IEC 27001:2013 (Annex A)

แนวทางปฏิบัติ

๑. หน้าที่ความรับผิดชอบต่อทรัพย์สินขององค์กร

๑.๑ กปจ.ควบคุมและกำกับให้มีการเก็บบันทึกทะเบียนทรัพย์สิน โดยใช้บัญชีรายการทรัพย์สิน (Asset Inventory) FM-DC-01 โดยข้อมูลที่จัดเก็บต้องประกอบด้วยข้อมูลที่จำเป็นในการค้นหาเพื่อการใช้งานในภายหลัง

๑.๒ ผู้มีหน้าที่ดูแลควบคุมการใช้งานทรัพย์สินสารสนเทศและผู้มีหน้าที่รับผิดชอบทรัพย์สินสารสนเทศ ดูแลทรัพย์สินอย่างเหมาะสม และทบทวนอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงทรัพย์สินหรือระบบงาน

๑.๓ จัดให้มีการใช้งานทรัพย์สินสารสนเทศอย่างเหมาะสม โดยพิจารณาตามบทบาทภาระหน้าที่งานและความจำเป็นเพื่อการปฏิบัติงาน
ISO/IEC 27001:2013 (Annex A): A.8.1.1-2

๒. การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา และอื่นๆ (Notebook, Tablet, etc.)

๒.๑ การอนุญาตให้ใช้ทรัพย์สินสารสนเทศ (Acceptable use of assets) เครื่องคอมพิวเตอร์ที่ กนอ. จัดหาให้ถือเป็นสินทรัพย์ของ กนอ. ผู้ใช้งานควรใช้งานอย่างเหมาะสมกับการทำงานเพื่อตอบสนองต่อภารกิจของ กนอ. อย่างมีประสิทธิภาพ หลีกเลี่ยงการนำไปใช้งานส่วนตัว

๒.๒ ซอฟต์แวร์ที่ติดตั้งบนเครื่องคอมพิวเตอร์ของ กนอ. ต้องมีลิขสิทธิ์อย่างถูกต้องตามกฎหมาย ห้ามผู้ใช้งานคัดลอกซอฟต์แวร์ต่างๆ รวมทั้งการนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย และไม่อนุญาตให้ผู้ใช้งานติดตั้ง เปลี่ยนแปลงหรือแก้ไขซอฟต์แวร์ในเครื่องคอมพิวเตอร์ของ กนอ.

๒.๓ ผู้ใช้งานต้องรับผิดชอบในการป้องกันการสูญหาย และความสูญหายของคอมพิวเตอร์และอุปกรณ์ที่ กนอ. จัดหาให้

๒.๔ ห้ามมิให้ผู้ใช้งานทำการเปลี่ยนแปลงหรือแก้ไขส่วนประกอบย่อย (Sub Component) ที่ติดตั้งอยู่ภายในเครื่องคอมพิวเตอร์ของ กนอ. รวมถึงแบตเตอรี่ของเครื่องคอมพิวเตอร์แบบพกพา

ISO/IEC 27001:2013 (Annex A): A.6.2.1, A.8.1.3, A.12.6.2

ตัวชี้วัดผลลัพธ์

๑. จัดทำรายการบัญชีทรัพย์สินสารสนเทศ (Information Asset Inventory) ครบถ้วน ๑๐๐%

๒. ทบทวนรายการทรัพย์สินสารสนเทศ (Information Asset) ปีละ ๑ ครั้ง

๓. ใช้งานซอฟแวร์ที่มีลิขสิทธิ์ถูกต้อง ๑๐๐%

ส่วนที่ ๒
การรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศ
(Data and Information Security)

วัตถุประสงค์

๑. เพื่อให้ กนอ. มีแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านข้อมูลสารสนเทศ (Data & Information Security)

๒. เพื่อให้ผู้รับผิดชอบและผู้มีส่วนเกี่ยวข้อง ได้แก่ ผู้บริหารระดับสูง ผู้บริหาร ผู้ดูแลระบบ เจ้าหน้าที่ หน่วยงานเจ้าของข้อมูล บุคคลภายนอกที่ปฏิบัติงานให้กับ กนอ. และบุคคลภายนอกที่ได้รับอนุญาตให้เข้าถึงและใช้งานสารสนเทศของ กนอ. รับทราบและทำความเข้าใจ รวมทั้งปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างเคร่งครัด

ขอบเขต

บังคับใช้กับทุกหน่วยงานใน กนอ.

อ้างอิงมาตรฐาน

๑. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศตามวิธีแบบปลอดภัย พ.ศ. ๒๕๕๕

๒. มาตรฐาน ISO/IEC 27001:2013 (Annex A)

แนวทางปฏิบัติ

๑. การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

๑.๑ ผู้ดูแลระบบต้องกำหนดชั้นความลับของข้อมูล กำหนดบัญชีรายชื่อผู้ใช้งานและรหัสผ่าน (Password) วิธีปฏิบัติในการจัดเก็บข้อมูล และวิธีปฏิบัติในการควบคุมการเข้าถึงการใช้งานสารสนเทศในแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบเทคโนโลยีสารสนเทศ รวมถึงวิธีการทำลายข้อมูลในแต่ละประเภทชั้นความลับ ตามระเบียบปฏิบัติ เรื่อง การชี้บ่งและจัดการสารสนเทศ QP-DC-04 ISO/IEC 27001:2013 (Annex A): A.8.2, A.8.3

๒. การแลกเปลี่ยนสารสนเทศ

๒.๑ ต้องกำหนดให้มีนโยบายและขั้นตอนปฏิบัติงานสำหรับการแลกเปลี่ยนสารสนเทศระหว่างหน่วยงานภายในองค์กร และระหว่างองค์กรกับหน่วยงานภายนอก รวมทั้งควบคุมการแลกเปลี่ยนข้อมูลสารสนเทศผ่านช่องทางการสื่อสารในรูปแบบข้อมูลอิเล็กทรอนิกส์

๒.๒ การแลกเปลี่ยนสารสนเทศผ่านช่องทางการสื่อสารทุกชนิดระหว่าง กนอ. กับหน่วยงานภายนอก ต้องได้รับการอนุมัติจากผู้บริหารของ กนอ.

๒.๓ ต้องควบคุมให้มีการจัดทำข้อตกลงในการแลกเปลี่ยนข้อมูลสารสนเทศหรือซอฟต์แวร์ระหว่างหน่วยงานกับบุคคลหรือหน่วยงานภายนอก

๒.๔ ข้อตกลงการแลกเปลี่ยนสารสนเทศต้องดำเนินการจัดทำอย่างเป็นลายลักษณ์อักษร

๒.๕ การแลกเปลี่ยนสารสนเทศระหว่าง กนอ. กับหน่วยงานภายนอกต้องดำเนินการ การแลกเปลี่ยนสารสนเทศด้วยวิธีการที่มีความมั่นคงปลอดภัยและสอดคล้องกับการจัดระดับชั้นสารสนเทศ

๒.๖ ผู้ดูแลระบบ ต้องป้องกันข้อมูลสารสนเทศที่มีการสื่อสารหรือแลกเปลี่ยนในการทำธุรกรรมทางออนไลน์ (Online Transaction) เพื่อมิให้มีการรับส่งข้อมูลที่ไม่สมบูรณ์ หรือส่งข้อมูลไปผิดที่ หรือมีการรั่วไหลของข้อมูลหรือข้อมูลถูกแก้ไขเปลี่ยนแปลง ถูกทำซ้ำใหม่ หรือถูกส่งซ้ำโดยมิได้รับอนุญาต

๒.๗ การป้องกันข้อมูลสารสนเทศที่มีการสื่อสารกันผ่านข้อมูลอิเล็กทรอนิกส์ (Electronic Messaging) เช่น จดหมายอิเล็กทรอนิกส์ (E-mail) EDI หรือ Instant Messaging) โดยใช้บริการ email ของ DGA ผู้ใช้งาน Email ต้องตระหนักถึงความเสี่ยงในการเปิดไฟล์แนบ หรือ Link ที่น่าสงสัยหากไม่แน่ใจให้ขอคำแนะนำจากผู้ดูแลระบบเพื่อป้องกันภัยคุกคามที่แฝงมาใน Email

ISO/IEC 27001:2013 (Annex A): A.13.2.1-3

๓. การควบคุมการโอนย้ายข้อมูล (Data Migration)

๓.๑ การโอนย้ายข้อมูล (Data Migration) กำหนดขั้นตอนการปฏิบัติอย่างชัดเจนด้วยวิธีการที่มีความมั่นคงปลอดภัย ทั้งนี้ เพื่อให้มั่นใจได้ว่าข้อมูลสารสนเทศยังคงมีความครบถ้วนถูกต้อง และพร้อมใช้งานอยู่เสมอ ปฏิบัติตามระเบียบปฏิบัติ เรื่อง การควบคุมการเปลี่ยนแปลง (Change Control) QP-DC-05

ISO/IEC 27001:2013 (Annex A): A.13.2

ตัวชี้วัดผลลัพธ์

๑. กำหนดแนวทางการจัดชั้นความลับของสารสนเทศเป็นลายลักษณ์อักษร

๒. สื่อสารชี้แจงแนวทางปฏิบัติไปยังผู้เกี่ยวข้อง

๓. ตรวจสอบการปฏิบัติโดยการตรวจประเมินภายใน (ISMS Audit) อย่างน้อยปีละ ๑ ครั้ง

ส่วนที่ ๓
การควบคุมการเข้าถึง
(Access Control)

วัตถุประสงค์

๑. เพื่อให้ กนอ. มีแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศสำหรับการควบคุมการเข้าถึงและการใช้งานสารสนเทศของ กนอ.

๒. เพื่อให้ผู้รับผิดชอบและผู้มีส่วนเกี่ยวข้อง ได้แก่ ผู้บริหารระดับสูง ผู้บริหาร ผู้ดูแลระบบ เจ้าหน้าที่หน่วยงานเจ้าของข้อมูล บุคคลภายนอกที่ปฏิบัติงานให้กับ กนอ. และบุคคลภายนอกที่ได้รับอนุญาตให้เข้าถึงและใช้งานสารสนเทศของ กนอ. รับทราบและทำความเข้าใจ รวมทั้งปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างเคร่งครัด

๓. เพื่อให้มีการตรวจสอบและติดตามการพิสูจน์ตัวบุคคลที่เข้าถึงและใช้งานสารสนเทศของ กนอ. ได้อย่างถูกต้อง

ขอบเขต

บังคับใช้กับทุกหน่วยงานใน กนอ.

อ้างอิงมาตรฐาน

๑. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศตามวิธีแบบปลอดภัย พ.ศ. ๒๕๕๕

๒. มาตรฐาน ISO/IEC 27001:2013 (Annex A)

แนวทางปฏิบัติ

๑. การควบคุมการเข้าถึงและการใช้งานสารสนเทศ (Access control Policy)

๑.๑ ผู้ดูแลระบบต้องจำแนกกลุ่มทรัพยากร ได้แก่ ข้อมูล สารสนเทศ ระบบเทคโนโลยีสารสนเทศ โดยกำหนดกลุ่มผู้ใช้งานและสิทธิ์ของกลุ่มผู้ใช้งาน อ้างอิงตาม Access Control Matrix FM-DC-03

๑.๒ ผู้ดูแลระบบต้องกำหนดสิทธิ์การเข้าถึงและการใช้งานสารสนเทศให้เหมาะสมตามสิทธิ์และหน้าที่ความรับผิดชอบ ในการปฏิบัติงานของผู้ใช้งานรวมทั้งการทบทวนสิทธิ์อย่างสม่ำเสมอทุก 1 ปี รายงานผลในคณะดำเนินการระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศของ กนอ.

๑.๒.๑ กำหนดสิทธิในการเข้าถึงและการใช้งานสารสนเทศที่เกี่ยวข้องให้เหมาะสมกับการใช้งาน ดังนี้

๑.๒.๑.๑ สิทธิ์ในการสร้างสารสนเทศ

๑.๒.๑.๒ สิทธิ์ในการอ่านหรือเรียกดูสารสนเทศ

๑.๒.๑.๓ สิทธิ์ในการปรับปรุงหรือเปลี่ยนแปลงสารสนเทศ

๑.๒.๑.๔ สิทธิ์ในการรับรองการปรับปรุงหรือเปลี่ยนแปลงสารสนเทศ

๑.๒.๑.๕ สิทธิ์ในการรับรองความครบถ้วนและถูกต้องของสารสนเทศ

๑.๒.๑.๖ สิทธิ์ในการมอบอำนาจหรือดำเนินการแทน

๑.๒.๑.๗ ไม่มีสิทธิ์

๑.๒.๒ การจัดแบ่งประเภทสารสนเทศ การกำหนดลำดับความสำคัญหรือระดับชั้นความลับของสารสนเทศ การกำหนดระดับชั้นในการเข้าถึงสารสนเทศ ดำเนินการตามระเบียบปฏิบัติ เรื่อง การชี้บ่งและจัดการสารสนเทศ (Classification and Labeling of Information and Handling of Assets) QP-DC-04

๑.๓ ผู้ดูแลระบบมีการติดตั้งระบบบันทึกและติดตามการเข้าถึงและการใช้งานสารสนเทศของ กนอ. และตรวจสอบการละเมิดความมั่นคงปลอดภัยด้านสารสนเทศโดยเก็บ Log ไว้เพื่อเป็นหลักฐานการเฝ้าระวังและตรวจสอบ

๑.๔ ผู้ดูแลระบบต้องจัดให้มีการบันทึกการผ่านเข้า-ออกพื้นที่ติดตั้งระบบเทคโนโลยีสารสนเทศโดยมี Finger Scan และบันทึกการเข้าออก Data Center FM-DC-08

๑.๕ ข้อกำหนดการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงและการใช้งานสารสนเทศ (Business requirements for access control)

๑.๕.๑ การเข้าถึงและการใช้งานสารสนเทศและสิทธิ์ที่เกี่ยวข้องกับสารสนเทศเป็นไปตามหน้าที่ความรับผิดชอบและภาระงานของบุคคลนั้นๆ โดยพิจารณาอนุญาตเท่าที่จำเป็นเพื่อการปฏิบัติงาน ISO/IEC 27001:2013 (Annex A): A.9.1

๒. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

๒.๑ ขั้นตอนปฏิบัติในการลงทะเบียนผู้ใช้งาน (User registration)

<u>สำหรับผู้ดูแลระบบ (System Administrator)</u>

๒.๑.๑ หน่วยงานของผู้ขอใช้ระบบสารสนเทศจัดทำบันทึกข้อความ เรียนฝ่ายดิจิทัล เพื่อดำเนินการตามขั้นตอนการลงทะเบียนผู้ใช้งาน (User Registration) และใช้ตรวจสอบสิทธิ์

๒.๑.๒ ระบุบัญชีรายชื่อผู้ใช้งานแยกกันเป็นรายบุคคล เพื่อไม่ให้เกิดความซ้ำซ้อนกัน

๒.๑.๓ กำหนดบัญชีรายชื่อผู้ใช้งานโดยกำหนดจากชื่อภาษาอังกฤษตามด้วยอักษรตัวแรกของนามสกุล หากซ้ำให้เพิ่มอักษรตัวที่สองหรือจนกว่าจะไม่ซ้ำกับชื่อผู้ใช้งานคนอื่น

๒.๑.๔ จำกัดการใช้งานบัญชีรายชื่อผู้ใช้งานแบบกลุ่มภายใต้บัญชีรายชื่อเดียวกันและอนุญาตให้ใช้ระบบเทคโนโลยีสารสนเทศเท่าที่จำเป็นต่อการปฏิบัติงานเท่านั้น

๒.๑.๕ ตรวจสอบและมอบหมายสิทธิ์ในการเข้าถึงระบบเทคโนโลยีสารสนเทศที่เหมาะสมต่อหน้าที่และความรับผิดชอบของผู้ใช้งาน

๒.๑.๖ จัดเก็บบันทึกขออนุมัติการเข้าใช้ระบบเทคโนโลยีสารสนเทศที่หน่วยงานผู้รับผิดชอบ

สำหรับผู้ใช้งาน (User)

๒.๑.๗ หน่วยงานของผู้ขอใช้ระบบสารสนเทศจัดทำบันทึกข้อความ เรียนฝ่ายดิจิทัล เพื่อดำเนินการตามขั้นตอนการลงทะเบียนผู้ใช้งาน (User Registration) และใช้ตรวจสอบสิทธิ์

๒.๑.๘ ผู้ดูแลระบบกำหนดหรือทบทวนหลักเกณฑ์ในการยกเลิกหรือเพิกถอนการอนุญาตและการระงับการใช้สิทธิ์ในการข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศของ กนอ. จากบัญชีรายชื่อผู้ใช้งานเมื่อมีการลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดการเป็นพนักงาน อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง ดังนี้

๒.๑.๘.๑ บรรจุพนักงานใหม่ ภายใน ๗ วันทำการ

๒.๑.๘.๒ เปลี่ยนแปลง/โอนย้าย/แต่งตั้ง/ปรับระดับ ภายใน ๗ วันทำการ

๒.๑.๘.๓ ลาออก ภายใน ๗ วันทำการ

๒.๒ การบริหารจัดการสิทธิ์ของผู้ใช้งาน (User management) โดยแสดงรายละเอียดที่เกี่ยวกับการควบคุมและจำกัดสิทธิ์ เพื่อให้ผู้ใช้งานสามารถเข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศแต่ละระบบตามการปฏิบัติหน้าที่ รวมถึงสิทธิ์จำเพาะ สิทธิ์พิเศษ และสิทธิ์อื่นๆ ที่เกี่ยวข้องกับการเข้าถึง ดังนี้

๒.๒.๑ ผู้ดูแลระบบกำหนดการมอบหมายหรือกำหนดสิทธิ์การใช้งานให้แก่ผู้ใช้งาน

๒.๒.๒ ผู้ดูแลระบบกำหนดระดับของสิทธิ์ในการเข้าถึงระบบเทคโนโลยีสารสนเทศที่เหมาะสมตามหน้าที่ความรับผิดชอบและตามความจำเป็นในการใช้งาน

๒.๒.๓ ผู้ดูแลระบบต้องมอบหมายสิทธิ์ที่สอดคล้องกับนโยบายควบคุมการเข้าถึง

๒.๒.๔ ผู้ดูแลระบบบันทึกและจัดเก็บข้อมูลการมอบหมายสิทธิ์ให้แก่ผู้ใช้งาน

๒.๒.๕ ในกรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุดผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจาก ผอ.ฝดจ. ก่อนการดำเนินการ โดยกำหนดระยะเวลาการใช้งานและระงับการใช้งานระบบเทคโนโลยีสารสนเทศตามเกณฑ์การกำหนดสิทธิ์

๒.๓ การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User password management) จัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม ดังนี้

๒.๓.๑ การกำหนดรายชื่อผู้ใช้งานต้องไม่ซ้ำกัน

๒.๓.๒ การเปลี่ยนแปลงและยกเลิกรหัสผ่าน เมื่อผู้ใช้งานลาออกหรือพ้นจากตำแหน่งหรือยกเลิกการใช้งาน ภายใน ๗ วัน

