ประกาศสำนักงานคณะกรรมการอาหารและยา
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
พ.ศ. ๒๕๖๖

เพื่อให้ระบบเทคโนโลยีสารสนเทศของสำนักงานคณะกรรมการอาหารและยา เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย สามารถดำเนินงานได้อย่างต่อเนื่อง สอดคล้องตามพระราชบัญญัติการปฏิบัติราชการทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๖๕ และตามมาตรฐานระบบบริหารจัดการความปลอดภัยของข้อมูล (ISO/IEC 27001:2013) ซึ่งกำหนดโดยองค์การระหว่างประเทศว่าด้วยการมาตรฐาน (The International Organization for Standardization)

อาศัยอำนาจตามความมาตรา ๓๖ และ ๓๗ แห่งพระราชบัญญัติระเบียบบริหารราชการแผ่นดิน พ.ศ. ๒๕๓๔ และที่แก้ไขเพิ่มเติม เลขาธิการคณะกรรมการอาหารและยาจึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ให้ยกเลิกประกาศสำนักงานคณะกรรมการอาหารและยา เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ลงวันที่ ๑๑ มกราคม พ.ศ. ๒๕๖๕

ข้อ ๒ นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานคณะกรรมการอาหารและยามีวัตถุประสงค์ ดังต่อไปนี้

๒.๑ เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานด้านสารสนเทศของสำนักงานคณะกรรมการอาหารและยา ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล

๒.๒ เพื่อเผยแพร่ให้เจ้าหน้าที่ทุกระดับในหน่วยงานสังกัดสำนักงานคณะกรรมการอาหารและยาได้รับทราบและถือปฏิบัติตามนโยบายอย่างเคร่งครัด

๒.๓ เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีการปฏิบัติให้ ผู้บริหาร ผู้ใช้งาน ผู้ดูแลระบบ และบุคคลภายนอกที่ปฏิบัติงานให้กับสำนักงานคณะกรรมการอาหารและยา ตระหนักถึงความสำคัญของการรักษาความมั่นคงในการใช้งานด้านสารสนเทศของสำนักงานคณะกรรมการอาหารและยา ในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด โดยจะทบทวนนโยบายปีละ ๑ ครั้ง

ข้อ ๓ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานคณะกรรมการอาหารและยา กำหนดประเด็นสำคัญ ดังต่อไปนี้

๓.๑ การควบคุมการเข้าถึงและใช้งานระบบสารสนเทศ

๓.๑.๑ การควบคุมการเข้าถึงระบบสารสนเทศ ต้องควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล ที่คำนึงถึงการใช้งานและความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศ โดยมีข้อกำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึง และสิทธิในการใช้งาน เพื่อให้ผู้ใช้งานในทุกระดับได้รับรู้ เข้าใจ และสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

๓.๑.๒ การบริหารจัดการการเข้าถึงของผู้ใช้งาน เพื่อควบคุมการเข้าถึงระบบสารสนเทศและป้องกันการเข้าถึงจากผู้ไม่ได้รับอนุญาต ต้องลงทะเบียนผู้ใช้งาน ตรวจสอบบัญชีผู้ใช้งาน อนุมัติและกำหนดรหัสผ่านการลงทะเบียนผู้ใช้งาน เพื่อให้ผู้ใช้งานได้รับอนุญาตเท่านั้นที่จะสามารถเข้าใช้งานระบบสารสนเทศได้ และต้องเก็บบันทึกข้อมูลการเข้าถึงและข้อมูลจราจรทางคอมพิวเตอร์ ตลอดจนบริหารจัดการสิทธิในการเข้าถึงข้อมูลให้เหมาะสมตามระดับชั้นความลับ ต้องทบทวนสิทธิการใช้งานและตรวจสอบการละเมิดความปลอดภัยอย่างสม่ำเสมอ

๓.๑.๓ การควบคุมการเข้าถึงเครือข่าย เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต ต้องกำหนดสิทธิในการเข้าถึงเครือข่ายให้ผู้ที่จะเข้าใช้งาน และต้องพิสูจน์ยืนยันตัวตน (Authentication) ของผู้ใช้ก่อนการเข้าใช้งาน ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์สำหรับใช้งานอินเทอร์เน็ต โดยผ่านระบบรักษาความปลอดภัยตามที่สำนักงานคณะกรรมการอาหารและยาจัดสรรไว้ และออกแบบระบบเครือข่ายโดยแบ่งเขต (Zone) การใช้งาน เพื่อทำให้การควบคุมและป้องกันภัยคุกคามได้อย่างเป็นระบบและมีประสิทธิภาพ

๓.๑.๔ การควบคุมการเข้าถึงระบบปฏิบัติการ เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต ต้องกำหนดสิทธิให้ผู้ที่จะเข้าใช้งาน และต้องพิสูจน์ยืนยันตัวตน (Authentication) ของผู้ใช้ก่อนเข้าใช้งาน ต้องระงับการใช้งานเมื่อผู้ใช้ไม่ใช้งานอย่างต่อเนื่องตามระยะเวลาที่กำหนด เพื่อจำกัดเวลาในการเชื่อมต่อระบบสารสนเทศ (Session Time-out) กำหนดมาตรการในการใช้งานโปรแกรมอรรถประโยชน์ต่างๆ เพื่อไม่ให้ละเมิดลิขสิทธิ์และป้องกันโปรแกรมไม่ประสงค์ดี

๓.๑.๕ การควบคุมการเข้าถึงโปรแกรมประยุกต์และแอพพลิเคชั่น ต้องกำหนดสิทธิการเข้าถึงระบบเทคโนโลยีสารสนเทศที่สำคัญ โปรแกรมประยุกต์หรือแอพพลิเคชั่นต่าง ๆ รวมถึงจดหมายอิเล็กทรอนิกส์ (E-Mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) และระบบงานต่าง ๆ โดยต้องให้สิทธิเพื่อการปฏิบัติงานในหน้าที่เท่านั้น และต้องได้รับความเห็นชอบจากหัวหน้าหน่วยงานเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

๓.๒ การจัดทำระบบสำรองข้อมูล เพื่อให้ระบบสารสนเทศของหน่วยงานสามารถให้บริการได้อย่างต่อเนื่องและมีเสถียรภาพ ต้องจัดทำระบบสารสนเทศและระบบสำรองข้อมูลที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน โดยคัดเลือกระบบสารสนเทศที่สำคัญเรียงลำดับความจำเป็นจากมากไปน้อย พร้อมทั้งกำหนดหน้าที่และความรับผิดชอบของเจ้าหน้าที่ในการสำรองข้อมูล และจัดทำแผนเตรียมความพร้อมในกรณีฉุกเฉินหรือในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์อย่างน้อยปีละ ๑ ครั้ง เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

๓.๓ การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ต้องตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยจัดการตรวจสอบภายในของหน่วยงาน (Internal Audit) หรือการตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Audit) อย่างน้อยปีละ ๑ ครั้ง เพื่อให้หน่วยงานได้ทราบถึงระบบความเสี่ยงและระดับความมั่นคงปลอดภัยด้านสารสนเทศ

ข้อ ๔ การพัฒนาระบบสารสนเทศต้องมีการกำหนดขั้นตอนการพิจารณา ทบทวน เพื่ออนุมัติการสร้าง การติดตั้ง การใช้งาน โดยระบบต้องมีคุณสมบัติ ดังนี้

๔.๑ สอดคล้องกับสถาปัตยกรรมระบบขององค์กร (Enterprise Architecture: EA) ในปัจจุบัน

๔.๒ สอดคล้องกับข้อกำหนดด้านความมั่นคงปลอดภัยของด้านสารสนเทศของสำนักงานคณะกรรมการอาหารและยา

๔.๓ สามารถทำงานร่วมกันกับระบบเดิมได้อย่างราบรื่น

๔.๔ ต้องผ่านการทดสอบระบบบนสภาวะแวดล้อมเดียวกันกับสภาวะแวดล้อมในการใช้งานจริงของผู้ใช้

๔.๕ ต้องเปรียบเทียบการตั้งค่าระบบ Active Directory (AD) ของสำนักงานคณะกรรมการอาหารและยา หรือระบบอื่น ๆ ที่กำหนด กับการตั้งค่าของ Center for Internet Security (CIS Benchmarks) พร้อมทั้งวิเคราะห์ถึงภัยคุกคาม (Threat) และช่องโหว่ (vulnerability)

ข้อ ๕ สำนักงานคณะกรรมการอาหารและยาต้องกำหนดการแบ่งประเภทและลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล โดยใช้แนวทางตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ และที่แก้ไขเพิ่มเติม, ระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. ๒๕๕๒ รวมถึงประกาศ กฎ ระเบียบ ข้อบังคับอื่นที่เกี่ยวข้อง

ข้อ ๖ ผู้บริหารระดับสูงของสำนักงานคณะกรรมการอาหารและยา มีหน้าที่ดูแลรับผิดชอบด้านสารสนเทศของสำนักงานคณะกรรมการอาหารและยา ให้การสนับสนุนและกำหนดทิศทางการดำเนินงานเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศที่ชัดเจน รวมทั้งมีการมอบหมายงานที่เกี่ยวข้องให้กับผู้ปฏิบัติงานอย่างชัดเจน ตลอดจนรับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นกับระบบสารสนเทศไม่ว่ากรณีใด ๆ

ข้อ ๗ แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้เป็นไปตามแนวปฏิบัติที่แนบท้ายประกาศนี้

ประกาศ ณ วันที่ ๒๕ มีนาคม พ.ศ. ๒๕๖๖

(นายไพศาล ตั้นคุ้ม)
เลขาธิการคณะกรรมการอาหารและยา

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของสำนักงานคณะกรรมการอาหารและยา

ตามประกาศสำนักงานคณะกรรมการอาหารและยา เรื่อง นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานคณะกรรมการอาหารและยา กำหนดให้มีการจัดทำแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานคณะกรรมการอาหารและยา เพื่อให้ระบบสารสนเทศของสำนักงานคณะกรรมการอาหารและยาเป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบสารสนเทศในลักษณะที่ไม่ถูกต้อง และจากการถูกคุกคามจากภัยต่าง ๆ ซึ่งอาจก่อให้เกิดความเสียหายต่อสำนักงานคณะกรรมการอาหารและยา นั้น

สำนักงานคณะกรรมการอาหารและยา จึงกำหนดแนวปฏิบัติในการใช้ระบบสารสนเทศให้มีความมั่นคงปลอดภัย ดังนี้

ข้อ ๑ คำนิยาม

“สำนักงาน” หมายถึง สำนักงานคณะกรรมการอาหารและยา

“หน่วยงาน” หมายถึง กอง กลุ่ม ศูนย์ และหน่วยงานที่มีฐานะเทียบเท่า ที่อยู่ในสังกัดสำนักงานคณะกรรมการอาหารและยา

“หน่วยงานภายนอก” หมายถึง องค์กรที่สำนักงานอนุญาตให้มีสิทธิในการเข้าถึงหรือใช้ข้อมูล หรือ ใช้งานระบบสารสนเทศของสำนักงาน โดยจะได้รับสิทธิตามประเภทการใช้งาน และต้องรับผิดชอบในการไม่เปิดเผยความลับของสำนักงาน โดยไม่ได้รับอนุญาต

“**ระบบคอมพิวเตอร์**” หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

“**ระบบเครือข่าย**” หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบสารสนเทศต่าง ๆ ของหน่วยงานได้ เช่น ระบบเครือข่ายแบบมีสาย (LAN) และระบบเครือข่ายแบบไร้สาย (Wireless LAN) เป็นต้น

“**ระบบสารสนเทศ**” หมายถึง ซอฟท์แวร์ระบบหรือซอฟท์แวร์ประยุกต์ที่ใช้ในการปฏิบัติงานของสำนักงาน หรือหน่วยงาน

“**ห้องระบบคอมพิวเตอร์**” หมายถึง สถานที่ติดตั้งเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์จัดการเครือข่ายทั้งหมด

“**ข้อมูล**” หมายถึง สิ่งที่สื่อความหมายให้รู้เรื่องราว ข้อเท็จจริง หรือ สิ่งใด ๆ ไม่ว่าการสื่อสารความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเองหรือโดยการผ่านวิธีการใด ๆ และได้จัดทำไว้ในรูปแบบเอกสาร แฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ฟิลม์ ภาพเคลื่อนไหว เสียงการบันทึกโดยเครื่องคอมพิวเตอร์ หรือ วิธีการอื่นใด ที่ทำให้สิ่งที่บันทึกไว้ ปรากฏได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์

“**ผู้ใช้งาน**” หมายถึง ข้าราชการ พนักงานราชการ ลูกจ้าง ผู้ดูแลระบบ ผู้รับบริการ หรือ ผู้ที่ได้รับอนุญาตให้ใช้ระบบคอมพิวเตอร์หรือระบบเครือข่ายของหน่วยงาน

“**ผู้บริหาร**” หมายถึง ผู้มีอำนาจในการบังคับบัญชาในหน่วยงาน ได้แก่ ผู้อำนวยการกอง เลขานุการกรม ผู้อำนวยการศูนย์ หัวหน้ากลุ่ม

“ผู้บริหารระดับสูง” หมายถึง เลขาธิการคณะกรรมการอาหารและยา รองเลขาธิการคณะกรรมการอาหารและยา หรือผู้ปฏิบัติหน้าที่แทน

“**ผู้ดูแลระบบ**” หมายถึง ผู้ที่ได้รับมอบหมายจากสำนักงานให้มีหน้าที่รับผิดชอบดูแลรักษา หรือจัดการระบบคอมพิวเตอร์และระบบเครือข่ายไม่ว่าส่วนหนึ่งส่วนใด

“ผู้รับจ้างดูแลหรือพัฒนาระบบ” หมายถึง ผู้ที่รับจ้างดูแลและบำรุงรักษา หรือพัฒนาระบบคอมพิวเตอร์และระบบเครือข่ายของสำนักงานไม่ว่าส่วนหนึ่งส่วนใด ที่อยู่ในการควบคุมของศูนย์ข้อมูลและสารสนเทศ

“เจ้าของข้อมูล” หมายถึง ผู้ได้รับมอบอำนาจจากผู้บริหารระดับสูงหรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่ให้รับผิดชอบข้อมูลของระบบสารสนเทศ โดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น ๆ หรือ ได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย

“บุคคลภายนอก” หมายถึง ผู้ประกอบการที่ยื่นคำขออนุญาตต่าง ๆ ผู้ดำเนินกิจการของผู้รับอนุญาต ผู้มีหน้าที่ปฏิบัติการ ผู้ร้องเรียนเรื่องราวต่าง ๆ ที่เกี่ยวข้องกับผลิตภัณฑ์สุขภาพหรือการทำงานของสำนักงาน

“**อุปกรณ์พกพา (Mobile Device)**” หมายถึง อุปกรณ์อิเล็กทรอนิกส์ เช่น โน้ตบุ๊ก แท็บเล็ต ตลอดจนการสื่อสารแบบไร้สาย เช่น วิทยุสื่อสาร โทรศัพท์มือถือ เป็นต้น

“**สินทรัพย์**” หมายถึง ข้อมูล หรือ ทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงาน เช่น เครื่องคอมพิวเตอร์แบบตั้งโต๊ะหรือแบบพกพา อุปกรณ์สื่อสารที่สามารถเชื่อมต่อกับระบบเครือข่าย อาทิเช่น อุปกรณ์พกพาที่มีความสามารถเชื่อมต่อกับระบบเครือข่ายได้ (Smart Devices) อุปกรณ์ระบบเครือข่าย ฮาร์ดแวร์ ซอฟต์แวร์ระบบหรือซอฟท์แวร์ประยุกต์ เป็นต้น

“**สิทธิของผู้ใช้งาน**” หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน โดยสำนักงาน หรือ หน่วยงานเป็นผู้พิจารณาสิทธิในการใช้สินทรัพย์

“**บัญชีผู้ใช้งาน (User Account)**” หมายถึง ชื่อผู้ใช้งาน (User Name) และ รหัสผ่าน (Password) เพื่อการเข้าสู่ระบบคอมพิวเตอร์และระบบเครือข่าย หรือ ระบบสารสนเทศ

“**การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ**” หมายถึง การอนุญาต การกำหนดสิทธิ หรือ การมอบอำนาจให้ผู้ใช้งานเข้าถึง หรือ ใช้งานระบบเครือข่ายหรือระบบสารสนเทศ ทั้งนี้การอนุญาตเช่นว่านั้น ให้ครอบคลุมการอนุญาตสำหรับบุคคลภายนอก รวมถึงข้อปฏิบัติเกี่ยวกับการป้องกันการเข้าถึงโดยมิชอบ

“**ความมั่นคงปลอดภัยด้านสารสนเทศ**” หมายถึง การธำรงไว้ซึ่งความลับ ความถูกต้องครบถ้วน และสภาพพร้อมใช้งาน รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง ความรับผิด การห้ามปฏิเสธความรับผิด และความน่าเชื่อถือ ของระบบคอมพิวเตอร์ ระบบเครือข่าย และระบบสารสนเทศ

“เหตุการณ์ด้านความมั่นคงปลอดภัย” หมายถึง การเกิดเหตุการณ์ สภาพของบริการ ระบบคอมพิวเตอร์ ระบบเครือข่าย หรือ ระบบสารสนเทศ ที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัย หรือมาตรการป้องกันที่ล้มเหลว หรือ เหตุการณ์อันไม่อาจคาดการณ์ไว้ก่อนได้ ที่เกี่ยวข้องกับความมั่นคงปลอดภัย

“**สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดการณ์**” หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดการณ์ไว้ก่อนได้ ซึ่งอาจมีผลให้ ระบบคอมพิวเตอร์ ระบบเครือข่าย หรือระบบสารสนเทศ ของสำนักงาน ถูกบุกรุก โจมตี หรือ ถูกคุกคาม

หมวดที่ ๑
การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

วัตถุประสงค์

๑. เพื่อควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัยของระบบสารสนเทศ

๒. เพื่อกำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึง การกำหนดสิทธิ และ การมอบอำนาจของสำนักงาน

๓. เพื่อให้ผู้ใช้งานได้รับรู้ เข้าใจ และสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

แนวปฏิบัติ

ส่วนที่ ๑ การควบคุมการเข้าถึงระบบสารสนเทศ (Access Control)

ข้อ ๑ ผู้ดูแลระบบ จะอนุญาตให้ผู้ใช้งานเข้าถึงระบบสารสนเทศที่ต้องการใช้งานได้ ต่อเมื่อได้รับอนุญาตจากเจ้าของข้อมูล ตามความจำเป็นต่อการใช้งาน เท่านั้น

ข้อ ๒ บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบสารสนเทศของสำนักงาน จะต้องขออนุญาตเป็นลายลักษณ์อักษรต่อผู้บริหารระดับสูงหรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่แทน

ข้อ ๓ ผู้ดูแลระบบ ต้องกำหนดสิทธิในการเข้าถึงข้อมูลและระบบสารสนเทศ ให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งาน และหน้าที่ความรับผิดชอบในการปฏิบัติงานของผู้ใช้งาน รวมทั้ง ทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ดังนี้

(๑) กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานระบบสารสนเทศ ที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจ ดังนี้

(๑.๑) กำหนดสิทธิของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง เช่น

- อ่านข้อมูลอย่างเดียว
- สร้าง/บันทึกข้อมูล
- ลบข้อมูล
- แก้ไขข้อมูล
- ไม่มีสิทธิ

(๑.๒) กำหนดเกณฑ์การระงับสิทธิ มอบอำนาจ ให้เป็นไปตามการบริหารจัดการ การเข้าถึงของผู้ใช้งาน (user access management) ที่ได้กำหนดไว้

(๑.๓) ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของสำนักงานจะต้องขออนุญาตเป็นลายลักษณ์อักษร และได้รับการพิจารณาอนุญาตจากผู้บริหารระดับสูงหรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่แทน

(๒) การแบ่งประเภทของข้อมูลและการจัดลำดับความสำคัญ หรือ ลำดับชั้นความลับของข้อมูล ใช้แนวทางตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ ซึ่งระเบียบดังกล่าวเป็นมาตรการที่ละเอียด รอบคอบ ถือว่าเป็นแนวทางที่เหมาะสม ในการจัดการเอกสารอิเล็กทรอนิกส์ และในการรักษาความปลอดภัยของเอกสารอิเล็กทรอนิกส์ โดยได้กำหนดกระบวนการและกรรมวิธีต่อเอกสารที่สำคัญไว้ ดังนี้

(๒.๑) จัดแบ่งประเภทของข้อมูล ออกเป็น

- ข้อมูลสารสนเทศด้านการบริหาร เช่น ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์ และคำรับรอง ข้อมูลบุคลากร ข้อมูลงบประมาณการเงินและบัญชี เป็นต้น
- ข้อมูลสารสนเทศด้านผลิตภัณฑ์สุขภาพ เช่น ข้อมูลใบอนุญาตขาย ข้อมูลใบอนุญาตผลิต ข้อมูลใบอนุญาตนำเข้า เป็นต้น

(๒.๒) จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น ๓ ระดับ คือ

- ข้อมูลที่มีระดับความสำคัญมาก
- ข้อมูลที่มีระดับความสำคัญปานกลาง
- ข้อมูลที่มีระดับความสำคัญน้อย

(๒.๓) จัดแบ่งลำดับชั้นความลับของข้อมูล

- ข้อมูลลับที่สุด หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด
- ข้อมูลลับมาก หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรง
- ข้อมูลลับ หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย
- ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