๒.๓.๓ การตั้งรหัสผ่านชั่วคราวต้องยากต่อการคาดเดาและต้องมีความแตกต่างกันและความหลากลายของอักขระ

๒.๓.๔ การส่งมอบรหัสผ่านชั่วคราวให้กับผู้ใช้งานต้องส่งมอบด้วยวิธีการที่ปลอดภัยพร้อมมีการประทับข้อความ “ลับ” บนซองบัญชีรายชื่อผู้ใช้งานและรหัสผ่าน (Password) โดยหลีกเลี่ยงการใช้บุคคลอื่นหรือผ่านทางซอฟต์แวร์ต่างๆ ในการจัดส่งรหัสผ่านซึ่งผู้ใช้งานควรตอบกลับทันทีหลังจากได้รับรหัสผ่านเรียบร้อยแล้ว

๒.๓.๕ ผู้ใช้งานต้องไม่บันทึกหรือเก็บรหัสผ่านไว้ในเครื่องคอมพิวเตอร์ในรูปแบบข้อความหรือไฟล์ที่ไม่ได้ป้องกันการเข้าถึง

๒.๓.๖ การเปลี่ยนรหัสผ่านต้องตรวจสอบบัญชีรายชื่อผู้ใช้งานและรหัสผ่านปัจจุบันให้ถูกต้องก่อนที่อนุญาตให้เปลี่ยนรหัสใหม่

๒.๓.๗ ในกรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุด ผู้ใช้งานนั้นต้องได้รับความเห็นชอบและอนุมัติจาก ผอ.ฝดจ. ก่อนการดำเนินการ โดยกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันที เมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และต้องกำหนดสิทธิ์พิเศษที่ได้รับว่าสามารถเข้าถึงได้ถึงระดับใดได้บ้างและต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

๒.๔ การทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน (Review of user access rights) ต้องมีกระบวนการทบทวนสิทธิ์การเข้าถึงของผู้ใช้งานระบบเทคโนโลยีสารสนเทศและปรับปรุงบัญชีรายชื่อผู้ใช้งานดังนี้

๒.๔.๑ สิทธิ์การเข้าถึงข้อมูลของผู้ใช้งาน (User access rights) ได้รับการพิจารณาทบทวนอย่างสม่ำเสมอตามช่วงระยะเวลาที่กำหนดทุกๆ ๖ เดือน หรือเมื่อการเปลี่ยนแปลง ดังนี้

๒.๔.๑.๑ การบรรจุพนักงานใหม่ ภายใน ๗ วัน

๒.๔.๑.๒ เมื่อมีคำสั่งเปลี่ยนแปลง/โอนย้าย/แต่งตั้งปรับระดับพนักงาน ภายใน ๗ วัน

๒.๔.๑.๓ การลาออกของพนักงาน ภายใน ๗ วัน

๒.๔.๑.๔ การเกษียณอายุราชการ ภายใน ๗ วัน

ISO/IEC 27001:2013 (Annex A): A.9.2.1-5, A.9.3, A.8.1.4

๓. การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

๓.๑ การกำหนดขั้นตอนการเข้าถึงระบบปฏิบัติการ ดังนี้

๓.๑.๑ ผู้ดูแลระบบต้องกำกับให้มีการควบคุมในการเข้าถึงระบบปฏิบัติการอย่างมั่นคงปลอดภัย โดยขั้นตอนการเข้าสู่ระบบ ต้องมีการเปิดเผยข้อมูลเกี่ยวกับระบบให้น้อยที่สุด เพื่อหลีกเลี่ยงผู้ใช้งานที่ไม่ได้รับอนุญาต

๓.๑.๒ ต้องกำหนดระยะเวลาสำหรับใช้ในการป้อนรหัสผ่าน (Password)

๓.๑.๓ ต้องกำหนดให้ระบบแสดงข้อความเตือน “อนุญาตเฉพาะบุคคลที่เกี่ยวข้องมีสิทธิ์เข้าใช้งานเท่านั้น”

๓.๒ การระบุและยืนยันตัวตนของผู้ใช้งาน (User identification and authentication)

๓.๒.๑ กำหนดให้มีบัญชีรายชื่อผู้ใช้งานของแต่ละบุคคลเพื่อใช้ในการพิสูจน์ตัวตนโดยผ่านระบบ Active Directory

๓.๒.๒ ผู้ใช้งานทุกคนต้องผ่านระบบพิสูจน์ตัวตนก่อนเข้าใช้งานระบบปฏิบัติการ โดยแสดงชื่อบัญชีผู้ใช้งานและรหัสผ่าน (Password)

๓.๓ การบริหารจัดการรหัสผ่าน (Password management system) มาตรการและการกำหนดรหัสผ่านตามมาตรฐานสากลที่พึงปฏิบัติ ดังนี้

๓.๓.๑ ผู้ใช้งาน ต้องกำหนดรหัสผ่านให้มีความมั่นคงปลอดภัย โดยรหัสผ่านจะต้องประกอบด้วย

๑) ความยาวไม่น้อยกว่า ๘ ตัวอักขระ

๒) การตั้งรหัสผ่านจะต้องประกอบไปด้วยอักขระอย่างน้อย ๔ ประเภท ดังนี้

- ตัวเลข (Numerical Character)
- ตัวอักษร (Alphabet) พิมพ์ใหญ่
- ตัวอักษร (Alphabet) พิมพ์เล็ก
- ตัวอักขระพิเศษ (Special Character)

๓.๓.๒ ผู้ใช้งาน ต้องไม่ตั้งรหัสผ่านด้วย ชื่อ วันเดือนปีเกิด หรือข้อความใดที่ง่ายต่อการล่วงรู้หรือง่ายต่อการคาดเดา

๓.๓.๓ ผู้ใช้งานต้องไม่ใช้งานรหัสผ่านซึ่งเคยใช้มาแล้ว อย่างน้อย ๓ รหัสผ่านที่เคยใช้งานล่าสุด

๓.๓.๔ ผู้ใช้งานจะต้องเปลี่ยนรหัสผ่าน ทุกๆ ๑๘๐ วันหรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน

๓.๓.๕ ผู้ใช้งาน ต้องใช้งานรหัสผ่านอย่างระมัดระวัง ไม่เปิดเผยรหัสผ่านให้ผู้อื่นได้รับรู้ และต้องรับผิดชอบหากเกิดความเสียหายจากการนำรหัสผ่านไปใช้ในทุกกรณี

๓.๓.๖ ผู้ใช้งาน ต้องไม่บันทึกหรือเก็บรหัสผ่านไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง และต้องไม่จดหรือบันทึกรหัสผ่านไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นโดยบุคคลอื่น

๓.๓.๗ ผู้ใช้งาน จะต้องเปลี่ยนรหัสผ่านครั้งแรกทันที หลังจากที่ได้รับชื่อการเข้าใช้งานและรหัสผ่าน

๓.๔ การใช้งานซอฟต์แวร์อรรถประโยชน์ (Use of system utilities) มีการจำกัดและควบคุมการใช้งานซอฟต์แวร์อรรถประโยชน์สำหรับเครื่องคอมพิวเตอร์ที่สำคัญ เนื่องจากการใช้งานซอฟต์แวร์บางชนิดสามารถทำให้ผู้ใช้งานละเมิดหรือฝ่าฝืนมาตรการป้องกันด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศได้ เพื่อป้องกันการกระทำดังกล่าวให้ดำเนินการดังนี้

๓.๔.๑ จำกัดสิทธิ์การเข้าถึงและกำหนดสิทธิ์ผู้ใช้งานอย่างรัดกุมในการอนุญาตให้ใช้ซอฟต์แวร์ช่วยเหลือต่างๆ โดยระบุในรายการซอฟต์แวร์อรรถประโยชน์ FM-DC-06

๓.๔.๒ อนุญาตให้ใช้งานซอฟต์แวร์ที่ กนอ. จัดหาให้และต้องมีลิขสิทธิ์เท่านั้น

๓.๔.๓ ห้ามติดตั้งซอฟต์แวร์ใดๆ โดยไม่ได้รับอนุญาต

๓.๔.๔ ผู้ดูแลระบบและผู้พัฒนาระบบ ต้องควบคุมให้มีการจำกัดการเข้าถึงซอร์สโค้ด (Source Code) ของโปรแกรม โดยมีระบบ Version Control เช่น Git เป็นต้น

ISO/IEC 27001:2013 (Annex A): A.9.4

๔. การควบคุมการเข้าถึงซอฟต์แวร์ประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and information access control) โดยต้องมีการควบคุมอย่างน้อยดังนี้

๔.๑ การควบคุมการเข้าถึงซอฟต์แวร์ประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Information access restriction)

๔.๑.๑ กนอ. ติดตั้งซอฟต์แวร์ประจำเครื่องสำหรับปฏิบัติงานทั่วไปให้แก่ผู้ใช้งาน ได้แก่ ซอฟต์แวร์ด้านงานเอกสาร เช่น Word ,Excel, Powerpoint, Browser เพื่อใช้ปฏิบัติงาน

๔.๑.๒ ผู้ปฏิบัติงานที่จำเป็นต้องใช้งาน Software เฉพาะเช่น ERP จะได้รับการติดตั้งซอฟต์แวร์เฉพาะที่จำเป็นต้องใช้งาน เช่น Java Runtime เป็นต้น

๔.๑.๓ การเข้าถึงแอปพลิเคชั่นผ่านทางเครือข่ายของ กนอ. ผู้ดูแลระบบต้องกำหนดให้มีการพิสูจน์ตัวตนผู้ใช้งานที่ปลอดภัย โดยใช้บัญชีรายชื่อผู้ใช้งานและรหัสผ่าน (Password)

๔.๑.๔ การเข้าถึงแอปพลิเคชั่นระยะไกลผ่านทางเครือข่ายอินเทอร์เน็ตให้ใช้ช่องทาง Secure Sockets Layer Virtual Private Network (SSL VPN) และต้องกำหนดให้มีการพิสูจน์ตัวตนผู้ใช้งานที่ปลอดภัย โดยใช้บัญชีรายชื่อผู้ใช้ (User account) และรหัสผ่าน (Password)

๔.๑.๕ ผู้ดูแลระบบ (System Administartor) ต้องกำหนดให้จำกัดเวลาการเชื่อมต่อ (Limitation of Connection Time) ๑๒ ชม. สำหรับการเข้าถึงแอปพลิเคชั่นและสารสนเทศต่อการเชื่อมต่อ ๑ ครั้ง

๔.๑.๖ ผู้ดูแลระบบ (System Administartor) ต้องบันทึกข้อมูลหรือพฤติกรรมการใช้งานข้อมูล โดยจัดเก็บ Audit Log เป็น Log File ที่ใช้เก็บข้อมูลการเข้าถึงระบบของผู้ใช้งานเพื่อตรวจสอบว่าใครนำเข้ามาใช้งานในระบบการตรวจสอบการบุกรุก

๔.๑.๗ ในกรณีมีการจ้างพนักงาน Outsource กำหนดมาตรการในการควบคุมการเข้าถึงแอปพลิเคชั่นและสารสนเทศ ดังนี้

๔.๑.๗.๑ กำหนดให้มีคณะกรรมการตรวจรับพัสดุเป็นผู้กำกับดูแลการดำเนินงานต่างๆ ของพนักงาน Outsource

๔.๑.๗.๒ แจ้งให้พนักงาน Outsource รับทราบและปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๔.๑.๗.๓ หากในสัญญาไม่ครอบคลุมข้อกำหนดด้านความมั่นคงปลอดภัยของสารสนเทศ ให้พนักงาน Outsource ลงนามในแบบฟอร์มการรักษาความลับของข้อมูล Non Disclosure Agreement

๔.๒ กำหนดคุณสมบัติการการเข้าถึงแอปพลิเคชั่นและสารสนเทศ ดังนี้

๔.๒.๑ ไม่มีหรือไม่แสดง Function ให้ความช่วยเหลือระหว่างการล็อกอิน (Login)

๔.๒.๒ บันทึกความพยายามในการล็อกอิน (Login) ที่สำเร็จและไม่สำเร็จ และแสดงประวัติการล็อกอิน (Login) ๓ ครั้งล่าสุด

๔.๒.๓ ตัดการเชื่อมต่อหลังจากการล็อกอิน (Login) ไม่สำเร็จเกินกว่า ๓ ครั้ง

๔.๓ การแยกระบบเทคโนโลยีสารสนเทศที่มีความสำคัญสูง (Network Diagram)

๔.๓.๑ ระบบเทคโนโลยีสารสนเทศมีความสำคัญต่อ กนอ. สูงต้องถูกแยกออกจากระบบเทคโนโลยีสารสนเทศอื่นๆ ได้แก่ ระบบการอนุมัติ-อนุญาตทางอิเล็กทรอนิกส์ (Electronics–permission & Privilege: e-PP) ระบบเทคโนโลยีสารสนเทศด้านการบัญชี การเงิน งบประมาณและพัสดุ (Enterprise Resource Planning: ERP) เว็บไซต์ของ กนอ. (Internet Website) ระบบ Mail.go.th และระบบการจัดการการไหลเวียนของงานในรูปแบบอิเล็กทรอนิกส์ (Workflow)

๔.๓.๒ จัดทำระบบสำรองของระบบเทคโนโลยีสารสนเทศที่มีความสำคัญสูงตามแนวปฏิบัติที่เกี่ยวข้องกับการสำรองข้อมูลและระบบเทคโนโลยีสารสนเทศ และการเตรียมความพร้อมกรณีฉุกเฉินตามที่ กนอ. กำหนดโดยมี DR Site สำหรับกรณีฉุกเฉิน

๔.๓.๓ มีเครื่องมือ (Tools) เพื่อใช้ในการตรวจสอบสภาพพร้อมใช้งานของระบบเทคโนโลยีสารสนเทศที่มีความสำคัญสูง ได้แก่ ระบบ Network Monitoing และระบบ Applicaton Monitoring ดูแลเฝ้าระวังโดยผู้ดูแลระบบของแต่ละระบบ

ISO/IEC 27001:2013 (Annex A): A.9.4

๔.๔ การปฏิบัติงานจากภายนอก กนอ. (Teleworking)

๔.๔.๑ กำหนดการเข้าถึงแอปพลิเคชั่นและสารสนเทศได้ ๒ ช่องทาง ดังนี้

๔.๔.๑.๑ การเข้าถึงแอปพลิเคชั่นและสารสนเทศที่เปิดให้ใช้งานจากภายนอกได้โดยตรง ได้แก่ Website : www.ieat.go.th ระบบ e-Mail ระบบ e-PP และระบบ workflow

๔.๔.๑.๒ การเข้าถึงแอปพลิเคชั่นและสารสนเทศผ่าน SSL-VPN ของ กนอ. ได้แก่ ERP

๔.๔.๒ ผู้ใช้งานที่ทำการเข้าถึงระบบเครือข่ายจากระยะไกลทุกคนต้องผ่านการพิสูจน์ตัวตนเพื่อเพิ่มความปลอดภัยและต้องมีการตรวจสอบ ได้แก่ รหัสผ่าน (Password) หรือวิธีการเข้ารหัส (Encryption)

๔.๔.๓ ไม่อนุญาตให้ใช้งานอุปกรณ์ฮาร์ดแวร์ที่เป็นของส่วนตัว เพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศจากระยะไกลหากอุปกรณ์ดังกล่าวไม่อยู่ภายใต้การควบคุมตามนโยบายความมั่นคงปลอดภัยของ กนอ.

๔.๔.๔ ต้องกำหนดชนิดของงาน ชั่วโมงการทำงาน ชั้นความลับของสารสนเทศ ระบบงานและบริการต่างๆ ของ กนอ. ที่อนุญาตและไม่อนุญาตให้มีการเข้าถึงระบบเครือข่ายจากระยะไกล

ISO/IEC 27001:2013 (Annex A): A.6.2

๕. การเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย (Server)

๕.๑ กำหนดมาตรการควบคุมการเข้าถึงและการใช้งานระบบเครือข่าย (Network) และคอมพิวเตอร์แม่ข่าย (Server) ดังนี้

๕.๑.๑ บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าถึงคอมพิวเตอร์แม่ข่ายของ กนอ. ต้องขออนุญาตเป็นลายลักษณ์อักษร แบบฟอร์มการขออนุญาตปฏิบัติงานของบุคคลภายนอก FM-DC-07 และต้องได้รับอนุญาตจาก ผอ.กองที่เกี่ยวข้องก่อนดำเนินการ

๕.๑.๒ ผู้ดูแลระบบต้องไม่เปิดพอร์ตที่ใช้ทิ้งเอาไว้โดยไม่จำเป็นและพอร์ตดังกล่าวต้องตัดการเชื่อมต่อ เมื่อไม่ได้ใช้งานแล้วโดยอัตโนมัติและเปิดให้ใช้ได้ต่อเมื่อมีการร้องขอที่จำเป็นเท่านั้น

๕.๑.๓ กำหนดให้การเข้าถึงคอมพิวเตอร์แม่ข่าย (Server) ต้องใช้มาตรการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าถึงระบบเทคโนโลยีสารสนเทศภายใน เช่น VPN หรือ SSL เป็นต้น

๕.๒ การติดตั้งซอฟต์แวร์บนเครื่องคอมพิวเตอร์แม่ข่าย (Server)

๕.๒.๑ ห้ามผู้ที่ไม่ได้รับอนุญาตเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือกระทำการใดๆ ต่ออุปกรณ์ของเครื่องแม่ข่าย อุปกรณ์ต่อพ่วง หรืออุปกรณ์ฮาร์ดแวร์อื่นๆ ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) หรืออุปกรณ์อื่นๆ ที่เกี่ยวข้อง โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ (System Administrator)

ISO/IEC 27001:2013 (Annex A): A.9.4, A.13.1.1

๕.๓ ทบทวนการทำงานของระบบเทคโนโลยีสารสนเทศหลังจากที่มีการเปลี่ยนแปลงระบบ

๕.๓.๑ แจ้งให้ผู้ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศได้รับทราบเกี่ยวกับการเปลี่ยนแปลงของระบบเพื่อให้บุคคลเหล่านั้นมีเวลาเพียงพอในการดำเนินการทดสอบและทบทวนก่อนที่จะดำเนินการเปลี่ยนแปลงระบบ

๕.๓.๒ พิจารณาวางแผนดำเนินการเปลี่ยนแปลงระบบเทคโนโลยีสารสนเทศรวมทั้งวางแผนด้านงบประมาณที่จำเป็นต้องใช้ในกรณีที่ กนอ. ต้องเปลี่ยนไปใช้ระบบเทคโนโลยีสารสนเทศใหม่

๕.๔ การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก

๕.๔.๑ ผู้พัฒนาระบบภายนอกต้องปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ กนอ. อย่างเคร่งครัด

๕.๔.๒ จัดให้มีการควบคุมโครงการพัฒนาซอฟต์แวร์สำหรับผู้รับจ้างจากภายนอก

๕.๔.๓ กำหนดเรื่องการสงวนสิทธิ์เพื่อตรวจสอบด้านคุณภาพและความถูกต้องของซอฟต์แวร์ที่มีการพัฒนา โดยระบุไว้ในสัญญาจ้างที่ทำกับผู้รับจ้างจากภายนอกนั้น

๕.๕ การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ (Log) โดยเก็บรักษาข้อมูลของผู้ใช้งานเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ใช้บริการนับตั้งแต่เริ่มใช้บริการและต้องเก็บรักษาไว้เป็นเวลาไม่น้อยกว่า ๙๐ วัน นับตั้งแต่การใช้งานสิ้นสุดลงการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ (Log) ต้องใช้วิธีการที่มั่นคงปลอดภัย โดยปฏิบัติตามระเบียบปฏิบัติเรื่อง การบันทึก จัดเก็บหลักฐาน และเฝ้าระวังระบบสารสนเทศ (Logging and Monitoring) QP-DC-06

ISO/IEC 27001:2013 (Annex A): A.14.2.3, A.12.4

ตัวชี้วัดผลลัพธ์

๑. จัดทำเอกสารกำหนดกลุ่มผู้ใช้งานและสิทธิการเข้าถึงเป็นลายลักษณ์อักษร

๒. ทบทวนสิทธิและกลุ่มผู้ใช้งานอย่างน้อยปีละ ๑ ครั้ง

๓. มีระบบยืนยันตัวตนที่สามารถทวนสอบกับข้อมูลจราจรทางคอมพิวเตอร์ได้ (log)

ส่วนที่ ๔
การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม
(Physical and Environmental Security)

วัตถุประสงค์

๑. เพื่อให้ กนอ. มีแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศสำหรับการรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and Environmental Security) ของ กนอ.

๒. เพื่อให้ผู้รับผิดชอบและผู้มีส่วนเกี่ยวข้อง ได้แก่ ผู้บริหารระดับสูง ผู้บริหาร ผู้ดูแลระบบ เจ้าหน้าที่หน่วยงานเจ้าของสารสนเทศ บุคคลภายนอกที่ปฏิบัติงานให้กับ กนอ. และบุคคลภายนอกที่ได้รับอนุญาตให้เข้าถึงและใช้งานสารสนเทศของ กนอ. รับทราบและทำความเข้าใจ รวมทั้งปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างเคร่งครัด

ขอบเขต

บังคับใช้กับทุกหน่วยงานใน กนอ.

อ้างอิงมาตรฐาน

๑. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศตามวิธีแบบปลอดภัย พ.ศ. ๒๕๕๕

๒. มาตรฐาน ISO/IEC 27001:2013 (Annex A)

แนวทางปฏิบัติ

๑. การรักษาความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม (Physical and Environmental Security)

๑.๑ การกำหนดบริเวณหรือพื้นที่

๑.๑.๑ กำหนดพื้นที่การใช้งานระบบเทคโนโลยีสารสนเทศที่ต้องมีการรักษาความมั่นคงปลอดภัย โดยกำหนดพื้นที่ดังนี้ Secure Area พื้นที่ควบคุม, Loading Area พื้นที่รับส่งสิ่งของ

๑.๑.๒ กำหนดการควบคุมการเข้า-ออกพื้นที่ที่ติดตั้งระบบเทคโนโลยีสารสนเทศ (Data Center) ควบคุมด้วย Finger Scan และผู้เข้าออกต้องลงบันทึกในบันทึกการเข้าออก Data Center FM-DC-08

๑.๑.๓ ควบคุมการเข้าออกพื้นที่ที่ต้องมีการรักษาความมั่นคงปลอดภัยด้านกายภาพ (Secure Area) ได้แก่ ศูนย์คอมพิวเตอร์ และห้องปฏิบัติงานของเจ้าหน้าที่ศูนย์คอมพิวเตอร์ (Securing offices, rooms and facilities) โดยต้องกำหนดให้เฉพาะผู้มีสิทธิที่สามารถเข้าออกได้ และมีการเก็บบันทึกการเข้าออกศูนย์คอมพิวเตอร์ และบันทึกการเข้าออกดังกล่าวต้องมีรายละเอียดเกี่ยวกับตัวบุคคล เวลาผ่านเข้าออก รวมถึงต้องมีการตรวจสอบบันทึกดังกล่าวอย่างสม่ำเสมอ

๑.๑.๔ Vendor ที่นำเครื่องคอมพิวเตอร์หรืออุปกรณ์คอมพิวเตอร์ที่ใช้ในการปฏิบัติงานและเชื่อมต่อเข้ากับระบบเครือข่ายของ กนอ. ต้องลงบันทึกในแบบฟอร์มการขออนุญาตปฏิบัติงานของบุคคลภายนอก FM-DC-07 และต้องได้รับอนุญาตจาก ผอ.กองที่เกี่ยวข้องกับงานนั้น หรือผู้ดูแลระบบที่ได้รับมอบหมายก่อนการใช้งาน

๑.๑.๕ ศูนย์คอมพิวเตอร์ มีการออกแบบและติดตั้งการป้องกันความมั่นคงปลอดภัยด้านกายภาพ เพื่อป้องกันภัยจากภายนอกทั้งที่ก่อโดยมนุษย์หรือภัยธรรมชาติ เช่น อัคคีภัย อุทกภัย การก่อจลาจล เป็นต้น

๑.๑.๖ กำหนดพื้นที่การส่งมอบอุปกรณ์ และพื้นที่การเตรียมหรือประกอบอุปกรณ์สารสนเทศก่อนนำเข้าศูนย์คอมพิวเตอร์ โดยต้องควบคุมการเข้าออกในช่วงที่มีการเคลื่อนย้ายหรือประกอบอุปกรณ์คอมพิวเตอร์ เพื่อหลีกเลี่ยงการเข้าถึงระบบสารสนเทศและข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต

ISO/IEC 27001:2013 (Annex A): A.11.1-6, A.11.2.1-2

๑.๒ การเดินสายไฟ สายสัญญาณ สายสื่อสาร และสายเคเบิ้ลอื่นๆ (Cabling security)

๑.๒.๑ หลีกเลี่ยงการเดินสายสัญญาณของระบบเครือข่ายที่ต้องผ่านบริเวณที่มีบุคคลภายนอกเข้าถึงได้

๑.๒.๒ ทำป้ายชื่อ (Label) สำหรับสายสัญญาณบนอุปกรณ์เครือข่ายเพื่อป้องกันการตัดต่อสัญญาณผิดเส้น

ISO/IEC 27001:2013 (Annex A): A.11.2.3

๑.๓ การบำรุงรักษาอุปกรณ์ (Equipment maintenance)

๑.๓.๑ บำรุงรักษาอุปกรณ์ของระบบเทคโนโลยีสารสนเทศตามรอบระยะเวลาที่กำหนดในสัญญาจ้างผู้ให้บริการ

๑.๓.๒ จัดเก็บบันทึกกิจกรรมการบำรุงรักษาทุกครั้ง ตามสัญญาจ้างผู้ให้บริการ โดยมีรายงานของผู้ให้บริการจัดส่งให้กับคณะกรรมการตรวจรับ

๑.๓.๓ จัดเก็บบันทึกปัญหาและข้อบกพร่องและวิธีแก้ปัญหาทุกครั้งที่พบ โดยผู้รับจ้างจะมีรายงานของจัดส่งให้กับคณะกรรมการตรวจรับ

ISO/IEC 27001:2013 (Annex A): A.11.2.4

๑.๔ การนำทรัพย์สินของ กนอ. ออกไปใช้งานนอก กนอ. (Removal of property)

๑.๔.๑ ผู้ใช้งานต้องแจ้งนำทรัพย์สินของ กนอ. ออกไปใช้งานนอก กนอ. และต้องได้รับการอนุญาตจาก ผอ.ฝดจ. โดยผู้ขอนำออกกรอกแบบฟอร์มขอนำสิ่งของออกนอกศูนย์คอมพิวเตอร์ FM-DC-09 หรือผู้ที่ได้รับมอบหมาย ก่อนดำเนินการ

๑.๔.๒ เมื่อนำทรัพย์สินของ กนอ. ส่งคืน ผู้ดูแลระบบต้องตรวจสอบการชำรุดเสียหายและบันทึกการนำทรัพย์สินของ กนอ. ออกไปใช้ภายนอก เพื่อเก็บไว้เป็นหลักฐานป้องกันการชำรุดสูญหาย

๑.๔.๓ ไม่ทิ้งอุปกรณ์หรือทรัพย์สินของ กนอ. ไว้โดยลำพังในที่สาธารณะ หรือบริเวณที่มีผู้ไม่เกี่ยวข้องสามารถเข้าถึงอุปกรณ์ประมวลผลได้ขณะผู้ใช้งานไม่อยู่ โดยผู้ใช้งานต้องรับผิดชอบดูแลเสมือนเป็นทรัพย์สินของตนเอง

๑.๔.๔ การปฏิบัติงานในการจัดเก็บข้อมูลอิเล็กทรอนิกส์ที่สามารถถอดหรือต่อพ่วงกับเครื่องคอมพิวเตอร์ได้ (Removable Media) ให้พิจารณาชั้นความลับของข้อมูล หากเป็นข้อมูลในชั้นความลับ Secret จำเป็นต้องเข้ารหัสข้อมูลก่อนจัดเก็บใน Removable media

๑.๔.๕ ต้องมีการป้องกันอุปกรณ์ที่ใช้จัดเก็บข้อมูลสารสนเทศ ในกรณีที่มีการเคลื่อนย้ายอุปกรณ์ เพื่อมิให้มีการเข้าถึงโดยมิได้รับอนุญาต หรือถูกนำไปใช้งานผิดประเภท หรืออุปกรณ์หรือข้อมูลสารสนเทศได้รับความเสียหาย

ISO/IEC 27001:2013 (Annex A): A.11.2.8,

๑.๕ การป้องกันอุปกรณ์ที่อยู่ภายนอกสำนักงาน กนอ. (Security of Equipment off-premises)

๑.๕.๑ อุปกรณ์ประมวลผลที่ติดตั้งอยู่นอกพื้นที่ของ กนอ. จะมีการพิจารณาถึงความเหมาะสมของตำแหน่งติดตั้ง ระบบสนับสนุนที่เหมาะสม ปลอดภัยและสะดวกในการบริหารจัดการ ได้แก่ DR Site บำรุงรักษาโดยผู้ให้บริการ(Vendor) พร้อมส่งรายงานมาให้ฝ่ายดิจิทัล

๑.๖ การกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง (Secure disposal or re-use of equipment)

๑.๖.๑ กำหนดให้ทำลายสารสนเทศสำคัญก่อนการกำจัดอุปกรณ์หรือหมดสัญญาการใช้งาน

๑.๖.๒ กำหนดมาตรการหรือเทคนิคการลบหรือเขียนทับบนสารสนเทศที่สำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูลก่อนอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้มีการเข้าถึงสารสนเทศที่สำคัญนั้นได้ เช่น ลบข้อมูลด้วย Software CBL Data Shredder

ISO/IEC 27001:2013 (Annex A): A.11.2.7

๑.๗ การรักษาความมั่นคงปลอดภัยสำหรับเอกสารของระบบเทคโนโลยีสารสนเทศ (Clear desk and clear screen policy)

๑.๗.๑ จัดเก็บเอกสารที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศไว้ในสถานที่ที่มั่นคงปลอดภัยเลี่ยงการเก็บไฟล์ไว้ที่หน้า Desktop ของคอมพิวเตอร์

๑.๗.๒ ผู้ใช้งาน ต้องไม่ทิ้งเอกสารที่เป็นลำดับชั้นความลับ ลับมาก ไว้ที่เครื่องถ่ายเอกสาร เครื่องปริ้นท์เตอร์ หรือเครื่องสแกนเนอร์ เมื่อสั่งพิมพ์หรือสำเนาแล้วต้องเก็บเอกสารทันที

๑.๗.๓ ผู้ใช้งาน ต้องไม่ทิ้งเอกสารสำคัญหรือสื่อบันทึกข้อมูลอิเล็กทรอนิกส์ (Removable Media) ไว้ในบริเวณที่ผู้ไม่เกี่ยวข้องเข้าถึงได้ เช่น พื้นที่สาธารณะ พื้นที่ใช้งานร่วมกับหน่วยงานภายนอก กนอ. เป็นต้น รวมถึงพิจารณาความจำเป็นในการเข้ารหัสข้อมูลตามชั้นความลับหากมีการเก็บข้อมูลที่มีความอ่อนไหวระดับ Confidential ขึ้นไป

ISO/IEC 27001:2013 (Annex A): A.8.3.1, A.11.2.9

๑.๘ การทำลายสื่อบันทึกข้อมูล (Disposal of Media) การทำลายสื่อบันทึกข้อมูลเมื่อยกเลิกการใช้งานเพื่อป้องกันข้อมูลรั่วไหล

๑.๘.๑ ผู้รับผิดชอบทำลายสื่อบันทึกข้อมูล จัดทำแบบขอทำลายสื่อบันทึกข้อมูลและข้อมูลบนสื่อบันทึกข้อมูล FM-DC-13 เสนอต่อ ผอ.ฝดจ.

๑.๘.๒ ผู้รับผิดชอบทำลายข้อมูลสื่อบันทึกข้อมูลที่ยกเลิกการใช้งาน โดยการทุบทำลายทางกายภาพ ให้ชำรุดจนไม่สามารถใช้งานได้

ISO/IEC 27001:2013 (Annex A): A.8.3.2

๑.๙ การเคลื่อนย้ายสื่อบันทึก (Physical media transfer

การเคลื่อนย้ายสื่อบันทึกเช่น Backup Disk ผู้ดูแลรับผิดชอบต้องดำเนินการด้วยความระมัดระวัง ป้องกันการสูญหาย ป้องกันข้อมูลรั่วไหล และป้องกันความเสียหายที่อาจกระทบต่อข้อมูลภายใน เช่น สนามแม่เหล็ก ความร้อน ความเย็น ความชื้น รวมถึงหากนำไปจัดเก็บภายนอก กนอ. จะต้องมั่นใจว่าสถานที่ดังกล่าวมีมาตรการดูแลที่เพียงพอและเหมาะสมในการป้องกันสื่อบันทึกไม่ให้สูญหาย ป้องกันข้อมูลรั่วไหล และป้องกันความเสียหายที่อาจกระทบต่อข้อมูลภายใน เช่น สนามแม่เหล็ก ความร้อน ความเย็น ความชื้น

๑.๑๐ อุปกรณ์สนับสนุนระบบสารสนเทศ (Supporting utilities) กนอ.มีอุปกรณ์ที่จำเป็นในการสนับสนุนระบบสารสนเทศสำหรับศูนย์คอมพิวเตอร์ได้แก่ UPS , ระบบดับเพลิง , ระบบทำความเย็น , เครื่องปั่นไฟ ซึ่งอุปกรณ์เหล่านี้มีการกำกับดูแลการบำรุงรักษาตามสัญญาจ้าง

ISO/IEC 27001:2013 (Annex A): A.8.3.3

ตัวชี้วัดผลลัพธ์

๑. กำหนดพื้นที่รักษาความมั่นคงปลอดภัยเข้มงวด (Secure Area) เป็นลายลักษณ์อักษรเพื่อวางมาตรการที่เหมาะสม

๒. ควบคุมการเข้าออกศูนย์คอมพิวเตอร์(Data Center) โดยการยืนยันตัวตนและมีบันทึกตรวจสอบชัดเจน

๓. ศูนย์คอมพิวเตอร์ (Data Center) มีระบบสนับสนุนเพียงพอ ได้แก่ ระบบดับเพลิง ระบบไฟฟ้าสำรอง ระบบควบคุมการเข้าออก บันทึกการเข้าออก CCTV

ส่วนที่ ๕
การรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร
(Communications Security)

วัตถุประสงค์

๑. เพื่อให้ กนอ. มีแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศสำหรับการรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร (Communications Security) ของ กนอ.

๒. เพื่อให้ผู้รับผิดชอบและผู้มีส่วนเกี่ยวข้อง ได้แก่ ผู้บริหารระดับสูง ผู้บริหาร ผู้ดูแลระบบ เจ้าหน้าที่หน่วยงานเจ้าของสารสนเทศ บุคคลภายนอกที่ปฏิบัติงานให้กับ กนอ. และบุคคลภายนอกที่ได้รับอนุญาตให้เข้าถึงและใช้งานสารสนเทศของ กนอ. รับทราบและทำความเข้าใจ รวมทั้งปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างเคร่งครัด

ขอบเขต

บังคับใช้กับทุกหน่วยงานใน กนอ.

อ้างอิงมาตรฐาน

๑. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศตามวิธีแบบปลอดภัย พ.ศ. ๒๕๕๕

๒. มาตรฐาน ISO/IEC 27001:2013 (Annex A)

แนวทางปฏิบัติ

๑. การควบคุมการเข้าถึงระบบเครือข่าย (Network access control)

๑.๑ การใช้บริการของระบบเครือข่าย (Network) ต้องกำหนดให้ผู้ใช้งาน (Users) สามารถเข้าถึงระบบเทคโนโลยีสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น ตาม Access Control Matrix FM-DC-03

๑.๑.๑ ห้ามผู้ใช้งานกระทำการใดๆ ที่เป็นการขัดต่อกฎหมายหรือศีลธรรมอันดีแห่งสาธารณชน โดยผู้ใช้งานรับรองว่าหากมีการกระทำการใดๆ ดังกล่าวย่อมถือว่าอยู่นอกเหนือความรับผิดชอบของ กนอ.

๑.๑.๒ กนอ. ไม่อนุญาตให้ผู้ใช้งานกระทำการใดๆ ที่เข้าข่ายลักษณะเพื่อการค้าหรือการแสวงหาผลกำไรผ่านระบบเครือข่าย เช่น การประกาศแจ้งความการซื้อหรือการจำหน่ายสินค้า การนำสารสนเทศไปซื้อขาย การรับบริการค้นหาสารสนเทศโดยคิดค่าบริการ การให้บริการโฆษณาสินค้าหรือการเปิดบริการอินเทอร์เน็ตแก่บุคคลทั่วไปเพื่อแสวงหากำไร เป็นต้น

๑.๑.๓ ผู้ใช้งานต้องไม่ละเมิดต่อผู้อื่น กล่าวคือ ผู้ใช้งานต้องไม่อ่าน เขียน ลบ เปลี่ยนแปลง หรือแก้ไขใดๆ ในส่วนที่มิใช่ของตนโดยไม่ได้รับอนุญาต การบุกรุก (Hack) เข้าสู่บัญชีรายชื่อผู้ใช้งาน (UserAccount) ของผู้อื่น การเผยแพร่ข้อความใดๆ ที่ก่อให้เกิดความเสียหายเสื่อมเสียแก่ผู้อื่น การใช้ภาษาไม่สุภาพหรือการเขียนข้อความที่ทำให้ผู้อื่นเสียหายถือเป็นการละเมิดสิทธิ์ของ กนอ. หรือผู้อื่นทั้งสิ้น ผู้ใช้งานต้องรับผิดชอบแต่เพียงฝ่ายเดียว กนอ. ไม่มีส่วนร่วมรับผิดชอบความเสียหายดังกล่าว

๑.๑.๔ ห้ามมิให้ผู้ใดเข้าใช้งานโดยไม่ได้รับอนุญาต การบุกรุกหรือพยายามบุกรุกเข้าสู่ระบบเครือข่ายถือว่าเป็นการพยายามรุกล้ำเขตหวงห้ามของ กนอ.