(๒.๔) จัดแบ่งระดับชั้นการเข้าถึง

- ระดับชั้นสำหรับผู้บริหารระดับสูง
- ระดับชั้นสำหรับผู้บริหาร
- ระดับชั้นสำหรับผู้ใช้งานทั่วไป
- ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย

(๒.๕) รูปแบบของเอกสารอิเล็กทรอนิกส์ แบ่งได้ดังนี้

- รูปแบบเอกสารข้อความ (Text Format) เป็นไฟล์ที่สร้างจากซอฟต์แวร์ เมื่อเปิดไฟล์จะสามารถเห็นตัวอักษรในไฟล์และอ่านข้อความนั้นได้ สามารถสร้าง เปิดและแก้ไขได้โดยใช้โปรแกรมแก้ไขข้อความ (Text Editor) ซึ่งมีรูปแบบย่อยหลายรูปแบบ เช่น TEXT Format, XML Data File, Document Format เป็นต้น

- รูปแบบเอกสาร (Portable Document File: PDF) เป็นไฟล์ที่สร้างจากซอฟต์แวร์ประเภท PDF Creator เพื่อจัดทำ e-Document เนื่องจากไฟล์ที่ได้มีคุณภาพสูง ไม่ผิดเพี้ยนจากต้นฉบับ และ ไม่สามารถแก้ไขต้นฉบับได้ เนื่องจากเอกสารรูปแบบนี้สามารถใช้งานข้ามระบบ (Cross Platform) โดยเป็นอิสระจาก ซอฟต์แวร์ ฮาร์ดแวร์ และระบบปฏิบัติการ (OS)
- รูปแบบเอกสารภาพ (Image Format) เป็นไฟล์ภาพที่สร้างจากซอฟต์แวร์ มีรูปแบบที่ใช้ เช่น JPEG Format, PNG or GIF Format, Bitmapping Format เป็นต้น

ข้อ ๔ ผู้ดูแลระบบ ต้องติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศของสำนักงาน และ เฝ้าระวังการละเมิดข้อกำหนดความปลอดภัยของระบบสารสนเทศ

ข้อ ๕ ผู้ดูแลระบบ ต้องบันทึกรายละเอียดการเข้าถึงระบบสารสนเทศ และ การแก้ไขเปลี่ยนแปลงสิทธิต่าง ๆ เพื่อเป็นหลักฐานในการตรวจสอบ

ข้อ ๖ ผู้ดูแลระบบ ต้องบันทึกการผ่านเข้า-ออกสถานที่ตั้งของระบบสารสนเทศ เพื่อเป็นหลักฐานสำหรับการตรวจสอบ

ข้อ ๗ กำหนดเวลาการเข้าถึงระบบสารสนเทศ ดังนี้

(๑) ระบบงานบริการ e-Service/e-Submission (Front Office) สำหรับผู้ใช้งานภายนอกสามารถเข้าถึงได้ตลอดเวลา

(๒) ระบบงานภายใน (Back Office) สำหรับผู้ใช้งานภายในสามารถเข้าถึงได้ตลอดเวลา

ส่วนที่ ๒ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

ข้อ ๘ ผู้ดูแลระบบ ต้องกำหนดการลงทะเบียนผู้ใช้งานใหม่ ดังนี้

(๑) จัดทำแบบฟอร์มการลงทะเบียนผู้ใช้งาน สำหรับระบบสารสนเทศ

(๒) ต้องตรวจสอบบัญชีผู้ใช้งาน เพื่อไม่ให้มีการลงทะเบียนซ้ำซ้อน

(๓) ต้องตรวจสอบและให้สิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ (ตามข้อ ๓)

(๔) ต้องส่งมอบเอกสาร หรือ สิ่งที่แสดงเป็นลายลักษณ์อักษรให้แก่ผู้ใช้งาน เพื่อแสดงถึงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งานในการเข้าถึงระบบสารสนเทศ

ข้อ ๙ ผู้ดูแลระบบ ต้องกำหนดสิทธิการใช้งานระบบสารสนเทศที่สำคัญเฉพาะการปฏิบัติงานในหน้าที่ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-Mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยต้องได้รับความเห็นชอบเป็นลายลักษณ์อักษรจากผู้บริหารระดับสูงหรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่

ข้อ ๑๐ ผู้ดูแลระบบต้องทบทวนบัญชีผู้ใช้งาน สิทธิการใช้งาน อย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต โดยปฏิบัติตามแนวทาง ดังนี้

(๑) พิมพ์รายชื่อของผู้ที่ยังมีสิทธิในระบบแยกตามหน่วยงาน

(๒) จัดส่งรายชื่อนั้นให้กับผู้บังคับบัญชาของหน่วยงานเพื่อทบทวนรายชื่อและสิทธิการใช้งาน

(๓) แก้ไขข้อมูล สิทธิต่าง ๆ ให้ถูกต้องตามที่ได้รับแจ้งกลับจากหน่วยงาน

(๔) ขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน เมื่อลาออกต้องดำเนินการภายใน ๓ วัน หรือเมื่อเปลี่ยนตำแหน่งงานภายใน ต้องดำเนินการภายใน ๗ วัน หรือ เมื่อถูกให้ออกจากราชการภายใน ๑ วัน หลังจากที่ได้รับแจ้งจากหน่วยงาน กรณีการยกเลิกสัญญาของลูกจ้างเหมา ให้หน่วยงานแจ้งว่าการยกเลิกสัญญานั้น เข้าข่ายเป็นการลาออกหรือให้ออก

ข้อ ๑๑ การบริหารจัดการบัญชีผู้ใช้

(๑) ให้ยกเลิกบัญชีผู้ใช้ (User Account) เมื่อผู้ใช้งานลาออก หรือ พ้นจากตำแหน่ง หรือ ยกเลิกการใช้งาน

(๒) กำหนดการสร้างชื่อบัญชีผู้ใช้และรหัสผ่าน (Password) เป็นไปตามข้อกำหนดของสำนักงานสำหรับแต่ละระบบงาน

(๓) กำหนดให้ผู้ใช้งานต้องไม่บันทึกหรือเก็บรหัสผ่าน ไว้ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึงโดยบุคคลอื่นนอกจากตนเอง

(๔) กำหนดรหัสผ่านเริ่มต้นให้กับผู้ใช้งานให้ยากต่อการเดา และส่งมอบรหัสผ่านให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย

(๕) การให้สิทธิสูงสุดเฉพาะกาลกับผู้ใช้งานคนใดก็ตาม จะต้องได้รับความเห็นชอบและอนุมัติจากผู้บริหารระดับสูงหรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่ โดยต้องกำหนดระยะเวลาการใช้งานและระงับการใช้งานในทันทีเมื่อพ้นระยะเวลาดังกล่าว หรือเมื่อบุคคลนั้น พ้นจากตำแหน่ง โดยให้กำหนดว่า ผู้ใช้งานนั้น สามารถเข้าถึงระดับใดได้ และ ต้องกำหนดกลุ่มบัญชีผู้ใช้งานต่างจากผู้ใช้งานตามปกติ

ข้อ ๑๒ ผู้ดูแลระบบ ต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับ ในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรง และ การเข้าถึงผ่านระบบสารสนเทศ รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทตามชั้นความลับ ดังต่อไปนี้

(๑) ควบคุมการเข้าถึงข้อมูลแต่ละประเภทตามชั้นความลับ ทั้งการเข้าถึงโดยตรง และการเข้าถึงผ่านระบบสารสนเทศ

(๒) กำหนดกลุ่มผู้ใช้งานให้กับชื่อผู้ใช้งาน เพื่อการตรวจสอบตัวตนจริงของผู้ใช้งานในแต่ละลำดับชั้นความลับของข้อมูล

(๓) กำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

(๔) การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL หรือ VPN หรือ XML Encryption เป็นต้น

(๕) กำหนดการเปลี่ยนรหัสผ่าน (Password) ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

(๖) กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล ในกรณีที่นำสินทรัพย์ออกนอกหน่วยงาน เช่น บำรุงรักษา ตรวจซ่อม ให้ดำเนินการสำรอง และ ลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

(๗) เจ้าของข้อมูลต้องตรวจสอบความเหมาะสมของสิทธิในการเข้าถึงข้อมูลของผู้ใช้งาน อย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิต่าง ๆ ที่ให้ไว้ยังคงมีความเหมาะสม

ข้อ ๑๓ การเชื่อมโยงแลกเปลี่ยนข้อมูล ให้ผู้บริหารระดับสูง พิจารณาประเด็นต่าง ๆ ทางด้านความมั่นคงปลอดภัยและจุดอ่อนต่าง ๆ ก่อนตัดสินใจเชื่อมโยงแลกเปลี่ยนข้อมูลระหว่างกันในระบบสารสนเทศ เช่น ระหว่าง สำนักงานกับหน่วยงานภายนอก ดังนี้

(๑) กำหนดนโยบายและมาตรการเพื่อควบคุม ป้องกัน และบริหารจัดการการเชื่อมโยงแลกเปลี่ยนข้อมูลระหว่างกัน

(๒) พิจารณาจำกัดหรือไม่อนุญาตการเข้าถึงข้อมูลลับ

(๓) พิจารณากำหนดผู้ใช้งานใดที่มีสิทธิหรือได้รับอนุญาตให้เข้าถึง

(๔) พิจารณาการลงทะเบียนผู้ใช้งาน

(๕) ต้องไม่อนุญาตการใช้งานข้อมูลสำคัญหรือข้อมูลลับ ในกรณีที่ระบบไม่มีมาตรการป้องกันเพียงพอ

ส่วนที่ ๓ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

ข้อ ๑๔ การใช้งานรหัสผ่าน ผู้ใช้งานต้องปฏิบัติ ดังนี้

(๑) ผู้ใช้งานมีหน้าที่ในการป้องกัน ดูแล รักษาข้อมูลบัญชีชื่อผู้ใช้งาน (User Account) และรหัสผ่าน (Password) โดยผู้ใช้งานแต่ละคนต้องมีบัญชีชื่อผู้ใช้งานของตนเอง ห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามเผยแพร่ แจกจ่าย หรือให้ผู้อื่นล่วงรู้รหัสผ่าน

(๒) กำหนดรหัสผ่านให้ประกอบด้วยตัวอักษรไม่น้อยกว่า ๘ ตัวอักษร ซึ่งต้องประกอบด้วย ตัวเลข (Numerical character) ตัวอักษร (Alphabet) และตัวอักษรพิเศษ (Special character)

(๓) ไม่กำหนดรหัสผ่านของบัญชีผู้ใช้ของตนเองจากชื่อหรือนามสกุลของตนเอง หรือบุคคลในครอบครัว

(๔) ไม่ใช้รหัสผ่านของบัญชีผู้ใช้ของตนเองในการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

(๕) ไม่ใช้ฟังก์ชั่นหรือโปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านแบบอัตโนมัติ (save password) สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่ผู้ใช้งานครอบครองอยู่

(๖) ไม่จดหรือบันทึกรหัสผ่านไว้ในสถานที่ ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

(๗) ผู้ใช้งานต้องเปลี่ยนรหัสผ่านในทุก ๙๐ วัน หรือ ทุกครั้งได้รับการแจ้งเตือนให้เปลี่ยนรหัสผ่าน

ข้อ ๑๕ การนำการเข้ารหัส (Encryption) มาใช้กับข้อมูลที่เป็นความลับ ผู้ใช้งานจะต้องปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ และที่แก้ไขเพิ่มเติม, ระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. ๒๕๕๒ รวมถึงประกาศ กฎ ระเบียบ ข้อบังคับอื่นที่เกี่ยวข้อง และต้องใช้วิธีการเข้ารหัสที่เป็นมาตรฐานสากล

ข้อ ๑๖ การกระทำใด ๆ ที่เกิดจากการใช้บัญชีผู้ใช้งาน ที่มีกฎหมายกำหนดให้เป็นความผิด ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม ให้ถือว่าเป็นความรับผิดชอบที่เจ้าของบัญชีผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้น

ข้อ ๑๗ ผู้ใช้งานต้องพิสูจน์ตัวตนทุกครั้งก่อนที่จะใช้ระบบคอมพิวเตอร์หรือระบบสารสนเทศของสำนักงาน หากเกิดปัญหาในการพิสูจน์ตัวตนนั้น ไม่ว่าจากการล็อกของรหัสผ่าน หรือจากความผิดพลาดใด ๆ ก็ตาม ผู้ใช้งานจะต้องแจ้งให้ผู้ดูแลระบบทราบทันที โดยปฏิบัติตามแนวทาง ดังนี้

(๑) ต้องพิสูจน์ตัวตนทุกครั้ง ก่อนเข้าถึงระบบปฏิบัติการของคอมพิวเตอร์ทุกประเภท

(๒) ต้องพิสูจน์ตัวตนทุกครั้ง ก่อนการใช้งานระบบคอมพิวเตอร์อื่นในเครือข่าย

(๓) ต้องพิสูจน์ตัวตนทุกครั้ง ก่อนการใช้งานอินเทอร์เน็ต และต้องบันทึกข้อมูลซึ่งสามารถระบุตัวตนของผู้ใช้งานได้

(๔) ต้องล็อกหน้าจอทุกครั้ง เมื่อผู้ใช้งานไม่อยู่ที่คอมพิวเตอร์ และ ต้องพิสูจน์ตัวตนทุกครั้ง ก่อนกลับมาใช้งานระบบสารสนเทศต่อ

(๕) ต้องตั้งเวลาพักหน้าจอ (screen saver) ให้กับคอมพิวเตอร์ทุกเครื่อง โดยเริ่มพักหน้าจอ หลังจากที่ผู้ใช้หยุดการใช้งานเป็นเวลา ๑๐ นาที

ข้อ ๑๘ ผู้ใช้งานต้องตระหนักและระมัดระวังต่อการใช้งานข้อมูล ไม่ว่าข้อมูลนั้นจะเป็นของสำนักงาน หรือเป็นของบุคคลภายนอก

ข้อ ๑๙ ห้ามไม่ให้เผยแพร่ เปลี่ยนแปลง ทำซ้ำ หรือทำลาย ข้อมูลที่เป็นความลับหรือมีระดับความสำคัญ ที่อยู่ในการครอบครอง/ดูแลของหน่วยงาน โดยไม่ได้รับอนุญาตจากผู้บริหารระดับสูง

ข้อ ๒๐ ผู้ใช้งานมีส่วนร่วมในการดูแลรักษาและรับผิดชอบต่อข้อมูลของสำนักงาน และข้อมูลของบุคคลภายนอก หากเกิดการสูญหาย หรือ นำไปใช้ในทางที่ผิด หรือเผยแพร่โดยไม่ได้รับอนุญาต ผู้ใช้งานต้องมีส่วนร่วมรับผิดชอบต่อความเสียหายนั้นด้วย

ข้อ ๒๑ ผู้ใช้งานต้องป้องกัน ดูแล รักษาไว้ซึ่งความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูล ตลอดจนเอกสาร สื่อบันทึกข้อมูลคอมพิวเตอร์ หรือสารสนเทศต่าง ๆ ที่เสี่ยงต่อการเข้าถึงโดยผู้ไม่มีสิทธิ

ข้อ ๒๒ ผู้ใช้งานมีสิทธิโดยชอบธรรมที่จะเก็บรักษา ใช้งาน และป้องกันข้อมูลส่วนบุคคลตามสมควร สำนักงานจะต้องให้การสนับสนุนและเคารพต่อสิทธิส่วนบุคคล และไม่อนุญาตให้บุคคลหนึ่งบุคคลใดละเมิดต่อข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตจากผู้ใช้งานที่ครอบครองข้อมูลนั้น ยกเว้นในกรณีที่สำนักงานต้องการตรวจสอบข้อมูลหรือคาดว่าข้อมูลนั้นเกี่ยวข้องกับสำนักงาน ซึ่งสำนักงานอาจแต่งตั้งผู้ทำหน้าที่ตรวจสอบ เพื่อตรวจสอบข้อมูลเหล่านั้นได้ตลอดเวลา โดยไม่ต้องแจ้งให้ผู้ใช้งานทราบ

ข้อ ๒๓ ห้ามใช้งานโปรแกรมประเภท Peer-to-Peer (หมายถึง วิธีการจัดเครือข่ายที่กำหนดให้คอมพิวเตอร์ในเครือข่ายแต่ละเครื่อง มีแฟ้มข้อมูลเก็บไว้ในตัวเอง ซึ่งผู้ใช้สามารถใช้แฟ้มข้อมูลจากคอมพิวเตอร์ แทนการใช้จากเครื่องบริการแฟ้ม (File Server) เท่านั้น) หรือ โปรแกรมที่มีความเสี่ยงในระดับเดียวกัน เช่น บิทเทอร์เรนท์ (Bittorrent), อีมูล (Emule) เป็นต้น เว้นแต่จะได้รับอนุญาตจากผู้บริหารระดับสูงหรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่

ข้อ ๒๔ ห้ามใช้งานโปรแกรมออนไลน์เพื่อความบันเทิง เช่น การดูหนัง ฟังเพลง เกมส์ เป็นต้น ในระหว่างเวลาปฏิบัติราชการ

ข้อ ๒๕ ห้ามใช้สินทรัพย์ของสำนักงาน เผยแพร่ ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใด ที่มีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมาย หรือ กระทบต่อภารกิจของสำนักงาน

ข้อ ๒๖ ห้ามใช้สินทรัพย์ของสำนักงาน เพื่อรบกวน ก่อให้เกิดความเสียหาย หรือใช้ในการโจรกรรมข้อมูล หรือสิ่งอื่นใดอันเป็นการขัดต่อกฎหมายและศีลธรรม หรือกระทบต่อภารกิจของสำนักงาน

ข้อ ๒๗ ห้ามใช้สินทรัพย์ของสำนักงาน เพื่อประโยชน์ทางการค้า

ข้อ ๒๘ ห้ามกระทำการใด ๆ เพื่อดักข้อมูล ไม่ว่าจะเป็นข้อความ ภาพ เสียง หรือสิ่งอื่นใดในระบบเครือข่ายของสำนักงาน ไม่ว่าจะด้วยวิธีการใด ๆ ก็ตาม

ข้อ ๒๙ ห้ามรบกวน ทำลาย หรือทำให้ระบบสารสนเทศของสำนักงานต้องหยุดชะงัก

ข้อ ๓๐ ห้ามใช้ระบบสารสนเทศของสำนักงาน เพื่อการควบคุมคอมพิวเตอร์ หรือ ระบบสารสนเทศภายนอก โดยไม่ได้รับอนุญาตจากผู้บริหารระดับสูงหรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่

ข้อ ๓๑ ห้ามกระทำการใด ๆ อันมีลักษณะเป็นการลักลอบใช้งานระบบคอมพิวเตอร์หรือระบบสารสนเทศ หรือดักรับรหัสผ่านของผู้อื่น ไม่ว่าจะเป็นไปเพื่อประโยชน์ในการเข้าถึงข้อมูล หรือเพื่อการใช้ทรัพยากร หรือเพื่อการอื่นใด ก็ตาม

ข้อ ๓๒ ห้ามติดตั้งอุปกรณ์หรือกระทำการใด ๆ เพื่อเข้าถึงระบบคอมพิวเตอร์ หรือระบบเครือข่าย หรือระบบสารสนเทศของสำนักงาน โดยไม่ได้รับอนุญาตจากผู้บริหารระดับสูงหรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่

ข้อ ๓๓ การควบคุมการไม่ทิ้งสินทรัพย์สารสนเทศที่สำคัญไว้ในที่ไม่ปลอดภัย (Clear desk and clear screen policy) ผู้ใช้งานต้องควบคุมเอกสาร ข้อมูล หรือสื่อต่าง ๆ ที่มีข้อมูลสำคัญจัดเก็บหรือบันทึกอยู่ ไม่ให้วางทิ้งไว้บนโต๊ะทำงาน หรือในสถานที่ไม่ปลอดภัยในขณะไม่ได้นำมาใช้งาน ตลอดจนการควบคุมหน้าจอคอมพิวเตอร์ (Desktop) ไม่ให้มีข้อมูลสำคัญปรากฏในขณะไม่ได้ใช้งาน

ส่วนที่ ๔ การบริหารจัดการสินทรัพย์ (Assets Management)

ข้อ ๓๔ ผู้ใช้งานต้องไม่เข้าไปในห้องระบบคอมพิวเตอร์ (หมายถึง สถานที่ติดตั้งเครื่องคอมพิวเตอร์แม่ข่าย และ/หรือ อุปกรณ์จัดการเครือข่าย) ที่เป็นเขตหวงห้ามโดยเด็ดขาด เว้นแต่จะได้รับอนุญาตจากผู้บริหารระดับสูงหรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่

ข้อ ๓๕ ผู้ใช้งานต้องไม่นำอุปกรณ์หรือชิ้นส่วนใด ออกจากห้องระบบคอมพิวเตอร์ เว้นแต่จะได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ ๓๖ ผู้ใช้งานต้องไม่นำเครื่องมือหรืออุปกรณ์อื่นใด เชื่อมต่อเข้าเครือข่ายเพื่อการประกอบธุรกิจส่วนบุคคล

ข้อ ๓๗ ผู้ใช้งานต้องไม่คัดลอกหรือทำสำเนาแฟ้มข้อมูลของผู้อื่น ก่อนได้รับอนุญาตจากเจ้าของแฟ้มข้อมูล และผู้ใช้งานต้องไม่ใช้หรือลบแฟ้มข้อมูลของผู้อื่น ไม่ว่ากรณีใด ๆ

ข้อ ๓๘ ผู้ใช้งานต้องทำลายข้อมูลสำคัญในอุปกรณ์สื่อบันทึกข้อมูล แฟ้มข้อมูล ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว และใช้เทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูล ก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้เข้าถึงข้อมูลสำคัญนั้นได้ และพิจารณาวิธีการทำลายข้อมูลบนสื่อบันทึกข้อมูลแต่ละประเภท ดังนี้