๑.๑.๕ การกำหนดบัญชีรายชื่อผู้ใช้งานเป็นการเฉพาะบุคคลเท่านั้น ผู้ใช้งานจะโอนหรือจ่ายแจกสิทธิ์นี้ให้กับผู้อื่นไม่ได้

๑.๑.๖ กำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบเทคโนโลยีสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

๑.๑.๗ ห้ามเปิดหรือใช้งานซอฟต์แวร์ประเภท Peer-to-Peer หรือซอฟต์แวร์ลักษณะเดียวกัน

๑.๑.๘ การใช้งานอินเทอร์เน็ตจะถูกบันทึกการใช้งานเป็นระยะเวลา ๙๐ วัน ตาม พ.ร.บ. ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐

๑.๒ การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอก กนอ. (User authentication for external connections)

๑.๒.๑ การแสดงตัวตน (Identification) ด้วยชื่อผู้ใช้งานและการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่าน (Password) หรือวิธีการอื่นที่ กนอ. กำหนด

๑.๒.๒ การเข้าสู่ระบบจากระยะไกล (Remote access) เพื่อเพิ่มความปลอดภัยจะต้องมีการตรวจสอบเพื่อพิสูจน์ตัวตนของผู้ใช้งานสิทธิ์ และมีการใช้การเข้ารหัส ได้แก่ VPN

๑.๓ การระบุอุปกรณ์บนเครือข่าย (Equipment identification in networks)

๑.๓.๑ จัดทำแผนผังระบบเครือข่าย (Network diagram) ของ กนอ. โดยมีรายละเอียดของระบบเครือข่ายภายในและระบบเครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งดำเนินการปรับปรุงให้เป็นปัจจุบันอยู่เสมอ อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง

๑.๔ การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote diagnostic and configuration port protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย

๑.๔.๑ กำหนดค่าเริ่มต้นพื้นฐานของระบบเครือข่ายต้องเป็นแบบอนุญาตบางส่วน และปฏิเสธทั้งหมด (Permit Any & Deny All)

๑.๔.๒ ผู้ดูแลระบบควบคุมการเปิด–ปิดพอร์ตของอุปกรณ์เครือข่ายเพื่อควบคุมการเข้าถึงพอร์ตของอุปกรณ์เครือข่ายต่างๆ โดยปิดพอร์ตที่เสี่ยงที่จะก่อให้เกิดความเสียหายต่อระบบเครือข่าย

๑.๔.๓ บุคคลภายนอกเข้ามาติดต่อหรือเข้ามาดำเนินการใดๆ ในห้องติดตั้งระบบเครือข่ายหรือระบบเทคโนโลยีสารสนเทศ (Data Center) จะต้องลงชื่อเข้า-ออกใน แบบฟอร์มบันทึกการเข้าออก Data

Center FM-DC-08 ให้ถูกต้องและได้รับการอนุญาตก่อนเข้าดำเนินการ และจะต้องมีเจ้าหน้าที่ของ กนอ. อยู่กับบุคคลที่เข้าดำเนินการตลอดเวลา

๑.๔.๔ บุคคลภายนอกเข้ามาดำเนินการบำรุงรักษาบริหารจัดการพอร์ตของอุปกรณ์เครือข่ายหรือบริหารจัดการผ่านระบบเครือข่ายต้องได้รับการอนุมัติจาก ผอ.ฝดจ. ก่อนการดำเนินการ ตามแบบฟอร์ม ขออนุญาตปฏิบัติงานของบุคคลภายนอก FM-DC-07

๑.๔.๕ ยกเลิกหรือปิดพอร์ตและบริการบนอุปกรณ์เครือข่ายที่ไม่มีความจำเป็นในการใช้งาน

๑.๕ การแบ่งแยกเครือข่าย (Segregation in networks)

๑.๕.๑ ออกแบบระบบเครือข่ายโดยจัดแบ่งตามกลุ่มของระบบเทคโนโลยีสารสนเทศที่มีการใช้งานตามกลุ่มของผู้ใช้งานโดยจัดแบบออกเป็นเขตภายใน (Internal zone) และเขตภายนอก (External zone) และเขตสำหรับการให้บริการ (Demilitarize zone : DMZ) เพื่อควบคุมและป้องกันการถูกโจมตี

๑.๕.๒ แบ่งแยกเครือข่ายเป็นเครือข่ายย่อยๆ ทางกายภาพตามอาคารและชั้นต่างๆ ด้วยวิธีแบ่งแยกเครือข่ายเสมือน (Virtual LAN: VLAN) รวมทั้งให้มีการแบ่งแยกเครือข่ายตามระบบหรือแอปพลิเคชันที่มีความสำคัญ

๑.๕.๓ ติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายไว้ในระบบเครือข่ายที่จัดสรรให้เฉพาะ ซึ่งแยกออกจากระบบเครือข่ายของผู้ใช้งานและติดตั้งไฟร์วอลล์ (Firewall) หรืออุปกรณ์เครือข่ายอื่นๆ เพื่อป้องกันทางเข้าเครือข่ายจากผู้ไม่หวังดี

๑.๖ การควบคุมการเชื่อมต่อทางเครือข่าย (Network connection control) ควบคุมการเข้าถึงหรือใช้งานระบบเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างหน่วยงานให้สอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึง ดังนี้

๑.๖.๑ ระบบเครือข่ายทั้งหมดที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ภายนอก กนอ. ต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือซอฟต์แวร์ในการทำ Packet filtering ได้แก่ การใช้ไฟร์วอลล์ (Firewall) หรือฮาร์ดแวร์อื่นๆ รวมทั้งต้องมีความสามารถในการตรวจจับมัลแวร์ (Malware) ด้วย ได้แก่ Anti virus Gateway

๑.๗ การควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control)

๑.๗.๑ ศูนย์ SOC ตรวจสอบการใช้งานของบุคคล ที่เข้าใช้งานระบบเครือข่ายในลักษณะที่ผิดปกติ และมีการแก้ไขเปลี่ยนแปลงระบบเครือข่าย โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

๑.๗.๒ การกำหนดหมายเลข IP address ของระบบเครือข่ายภายในมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อกับระบบเครือข่ายของ กนอ. สามารถมองเห็นโครงสร้างของระบบเครือข่ายได้โดยง่าย

๑.๗.๓ การใช้เครื่องมือต่าง ๆ (Tools) เพื่อการตรวจสอบระบบเครือข่ายต้องได้รับการมอบหมายจากผู้ดูแลระบบและจำกัดการใช้งานเฉพาะเท่าที่จำเป็น และดำเนินการโดยผู้ที่มีความรู้ความสามารถ

ISO/IEC 27001:2013 (Annex A): A.9.1.2, A.13.1.1-3

๒. การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN access control)

๒.๑ ผู้ดูแลระบบ (System Administrator)

๒.๑.๑ ผู้ดูแลระบบทำการลงทะเบียนกำหนดสิทธิ์การเข้าถึงระบบเครือข่ายไร้สายของผู้ใช้งานก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ผู้ดูแลระบบอนุญาตให้ผู้ใช้งานตามความจำเป็นในการใช้งานเท่านั้น

๒.๑.๒ ต้องทำการลงทะเบียนอุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายไร้สาย (Wireless LAN client) ทุกตัว

๒.๑.๓ ต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (Access point) เพื่อป้องกันไม่ให้สัญญาณของอุปกรณ์กระจายสัญญาณรั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายและป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้

๒.๑.๔ ต้องเปลี่ยนค่า SSID (Service set identifier) ที่ถูกกำหนดเป็นค่าเริ่มต้นที่มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณมาใช้งาน

๒.๑.๕ ต้องกำหนดค่าใช้ WPA2 (Wi-Fi protected access) ในการเข้ารหัสข้อมูลระหว่างอุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายไร้สาย (Wireless LAN client) และอุปกรณ์กระจายสัญญาณ (Access point) เพื่อให้ยากต่อการดักจับและทำให้ปลอดภัยมากขึ้น

๒.๑.๖ ติดตั้งอุปกรณ์ป้องกันการบุกรุก (Firewall) ระหว่างเครือข่ายไร้สายกับระบบเครือข่ายภายในของ กนอ.

๒.๑.๗ ใช้ซอฟต์แวร์หรือฮาร์ดแวร์ในการตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ โดย ผู้ให้บริการ (Vendor) ของระบบ wifi เพื่อตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยที่เกิดขึ้นในระบบเครือข่ายไร้สายและเมื่อตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติให้รายงานต่อ ผอ.ฝดจ. หรือ ผอ.ฝกจ. ทราบโดยทันที

ISO/IEC 27001:2013 (Annex A): A.9.1.2

ตัวชี้วัดผลลัพธ์

๑. การเข้าถึงเครือข่ายเป็นไปตามสิทธิและกลุ่มผู้ใช้งานที่ได้รับอนุญาตเท่านั้นตาม Access Control Matrix

๒. มีการจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log) ๙๐ วันตามกฎหมาย

๓. มีระบบตรวจสอบความผิดปกติในเครือข่ายและขั้นตอนการตอบสนองกรณีเกิดเหตุ Incident

ส่วนที่ ๖
การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ
(IT operations security)

วัตถุประสงค์

๑. เพื่อให้ กนอ. มีแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศสำหรับการรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยสารสนเทศ (IT operation security) ของ กนอ.

๒. เพื่อให้ผู้รับผิดชอบและผู้มีส่วนเกี่ยวข้อง ได้แก่ ผู้บริหารระดับสูง ผู้บริหาร ผู้ดูแลระบบ เจ้าหน้าที่หน่วยงานเจ้าของสารสนเทศ บุคคลภายนอกที่ปฏิบัติงานให้กับ กนอ. และบุคคลภายนอกที่ได้รับอนุญาตให้เข้าถึงและใช้งานสารสนเทศของ กนอ. รับทราบและทำความเข้าใจ รวมทั้งปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างเคร่งครัด

ขอบเขต

บังคับใช้กับทุกหน่วยงานใน กนอ.

อ้างอิงมาตรฐาน

๑. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศตามวิธีแบบปลอดภัย พ.ศ. ๒๕๕๕

๒. มาตรฐาน ISO/IEC 27001:2013 (Annex A)

แนวทางปฏิบัติ

ผู้รับผิดชอบและผู้มีส่วนเกี่ยวข้อง ต้องกำหนดให้มีการดูแลเอกสารขั้นตอนหรือวิธีปฏิบัติงานประจำในด้านต่างๆ ที่สำคัญ รวมทั้งดำเนินการทบทวนและปรับปรุงขั้นตอนหรือวิธีการปฏิบัติงานให้เป็นปัจจุบันอยู่เสมอ เพื่อให้บุคลากรสามารถนำไปปฏิบัติได้

๑. การบริหารจัดการขีดความสามารถของระบบ (Capacity Management)

๑.๑ ฝ่ายดิจิทัลพิจารณาทรัพยากรระบบ (Capacity Plan) ของระบบเทคโนโลยีสารสนเทศ

๑.๒ มีการติดตามและเฝ้าระวังการใช้ทรัพยากรของระบบเทคโนโลยีสารสนเทศ

๑.๓ นำข้อมูลการเฝ้าระวัง และการวิเคราะห์ (Utilization Analysis) มาปรับปรุงการจัดการทรัพยากรของระบบเทคโนโลยีสารสนเทศ โดยจัดทำเป็นโครงการด้านสารสนเทศในแต่ละปี

ISO/IEC 27001:2013 (Annex A): A.12.1.3

๒. การรักษาความมั่นคงปลอดภัยของเครื่องแม่ข่าย (Server) และอุปกรณ์ที่ใช้ปฏิบัติงานของผู้ใช้เทคโนโลยีสารสนเทศ (Endpoint)

๒.๑ กำหนดกฎเกณฑ์ควบคุมการติดตั้งซอฟต์แวร์โดยผู้ใช้งาน เพื่อให้ผู้ใช้งานปฏิบัติตาม โดยกำหนดรายการ Software Baseline ที่อนุญาตให้ติดตั้ง เช่น Office, browser,Acrobat reader, ms team ,line สำหรับกลุ่มงานที่ต้องใช้ Software เฉพาะเช่น ERP ก็จะติดตั้ง Software ที่จำเป็นให้เพื่อใช้ปฏิบัติงาน

๒.๒ มีมาตรการในการตรวจหา ป้องกันและกู้คืนจากโปรแกรมไม่ประสงค์ดี ด้วยการติดตั้งซอฟต์แวร์ Anti Virus และ Update ให้ทันสมัยอย่างสม่ำเสมอโดยกำหนดให้ Auto update จากเครื่องผู้ใช้งาน

๒.๓ จำกัดสิทธิ์การเข้าถึงเครื่องแม่ข่ายเพื่อควบคุมให้ผู้ใช้งานสามารถใช้งานเฉพาะระบบที่ได้รับอนุญาตเท่านั้น

๒.๔ ศูนย์ SOC ตรวจจับการบุกรุกเพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของ กนอ. ในลักษณะที่ผิดปกติ

๒.๕ หมายเลข IP Address ภายในระบบเครือข่ายของ กนอ. จำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อกับระบบเครือข่ายของ กนอ. สามารถมองเห็นได้

๒.๖ ปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้ใช้งานได้อย่างจำกัดระยะเวลาเท่าที่จำเป็นโดยต้องได้รับการอนุญาตจากผู้รับผิดชอบเป็นลายลักษณ์อักษรโดยทำบันทึกขออนุมัติ ผอ.กปจ.

๒.๗ การรักษาความปลอดภัยของ Application ที่ให้บริการผ่านเครือข่ายสาธารณะ (Securing application services on public networks) และการป้องกันความปลอดภัยให้แก่Transactionของการให้บริการ (Protecting application services transactions) โดยเมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบเทคโนโลยีสารสนเทศนั้น (Session time-out) ผู้ดูแลระบบต้องตัดเวลาการใช้งานของเครื่องคอมพิวเตอร์เมื่อผู้ใช้งานไม่ได้ใช้งานเป็นระยะเวลาเกิน ๓๐ นาที (Session Timeout)
ISO/IEC 27001:2013 (Annex A): A.12.2.1,A14.1.2-3

๓. การสำรองข้อมูล (Data Backup)

๓.๑ ให้มีการสำรองข้อมูลสำหรับสารสนเทศ ซอฟต์แวร์ ฐานข้อมูล ค่าการตั้งค่าระบบ (Configuration) และอิมเมจของระบบ และให้มีการทดสอบความพร้อมใช้ของข้อมูลอย่างสม่ำเสมอตามที่ กนอ. กำหนด ตามระเบียบปฏิบัติเรื่อง การสำรองข้อมูลและสารสนเทศ (Backup Management) QP-DC-07
ISO/IEC 27001:2013 (Annex A): A.12.3.1

๔. การจัดเก็บข้อมูลบันทึกเหตุการณ์ (Logging) ของเครื่องแม่ข่าย ระบบงาน และอุปกรณ์เครือข่ายที่สำคัญ

เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์มีความถูกต้องตามกฎหมายให้ปฏิบัติตามระเบียบปฏิบัติเรื่อง การบันทึก จัดเก็บหลักฐาน และเฝ้าระวังระบบสารสนเทศ (Logging and Monitoring) QP-DC-06
ISO/IEC 27001:2013 (Annex A): A.12.4.1-4

๕. การติดตามดูแลระบบและเฝ้าระวังภัยคุกคาม

๕.๑ กำหนดให้มีการติดตาม ตรวจสอบ วิเคราะห์และรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศและเหตุละเมิดความมั่นคงปลอดภัยสารสนเทศ

๕.๒ ให้มีการประเมินและตัดสินใจต่อเหตุการณ์และจุดอ่อนด้านความมั่นคงปลอดภัยสารสนเทศ

๕.๓ ให้มีการตอบสนองต่อเหตุละเมิดความมั่นคงปลอดภัยสารสนเทศ ให้ผู้มีอำนาจสูงกว่าในการจัดการต่อเหตุละเมิดความมั่นคงปลอดภัยสารสนเทศ

๕.๔ ให้มีการรายงานสถานการณ์ด้านความมั่นคงปลอดภัยสารสนเทศให้ผู้มีอำนาจให้เร็วที่สุดเท่าที่จะทำได้

๕.๕ ให้มีการจัดเก็บข้อมูลสารสนเทศเพื่อใช้เป็นหลักฐาน เก็บไว้ในกรณีมีการละเมิดความมั่นคงปลอดภัยสารสนเทศ และต้องทำให้มั่นใจได้ว่าหลักฐานจะไม่ถูกเปลี่ยนแปลงหรือทำลาย

ดำเนินการตามระเบียบปฏิบัติเรื่อง การรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยของสารสนเทศ (Reporting Information Security Incident) QP-DC-09
ISO/IEC 27001:2013 (Annex A): A.16.1.1-7

๖. การบริหารจัดการช่องโหว่ (Vulnerability Management)

๖.๑ กระบวนการติดตามข้อมูลเกี่ยวกับช่องโหว่ของระบบเทคโนโลยีสารสนเทศที่มีการใช้งานอย่างสม่ำเสมอ

๖.๒ การบริหารจัดการเพื่อแก้ไขช่องโหว่ โดยการประเมินความเสี่ยงสำหรับช่องโหว่ของระบบเทคโนโลยีสารสนเทศ และกำหนดมาตรการที่เหมาะสมเพื่อจัดการกับความเสี่ยงที่เกิดจากช่องโหว่ทางเทคนิคของระบบ รวมทั้งการประสานงานเพื่อให้ผู้ที่เกี่ยวข้องดำเนินการแก้ไขช่องโหว่ตามความเหมาะสม

๖.๓ ติดตามและศึกษาแหล่งสารสนเทศข่าวสาร เพื่อใช้ในการติดตามช่องโหว่ของระบบเทคโนโลยีสารสนเทศของ กนอ. ดำเนินการตามระเบียบปฏิบัติเรื่อง การจัดการช่องโหว่ด้านความมั่นคงปลอดภัยของสารสนเทศ (Technical Vulnerability Management) QP-DC-08
ISO/IEC 27001:2013 (Annex A): A.12.6.1

๗. การทดสอบเจาะระบบ (Penetration Test)