ประเภทสื่อบันทึกข้อมูล	วิธีทำลาย
กระดาษ	ให้ทำลายด้วยเครื่องทำลายเอกสาร
Flash Drive/Memory Stick/Memory Card	- ให้ทำลายข้อมูลบน Flash Drive ตามมาตรฐาน DOD ๕๒๒๐.๒๒ M ของกระทรวงกลาโหมสหรัฐอเมริกา ซึ่งเป็นมาตรฐานการทำลายข้อมูลโดยการเขียนทับข้อมูลเดิมหลายรอบ - ใช้วิธีการทุบหรือบดให้เสียหาย
แผ่น CD/DVD	ให้ทำลายด้วยเครื่องทำลายเอกสาร
เทป	ให้ทุบหรือบดให้เสียหาย หรือเผาทำลาย
ฮาร์ดดิสก์	- ให้ทำลายข้อมูลบนฮาร์ดดิสก์ตามมาตรฐาน DOD ๕๒๒๐.๒๒ M ของกระทรวงกลาโหมสหรัฐอเมริกา ซึ่งเป็นมาตรฐานการทำลายข้อมูลโดยการเขียนทับข้อมูลเดิมหลายรอบ - ใช้วิธีการทุบหรือบดให้เสียหาย

ข้อ ๓๙ ผู้ใช้งานต้องรับผิดชอบต่อสินทรัพย์ที่สำนักงานมอบไว้ให้ใช้งาน เสมือนหนึ่งเป็นสินทรัพย์ของผู้ใช้งานเอง โดยบรรดารายการสินทรัพย์ (Asset lists) ที่ผู้ใช้งานต้องรับผิดชอบ การรับหรือคืนสินทรัพย์ จะต้องได้รับการบันทึกและตรวจสอบทุกครั้งโดยเจ้าหน้าที่ที่สำนักงานมอบหมายให้รับผิดชอบการดูแลสินทรัพย์

ข้อ ๔๐ กรณีที่ผู้ใช้งานนำสินทรัพย์ออกนอกสำนักงาน ผู้ใช้งานต้องดูแลและรับผิดชอบสินทรัพย์ของสำนักงานที่ได้รับไว้ใช้งาน

ข้อ ๔๑ ผู้ใช้งานต้องชดใช้ค่าเสียหาย ไม่ว่าสินทรัพย์นั้นจะชำรุด หรือสูญหายตามมูลค่าของสินทรัพย์ หากความเสียหายนั้นเกิดจากความประมาทเลินเล่อของผู้ใช้งาน

ข้อ ๔๒ ผู้ใช้งานต้องไม่ให้ผู้อื่นยืมสินทรัพย์ ไม่ว่าในกรณีใด ๆ เว้นแต่การยืมนั้น ได้รับการอนุมัติเป็นลายลักษณ์อักษรจากผู้บริหารระดับสูงหรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่

ข้อ ๔๓ ผู้ใช้งานมีสิทธิใช้สินทรัพย์หรือระบบสารสนเทศที่สำนักงานจัดเตรียมไว้ให้ใช้งานตามวัตถุประสงค์ในการทำงานของสำนักงาน ห้ามมิให้ผู้ใช้งานนำสินทรัพย์และระบบสารสนเทศ ไปใช้ในกิจกรรมที่สำนักงานไม่ได้กำหนด หรือในกิจกรรมที่ก่อให้เกิดความเสียหายต่อสำนักงาน

ข้อ ๔๔ ความเสียหายใด ๆ ที่เกิดจากการละเมิดตามข้อ ๔๒ ให้ถือเป็นความผิดส่วนบุคคลโดยผู้ใช้งานต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

ส่วนที่ ๕ การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

ข้อ ๔๕ มาตรการควบคุมการเข้า-ออกห้องระบบคอมพิวเตอร์

(๑) ผู้ติดต่อจากหน่วยงานภายนอก ต้องแลกบัตรที่ใช้ระบุตัวตน เช่น บัตรประชาชน หรือใบอนุญาตขับขี่ กับเจ้าหน้าที่รักษาความปลอดภัย เพื่อรับบัตรผู้ติดต่อ (Visitor) แล้วลงบันทึกข้อมูลลงในสมุดบันทึก ตามที่ระบุไว้ในเอกสาร **“บันทึกการเข้าออกพื้นที่”**

(๒) ผู้ติดต่อจากหน่วยงานภายนอก ที่นำอุปกรณ์คอมพิวเตอร์ หรืออุปกรณ์มาใช้ในการปฏิบัติงานที่ห้องระบบคอมพิวเตอร์ ต้องลงบันทึกรายการอุปกรณ์ในแบบฟอร์มขออนุญาตเข้าออก ตามที่ระบุไว้ในเอกสาร **“บันทึกการเข้าออกพื้นที่”** ให้ถูกต้องชัดเจน

(๓) ผู้ดูแลระบบ ต้องตรวจสอบความถูกต้องของข้อมูลในสมุดบันทึก แบบฟอร์มขออนุญาตเข้าออก กับเจ้าหน้าที่รักษาความปลอดภัยเป็นประจำทุกเดือน

ข้อ ๔๖ ผู้ใช้งานที่จะนำคอมพิวเตอร์ อุปกรณ์ใด ๆ มาเชื่อมต่อกับระบบคอมพิวเตอร์ ระบบเครือข่ายของสำนักงาน ต้องได้รับอนุญาตจากผู้บริหารระดับสูงหรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่ และต้องปฏิบัติตามนโยบายนี้อย่างเคร่งครัด โดยผู้ใช้งานต้องกรอกแบบฟอร์มขอเชื่อมต่อระบบเครือข่าย โดยดาวน์โหลดจากเว็บไซต์ของสำนักงาน

ข้อ ๔๗ การขอใช้พื้นที่ Web Server ชื่อโดเมนย่อย (Sub Domain Name) ที่สำนักงานรับผิดชอบ จะต้องทำหนังสือขออนุญาตใช้พื้นที่ Web Server ชื่อโดเมนย่อย (Sub Domain Name) รวมทั้งขอติดตั้งโปรแกรมที่จะใช้งาน ต่อผู้บริหารระดับสูงหรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่ โดยโปรแกรมที่จะติดตั้งนั้น ต้องไม่ส่งผลกระทบต่อการทำงานของระบบคอมพิวเตอร์ หรือระบบสารสนเทศ หรือการใช้งานของผู้ใช้งานอื่น ๆ

ข้อ ๔๘ ห้ามผู้ใด เคลื่อนย้าย ติดตั้งเพิ่มเติม หรือกระทำการใด ๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลัก เป็นต้น โดยไม่ได้รับอนุญาตจากผู้อำนวยการศูนย์ข้อมูลและสารสนเทศหรือผู้ปฏิบัติหน้าที่แทน

ข้อ ๔๙ ผู้ดูแลระบบ ต้องควบคุมการเข้าถึงระบบเครือข่าย เพื่อให้สามารถบริหารจัดการระบบเครือข่ายได้อย่างมีประสิทธิภาพ ดังต่อไปนี้

(๑) ต้องจำกัดสิทธิการใช้งานเพื่อควบคุมผู้ใช้งานให้สามารถใช้งานได้เฉพาะระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น

(๒) ต้องจำกัดเส้นทางการเข้าถึงระบบเครือข่ายที่ใช้งานร่วมกัน

(๓) ต้องจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่าย เพื่อมิให้ผู้ใช้งานสามารถใช้เส้นทางอื่น ๆ ได้

(๔) ระบบเครือข่ายทั้งหมดของสำนักงานที่เชื่อมต่อกับระบบเครือข่ายอื่น ๆ ภายนอกสำนักงาน ต้องเชื่อมต่อผ่านระบบป้องกันเครือข่าย (Firewall) ที่สามารถในการตรวจจับโปรแกรมที่ไม่พึงประสงค์ หรือประสงค์ร้าย รวมทั้งสามารถตรวจสอบการใช้งานในลักษณะที่ผิดปกติของผู้ใช้งานระบบเครือข่ายของสำนักงาน

(๕) การเข้าสู่ระบบเครือข่ายภายในของสำนักงาน โดยผ่านทางระบบอินเทอร์เน็ต จำเป็นต้องลงบันทึกเข้าใช้งาน โดยแสดงตัวเข้าใช้งาน (Login) ด้วยชื่อบัญชีผู้ใช้งาน (User Account) เพื่อพิสูจน์ยืนยันตัวตน (Authentication) ของผู้ใช้งานก่อนทุกครั้ง

(๖) ต้องป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อกับระบบเครือข่ายของสำนักงาน สามารถมองเห็น IP Address ของระบบเครือข่ายภายในของสำนักงาน

(๗) ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอก ตลอดจนอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอย่างสม่ำเสมอ

(๘) การระบุอุปกรณ์บนเครือข่าย

- ผู้ดูแลระบบต้องเก็บบัญชีการขอเชื่อมต่อเครือข่าย ได้แก่ รายชื่อผู้ขอใช้งาน รายละเอียดเครื่องคอมพิวเตอร์ที่ขอใช้ IP Address และสถานที่ติดตั้ง
- ผู้ดูแลระบบต้องจำกัดสิทธิของผู้ใช้งานที่สามารถเข้าใช้อุปกรณ์ได้
- ต้องระบุหมายเลขอุปกรณ์ที่เชื่อมต่อจากเครือข่ายภายนอกว่า สามารถให้เข้าเชื่อมต่อกับเครือข่ายภายในได้หรือไม่
- อุปกรณ์เครือข่ายต้องสามารถตรวจสอบ IP Address ของทั้งต้นทางและปลายทางได้
- ผู้ขอใช้งานต้องกรอกแบบฟอร์มขอเชื่อมต่อเครือข่าย โดยดาวน์โหลดจากเว็บไซต์ของสำนักงาน
- การใช้งานอุปกรณ์บนเครือข่ายต้องพิสูจน์ตัวตนทุกครั้งที่ใช้อุปกรณ์

ข้อ ๕๐ ผู้ดูแลระบบ ต้องบริหารจัดการคอมพิวเตอร์แม่ข่าย (Server) และรับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่าต่าง ๆ ของซอฟต์แวร์ระบบ (Systems Software) ของคอมพิวเตอร์แม่ข่าย (Server)

ข้อ ๕๑ การติดตั้งหรือปรับปรุงซอฟต์แวร์ของระบบสารสนเทศต้องขออนุมัติจากผู้ดูแลระบบ ก่อนติดตั้ง

ข้อ ๕๒ กำหนดให้มีการจัดเก็บซอร์สโค้ด ไลบรารี่ และเอกสารสำหรับซอฟต์แวร์ของระบบสารสนเทศไว้ในสถานที่ที่มีความมั่นคงปลอดภัย

ข้อ ๕๓ จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ที่ถูกต้อง เพื่อใช้ระบุตัวบุคคลผู้เข้าใช้งานระบบคอมพิวเตอร์และระบบเครือข่าย ได้ตามพระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม

ข้อ ๕๔ กำหนดมาตรการควบคุมการใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) จากผู้ใช้งานภายนอกหน่วยงาน เพื่อดูแลรักษาความปลอดภัยของระบบ ตามแนวทางปฏิบัติดังต่อไปนี้

(๑) บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) ของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษรจากผู้บริหารระดับสูงหรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่ โดยแสดงหลักฐาน ระบุเหตุผล หรือความจำเป็นอย่างเพียงพอ

(๒) มีการควบคุมช่องทาง (Port) ที่ใช้เข้าสู่ระบบอย่างรัดกุม

(๓) วิธีการใด ๆ ที่สามารถเข้าถึงข้อมูล หรือระบบข้อมูลได้จากระยะไกล ต้องได้รับการอนุญาตจากผู้บริหารระดับสูงหรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่

(๔) ต้องจัดทำบันทึกเข้าสู่ระบบเครือข่ายภายใน หรือระบบสารสนเทศ (Login) ของสำนักงานจากระยะไกล โดยระบุชื่อผู้ใช้งาน ที่ผ่านการพิสูจน์ยืนยันตัวตน (Authentication) ก่อนใช้งานอย่างถูกต้อง

ข้อ ๕๕ กำหนดให้มีการแบ่งแยกเครือข่าย ดังต่อไปนี้

(๑) Internet แบ่งแยกเครือข่ายเป็นเครือข่ายย่อย ๆ ตามอาคารต่าง ๆ เพื่อควบคุมการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต

(๒) Intranet แบ่งเครือข่ายภายในและเครือข่ายภายนอก เพื่อความปลอดภัยในการใช้งานระบบสารสนเทศภายใน

ข้อ ๕๖ ต้องกำหนดวิธีการป้องกันเครือข่ายและอุปกรณ์ต่าง ๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจน และทบทวนการกำหนดค่า Parameter ต่าง ๆ เช่น IP Address อย่างน้อยปีละ ๑ ครั้ง นอกจากนี้ การกำหนดแก้ไขหรือเปลี่ยนแปลงค่า parameter ต้องแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

ข้อ ๕๗ ระบบเครือข่ายทั้งหมดที่เชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกหน่วยงาน ต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก หรือโปรแกรมในการทำ Packet filtering เช่น ไฟร์วอลล์ (Firewall) หรือฮาร์ดแวร์อื่น ๆ ที่มีความสามารถในการตรวจจับโปรแกรมไม่ประสงค์ดี (Malware) ด้วย

ข้อ ๕๘ ต้องติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการบุกรุกผ่านระบบเครือข่าย การใช้งานในลักษณะที่ผิดปกติ และการแก้ไขเปลี่ยนแปลงระบบเครือข่าย โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

ข้อ ๕๙ ต้องจัดระบบป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อกับระบบเครือข่ายของสำนักงาน สามารถมองเห็น IP address ของระบบเครือข่ายภายในได้ เพื่อมิให้บุคคลภายนอก รู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายภายในของสำนักงานได้โดยง่าย

ข้อ ๖๐ การใช้เครื่องมือต่าง ๆ (Tools) เพื่อการตรวจสอบระบบเครือข่ายต้องได้รับการอนุมัติจากผู้ดูแลระบบและจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

ส่วนที่ ๖ การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

ข้อ ๖๑ ผู้ดูแลระบบ ต้องกำหนดวิธีการลงทะเบียนบุคลากรใหม่ของสำนักงาน (โดยปฏิบัติตามข้อ ๘) ในการใช้งานตามความจำเป็น รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน (โดยปฏิบัติตามข้อ ๑๐) เช่น การลาออกหรือพ้นจากตำแหน่ง การยกเลิกการใช้งาน หรือ การเปลี่ยนตำแหน่งงานภายในสำนักงาน เป็นต้น

ข้อ ๖๒ กำหนดขั้นตอนการปฏิบัติเพื่อเข้าใช้งาน

(๑) ผู้ใช้งานต้องกำหนดรหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ที่ได้รับมอบ

(๒) หลังจากติดตั้งระบบเสร็จ ต้องยกเลิกบัญชีผู้ใช้งาน หรือเปลี่ยนรหัสผ่านของผู้ใช้งานทุกรายที่ถูกกำหนดเอาไว้เป็นค่าเริ่มต้นที่มาพร้อมกับระบบ ในทันที

(๓) ผู้ใช้งานต้องตั้งค่าการใช้งานโปรแกรมพักหน้าจอ (Screen saver) เพื่อล็อกหน้าจอภาพเมื่อไม่ได้ใช้งาน ซึ่งผู้ใช้งานต้องใส่รหัสผ่าน (Password) เพื่อเข้าใช้งานต่อ

(๔) ผู้ใช้งานต้องบันทึกเข้าใช้งาน (Login) ทุกครั้งก่อนเข้าใช้ระบบปฏิบัติการ และต้องลงบันทึกออก (Logout) ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

(๕) ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อบัญชีผู้ใช้งาน (User Account) ของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ของหน่วยงานร่วมกัน

(๖) ห้ามเปิดหรือใช้งานโปรแกรมประเภท Peer-to-Peer หรือ โปรแกรมที่มีความเสี่ยง เว้นแต่จะได้รับอนุญาตจากผู้บริหารระดับสูงหรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่

(๗) ผู้ใช้งานสามารถขอใช้งานซอฟท์แวร์ได้ตามหน้าที่หรือความจำเป็น เว้นแต่จะได้รับอนุญาตจากผู้บริหารระดับสูงหรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่ โดยผู้ดูแลระบบจะเป็นผู้ติดตั้งให้เท่านั้น

(๘) ห้ามผู้ใช้งานติดตั้ง หรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากตรวจพบ ถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานต้องรับผิดชอบแต่เพียงผู้เดียว

(๙) ซอฟท์แวร์ที่สำนักงานจัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็น ห้ามผู้ใช้งานติดตั้ง ถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่น

(๑๐) ห้ามใช้สินทรัพย์ที่เป็นของสำนักงาน เพื่อประโยชน์ทางการค้า

(๑๑) ห้ามสร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์ที่นำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์ แสดงข้อความรูปภาพที่ไม่เหมาะสม หรือขัดต่อศีลธรรมประเพณีอันดีงามของประเทศไทย

(๑๒) ห้ามผู้ใช้งานของสำนักงาน ควบคุมคอมพิวเตอร์ หรือระบบสารสนเทศของหน่วยงานภายนอกโดยไม่ได้รับอนุญาตจากผู้บริหารระดับสูงหรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่

ข้อ ๖๓ ให้ผู้ใช้งานแสดงตัวตนด้วยชื่อผู้ใช้งาน และ พิสูจน์ยืนยันตัวตน (User Identification and Authentication) ด้วยรหัสผ่าน เพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนทุกครั้ง

ข้อ ๖๔ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่กำหนดไว้ ให้จำกัดและควบคุมการใช้งานโปรแกรมอรรถประโยชน์ (Utility) สำหรับโปรแกรมคอมพิวเตอร์ที่สำคัญ เนื่องจากโปรแกรมอรรถประโยชน์บางชนิดสามารถช่วยผู้ใช้งานให้หลีกเลี่ยงมาตรการป้องกันทางด้านความมั่นคงปลอดภัยของระบบได้ ทั้งนี้ให้ดำเนินการ ดังนี้

(๑) เพื่อจำกัดและควบคุมการใช้งาน โปรแกรมอรรถประโยชน์ที่จะใช้งาน ต้องผ่านการรับรองให้ใช้จากผู้ดูแลระบบ และต้องมีความสามารถในการพิสูจน์ยืนยันตัวตนผู้ใช้งานในการเข้าใช้งานโปรแกรม

(๒) การใช้งานโปรแกรมอรรถประโยชน์ ต้องไม่เป็นการละเมิดลิขสิทธิ์

(๓) ต้องจัดเก็บชุดติดตั้งโปรแกรมอรรถประโยชน์ แยกจากชุดติดตั้งซอฟต์แวร์ระบบสารสนเทศ

(๔) ต้องจำกัดสิทธิผู้ที่ได้รับอนุญาตให้ใช้งานโปรแกรมอรรถประโยชน์

(๕) ต้องป้องกันมิให้ผู้ใช้งานสามารถเข้าถึงหรือใช้งานโปรแกรมอรรถประโยชน์ได้ และต้องถอดถอนการติดตั้งโปรแกรมอรรถประโยชน์ รวมทั้งซอฟต์แวร์ที่เกี่ยวข้องกับระบบสารสนเทศ เมื่อไม่จำเป็นต้องใช้งาน

ข้อ ๖๕ การกำหนดเวลาใช้งานระบบสารสนเทศ (Session time-out)

(๑) ระบบสารสนเทศต้องมีฟังก์ชั่นในการกำหนดระยะเวลาในการใช้งาน และตัดการใช้งาน รวมทั้งปิดการใช้งาน หลังจากที่ไม่มีกิจกรรมการใช้งานเป็นเวลา ๑๕ นาที

(๒) ฟังก์ชั่นของระบบสารสนเทศที่มีความเสี่ยงสูง ต้องกำหนดระยะเวลาในการใช้งาน และตัดการใช้งาน รวมทั้งปิดการใช้งาน หลังจากที่ไม่มีกิจกรรมการใช้งาน ต้องสั้นกว่าระยะเวลาปกติ

ข้อ ๖๖ การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of connection time)

(๑) ระบบสารสนเทศต้องจำกัดระยะเวลาการเชื่อมต่อสำหรับการใช้งาน เพื่อให้ผู้ใช้งานสามารถใช้งานได้นานที่สุดภายในช่วงเวลาที่สำนักงานกำหนดเท่านั้น

(๒) ระบบสารสนเทศที่มีความสำคัญสูง ที่ใช้งานในสถานที่ที่มีความเสี่ยง (ในที่สาธารณะหรือพื้นที่ภายนอกสำนักงาน) ต้องจำกัดช่วงเวลาการเชื่อมต่อ

ส่วนที่ ๗ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application and Information Access Control)

ข้อ ๖๗ ผู้ดูแลระบบ ต้องกำหนดวิธีการลงทะเบียนบุคลากรใหม่ของสำนักงาน (โดยปฏิบัติตามข้อ ๘) ในการใช้งานตามความจำเป็น รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน (โดยปฏิบัติตามข้อ ๑๐) เช่น การลาออกหรือพ้นจากตำแหน่ง การยกเลิกการใช้งาน หรือ การเปลี่ยนตำแหน่งงานภายในสำนักงาน เป็นต้น

ข้อ ๖๘ ผู้ดูแลระบบ ต้องกำหนดสิทธิการใช้งานระบบสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-Mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่ และต้องได้รับความเห็นชอบจากผู้บริหารระดับสูงหรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่ เป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

ข้อ ๖๙ ผู้ดูแลระบบ ต้องกำหนดระยะเวลาในการเชื่อมต่อระบบสารสนเทศที่ใช้ในการปฏิบัติงานต่าง ๆ เมื่อผู้ใช้งานไม่ใช้งานระบบสารสนเทศเป็นเวลา ๑๕ นาที ระบบจะต้องตัดการใช้งาน โดยผู้ใช้งานต้องลงบันทึกเข้าใช้งาน (Login) อีกครั้งก่อนใช้งานต่อ

ข้อ ๗๐ ผู้ดูแลระบบ ต้องบริหารจัดการสิทธิการใช้งานระบบและรหัสผ่าน (Password) ของผู้ใช้งาน ดังต่อไปนี้

(๑) ต้องเปลี่ยนแปลงหรือยกเลิกรหัสผ่าน เมื่อผู้ใช้งาน ลาออก หรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน

(๒) ผู้ใช้งานต้องไม่บันทึกหรือเก็บรหัสผ่านไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึงโดยบุคคลอื่น นอกจากตนเอง

(๓) กำหนดให้ชื่อบัญชีผู้ใช้งานต้องไม่ซ้ำกัน

(๔) การให้สิทธิสูงสุดเฉพาะกาลกับผู้ใช้งานคนใดก็ตาม จะต้องได้รับความเห็นชอบและอนุมัติจากผู้บริหารระดับสูงหรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่ โดยต้องกำหนดระยะเวลาการใช้งานและระงับการใช้งานในทันทีเมื่อพ้นระยะเวลาดังกล่าว หรือเมื่อบุคคลนั้น พ้นจากตำแหน่ง โดยให้กำหนดว่า ผู้ใช้งานนั้น สามารถเข้าถึงระดับใดได้ และ ต้องกำหนดกลุ่มบัญชีผู้ใช้งานต่างจากผู้ใช้งานตามปกติ

ข้อ ๗๑ ผู้ดูแลระบบ ต้องบริหารจัดการการเข้าถึงข้อมูลตามชั้นความลับในการควบคุมการเข้าถึงข้อมูลแต่ละประเภท ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบสารสนเทศ รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทตามชั้นความลับ ดังต่อไปนี้

(๑) ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทตามชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบสารสนเทศ

(๒) ต้องกำหนดรายชื่อบัญชีผู้ใช้งาน (User Account) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้งานข้อมูล ในแต่ละชั้นความลับของข้อมูล

(๓) กำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

(๔) การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรเข้ารหัส (Encryption) ตามมาตรฐานสากล เช่น SSL, VPN หรือ XML Encryption เป็นต้น

(๕) กำหนดการเปลี่ยนรหัสผ่าน (Password) ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

(๖) กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล ในกรณีที่นำสินทรัพย์ออกนอกหน่วยงาน เช่น บำรุงรักษา ตรวจซ่อม โดยให้สำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

ข้อ ๗๒ ระบบที่ไวต่อการรบกวน (Sensitive System) มีผลกระทบและมีความสำคัญสูง ให้ปฏิบัติดังนี้

(๑) แยกระบบที่ไวต่อการรบกวนออกจากระบบอื่น ๆ

(๒) ควบคุมสภาพแวดล้อมของระบบ โดยมีห้องปฏิบัติงานแยกเป็นสัดส่วน

(๓) กำหนดสิทธิการใช้ระบบ ให้เป็นการเฉพาะกับผู้ใช้งานที่เกี่ยวข้องเท่านั้น

ข้อ ๗๓ การใช้งานอุปกรณ์พกพา (Mobile Device) ต้องปฏิบัติดังต่อไปนี้

(๑) ตรวจสอบความพร้อมของอุปกรณ์ที่จะนำไปใช้งานว่าอยู่ในสภาพพร้อมใช้งานหรือไม่ และตรวจสอบโปรแกรมมาตรฐานว่า ถูกต้องตามลิขสิทธิ์

(๒) ระมัดระวังไม่ให้บุคคลภายนอกคัดลอกข้อมูลจากอุปกรณ์พกพาที่นำไปใช้ได้ เว้นแต่ข้อมูลที่ได้มีการเผยแพร่เป็นการทั่วไป

(๓) เมื่อหมดความจำเป็นต้องใช้อุปกรณ์พกพาแล้ว ให้นำส่งคืนเจ้าหน้าที่ผู้รับผิดชอบในทันที

(๔) เจ้าหน้าที่ผู้รับผิดชอบในการรับคืนต้องตรวจสอบสภาพความพร้อมใช้งานของอุปกรณ์พกพาที่รับคืนด้วย

(๕) หากปรากฏว่าความเสียหายที่เกิดขึ้นนั้น เกิดจากความประมาทอย่างร้ายแรงของผู้นำไปใช้ ผู้นำไปใช้ต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

ส่วนที่ ๘ การบริหารจัดการซอฟต์แวร์และลิขสิทธิ์ และการป้องกันโปรแกรมไม่ประสงค์ดี (Software Licensing and intellectual property and Preventing Malware)

ข้อ ๗๔ ซอฟต์แวร์ที่สำนักงานอนุญาตให้ใช้งาน หรือที่สำนักงานมีลิขสิทธิ์ ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่และความจำเป็น โดยห้ามผู้ใช้งานติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากตรวจพบ ถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานต้องรับผิดชอบแต่เพียงผู้เดียว

ข้อ ๗๕ ซอฟท์แวร์ที่สำนักงานจัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็น ห้ามผู้ใช้งานติดตั้ง ถอดถอนเปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่น ยกเว้นได้รับการอนุญาตจากผู้บริหารระดับสูงหรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่ หรือผู้ที่มีสิทธิในลิขสิทธิ์

ข้อ ๗๖ คอมพิวเตอร์ของผู้ใช้งานต้องติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ (Anti virus) ตามที่สำนักงานประกาศให้ใช้ เว้นแต่คอมพิวเตอร์นั้นเป็นเครื่องที่ใช้เพื่อการศึกษาหรือทดสอบที่ได้รับอนุญาตจากผู้บริหารระดับสูงหรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่

ข้อ ๗๗ ต้องตรวจสอบข้อมูล แฟ้มข้อมูล ซอฟต์แวร์ หรือสิ่งอื่นใด ที่ได้รับจากผู้ใช้งานอื่น เพื่อตรวจจับไวรัสคอมพิวเตอร์และโปรแกรมไม่ประสงค์ดี ก่อนนำมาใช้งานหรือเก็บบันทึกทุกครั้ง

ข้อ ๗๘ ผู้ใช้งานต้องปรับปรุงข้อมูล สำหรับตรวจสอบและปรับปรุงระบบปฏิบัติการ (Update patch) ให้ใหม่เสมอ เพื่อป้องกันความเสียหายที่อาจเกิดขึ้น

ข้อ ๗๙ ผู้ใช้งานต้องระวังไวรัสและโปรแกรมไม่ประสงค์ดีตลอดเวลา รวมทั้งเมื่อพบสิ่งผิดปกติ ผู้ใช้งานจะต้องแจ้งเหตุแก่ผู้ดูแลระบบ

ข้อ ๘๐ เมื่อผู้ใช้งานพบว่าเครื่องคอมพิวเตอร์ติดไวรัส ผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์เข้าสู่ระบบเครือข่าย และต้องแจ้งแก่ผู้ดูแลระบบ

ข้อ ๘๑ ห้ามลักลอบทำสำเนา เปลี่ยนแปลง ลบทิ้ง ซึ่งข้อมูล ข้อความ เอกสาร หรือสิ่งใดๆ ที่เป็นสินทรัพย์ของสำนักงาน หรือของผู้อื่น โดยไม่ได้รับอนุญาตจากผู้บริหารระดับสูงหรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่

ข้อ ๘๒ ห้ามเผยแพร่ไวรัสคอมพิวเตอร์ โปรแกรมไม่ประสงค์ดี หรือโปรแกรมอันตรายใด ๆ ที่อาจก่อให้เกิดความเสียหายต่อสินทรัพย์ของสำนักงาน แต่การพัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ อาจกระทำได้โดยห้ามดำเนินการดังนี้

(๑) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ที่จะทำลายกลไกรักษาความปลอดภัยของระบบคอมพิวเตอร์ ระบบเครือข่ายและระบบสารสนเทศ รวมทั้งการกระทำในลักษณะที่เป็นการแอบใช้รหัสผ่าน การลักลอบทำสำเนาข้อมูลของบุคคลอื่น หรือแกะรหัสผ่านของบุคคลอื่น

(๒) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ซึ่งทำให้ผู้ใช้งานมีสิทธิและลำดับความสำคัญในการครอบครองทรัพยากรระบบมากกว่าผู้ใช้งานอื่น

(๓) พัฒนาโปรแกรมใด ๆ ที่จะทำซ้ำตัวโปรแกรม หรือแฝงตัวโปรแกรมไปกับโปรแกรมอื่นในลักษณะเช่นเดียวกับหนอนหรือไวรัสคอมพิวเตอร์

(๔) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ที่จะทำลายระบบจำกัดสิทธิการใช้ (License) ซอฟต์แวร์

(๕) สร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์ที่นำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์ แสดงข้อความรูปภาพที่ไม่เหมาะสม หรือขัดต่อศีลธรรมประเพณีอันดีงามของประเทศไทย

ข้อ ๘๓ การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก (Outsourced software development)

(๑) จัดให้มีกระบวนการควบคุมโครงการพัฒนาซอฟต์แวร์ที่จัดจ้างผู้รับจ้างพัฒนาภายนอก

(๒) สำนักงานถือสิทธิในทรัพย์สินทางปัญญาสำหรับซอร์สโค้ดของซอฟต์แวร์ที่ได้รับการพัฒนาโดยผู้รับจ้างพัฒนาภายนอก

(๓) กำหนดการสงวนสิทธิ์ที่จะตรวจสอบคุณภาพและความถูกต้องของซอฟต์แวร์ที่จะพัฒนา โดยให้ระบุไว้ในสัญญาจ้างที่จะทำกับผู้รับจ้างพัฒนาภายนอกนั้น

(๔) ให้ตรวจสอบโปรแกรมไม่ประสงค์ดี ในซอฟต์แวร์ต่าง ๆ ที่จะติดตั้งก่อนติดตั้งทุกครั้ง

(๕) หลังจากติดตั้งระบบเพื่อใช้งาน ต้องยกเลิกบัญชีผู้ใช้งาน หรือเปลี่ยนรหัสผ่านของผู้ใช้งานทุกรายที่ถูกกำหนดเอาไว้เป็นค่าเริ่มต้นที่มาพร้อมกับระบบ ในทันที

ส่วนที่ ๙ การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)

ข้อ ๘๔ ต้องตรวจสอบว่าอุปกรณ์ซึ่งเป็นของส่วนตัว ที่จะใช้เข้าถึงระบบสารสนเทศของสำนักงานจากระยะไกล ได้รับการติดตั้งโปรแกรมป้องกันไวรัสและการใช้งานไฟร์วอลล์ตามที่สำนักงานกำหนด

ข้อ ๘๕ ต้องจัดเตรียมอุปกรณ์สำหรับการปฏิบัติงานจากระยะไกล การจัดเก็บข้อมูล และอุปกรณ์พกพาไว้ให้ผู้ใช้งานจากระยะไกล

ข้อ ๘๖ ผู้ใช้งานจากระยะไกล ต้องพิสูจน์ตัวตนก่อนเข้าใช้งานเพื่อเพิ่มความปลอดภัย เช่น รหัสผ่าน หรือวิธีการเข้ารหัส เป็นต้น

ข้อ ๘๗ ไม่อนุญาตให้ใช้งานอุปกรณ์ซึ่งเป็นของส่วนตัวที่ไม่อยู่ภายใต้การควบคุมตามนโยบายความมั่นคงปลอดภัยของสำนักงานในการเข้าถึงระบบสารสนเทศของหน่วยงานจากระยะไกล

ข้อ ๘๘ ต้องกำหนดชนิดของงาน ชั่วโมงการทำงาน ชั้นความลับของข้อมูล ระบบงานและบริการต่าง ๆ ของสำนักงาน ที่อนุญาตหรือไม่อนุญาตให้ปฏิบัติงานจากระยะไกล

ข้อ ๘๙ ต้องกำหนดขั้นตอนปฏิบัติสำหรับการขออนุมัติ การขอยกเลิก การกำหนดหรือปรับปรุงสิทธิในการเข้าถึงระบบสารสนเทศ และการคืนอุปกรณ์ที่ใช้ปฏิบัติงานจากระยะไกล

ส่วนที่ ๑๐ การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

ข้อ ๙๐ ผู้ดูแลระบบ ต้องออกแบบควบคุมอุปกรณ์เครือข่ายแบบไร้สาย (Access Point) ให้กระจายสัญญาณออกนอกพื้นที่ใช้งานให้น้อยที่สุด

ข้อ ๙๑ ทันทีที่นำอุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point) มาใช้งาน ผู้ดูแลระบบ ต้องเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าเริ่มต้น (Default) จากผู้ผลิต และให้ซ่อนค่าดังกล่าวด้วย

ข้อ ๙๒ ผู้ดูแลระบบ ต้องกำหนดรูปแบบ Wireless Security ให้เป็น WPA/WPA๒ (Wi-Fi Protected Access) ในการเข้ารหัสข้อมูลระหว่างเครื่องลูกข่าย (Wireless LAN Client) และอุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point) โดยไม่ให้แสดงชื่อระบบเครือข่ายไร้สาย

ข้อ ๙๓ ผู้ดูแลระบบ ต้องควบคุมการเข้าถึงระบบเครือข่ายไร้สาย โดยอนุญาตเฉพาะอุปกรณ์ที่มี MAC Address (Media Access Control Address) และบัญชีผู้ใช้งาน (User Account) ของผู้ใช้งานที่มีสิทธิในการเข้าใช้งานระบบเครือข่ายไร้สาย ตามที่กำหนดไว้เท่านั้น

ข้อ ๙๔ ผู้ดูแลระบบ ต้องติดตั้งไฟร์วอลล์ (Firewall) ระหว่างระบบเครือข่ายไร้สายกับระบบเครือข่ายภายในของสำนักงาน

ข้อ ๙๕ ผู้ดูแลระบบ ควรกำหนดให้ผู้ใช้งานในระบบเครือข่ายไร้สาย ติดต่อสื่อสารกับเครือข่ายภายในสำนักงานผ่านทาง VPN (Virtual Private Network) เพื่อช่วยป้องกันการบุกรุกในระบบเครือข่ายไร้สาย

ข้อ ๙๖ ผู้ดูแลระบบ ต้องลงทะเบียนอุปกรณ์ทุกตัวที่ใช้เข้าถึงระบบเครือข่ายไร้สาย

ข้อ ๙๗ ผู้ดูแลระบบ ต้องใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สาย เพื่อตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยที่เกิดขึ้นในระบบเครือข่ายไร้สาย และส่งรายงานผลการตรวจสอบทุก ๓ เดือน และในกรณีที่ตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติ ให้ผู้ดูแลระบบรายงานต่อผู้บริหารระดับสูงหรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่ ทราบทันที

ข้อ ๙๘ ผู้ดูแลระบบ ต้องควบคุมดูแลไม่ให้บุคคลหรือหน่วยงานภายนอกที่ไม่ได้รับอนุญาต ใช้งานระบบเครือข่ายไร้สายในการเข้าสู่ระบบเครือข่ายและระบบสารสนเทศของสำนักงาน

ข้อ ๙๙ ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของสำนักงาน จะต้องลงทะเบียนกับผู้ดูแลระบบ และต้องได้รับอนุญาตจากผู้บริหารระดับสูงหรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่ เป็นลายลักษณ์อักษร

ข้อ ๑๐๐ ผู้ดูแลระบบ ต้องกำหนดสิทธิผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงาน รวมทั้ง ทบทวนสิทธิในการเข้าถึงอย่างสม่ำเสมอ

ส่วนที่ ๑๑ การควบคุมการใช้งานอุปกรณ์ป้องกันเครือข่าย (Firewall Control)

ข้อ ๑๐๑ ผู้ดูแลระบบมีหน้าที่ในการบริหารจัดการ การติดตั้งและกำหนดค่าของอุปกรณ์ป้องกันเครือข่ายทั้งหมด

ข้อ ๑๐๒ ต้องกำหนดค่าเริ่มต้นของอุปกรณ์ป้องกันเครือข่าย (Firewall) ให้เป็นปฏิเสธทั้งหมด (Deny)

ข้อ ๑๐๓ บริการ (Services) และเส้นทางเชื่อมต่ออินเทอร์เน็ตที่ไม่อนุญาตตามนโยบายความมั่นคงปลอดภัยของสำนักงาน จะต้องถูกบล็อก (Block) โดย Firewall

ข้อ ๑๐๔ ผู้ใช้งานอินเทอร์เน็ตจะต้องพิสูจน์ตัวตน (Authentication) ก่อนการใช้งานทุกครั้ง

ข้อ ๑๐๕ จะต้องบันทึกการเปลี่ยนแปลงค่าบริการและการเชื่อมต่อที่อนุญาต ทุกครั้งที่เปลี่ยนแปลงค่าต่าง ๆ ของอุปกรณ์ป้องกันเครือข่าย เช่น ค่า Parameter เป็นต้น

ข้อ ๑๐๖ ให้เฉพาะผู้ได้รับมอบหมายให้ดูแลจัดการเท่านั้น ที่สามารถเข้าถึงตัวอุปกรณ์ป้องกันเครือข่าย

ข้อ ๑๐๗ จะต้องส่งข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์ป้องกันเครือข่าย ไปจัดเก็บที่อุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ โดยจัดเก็บข้อมูลจราจรไม่น้อยกว่า ๙๐ วัน

ข้อ ๑๐๘ การให้บริการอินเทอร์เน็ตกับเครื่องคอมพิวเตอร์ลูกข่าย จะเปิดพอร์ตการเชื่อมต่อพื้นฐานของโปรแกรมทั่วไปที่อนุญาตให้ใช้งาน หากผู้ใช้งานมีความจำเป็นที่จะใช้งานพอร์ตการเชื่อมต่อที่นอกเหนือไปจากที่กำหนด จะต้องได้รับอนุญาตจากผู้บริหารระดับสูงหรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่

ข้อ ๑๐๙ จะต้องกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายเฉพาะพอร์ตการเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น โดยข้อกำหนดตามนโยบายการป้องกันเครือข่าย (Policy) จะต้องถูกระบุให้กับเครื่องคอมพิวเตอร์แม่ข่ายแต่ละเครื่องที่ให้บริการจริง

ข้อ ๑๑๐ จะต้องสำรองข้อมูลค่าต่าง ๆ ที่กำหนดของอุปกรณ์ป้องกันเครือข่าย เป็นประจำทุกสัปดาห์หรือทุกครั้งก่อนที่จะเปลี่ยนแปลง

ข้อ ๑๑๑ เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบสารสนเทศของสำนักงาน ที่มีลักษณะที่เป็นอินทราเน็ต จะไม่อนุญาตให้เชื่อมต่อเพื่อใช้งานผ่านอินเทอร์เน็ต เว้นแต่มีความจำเป็น โดยจะต้องกำหนดเป็นกรณีไป

ข้อ ๑๑๒ สำนักงานมีสิทธิที่จะระงับหรือบล็อกการใช้งานของเครื่องคอมพิวเตอร์ลูกข่ายที่มีพฤติกรรมการใช้งานที่ผิดนโยบายการป้องกันเครือข่าย หรือเกิดจากการทำงานของโปรแกรมที่มีความเสี่ยงต่อความปลอดภัยจนกว่าจะได้รับการแก้ไข

ข้อ ๑๑๓ จะต้องบันทึกรายการของการเชื่อมต่อในลักษณะของการควบคุมระยะไกล (Remote Login) จากภายนอกมายังเครื่องแม่ข่ายหรืออุปกรณ์เครือข่ายภายใน ตามแบบการขออนุญาตดำเนินการเกี่ยวกับเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย และต้องได้รับอนุญาตจากผู้บริหารระดับสูงหรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่ ก่อน

ข้อ ๑๑๔ ผู้ละเมิดนโยบายด้านความปลอดภัยของอุปกรณ์ป้องกันเครือข่าย จะถูกระงับการใช้งานอินเทอร์เน็ตทันที

ส่วนที่ ๑๒ การควบคุมการใช้จดหมายอิเล็กทรอนิกส์ (E-Mail)

ข้อ ๑๑๕ การขอใช้งานจดหมายอิเล็กทรอนิกส์ (E-Mail) ผู้ขอใช้งานจะต้องลงทะเบียน โดยยื่นคำขอกับผู้ดูแลระบบ โดยได้รับความเห็นชอบจากผู้บริหาร

ข้อ ๑๑๖ ให้เปลี่ยนรหัสผ่านในทันที เมื่อได้รับรหัสผ่าน (Password) ในการเข้าระบบจดหมายอิเล็กทรอนิกส์ (E-Mail) ครั้งแรก

ข้อ ๑๑๗ ไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์

ข้อ ๑๑๘ เปลี่ยนรหัสผ่าน (Password) ทุก ๓-๖ เดือน

ข้อ ๑๑๙ ไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-Mail Address) ของผู้อื่น เพื่ออ่าน หรือรับ หรือส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของจดหมายอิเล็กทรอนิกส์ และให้ถือว่า เจ้าของจดหมายอิเล็กทรอนิกส์ เป็นผู้รับผิดชอบต่อการใช้งานในจดหมายอิเล็กทรอนิกส์ นั้น