๗.๑ ให้มีการทดสอบเจาะระบบ (Penetration Test) เพื่อพิจารณาความเสี่ยงสำหรับช่องโหว่ของระบบเทคโนโลยีสารสนเทศสำหรับระบบที่มีความสำคัญ ที่อาจทำให้ผู้ไม่หวังดีสามารถโจมตีได้ โดยจัดให้มีผู้เชี่ยวชาญภายในหรือภายนอกที่มีความเป็นอิสระทำหน้าที่ทดสอบเจาะระบบ สม่ำเสมออย่างน้อยปีละ ๑ ครั้ง

ISO/IEC 27001:2013 (Annex A): A.12.7.1

๘. การบริหารจัดการการเปลี่ยนแปลง (Change Management)

ดำเนินการบริหารจัดการและควบคุมการเปลี่ยนแปลง แก้ไข หรือปรับปรุงระบบสารสนเทศ ซอฟต์แวร์ประยุกต์ และอุปกรณ์คอมพิวเตอร์ต่างๆ ให้ปฏิบัติตามรายการดังต่อไปนี้เป็นอย่างน้อย

๘.๑ ให้ขออนุมัติการดำเนินงานจากผู้มีอำนาจในกรณีดังต่อไปนี้

๘.๑.๑ การติดตั้งอุปกรณ์คอมพิวเตอร์ที่ถูกจัดซื้อใหม่

๘.๑.๒ การติดตั้งซอฟต์แวร์ประยุกต์ที่ถูกจัดซื้อใหม่

๘.๑.๓ การติดตั้งระบบสารสนเทศที่ถูกพัฒนาใหม่

๘.๑.๔ การปรับปรุงซอฟต์แวร์ประยุกต์หรือระบบสารสนเทศจากรุ่น (Version) เก่าเป็นรุ่นใหม่

๘.๑.๕ การปรับปรุงโครงสร้างฐานข้อมูลของระบบสารสนเทศ

๘.๒ วางแผนการเปลี่ยนแปลง ซึ่งประกอบด้วย การติดตั้ง การทดสอบบนเครื่องคอมพิวเตอร์สำหรับการทดสอบ การแจ้งผลการทดสอบแก่ผู้บังคับบัญชา การใช้งานจริง (Production) และการถอยกลับกรณีการเปลี่ยนแปลงมีผลกระทบในทางลบต่อความพร้อมใช้งานของระบบสารสนเทศ ซอฟต์แวร์ประยุกต์ หรืออุปกรณ์คอมพิวเตอร์ โดยระบุในแบบฟอร์มควบคุมการเปลี่ยนแปลง (FM-DC-12)

๘.๓ ประกาศให้ผู้เกี่ยวของในฝ่ายดิจิทัลได้ทราบถึงวันและเวลาที่จะดำเนินการเปลี่ยนแปลง รวมทั้งผลกระทบจากการเปลี่ยนแปลงนั้น

๘.๔ สำรองข้อมูลที่เกี่ยวข้องกับการเปลี่ยนแปลงไว้ในสื่อบันทึกข้อมูลที่แยกออกจากเครื่องคอมพิวเตอร์แม่ข่ายที่เกี่ยวข้องกับการเปลี่ยนแปลงนั้น

๘.๕ ประเมินผลกระทบภายหลังจากการเปลี่ยนแปลงเสร็จสิ้น หากประเมินแล้วพบว่าการเปลี่ยนแปลงส่งผลกระทบในทางลบต่อความพร้อมใช้งานของระบบสารสนเทศ ซอฟต์แวร์ประยุกต์ หรืออุปกรณ์คอมพิวเตอร์ ให้ดำเนินการถอยกลับตามแผนการเปลี่ยนแปลง

ISO/IEC 27001:2013 (Annex A): A.12.1.2

๙. การบริหารจัดการการตั้งค่าระบบ (System Configuration Management)

๙.๑ ให้มีการตั้งค่าระบบให้มีความมั่นคงปลอดภัย โดยกำหนดค่าขั้นต่ำตามมาตรฐานด้านความมั่นคงปลอดภัย (Security Baseline) ให้กับระบบเทคโนโลยีสารสนเทศที่สำคัญของ กนอ. โดยอ้างอิงจาก Center for Internet Security (CIS) หรือแหล่งข้อมูลที่น่าเชื่อถืออื่นๆ

ISO/IEC 27001:2013 (Annex A): A.11.2.1, A.12.5.1

๑๐. การบริหารจัดการ Patch (Patch Management)

๑๐.๑ จัดให้มีกระบวนการในการควบคุมการติดตั้ง patch ของระบบที่ใช้งานจริง เพื่อให้สามารถติดตั้ง Patch ที่สำคัญในการรักษาความมั่นคงปลอดภัยได้อย่างทันการณ์โดยปฏิบัติตามระเบียบปฏิบัติเรื่อง การจัดการช่องโหว่ด้านความมั่นคงปลอดภัยของสารสนเทศ (Technical Vulnerability Management) QP-DC-08

ISO/IEC 27001:2013 (Annex A): A.12.6.1

๑๑. การใช้บริการคอมพิวเตอร์เสมือน (Cloud Computing)

๑๑.๑ มีแนวทางในการบริหารความเสี่ยงที่เกี่ยวข้องกับการใช้บริการ Cloud Computing โดยเลือกใช้ผู้ให้บริการที่มีมาตรฐานและน่าเชื่อถือ มีมาตรการด้านความมั่นคงปลอดภัย

๑๑.๒ พิจารณา Service Level Agreement หรือข้อตกลงการให้บริการของผู้ให้บริการครอบคลุมด้านบริการและด้านความมั่นคงปลอดภัยของสารสนเทศ เพื่อให้มั่นใจว่าผู้ให้บริการสามารถดูแลความมั่นคงปลอดภัยได้อย่างมีประสิทธิภาพ

ISO/IEC 27001:2013 (Annex A): A.14.1.1-3

๑๒. การตรวจสอบระบบสารสนเทศ (Information systems audit considerations)

๑๒.๑ จัดให้มีการตรวจสอบภายในระบบสารสนเทศ ISMS Audit ปีละครั้ง โดยผู้รับผิดชอบด้านการตรวจสอบระบบสารสนเทศ ต้องจัดทำแผนการตรวจสอบระบบสารสนเทศและขั้นตอนการปฏิบัติงานการตรวจสอบระบบสารสนเทศ โดยการกำหนดประเด็นตรวจประเมินครอบคลุมเรื่องความสอดคล้องตามข้อกำหนดด้านความมั่นคงปลอดภัยและมาตรฐานที่เกี่ยวข้อง (Compliance with security policies and standards และ Technical compliance Review)

๑๒.๒ การตรวจประเมินดำเนินการตามระเบียบปฏิบัติเรื่องการตรวจประเมินภายใน QP-DC-02

๑๒.๓ ในหัวข้อ Independent review of information security กนอ.เป็นรัฐวิสาหกิจที่ได้รับการตรวจประเมินตามหลักเกณฑ์การประเมินกระบวนการปฏิบัติงานและการจัดการ (Core Business Enablers) ของรัฐวิสาหกิจทุกปี ซึ่งมีการประเมินด้านความมั่นคงปลอดภัยของสารสนเทศในหมวด5 (Digital Technology) ข้อ5 การบริหารความมั่นคงปลอดภัยสารสนเทศ (Information Security Management)

ISO/IEC 27001:2013 (Annex A): A.12.7.1,A18.2.1-3

ตัวชี้วัดผลลัพธ์

๑. มีการสำรองข้อมูลตามแผนงานสำรองข้อมูลอย่างครบถ้วน

๒. มีการทดสอบกู้คืนข้อมูลตามแผนงานอย่างครบถ้วน อย่างน้อยปีละ ๑ ครั้ง

๓. มีการตรวจสอบช่องโหว่ด้านความมั่นคงปลอดภัยของสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง

ส่วนที่ ๗
การจัดหาและการพัฒนาระบบเทคโนโลยีสารสนเทศ
(System Acquisition and Development)

วัตถุประสงค์

๑. เพื่อให้ กนอ. มีแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศสำหรับจัดหาและการพัฒนาระบบเทคโนโลยีสารสนเทศ (System acquisition and development) ของ กนอ.

๒. เพื่อให้ผู้รับผิดชอบและผู้มีส่วนเกี่ยวข้อง ได้แก่ ผู้บริหารระดับสูง ผู้บริหาร ผู้ดูแลระบบ เจ้าหน้าที่หน่วยงานเจ้าของสารสนเทศ บุคคลภายนอกที่ปฏิบัติงานให้กับ กนอ. และบุคคลภายนอกที่ได้รับอนุญาตให้เข้าถึงและใช้งานสารสนเทศของ กนอ. รับทราบและทำความเข้าใจ รวมทั้งปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างเคร่งครัด

ขอบเขต

บังคับใช้กับทุกหน่วยงานใน กนอ.

อ้างอิงมาตรฐาน

๑. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศตามวิธีแบบปลอดภัย พ.ศ. ๒๕๕๕

๒. มาตรฐาน ISO/IEC 27001:2013 (Annex A)

แนวทางปฏิบัติ

๑. การกำหนดความต้องการด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ (Security Requirements of Information Systems)

ระบุข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสารสนเทศไว้เป็นส่วนหนึ่งของเอกสารแสดงขอบเขตของงาน (TOR) ทั้งงานพัฒนาระบบสารสนเทศใหม่หรืองานปรับปรุงระบบสารสนเทศเดิม ดังนี้

๑.๑. อ้างอิงข้อมูลความต้องการด้านความมั่นคงปลอดภัย (Security Requirement) จาก OWASP (www.owasp.org) ในกรณีการจัดจ้างพัฒนาระบบสารสนเทศในรูปแบบเว็บ (Web Application)

๑.๒. กำหนดการป้องกันทางกายภาพที่เหมาะสมเป็นข้อกำหนดหนึ่งในเอกสารแสดงขอบเขตของงาน (TOR) ในกรณีการจัดหาระบบสารสนเทศที่มีอุปกรณ์ติดตั้งในพื้นที่สาธารณะ (Public Zone)

๑.๓. กำหนดการทดสอบตามขั้นตอนต่างๆ ในเอกสารแสดงขอบเขตของงาน (TOR)

๒. การรักษาความมั่นคงปลอดภัยในกระบวนการพัฒนาระบบสารสนเทศ (Security in Development and Support Process)

๒.๑ จัดให้มีการควบคุมการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบสารสนเทศตามระเบียบปฏิบัติ เรื่อง การควบคุมการเปลี่ยนแปลง (QP-DC-05) จัดเก็บรุ่น (Version) ของระบบสารสนเทศก่อนการเปลี่ยนแปลง และมีกระบวนการถอยกลับสู่สภาพเดิมของระบบ (Fallback) ในกรณีระบบสารสนเทศทำงานผิดพลาดหรือไม่สามารถใช้งานได้

๒.๒ ปรับปรุงเอกสารประกอบระบบสารสนเทศ เช่น เอกสารแสดงรายละเอียดของโครงสร้างข้อมูล คู่มือระบบ ขั้นตอนการทำงานของระบบ ฯลฯ หลังจากการแก้ไขหรือเปลี่ยนแปลงระบบสารสนเทศ รวมทั้ง มีการจัดเก็บเอกสารดังกล่าวในที่ปลอดภัยและสะดวกต่อการใช้งาน

๒.๓ สื่อสารให้กับเจ้าหน้าที่ผู้เกี่ยวข้องได้รับทราบและสามารถปฏิบัติงานได้อย่างถูกต้อง

๒.๔ บันทึกและจัดเก็บหลักฐานที่เกี่ยวข้องกับการแก้ไขหรือเปลี่ยนแปลงระบบสารสนเทศตามระเบียบปฏิบัติ เรื่อง การควบคุมการเปลี่ยนแปลง (QP-DC-05)

๒.๕ จัดให้มีการทดสอบระบบสารสนเทศที่ได้รับการพัฒนา แก้ไข หรือเปลี่ยนแปลงเพื่อให้มั่นใจว่าระบบสามารถประมวลผลได้ถูกต้องครบถ้วน และเป็นไปตามความต้องการของผู้ใช้งาน (System Acceptance Testing) พร้อมทั้งทบทวนผลกระทบตามแผนบริหารความต่อเนื่องทางธุรกิจ หรือ BCP (Business Continuity Plan) และปรับปรุงแผนดังกล่าวให้สอดคล้องกับการพัฒนา แก้ไข หรือเปลี่ยนแปลงระบบสารสนเทศดังกล่าว ทั้งนี้ผู้ทดสอบระบบจะใช้ข้อมูล (Data) สำหรับทดสอบ ซึ่งไม่มีผลกระทบใดๆ กับระบบสารสนเทศ (Dummy Data)

๒.๖ ควบคุมสภาพแวดล้อมของการพัฒนาระบบสารสนเทศ (Development Environment) ซึ่งประกอบด้วย บุคลากรผู้พัฒนาระบบ ขั้นตอนการพัฒนาระบบ และเทคโนโลยีสำหรับการพัฒนาระบบ ให้มีความมั่นคงปลอดภัย

๒.๗ พัฒนาระบบงานบนสภาพแวดล้อมที่แยกกันระว่าง Development, Testing และOperating Environment

๒.๘ การรักษาความลับของข้อมูลที่นำมาประมวลผล จัดเก็บ และส่งผ่านระบบสารสนเทศ ตลอดจนการควบคุมการนำข้อมูลเข้าและออกจากระบบที่อยู่ระหว่างการพัฒนา ตามสัญญารักษาความปลอดภัยของข้อมูลและสารสนเทศ (Non-disclosure Agreement)

๒.๙ ในการตรวจรับงาน กำหนดให้มีผู้ใช้งานหรือผู้ทดสอบอื่นที่เป็นอิสระจากผู้พัฒนาระบบสารสนเทศ ดำเนินการทดสอบระบบสารสนเทศที่ได้รับการพัฒนา แก้ไข หรือเปลี่ยนแปลง เพื่อให้มั่นใจว่าระบบสารสนเทศดังกล่าวสามารถทำงานได้อย่างถูกต้องตรงความต้องการของผู้ใช้งานและเป็นไปตามนโยบายด้านความมั่นคงปลอดภัย

๒.๑๐ หลีกเลี่ยงการดัดแปลงหรือปรับแต่งระบบสารสนเทศที่ผ่านการตรวจรับและใช้งานจริงเพื่อลดความเสี่ยงและผลกระทบต่อระบบสารสนเทศ แต่หากจำเป็นต้องดัดแปลงหรือปรับแต่ง ต้องพิจารณาถึงความเสี่ยงและผลกระทบ ตลอดจนกำหนดมาตรการรองรับความเสี่ยงหรือผลกระทบนั้น ตามระเบียบปฏิบัติ เรื่อง การควบคุมการเปลี่ยนแปลง (QP-DC-05) โดยต้องได้รับการอนุมัติจากผู้แทนฝ่ายบริหาร (ISMR) ก่อน

ISO/IEC 27001:2013 (Annex A): A.14.2.1-9

ตัวชี้วัดผลลัพธ์

๑. ระบุข้อกำหนดด้านความมั่นคงปลอดภัยของสารสนเทศใน TOR ที่เกี่ยวข้องกับด้านดิจิทัล โดยกำหนดเป็นลายลักษณ์อักษร

๒. โครงการด้านการพัฒนาระบบงานดิจิทัล ต้องมีการแยกสภาพแวดล้อมอย่างชัดเจน ได้แก่ Development, Testing และ Operating Environment

ส่วนที่ ๘
การบริหารจัดการเหตุการณ์ผิดปกติและปัญหาด้านเทคโนโลยีสารสนเทศ
(IT Incident and Problem Management)

วัตถุประสงค์

๑. เพื่อให้ กนอ. มีแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศสำหรับการบริหารจัดการเหตุการณ์ผิดปกติและปัญหาด้านเทคโนโลยีสารสนเทศ (IT Incident and Problem Management) ของ กนอ.

๒. เพื่อให้ผู้รับผิดชอบและผู้มีส่วนเกี่ยวข้อง ได้แก่ ผู้บริหารระดับสูง ผู้บริหาร ผู้ดูแลระบบ เจ้าหน้าที่หน่วยงานเจ้าของสารสนเทศ บุคคลภายนอกที่ปฏิบัติงานให้กับ กนอ. และบุคคลภายนอกที่ได้รับอนุญาตให้เข้าถึงและใช้งานสารสนเทศของ กนอ. รับทราบและทำความเข้าใจ รวมทั้งปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างเคร่งครัด

ขอบเขต

บังคับใช้กับทุกหน่วยงานใน กนอ.

อ้างอิงมาตรฐาน

๑. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศตามวิธีแบบปลอดภัย พ.ศ. ๒๕๕๕

๒. พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๓. มาตรฐาน ISO/IEC 27001:2013 (Annex A)

แนวทางปฏิบัติ

๑. การบริหารจัดการเหตุการณ์ผิดปกติและปัญหาด้านเทคโนโลยีสารสนเทศ

๑.๑ ให้มีการบันทึกจัดเก็บข้อมูลและรายงานอุบัติการณ์เกี่ยวกับเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ ผ่านช่องทางบริหารจัดการที่กำหนดไว้อย่างเหมาะสมและรวดเร็วทันการณ์

๑.๒ ให้ต้องบันทึกและรายงานช่องโหว่หรือจุดอ่อนใดๆ ด้านเทคโนโลยีสารสนเทศ ที่อาจสังเกตพบระหว่างการใช้งานระบบสารสนเทศ ผ่านช่องทางบริหารจัดการที่กำหนดไว้อย่างเหมาะสม

๑.๓ กำหนดขอบเขตความรับผิดชอบของผู้มีส่วนเกี่ยวข้อง และขั้นตอนการปฏิบัติงาน เพื่อตอบสนองต่อสถานการณ์ด้านเทคโนโลยีสารสนเทศที่ไม่พึงประสงค์ หรือไม่อาจคาดคิด อย่างรวดเร็ว มีระเบียบและมีประสิทธิผล

๑.๔ ผู้ดูแลระบบ และผู้ให้บริการภายนอก ที่ทำหน้าที่แก้ไขอุบัติการณ์ด้านเทคโนโลยีสารสนเทศ ต้องดำเนินการรวบรวม จัดเก็บ และนำเสนอหลักฐาน ให้สอดคล้องกับหลักเกณฑ์ของกฎหมายที่ใช้บังคับ หากมีขั้นตอนการติดตามผลกับบุคคลหรือหน่วยงานภายหลังจากเกิดสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดคิด ซึ่งเกี่ยวข้องกับการดำเนินการทางกฎหมาย (ไม่ว่าทางแพ่งหรือทางอาญา)
ISO/IEC 27001:2013 (Annex A): A.16.1.1-7

๒. การรับมือเหตุการณ์ผิดปกติทางไซเบอร์

๒.๑ มาตรการในการเตรียมความพร้อมสำหรับเหตุการณ์ด้านความปลอดภัยไซเบอร์ (Preparing for a Cyber security Incident)

๒.๒ มาตรการในการตอบสนองต่อเหตุการณ์ด้านความปลอดภัยทางไซเบอร์ (responding to cyber security incident)

๒.๓ ติดตามสถานการณ์ด้านความปลอดภัยทางไซเบอร์ (Following up the cyber security incident) ดำเนินการตามระเบียบปฏิบัติเรื่อง การรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยของสารสนเทศ (Reporting Information Security Incident) QP-DC-09

ISO/IEC 27001:2013 (Annex A): A.16.1.1-7

ตัวชี้วัดผลลัพธ์

๑. มีระบบการเฝ้าระวังความผิดปกติในเครือข่ายและระบบคอมพิวเตอร์ตลอดเวลา

๒. การตอบสนองกรณีเกิดเหตุผิดปกติในเครือข่ายโดยศูนย์เฝ้าระวังความปลอดภัยทางไซเบอร์ (SOC) มีการกำหนด SLA เป็นลายลักษณ์อักษร

ส่วนที่ ๙
การจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ
(IT Contingency Plan)

วัตถุประสงค์

๑. เพื่อให้ กนอ. มีแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศสำหรับการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan) ของ กนอ.