ข้อ ๑๒๐ หลังจากเสร็จสิ้นการใช้งานระบบจดหมายอิเล็กทรอนิกส์ ผู้ใช้งานต้องลงบันทึกออก (Logout) จากระบบทุกครั้ง

ข้อ ๑๒๑ การส่งข้อมูลที่เป็นความลับ ไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์ เว้นเสียแต่ว่าจะใช้วิธีการเข้ารหัสข้อมูลที่สำนักงานกำหนดไว้ และให้ใช้ความระมัดระวังในการระบุชื่อที่อยู่จดหมายอิเล็กทรอนิกส์ของผู้รับให้ถูกต้อง เพื่อป้องกันการส่งผิด

ข้อ ๑๒๒ ห้ามส่งจดหมายอิเล็กทรอนิกส์ที่มีลักษณะเป็นจดหมายขยะ (Spam Mail)

ข้อ ๑๒๓. ห้ามส่งจดหมายอิเล็กทรอนิกส์ที่มีลักษณะเป็นจดหมายลูกโซ่ (Chain Letter)

ข้อ ๑๒๔ ห้ามส่งจดหมายอิเล็กทรอนิกส์ที่มีลักษณะเป็นการละเมิดต่อกฎหมาย หรือสิทธิของบุคคลอื่น

ข้อ ๑๒๕ ห้ามส่งจดหมายอิเล็กทรอนิกส์ที่มีไวรัสไปให้กับบุคคลอื่นโดยเจตนา

ข้อ ๑๒๖ ให้ระบุชื่อของผู้ส่งในจดหมายอิเล็กทรอนิกส์ทุกฉบับที่ส่งไป

ข้อ ๑๒๗ ให้สำรองข้อมูลจดหมายอิเล็กทรอนิกส์ตามความจำเป็นอย่างสม่ำเสมอ

ข้อ ๑๒๘ ผู้ใช้งานต้องตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนเปิดใช้งาน เพื่อตรวจสอบเอกสารแนบ เป็นการป้องกันในการเปิดเอกสารที่เป็นแฟ้มข้อมูลประเภทโปรแกรม (executable file) เช่น .exe .com เป็นต้น

ข้อ ๑๒๙ ผู้ใช้งานต้องไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

ข้อ ๑๓๐ ผู้ใช้งานต้องไม่ใช้ข้อความที่ไม่สุภาพ หรือรับส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสม หรือข้อมูลอันอาจทำให้เสียชื่อเสียงของสำนักงานหรือทำให้เกิดความแตกแยกระหว่างหน่วยงาน ผ่านทางจดหมายอิเล็กทรอนิกส์

ข้อ ๑๓๑ ผู้ใช้งานต้องตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ของตนเองทุกวัน และควรจัดเก็บแฟ้มข้อมูลและจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจำนวนน้อยที่สุด รวมทั้ง ควรลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้เนื้อที่ระบบจดหมายอิเล็กทรอนิกส์

ข้อ ๑๓๒ ผู้ใช้งาน ควรโอนย้ายจดหมายอิเล็กทรอนิกส์ที่จะใช้อ้างอิงภายหลังมายังเครื่องคอมพิวเตอร์ของตน เพื่อป้องกันมิให้ผู้อื่นแอบอ่านจดหมายอิเล็กทรอนิกส์ได้

ข้อ ๑๓๓ ผู้ใช้งานต้องใช้จดหมายอิเล็กทรอนิกส์ภาครัฐ สำหรับใช้รับ-ส่งข้อมูลในงานราชการตามมติคณะรัฐมนตรี เมื่อวันที่ ๑๘ ธันวาคม ๒๕๕๐ เรื่อง การพัฒนาระบบจดหมายอิเล็กทรอนิกส์กลางเพื่อการสื่อสารในภาครัฐ

ส่วนที่ ๑๓ การควบคุมการใช้อินเทอร์เน็ต (Internet)

ข้อ ๑๓๔ ผู้ดูแลระบบ ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์ เพื่อการเข้าใช้งานอินเทอร์เน็ต โดยให้เชื่อมต่อผ่านระบบรักษาความปลอดภัยที่สำนักงานกำหนดไว้เท่านั้น เช่น Proxy, Firewall, IPS-IDS เป็นต้น ห้ามผู้ใช้งานเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น เช่น Dial-up Modem เว้นแต่ว่ามีเหตุผลความจำเป็นและต้องได้รับอนุญาตจากผู้บริหารระดับสูงหรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่ เป็นลายลักษณ์อักษร

ข้อ ๑๓๕ เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพาที่จะเชื่อมต่ออินเทอร์เน็ตผ่านเว็บเบราเซอร์ (Web browser) ต้องติดตั้งโปรแกรมป้องกันไวรัส และอุดช่องโหว่ของระบบปฏิบัติการ

ข้อ ๑๓๖ ต้องตรวจจับไวรัส (Virus Scanning) โดยโปรแกรมป้องกันไวรัสก่อนรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเทอร์เน็ตทุกครั้ง

ข้อ ๑๓๗ ไม่ใช้ระบบอินเทอร์เน็ต (Internet) ของสำนักงาน เพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนตัว และเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือน หรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคมหรือละเมิดสิทธิของผู้อื่น หรือข้อมูลที่อาจก่อให้เกิดความเสียหายให้กับสำนักงาน

ข้อ ๑๓๘ ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของสำนักงานที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต (Internet)

ข้อ ๑๓๙ ให้ระมัดระวังการดาวน์โหลดโปรแกรมใช้งาน จากระบบอินเทอร์เน็ต (Internet) และการปรับปรุงโปรแกรมต่าง ๆ ให้เป็นปัจจุบัน (Update) ต้องไม่ละเมิดลิขสิทธิ์

ข้อ ๑๔๐ ต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของหน่วยงาน ผ่านกระดานสนทนาอิเล็กทรอนิกส์ (Webboard) หรือ เครือข่ายสังคมออนไลน์ (Social Media)

ข้อ ๑๔๑ ไม่เสนอความคิดเห็น หรือใช้ข้อความที่ยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของสำนักงาน หรือทำลายความสัมพันธ์กับบุคลากรของหน่วยงานภายนอก ผ่านกระดานสนทนาอิเล็กทรอนิกส์ (Webboard) หรือ เครือข่ายสังคมออนไลน์ (Social Media)

ข้อ ๑๔๒ ผู้ใช้งานต้องไม่นำเข้าข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามก รวมทั้งต้องไม่เผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเทอร์เน็ต

ข้อ ๑๔๓ ให้ออกจากระบบอินเทอร์เน็ต (Internet) และปิดเว็บเบราเซอร์ หลังจากใช้งานอินเทอร์เน็ตเสร็จแล้ว เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น

ข้อ ๑๔๔ ผู้ใช้งานต้องปฏิบัติตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์อย่างเคร่งครัด

ส่วนที่ ๑๔ การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล

ข้อ ๑๔๕ แนวทางปฏิบัติการใช้งานทั่วไป

(๑) เครื่องคอมพิวเตอร์ที่สำนักงานอนุญาตให้ใช้งาน เป็นสินทรัพย์ของสำนักงานเพื่อใช้ในงานราชการ

(๒) โปรแกรมที่จะติดตั้งลงบนเครื่องคอมพิวเตอร์ของสำนักงาน ต้องเป็นโปรแกรมที่สำนักงานซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้น ห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

(๓) ไม่อนุญาตให้ผู้ใช้งานติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ส่วนบุคคลของสำนักงาน

(๔) การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ส่วนบุคคล ไปตรวจซ่อมจะต้องกระทำโดยเจ้าหน้าที่ของหน่วยงาน หรือผู้รับจ้างเหมาบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้ทำสัญญากับสำนักงาน เท่านั้น

(๕) ต้องตรวจสอบหาไวรัสโดยโปรแกรมป้องกันไวรัส ก่อนใช้งานสื่อบันทึกพกพาต่าง ๆ

(๖) ผู้ใช้งาน มีหน้าที่รับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์ที่ตนเองได้รับมอบให้ใช้งาน

(๗) ปิดเครื่องคอมพิวเตอร์ส่วนบุคคลที่ตนเองครอบครองใช้งานอยู่ เมื่อเสร็จสิ้นการใช้งานประจำวัน หรือเมื่อมีการยุติการใช้งานเกินกว่า ๑ ชั่วโมง

(๘) ตั้งค่าพักหน้าจอ (Screen Saver) ของเครื่องคอมพิวเตอร์ที่ตนเองรับผิดชอบ ให้ล็อกหน้าจอหลังจากที่ไม่ได้ใช้งานเกินกว่า ๑๕ นาที เพื่อป้องกันบุคคลอื่นมาใช้งานที่เครื่องคอมพิวเตอร์

(๙) ห้ามนำเครื่องคอมพิวเตอร์ที่เป็นทรัพย์สินส่วนตัว มาใช้กับระบบเครือข่ายของหน่วยงาน ยกเว้นจะได้รับการตรวจสอบจากผู้ดูแลระบบของสำนักงานก่อนใช้งาน

ข้อ ๑๔๖ ให้ผู้ใช้งานปฏิบัติตามแนวทางการบริหารจัดการรหัสผ่านที่ระบุไว้ใน เอกสาร “การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน”

ข้อ ๑๔๗ การป้องกันจากโปรแกรมไม่ประสงค์ดี (Malware)

(๑) ต้องตรวจสอบหาไวรัสบนสื่อต่าง ๆ เช่น Flash Drive และ Data Storage อื่น ๆ ก่อนใช้งานกับเครื่องคอมพิวเตอร์

(๒) ผู้ใช้งานต้องตรวจสอบเอกสารที่แนบมากับจดหมายอิเล็กทรอนิกส์ หรือแฟ้มข้อมูลที่ดาวน์โหลดมาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัส ก่อนใช้งาน

(๓) ผู้ใช้งานต้องตรวจจับชุดคำสั่งไม่ประสงค์ดีบนแฟ้มข้อมูลคอมพิวเตอร์ที่จะสร้างความเสียหาย ทำลาย หรือแก้ไขเปลี่ยนแปลงข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นจนกระทั่งไม่สามารถใช้ปฏิบัติงานได้ตรงตามคำสั่งที่กำหนดไว้

ข้อ ๑๔๘ การสำรองข้อมูลและการกู้คืน

(๑) ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ส่วนบุคคลที่ได้รับมอบ ไว้บนสื่อบันทึกต่าง ๆ เช่น CD, DVD, External Hard Disk เป็นต้น

(๒) ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล และทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

(๓) ผู้ใช้งานต้องประเมินความเสี่ยงของข้อมูลที่เก็บไว้บนฮาร์ดดิสก์ (Hard Disk) เพื่อมิให้เกิดความเสียหายต่อการดำเนินงานของหน่วยงาน

(๔) แผ่นสื่อสำรองข้อมูลที่ไม่ใช้งานแล้ว ต้องทำลายไม่ให้สามารถนำไปใช้งานได้อีก

ส่วนที่ ๑๕ การใช้งานเครื่องคอมพิวเตอร์แบบพกพา

ข้อ ๑๔๙ แนวทางปฏิบัติการใช้งานทั่วไป

(๑) เครื่องคอมพิวเตอร์แบบพกพาที่สำนักงานอนุญาตให้ใช้งาน เป็นสินทรัพย์ของสำนักงานเพื่อใช้ในงานราชการ

(๒) โปรแกรมที่จะติดตั้งลงบนเครื่องคอมพิวเตอร์แบบพกพาของสำนักงาน ต้องเป็นโปรแกรมที่สำนักงานซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้น ห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

(๓) ผู้ใช้งานต้องศึกษาและปฏิบัติตามคู่มือการใช้งานอย่างละเอียด เพื่อให้ใช้งานได้อย่างปลอดภัยและมีประสิทธิภาพ

(๔) ไม่ดัดแปลงแก้ไขส่วนประกอบต่าง ๆ ของคอมพิวเตอร์แบบพกพา และรักษาให้มีสภาพเดิม

(๕) ควรนำคอมพิวเตอร์แบบพกพาใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพาขณะเคลื่อนย้าย เพื่อป้องกันอันตรายจากการกระทบกระเทือน เช่น การตกจากโต๊ะทำงาน หรือหลุดมือ เป็นต้น

(๖) หลีกเลี่ยงการใช้นิ้วหรือของแข็ง เช่น ปลายปากกา กดสัมผัสจอภาพแบบ LCD จนเกิดเป็นรอยขีดข่วนหรือแตกเสียหาย

(๗) ไม่วางของทับบนจอภาพและแป้นพิมพ์

(๘) ให้เช็ดทำความสะอาดจอภาพอย่างเบามือที่สุด และต้องเช็ดไปในแนวทางเดียวกันห้ามเช็ดแบบหมุนวน เพราะจะสร้างรอยขีดข่วนบนจอภาพ

(๙) ต้องปิดเครื่องคอมพิวเตอร์แบบพกพาสักระยะหนึ่ง เมื่อใช้งานเป็นระยะเวลานาน ๆ ในสภาพที่มีอากาศร้อนจัด เพื่อพักเครื่องก่อนเปิดใช้งานใหม่อีกครั้ง

(๑๐)ให้ยกเครื่องคอมพิวเตอร์แบบพกพาจากฐานบริเวณใต้แป้นพิมพ์เมื่อจะเคลื่อนย้ายเครื่องขณะที่เปิดใช้งานอยู่ ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น

ข้อ ๑๕๐ ความปลอดภัยทางด้านกายภาพ

(๑) ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันเครื่องคอมพิวเตอร์สูญหาย เช่น ควรล็อคเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

(๒) ผู้ใช้งานไม่เก็บหรือใช้งานคอมพิวเตอร์แบบพกพาในสถานที่ที่มีความร้อน/ความชื้น/ฝุ่นละอองสูง และต้องระวังป้องกันการตกกระทบ

ข้อ ๑๕๑ การควบคุมการเข้าถึงระบบปฏิบัติการ

(๑) ผู้ใช้งานต้องกำหนดบัญชีผู้ใช้งาน (User Account) ในการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์แบบพกพา

(๒) ผู้ใช้งานต้องกำหนดรหัสผ่านให้มีคุณภาพดี อย่างน้อยตามที่ระบุไว้ในเอกสาร “การบริหารจัดการสิทธิการใช้งานระบบและรหัสผ่าน”

(๓) ผู้ใช้งานต้องตั้งค่าการใช้งานโปรแกรมพักหน้าจอ (Screen saver) เพื่อล็อกหน้าจอภาพเมื่อไม่ได้ใช้งานเป็นเวลา ๑๕ นาที ซึ่งผู้ใช้งานต้องใส่รหัสผ่าน (Password) เพื่อเข้าใช้งานต่อ

(๔) ผู้ใช้งานต้องออกจากระบบ (Logout) ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

ข้อ ๑๕๒ ผู้ใช้งานต้องปฏิบัติตามแนวทางการบริหารจัดการรหัสผ่านที่ระบุไว้ในเอกสาร “การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน”

ข้อ ๑๕๓ การสำรองข้อมูลและการกู้คืน

(๑) ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์แบบพกพาที่ได้รับมอบ ไว้บนสื่อบันทึกต่าง ๆ เช่น CD, DVD, External Hard Disk เป็นต้น

(๒) ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล และทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

(๓) ผู้ใช้งานต้องประเมินความเสี่ยงของข้อมูลที่เก็บไว้บนฮาร์ดดิสก์ (Hard Disk) เพื่อมิให้เกิดความเสียหายต่อการดำเนินงานของหน่วยงาน

(๔) แผ่นสื่อสำรองข้อมูลที่ไม่ใช้งานแล้ว ต้องทำลายไม่ให้สามารถนำไปใช้งานได้อีก

ส่วนที่ ๑๖ การตรวจจับการบุกรุก (Intrusion Detection System/Intrusion Prevention System Policy: IDS/IPS)

ข้อ ๑๕๔ นโยบายตรวจจับการบุกรุก (IDS/IPS Policy) เป็นนโยบายการติดตั้งระบบตรวจสอบการบุกรุก และตรวจสอบความปลอดภัยของเครือข่าย เพื่อป้องกันสินทรัพย์ ระบบสารสนเทศ และข้อมูลบนเครือข่ายภายในของสำนักงาน ให้มีความมั่นคงปลอดภัย เป็นแนวทางการปฏิบัติเกี่ยวกับการตรวจสอบการบุกรุกเครือข่าย พร้อมกับบทบาทและความรับผิดชอบที่เกี่ยวข้อง

ข้อ ๑๕๕ นโยบายตรวจจับการบุกรุกครอบคลุมทุกโฮสต์ (Host) ในเครือข่ายของสำนักงานและระบบเครือข่ายทั้งหมด รวมถึงเส้นทางที่ไม่อยู่ในเครือข่ายอินเทอร์เน็ตที่ข้อมูลอาจเดินทาง ทุกเส้นทาง

ข้อ ๑๕๖ ระบบทั้งหมดที่สามารถเข้าถึงได้จากอินเทอร์เน็ตหรือที่สาธารณะ จะต้องผ่านการตรวจสอบจากระบบตรวจจับการบุกรุก

ข้อ ๑๕๗ ระบบทั้งหมดใน DMZ (Demilitarized zone) จะต้องได้รับการตรวจสอบรูปแบบการให้บริการก่อนติดตั้งและเปิดให้บริการ

ข้อ ๑๕๘ ต้องบันทึกผลการตรวจสอบโฮสต์ (Host) และระบบเครือข่ายทั้งหมดที่มีการส่งผ่านข้อมูลผ่านระบบตรวจจับการบุกรุก

ข้อ ๑๕๙ ต้องตรวจสอบและ Update Patch/Signature ของระบบตรวจจับการบุกรุกเป็นประจำ

ข้อ ๑๖๐ ผู้ดูแลระบบต้องตรวจสอบเหตุการณ์ ข้อมูลจราจร พฤติกรรมการใช้งาน กิจกรรม และบันทึกปริมาณข้อมูลเข้าใช้งานเครือข่ายเป็นประจำทุกวัน

ข้อ ๑๖๑ ระบบตรวจจับการบุกรุก จะทำงานภายใต้กฎควบคุมพื้นฐานของอุปกรณ์ป้องกันเครือข่าย ที่ใช้ในการเข้าถึงเครือข่ายของระบบสารสนเทศตามปกติ

ข้อ ๑๖๒ ต้องตรวจสอบข้อมูลเครื่องคอมพิวเตอร์แม่ข่ายที่ติดตั้งระบบตรวจจับการบุกรุก (host-based IDS) เป็นประจำทุก ๆ วัน

ข้อ ๑๖๓ จะต้องรายงานพฤติกรรมการใช้งาน กิจกรรม หรือเหตุการณ์ทั้งหมด ที่มีความเสี่ยงต่อการบุกรุก การโจมตีระบบ พฤติกรรมที่น่าสงสัย หรือการพยายามเข้าระบบ ทั้งที่ประสบความสำเร็จและไม่ประสบความสำเร็จ ให้ผู้บริหารระดับสูงหรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่ ทราบทันทีที่ตรวจพบ

ข้อ ๑๖๔ จะต้องรายงานพฤติกรรม กิจกรรมที่น่าสงสัย หรือระบบการทำงานที่ผิดปกติ ให้ผู้บริหารระดับสูงหรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่ ทราบภายใน ๑ ชั่วโมงหลังจากตรวจพบ

ข้อ ๑๖๕ ต้องเก็บบันทึกข้อมูลการตรวจสอบการบุกรุกทั้งหมดไว้ไม่น้อยกว่า ๙๐ วัน

ข้อ ๑๖๖ ระบบตรวจจับการบุกรุกต้องตอบสนองต่อเหตุการณ์ที่เกิดขึ้นในรูปแบบต่าง ๆ ได้แก่ รายงานผลการตรวจพบของเหตุการณ์ต่าง ๆ ดำเนินการตามขั้นตอนเพื่อลดความเสียหาย ลบซอฟต์แวร์ไม่ประสงค์ดีที่ตรวจพบ ป้องกันเหตุการณ์ที่อาจเกิดอีกในอนาคต และดำเนินการตามแผน

ข้อ ๑๖๗ สำนักงานมีสิทธิ์ในการยุติการเชื่อมต่อเครือข่ายของเครื่องคอมพิวเตอร์ที่มีพฤติกรรมเสี่ยงต่อการบุกรุกระบบ โดยไม่ต้องแจ้งแก่ผู้ใช้งานทราบล่วงหน้า

ข้อ ๑๖๘ ผู้ที่ถูกตรวจสอบว่า พยายามละเมิดนโยบายด้านความมั่นคงปลอดภัยของสำนักงาน พยายามเข้าถึงระบบโดยมิชอบ โจมตีระบบ หรือมีพฤติกรรมเสี่ยงต่อการทำงานของระบบสารสนเทศ จะถูกระงับการใช้เครือข่ายทันที และหากการกระทำดังกล่าว เป็นการกระทำความผิดตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ หรือเป็นการกระทำที่ส่งผลให้เกิดความเสียหายต่อข้อมูล และสินทรัพย์ของสำนักงาน จะต้องถูกดำเนินคดีตามขั้นตอนของกฎหมาย

ส่วนที่ ๑๗ การติดตั้งและกำหนดค่าของระบบ (System Installation and Configuration)

ข้อ ๑๖๙ ปรับปรุงระบบปฏิบัติการ (Operating System Update) ดังนี้

(๑) ตรวจสอบเครื่องแม่ข่าย และอุปกรณ์ระบบ

(๒) ติดตั้งระบบปฏิบัติการตรงตามความต้องการการใช้งาน

(๓) กำหนดชื่อและรหัสผ่าน ผู้ดูแลระบบ และชื่อผู้ใช้งาน (User)

(๔) กำหนดค่าติดตั้ง ชื่อเครื่อง (Computer Name)/IP Address

(๕) ปรับปรุง/กำหนดค่าระดับความปลอดภัยของระบบปฏิบัติการ (กรณีที่ระบบปฏิบัติการที่มี Service Patch Update)

(๖) ติดตั้งโปรแกรม Antivirus/ปรับปรุง Virus Definition และกำหนดค่าการตรวจสอบระบบการตรวจจับและปรับปรุงโปรแกรม

ข้อ ๑๗๐ บริหารบัญชีผู้ใช้งาน/สิทธิการเข้าถึงและการใช้งานระบบ (User Account Management) ดังนี้

(๑) กำหนดบัญชีผู้ดูแลระบบ (System Administrator Account)

(๒) กำหนดบัญชีผู้ใช้งาน (User Account)

(๓) บันทึกบัญชีผู้ใช้งานและสิทธิการเข้าใช้ระบบ

ข้อ ๑๗๑ ปรับปรุงการรักษาความปลอดภัย/Anti Virus (System Security & Antivirus Update) ดังนี้

(๑) ติดตาม เฝ้าระวัง การทำงานของคอมพิวเตอร์และการเข้าใช้ระบบปฏิบัติการ

(๒) ตรวจสอบการทำงาน (Performance) ของระบบปฏิบัติการ หรือตรวจสอบจากระบบรักษาความปลอดภัยที่ติดตั้ง

(๓) ปรับปรุง/กำหนดค่าระบบความปลอดภัย ให้เหมาะสมกับสภาพการใช้งาน

(๔) ปรับปรุงโปรแกรม Antivirus และ Definition ให้ทันสมัยเป็นประจำทุกสัปดาห์

(๕) ตรวจจับไวรัสคอมพิวเตอร์ (Scan) เป็นประจำ

ข้อ ๑๗๒ ติดตั้ง/ปรับปรุงระบบจัดการฐานข้อมูล (Database Management Operation) ดังนี้

(๑) ติดตั้งระบบจัดการฐานข้อมูล ตามความต้องการของระบบสารสนเทศ

(๒) กำหนดค่าระบบหรือโปรแกรมฐานข้อมูล ให้ทำงานร่วมกับระบบปฏิบัติการได้อย่างถูกต้อง และมีประสิทธิภาพ ตามข้อกำหนดของระบบฐานข้อมูล

(๓) สร้าง และกำหนดรายชื่อผู้บริหารระบบฐานข้อมูล (Database Admin) ชื่อผู้ใช้งานอื่นและสิทธิการใช้งาน

(๔) ปรับปรุง/กำหนดค่าระบบให้เหมาะสม หรือป้องกันการเกิดปัญหาเป็นประจำ

ข้อ ๑๗๓ ติดตั้งฐานข้อมูลโปรแกรมระบบสารสนเทศหรือกำหนดค่าระบบของโปรแกรม รวมทั้งกำหนดบัญชีผู้ใช้และสิทธิการเข้าใช้งานหรือเข้าถึงฐานข้อมูล

(๑) ติดตั้งโปรแกรมระบบสารสนเทศตามความต้องการ หรือรุ่นการพัฒนา

(๒) กำหนดค่าโปรแกรมหรือบริการ (services) ให้ทำงานร่วมกับระบบปฏิบัติการ ได้อย่างถูกต้องและมีประสิทธิภาพ

(๓) ติดตั้งฐานข้อมูลและเชื่อมต่อระบบสารสนเทศ และทดสอบการใช้งาน ตามกำหนด

(๔) แจ้งผู้ใช้งานให้ใช้งาน โดยแจ้งชื่อบัญชีผู้ใช้และสิทธิการเข้าใช้ระบบสารสนเทศตามที่กำหนดไว้

(๕) กำหนดเกณฑ์การสำรอง/สำเนา/ทดสอบกู้คืน (Restore Test)

(๖) บันทึกข้อกำหนด ค่าติดตั้ง และบัญชีผู้ใช้งานแต่ละระดับของระบบสารสนเทศทุกครั้งที่สร้างหรือปรับปรุง

ส่วนที่ ๑๘ การจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log)

ข้อ ๑๗๔ จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วน ถูกต้องแท้จริง ระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้ และข้อมูลที่ใช้ในการจัดเก็บ โดยให้กำหนดชั้นความลับในการเข้าถึงข้อมูลดังกล่าว และต้องเก็บบันทึกไว้อย่างน้อย ๙๐ วัน

ข้อ ๑๗๕ ห้ามแก้ไขข้อมูลจราจรคอมพิวเตอร์ (Log) ที่เก็บรักษาไว้

ข้อ ๑๗๖ กำหนดให้บันทึกการทำงานของระบบบันทึกการเข้าใช้งานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้า-ออกระบบ บันทึกการพยายามเข้าสู่ระบบ เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกไว้อย่างน้อย ๙๐ วัน นับตั้งแต่การใช้งานสิ้นสุดลง โดยปฏิบัติตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

ข้อ ๑๗๗ ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่าง ๆ และจำกัดสิทธิการเข้าถึงบันทึกเหล่านั้น ให้เฉพาะเจ้าหน้าที่ที่ได้รับมอบหมายเท่านั้น

หมวดที่ ๒
การรักษาความปลอดภัยฐานข้อมูลและสำรองข้อมูล

วัตถุประสงค์

๑. เพื่อให้ระบบสารสนเทศของสำนักงานสามารถให้บริการได้อย่างต่อเนื่อง

๒. เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติ และความรับผิดชอบของผู้ดูแลระบบในการปฏิบัติงานให้กับสำนักงานอย่างเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

๓. เพื่อให้ผู้ใช้งานรับรู้ เข้าใจ และสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

แนวปฏิบัติ

ส่วนที่ ๑ การรักษาความปลอดภัยฐานข้อมูล

ข้อ ๑ กำหนดสิทธิและความสำคัญของข้อมูลและฐานข้อมูล

(๑) จัดทำบัญชีฐานข้อมูล การจำแนกกลุ่มทรัพยากรของระบบสารสนเทศ หรือการทำงาน โดยให้กำหนดกลุ่มผู้ใช้งานและสิทธิของกลุ่มผู้ใช้งาน

(๒) กำหนดเกณฑ์การอนุญาตให้เข้าถึงระบบสารสนเทศ ที่เกี่ยวข้องกับการอนุญาตการกำหนดสิทธิหรือการมอบอำนาจ ดังนี้

(๒.๑) กำหนดสิทธิของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง เช่น

- อ่านข้อมูลอย่างเดียว
- สร้าง/บันทึกข้อมูล
- ลบข้อมูล
- แก้ไขข้อมูล
- ไม่มีสิทธิ

(๒.๒) กำหนดเกณฑ์การระงับสิทธิ มอบอำนาจ ให้เป็นไปตามการบริหารจัดการ การเข้าถึงของผู้ใช้งาน (user access management) ที่ได้กำหนดไว้

(๒.๓) ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของสำนักงานจะต้องขออนุญาตเป็นลายลักษณ์อักษร และได้รับการพิจารณาอนุญาตจากผู้บริหารระดับสูงหรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่แทน

(๓) ขั้นตอนปฏิบัติเพื่อการจัดเก็บข้อมูล

(๓.๑) จัดแบ่งประเภทของข้อมูล ออกเป็น

- ข้อมูลสารสนเทศด้านการบริหาร เช่น ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์ และ คำรับรอง ข้อมูลบุคลากร ข้อมูลงบประมาณการเงินและบัญชี เป็นต้น
- ข้อมูลสารสนเทศด้านผลิตภัณฑ์สุขภาพ เช่น ข้อมูลใบอนุญาตขาย ข้อมูลใบอนุญาตผลิต ข้อมูลใบอนุญาตนำเข้า เป็นต้น

(๓.๒) จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น ๓ ระดับ คือ

- ข้อมูลที่มีระดับความสำคัญมาก
- ข้อมูลที่มีระดับความสำคัญปานกลาง
- ข้อมูลที่มีระดับความสำคัญน้อย

(๓.๓) จัดแบ่งลำดับชั้นความลับของข้อมูล

- ข้อมูลลับที่สุด หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด
- ข้อมูลลับมาก หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรง
- ข้อมูลลับ หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย
- ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

(๓.๔) จัดแบ่งระดับชั้นการเข้าถึง

- ระดับชั้นสำหรับผู้บริหารระดับสูง
- ระดับชั้นสำหรับผู้บริหาร
- ระดับชั้นสำหรับผู้ใช้งานทั่วไป
- ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย

(๓.๕) การกำหนดช่วงเวลาที่เข้าถึงได้

(๓.๖) การกำหนดช่องทางที่สามารถเข้าถึงได้

ข้อ ๒ ข้อมูล ข่าวสารสารสนเทศทุกประเภทในฐานข้อมูลต้องได้รับการจัดระดับการการเข้าถึงหรือทำงาน รวมทั้งรายละเอียดอื่น ๆ ที่จำเป็นต่อมาตรการรักษาความปลอดภัย

ข้อ ๓ การปฏิบัติเกี่ยวกับข้อมูลที่เป็นความลับให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ และแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ หมวดที่ ๑ ข้อ ๑๒

ข้อ ๔ ผู้บริหารหรือผู้ได้รับมอบหมายให้ปฏิบัติหน้าที่ของหน่วยงานเป็นผู้พิจารณาคุณสมบัติของผู้ใช้งาน และโปรแกรมที่ใช้จัดการข้อมูลตามสิทธิของผู้ใช้งาน และมีหน้าที่รับผิดชอบในการจัดทำแฟ้มลงบันทึกการใช้งาน (Log File) สำหรับฐานข้อมูลตามความจำเป็น เพื่อประโยชน์ในการตรวจสอบความถูกต้องของการใช้งานฐานข้อมูล

ข้อ ๕ การใช้ฐานข้อมูลร่วมหรือแลกเปลี่ยนข้อมูลกับหน่วยงานภายนอก หรือหน่วยงานภายนอกขอใช้ข้อมูล ให้จัดทำบันทึกข้อตกลงการใช้หรือแลกเปลี่ยนข้อมูลสารสนเทศระหว่างสำนักงานกับหน่วยงานภายนอก ดังต่อไปนี้

(๑) กำหนดนโยบาย ขั้นตอนปฏิบัติ และ มาตรฐานเพื่อป้องกันข้อมูลและสื่อบันทึกข้อมูลที่จะจัดส่งระหว่างกัน

(๒) กำหนดหน้าที่ความรับผิดชอบของผู้เกี่ยวข้องและขั้นตอนปฏิบัติในการแลกเปลี่ยนหรือใช้ข้อมูลร่วมกัน เช่น วิธีการรับ-ส่ง เป็นต้น

(๓) กำหนดหน้าที่และความรับผิดชอบของแต่ละฝ่ายในการป้องกันข้อมูลรั่วไหลหรือสูญหาย ตลอดจนระบุผู้รับผิดชอบในกรณีที่ข้อมูลสูญหาย หรือเสียหาย

(๔) กำหนดขั้นตอนในการตรวจสอบผู้ส่งข้อมูลและผู้รับข้อมูลเพื่อป้องกันการปฏิเสธความรับผิดชอบ

(๕) กำหนดสิทธิในการเข้าถึงข้อมูลของแต่ละฝ่าย

(๖) กำหนดมาตรฐานทางเทคนิคที่ใช้ในการเข้าถึงข้อมูลหรือซอฟต์แวร์

(๗) กำหนดมาตรการพิเศษสำหรับป้องกันเอกสาร ข้อมูล ซอฟต์แวร์ หรืออื่น ๆ ที่มีความสำคัญ เช่น กุญแจที่ใช้ในการเข้ารหัส เป็นต้น

ส่วนที่ ๒ การสำรองข้อมูลและกู้คืน (Back up and Recovery)

ข้อ ๖ พิจารณาคัดเลือกระบบสารสนเทศที่สำคัญ และจัดทำระบบสำรองข้อมูลที่เหมาะสม และให้อยู่ในสภาพพร้อมใช้งาน โดยเรียงลำดับความสำคัญจากมากไปน้อย

ข้อ ๗ กำหนดหน้าที่และความรับผิดชอบของเจ้าหน้าที่ในการสำรองข้อมูล

ข้อ ๘ จัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของสำนักงาน พร้อมทั้งกำหนดระบบสารสนเทศที่ต้องมีระบบสำรองข้อมูล และจัดทำแผนเตรียมพร้อมสำหรับกรณีฉุกเฉินโดยให้ทบทวนแผน อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๙ กำหนดการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบโดยให้รวมถึงความถี่ในการสำรองข้อมูล หากระบบใดที่มีการเปลี่ยนแปลงบ่อย ให้เพิ่มความถี่ในการสำรองข้อมูล โดยให้มีวิธีการสำรองข้อมูล ดังนี้

(๑) กำหนดประเภทของข้อมูล และความถี่ในการสำรองข้อมูล

(๒) กำหนดรูปแบบการสำรองข้อมูลให้เหมาะสม

(๓) บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วัน/เวลา ชื่อข้อมูลที่สำรอง สถานะการสำรองข้อมูล (สำเร็จ/ไม่สำเร็จ) ขนาดของข้อมูล เป็นต้น

(๔) ตรวจสอบค่า configuration ของระบบการสำรองข้อมูล

(๕) จัดเก็บข้อมูลที่สำรองในสื่อเก็บข้อมูล โดยแสดงชื่อข้อมูล ซอฟต์แวร์ วันที่/เวลา และผู้สำรองข้อมูล บนสื่อเก็บข้อมูลอย่างชัดเจน

(๖) จัดเก็บข้อมูลที่สำรองไว้ในสถานที่ปลอดภัยที่แยกจากห้องระบบคอมพิวเตอร์

(๗) จัดระบบป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่ที่ใช้จัดเก็บข้อมูลสำรอง

(๘) ทดสอบการกู้คืนข้อมูลสำรอง (Recovery) อย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ

(๙) จัดทำขั้นตอนการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่สำรองไว้

(๑๐) ตรวจสอบ และ ทดสอบประสิทธิภาพและประสิทธิผลของขั้นตอนการกู้คืนข้อมูลอย่างสม่ำเสมออย่างน้อยปีละ ๑ ครั้ง หรือตามความเหมาะสมโดยคำนึงถึงความเสี่ยงต่าง ๆ ที่จะเกิดขึ้น

(๑๑) กำหนดให้ใช้การเข้ารหัสข้อมูลกับข้อมูลลับที่สำรองไว้

ข้อ ๑๐ ต้องจัดทำแผนบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Plan) เพื่อรองรับกรณีฉุกเฉินที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ ให้สามารถใช้งานระบบสารสนเทศได้เป็นปกติอย่างต่อเนื่อง ดังนี้

(๑) กำหนดหน้าที่ และความรับผิดชอบของผู้เกี่ยวข้องทั้งหมด

(๒) ประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญ และกำหนดมาตรการเพื่อลดความเสี่ยง เช่น ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว เกิดเหตุจลาจล ที่มีผลให้ไม่สามารถเข้าใช้งานระบบสารสนเทศได้ เป็นต้น

(๓) กำหนดขั้นตอนในการกู้คืนระบบสารสนเทศ

(๔) กำหนดขั้นตอนในการสำรองข้อมูล และทดสอบการกู้คืนข้อมูลที่สำรองไว้

(๕) กำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอก เช่น ผู้ให้บริการเครือข่าย ฮาร์ดแวร์ ซอฟต์แวร์ เป็นต้น

(๖) สร้างความตระหนัก หรือให้ความรู้แก่เจ้าหน้าที่ผู้เกี่ยวข้องกับขั้นตอนการปฏิบัติ หรือ สิ่งที่ต้องทำเมื่อเกิดเหตุฉุกเฉิน

ข้อ ๑๑ ทบทวนแผนบริหารความต่อเนื่องทางธุรกิจดังกล่าว ให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๑๒ ต้องกำหนดหน้าที่และความรับผิดชอบของเจ้าหน้าที่ผู้ดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรองข้อมูล และการจัดทำแผนบริหารความต่อเนื่องทางธุรกิจ ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

ข้อ ๑๓ ต้องทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรองข้อมูล และแผนบริหารความต่อเนื่องทางธุรกิจ อย่างน้อยปีละ ๑ ครั้ง หรือตามความเหมาะสมโดยคำนึงถึงความเสี่ยงต่าง ๆ ที่จะเกิดขึ้น เพื่อให้ระบบมีสภาพพร้อมใช้งานอยู่เสมอ

ข้อ ๑๔ ทบทวนระบบสารสนเทศ ระบบสำรองข้อมูล และแผนบริหารความต่อเนื่องทางธุรกิจ ให้เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน อย่างน้อยปีละ ๑ ครั้ง

หมวดที่ ๓
การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

วัตถุประสงค์

๑. เพื่อตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศ หรือสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่ได้คาดการณ์ไว้ล่วงหน้า

๒. เพื่อป้องกันและลดระดับความเสี่ยงที่อาจจะเกิดขึ้นกับระบบสารสนเทศ

๓. เพื่อเป็นแนวทางในการปฏิบัติ เมื่อเกิดความเสี่ยงที่เป็นอันตรายต่อระบบสารสนเทศ

แนวปฏิบัติ

ส่วนที่ ๑ การตรวจสอบและประเมินความเสี่ยง

ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศหรือสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่ได้คาดการณ์ไว้ล่วงหน้า ที่อาจเกิดขึ้นกับระบบสารสนเทศ โดยผู้ตรวจสอบภายในของสำนักงาน (Internal Auditor) หรือผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยของระบบสารสนเทศจากภายนอก (External Auditor) อย่างน้อยปีละ ๑ ครั้ง เพื่อให้สำนักงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยของระบบสารสนเทศ โดยมีแนวทางในการตรวจสอบและประเมินความเสี่ยงที่ต้องคำนึงถึง ดังนี้

ข้อ ๑ จัดลำดับความสำคัญของความเสี่ยง

ข้อ ๒ ค้นหาวิธีการดำเนินการเพื่อลดความเสี่ยง

ข้อ ๓ ศึกษาข้อดีข้อเสียของวิธีการดำเนินการเพื่อลดความเสี่ยง

ข้อ ๔ สรุปผลข้อเสนอแนะและแนวทางแก้ไขเพื่อลดความเสี่ยงที่ตรวจสอบได้

ข้อ ๕ ตรวจสอบและประเมินความเสี่ยง รวมทั้งจัดทำรายงานพร้อมข้อเสนอแนะ

ข้อ ๖ กำหนดมาตรการในการตรวจประเมินระบบสารสนเทศ อย่างน้อย ดังนี้

(๑) ให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบแบบอ่านได้อย่างเดียว (read only)

(๒) ในกรณีที่จำเป็นต้องเข้าถึงข้อมูลในแบบอื่น ๆ ให้สร้างสำเนาสำหรับข้อมูลนั้นให้ผู้ตรวจสอบใช้งาน รวมทั้งต้องทำลายหรือลบโดยทันทีที่ตรวจสอบเสร็จสิ้น หรือต้องจัดเก็บไว้โดยป้องกันเป็นอย่างดี

(๓) กำหนดให้ระบุและจัดสรรทรัพยากรที่จำเป็นต้องใช้ในการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัยของระบบสารสนเทศ

(๔) ให้เฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้ง บันทึกกิจกรรมการเข้าถึงข้อมูล (log file) แสดงการเข้าถึงข้อมูล รวมถึงวันและเวลาที่เข้าถึงระบบสารสนเทศที่สำคัญ ๆ

(๕) กำหนดให้แยกการติดตั้งเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ ออกจากระบบให้บริการจริง หรือระบบที่ใช้ในการพัฒนา และจัดเก็บป้องกันเครื่องมือนั้นจากการเข้าถึงโดยไม่ได้รับอนุญาต

ส่วนที่ ๒ ความเสี่ยงที่อาจเป็นอันตรายต่อระบบสารสนเทศ

ภัยด้านความมั่นคงปลอดภัยของระบบสารสนเทศ แยกได้ ๔ ประเภท ดังนี้

ประเภทที่ ๑ ภัยจากเจ้าหน้าที่ของสำนักงาน (Human Error) เช่น เจ้าหน้าที่ขาดความรู้ความเข้าใจในการใช้งานอุปกรณ์คอมพิวเตอร์ ทั้งด้านฮาร์ดแวร์และซอฟท์แวร์ ซึ่งอาจทำให้ระบบสารสนเทศเสียหาย ใช้งานไม่ได้ เกิดการชะงักงันหรือหยุดทำงาน ซึ่งส่งผลให้ไม่สามารถใช้งานระบบสารสนเทศได้อย่างเต็มประสิทธิภาพ โดยกำหนดแนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบสารสนเทศไว้ ดังนี้

(๑) จัดอบรมเจ้าหน้าที่ของสำนักงาน ให้มีความรู้ความเข้าใจในด้านฮาร์ดแวร์และซอฟท์แวร์เบื้องต้นเพื่อลดความเสี่ยงให้เกิดน้อยที่สุด

(๒) จัดทำหนังสือแจ้งเวียนหน่วยงาน เรื่องการใช้และการประหยัดพลังงานให้กับเครื่องคอมพิวเตอร์และอุปกรณ์ เพื่อเป็นแนวทางปฏิบัติได้อย่างถูกต้อง

ประเภทที่ ๒ ภัยจากซอฟท์แวร์ ที่สร้างความเสียหายให้แก่เครื่องคอมพิวเตอร์ หรือระบบเครือข่าย ประกอบด้วย ไวรัสคอมพิวเตอร์ (Computer Virus), หนอนอินเทอร์เน็ต (Internet Worm), ม้าโทรจัน (Trojan Horse), และข่าวไวรัสหลอกลวง (Hoax) ซึ่งซอฟท์แวร์เหล่านี้อาจรบกวนการทำงาน และก่อให้เกิดความเสียหายให้แก่ระบบสารสนเทศ ถึงขั้นทำให้ระบบเครือข่ายใช้งานไม่ได้ โดยกำหนดแนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ภัยจากซอฟท์แวร์ ดังนี้