๒. เพื่อให้ผู้รับผิดชอบและผู้มีส่วนเกี่ยวข้อง ได้แก่ ผู้บริหารระดับสูง ผู้บริหาร ผู้ดูแลระบบ เจ้าหน้าที่หน่วยงานเจ้าของสารสนเทศ บุคคลภายนอกที่ปฏิบัติงานให้กับ กนอ. และบุคคลภายนอกที่ได้รับอนุญาตให้เข้าถึงและใช้งานสารสนเทศของ กนอ. รับทราบและทำความเข้าใจ รวมทั้งปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างเคร่งครัด

ขอบเขต

บังคับใช้กับทุกหน่วยงานใน กนอ.

อ้างอิงมาตรฐาน

๑. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศตามวิธีแบบปลอดภัย พ.ศ. ๒๕๕๕

๒. พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๓. มาตรฐาน ISO/IEC 27001:2013 (Annex A)

แนวทางปฏิบัติ

๑. การพิจารณาระบบเทคโนโลยีสารสนเทศที่สำคัญ

๑.๑ จัดทำบัญชีระบบเทคโนโลยีสารสนเทศและกำหนดลำดับความสำคัญ

๑.๒ กำหนดวิธีการและความถี่ของการสำรองข้อมูลที่เหมาะสมให้อยู่ในสภาพพร้อมใช้ตามที่ กนอ. กำหนด

๒. การจัดทำแผนความต่อเนื่องทางธุรกิจ (BCP)

เพื่อเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์และปรับปรุงให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับภารกิจของ กนอ. ตามแนวทางต่อไปนี้

๒.๑ ประเมินความเสี่ยงสำหรับระบบเทคโนโลยีสารสนเทศที่มีความสำคัญและกำหนดมาตรการเพื่อลดความเสี่ยง ได้แก่ ไฟดับเป็นระยะเวลานาน ไฟไหม้ น้ำท่วม แผ่นดินไหว การชุมนุมประท้วง การปิดล้อมพื้นที่จนทำให้ไม่สามารถเข้าใช้ระบบเทคโนโลยีสารสนเทศได้

๒.๒ กำหนดขั้นตอนปฏิบัติในการสำรองข้อมูล การกู้คืนระบบ และการทดสอบการกู้คืนระบบเทคโนโลยีสารสนเทศ

๒.๓ กำหนดช่องทางการติดต่อกับผู้ให้บริการภายนอก ได้แก่ ผู้ให้บริการระบบสำรองข้อมูล ผู้ให้บริการเครือข่าย หรือ ผู้ให้บริการคลาวด์

๓. การกำหนดหน้าที่และความรับผิดชอบ

๓.๑ ผู้ที่เกี่ยวข้องในการจัดทำและการทบทวนแผนความต่อเนื่องทางธุรกิจ (BCP-IT)

๓.๒ ผู้ดูแลระบบเทคโนโลยีสารสนเทศ ระบบเครือข่าย และระบบสำรองข้อมูล

๓.๓ ผู้ที่เกี่ยวข้องทั้งหมดตามแผนผังสายการบังคับบัญชา (Lines of authority) เมื่อเกิดสถานการณ์ฉุกเฉิน (ภาคผนวก)

๔. การฝึกซ้อม

ดำเนินการฝึกซ้อมตามแผนความต่อเนื่องทางธุรกิจ (BCP-IT) เพื่อทดสอบสภาพความพร้อมใช้งานของระบบเทคโนโลยีสารสนเทศและระบบสำรอง อย่างน้อยปีละ ๑ ครั้ง

๕. การทบทวน

๕.๑ ทบทวนและปรับปรุงแผนความต่อเนื่องทางธุรกิจ (BCP-IT) ให้เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้และสามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับภารกิจของ กนอ. อย่างน้อยปีละ ๑ ครั้ง (ภาคผนวก)

๕.๒ ให้ความรู้และสร้างความตระหนักแก่เจ้าหน้าที่หรือผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติหรือสิ่งที่ต้องทำเมื่อเกิดเหตุฉุกเฉิน

๕.๓ ควบคุมให้มีการประเมินความต้องการด้านการรักษาสภาพพร้อมใช้งาน (Availability) ของระบบที่มีความสำคัญสูง และกำกับให้มีการติดตั้งอุปกรณ์หรือระบบเพื่อรักษาความต่อเนื่องในการดำเนินงาน (Redundancy) ที่เหมาะสม

ISO/IEC 27001:2013 (Annex A): A.17.1.1-3, A.17.2

ตัวชี้วัดผลลัพธ์

๑. มีแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษร

๒. มีการทบทวนแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง

๓. มีการฝึกซ้อมแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง

ส่วนที่ ๑๐
การบริหารจัดการผู้ให้บริการภายนอก
(Third Party Management)

วัตถุประสงค์

๑. เพื่อให้ กนอ. มีแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศสำหรับการรักษาความมั่นคงปลอดภัย (Third Party Management) ของ กนอ.

๒. เพื่อให้ผู้รับผิดชอบและผู้มีส่วนเกี่ยวข้อง ได้แก่ ผู้ให้บริการภายนอก บุคคลภายนอกที่ปฏิบัติงานให้กับ กนอ. และบุคคลภายนอกที่ได้รับอนุญาตให้เข้าถึงและใช้งานสารสนเทศของ กนอ. รับทราบและทำความเข้าใจ รวมทั้งปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างเคร่งครัด

ขอบเขต

๑. ผู้ให้บริการภายนอก

๒. บุคคลภายนอกที่ปฏิบัติงานให้กับ กนอ.

๓. บุคคลภายนอกที่ได้รับอนุญาตให้เข้าถึงและใช้งานสารสนเทศของ กนอ.

อ้างอิงมาตรฐาน

๑. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศตามวิธีแบบปลอดภัย พ.ศ. ๒๕๕๕

๒. มาตรฐาน ISO/IEC 27001:2013 (Annex A)

แนวทางปฏิบัติ

๑. การบริหารจัดการข้อตกลงการให้บริการ (Service Level Agreement: SLA) และข้อตกลงด้านการรักษาความลับของข้อมูล (Non-Disclosure Agreement: NDA)

๑.๑ การจัดจ้างผู้ให้บริการภายนอกเพื่อเข้ามาดำเนินงานที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ ฝ่ายดิจิทัลต้องมีการกำหนดข้อตกลงการให้บริการ (SLA) และข้อตกลงด้านการรักษาความลับของข้อมูล (NDA) ไว้ในเอกสารจัดจ้างหรือสัญญา

๑.๒ กำหนดให้มีการติดตาม ทบทวน และตรวจประเมินการให้บริการของผู้ให้บริการภายนอกให้สอดคล้องกับข้อกำหนดการจ้างและระยะเวลาในการจ้างผู้ให้บริการภายนอกรายนั้นๆ ซึ่งการติดตามและทบทวนการให้บริการของผู้ให้บริการภายนอกเพื่อทำให้มั่นใจว่าผู้ให้บริการภายนอกยังคงปฏิบัติตามข้อตกลงการให้บริการ ข้อตกลงด้านการรักษาความลับของข้อมูล และเงื่อนไขที่ได้ระบุไว้ในข้อสัญญา

๒. การรักษาความมั่นคงปลอดภัยของสารสนเทศสำหรับผู้ให้บริการจากภายนอก (Information Security in Supplier Relationships)

เพื่อลดความเสี่ยงจากการเข้าถึงทรัพย์สินสารสนเทศของ กนอ. โดยผู้ให้บริการจากภายนอก ซึ่งจำเป็นต้องเข้าถึงทรัพย์สินสารสนเทศในระดับชั้นความลับ Confidential ขึ้นไป ของ กนอ. ให้หน่วยงานที่เป็นผู้ดูแลผู้ให้บริการจากภายนอกนั้น ดำเนินการดังต่อไปนี้

๒.๑ ระบุการคุ้มครองข้อมูลสารสนเทศในสัญญาหรือจัดทำข้อตกลงเกี่ยวกับการรักษาความมั่นคงปลอดภัยของสารสนเทศอย่างเป็นลายลักษณ์อักษร ตามขั้นตอนการปฏิบัติงาน การทำสัญญารักษาความปลอดภัยของข้อมูลและสารสนเทศ (Non-disclosure Agreement) พร้อมทั้งมีการลงนามร่วมกันระหว่าง กนอ. กับผู้ให้บริการจากภายนอก

๒.๒ กำหนดให้ผู้ให้บริการจากภายนอกระบุชื่อและช่องทางสำหรับติดต่อบุคคลหรือหน่วยงานอื่นที่เกี่ยวข้องโดยเฉพาะอย่างยิ่งบุคคลหรือหน่วยงานที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของสารสนเทศอย่างเป็นลายลักษณ์อักษร

๒.๓ กรณีการเคลื่อนย้ายหรือโอนข้อมูลและมีความจำเป็นต้องส่งข้อมูลดังกล่าวให้กับผู้ให้บริการจากภายนอก เจ้าหน้าที่ผู้เกี่ยวข้องพิจารณาระดับชั้นความลับของข้อมูลและปฏิบัติตามระเบียบปฏิบัติ เรื่อง การชี้บ่งและจัดการสารสนเทศ QP-DC-04

๒.๔ การควบคุมการส่งมอบงานของผู้ให้บริการจากภายนอก (Supplier Service Delivery Management) หน่วยงานผู้ดูแลผู้ให้บริการจากภายนอกดำเนินการติดตาม ทบทวน และตรวจสอบการปฏิบัติงาน ตลอดจนการส่งมอบงานของผู้ให้บริการจากภายนอก ตามข้อตกลงระหว่างหน่วยงานกับผู้ให้บริการ

๒.๕ ในกรณีที่ผู้ให้บริการจากภายนอกมีการเปลี่ยนแปลงกระบวนการ ขั้นตอน วิธีการปฏิบัติงานหรือนโยบายด้านความมั่นคงปลอดภัยของสารสนเทศ รวมถึง การที่ กนอ. เปลี่ยนแปลงผู้ให้บริการจากภายนอก ISMR มีการทบทวนความเสี่ยงจากการเปลี่ยนแปลงดังกล่าว และกำหนดกระบวนการบริหารจัดการความเสี่ยงนั้นอย่างเหมาะสม

ISO/IEC 27001:2013 (Annex A): A.15.1.1-3

ตัวชี้วัดผลลัพธ์

๑. มีข้อกำหนดด้านความมั่นคงปลอดภัยของสารสนเทศที่เกี่ยวข้องกับผู้ให้บริการภายนอกชัดเจนเป็นลายลักษณ์อักษร

๒. มีการกำกับดูแลด้านความมั่นคงปลอดภัยของสารสนเทศ โดยระบุเป็นสัญญาหรือข้อกำหนดและขอบเขตของงาน (TOR) ครบถ้วนทุกโครงการ

ส่วนที่ ๑๑
การใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ
(IT Outsourcing Policy)

วัตถุประสงค์

๑. เพื่อให้ กนอ. มีแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศสำหรับการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ (IT Outsourceing Policy) ของ กนอ.

๒. เพื่อให้ผู้รับผิดชอบและผู้มีส่วนเกี่ยวข้อง ได้แก่ ผู้ให้บริการภายนอก บุคคลภายนอกที่ปฏิบัติงานให้กับ กนอ. และบุคคลภายนอกที่ได้รับอนุญาตให้เข้าถึงและใช้งานสารสนเทศของ กนอ. รับทราบและทำความเข้าใจ รวมทั้งปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างเคร่งครัด

ขอบเขต

๑. ผู้ให้บริการภายนอก

๒. บุคคลภายนอกที่ปฏิบัติงานให้กับ กนอ.

๓. บุคคลภายนอกที่ได้รับอนุญาตให้เข้าถึงและใช้งานสารสนเทศของ กนอ.

อ้างอิงมาตรฐาน

๑. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศตามวิธีแบบปลอดภัย พ.ศ. ๒๕๕๕

๒. มาตรฐาน ISO/IEC 27001:2013 (Annex A)

แนวทางปฏิบัติ

๑. การจัดจ้างผู้ให้บริการภายนอกเพื่อเข้ามาดำเนินงานที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ ฝ่ายดิจิทัลต้องมีการกำหนดและตกลงเกี่ยวกับความต้องการด้านความมั่นคงปลอดภัยสารสนเทศกับผู้ให้บริการภายนอกไว้ในเอกสารจัดจ้างหรือสัญญา เพื่อลดความเสี่ยงที่เกี่ยวข้องกับการเข้าถึงทรัพย์สินของ กนอ. โดยผู้ให้บริการภายนอก

๒. มีการระบุความเสี่ยงอันเกิดจากการจ้างช่วงและการสื่อสารโดยผู้ให้บริการภายนอก เช่น การจ้างช่วงต้องมีการแจ้งให้ กนอ. ได้รับทราบ หากผู้รับจ้างมีการดำเนินการในลักษณะดังกล่าวอย่างเป็นลายลักษณ์อักษรและระบุในสัญญาเกี่ยวกับความรับผิดชอบต่อความเสี่ยงที่เกิดขึ้นจากการจ้างช่วง

๓. กำหนดให้มีการติดตาม ทบทวน และตรวจประเมินการให้บริการของผู้ให้บริการภายนอกให้สอดคล้องกับระยะเวลาในการจ้างผู้ให้บริการภายนอกรายนั้นๆ ซึ่งการติดตามและทบทวนการให้บริการ

ของผู้ให้บริการภายนอกเพื่อทำให้มั่นใจว่าผู้ให้บริการภายนอกยังคงปฏิบัติตามข้อตกลงด้านความมั่นคงปลอดภัยสารสนเทศและเงื่อนไขที่ได้ระบุไว้ในสัญญาจ้าง

๔. การเปลี่ยนแปลงที่เกี่ยวข้องกับบริการที่ได้รับจากผู้ให้บริการภายนอกทั้งในส่วนที่ร้องขอการเปลี่ยนแปลงโดย กนอ. เองและส่วนที่ร้องขอการเปลี่ยนแปลงโดยผู้ให้บริการภายนอกโดยมีการรายงานในการตรวจรับงานตามสัญญา

ISO/IEC 27001:2013 (Annex A): A.15.2.1-2

ตัวชี้วัดผลลัพธ์

๑. การจัดทำสัญญาจ้างโครงการด้านดิจิทัล มีการระบุข้อกำหนดด้านความมั่นคงปลอดภัยของสารสนเทศทุกโครงการ

๒. มีการกำกับดูแลด้านความมั่นคงปลอดภัยของสารสนเทศ โดยระบุเป็นสัญญาหรือข้อกำหนดและขอบเขตของงาน (TOR) ครบถ้วนทุกโครงการ

ส่วนที่ ๑๒
การบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ
(Information Security Risk Management)

วัตถุประสงค์

๑. เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศของ กนอ.

๒. เพื่อเป็นการป้องกันและลดระดับความเสี่ยงที่อาจจะเกิดขึ้นกับสารสนเทศของ กนอ.

ขอบเขต

บังคับใช้กับทุกหน่วยงานใน กนอ.

อ้างอิงมาตรฐาน

๑. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศตามวิธีแบบปลอดภัย พ.ศ. ๒๕๕๕

๒. มาตรฐาน ISO/IEC 27001:2013 (Annex A)

๓. คู่มือการบริหารความเสี่ยงและควบคุมภายใน การนิคมอุตสาหกรรมแห่งประเทศไทย ปีงบประมาณ ๒๕๖๕

แนวทางปฏิบัติ

๑. การประเมินความเสี่ยง (Risk Assessment)

๑.๑ ให้มีการระบุความเสี่ยง (risk identification) เพื่อระบุความเสี่ยงที่อาจส่งผลกระทบต่อองค์กร

๑.๒ ให้มีการวิเคราะห์ความเสี่ยง (risk analysis) เพื่อวิเคราะห์ผลกระทบ (Impact) และโอกาสเกิด (Likelihood) ของเหตุการณ์ความเสี่ยงที่เกิดขึ้นต่อองค์กร

๑.๓ ให้มีการประเมินค่าความเสี่ยง (risk evaluation) หลังจากพิจารณาโอกาสเกิดเหตุการณ์ (Likelihood) และผลกระทบ (Impact) ของแต่ละปัจจัยเสี่ยงแล้ว โดยนำผลที่ได้มาพิจารณาความสัมพันธ์ระหว่างโอกาสที่จะเกิดความเสี่ยง และผลกระทบของความเสี่ยง ว่าก่อให้เกิดระดับของความเสี่ยงในระดับใด

๑.๔ ให้มีการจัดลำดับความรุนแรงของความเสี่ยงที่มีผลต่อองค์กร เพื่อพิจารณากำหนดกิจกรรมการควบคุมในแต่ละสาเหตุของความเสี่ยงที่สำคัญให้เหมาะสม

๑.๕ ให้มีการติดตามและทบทวนความเสี่ยง (risk monitoring and review) โดยการกำหนดผู้รับผิดชอบและจัดให้มีกระบวนการในการติดตามตัวชี้วัดความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศตามที่กำหนดและทบทวนการประเมินความเสี่ยงด้านสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง

๑.๖ ให้มีการรายงานความเสี่ยง (Risk reporting) โดยการนำเสนอผลการบริหารแผนความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศพร้อมกับการรายงานผลการประเมินและการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ โดยเชื่อมโยงกับความเสี่ยงในระดับองค์กร

ปฏิบัติตามระเบียบปฏิบัติ เรื่องการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยของสารสนเทศ QP-DC-10

๒. การจัดการความเสี่ยง (Risk Treatment)

๒.๑ ให้มีการกำหนดมาตรการ หรือแผนงาน เพื่อลดโอกาสที่จะเกิดความเสี่ยง หรือลดความเสียหายของผลกระทบที่อาจเกิดขึ้นจากความเสี่ยง

๒.๒ ให้มีการกำหนดแนวทางการจัดการความเสี่ยง โดยสามารถปรับเปลี่ยนให้เหมาะสมกับสถานการณ์ เช่น การยอมรับความเสี่ยง (Take), การควบคุมความเสี่ยง (Treat), การถ่ายโอนความเสี่ยง (Transfer), การหลีกเลี่ยงความเสี่ยง (Terminate) เป็นต้น

ปฏิบัติตามระเบียบปฏิบัติ เรื่องการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยของสารสนเทศ QP-DC-10
ISO/IEC 27001:2013 6.1

ตัวชี้วัดผลลัพธ์

๑. มีขั้นตอนการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยของสารสนเทศเป็นลายลักษณ์อักษร
๒. ทบทวนผลการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยของสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง

ส่วนที่ ๑๓
การกำหนดหน้าที่ความรับผิดชอบของผู้ปฏิบัติงาน
(Role and responsibility)

วัตถุประสงค์

เพื่อให้ กนอ. มีแนวปฏิบัติในการกำหนดหน้าที่ความรับผิดชอบของผู้ปฏิบัติงานในการบริหารจัดการ การพัฒนา ปรับปรุง บำรุงรักษา ตรวจสอบและติดตามระบบเทคโนโลยีสารสนเทศของ กนอ. เพื่อให้สามารถให้บริการได้อย่างต่อเนื่องและมีประสิทธิภาพ รวมทั้งกำกับผู้ใช้งานให้ปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ขอบเขต

บังคับใช้กับทุกหน่วยงานใน กนอ.