(๑) ติดตั้งอุปกรณ์ป้องกันเครือข่ายที่ระบบเครือข่าย เพื่อให้ทำหน้าที่กำหนดสิทธิในการเข้าใช้งานระบบเครือข่าย และป้องกันการบุกรุกจากภายนอก

(๒) ติดตั้งโปรแกรมป้องกันไวรัส ดักจับไวรัสที่เข้ามาในระบบเครือข่าย ที่สามารถตรวจสอบชนิดของไวรัสชนิดที่ทำความเสียหายกับระบบเครือข่าย

ประเภทที่ ๓ ภัยจากไฟไหม้ หรือ ระบบไฟฟ้า จัดเป็นภัยที่สร้างความเสียหายให้แก่ ระบบสารสนเทศ อย่างร้ายแรง โดยกำหนดแนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ ดังนี้

(๑) ติดตั้งอุปกรณ์สำรองไฟฟ้า (UPS) เพื่อควบคุมการจ่ายกระแสไฟฟ้าให้กับระบบคอมพิวเตอร์แม่ข่าย (Server) ในกรณีกระแสไฟฟ้าขัดข้อง ระบบคอมพิวเตอร์แม่ข่ายจะสามารถให้บริการได้ในระยะเวลาที่สามารถจัดเก็บและสำรองข้อมูลไว้อย่างปลอดภัย

(๒) ติดตั้งอุปกรณ์ตรวจจับควัน สำหรับเหตุการณ์กระแสไฟฟ้าขัดข้องหรือมีควันไฟเกิดขึ้นภายในห้องระบบคอมพิวเตอร์ อุปกรณ์ดังกล่าวต้องส่งสัญญาณแจ้งเตือนให้หน่วยรักษาความปลอดภัยทราบและรีบเข้ามาระงับเหตุฉุกเฉินในทันที โดยให้ตรวจสอบความพร้อมของอุปกรณ์อย่างสม่ำเสมอ

(๓) ติดตั้งอุปกรณ์ดับเพลิงชนิดก๊าซ ที่ห้องระบบคอมพิวเตอร์ เพื่อใช้ในกรณีเหตุไฟไหม้ โดยให้ตรวจสอบความพร้อมของอุปกรณ์อย่างสม่ำเสมอ

ประเภทที่ ๔ ภัยจากน้ำท่วม (อุทกภัย) ความเสี่ยงต่อความเสียหายจากน้ำท่วม จัดเป็นภัยที่สร้างความเสียหายให้แก่ระบบสารสนเทศ อย่างร้ายแรง โดยกำหนดแนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ ดังนี้

(๑) เฝ้าระวังอุทกภัย โดยติดตามพยากรณ์อากาศของกรมอุตุนิยมวิทยาตลอดเวลา

(๒) ถอดเทปสำรองข้อมูลทั้งหมด ไปเก็บในที่ปลอดภัย

(๓) ตัดระบบไฟฟ้าในห้องระบบคอมพิวเตอร์ โดยปิดเบรคเกอร์เครื่องปรับอากาศ เพื่อป้องกันเครื่องควบคุมเสียหาย และป้องกันภัยจากไฟฟ้า

(๔) ย้ายเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่ายไปไว้บนที่สูง

(๕) เมื่อน้ำลดลงแล้ว ให้ช่างไฟฟ้าตรวจสอบการทำงานระบบไฟฟ้าในห้องระบบคอมพิวเตอร์ และเตรียมความพร้อมของห้องระบบคอมพิวเตอร์เพื่อติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย

(๖) ติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย พร้อมทั้งทดสอบการใช้งานเครื่องคอมพิวเตอร์แม่ข่ายแต่ละเครื่อง ตรวจสอบการเชื่อมต่อของระบบเครือข่ายกับเครื่องคอมพิวเตอร์ลูกข่าย

(๗) แจ้งให้หน่วยงานที่เกี่ยวข้องทราบ เพื่อเข้าใช้งานตามปกติ

หมวดที่ ๔
การรักษาความปลอดภัยด้านกายภาพ สถานที่ และสภาพแวดล้อม

วัตถุประสงค์

(๑) เพื่อกำหนดมาตรการในการควบคุมและป้องกันระบบการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ ในการเข้าใช้งานหรือเข้าถึงพื้นที่ใช้งาน โดยพิจารณาตามความสำคัญของอุปกรณ์ ระบบสารสนเทศข้อมูล โดยให้มีผลบังคับใช้กับผู้ใช้งานและรวมถึงบุคคลหรือหน่วยงานภายนอกที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศของสำนักงาน

แนวปฏิบัติ

ข้อ ๑ อาคาร สถานที่ และพื้นที่ใช้งานระบบสารสนเทศ หมายถึง ที่ตั้งของระบบคอมพิวเตอร์ ระบบเครือข่าย หรือระบบสารสนเทศ พื้นที่เตรียมข้อมูลจัดเก็บคอมพิวเตอร์และอุปกรณ์ พื้นที่ปฏิบัติงานของบุคลากรทางคอมพิวเตอร์ รวมทั้งเครื่องคอมพิวเตอร์ส่วนบุคคลและอุปกรณ์ประกอบที่ติดตั้งประจำโต๊ะทำงาน

ข้อ ๒ ห้องระบบคอมพิวเตอร์ ต้องมีลักษณะ ดังนี้

(๑) เป็นเขตหวงห้ามเด็ดขาด หรือเขตหวงห้ามเฉพาะ โดยพิจารณาตามความสำคัญแล้วแต่กรณี

(๒) เป็นที่เฉพาะ ที่อนุญาตเฉพาะให้บุคคลที่เกี่ยวข้องเท่านั้นผ่านเข้า-ออก

(๓) ต้องไม่มีป้ายหรือสัญลักษณ์ที่บ่งบอกถึงสถานะการเป็นที่ตั้งของระบบสารสนเทศที่สำคัญ

(๔) ต้องปิดล็อก หรือใส่กุญแจประตูหรือหน้าต่างห้องไว้เสมอ เมื่อไม่มีเจ้าหน้าที่ประจำอยู่

(๕) ให้ติดตั้งเครื่องโทรสารหรือเครื่องถ่ายเอกสารแยกออกจากบริเวณดังกล่าว

(๖) ไม่อนุญาตให้ถ่ายรูปหรือบันทึกภาพเคลื่อนไหวในบริเวณดังกล่าว เป็นอันขาด ยกเว้นแต่จะได้รับอนุญาตจากผู้บริหารหรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่

(๗) จัดพื้นที่สำหรับการส่งมอบผลิตภัณฑ์ ให้แยกออกจากบริเวณที่มีสินทรัพย์ เพื่อป้องกันการเข้าถึงระบบสารสนเทศจากผู้ไม่ได้รับอนุญาต

ข้อ ๓ การกำหนดบริเวณที่ต้องรักษาความมั่นคงปลอดภัย

(๑) จำแนกและกำหนดพื้นที่ของระบบสารสนเทศ อย่างเหมาะสมเพื่อเฝ้าระวัง ควบคุม รักษาความมั่นคงปลอดภัย จากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่น ๆ ที่อาจเกิดขึ้นได้

(๒) กำหนดและแบ่งบริเวณพื้นที่ใช้งานระบบสารสนเทศให้ชัดเจน รวมทั้งจัดทำแผนผังแสดงพื้นที่ใช้งาน และประกาศให้รับทราบทั่วกัน การกำหนดพื้นที่ดังกล่าวอาจแบ่งออกได้เป็นพื้นที่ทำงานทั่วไป (General Working Area) พื้นที่ทำงานของผู้ดูแลระบบ (System Administrator Area) พื้นที่ติดตั้งอุปกรณ์ระบบสารสนเทศ (IT Equipment Area) พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data Storage Area) และพื้นที่ใช้งานเครือข่ายไร้สาย (Wireless LAN Coverage Area) เป็นต้น

ข้อ ๔ การควบคุมการเข้า-ออก อาคารสถานที่

(๑) กำหนดสิทธิผู้ใช้งานที่มีสิทธิ์ผ่านเข้า-ออก และช่วงเวลาที่สามารถผ่านเข้า-ออกในแต่ละพื้นที่อย่างชัดเจน

(๒) บุคคลภายนอกหรือผู้มาติดต่อ จะต้องให้แลกบัตรที่ใช้ระบุตัวตนของบุคคลนั้น ๆ เช่น บัตรประชาชน ใบอนุญาตขับขี่ เป็นต้นกับเจ้าหน้าที่รักษาความปลอดภัย โดยให้ลงบันทึกข้อมูลบัตรในสมุดบันทึกและรับแบบฟอร์มการเข้าออกพร้อมกับบัตรผู้ติดต่อ (Visitor)

(๓) ให้บันทึกวันและเวลาการเข้า-ออกพื้นที่สำคัญของผู้ที่มาติดต่อ (Visitors)

(๔) ผู้มาติดต่อต้องติดบัตรให้เห็นอย่างชัดเจนตลอดระยะเวลาที่อยู่ภายในสำนักงาน

(๕) เจ้าหน้าที่ของบริษัทผู้รับจ้างต้องติดบัตรให้เห็นชัดเจนตลอดระยะเวลาการทำงาน

(๖) จัดเก็บบันทึกการเข้า-ออกพื้นที่หรือบริเวณที่มีความสำคัญ เช่น (Data Center) เป็นต้น เพื่อตรวจสอบในภายหลังเมื่อมีความจำเป็น

(๗) ให้ดูแลผู้มาติดต่อตลอดเวลาที่อยู่ในพื้นที่หรือบริเวณที่มีความสำคัญ จนกระทั่งผู้มาติดต่อเสร็จสิ้นภารกิจและออกจากพื้นที่ เพื่อป้องกันการสูญหายของทรัพย์สินหรือป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต

(๘) มีระเบียบปฏิบัติในการขออนุญาตเข้าพื้นที่หรือบริเวณที่มีความสำคัญของบุคคลภายนอก โดยต้องมีเหตุผลที่เพียงพอในการขออนุญาต

(๙) ทำความเข้าใจกับผู้มาติดต่อถึงกฎเกณฑ์หรือข้อกำหนดต่าง ๆ ที่ต้องปฏิบัติระหว่างที่อยู่ในพื้นที่หรือบริเวณที่มีความสำคัญ

(๑๐) ควบคุมการเข้าถึงพื้นที่ที่มีข้อมูลสำคัญจัดเก็บหรือประมวลผลอยู่

(๑๑) ไม่อนุญาตให้ผู้ไม่มีกิจเข้าไปในพื้นที่หรือบริเวณที่มีความสำคัญ เว้นแต่ได้รับอนุญาตจากผู้บริหารระดับสูงหรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่

(๑๒) พิสูจน์ตัวตน เช่น การใช้บัตรผ่านเข้า-ออก รหัสผ่าน เป็นต้น เพื่อควบคุมการเข้า-ออกพื้นที่หรือบริเวณที่มีความสำคัญ

(๑๓) ให้ทบทวน หรือยกเลิกสิทธิในการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญ อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๕ ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting Utilities)

(๑) มีระบบสนับสนุนการทำงานของระบบสารสนเทศของสำนักงานที่เพียงพอต่อความต้องการใช้งาน โดยให้มีระบบดังต่อไปนี้

- ระบบสำรองกระแสไฟฟ้า (UPS)
- เครื่องกำเนิดกระแสไฟฟ้าสำรอง (Generator)
- ระบบระบายอากาศ
- ระบบปรับอากาศ และควบคุมความชื้น

(๒) เพื่อลดความเสี่ยงของสภาวะระบบสนับสนุนล้มเหลว ให้ตรวจสอบหรือทดสอบระบบสนับสนุนอย่างน้อยปีละ ๑ ครั้ง

(๓) ติดตั้งระบบแจ้งเตือน ในกรณีที่ระบบสนับสนุนการทำงานภายในห้องระบบคอมพิวเตอร์ ทำงานผิดปกติหรือหยุดการทำงาน

ข้อ ๖ การเดินสายไฟ สายสื่อสาร และสายเคเบิ้ลอื่น ๆ (Cabling Security)

(๑) หลีกเลี่ยงการเดินสายสัญญาณเครือข่ายของสำนักงานเข้าไปในบริเวณบุคคลภายนอกเข้าถึงได้

(๒) ให้ร้อยท่อสายสัญญาณต่าง ๆ เพื่อป้องกันความเสียหายจากการดักจับสัญญาณ หรือการตัดสายสัญญาณ

(๓) ให้เดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการรบกวนของสัญญาณซึ่งกันและกัน

(๔) ทำป้ายชื่อบนสายสัญญาณและบนอุปกรณ์เพื่อป้องกันการเชื่อมต่อสัญญาณผิดเส้น

(๕) จัดทำผังสายสัญญาณสื่อสารต่าง ๆ ให้ครบถ้วนและถูกต้อง

(๖) ให้ปิดห้องที่มีสายสัญญาณสื่อสารต่าง ๆ โดยใส่สลักให้สนิท เพื่อป้องกันบุคคลภายนอกเข้าถึง

(๗) พิจารณาใช้งานสายไฟเบอร์ออฟติก แทนสายสัญญาณสื่อสารแบบเดิม (เช่น สายสัญญาณแบบ coaxial cable) สำหรับระบบสารสนเทศที่สำคัญ

(๘) สำรวจระบบสายสัญญาณสื่อสารทั้งหมด เพื่อตรวจค้นการติดตั้งอุปกรณ์ดักจับสัญญาณโดยผู้ไม่ประสงค์ดี

ข้อ ๗ การบำรุงรักษาอุปกรณ์ (Equipment Maintenance)

(๑) กำหนดให้บำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่แนะนำโดยผู้ผลิต

(๒) ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามที่ผู้ผลิตแนะนำ

(๓) จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้ง เพื่อใช้ตรวจสอบหรือประเมินในภายหลัง

(๔) จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ประเมินและปรับปรุงอุปกรณ์ดังกล่าว

(๕) ควบคุมและสอดส่องดูแลการปฏิบัติงานของผู้ให้บริการภายนอก ที่มาบำรุงรักษาอุปกรณ์ภายในสำนักงาน

(๖) ผู้รับจ้างดูแลระบบต้องได้รับให้สิทธิในการเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญ

ข้อ ๘ การนำทรัพย์สินของสำนักงานออกนอกสำนักงาน (Removal of Property)

(๑) ต้องได้รับอนุญาตจากผู้บริหารก่อนนำอุปกรณ์หรือทรัพย์สินนั้นออกไปใช้งานนอกสำนักงาน

(๒) กำหนดผู้รับผิดชอบในการเคลื่อนย้ายหรือนำอุปกรณ์ออกนอกสำนักงาน

(๓) กำหนดระยะเวลาของการนำอุปกรณ์ออกไปใช้งานนอกสำนักงาน

(๔) เมื่อนำอุปกรณ์ส่งคืน ให้ตรวจสอบว่าสอดคล้องกับระยะเวลาที่อนุญาตและตรวจสอบการชำรุดเสียหายของอุปกรณ์ด้วย

(๕) บันทึกข้อมูลการนำอุปกรณ์ของสำนักงานออกไปใช้งานนอกสำนักงาน เพื่อเป็นหลักฐานป้องกันการสูญหาย รวมทั้งบันทึกข้อมูลเพิ่มเติมเมื่อนำอุปกรณ์ส่งคืน

ข้อ ๙ การป้องกันอุปกรณ์ที่ใช้งานอยู่นอกสำนักงาน (Security of Equipment off-premises)

(๑) กำหนดมาตรการความปลอดภัยเพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์หรือสินทรัพย์ของสำนักงานออกไปใช้งาน เช่น การขนส่ง การเกิดอุบัติเหตุกับอุปกรณ์ เป็นต้น

(๒) ไม่ทิ้งอุปกรณ์หรือสินทรัพย์ของสำนักงานไว้โดยลำพังโดยไม่มีผู้ดูแล

(๓) เจ้าหน้าที่ต้องรับผิดชอบดูแลอุปกรณ์หรือสินทรัพย์ไม่ให้เสียหายหรือชำรุด

ข้อ ๑๐ การกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง (Secure Disposal or re-use of Equipment)

(๑) ให้ทำลายข้อมูลสำคัญในอุปกรณ์ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว

(๒) มีมาตรการหรือเทคนิคในการลบ หรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์ สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้เข้าถึงข้อมูลสำคัญ

หมวดที่ ๕
การปฏิบัติเพื่อตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยทางระบบสารสนเทศ

วัตถุประสงค์

(๑) เพื่อกำหนดมาตรการในการป้องกันการบุกรุกและการโจมตี หรือเหตุการณ์ละเมิดความปลอดภัยระบบสารสนเทศให้มีความมั่นคงปลอดภัย

แนวปฏิบัติ

ข้อ ๑ การจัดการระบบป้องกันผู้บุกรุก

(๑) ตรวจสอบ Log File หรือรายงานของระบบป้องกันการบุกรุก โดยให้ตรวจสอบในประเด็นดังต่อไปนี้

- ความถี่ในการโจมตี และประเภทของการโจมตี
- ลักษณะของการโจมตีว่าสามารถคาดการณ์ได้หรือไม่
- ระดับความรุนแรง
- หมายเลขไอพีของเครือข่ายของผู้โจมตี

ข้อ ๒ การจัดการระบบไฟร์วอลล์

(๑) ตรวจระบบป้องกันการบุกรุก อย่างน้อยเดือนละ ๑ ครั้ง

(๒) ตรวจสอบบันทึกของ Log File และรายงานของไฟร์วอลล์ โดยให้ตรวจสอบรายการดังต่อไปนี้

- Packet ที่ไฟร์วอลล์ได้บล็อก
- ลักษณะของ Packet ที่ถูกบล็อก
- Packet ของหมายเลขไอพีของเครือข่ายที่ถูกบล็อกตามจำนวนมากไปหาน้อย

(๓) เมื่อตรวจพบการโจมตีระบบหรือเหตุการณ์ละเมิดความปลอดภัยระบบสารสนเทศ ให้แจ้งผู้บริหารระดับสูงหรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่ เพื่อขอการตัดสินใจในการแก้ไขปัญหา

ข้อ ๓ การจัดการระบบป้องกันภัยคุกคามทางอินเทอร์เน็ตหรือโปรแกรมไม่ประสงค์ดี (Malware) ซึ่งครอบคลุมถึง ไวรัส หนอนอินเทอร์เน็ต โปรแกรมโทรจัน รวมถึงสปายแวร์

(๑) ตรวจสอบ Log File และรายงานของอุปกรณ์ที่เกี่ยวข้องกับระบบป้องกันภัยคุกคามทางอินเทอร์เน็ต โดยให้ตรวจสอบรายการดังต่อไปนี้

- ประเภทของโปรแกรมไม่ประสงค์ดีที่ถูกพบเรียงลำดับจากมากไปหาน้อย
- เครือข่ายที่ส่งโปรแกรมไม่ประสงค์ดี และปลายทางของการส่ง
- โปรแกรมไม่ประสงค์ดีถูกส่งออกจากหรือผ่านเครือข่ายภายในสำนักงานหรือไม่

(๒) ศึกษาหาวิธีแก้ไขเครื่องคอมพิวเตอร์ที่ติดโปรแกรมไม่ประสงค์ดี โดยเฉพาะประเภทที่ตรวจพบว่ากระจาย อยู่ในเครือข่ายของสำนักงาน

(๓) ให้ระงับการเชื่อมต่อของเครื่องคอมพิวเตอร์ที่ติดโปรแกรมไม่ประสงค์ดีกับระบบเครือข่าย แล้วแก้ไขเครื่องคอมพิวเตอร์นั้นทันทีที่ตรวจสอบพบว่า เครื่องคอมพิวเตอร์ภายในเครือข่ายติดโปรแกรมไม่ประสงค์ดี หรือเป็นเครื่องที่ส่งโปรแกรมไม่ประสงค์ดีออกไปสู่เครือข่ายภายนอก

หมวดที่ ๖
การสร้างความตระหนักในการรักษาความปลอดภัยของระบบสารสนเทศ

วัตถุประสงค์

๑. เพื่อสร้างความรู้ความเข้าใจ ในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์ให้แก่ผู้ใช้งานของสำนักงาน

๒. เพื่อให้การเกิดความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์

๓. เพื่อป้องกันและลดการกระทำความผิดที่เกิดขึ้นจากการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์โดยไม่ตั้งใจ

แนวปฏิบัติ

ข้อ ๑ จัดให้ทบทวน ปรับปรุงนโยบายและแนวปฏิบัติให้เป็นปัจจุบันอยู่เสมออย่างน้อยปีละ ๑ ครั้ง

ข้อ ๒ จัดฝึกอบรมแนวปฏิบัติตามแนวนโยบายอย่างสม่ำเสมอ โดยผสานความรู้ความเข้าใจในนโยบาย และวิธีปฏิบัติตามแนวทางในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ไว้ในหลักสูตรอบรมต่าง ๆ ตามแผนการฝึกอบรมของหน่วยงาน

ข้อ ๓ จัดสัมมนาเพื่อเผยแพร่นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และสร้างความตระหนักถึงความสำคัญของการปฏิบัติให้กับเจ้าหน้าที่ โดยจัดแผนการสัมมนาปีละไม่น้อยกว่า ๑ ครั้ง

ข้อ ๔ ประชาสัมพันธ์ ให้ความรู้เกี่ยวกับแนวปฏิบัติ ในลักษณะเกร็ดความรู้ หรือข้อระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย เช่น ติดประกาศ ฯลฯ โดยปรับเปลี่ยนเกร็ดความรู้อยู่เสมอ

ข้อ ๕ กระตุ้นการมีส่วนร่วมโดยผ่านการกำกับ ติดตาม ประเมินผล และสำรวจความต้องการของผู้ใช้งาน

ข้อ ๖ ให้ความรู้ความเข้าใจเกี่ยวกับโปรแกรมไม่ประสงค์ดีแก่ผู้ใช้งาน เพื่อให้ตระหนักในปัญหา สามารถป้องกันตนได้ และให้ทราบขั้นตอนปฏิบัติเมื่อพบตรวจพบโปรแกรมไม่ประสงค์ดี

ข้อ ๗ ให้ความรู้ความเข้าใจเกี่ยวกับเหตุการณ์ด้านความมั่นคงปลอดภัยและสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่ได้คาดการณ์ แก่ผู้ใช้งาน เพื่อให้สามารถปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของสำนักงานได้อย่างถูกต้อง

ข้อ ๘ ผู้ใช้งานต้องตระหนักและปฏิบัติตามกฎหมายใด ๆ ที่ได้ประกาศใช้ในประเทศไทยรวมทั้งกฎระเบียบของสำนักงาน และข้อตกลงระหว่างประเทศอย่างเคร่งครัด โดยให้ถือว่าการละเลยเพิกเฉย เป็นความผิดส่วนบุคคลซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

หมวดที่ ๗
หน้าที่และความรับผิดชอบ

วัตถุประสงค์

(๑) เพื่อกำหนดหน้าที่ความรับผิดชอบของผู้บริหารระดับสูง ผู้บริหาร เจ้าหน้าที่ ตลอดจนผู้ที่ได้รับมอบหมายให้ดูแลรับผิดชอบด้านสารสนเทศ

แนวปฏิบัติ

ข้อ ๑ **ระดับนโยบาย** ผู้รับผิดชอบ ได้แก่

- ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CSO/CIO)
- ผู้อำนวยการศูนย์ข้อมูลและสารสนเทศ หรือเทียบเท่าระดับผู้อำนวยการ

(๑) รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตาม กำกับดูแล ควบคุมตรวจสอบเจ้าหน้าที่ในระดับปฏิบัติ

(๒) รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น ในกรณีที่ระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ข้อ ๒ **ระดับบริหาร** ผู้รับผิดชอบ ได้แก่ ผู้อำนวยการศูนย์ข้อมูลและสารสนเทศ หัวหน้ากลุ่มหรือเทียบเท่าหัวหน้ากลุ่ม

(๑) รับผิดชอบ กำกับ ดูแลการปฏิบัติงานของผู้ปฏิบัติ ตลอดจนศึกษา ทบทวน วางแผนติดตามการบริหารความเสี่ยง และระบบรักษาความปลอดภัยฐานข้อมูลและเทคโนโลยีสารสนเทศ

(๒) รับผิดชอบในการควบคุม ดูแล รักษาความปลอดภัย ระบบสารสนเทศและระบบฐานข้อมูล

ข้อ ๓ **ระดับปฏิบัติ** ผู้รับผิดชอบ ได้แก่

- ผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่จากผู้บริหารระดับสูง เช่น นักวิชาการคอมพิวเตอร์ เจ้าหน้าที่เครื่องคอมพิวเตอร์ เป็นต้น

(๑) ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

(๒) ประสานการปฏิบัติงานตามแผนป้องกันและแก้ไขปัญหาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ

(๓) รับผิดชอบควบคุม ดูแล รักษาความปลอดภัย และบำรุงรักษา ระบบเครื่องคอมพิวเตอร์ ระบบเครือข่าย ห้องควบคุมระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย

(๔) สำรองข้อมูลและเรียกคืนข้อมูล (Backup and Recovery) ตามรอบระยะเวลาที่กำหนด

(๕) ป้องกันการถูกเจาะระบบ และแก้ไขปัญหาการถูกเจาะเข้าระบบฐานข้อมูลจากบุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาต

(๖) รับผิดชอบในการรักษาความปลอดภัยของระบบอินเทอร์เน็ต

(๗) ปฏิบัติงานอื่น ๆ ตามที่ได้รับมอบหมายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงาน

หมวดที่ ๘
การพัฒนาระบบสารสนเทศ

วัตถุประสงค์

(๑) เพื่อกำหนดขั้นตอนและข้อกำหนดต่าง ๆ ในการจัดทำโครงการพัฒนาระบบสารสนเทศของสำนักงาน ให้สอดคล้องกับสถาปัตยกรรมระบบ (Enterprise Architecture: EA) ของสำนักงาน นโยบายด้านความมั่นคงปลอดภัยของระบบสารสนเทศตลอดจนข้อกำหนดในการปฏิบัติตามแนวนโยบายดังกล่าว ของสำนักงาน

แนวปฏิบัติ

ข้อ ๑ การพัฒนาระบบสารสนเทศต้องกำหนดขั้นตอนการพิจารณา ทบทวน เพื่ออนุมัติการสร้าง การติดตั้ง การใช้งาน โดยระบบต้องมีคุณสมบัติ ดังนี้

(๑) สอดคล้องกับสถาปัตยกรรมระบบของสำนักงาน (Enterprise Architecture: EA)

(๒) สอดคล้องกับข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสารสนเทศของสำนักงาน

(๓) สามารถทำงานร่วมกันกับระบบเดิมที่ยังใช้งานอยู่ได้อย่างราบรื่น

(๔) ต้องทดสอบระบบในขั้นตอนการพัฒนาบนสภาวะแวดล้อมเดียวกันกับสภาวะแวดล้อมในการใช้งานจริง

(๕) ต้องเปรียบเทียบการตั้งค่าระบบ Active Directory (AD) ของสำนักงานคณะกรรมการอาหารและยา หรือระบบอื่น ๆ ที่กำหนด กับการตั้งค่าของ Center for Internet Security (CIS Benchmarks) พร้อมทั้งวิเคราะห์ถึงภัยคุกคาม (Threat) และช่องโหว่ (vulnerability)

(๖) การจัดหาครุภัณฑ์คอมพิวเตอร์ที่ใช้ในโครงการ ให้พิจารณาจัดหาโดยการใช้บริการของสำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติหรือวิธีการเช่า หากมีความจำเป็นที่จะต้องจัดซื้อครุภัณฑ์คอมพิวเตอร์ดังกล่าว ให้ผู้รับผิดชอบโครงการจัดทำข้อเสนอต่อคณะกรรมการด้านสารสนเทศของสำนักงาน เพื่อชี้แจงเหตุผลและความจำเป็น ตลอดจนความคุ้มค่าเมื่อเทียบกับการเช่าหรือเช่าซื้อตามวงเงินที่จะใช้จัดซื้อ โดยให้ยึดเกณฑ์ราคากลางและคุณลักษณะพื้นฐานครุภัณฑ์คอมพิวเตอร์ฉบับล่าสุดของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมเป็นเกณฑ์ในการกำหนดคุณลักษณะพื้นฐานขั้นต่ำและเพดานราคาของครุภัณฑ์คอมพิวเตอร์

ข้อ ๒ ในการเสนอโครงการพัฒนาระบบสารสนเทศต้องดำเนินการตามขั้นตอนการพิจารณา ทบทวน เพื่ออนุมัติการสร้าง การติดตั้ง การใช้งาน ดังนี้

(๑) ทบทวนสถานการณ์การทำงานและสำรวจความต้องการ

(๒) จัดทำข้อเสนอโครงการพัฒนาระบบสารสนเทศ โดยมีผู้แทนศูนย์ข้อมูลและสารสนเทศร่วมในการจัดทำ

(๓) เสนอคณะกรรมการด้านสารสนเทศของสำนักงานพิจารณาข้อเสนอโครงการพัฒนาระบบสารสนเทศ

(๔) จัดทำร่างข้อกำหนดของโครงการพัฒนาระบบสารสนเทศ โดยมีผู้แทนศูนย์ข้อมูลและสารสนเทศร่วมในการจัดทำ

(๕) เสนอคณะกรรมการด้านสารสนเทศของสำนักงานพิจารณาร่างข้อกำหนดของโครงการพัฒนาระบบสารสนเทศ

(๖) เสนอขออนุมัติโครงการจากผู้บริหารระดับสูงด้านเทคโนโลยีสารสนเทศ (CIO) ของกระทรวง

(๗) เสนอขออนุมัติงบประมาณจากสำนักงบประมาณ/สำนักงานคณะกรรมการอาหารและยา

(๘) ดำเนินการตามระเบียบพัสดุฯ ต่อไป

ข้อ ๓ การพัฒนาระบบสารสนเทศหลังจากทำสัญญาจ้างพัฒนาแล้ว ให้จัดการควบคุมการพัฒนาระบบสารสนเทศที่จัดจ้างผู้รับจ้างพัฒนาภายนอก ดังนี้

(๑) ชี้แจงแนวความคิดของระบบและข้อกำหนดมาตรฐาน พร้อมด้วยกระบวนการทำงานให้ผู้รับจ้างพัฒนาภายนอกทราบ

(๒) กำหนดหน้าที่และความรับผิดชอบของผู้เกี่ยวข้องในการพัฒนาระบบสารสนเทศ

(๓) กำหนดตารางเวลาในการพัฒนาแบบละเอียด โดยให้ผู้รับจ้างพัฒนาภายนอกนำเสนอความคืบหน้าของการพัฒนาระบบสารสนเทศ เช่น สัปดาห์ละครั้ง หรือ สองสัปดาห์ต่อครั้ง เป็นต้น

(๔) ตรวจสอบและติดตามการพัฒนาระบบสารสนเทศตามตารางเวลาในการพัฒนาแบบละเอียด ในการตรวจสอบและติดตามแต่ละครั้งต้องประกอบด้วยตัวแทนจาก ๓ ฝ่าย ดังนี้

๑) ศูนย์ข้อมูลและสารสนเทศ

๒) กองที่เกี่ยวข้อง

๓) ผู้รับจ้าง

(๕) ทดสอบระบบบนสภาวะแวดล้อมเดียวกันกับสภาวะแวดล้อมในการใช้งานจริง ก่อนส่งมอบงาน

(๖) ผู้รับจ้างต้องเปรียบเทียบการตั้งค่าระบบ Active Directory (AD) ของสำนักงานคณะกรรมการอาหารและยา หรือระบบอื่น ๆ ที่กำหนด กับการตั้งค่าของ Center for Internet Security (CIS Benchmarks) พร้อมทั้งวิเคราะห์ถึงภัยคุกคาม (Threat) และช่องโหว่ (vulnerability) ก่อนส่งมอบงาน

ข้อ ๔ การตรวจรับระบบสารสนเทศที่ผู้รับจ้างพัฒนาภายนอกส่งมอบ ให้ดำเนินการตามระเบียบพัสดุฯ โดยมีข้อกำหนดการบริการผู้รับจ้างพัฒนาภายนอกหลังตรวจรับระบบสารสนเทศในระยะเวลารับประกัน ดังนี้

(๑) ให้ผู้รับจ้างพัฒนาภายนอก แก้ไขปัญหาให้แล้วเสร็จภายใน ๒๔ ชั่วโมงนับตั้งแต่ได้รับแจ้ง หากไม่สามารถแก้ไขได้ภายในเวลาดังกล่าว ให้ผู้รับจ้างพัฒนาภายนอกแจ้งให้ผู้ดูแลระบบทราบถึงสภาพปัญหาและแนวทางการแก้ไขภายในเวลา ๒ ชั่วโมงนับตั้งแต่ได้รับแจ้ง ทั้งนี้ ต้องใช้เวลาแก้ไขไม่เกิน ๗๒ ชั่วโมง

(๒) ผู้รับจ้างพัฒนาภายนอก ต้องจัดให้มีผู้ให้บริการตามข้อกำหนดในสัญญาจ้าง โดยประกอบด้วย ผู้จัดการโครงการ นักวิเคราะห์ระบบ นักเขียนโปรแกรม เป็นต้น ประจำสำนักงานตลอดเวลาทำการตามที่สำนักงานกำหนด

หมวดที่ ๙
การจัดหาครุภัณฑ์คอมพิวเตอร์

วัตถุประสงค์

(๑) เพื่อกำหนดขั้นตอนและข้อกำหนดต่าง ๆ ในการจัดหาครุภัณฑ์คอมพิวเตอร์เพื่อใช้ในการกิจการของสำนักงาน ให้สอดคล้องกับสถาปัตยกรรมระบบ (Enterprise Architecture: EA) นโยบายด้านความมั่นคงปลอดภัยของระบบสารสนเทศตลอดจนข้อกำหนดในการปฏิบัติตามแนวนโยบายดังกล่าว ของสำนักงาน

(๒) เพื่อกำหนดขั้นตอนและข้อกำหนดต่าง ๆ ในการจัดซื้อให้เหมาะสมกับเหตุผลและความจำเป็น ตลอดจนความคุ้มค่าเมื่อเทียบกับวงเงินที่จะจัดซื้อ โดยให้ยึดเกณฑ์ราคากลางและคุณลักษณะพื้นฐานครุภัณฑ์คอมพิวเตอร์ฉบับล่าสุดของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมเป็นเกณฑ์ในการกำหนดคุณลักษณะพื้นฐานขั้นต่ำและเพดานราคาของครุภัณฑ์คอมพิวเตอร์

แนวปฏิบัติ

ข้อ ๑ การจัดหาครุภัณฑ์คอมพิวเตอร์ให้พิจารณาแนวทางในการจัดหาตามลำดับ ดังนี้

(๑) ใช้ครุภัณฑ์คอมพิวเตอร์ที่สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติมีให้บริการโดยไม่คิดมูลค่า

(๒) ให้เช่า หรือเช่าซื้อตามแต่สมควร ในกรณีที่สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติไม่มีให้บริการโดยไม่คิดมูลค่า

(๓) ให้จัดซื้อตามเหมาะสมกับเหตุผลและความจำเป็น ตลอดจนความคุ้มค่าเมื่อเทียบกับวงเงินที่จะจัดซื้อ โดยให้ยึดเกณฑ์ราคากลางและคุณลักษณะพื้นฐานครุภัณฑ์คอมพิวเตอร์ฉบับล่าสุดของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมเป็นเกณฑ์ในการกำหนดคุณลักษณะพื้นฐานขั้นต่ำและเพดานราคาของครุภัณฑ์คอมพิวเตอร์

ข้อ ๒ การจัดซื้อครุภัณฑ์คอมพิวเตอร์ ให้ผู้รับผิดชอบจัดทำข้อเสนอต่อคณะกรรมการด้านสารสนเทศของสำนักงาน เพื่อชี้แจงเหตุผลและความจำเป็น ตลอดจนความคุ้มค่าเมื่อเทียบการเช่าหรือเช่าซื้อตามวงเงินที่จะใช้จัดซื้อ โดยให้ยึดเกณฑ์ราคากลางและคุณลักษณะพื้นฐานครุภัณฑ์คอมพิวเตอร์ฉบับล่าสุดของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมเป็นเกณฑ์ในการกำหนดคุณลักษณะพื้นฐานขั้นต่ำและเพดานราคาของครุภัณฑ์คอมพิวเตอร์

ข้อ ๓ ในการเสนอโครงการจัดหาครุภัณฑ์คอมพิวเตอร์ต้องดำเนินการตามขั้นตอนการพิจารณา ทบทวน การติดตั้ง การใช้งาน ดังนี้

(๑) ทบทวนสถานการณ์การทำงานและสำรวจความต้องการ

(๒) จัดทำข้อเสนอโครงการจัดหาครุภัณฑ์คอมพิวเตอร์ โดยมีผู้แทนศูนย์ข้อมูลและสารสนเทศร่วมในการจัดทำ

(๓) เสนอคณะกรรมการด้านสารสนเทศของสำนักงานพิจารณาข้อเสนอโครงการจัดหาครุภัณฑ์คอมพิวเตอร์

(๔) จัดทำร่างข้อกำหนดของโครงการจัดหาครุภัณฑ์คอมพิวเตอร์ โดยมีผู้แทนศูนย์ข้อมูลและสารสนเทศร่วมในการจัดทำ

(๕) เสนอคณะกรรมการด้านสารสนเทศของสำนักงานพิจารณาร่างข้อกำหนดของโครงการจัดหาครุภัณฑ์คอมพิวเตอร์

(๖) เสนอขออนุมัติโครงการจากผู้บริหารเทคโนโลนีสารสนเทศระดับสูง (CIO) ของกระทรวง

(๗) เสนอขออนุมัติงบประมาณจากสำนักงบประมาณ/สำนักงานคณะกรรมการอาหารและยา

(๘) ดำเนินการตามระเบียบพัสดุฯ ต่อไป

ข้อ ๔ การตรวจสอบคุณสมบัติและการใช้งานครุภัณฑ์คอมพิวเตอร์ที่จัดหา

(๑) ชี้แจงแนวความคิดของระบบและข้อกำหนดมาตรฐาน พร้อมด้วยกระบวนการทำงานให้คู่สัญญาทราบ

(๒) กำหนดหน้าที่และความรับผิดชอบของผู้เกี่ยวข้องในการติดตั้งครุภัณฑ์คอมพิวเตอร์

(๓) กำหนดตารางเวลาในการติดตั้งครุภัณฑ์คอมพิวเตอร์แบบละเอียด โดยให้คู่สัญญานำเสนอความคืบหน้าของการติดตั้งครุภัณฑ์คอมพิวเตอร์ เช่น สัปดาห์ละครั้ง หรือ สองสัปดาห์ต่อครั้ง เป็นต้น

(๔) ตรวจสอบคุณสมบัติของครุภัณฑ์คอมพิวเตอร์พร้อม BurnIn ก่อนหรือหลังการติดตั้งตามแต่กรณี และติดตามการติดตั้งครุภัณฑ์คอมพิวเตอร์ตามตารางเวลาในการติดตั้งครุภัณฑ์คอมพิวเตอร์แบบละเอียด

(๕) ทดสอบการใช้งานจริง ก่อนส่งมอบงาน

ข้อ ๕ การตรวจรับครุภัณฑ์คอมพิวเตอร์ที่คู่สัญญาส่งมอบ ให้ดำเนินการตามระเบียบพัสดุฯ โดยมีข้อกำหนดการบริการของคู่สัญญาหลังตรวจรับ ในระยะเวลารับประกัน ดังนี้

(๑) ให้คู่สัญญา แก้ไขคอมพิวเตอร์ให้แล้วเสร็จภายใน ๑ ชั่วโมงนับตั้งแต่ได้รับแจ้ง หากไม่สามารถแก้ไขได้ภายในเวลาดังกล่าว ให้คู่สัญญาแจ้งให้ผู้ดูแลระบบทราบถึงสภาพปัญหาและแนวทางการแก้ไขภายในเวลา ๒ ชั่วโมงนับตั้งแต่ได้รับแจ้ง ทั้งนี้ ต้องใช้เวลาแก้ไขไม่เกิน ๒๔ ชั่วโมง

(๒) คู่สัญญา ต้องจัดให้มีผู้ให้บริการตามข้อกำหนดในสัญญาจ้าง โดยประกอบด้วย วิศวกรระบบ ช่างเทคนิค เป็นต้น ประจำสำนักงานตลอดเวลาทำการตามที่สำนักงานกำหนด

หมวดที่ ๑๐
แนวปฏิบัติ เมื่อเกิดฟิชชิ่ง (Phishing) ที่เว็บเซิร์ฟเวอร์ (Webserver) ของสำนักงาน

วัตถุประสงค์

(๑) เพื่อกำหนดมาตรการในการแก้ไขปัญหาการเกิดฟิชชิ่ง (Phishing) ได้อย่างรวดเร็ว ไม่ให้เกิดความเสียหาย และส่งผลกระทบต่อหน่วยงานทั้งภายในและภายนอกที่ใช้งานระบบสารสนเทศ

แนวปฏิบัติ

ข้อ ๑ เมื่อผู้ดูแลระบบเครือข่ายของสำนักงานได้รับแจ้งหรือตรวจพบว่า เว็บเซิร์ฟเวอร์ของหน่วยงานใด ๆ เป็นช่องทางให้ผู้ไม่หวังดีทำฟิชชิ่ง (Phishing) ผู้ดูแลระบบของสำนักงานต้องดำเนินการ ดังนี้

(๑) บล็อค IP Address ของเว็บเซิร์ฟเวอร์ที่โดนฟิชชิ่ง หรือแจ้งผู้ให้บริการเส้นทางเครือข่ายของสำนักงานดำเนินการโดยเร่งด่วน

(๒) แจ้งผู้ดูแลเซิร์ฟเวอร์ของหน่วยงานที่ถูกทำฟิชชิ่ง ทาง e-Mail หรือทางโทรศัพท์ เพื่อให้แก้ไขปัญหา

ข้อ ๒ เมื่อหน่วยงานแก้ไขปัญหาเรียบร้อยแล้ว ให้ประสานไปยังผู้ดูแลระบบเครือข่ายของสำนักงานหรือผู้ให้บริการเส้นทางเครือข่ายของสำนักงาน เพื่อปลดบล็อค IP Address

ข้อ ๓ ผู้ดูแลเว็บเซิร์ฟเวอร์ของสำนักงานต้องตรวจสอบเว็บเซิร์ฟเวอร์และเว็บไซต์ภายในสำนักงาน รวมทั้งติดตั้งโปรแกรมปรับปรุงช่องโหว่ (patch) อย่างสม่ำเสมอ เพื่อป้องกันผู้ที่ไม่หวังดีในการเข้ามาทำฟิชชิ่ง