อ้างอิงมาตรฐาน

๑. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศตามวิธีแบบปลอดภัย พ.ศ. ๒๕๕๕

๒. มาตรฐาน ISO/IEC 27001:2013 (Annex A)

แนวทางปฏิบัติ

๑. การกำหนดหน้าที่ความรับผิดชอบของผู้ปฏิบัติงาน

๑.๑ ผู้ปฏิบัติงานระดับนโยบาย

<u>ผู้รับผิดชอบ</u>

๑.๑.๑ ผู้บริหารระดับสูงสุด (ผู้ว่าการ)

๑.๑.๒ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO)

<u>หน้าที่/ความรับผิดชอบ</u>

๑.๑.๓ กำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา บริหารจัดการด้านเทคโนโลยีสารสนเทศ

๑.๑.๔ กำกับดูแลการปฏิบัติงานของผู้ปฏิบัติงานในระดับบริหาร

๑.๑.๕ รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายใดๆ ที่เกิดจากระบบเทคโนโลยีสารสนเทศ ซึ่งเกิดขึ้นกับองค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากละเลย การละเมิดหรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๑.๒ ระดับบริหาร

ผู้รับผิดชอบ

๑.๒.๑ ผู้อำนวยการฝ่ายดิจิทัล (ผอ.ฝดจ.)

๑.๒.๒ ผู้อำนวยการกองปฏิบัติการเทคโนโลยีสารสนเทศ (ผอ.ฝกจ.)

๑.๒.๓ ผู้อำนวยการกองพัฒนาระบบงานสารสนเทศ (ผอ.กพส.)

หน้าที่/ความรับผิดชอบ

๑.๒.๔ กำกับดูแลการปฏิบัติงานของผู้ปฏิบัติงานในระดับปฏิบัติ

๑.๒.๕ กำกับดูแลการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ

๑.๒.๖ จัดทำและทบทวนแผนความต่อเนื่องทางธุรกิจด้านเทคโนโลยีสารสนเทศ (BCP-IT)

๑.๒.๗ บริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

๑.๒.๘ รายงานการละเมิดหรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๑.๓ ระดับปฏิบัติ

ผู้รับผิดชอบ

ผู้ดูแลระบบที่ได้รับมอบหมายให้ปฏิบัติหน้าที่เกี่ยวกับระบบเทคโนโลยีสารสนเทศ

หน้าที่/ความรับผิดชอบ

๑.๓.๑ กำหนดบัญชีรายชื่อ (User account) และรหัสผ่าน (Password) สำหรับผู้ดูแลระบบและผู้ใช้งาน

๑.๓.๒ ดูแลรักษาระบบเทคโนโลยีสารสนเทศ

๑.๓.๓ ติดตั้งเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบการเข้ารหัสสารสนเทศ ระบบป้องกันและตรวจจับการบุกรุก ระบบป้องกันและกำจัดซอฟต์แวร์ประสงค์ร้าย รวมทั้งอุปกรณ์และระบบอื่นใดที่จำเป็นเพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถใช้งานได้อย่างมั่นคง

๑.๓.๔ ตรวจสอบและติดตามการใช้งานระบบเทคโนโลยีสารสนเทศให้เป็นไปด้วยความเรียบร้อยและมีประสิทธิภาพ หากตรวจพบสิ่งผิดปกติให้รีบดำเนินการแก้ไขในทันทีเพื่อป้องกันและบรรเทาความเสียหายที่อาจเกิดขึ้น ในกรณีที่สิ่งผิดปกติดังกล่าวเกิดขึ้นจากการละเมิดหรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้รีบแจ้งผู้ใช้งานผู้นั้นให้ยุติการกระทำดังกล่าวในทันที และพิจารณาระงับการเข้าถึงและการใช้งานระบบเทคโนโลยีสารสนเทศในทันที

๑.๓.๕ ติดตั้งและปรับปรุงการแก้ไขข้อบกพร่อง (Patch) ของระบบเทคโนโลยีสารสนเทศให้มีความมั่นคงและทันสมัยอยู่เสมอ

๑.๓.๖ ตรวจสอบความมั่นคงของระบบเทคโนโลยีสารสนเทศทุก ๖ เดือน

๑.๓.๗ เปลี่ยนรหัสผ่านสำหรับการเข้าถึงและการใช้งานระบบเทคโนโลยีสารสนเทศทุก ๓ เดือน หรือเมื่อมีความจำเป็น

๑.๓.๘ สำรองข้อมูลตามแผนการสำรองข้อมูล FM-DC-17

๑.๓.๙ ลบหรือทำลายสารสนเทศหรือซอฟต์แวร์คอมพิวเตอร์ที่เกี่ยวข้องกับการปฏิบัติงานอย่างถาวร เมื่อไม่มีความจำเป็นหรือเมื่อหมดสัญญาเช่า

๑.๓.๑๐ บันทึกการเข้าถึงและการใช้งานระบบเทคโนโลยีสารสนเทศ (Log File) ย้อนหลังอย่างน้อย ๙๐ วัน

๑.๓.๑๑ ดูแลรักษาและตรวจสอบช่องทางการสื่อสาร (Communication port) ของระบบเทคโนโลยีสารสนเทศทุก ๖ เดือน และปิดช่องทางการสื่อสาร (Communication port) ที่ไม่มีความจำเป็นต้องใช้งานในทันที

๑.๓.๑๒ ดูแลรักษาและปรับปรุงบัญชีรายชื่อผู้ใช้งานให้ถูกต้องและเป็นปัจจุบันอยู่เสมอ โดยให้ยกเลิกสิทธิ์ของผู้ใช้งานทันทีที่พ้นสภาพจากการเป็นผู้ใช้งาน

๑.๓.๑๓ กำหนดหลักสูตรและจัดฝึกอบรมเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง

๑.๓.๑๔ จัดทำรายงานการเข้าถึงและการใช้งานระบบเทคโนโลยีสารสนเทศ และนำเสนอต่อ ผอ.ฝดจ. ผอ.กปจ. หรือ ผอ.กพจ. เพื่อทราบหรือเพื่อพิจารณาสั่งการเกี่ยวกับการแก้ไข การปรับปรุงประสิทธิภาพและการให้บริการต่อไป

๑.๓.๑๕ ตั้งสัญญาณนาฬิกาของเครื่องคอมพิวเตอร์ ระบบเทคโนโลยีสารสนเทศให้ตรงกับเวลามาตรฐานสากลจากเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการเทียบเวลา (A.12.4.4)

๑.๓.๑๖ ซักซ้อมแผนสร้างความต่อเนื่องทางธุรกิจ (BCP-IT) อย่างน้อยปีละ ๑ ครั้ง เพื่อเตรียมพร้อมในกรณีเกิดเหตุฉุกเฉิน

๑.๓.๑๗ การดำเนินการสำหรับระบบเครือข่ายแบบไร้สาย (wireless LAN)

๑.๓.๑๗.๑ กำหนดให้มีการเข้ารหัสสารสนเทศระหว่างเครื่องคอมพิวเตอร์และอุปกรณ์ที่ใช้ในการรับและส่งสัญญาณ ตามมาตรฐานของเทคโนโลยีไม่ต่ำกว่า WPA (Wi-Fi Protected Access)

๑.๓.๑๗.๒ กำหนดให้มีกลไกการตรวจสอบพิสูจน์ตัวตนของผู้ใช้งาน (User Authentication) ที่มีความมั่นคง เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้าถึงและเข้าใช้งานได้ด้วย Active Directory ที่ติดตั้งไว้เพื่อทำหน้าที่ตรวจสอบพิสูจน์ตัวตนของผู้ใช้งานจากฐานข้อมูลผู้ใช้งานที่ได้รับอนุญาตเท่านั้น

๑.๓.๑๗.๓ ติดตั้งระบบจัดเก็บบันทึกการเข้าถึงและการใช้งานระบบเครือข่ายแบบไร้สายและตรวจสอบและรายงานผลอย่างน้อยเดือยละ ๑ ครั้ง เพื่อให้ ผอ.กปจ. รับทราบ ในกรณีที่ตรวจสอบพบการใช้ที่ผิดปกติให้ ผอ.กปจ. รายงานต่อ ผอ.ฝดจ. ทราบในทันที

๑.๓.๑๗.๔ กำหนดให้ผู้ใช้งานต้องไม่ใช้งานช่องรับและส่งสัญญาณทางอินฟราเรดหรือ Bluetooth ในขณะที่กำลังใช้งานระบบเครือข่ายแบบไร้สายเพื่อป้องกันการรั่วไหลของสารสนเทศ

๑.๓.๑๗.๕ ติดตั้งระบบตรวจจับผู้บุกรุกหรือไฟร์วอลล์ (Firewall)

๑.๓.๑๗.๖ ติดตั้งและใช้งานซอฟต์แวร์คอมพิวเตอร์สำหรับป้องกันและกำจัดซอฟต์แวร์ประสงค์ร้าย รวมทั้งทำการปรับปรุงให้ทันสมัยอยู่เสมอ

๑.๓.๑๗.๗ กำกับดูแลไม่ให้ผู้ใช้งานใช้งานระบบเทคโนโลยีสารสนเทศ ได้แก่ ระบบเทคโนโลยีสารสนเทศด้านบัญชี การเงิน งบประมาณ การบริหารงานพัสดุ การบริหารงานบุคคล (ระบบ ERP) ระบบอินทราเน็ต (Intranet) ระบบสารบรรณอิเล็กทรอนิกส์ และฐานข้อมูลต่างๆ ผ่านระบบเครือข่ายแบบไร้สาย

๑.๓.๑๗.๘ ปฏิบัติหน้าที่อื่นใดที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ ผอ.ฝดจ. ผอ.กปจ. และ ผอ.กพจ. มอบหมาย

๑.๔ ควบคุมให้มีการกำหนดเนื้องานหรือหน้าที่ความรับผิดชอบต่างๆ เกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศไว้อย่างชัดเจน และแบ่งแยกหน้าที่ความรับผิดชอบเพื่อป้องกันความเสี่ยงในการกระทำความผิด (Segegration of Duties) (A.6.1.2)

๑.๕ ควบคุมให้มีการกำหนดขั้นตอนและช่องทางในการติดต่อกับหน่วยงานภายนอกที่มีหน้าที่ในการกำกับดูแล หรือหน่วยงานที่เกี่ยวข้องกับการบังคับใช้กฎหมาย รวมทั้งหน่วยงานที่ควบคุมดูแลสถานการณ์ฉุกเฉินภายใต้สถานการณ์ต่างๆ ไว้อย่างชัดเจน (A.6.1.3) ตามแบบฟอร์มบัญชีรายชื่อหน่วยงานภาครัฐที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ FM-DC-32

๑.๖ ควบคุมให้มีการกำหนดขั้นตอนและช่องทางในการติดต่อกับหน่วยงานภายนอกที่มีความเชี่ยวชาญเฉพาะด้านหรือหน่วยงานที่มีความเชี่ยวชาญด้านความมั่นคงปลอดภัยด้านสารสนเทศภายใต้สถานการณ์ต่างๆ ไว้อย่างชัดเจน (A.6.1.4) ตามแบบฟอร์มบัญชีรายชื่อกลุ่ม สมาคม หรือชมรมที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยของสารสนเทศ FM-DC-33

๑.๗ กำหนดให้มีการควบคุมความมั่นคงปลอดภัยด้านสารสนเทศในการบริหารจัดการโครงการทั้งแผนงานของ กนอ. และโครงการที่จัดซื้อจัดจ้างโดยผู้ให้บริการภายนอกเป็นผู้ดำเนินการ โดยพิจารณาถึงความเสี่ยงด้านสารสนเทศ และกำหนดแนวทางจัดการความเสี่ยงในระหว่างการดำเนินโครงการ โดยพิจารณาความเสี่ยงในโครงการนั้น มาตรการรองรับที่มีอยู่เพียงพอหรือไม่ หากไม่เพียงพอให้ผู้รับผิดชอบกำหนดมาตรการที่เหมาะสมในการกำกับโครงการและเชื่อมโยงกับการตรวจรับงาน
ISO/IEC 27001:2013 (Annex A): A.6.1.1-5

๒. การกำหนดความปลอดภัยด้านทรัพยากรบุคคล

๒.๑ การระบุหน้าที่และความรับผิดชอบด้านความมั่นคงปลอดภัยของสารสนเทศ ดำเนินการผ่านนโยบายความมั่นคงปลอดภัยและการมอบหมายหน้าที่ความรับผิดชอบของแต่ละตำแหน่งงาน

๒.๒ มีกระบวนการคัดเลือกบุคลากรอย่างเหมาะสม การตรวจสอบภูมิหลังของผู้สมัครงานต้องมีการดำเนินการโดยมีความสอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับ และจริยธรรมที่เกี่ยวข้อง และต้องดำเนินการในระดับที่เหมาะสมกับตำแหน่งหน้าที่ (ต้นสังกัดทำเรื่องสรรหาบุคคลากรตามสายงานนำเสนอผู้ว่าการเพื่อพิจารณาอนุมัติดำเนินการ)

๒.๓ มีการทำข้อตกลงการปฏิบัติงานตามที่ กนอ. กำหนดไว้ตามสัญญาการจ้างงาน

๒.๔ มีการฝึกอบรม ให้ความรู้ และสร้างความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศ โดยฝ่ายดิจิทัล จัดให้มีการอบรมหลักสูตรด้านความมั่นคงปลอดภัยปีละครั้ง โดยมีการสำรวจความต้องการฝึกอบรมตามแบบฟอร์มFM-DC-34 ผ่านโครงการสารสนเทศของแต่ละปี จัดทำแผนการฝึกอบรมFM-DC-37 โดยมีบันทึกการฝึกอบรมตามแบบฟอร์มบันทึกอบรม FM-DC-31 และแบบฟอร์มประเมินผลการฝึกอบรม FM-DC-35

๒.๕ กรณีพบการกระทำความผิดด้านความมั่นคงปลอดภัยของสารสนเทศ คณะกรรมการสอบสวนของ กนอ.จะดำเนินการสอบสวน และรายงานผลต่ออนุกรรมการฯ เพื่อพิจารณา หากมีมติกล่าวโทษผู้กระทำความผิด จะส่งเรื่องตามขั้นตอนทางวินัยของ กนอ.

๒.๖ กรณีบุคลากรลาออก หรือเปลี่ยนแปลงหน้าที่งาน เมื่อได้รับเรื่องจากหน่วยงานที่เกี่ยวข้อง ฝ่ายดิจิทัลจะรับคืนทรัพย์สินสารสนเทศเพื่อดำเนินการตามขั้นตอนด้านความมั่นคงปลอดภัยที่เกี่ยวข้อง โดยการตรวจสอบทรัพย์สินสารสนเทศ การลบข้อมูล การทบทวนสิทธิ การถอดสิทธิการเข้าถึงเครือข่ายระบบงานต่างๆ หลังจากดำเนินการแล้วผู้รับผิดชอบจะทำบันทึกรายงานถึงผู้บังคับบัญชา

ISO/IEC 27001:2013 (Annex A): A.7.1, A.7.2, A.7.3

๓. การไม่ละเมิดทรัพย์สินทางปัญญาของผู้อื่น

๓.๑ ปฏิบัติตามเงื่อนไขการใช้งานที่กำหนดไว้ของซอฟต์แวร์หรือทรัพย์สินทางปัญญาอื่นๆ ที่ กนอ. หรือผู้ใช้งานมีใช้งานหรือครอบครอง

๓.๒ ห้ามทำซ้ำ เปลี่ยนแปลง หรือแก้ไขทรัพย์สินทางปัญญาไปสู่รูปแบบอื่นที่เป็นการละเมิดเงื่อนไขหรือข้อตกลงการใช้งาน

๓.๓ ห้ามสำเนาทั้งหมดหรือบางส่วนของหนังสือ บทความ รายงาน หรือเอกสารอื่นๆ ที่เป็นการละเมิดเงื่อนไขของเจ้าของทรัพย์สินทางปัญญา

๔. การประเมินผลการปฏิบัติตามนโยบาย หลักเกณฑ์ หรือกระบวนการใดๆ รวมทั้งข้อกำหนดด้านความมั่นคงปลอดภัยด้านสารสนเทศ

๔.๑ คณะทำงาน ต้องควบคุม กำกับ ติดตามให้มีการระบุไว้ให้ชัดเจนถึงแนวทางในการดำเนินงานของระบบสารสนเทศที่มีความสอดคล้องกฎหมาย พระราชบัญญัติ กฎระเบียบ ข้อบังคับที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศโดยต้องจัดทำเป็นเอกสาร และมีการปรับปรุงให้เป็นปัจจุบัน

๔.๒ ผู้ใช้งาน ต้องดำเนินงานด้วยความระมัดระวังและป้องกันมิให้ข้อมูลสารสนเทศที่สำคัญเกิดความเสียหาย สูญหายหรือถูกปลอมแปลง โดยให้สอดคล้องกับกฎหมาย พระราชบัญญัติ กฎระเบียบ ข้อบังคับที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศและข้อกำหนดการให้บริการ

๔.๓ คณะทำงาน ต้องควบคุมให้มีการคุ้มครองข้อมูลส่วนบุคคลโดยให้สอดคล้องกับกฎหมาย พระราชบัญญัติ กฎระเบียบ ข้อบังคับที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ

๔.๔ ผู้ดูแลระบบ ต้องใช้เทคนิคการเข้ารหัสลับ ที่สอดคล้องกับกฎหมาย พระราชบัญญัติ กฎระเบียบ ข้อบังคับที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ

๔.๕ บุคลากร ต้องดำเนินงานอยู่ในขอบเขตความรับผิดชอบตามนโยบายความมั่นคงปลอดภัยสารสนเทศขององค์กร รวมถึงปฏิบัติตามข้อกำหนดสัญญา กฎหมาย พระราชบัญญัติ กฎระเบียบ และข้อบังคับที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ

๔.๖ องค์กร ต้องจัดให้มีการทบทวนตรวจสอบระบบสารสนเทศในด้านเทคนิคอย่างสม่ำเสมอเพื่อให้สอดคล้องกับมาตรฐานการพัฒนางานด้านความมั่นคงปลอดภัยด้านสารสนเทศ

ISO/IEC 27001:2013 (Annex A): A.18.1.2

ตัวชี้วัดผลลัพธ์

๑. มีการกำหนดบทบาทหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยของสารสนเทศเป็นลายลักษณ์อักษร

๒. สื่อสารถ่ายทอดบทบาทหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยของสารสนเทศให้แก่บุคลากรของ กนอ. อย่างน้อยปีละ ๑ ครั้ง

๓. มีการจัดทำแผนการฝึกอบรมด้านความมั่นคงปลอดภัยของสารสนเทศเป็นลายลักษณ์อักษร ทุกปี

๔. จัดฝึกอบรมได้เป็นไปตามแผนงานครบถ้วน

ส่วนที่ ๑๔
การป้องกันโปรแกรมไม่ประสงค์ดี
(Malicious Software Prevention)

วัตถุประสงค์

เพื่อให้ระบบเทคโนโลยีสารสนเทศของ กนอ. สามารถให้บริการได้อย่างต่อเนื่องและมีประสิทธิภาพ รวมทั้งกำกับผู้ใช้งานให้ปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ขอบเขต

บังคับใช้กับทุกหน่วยงานใน กนอ.

อ้างอิงมาตรฐาน

๑. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศตามวิธีแบบปลอดภัย พ.ศ. ๒๕๕๕

๒. มาตรฐาน ISO/IEC 27001:2013 (Annex A)

แนวทางปฏิบัติ

๑. กนอ. ติดตั้งซอฟต์แวร์ป้องกันไวรัสให้แก่เครื่องคอมพิวเตอร์ทุกเครื่องทั้งเครื่องแม่ข่าย (Server) และเครื่องของผู้ใช้งาน (Client) เพื่อป้องกันซอฟต์แวร์ไม่ประสงค์ดี และตั้งค่าให้ Update Anti Virus แบบอัตโนมัติทุกเครื่องเพื่อให้การตรวจจับมีประสิทธิภาพ

๒. การตรวจสอบการ Update Anti Virus ทุก ๓ เดือน เพื่อให้มั่นใจว่าระบบตรวจจับไวรัสมีความทันสมัยกับภัยคุกคาม โดยบันทึกในแบบฟอร์มการตรวจสอบการ Update Anti Virus (FM-DC-10)

๓. กนอ. มีศูนย์เฝ้าระวังความปลอดภัยทางไซเบอร์ (SOC) ซึ่งเฝ้าระวังภัยคุกคามในระบบเครือข่ายตลอดเวลา ตรวจสอบความผิดปกติที่เกิดขึ้นพร้อมแจ้งมายังทีม IR Team ของกนอ. เพื่อดำเนินการแก้ไขป้องกันอย่างมีประสิทธิภาพ

๔. หากตรวจพบไวรัสหรือโปรแกรมไม่ประสงค์ดี ให้บันทึกในแบบฟอร์มบันทึกเหตุละเมิดความมั่นคงปลอดภัยของสารสนเทศ (FM-DC-02) และปฏิบัติตามระเบียบปฏิบัติเรื่อง การรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยของสารสนเทศ(Reporting Information Security Incident) QP-DC-09

๕. ผู้ใช้งานต้องตรวจสอบไวรัสจากซอฟต์แวร์ป้องกันไวรัสที่เชื่อถือได้ก่อนการใช้งานสื่อบันทึกพกพาต่างๆ โดยคอมพิวเตอร์ทุกเครื่องได้ติดตั้ง Antivirus เพื่อป้องกันซอฟต์แวร์ที่ไม่ประสงค์ดี

๖. มีการสื่อสารสร้างความตระหนักให้แก่ผู้ใช้งานได้ทราบถึงแนวปฏิบัติในการลดความเสี่ยงจากไวรัสคอมพิวเตอร์ เช่น การไม่เข้าเว็บไซต์ที่มีความเสี่ยง การไม่เปิด Link จาก e-mail เป็นต้น
ISO/IEC 27001:2013 (Annex A): A.12.2

ตัวชี้วัดผลลัพธ์

๑. ติดตั้งซอฟต์แวร์ป้องกันไวรัสครบถ้วนทุกเครื่องคอมพิวเตอร์

๒. ทบทวนการ Update ซอฟต์แวร์ป้องกันไวรัสทุก ๓ เดือน

ส่วนที่ ๑๕
การรักษาความมั่นคงปลอดภัยเว็บไซต์และการใช้งานอินเทอร์เน็ต
(Website and Internet Security)

วัตถุประสงค์

เพื่อให้ระบบเทคโนโลยีสารสนเทศของ กนอ. มีความมั่นคงปลอดภัย สามารถให้บริการได้อย่างต่อเนื่องและมีประสิทธิภาพ รวมทั้งกำกับผู้ใช้งานให้ปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ขอบเขต

บังคับใช้กับทุกหน่วยงานใน กนอ.

อ้างอิงมาตรฐาน

๑. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศตามวิธีแบบปลอดภัย พ.ศ. ๒๕๕๕

๒. มาตรฐาน ISO/IEC 27001:2013 (Annex A)

แนวทางปฏิบัติ

๑. การควบคุมการใช้งานระบบจดหมายอิเล็กทรอนิกส์

๑.๑ <u>สำหรับผู้ดูแลระบบ</u>

๑.๑.๑ กำหนดสิทธิ์ตามความเหมาะสมกับการใช้บริการและหน้าที่ความรับผิดชอบของผู้ใช้งาน

๑.๑.๒ กพจ. ทบทวนสิทธิ์การเข้าใช้งานและปรับปรุงบัญชีรายชื่อผู้ใช้งานอย่างน้อยปีละ ๑ ครั้ง หรือในทันทีเมื่อมีการเปลี่ยนแปลง ได้แก่ ลาออกเปลี่ยนตำแหน่งโอนย้ายหรือสิ้นสุดการจ้าง รวมกรณีเกษียณอายุ บันทึกในแบบฟอร์มการทบทวนสิทธิ์ FM-DC-05

๑.๑.๓ ควบคุมการเข้าถึงตามแนวทางการบริหารจัดการเข้าถึงของผู้ใช้งาน (User Access Management) ที่ได้กำหนดไว้อย่างเคร่งครัด ตาม Access Contol Matrix FM-DC-03

๑.๒ <u>สำหรับผู้ใช้งาน</u>

๑.๒.๑ หน่วยงานของผู้ขอใช้ระบบสารสนเทศจัดทำบันทึกข้อความขอใช้ระบบสารสนเทศแจ้งฝ่ายดิจิทัลดำเนินการ

๑.๒.๒ เมื่อได้รับรายชื่อผู้ใช้งานและรหัสผ่าน (Password) แล้ว การเข้าสู่ระบบในครั้งแรกนั้นต้องเปลี่ยนรหัสผ่านโดยทันที

๑.๒.๓ ต้องไม่บันทึกหรือจัดเก็บรหัสผ่านในเครื่องคอมพิวเตอร์ส่วนบุคคลในรูปแบบที่ไม่ได้รับการป้องกันหรือการเข้ารหัสข้อมูล

๑.๒.๔ ต้องเปลี่ยนรหัสผ่าน (Password) ตามช่วงระยะเวลาที่กำหนด ทุก ๖ เดือน

๑.๒.๕ ต้องไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (e-mail address) ของผู้อื่นเพื่ออ่านหรือรับ-ส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของที่อยู่จดหมายอิเล็กทรอนิกส์ และให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์ต้องเป็นผู้รับผิดชอบต่อการใช้งานระบบจดหมายอิเล็กทรอนิกส์ของตน

๑.๒.๖ หลังจากใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ผู้ใช้งานต้องลงบันทึกออก (Logout) ทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์ (e-mail) ของตัวเอง

๑.๒.๗ ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับระดับ Confidential ต้องระบุความสำคัญลงในหัวข้อจดหมายอิเล็กทรอนิกส์ พร้อมกับทำการเข้ารหัส (Encryption) เอกสารแนบ

๑.๒.๘ ต้องเก็บรักษาบัญชีรายชื่อผู้ใช้ (User account) และรหัสผ่าน (Password) ของตนเองให้เป็นความลับ

๒. การใช้งานระบบอินเทอร์เน็ต (Internet)

๒.๑ ผู้ใช้งานต้องเชื่อมต่อเครื่องคอมพิวเตอร์เพื่อการเข้าใช้งานระบบอินเทอร์เน็ต (Internet) ผ่านระบบรักษาความปลอดภัยที่หน่วยงานจัดสรรไว้เท่านั้นและห้ามผู้ใช้งานทำการเชื่อมต่อเครื่องคอมพิวเตอร์ผ่านช่องทางอื่นยกเว้นแต่ว่ามีเหตุผลความจำเป็นและทำการขออนุญาตจาก ผอ.ฝดจ. เป็นลายลักษณ์อักษรก่อนการดำเนินการ

๒.๒ ผู้ใช้งานต้องเข้าถึงแหล่งข้อมูลตามสิทธิ์ที่ได้รับตามหน้าที่และความรับผิดชอบเพื่อประสิทธิภาพของระบบเครือข่ายและความปลอดภัยทางข้อมูลของ กนอ. และต้องไม่ใช้ระบบอินเทอร์เน็ตของ กนอ. เพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคลและทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสมได้แก่ เว็บไซต์ที่ขัดต่อศีลธรรมเว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติศาสนาพระมหากษัตริย์หรือเว็บไซต์ที่เป็นภัยต่อสังคมหรือละเมิดสิทธิ์ของผู้อื่นหรือข้อมูลที่อาจก่อความเสียหายให้กับ กนอ.

๒.๓ ใช้งานและดำเนินการกับข้อมูลเป็นไปตามมาตรการคุ้มครองข้อมูลในชั้นความลับนั้นๆ (Information Classification)

๒.๔ ผู้ใช้งานต้องระมัดระวังการดาวน์โหลดซอฟต์แวร์จากระบบอินเทอร์เน็ตรวมถึงการดาวน์โหลดการอัพเดท (Update) ซอฟต์แวร์ต่างๆ ต้องไม่ละเมิดลิขสิทธิ์หรือสินทรัพย์ทางปัญญา

๒.๕ การใช้งานกระดานสนทนาอิเล็กทรอนิกส์ (Webboard) ผู้ใช้งานต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของ กนอ.

๒.๖ การใช้งานกระดานสนทนาอิเล็กทรอนิกส์ (Webboard) ผู้ใช้งานต้องไม่เสนอความคิดเห็นหรือใช้ข้อความที่ยั่วยุให้ร้ายที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของ กนอ. การทำลายความสัมพันธ์กับบุคคลากรของหน่วยงานอื่นๆ

๒.๗ หลังจากใช้งานระบบอินเทอร์เน็ตเสร็จแล้วให้ผู้ใช้งานทำการปิดเว็บเบราเซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่นๆ

๓. การใช้งานเครือข่ายสังคมออนไลน์ (Social network)

๓.๑ อนุญาตให้ใช้งานเครือข่ายสังคมออนไลน์ในรูปแบบและลักษณะตามที่ กนอ. ได้กำหนดไว้

๓.๒ ผู้ใช้งานที่ใช้งานเครือข่ายสังคมออนไลน์ต้องมีความตระหนักเรื่องความมั่นคงปลอดภัยอยู่เสมอ และต้องรับผิดชอบหากเกิดความเสียหายใดๆ ที่มีผลกระทบกับ กนอ.

๓.๓ หากเกิดปัญหาจากการใช้งานเครือข่ายสังคมออนไลน์ที่อาจมีผลกระทบกับ กนอ. ผู้ใช้งานต้องแจ้งต่อฝ่ายดิจิทัลโดยเร็วที่สุดเพื่อดำเนินการตามความเหมาะสม

ISO/IEC 27001:2013 (Annex A): A.13.1.2

ตัวชี้วัดผลลัพธ์

๑. สื่อสารประชาสัมพันธ์ให้ผู้ใช้งานทราบถึงแนวทางการใช้งานอินเตอร์เน็ตที่เหมาะสมและปลอดภัยอย่างน้อยปีละ ๑ ครั้ง

ส่วนที่ ๑๖
การรักษาความปลอดภัยในอุปกรณ์ที่ใช้ปฏิบัติงาน
(Endpoint Security)

วัตถุประสงค์

เพื่อให้อุปกรณ์ด้านเทคโนโลยีสารสนเทศของ กนอ. สามารถให้บริการได้อย่างต่อเนื่องและมีประสิทธิภาพ รวมทั้งกำกับผู้ใช้งานให้ปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ขอบเขต

บังคับใช้กับทุกหน่วยงานใน กนอ.

อ้างอิงมาตรฐาน

๑. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศตามวิธีแบบปลอดภัย พ.ศ. ๒๕๕๕

๒. มาตรฐาน ISO/IEC 27001:2013 (Annex A)

แนวทางปฏิบัติ

๑. กำหนดให้มีการจัดวางและป้องกันอุปกรณ์สารสนเทศอย่างเหมาะสม มั่นคงแข็งแรง เพื่อลดความเสี่ยงจากภัยธรรมชาติหรืออันตรายต่างๆ และเพื่อป้องกันการเข้าถึงโดยมิได้รับอนุญาต

๒. มีการป้องกันอุปกรณ์สารสนเทศ ที่อาจเกิดจากไฟฟ้าขัดข้อง (Power Failure) หรือที่อาจหยุดชะงักจากข้อผิดพลาดของโครงสร้างพื้นฐาน (Supporting Utilities) โดยติดตั้ง และบำรุงรักษา อุปกรณ์หรือระบบสนับสนุนในการรักษาความมั่นคงปลอดภัยของศูนย์คอมพิวเตอร์ ได้แก่ อุปกรณ์ดับเพลิง อุปกรณ์สำรองไฟฟ้า ระบบควบคุมอุณหภูมิและความชื้น

๓. มีการบำรุงรักษาอุปกรณ์อย่างสม่ำเสมอผ่านสัญญาจ้างผู้ให้บริการ

ISO/IEC 27001:2013 (Annex A): A.11.2.1-2

ตัวชี้วัดผลลัพธ์

๑. มีการบำรุงรักษาอุปกรณ์คอมพิวเตอร์และอุปกรณ์สนับสนุนครบถ้วนทุกอุปกรณ์

ส่วนที่ ๑๗
การบริหารจัดการการเข้ารหัสข้อมูลสารสนเทศและการบริหารจัดการกุญแจ

วัตถุประสงค์

เพื่อให้ระบบเทคโนโลยีสารสนเทศของ กนอ. มีความมั่นคงปลอดภัย ป้องกันการรั่วไหลข้อมูล การรักษาความลับ สามารถให้บริการได้อย่างต่อเนื่องและมีประสิทธิภาพ รวมทั้งกำกับผู้ใช้งานให้ปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ขอบเขต

บังคับใช้กับทุกหน่วยงานใน กนอ.

อ้างอิงมาตรฐาน

๑. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศตามวิธีแบบปลอดภัย พ.ศ. ๒๕๕๕

๒. มาตรฐาน ISO/IEC 27001:2013 (Annex A)

แนวทางปฏิบัติ

๑. การเข้ารหัสข้อมูล

ข้อมูลที่สำคัญของ กนอ. ต้องกำหนดให้มีนโยบายและมาตรการการเข้ารหัสข้อมูลตามมาตรฐานสากล หรือให้สอดคล้องกับข้อตกลง ระเบียบข้อบังคับและกฎหมายที่เกี่ยวข้อง ดังนี้

๑.๑ กำหนดให้มีการจัดประเภทของข้อมูลสารสนเทศและการสื่อสารที่จะต้องได้รับการเข้ารหัส ได้แก่ ข้อมูลในชั้นความลับ Secret หากมีการส่งให้ผู้อื่น จำเป็นต้องเข้ารหัสเพื่อป้องกันการรั่วไหล

๑.๒ ผู้ดูแลระบบ ต้องกำหนดให้มีการใช้โปรแกรมที่มีความสามารถในการเข้ารหัสข้อมูล เพื่อให้บุคลากรใช้เป็นมาตรฐานเดียวกัน โดยโปรแกรมจะต้องทำหน้าที่ในการเข้ารหัสข้อมูลอย่างเหมาะสม เมื่อมีการเชื่อมต่อผ่านระบบเครือข่ายภายในองค์กร ไปยังเครื่องคอมพิวเตอร์แม่ข่าย หรืออุปกรณ์เครือข่ายต่างๆ ขององค์กร

๑.๓ ผู้ดูแลระบบ ต้องกำหนดให้มีการใช้โปรแกรมที่มีความสามารถในการเข้ารหัสข้อมูล เพื่อให้บุคลากรใช้เป็นมาตรฐานเดียวกัน โดยโปรแกรมจะต้องทำหน้าที่ในการเข้ารหัสข้อมูลอย่างเหมาะสม เมื่อมีการเชื่อมต่อจากเครือข่ายภายนอกองค์กรเข้ามายังเครือข่ายภายในองค์กร

๑.๔ ในกรณีที่มีความจำเป็นต้องเข้ารหัสข้อมูล กำหนดให้มีแนวทางการบริหารจัดการกุญแจ (Key) ที่ใช้เข้ารหัสข้อมูล เพื่อรองรับการใช้งานเทคนิคที่เกี่ยวข้องกับการเข้ารหัสลับของหน่วยงาน โดยให้มีการควบคุม กำกับ ติดตาม ให้ครอบคลุมตลอดทั้งวงจรในการนำกุญแจรหัสลับ ไปใช้งาน ได้แก่

๑.๔.๑ การสร้างกุญแจรหัสลับ ผู้ใช้งานซอฟแวร์เข้ารหัสทำการสร้างกุญแจเพื่อนำไปใช้งาน

๑.๔.๒ การจัดเก็บและดูแลรักษากุญแจรหัสลับ ผู้ใช้งานจัดเก็บและรักษากุญแจให้ปลอดภัย ป้องกันผู้ไม่เกี่ยวข้องเข้าถึง

๑.๔.๓ การนำกุญแจรหัสลับไปใช้ ผู้ใช้งานนำกุญแจไปใช้งานเพื่อถอดรหัสและป้องกันให้กุญแจปลอดภัยจากผู้ไม่เกี่ยวข้อง

ISO/IEC 27001:2013 (Annex A): A.10.1

ตัวชี้วัดผลลัพธ์

๑. ข้อมูลในชั้นความลับ Secret หากมีการส่งข้อมูลให้ผู้อื่น จะต้องเข้ารหัสก่อนทุกครั้ง

๒. สื่อสารประชาสัมพันธ์ให้ผู้ที่เกี่ยวข้องทราบถึงแนวทางการบริหารจัดการการเข้ารหัสข้อมูลสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง