ประกาศสำนักงานนโยบายและแผนทรัพยากรธรรมชาติและสิ่งแวดล้อม
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
สำนักงานนโยบายและแผนทรัพยากรธรรมชาติและสิ่งแวดล้อม
พ.ศ. ๒๕๖๔

พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ มาตรา ๕ กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐ หรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ และมาตรา ๗ กำหนดให้หน่วยงานของรัฐจัดทำเป็นประกาศ และต้องได้รับความเห็นชอบจากคณะกรรมการหรือหน่วยงานที่คณะกรรมการมอบหมาย จึงมีผลใช้บังคับได้ และพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๔๔ กำหนดให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำประมวลแนวทางปฏิบัติ และกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงาน ให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยเร็ว

สำนักงานนโยบายและแผนทรัพยากรธรรมชาติและสิ่งแวดล้อม (สผ.) จึงได้กำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อเป็นกรอบแนวทางในการบริหารจัดการและการดำเนินงานด้านระบบสารสนเทศของ สผ. ให้เป็นไปอย่างมีประสิทธิภาพ และมีความมั่นคงปลอดภัย โดยมีรายละเอียดดังนี้

ข้อ ๑. ประกาศนี้เรียกว่า “นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สำนักงานนโยบายและแผนทรัพยากรธรรมชาติและสิ่งแวดล้อม พ.ศ. ๒๕๖๔”

ข้อ ๒. วัตถุประสงค์

๒.๑ เพื่อกำหนดนโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงและปลอดภัยด้านสารสนเทศ เพื่อให้ผู้บริหาร ข้าราชการ และเจ้าหน้าที่ สผ. รวมทั้งผู้ที่ปฏิบัติงานเกี่ยวข้องกับระบบสารสนเทศของ สผ. นำไปปฏิบัติอย่างเคร่งครัด

๒.๒ เพื่อให้การบริหารจัดการและการดำเนินงานด้านสารสนเทศของ สผ. มีความมั่นคงปลอดภัย สามารถสนับสนุนการปฏิบัติงานตามภารกิจของ สผ. ได้อย่างมีประสิทธิภาพและประสิทธิผล รวมทั้งได้รับความเชื่อถือจากผู้ที่เกี่ยวข้อง

ข้อ ๓. ขอบเขต

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สำนักงานนโยบายและแผนทรัพยากรธรรมชาติและสิ่งแวดล้อม มีขอบเขตครอบคลุม ดังนี้

คำนิยาม

ส่วนที่ ๑ แนวปฏิบัติในการควบคุมการเข้าถึงและการใช้งานสารสนเทศ

ส่วนที่ ๒ แนวปฏิบัติในการบริหารจัดการข้อมูลตามระดับชั้นความลับ

ส่วนที่ ๓ แนวปฏิบัติในการบริหารจัดการการเข้าถึงของผู้ใช้งาน

ส่วนที่ ๔ แนวปฏิบัติในการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน

ส่วนที่ ๕ แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

ส่วนที่ ๖ แนวปฏิบัติในการควบคุมการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย

ส่วนที่ ๗ แนวปฏิบัติในการควบคุมการเข้าถึงเครือข่าย

ส่วนที่ ๘ แนวปฏิบัติในการควบคุมการเข้าถึงระบบปฏิบัติการ

ส่วนที่ ๙ แนวปฏิบัติในการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ

ส่วนที่ ๑๐ แนวปฏิบัติในการใช้งานระบบอินเทอร์เน็ต

ส่วนที่ ๑๑ แนวปฏิบัติในการใช้งานเครือข่ายสังคมออนไลน์

ส่วนที่ ๑๒ แนวปฏิบัติในการใช้งานระบบจดหมายอิเล็กทรอนิกส์

ส่วนที่ ๑๓ แนวปฏิบัติในการใช้งานเครื่องคอมพิวเตอร์และเครื่องคอมพิวเตอร์แบบพกพาของสำนักงาน

ส่วนที่ ๑๔ แนวปฏิบัติในการจัดเก็บข้อมูลจราจรคอมพิวเตอร์

ส่วนที่ ๑๕ แนวปฏิบัติในการพัฒนาและปรับปรุงระบบสารสนเทศให้มีความปลอดภัย

ส่วนที่ ๑๖ แนวปฏิบัติในการสำรองข้อมูลสำคัญและการเตรียมรับมือกับเหตุฉุกเฉิน

ส่วนที่ ๑๗ แนวปฏิบัติในการเชื่อมโยงระบบงานกับหน่วยงานภายนอก

ส่วนที่ ๑๘ แนวปฏิบัติในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

ส่วนที่ ๑๙ แนวปฏิบัติในการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย

ส่วนที่ ๒๐ แนวปฏิบัติในการสร้างความตระหนักเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ

ภาคผนวก

ข้อ ๔. ความรับผิดชอบ

๔.๑ ระดับนโยบาย

๔.๑.๑ กำหนดให้ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Officer: CEO) เป็นผู้รับผิดชอบต่อความเสี่ยงความเสียหาย หรืออันตรายที่เกิดขึ้น กรณีระบบคอมพิวเตอร์ หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กร หรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่องละเลย หรือฝ่าฝืนการปฏิบัติ ตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๔.๑.๒ กำหนดให้ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer: CIO) เป็นผู้รับผิดชอบในการสั่งการตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๔.๑.๓ กำหนดให้ผู้อำนวยการกองติดตามประเมินผลสิ่งแวดล้อม เป็นผู้รับผิดชอบในการกำกับดูแล รวมทั้งให้คำปรึกษา และข้อเสนอแนะแก่เจ้าหน้าที่ระดับปฏิบัติ

๔.๒ ระดับปฏิบัติ

๔.๒.๑ กำหนดให้กลุ่มงานระบบฐานข้อมูลและเทคโนโลยีสารสนเทศ กองติดตามประเมินผลสิ่งแวดล้อม ทำหน้าที่ให้คำปรึกษาและข้อเสนอแนะ รวมทั้งดูแลให้การปฏิบัติงานของเจ้าหน้าที่เป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๔.๒.๒ กำหนดให้เจ้าหน้าที่ของ สผ. ทุกคน และผู้ที่ได้รับมอบหมายจาก สผ. ให้ปฏิบัติงานเกี่ยวข้องกับระบบสารสนเทศ ต้องปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างเคร่งครัด

ข้อ ๕. กำหนดให้มีการควบคุมการเข้าถึงควบคุมและการใช้งานสารสนเทศ รวมถึงระบบเครือข่าย ระบบปฏิบัติการ โปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ เพื่อควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูลของ สผ. ให้มีความมั่นคงและปลอดภัย

ข้อ ๖. กำหนดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศของสำนักงาน (Information security audit and assessment) ปีละ ๑ ครั้ง

ข้อ ๗. กำหนดให้มีการสำรองและกู้คืนข้อมูลสำคัญ และจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินเพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

ข้อ ๘. กำหนดให้มีการทบทวนและปรับปรุงนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ปีละ ๑ ครั้ง

ข้อ ๙. กำหนดให้มีการจัดทำแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่สอดคล้องกับนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตามความเหมาะสมและจำเป็น โดยจัดทำเพิ่มเติมไว้ในเอกสารแนบท้ายของประกาศฉบับนี้

ข้อ ๑๐. กำหนดให้มีการเผยแพร่ประกาศฉบับนี้ให้บุคลากรของ สผ. ทราบโดยทั่วกัน ทั้งการแจ้งเป็นลายลักษณ์อักษร และแจ้งเวียนผ่านระบบสารบรรณอิเล็กทรอนิกส์ รวมทั้งประกาศในระบบอินทราเน็ตของ สผ. รวมทั้งมีการจัดทำนโยบายฯ ฉบับผู้รับบริการ เผยแพร่ในเว็บไซต์ของ สผ.

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

ประกาศ ณ วันที่ ๘ เดือนตุลาคม พ.ศ. ๒๕๖๔

(นายปิ่นสักก์ สุรัสวดี)
รองปลัดกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม
รักษาราชการแทนเลขาธิการ
สำนักงานนโยบายและแผนทรัพยากรธรรมชาติ
และสิ่งแวดล้อม

เอกสารแนบท้ายประกาศสำนักงานนโยบายและแผนทรัพยากรธรรมชาติและสิ่งแวดล้อม
เรื่อง

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สำนักงานนโยบายและแผนทรัพยากรธรรมชาติและสิ่งแวดล้อม

พ.ศ. ๒๕๖๔

สารบัญ

หน้า

คำนิยาม

คำนิยามที่ใช้ในนโยบายฯ ฉบับนี้ ประกอบด้วย

“สำนักงาน” หมายถึง สำนักงานนโยบายและแผนทรัพยากรธรรมชาติและสิ่งแวดล้อม

“หน่วยงาน” หมายถึง กอง/กลุ่มอิสระภายในสำนักงานนโยบายและแผนทรัพยากรธรรมชาติและสิ่งแวดล้อม

“ผู้บริหารระดับสูงสุด” (Chief Executive Officer: CEO) หมายถึง เลขาธิการสำนักงานนโยบายและแผนทรัพยากรธรรมชาติและสิ่งแวดล้อม

“ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง” (Chief Information Officer: CIO) หมายถึง ผู้บริหารเทคโนโลยีระดับสูงของสำนักงานนโยบายและแผนทรัพยากรธรรมชาติและสิ่งแวดล้อม

“ผู้บังคับบัญชา” หมายถึง ผู้มีอำนาจสั่งการในระดับต่าง ๆ ตามโครงสร้างการบริหารงานของสำนักงาน

“ผู้ดูแลระบบสารสนเทศ” หมายถึง ผู้ที่ได้รับมอบหมายจากสำนักงานให้ทำหน้าที่ดูแลระบบสารสนเทศในภาพรวม รวมทั้งรับผิดชอบในการควบคุมการเข้าถึงข้อมูลและสารสนเทศในระบบงานของสำนักงาน ในที่นี้หมายถึง กลุ่มงานระบบฐานข้อมูลและเทคโนโลยีสารสนเทศ กองติดตามประเมินผลสิ่งแวดล้อม

“ผู้ดูแลเครือข่าย” หมายถึง ผู้ที่ได้รับมอบหมายจากสำนักงานให้มีหน้าที่ดูแลระบบเครือข่ายของสำนักงาน

“ผู้รับผิดชอบระบบ” หมายถึง หน่วยงานในสำนักงานที่เป็นผู้กำหนดให้มีการพัฒนาระบบหรือระบบงานนั้น ๆ

“ผู้ดูแลระบบ” (System Administrator) หมายถึง ผู้ที่ได้รับมอบหมายจากสำนักงานให้ทำหน้าที่บริหารจัดการบัญชีรายชื่อผู้มีสิทธิในการเข้าถึงระบบงาน เช่น การให้สิทธิ การเพิ่มสิทธิ การลดสิทธิ การยกเลิกสิทธิ รวมทั้งการพัฒนา ปรับปรุงดูแลบำรุงรักษาระบบงานต่าง ๆ ภายในสำนักงาน

“ผู้พัฒนาระบบ” หมายถึง ผู้ที่ได้รับมอบหมายจากสำนักงานให้ดำเนินการพัฒนาและปรับปรุงระบบหรือระบบงานต่าง ๆ ของสำนักงาน

“ผู้ให้บริการภายนอก” (External Service Provider) หมายถึง หน่วยงานภายนอกที่รับจ้างปฏิบัติงานด้านเทคโนโลยีสารสนเทศตามความต้องการของสำนักงาน เช่น ผู้ให้บริการอินเทอร์เน็ต ผู้ให้บริการด้านฮาร์ดแวร์ ผู้ให้บริการด้านซอฟต์แวร์ เป็นต้น

“เจ้าของข้อมูล” หมายถึง กลุ่มงาน/กลุ่มอิสระ ที่รับผิดชอบในการรวบรวม จัดหา และจัดเก็บข้อมูลตามภารกิจหรือข้อมูลที่เกี่ยวข้องกับภารกิจของตนเอง

“ผู้ใช้งาน” หมายถึง ผู้บริหาร ข้าราชการ พนักงานราชการ พนักงานกองทุนสิ่งแวดล้อม ลูกจ้างของสำนักงาน และผู้ที่ได้รับอนุญาตให้ปฏิบัติงานด้านสารสนเทศของสำนักงาน ผู้รับบริการ และผู้ใช้งานทั่วไป

“สิทธิของผู้ใช้งาน” หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใด ที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศของสำนักงาน

“บัญชีผู้ใช้งาน” (User account) หมายถึง บัญชีรายชื่อผู้เข้าถึงและรหัสผ่านในการใช้งานระบบสารสนเทศของสำนักงาน

“ชื่อผู้ใช้งาน” (Username) หมายถึง ชุดของตัวอักษร หรือตัวเลขที่ถูกกำหนดขึ้นเพื่อใช้ในการเข้าใช้งานระบบคอมพิวเตอร์ และระบบเครือข่ายที่มีการกำหนดสิทธิการใช้งานไว้

“รหัสผ่าน” (Password) หมายถึง กลุ่มข้อความที่ประกอบด้วยตัวอักษร ตัวเลขหรือเครื่องหมายที่ผู้ใช้งานระบบสารสนเทศกำหนดขึ้น เพื่อใช้ในการระบุตัวตนและสิทธิในการเข้าใช้งานเครื่องคอมพิวเตอร์หรือระบบสารสนเทศ

“การยืนยันตัวตน” (Authentication) หมายถึง วิธีการที่ใช้ในการตรวจสอบผู้ที่มาใช้งานระบบเครือข่ายอินเทอร์เน็ต โดยระบบจะทำการตรวจสอบจาก username และ password ว่าถูกต้องหรือไม่ โดยมีจุดประสงค์หลักเพื่อพิสูจน์ตัวตนของผู้ที่เข้าใช้งาน และตรวจสอบสิทธิการใช้งานของบุคคลนั้น

“ข้อมูลส่วนบุคคล” หมายถึง ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

“สินทรัพย์” หมายถึง ทรัพย์สินหรือสิ่งใดก็ตาม ทั้งที่มีตัวตนและไม่มีตัวตน ที่มีมูลค่าหรือคุณค่าสำหรับสำนักงาน

“ทรัพย์สินสารสนเทศ” หมายถึง ระบบเครือข่ายและอุปกรณ์เครือข่าย ระบบคอมพิวเตอร์ เครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ ระบบงาน ระบบสารสนเทศ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์ของสำนักงาน

“สารสนเทศ” (Information) หมายถึง ข้อมูลที่ผ่านการประมวลผลแล้ว ซึ่งมีการจัดระเบียบข้อมูลให้อยู่ในรูปของตัวเลข ข้อความ รูปภาพ หรือกราฟิก ในลักษณะที่ผู้ใช้งานสามารถเข้าใจได้ง่าย

“ระบบสารสนเทศ” (Information system) หมายถึง ระบบที่มีการนำคอมพิวเตอร์มาใช้ในการรวบรวม จัดเก็บ ประมวลผล สร้างสารสนเทศ หรือจัดการกับข้อมูล เพื่อใช้สนับสนุนการทำงาน การตัดสินใจ การวางแผน และการบริหารงานของสำนักงาน ซึ่งในที่นี้หมายความถึง เว็บไซต์ เว็บเพจ เว็บแอปพลิเคชัน โมบายแอปพลิเคชัน และฐานข้อมูล

“ระบบเทคโนโลยีสารสนเทศ” (Information technology systems) หมายถึง ระบบงานโปรแกรมประยุกต์ ระบบปฏิบัติการ เครื่องคอมพิวเตอร์ เซิร์ฟเวอร์ให้บริการระบบงาน เครือข่าย อุปกรณ์เครือข่าย และอุปกรณ์คอมพิวเตอร์อื่น ๆ

“ระบบงาน” (Application systems) หมายถึง ระบบสารสนเทศที่ทำงานอยู่บนเครื่องคอมพิวเตอร์เพื่อให้บริการต่าง ๆ ซึ่งรวมถึงให้บริการงานตามภารกิจของสำนักงาน เช่น ระบบงานบุคลากร ระบบงานบัญชี เป็นต้น

“ระบบปฏิบัติการ” (Operating system) หมายถึง โปรแกรมประยุกต์ที่ใช้ซอฟต์แวร์ในการควบคุมการปฏิบัติงานของคอมพิวเตอร์

“ระบบเครือข่าย” (Network system) หมายถึง ระบบเครือข่ายคอมพิวเตอร์ของสำนักงาน

“ระบบอินเทอร์เน็ต” (Internet) หมายถึง ระบบเครือข่ายคอมพิวเตอร์ที่เชื่อมต่อระหว่างระบบเครือข่ายคอมพิวเตอร์ของสำนักงานเข้ากับเครือข่ายคอมพิวเตอร์ต่าง ๆ ทั่วโลก

“ระบบอินทราเน็ต” (Intranet) หมายถึง ระบบเครือข่ายภายในของสำนักงาน ซึ่งมีการเชื่อมต่อกับคอมพิวเตอร์เช่นเดียวกับระบบอินเทอร์เน็ต แต่จะเปิดให้ใช้งานได้เฉพาะบุคลากรของสำนักงานเท่านั้น

“ระบบคลาวด์” (Cloud) หรือ คลาวด์ คอมพิวติ้ง (Cloud Computing) หมายถึง ระบบคอมพิวเตอร์ที่เกิดขึ้นเพื่อรองรับการทำงานของผู้ใช้งาน ทั้งด้านระบบเครือข่าย ด้านการจัดเก็บข้อมูล ด้านการติดตั้งฐานข้อมูล หรือการใช้งานซอฟต์แวร์เฉพาะด้านในธุรกิจต่าง ๆ เป็นต้น โดยที่ผู้ใช้บริการไม่จำเป็นต้องติดตั้งระบบทั้งฮาร์ดแวร์และซอฟต์แวร์ไว้ที่สำนักงานของตน

“โมบายแอปพลิเคชัน” (Mobile application) หมายถึง โปรแกรมประยุกต์ ซึ่งพัฒนาขึ้นเพื่อการใช้งานบนอุปกรณ์สื่อสารเคลื่อนที่หรือสมาร์ทโฟนโดยเฉพาะ

“อุปกรณ์คอมพิวเตอร์” หมายถึง อุปกรณ์อิเล็กทรอนิกส์ที่เชื่อมต่อกับหรือทำงานเป็นส่วนหนึ่งของคอมพิวเตอร์ ซึ่งอาจทำหน้าที่ในการสื่อสารข้อมูล ประมวลผลข้อมูล บันทึกข้อมูล หรือสนับสนุนการทำงานของคอมพิวเตอร์ในลักษณะต่าง ๆ เช่น อุปกรณ์เครือข่าย (เช่น สวิทช์ เราเตอร์) เครื่องพิมพ์ เครื่องสแกนภาพ และเครื่องสำรองไฟฟ้า (UPS) เป็นต้น

“ดิจิทัล” หมายถึง เทคโนโลยีที่ใช้วิธีการนำสัญลักษณ์ศูนย์และหนึ่ง หรือสัญลักษณ์อื่น มาแทนค่าสิ่งทั้งปวง เพื่อใช้สร้างหรือก่อให้เกิดระบบต่าง ๆ เพื่อให้มนุษย์ใช้ประโยชน์

“พอร์ต” (Port) หมายถึง ช่องสัญญาณบนอุปกรณ์เครือข่าย เช่น บนสวิทช์ หรือเร้าเต้อร์ โดยทั่วไป ช่องสัญญาณนี้สามารถใช้ในการติดต่อสื่อสารข้อมูลกับเครือข่าย คอมพิวเตอร์ และอุปกรณ์เครือข่ายต่าง ๆ

“โพรโทคอล” (Protocol) หมายถึง ข้อกำหนดหรือข้อตกลงในการสื่อสารระหว่างเครื่องคอมพิวเตอร์หรือการสื่อสารในระบบเครือข่าย

“โดเมนเนม” (Domain name) หมายถึง ชื่อที่ใช้ในการอ้างอิงเพื่อไปยังเว็บไซต์ต่าง ๆ ที่อยู่บนเครือข่ายอินเทอร์เน็ต ทั้งในการเข้าชมผ่านบราวเซอร์ของผู้ใช้ทั่วไป รวมไปถึงผู้ดูแลระบบโดเมนเนม ซึ่งเครื่องคอมพิวเตอร์ที่ทำหน้าที่เผยแพร่เว็บไซต์ จะมีโดนเมนเนมเฉพาะ ไม่ซ้ำกับใคร

“โดเมนย่อย” (Sub domain) หมายถึง ชื่อเว็บไซต์ย่อยของเว็บไซต์หลัก

“เว็บเซิร์ฟเวอร์” (Web server) หมายถึง เครื่องคอมพิวเตอร์ ที่ติดตั้งโปรแกรมคอมพิวเตอร์ซึ่งทำหน้าที่ให้บริการข้อมูล แก่ Client หรือเครื่องคอมพิวเตอร์ที่ขอรับบริการ ในรูปแบบ สื่อผสม ผ่านระบบเครือข่าย โดยสามารถแสดงผล ผ่านโปรแกรมเว็บบราวเซอร์

“ข้อมูลจราจรคอมพิวเตอร์” (Log file) หมายถึง ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง วันที่ ปริมาณ ระยะเวลา ชนิดของบริการหรืออื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น ๆ

“IP” (Internet protocol) หมายถึง มาตรฐานหรือข้อกำหนดที่สร้างขึ้นเพื่อการติดต่อสื่อสารระหว่างเครื่องคอมพิวเตอร์ในเครือข่ายคอมพิวเตอร์

“IP address” หมายถึง หมายเลขประจำเครื่องของเครื่องคอมพิวเตอร์แต่ละเครื่อง

“VPN” (Virtual Private Network) การเข้ารหัสลับ เพื่อให้สามารถรับ-ส่งข้อมูลได้ปลอดภัยมากขึ้น และสามารถเชื่อมต่อกับเซิร์ฟเวอร์/อุปกรณ์ที่อยู่ใน VPN เดียวกันได้สะดวกขึ้น

“SSL” (Secure Socket Layer) หมายถึง เทคโนโลยีรักษาความปลอดภัยสำหรับการเข้ารหัสลับ ระหว่างผู้ใช้งานอินเทอร์เน็ตและเซิร์ฟเวอร์ โดย SSL ถือเป็นมาตรฐานความปลอดภัยที่ได้รับความนิยม และมีการใช้งานทั่วโลก เพื่อป้องกันการถูกดักจับข้อมูล (Sniffer) บนโครงข่ายอินเทอร์เน็ต

“TLS” (Transport Layer Security) หมายถึง เทคโนโลยีการเข้ารหัสลับ เพื่อเพิ่มความปลอดภัยในการสื่อสารหรือส่งข้อมูลบนเครือข่ายอินเทอร์เน็ต ระหว่างเครื่องเซิร์ฟเวอร์กับเว็บเบราว์เซอร์หรือ Application ที่ใช้งาน ซึ่งพัฒนาต่อมาจาก Secure Sockets Layer (SSL)

“NAT” (Network Address Translation) หมายถึง วิธีการหนึ่งในการแปลงและแปล IP Address ของระบบเครือข่ายภายใน ให้เป็น IP Address สำหรับสื่อสารบนอินเทอร์เน็ต

“Source code” หมายถึง คำสั่งหรือโค้ดในโปรแกรม ซึ่งเขียนด้วยภาษาคอมพิวเตอร์ภาษาต่าง ๆ เช่น ภาษาซี (C) ภาษาจาวา (Java) ภาษาพีเอชพี (PHP) ภาษาปาสคาล (Pascal) และอื่น ๆ

“LCD” (Liquid Crystal Display) หมายถึง หน้าจอแสดงผลแบบดิจิทัล ที่ใช้วัสดุที่มีลักษณะเป็นของเหลวแทนการใช้หลอดภาพแบบเก่า

“จดหมายอิเล็กทรอนิกส์” (E-mail) หมายถึง จดหมายที่มีการรับส่งข้อความหรือข่าวสารระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และระบบเครือข่ายที่เชื่อมโยงถึงกัน

“สื่อสังคมออนไลน์” (Social Media and Social network) หมายถึง สื่อดิจิทัลที่เป็นเครื่องมือในการปฏิบัติการทางสังคม (Social Tool) หรือที่ใช้เผยแพร่ข้อมูลและแสดงความคิดเห็นบนโลกออนไลน์ เพื่อใช้สื่อสารระหว่างกันในเครือข่ายทางสังคม (Social Network) ผ่านทางเว็บไซต์และโปรแกรมประยุกต์บนสื่อใด ๆ ที่มีการเชื่อมต่อกับอินเทอร์เน็ต โดยเน้นให้ผู้ใช้ทั้งที่เป็นผู้ส่งสารและผู้รับสารมีส่วนร่วม (Collaborative) อย่างสร้างสรรค์ ในการผลิตเนื้อหาขึ้นเอง (User-Generate Content: UGC) ในรูปของข้อมูล ภาพ และเสียง

“ความเสี่ยง” (Risk) หมายถึง เหตุการณ์หรือการกระทำใด ๆ ที่อาจเกิดขึ้นภายใต้สถานการณ์ที่ไม่แน่นอน และจะส่งผลกระทบ สร้างความเสียหาย ความล้มเหลว หรือลดโอกาสที่จะบรรลุความสำเร็จต่อการบรรลุเป้าหมายและวัตถุประสงค์ ทั้งในระดับองค์กร ระดับหน่วยงาน และระดับบุคคล

“การบริหารความเสี่ยง” (Risk Management) หมายถึง การบริหารปัจจัยและควบคุมกิจกรรม รวมทั้งกระบวนการดำเนินงานต่าง ๆ โดยลดมูลเหตุแต่ละโอกาสจากการคาดการณ์และลดผลเสียที่อาจเกิดขึ้นจากความไม่แน่นอน ที่องค์กรจะเกิดความเสียหาย ให้ระดับของความเสียหายและขนาดของความเสียหายที่จะเกิดขึ้นในอนาคตอยู่ในระดับที่องค์กรยอมรับได้

“วิทยาการเข้ารหัสลับ” (Cryptography) หมายถึง การแปลงข้อความหรือข้อมูลอิเล็กทรอนิกส์จากรูปแบบที่อ่านได้ ให้อยู่ในรูปแบบที่อ่านไม่ได้ ด้วยการเข้ารหัสลับ (Encryption) ทำให้ข้อมูลนั้นเป็นความลับ ซึ่งผู้ที่มีสิทธิเท่านั้นจะสามารถอ่านข้อมูลนั้นได้ด้วยการถอดรหัสลับ (Decryption)

“การเข้าสู่ระบบจากระยะไกล” (Remote access) หมายถึง วิธีการเข้าถึงคอมพิวเตอร์และเครือข่ายจากระยะทางไกล ซึ่งทำให้ผู้ใช้สามารถเข้าควบคุมเครื่องคอมพิวเตอร์เป้าหมายได้เหมือนกับนั่งทำงานอยู่ที่หน้าเครื่องเอง ไม่ว่าจะเป็นการจัดการไฟล์ต่าง ๆ ใช้งานโปรแกรม หรือแม้กระทั่งการพิมพ์งานก็สามารถทำได้ผ่านทางเครือข่ายอินเทอร์เน็ต

“การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ” หมายถึง การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

“ความมั่นคงปลอดภัยด้านสารสนเทศ” (Information security) หมายถึง การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (authenticity) ความรับผิด (accountability) การห้ามปฏิเสธความรับผิด (non-repudiation) และความน่าเชื่อถือ (reliability)

“การรักษาความมั่นคงปลอดภัยด้านสารสนเทศ” หมายถึง การป้องกันอันตรายใด ๆ ที่อาจเกิดกับสารสนเทศและระบบสารสนเทศของสำนักงาน จากการเข้าถึง ใช้ เปิดเผย เปลี่ยนแปลงแก้ไข ทำให้สูญหาย เสียหาย หรือถูกทำลาย เป็นต้น ทั้งที่เกิดจากความรู้เท่าไม่ถึงการณ์ ความประมาทเลินเล่อ หรือการโจมตีจากผู้ไม่ประสงค์ดี

“เหตุการณ์ด้านความมั่นคงปลอดภัย” (Information security event) หมายถึง กรณีที่ระบุการเกิดเหตุการณ์ สภาพของการบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืน

นโยบายด้านความมั่นคงปลอดภัย หรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

“สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด” (information security incident) หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (unwanted or unexpected) ซึ่งอาจทำให้ระบบของสำนักงานถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

ส่วนที่ ๑
แนวปฏิบัติในการควบคุมการเข้าถึงและการใช้งานสารสนเทศ

วัตถุประสงค์

๑. เพื่อควบคุมการเข้าถึงและการใช้งานสารสนเทศของสำนักงานให้เป็นไปอย่างมีประสิทธิภาพและปลอดภัย

๒. เพื่อให้บุคลากรของสำนักงานและผู้ที่เกี่ยวข้อง ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงาน

ผู้รับผิดชอบ

๑. กองติดตามประเมินผลสิ่งแวดล้อม/กลุ่มงานระบบฐานข้อมูลและเทคโนโลยีสารสนเทศ
๒. ผู้ดูแลระบบสารสนเทศ
๓. ผู้ดูแลระบบ
๔. ผู้ใช้งาน

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชั่น ๒.๕) ประจำปี พ.ศ. ๒๕๕๐ ของศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕

แนวปฏิบัติ

การควบคุมการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Business requirements for access control) มีข้อปฏิบัติ ๒ ส่วน ประกอบด้วย การควบคุมการเข้าถึงและการใช้งานสารสนเทศ (Acess control) รวมทั้งการปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจ และข้อกำหนดด้านความมั่นคงปลอดภัย โดยมีแนวปฏิบัติดังนี้

๑. การควบคุมการเข้าถึงและใช้งานสารสนเทศ (Access control) เพื่อควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูลของสำนักงาน ให้มีความมั่นคงและปลอดภัย มีข้อปฏิบัติดังนี้

๑.๑ ผู้ดูแลระบบสารสนเทศจัดทำบัญชีรายการทรัพย์สินสารสนเทศและระบบสารสนเทศของสำนักงาน โดยระบุหน่วยงานเจ้าของข้อมูลและผู้ดูแลระบบ รวมทั้งสถานที่จัดเก็บฐานข้อมูลและระบบสารสนเทศแต่ละระบบ

๑.๒ ผู้ดูแลระบบสารสนเทศและผู้ดูแลระบบของหน่วยงานภายในสำนักงาน กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสนเทศของสำนักงาน ได้แก่

๑) กำหนดสิทธิของกลุ่มผู้ใช้งานแต่ละกลุ่ม ได้แก่
- สิทธิอ่านอย่างเดียว (Read-only)
- สิทธิเพิ่มข้อมูล (Create)

- สิทธิแก้ไขข้อมูล (Edit)
- สิทธิลบข้อมูล (Delete)
- สิทธิอนุมัติ/อนุญาต (Approve/Authorize)

๒) ผู้ดูแลระบบสารสนเทศและผู้ดูแลระบบ มีแนวทางในการบริหารจัดการสิทธิในการเข้าถึงระบบงานของผู้ใช้งาน ดังนี้

- กำหนดให้บุคลากรใหม่ต้องขออนุมัติเข้าใช้งานระบบงานภายในสำนักงาน โดยต้องกรอกข้อมูลเพื่อขออนุญาตใช้งาน ตามแบบฟอร์มที่กลุ่มงานระบบฐานข้อมูลและเทคโนโลยีสารสนเทศกำหนด
- สร้างบัญชีผู้ใช้งานและรหัสผ่าน เพื่อใช้เป็นข้อมูลยืนยันตัวตนของผู้ใช้งาน โดยดำเนินการตามแนวปฏิบัติในการตั้งและการใช้งานรหัสผ่าน
- จัดเก็บข้อมูลการขออนุญาตใช้งานของผู้ใช้งานแต่ละคน เพื่อใช้ในการอ้างอิงหรือตรวจสอบในภายหลัง
- กำหนดให้มีการถอดถอนหรือเปลี่ยนแปลงสิทธิการเข้าถึงระบบงาน เมื่อผู้ใช้งานมีการลาออก เปลี่ยนแปลง โอน ย้าย หรือเกษียณอายุ
- กำหนดให้มีการทบทวนบัญชีผู้ใช้งานของระบบต่าง ๆ อย่างสม่ำเสมอ เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต

๓) การกำหนดเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง การกำหนดสิทธิ หรือการมอบอำนาจและการระงับสิทธิ ให้ดำเนินการตามแนวปฏิบัติในการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User access management) ที่กำหนดไว้

๑.๓ กำหนดสิทธิในการผ่านเข้าสู่ระบบสารสนเทศ กรณีการเข้าถึงระบบสารสนเทศจากผู้พัฒนาระบบ ผู้ดูแลเครือข่าย หรือหน่วยงานภายนอก เพื่อดำเนินการใด ๆ จะต้องได้รับอนุญาตจากผู้อำนวยการกลุ่มงานระบบฐานข้อมูลและเทคโนโลยีสารสนเทศก่อนเข้าดำเนินการทุกครั้ง และหลังจากดำเนินการเสร็จสิ้นจะต้องยกเลิกสิทธินั้นทันที และหากการดำเนินการดังกล่าวส่งผลกระทบต่อระบบ ผู้ดำเนินการจะต้องเป็นผู้รับผิดชอบ

๑.๔ การกำหนดระยะเวลาในการเข้าถึงข้อมูลและระบบสารสนเทศของสำนักงาน แบ่งออกเป็น

๑) ข้อมูลและสารสนเทศที่เผยแพร่บนเว็บไซต์และระบบสารสนเทศทั่วไปของสำนักงาน สามารถเข้าถึงได้ตลอด ๒๔ ชั่วโมง

๒) ข้อมูลและสารสนเทศที่เป็นเอกสารของสำนักงาน สามารถเข้าถึงได้ในช่วงวันและเวลาราชการ คือ วันจันทร์-ศุกร์ ระหว่างเวลา ๐๘.๓๐-๑๖.๓๐ น. หรือตามความจำเป็น โดยต้องได้รับอนุญาตจากผู้บังคับบัญชาเป็นกรณีไป

๓) ระบบงานภายใน (Back Office) สำหรับผู้ใช้งานภายในสำนักงาน สามารถเข้าถึงได้ตลอด ๒๔ ชั่วโมง โดยผู้ใช้งานต้องลงชื่อเข้าใช้งานและปฏิบัติตามแนวทางที่ผู้ดูแลระบบสารสนเทศของสำนักงานกำหนด

๑.๕ ช่องทางในการเข้าถึงข้อมูลและระบบสารสนเทศของสำนักงาน กำหนดให้สามารถเข้าถึงได้ทั้งจากภายในและภายนอกสำนักงาน ทั้งโดยการติดต่อด้วยตนเอง การทำหนังสือเป็นลายลักษณ์อักษร และการเข้าถึงผ่านทางเว็บไซต์หรือโมบายแอปพลิเคชันของสำนักงาน เป็นต้น

๒. กำหนดให้มีการปรับปรุงการควบคุมการเข้าถึงและใช้งานสารสนเทศ (Access control) ให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจ และข้อกำหนดด้านความมั่นคงปลอดภัยในการเข้าถึงและใช้งานสารสนเทศ

ส่วนที่ ๒
แนวปฏิบัติในการบริหารจัดการข้อมูลตามระดับชั้นความลับ

วัตถุประสงค์

เพื่อให้การบริหารจัดการข้อมูลในแต่ละระดับชั้นความลับของสำนักงานเป็นไปอย่างมีประสิทธิภาพและปลอดภัย

ผู้รับผิดชอบ

๑. กองติดตามประเมินผลสิ่งแวดล้อม/กลุ่มงานระบบฐานข้อมูลและเทคโนโลยีสารสนเทศ
๒. ผู้ดูแลระบบสารสนเทศ
๓. ผู้ดูแลระบบ
๔. ผู้ใช้งาน

อ้างอิงมาตรฐาน

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓

ระเบียบว่าด้วยการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔

ระเบียบว่าด้วยการรักษาความลับของทางราชการ (ฉบับที่ ๒) พ.ศ. ๒๕๖๑

นโยบายข้อมูลสำนักงานนโยบายและแผนทรัพยากรธรรมชาติและสิ่งแวดล้อม

แนวปฏิบัติ

การกำหนดเกี่ยวกับข้อมูล ให้ปฏิบัติตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐ ระเบียบว่าด้วยการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ ระเบียบว่าด้วยการรักษาความลับของทางราชการ (ฉบับที่ ๒) พ.ศ. ๒๕๖๑ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และระเบียบอื่นที่เกี่ยวข้อง รวมทั้งนโยบายข้อมูลของสำนักงาน โดยมีแนวปฏิบัติดังนี้

๑. การกำหนดประเภทข้อมูลของสำนักงาน แบ่งออกเป็น ๒ ลักษณะ ดังนี้

๑.๑ ประเภทของข้อมูลแบ่งตามวัตถุประสงค์ของการใช้งาน เป็น ๓ ประเภท คือ

๑) ข้อมูลเพื่อการบริหาร เช่น ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์ คำรับรองการปฏิบัติราชการ ข้อมูลบุคลากร งบประมาณ การเงินและบัญชี เป็นต้น

๒) ข้อมูลเพื่อสนับสนุนการดำเนินงานตามพันธกิจและยุทธศาสตร์ของสำนักงานให้บรรลุเป้าหมาย เช่น กฎหมาย ระเบียบ การใช้จ่ายงบประมาณ เป็นต้น

๓) ข้อมูลเพื่อการบริการ เช่น ข้อมูลวิชาการและองค์ความรู้

๑.๒ ประเภทของข้อมูลแบ่งตามลักษณะของข้อมูล เป็น ๔ ประเภท คือ

๑) ข้อมูลสาธารณะ หมายถึง ข้อมูลที่สามารถเปิดเผยได้ สามารถนำไปใช้ได้อย่างอิสระ ไม่ว่าจะเป็นข้อมูลข่าวสาร ข้อมูลอิเล็กทรอนิกส์ เป็นต้น

๒) ข้อมูลส่วนบุคคล หมายถึง ข้อมูลเกี่ยวกับสิ่งเฉพาะตัวของบุคคล ที่ทำให้สามารถระบุตัวหรือรู้ตัวของบุคคลนั้น ๆ ได้ ไม่ว่าจะเป็นข้อมูลการศึกษา ประวัติ สุขภาพ ลายพิมพ์นิ้วมือ เป็นต้น

๓) ข้อมูลลับของราชการ หมายถึง ข้อมูลที่อยู่ในความครอบครองหรือควบคุมดูแลของหน่วยงานของรัฐที่มีคำสั่งไม่ให้มีการเปิดเผย และมีการกำหนดชั้นความลับของข้อมูล

๔) ข้อมูลความมั่นคง หมายถึง ข้อมูลเกี่ยวกับความมั่นคงของรัฐที่ทำให้เกิดความสงบเรียบร้อย การมีเสถียรภาพเป็นปึกแผ่น ปลอดภัยจากภัยคุกคาม เป็นต้น

๒. การกำหนดระดับความสำคัญของข้อมูล เจ้าของข้อมูลต้องกำหนดระดับความสำคัญของข้อมูล โดยแบ่งออกเป็น ๓ ระดับ คือ

๒.๑ ข้อมูลที่มีระดับความสำคัญมาก

๒.๒ ข้อมูลที่มีระดับความสำคัญปานกลาง

๒.๓ ข้อมูลที่มีระดับความสำคัญน้อย

๓. การกำหนดลำดับชั้นความลับของข้อมูล แบ่งตามระเบียบว่าด้วยการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ ออกเป็น ๓ ระดับ คือ

๓.๑ ลับที่สุด (Top secret) หมายถึง ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วน จะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งภาครัฐร้ายแรงที่สุด

๓.๒ ลับมาก (Secret) หมายถึง ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วน จะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรง

๓.๓ ลับ (Confidential) หมายถึง ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วน จะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐ

๔. การกำหนดให้ข้อมูลข่าวสารอยู่ในชั้นความลับใด ให้เจ้าของข้อมูลพิจารณาถึงองค์ประกอบอย่างน้อยดังต่อไปนี้

๔.๑ ความสำคัญของเนื้อหา เช่น ข้อมูลที่เป็นประโยชน์ต่อสาธารณะ หรือข้อมูลที่เกี่ยวข้องกับบุคคล

๔.๒ แหล่งที่มาของข้อมูลข่าวสาร เช่น มาจากเอกสารลับ หรือเอกสารที่เผยแพร่ต่อสาธารณะ

๔.๓ วิธีการนำไปใช้ประโยชน์ เช่น สามารถนำไปใช้ในเชิงพาณิชย์ได้หรือไม่

๔.๔ จำนวนบุคคลที่ควรรับทราบ เช่น ควรรับทราบเฉพาะผู้มีส่วนเกี่ยวข้อง หรือสามารถเผยแพร่แก่คนทั่วไปได้

๔.๕ ผลกระทบหากมีการเปิดเผย เช่น อาจส่งผลกระทบต่อการปฏิบัติงานของสำนักงาน หรือเกิดความเสียหายต่อบุคคล รวมถึงผลกระทบที่อาจเกิดขึ้นต่อรัฐ และความมั่นคงของประเทศ

๔.๖ หน่วยงานของรัฐที่รับผิดชอบในฐานะเจ้าของเรื่องหรือผู้อนุมัติ เช่น หน่วยงานทางด้านความมั่นคง หรือหน่วยงานทั่วไป

๕. การกำหนดระดับชั้นการเข้าถึงข้อมูล แบ่งออกเป็น ๓ ระดับ คือ

๕.๑ ข้อมูลที่สามารถเข้าถึงได้ทุกกลุ่มผู้ใช้งาน หมายถึง ข้อมูลพื้นฐานที่ผู้ใช้งานได้รับอนุญาตจากเจ้าหน้าที่รับผิดชอบข้อมูลและระบบงานในการใช้งาน

๕.๒ ข้อมูลที่สามารถเข้าถึงได้เฉพาะผู้ใช้งานที่ได้รับอนุมัติสิทธิ หมายถึง ข้อมูลที่ผู้ใช้งานได้รับอนุญาตจากเจ้าหน้าที่ที่รับผิดชอบข้อมูลและผู้ดูแลระบบได้ตามความจำเป็นต่อการใช้งาน

๕.๓ ข้อมูลที่สามารถเข้าถึงได้เฉพาะผู้มีสิทธิสูงสุดในการบริหารจัดการระบบสารสนเทศ หมายถึง ข้อมูลที่สามารถเข้าถึงได้เฉพาะผู้ดูแลระบบสารสนเทศ

๖. การดำเนินการใด ๆ ที่เกี่ยวกับข้อมูลส่วนบุคคล ให้ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของสำนักงาน

๗. เอกสารที่เป็นความลับหรือมีระดับความสำคัญซึ่งพิมพ์ออกมาจากเครื่องพิมพ์ ให้ปฏิบัติตามระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ และระเบียบว่าด้วยการรักษาความลับของทางราชการ (ฉบับที่ ๒) พ.ศ. ๒๕๖๑ และระเบียบอื่น ๆ ที่เกี่ยวข้อง ดังนี้

๗.๑ จัดหมวดหมู่เอกสารที่เป็นความลับหรือที่มีระดับความสำคัญสูงไว้ต่างหาก

๗.๒ จัดเก็บและกำหนดวิธีการป้องกันที่มีความปลอดภัยอย่างเพียงพอ

๗.๓ การสำเนาเอกสารที่เป็นความลับหรือเอกสารที่มีระดับความสำคัญสูงต้องได้รับอนุญาตจากผู้เป็นเจ้าของ

๗.๔ ระมัดระวังการกระจายหรือแจกจ่ายเอกสารที่เป็นความลับของสำนักงานไปยังกลุ่มผู้รับที่มีความจำเป็นต้องรับรู้เท่านั้น

๗.๕ ตรวจสอบความถูกต้องของเอกสารก่อนนำไปใช้งาน

๗.๖ ให้ทำลายเอกสารที่เป็นความลับหรือมีระดับความสำคัญสูงเมื่อหมดความจำเป็นในการใช้งาน

๘. การทำลายสื่อบันทึกข้อมูลและข้อมูลอิเล็กทรอนิกส์ เจ้าของข้อมูลต้องปฏิบัติตามแนวทางดังนี้

๘.๑ ต้องทำการล้างข้อมูลที่บันทึกอยู่ในฮาร์ดดิสก์หรือสื่อบันทึกข้อมูล ก่อนการส่งซ่อมหรือเปลี่ยนอุปกรณ์

๘.๒ ต้องทำการลบข้อมูลที่บันทึกอยู่ในฮาร์ดดิสก์หรือสื่อบันทึกข้อมูล ก่อนทำการทำลายหรือจำหน่าย

๘.๓ ต้องทำการฟอร์แมตฮาร์ดดิสก์ เพื่อป้องกันการกู้คืนข้อมูลในฮาร์ดดิสก์ ตามมาตรฐานการทำลายข้อมูลบนฮาร์ดดิสก์ของกระทรวงกลาโหมสหรัฐอเมริกา DOD ๕๒๒๐.๒๒-M (ซึ่งมีการเขียนทับข้อมูลเดิมเป็นจำนวนหลายรอบ)

๘.๔ ลบข้อมูลการดำเนินงานที่ไม่ได้ใช้งานแล้วออกจากฐานข้อมูล และสำรองข้อมูล และจัดเก็บไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล

๘.๕ ต้องได้รับความเห็นชอบจากผู้บังคับบัญชาในการทำลายสื่อบันทึกข้อมูล และเจ้าของข้อมูลในการลบข้อมูลอิเล็กทรอนิกส์ออกจากฐานข้อมูล

ส่วนที่ ๓
แนวปฏิบัติในการบริหารจัดการการเข้าถึงของผู้ใช้งาน

วัตถุประสงค์

เพื่อควบคุมการเข้าถึงระบบสารสนเทศของผู้ใช้งานให้เป็นไปอย่างมีประสิทธิภาพและปลอดภัย

ผู้รับผิดชอบ

๑. กองติดตามประเมินผลสิ่งแวดล้อม/กลุ่มงานระบบฐานข้อมูลและเทคโนโลยีสารสนเทศ
๒. ผู้ดูแลระบบสารสนเทศ
๓. ผู้ดูแลระบบ
๔. ผู้ใช้งาน

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชั่น ๒.๕) ประจำปี พ.ศ. ๒๕๕๐ ของศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕

แนวปฏิบัติ

การควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว และผ่านการฝึกอบรมหลักสูตรการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (Information security awareness training) เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต ผู้ดูแลระบบสารสนเทศ และผู้ดูแลระบบ ต้องปฏิบัติอย่างน้อยดังนี้

๑. จัดฝึกอบรมเกี่ยวกับการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (Information security awareness training) เพื่อสร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ อย่างน้อยปีละ ๑ ครั้ง รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

๒. กำหนดขั้นตอนการปฏิบัติในการลงทะเบียนผู้ใช้งาน (User registration) ประกอบด้วย

๒.๑ จัดทำแบบฟอร์มการขอใช้งานระบบสารสนเทศ เพื่อให้ผู้ใช้งานกรอกข้อมูล เพื่อประกอบการพิจารณาอนุญาตของผู้อำนวยการกลุ่มงานระบบฐานข้อมูลและสารสนเทศให้ผู้ใช้งานเข้าถึงระบบสารสนเทศของสำนักงาน

๒.๒ กำหนดสิทธิในการใช้งาน รวมทั้งกำหนดบัญชีชื่อผู้ใช้งานเป็นรายบุคคล โดยจะต้องไม่มีบัญชีชื่อผู้ใช้งานที่ซ้ำซ้อนกัน

๒.๓ การกำหนดชื่อผู้ใช้ (username) จะกำหนดจากชื่อภาษาอังกฤษ หากซ้ำให้เพิ่ม มหัพภาค (.) และตามด้วยตัวอักษรแรกของนามสกุล หากซ้ำให้เพิ่มตัวอักษรที่สองหรือจนกว่าจะไม่ซ้ำกับชื่อผู้ใช้งานคนอื่น

๒.๔ จำกัดการใช้งานบัญชีผู้ใช้งานแบบกลุ่มภายใต้ชื่อบัญชีรายชื่อเดียวกัน และอนุญาตให้ใช้เท่าที่จำเป็น

๒.๕ ตรวจสอบและมอบหมายสิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ และ/หรือตามความจำเป็น

๒.๖ การอนุญาตในการเข้าถึงระบบสารสนเทศ จะต้องได้รับการพิจารณาอนุญาตจากผู้อำนวยการกลุ่มงานระบบฐานข้อมูลและเทคโนโลยีสารสนเทศ หรือผู้ดูแลระบบที่ได้รับมอบหมาย

๒.๗ เมื่อผู้ใช้งานลาออก เกษียณอายุราชการ โอน ย้าย เปลี่ยนแปลงสังกัด เปลี่ยนตำแหน่งงานภายในองค์กร หรือสิ้นสุดการจ้าง เป็นต้น ให้เพิกถอนการอนุญาตให้เข้าถึงระบบสารสนเทศและการตัดชื่อผู้ใช้งานดังกล่าวออกจากทะเบียนผู้ใช้งาน

๒.๘ มีการตรวจสอบการใช้งานของผู้ใช้งานอย่างสม่ำเสมอ เพื่อป้องกันมิให้มีการใช้งานระบบสารสนเทศผิดวัตถุประสงค์

๓. บริหารจัดการสิทธิของผู้ใช้งาน (User management) โดยแสดงรายละเอียดที่เกี่ยวกับการควบคุมและจำกัดสิทธิเพื่อให้สามารถเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นๆ ที่เกี่ยวข้องกับการเข้าถึง ดังนี้

๓.๑ มีการกำหนดระดับสิทธิในการเข้าถึงระบบสารสนเทศที่เหมาะสมตามหน้าที่ความรับผิดชอบและตามความจำเป็นในการใช้งาน

๓.๒ การมอบหมายสิทธิ ต้องสอดคล้องกับแนวปฏิบัติในการควบคุมการเข้าถึงและการใช้งานสารสนเทศ

๓.๓ มีการบันทึกและจัดเก็บข้อมูลการมอบหมายสิทธิให้แก่ผู้ใช้งาน

๔. การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User password management) โดยจัดทำกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม ดังนี้

๔.๑ มีขั้นตอนปฏิบัติสำหรับการตั้งหรือเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัย โดยกำหนดให้รหัสผ่านต้องมีมากกว่าหรือเท่ากับ ๘ ตัวอักษร โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวเลข และตัวอักขระพิเศษต่าง ๆ

๔.๒ การตั้งรหัสผ่านชั่วคราว ต้องยากต่อการเดา และต้องมีความแตกต่างกัน

๔.๓ ส่งมอบรหัสผ่าน (Password) ชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย โดยหลีกเลี่ยงการใช้บุคคลอื่น หรือการส่งจดหมายอิเล็กทรอนิกส์ (E-mail) ในการจัดส่งรหัสผ่าน และผู้ใช้งานควรตอบกลับทันทีหลังจากได้รับรหัสผ่าน

๔.๔ ผู้ใช้งานต้องเปลี่ยนรหัสผ่านโดยทันที เมื่อได้รับรหัสผ่านครั้งแรก หรือได้รับรหัสผ่านใหม่ และควรเปลี่ยนให้รหัสผ่านยากต่อการคาดเดา

๔.๕ เปลี่ยนรหัสผ่านทันทีหลังจากติดตั้งซอฟต์แวร์แล้ว

๔.๖ การเปลี่ยนรหัสผ่าน ต้องตรวจสอบบัญชีชื่อผู้ใช้งานและรหัสผ่านปัจจุบันให้ถูกต้อง ก่อนที่จะอนุญาตให้เปลี่ยนรหัสใหม่

๔.๗ ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

๕. การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of user access rights) ต้องมีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศและปรับปรุงบัญชีผู้ใช้งาน อย่างน้อยปีละ ๑ ครั้ง เพื่อป้องกันการเข้าถึงระบบสารสนเทศโดยไม่ได้รับอนุญาต โดยปฏิบัติตามแนวทางดังนี้

๕.๑ พิมพ์รายชื่อของผู้ที่ยังมีสิทธิในระบบแยกตามหน่วยงานภายในสำนักงาน

๕.๒ จัดส่งรายชื่อผู้ใช้งานให้กับผู้บังคับบัญชาของหน่วยงานภายในสำนักงาน เพื่อตรวจสอบว่ารายชื่อผู้ใช้งานมีการเปลี่ยนแปลงหรือไม่ หรือมีการเปลี่ยนแปลงแล้ว แต่ยังไม่ได้มีการแก้ไขสิทธิการเข้าถึงให้ถูกต้องหรือไม่

๕.๓ ผู้บังคับบัญชาของหน่วยงานภายในสำนักงานแจ้งกลับว่ามีรายชื่อใดที่ต้องดำเนินการแก้ไขให้ถูกต้อง

๕.๔ ดำเนินการแก้ไขข้อมูลสิทธิให้ถูกต้องตามที่ได้รับแจ้ง

ส่วนที่ ๔
แนวปฏิบัติในการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน

วัตถุประสงค์

เพื่อกำหนดหน้าที่ความรับผิดชอบในการใช้งานระบบสารสนเทศของผู้ใช้งานให้เป็นไปอย่างมีประสิทธิภาพและปลอดภัย

ผู้รับผิดชอบ

๑. กองติดตามประเมินผลสิ่งแวดล้อม/กลุ่มงานระบบฐานข้อมูลและเทคโนโลยีสารสนเทศ
๒. ผู้ดูแลระบบสารสนเทศ
๓. ผู้ดูแลระบบ
๔. ผู้ใช้งาน

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชั่น ๒.๕) ประจำปี พ.ศ. ๒๕๕๐ ของศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕

แนวปฏิบัติ

การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศ และการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ มีแนวปฏิบัติอย่างน้อยดังนี้

๑. การกำหนดแนวปฏิบัติในการใช้งานรหัสผ่าน (Password use) สำหรับผู้ใช้งาน เพื่อให้มีการกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ มีแนวปฏิบัติดังนี้

๑.๑ ผู้ใช้งานที่เป็นเจ้าของบัญชีผู้ใช้งาน (User Account) ต้องเป็นผู้รับผิดชอบในผลต่างๆ อันจะเกิดขึ้นจากการใช้บัญชีผู้ใช้บริการของเครื่องคอมพิวเตอร์และเครือข่าย เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

๑.๒ ผู้ใช้งานจะต้องเก็บรักษาบัญชีผู้ใช้งานไว้เป็นความลับและห้ามเปิดเผยต่อบุคคลอื่น ห้ามโอนจำหน่าย หรือจ่ายแจกให้แก่ผู้อื่น โดยมิได้รับอนุญาต

๑.๓ ผู้ใช้งานต้องเก็บรักษารหัสผ่านที่ได้รับให้เป็นความลับเฉพาะบุคคล ไม่เปิดเผยให้ผู้อื่นรับทราบ ทั้งรหัสผ่านของตนเองและของกลุ่ม

๑.๔ หลีกเลี่ยงการกำหนดรหัสผ่านส่วนบุคคล จากอักขระที่เรียงกัน กลุ่มคำที่เหมือนกัน หรือชื่อนามสกุลของตนเอง หรือบุคคลในครอบครัว หรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือคำศัพท์ที่ใช้ในพจนานุกรม

๑.๕ หลีกเลี่ยงการใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

๑.๖หลีกเลี่ยงการจดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

๑.๗ หลีกเลี่ยงการใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save password)

๑.๘ กรณีที่มีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่นเนื่องจากงาน หลังจากดำเนินการเรียบร้อยแล้ว ให้ทำการเปลี่ยนรหัสผ่านโดยทันที

๑.๙ ควรมีการเปลี่ยนรหัสผ่าน ทุก ๖ เดือน หรือเปลี่ยนรหัสผ่านทันที เมื่อทราบว่ารหัสผ่านถูกเปิดเผยหรือล่วงรู้

๒. การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ เพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของสำนักงานในขณะที่ไม่มีผู้ดูแล มีแนวปฏิบัติดังนี้

๒.๑ ผู้ดูแลระบบสร้างความตระหนักให้เกิดความเข้าใจถึงความสำคัญในการป้องกันการเข้าถึงอุปกรณ์ และผลกระทบที่อาจเกิดขึ้นจากการที่บุคคลอื่นเข้าใช้งาน

๒.๒ ผู้ใช้งานต้องออกจากระบบสารสนเทศทันทีที่เสร็จสิ้นการใช้งาน

๒.๓ ผู้ใช้งานต้องล็อคเครื่องคอมพิวเตอร์ เมื่อไม่ได้ถูกใช้งาน หรือปล่อยทิ้งไว้โดยไม่ได้ดูแลชั่วคราว

๒.๔ ผู้ใช้งานต้องตั้งค่าการใช้งานโปรแกรมรักษาจอภาพ (Screen Saver) เพื่อทำการล็อคหน้าจอภาพเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งาน ผู้ใช้งานต้องใส่รหัสผ่าน (Password) เพื่อเข้าใช้งาน

๒.๕ ให้ยุติหรือปิดหน้าจอการใช้งานระบบสารสนเทศโดยอัตโนมัติ หากไม่มีการใช้งานเกินระยะเวลาสูงสุดที่กำหนดไว้

๓. การควบคุมทรัพย์สินสารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear desk and clear screen policy) ต้องควบคุมไม่ให้ทรัพย์สินสารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์หรือสารสนเทศ อยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน มีแนวปฏิบัติดังนี้

๓.๑ การควบคุมทรัพย์สินสารสนเทศของสำนักงาน

๑) ดูแลทรัพย์สินสารสนเทศของสำนักงานให้อยู่ในสภาพปลอดภัยอยู่เสมอ

๒) ไม่ทิ้งหรือปล่อยทรัพย์สินสารสนเทศที่สำคัญไว้ในสถานที่ที่ไม่ปลอดภัย

๓) กรณีที่ต้องการนำทรัพย์สินสารสนเทศของสำนักงานออกจากพื้นที่ใช้งาน ต้องได้รับอนุมัติจากหัวหน้างานก่อนทุกครั้ง

๓.๒ ผู้ใช้งานต้องออกจากระบบสารสนเทศทุกครั้ง เมื่อว่างเว้นจากการใช้งาน เพื่อป้องกันบุคคลอื่นนำไปใช้ในทางที่ไม่เหมาะสม

๔. การจัดการข้อมูลที่เป็นความลับ ผู้ใช้งานอาจพิจารณานำวิทยาการเข้ารหัสลับ (Cryptography) มาใช้กับข้อมูลที่เป็นความลับที่อยู่ในรูปอิเล็กทรอนิกส์ โดยปฏิบัติให้สอดคล้องกับระเบียบว่าด้วยการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ และระเบียบว่าด้วยการรักษาความลับของทางราชการ (ฉบับที่ ๒) พ.ศ. ๒๕๖๑ และระเบียบอื่น ๆ ที่เกี่ยวข้อง ตัวอย่างเช่น การใช้โพรโทคอล TLS (Transport Layer Security) ในการส่งข้อมูลที่เป็นความลับผ่านเครือข่าย และการเข้ารหัสลับ โดยใช้มาตรฐาน AES (Advanced Encryption Standards) ในการจัดเก็บข้อมูลที่เป็นความลับ เป็นต้น

ส่วนที่ ๕
แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยทางด้านภายภาพและสิ่งแวดล้อม

วัตถุประสงค์

เพื่อให้ระบบสารสนเทศของสำนักงานมีความปลอดภัยทั้งทางด้านกายภาพและสิ่งแวดล้อม

ผู้รับผิดชอบ

๑. กองติดตามประเมินผลสิ่งแวดล้อม/กลุ่มงานระบบฐานข้อมูลและเทคโนโลยีสารสนเทศ

๒. ผู้ดูแลระบบสารสนเทศ

๓. ผู้ดูแลระบบ

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชั่น ๒.๕) ประจำปี พ.ศ. ๒๕๕๐ ของศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕

แนวปฏิบัติ

การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and environmental security) ของสำนักงาน มีแนวปฏิบัติดังนี้

๑. การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศในภาพรวมของสำนักงาน

๑.๑ การจัดการสภาพแวดล้อมทางกายภาพ

๑) จำแนกและกำหนดพื้นที่การใช้งานและสถานที่จัดเก็บอุปกรณ์ต่าง ๆ ที่เกี่ยวข้องกับระบบสารสนเทศและเครือข่าย

๒) จัดวางอุปกรณ์ในพื้นที่หรือบริเวณที่เหมาะสม เพื่อหลีกเลี่ยงการเข้าถึงพื้นที่ของระบบสารสนเทศ

๓) แยกเก็บอุปกรณ์ที่มีความสำคัญไว้ในที่ที่มีความปลอดภัย

๔) ให้มีการใช้ระบบสำรองไฟฟ้ากับเครื่องคอมพิวเตอร์และระบบสารสนเทศ เพื่อให้สามารถใช้งานได้ต่อเนื่องในกรณีที่อาจเกิดจากไฟฟ้าขัดข้อง (Power failure) และเพื่อป้องกันความเสียหายที่เกิดจากความไม่สม่ำเสมอของกระแสไฟฟ้า และต้องทดสอบระบบสำรองไฟฟ้าอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าอยู่ในสภาพพร้อมใช้งาน

๑.๒ การกำหนดบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย

๑) ให้กลุ่มงานระบบฐานข้อมูลและเทคโนโลยีสารสนเทศเป็นผู้กำหนดพื้นที่ผู้ใช้งาน พื้นที่ใช้งานระบบสารสนเทศให้ชัดเจน และจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้รับทราบทั่วกัน โดยการกำหนดพื้นที่ดังกล่าวแบ่งออกได้เป็นพื้นที่ทำงาน พื้นที่ติดตั้งและจัดเก็บอุปกรณ์ระบบสารสนเทศหรือระบบเครือข่าย พื้นที่ใช้งานระบบเครือข่ายไร้สาย เป็นต้น

๒) ให้กลุ่มงานระบบฐานข้อมูลและเทคโนโลยีสารสนเทศเป็นผู้กำหนดสิทธิในการเข้าถึงพื้นที่ใช้งานระบบสารสนเทศ

๓) ให้มีการทบทวนสิทธิการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญอย่างสม่ำเสมอ

๔) ให้ฝ่ายอาคารสถานที่จัดให้มีการรักษาความปลอดภัยของอาคาร ห้องควบคุมระบบเครือข่าย รวมทั้งอุปกรณ์เชื่อมโยงเครือข่ายภายในอาคาร เพื่อป้องกันการเข้าพื้นที่โดยไม่ได้รับอนุญาต การลักลอบก่อวินาศกรรม การโจรกรรม หรือการทำลายอุปกรณ์ ระบบประมวลผล ระบบฐานข้อมูล และระบบเครือข่าย

๑.๓ การเดินสายไฟ สายสื่อสาร และสายเคเบิ้ลอื่นๆ (cabling security)

๑) หลีกเลี่ยงการเดินสายสัญญาณเครือข่ายของสำนักงานในลักษณะที่ต้องผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกเข้าถึงได้

๒) ให้มีการร้อยท่อสายสัญญาณต่างๆ เพื่อป้องกันการดักจับสัญญาณ หรือการตัดสายสัญญาณเพื่อทำให้เกิดความเสียหาย

๓) ให้เดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซงหรือรบกวนของสัญญาณซึ่งกันและกัน

๔) ทำป้ายชื่อสำหรับสายสัญญาณและบนอุปกรณ์เพื่อป้องกันการตัดต่อสัญญาณผิดเส้น

๕) จัดทำผังสายสัญญาณสื่อสารต่าง ๆ ให้ครบถ้วนและถูกต้อง

๑.๔ การบำรุงรักษาอุปกรณ์ (Equipment maintenance)

๑) ให้มีการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่แนะนำโดยผู้ผลิต

๒) ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามที่ผู้ผลิตแนะนำอย่างเคร่งครัด

๓) จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้ง เพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง

๔) จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว

๕) ควบคุมและสอดส่องดูแลการปฏิบัติงานของผู้ให้บริการภายนอกที่มาทำการบำรุงรักษาอุปกรณ์ภายในสำนักงาน

๖) จัดให้มีการอนุมัติสิทธิการเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญโดยผู้รับจ้างให้บริการบำรุงรักษาอุปกรณ์จากภายนอก เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๑.๕ การจำกัดบริเวณการเข้าถึง หรือการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอก (Public Access, Delivery and Loading Areas)

๑) จำกัดการเข้าถึงพื้นที่หรือบริเวณที่มีการส่งมอบหรือขนถ่ายผลิตภัณฑ์ เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

๒) จำกัดบุคลากรซึ่งสามารถเข้าถึงพื้นที่หรือบริเวณส่งมอบนั้น

๓) จัดพื้นที่หรือบริเวณส่งมอบไว้ต่างหาก เพื่อหลีกเลี่ยงการเข้าถึงพื้นที่อื่น ๆ ภายในสำนักงาน

๔) ต้องลงทะเบียนและตรวจนับผลิตภัณฑ์ที่ส่งมอบโดยผู้ขายหรือผู้ให้บริการภายนอกให้สอดคล้องกับระเบียบพัสดุ หรือขั้นตอนปฏิบัติสำหรับการบริหารจัดการทรัพย์สินขององค์กร

๒. การรักษาความปลอดภัยห้องคอมพิวเตอร์แม่ข่าย (Server room)

๒.๑ ติดตั้งระบบควบคุมการเข้า-ออกที่บริเวณประตูทางเข้า

๒.๒ ติดตั้งกล้องวงจรปิดเพื่อบันทึกเหตุการณ์ภายในห้องไว้ตลอดเวลา เพื่อตรวจสอบกรณีเกิดความผิดปกติ หรือเกิดเหตุการณ์ด้านความมั่นคงปลอดภัย

๒.๓ ห้ามนำอาหารและเครื่องดื่ม เข้าไปในบริเวณห้องคอมพิวเตอร์แม่ข่าย

๒.๔ มีระบบสนับสนุนการทำงานของระบบสารสนเทศอย่างเพียงพอ เช่น ระบบกระแสไฟฟ้าสำรอง และป้องกันอุปกรณ์ไฟฟ้าเสียหายจากการเกิดกระแสไฟฟ้าผิดปกติ ระบบปรับอากาศ ระบบระบายอากาศ ระบบควบคุมความชื้น และระบบดับเพลิง เป็นต้น และต้องตรวจสอบหรือทดสอบการทำงานของระบบสนับสนุนอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าระบบต่าง ๆ สามารถทำงานได้ตามปกติ และลดความเสี่ยงจากการทำงานของระบบล้มเหลว

๒.๕ กำหนดให้เฉพาะเจ้าหน้าที่กลุ่มงานระบบฐานข้อมูลและเทคโนโลยีสารสนเทศเท่านั้นที่มีสิทธิในการเข้า-ออก

๒.๖ ให้มีการทบทวนสิทธิการเข้าถึงพื้นที่ทุกครั้งที่มีการเปลี่ยนแปลงเจ้าหน้าที่ของกลุ่มงานระบบฐานข้อมูลและเทคโนโลยีสารสนเทศ

๒.๗ อนุญาตให้เฉพาะผู้มีสิทธิและความจำเป็นเข้าถึงพื้นที่ได้เท่านั้น และให้มีเจ้าหน้าที่ของกลุ่มงานระบบฐานข้อมูลและเทคโนโลยีสารสนเทศดูแลบุคคลภายนอก หรือผู้มาติดต่อทุกครั้งจนเสร็จสิ้นภารกิจ

๒.๘ จัดทำแบบฟอร์มเพื่อบันทึกการเข้า-ออก สำหรับบุคคลภายนอกหรือผู้มาติดต่อ และกรณีที่บุคคลภายนอกหรือผู้มาติดต่อ ต้องการนำเครื่องคอมพิวเตอร์หรืออุปกรณ์เครือข่ายเข้ามาใช้งาน ในบริเวณพื้นที่ ต้องบันทึกรายการอุปกรณ์ในแบบฟอร์มการเข้า-ออก ในด้วยทุกครั้ง

๓. การรักษาความมั่นคงปลอดภัยสำหรับห้องทำงานและทรัพย์สินอื่น ๆ

๓.๑ ผู้ใช้งานต้องระมัดระวัง และดูแลทรัพย์สินของสำนักงานที่ตนเองใช้งาน หรือถือครองเสมือนเป็นทรัพย์สินของตนเอง หากเกิดความสูญหาย หรือเสียหายโดยประมาทเลินเล่อ ต้องรับผิดชอบหรือชดใช้ต่อความเสียหายนั้น

๓.๒ ผู้ใช้งานต้องเก็บเอกสาร ข้อมูล หรือสื่อบันทึกข้อมูลสำคัญไว้ในที่ปลอดภัย เช่น ในตู้หรือโต๊ะที่มีสามารถล็อกได้ และแยกเอกสารสำคัญสำหรับทำลายไว้ต่างหาก เพื่อความปลอดภัยของทรัพย์สินราชการ

๓.๓ นำเอกสารออกจากเครื่องพิมพ์ทันทีที่พิมพ์งานเสร็จ

๓.๔ ต้องไม่ให้ผู้ที่ไม่ได้รับอนุญาตใช้อุปกรณ์คอมพิวเตอร์และสื่อสารต่าง ๆ โดยไม่ได้รับอนุญาต

ส่วนที่ ๖
แนวปฏิบัติในการควบคุมการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย

วัตถุประสงค์

๑. เพื่อป้องกันการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่ายของสำนักงานจากผู้ที่ไม่ได้รับอนุญาตและผู้ไม่ประสงค์ดี

๒. เพื่อให้เครื่องคอมพิวเตอร์แม่ข่ายของสำนักงานสามารถใช้งานได้อย่างปลอดภัย

ผู้รับผิดชอบ

๑. กองติดตามประเมินผลสิ่งแวดล้อม/กลุ่มงานระบบฐานข้อมูลและเทคโนโลยีสารสนเทศ

๒. ผู้ดูแลระบบสารสนเทศ

๓. ผู้ดูแลระบบ

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชั่น ๒.๕) ประจำปี พ.ศ. ๒๕๕๐ ของศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕

แนวปฏิบัติ

การควบคุมการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่ายของสำนักงานให้ปลอดภัยจากผู้ที่ไม่ได้รับอนุญาตและผู้ไม่ประสงค์ดี มีแนวปฏิบัติดังนี้

๑. การควบคุมการติดตั้งซอฟต์แวร์ลงไปยังระบบเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ

๑.๑ ให้กลุ่มงานระบบฐานข้อมูลและเทคโนโลยีสารสนเทศกำหนดมาตรการควบคุมการเข้า-ออกห้องควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server)

๑.๒ ผู้ใช้บริการจะนำเครื่องคอมพิวเตอร์และอุปกรณ์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์และระบบเครือข่ายของสำนักงาน ต้องได้รับอนุญาตจากผู้อำนวยการกลุ่มงานระบบฐานข้อมูลและเทคโนโลยีสารสนเทศ และต้องปฏิบัติตามนโยบายนี้โดยเคร่งครัด

๑.๓ การขออนุญาตใช้งานพื้นที่เว็บเซิร์ฟเวอร์ (Web Server) และชื่อโดเมนย่อย (Sub Domain Name) ที่สำนักงานรับผิดชอบอยู่ จะต้องทำหนังสือขออนุญาตต่อผู้อำนวยการกลุ่มงานระบบฐานข้อมูลและเทคโนโลยีสารสนเทศ และจะต้องไม่ติดตั้งโปรแกรมใด ๆ ที่ส่งผลกระทบต่อการทำงานของระบบและผู้ใช้บริการอื่น ๆ

๑.๔ ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใด ๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลัก โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบสารสนเทศ

๑.๕ ผู้ดูแลระบบสารสนเทศต้องควบคุมการเข้าถึงระบบเครือข่าย เพื่อบริหารจัดการระบบเครือข่ายได้อย่างมีประสิทธิภาพ ดังต่อไปนี้

๑) มีวิธีการจำกัดสิทธิการใช้งานเพื่อควบคุมผู้ใช้บริการให้สามารถใช้งานเฉพาะระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น

๒) มีวิธีการจำกัดเส้นทางการเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน

๓) กำหนดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่าย เพื่อไม่ให้ผู้ใช้บริการสามารถใช้เส้นทางอื่น ๆ ได้

๔) ระบบเครือข่ายทั้งหมดของสำนักงานที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกสำนักงานต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก

๕) ระบบเครือข่ายต้องติดตั้งระบบตรวจจับการบุกรุก (Intrusion Prevention System/ Intrusion Detection System) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของสำนักงานในลักษณะที่ผิดปกติ

๖) การเข้าสู่ระบบเครือข่ายภายในสำนักงาน โดยผ่านทางระบบอินเทอร์เน็ตต้องลงชื่อเข้า (Log in) โดยระบุชื่อผู้ใช้งานและรหัสผ่าน เพื่อพิสูจน์ยืนยันตัวตน (Authentication)

๗) เลขที่อยู่ไอพี (IP Address) ภายในของระบบเครือข่ายภายในของสำนักงาน จำเป็นต้องมีการป้องกันมิให้สำนักงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้

๘) จัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอก ที่สามารถระบุบนระบบเครือข่าย พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๙) การใช้เครื่องมือต่าง ๆ เพื่อการตรวจสอบระบบเครือข่าย ต้องได้รับการอนุมัติจากผู้ดูแลระบบสารสนเทศ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

๑.๖ ผู้ดูแลระบบสารสนเทศต้องบริหารควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server) และรับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย ในการกำหนดแก้ไข หรือเปลี่ยนแปลงค่าต่าง ๆ ของซอฟต์แวร์ระบบ (Systems Software)

๑.๗ ให้กลุ่มงานระบบฐานข้อมูลและเทคโนโลยีสารสนเทศกำหนดมาตรการควบคุมการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์ (Log) มีความถูกต้อง และสามารถระบุถึงตัวบุคคลได้ตามแนวทาง ดังต่อไปนี้

๑) จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วน ถูกต้อง แท้จริง และระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้และข้อมูลที่ใช้ในการจัดเก็บ ต้องกำหนดชั้นความลับในการเข้าถึงข้อมูลและผู้ดูแลระบบไม่ได้รับอนุญาตในการแก้ไขข้อมูลที่เก็บรักษาไว้ ยกเว้นผู้ตรวจสอบระบบสารสนเทศของสำนักงาน (Internal IT Auditor) หรือบุคคลที่สำนักงานมอบหมาย

๒) กำหนดให้มีการบันทึกการทำงานของระบบบันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุกเช่น บันทึกการเข้า-ออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน Command Line และ Firewall Log เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย ๙๐ วัน นับตั้งแต่การใช้บริการสิ้นสุดลง

๓) ตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานระบบอย่างสม่ำเสมอ

๔) ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่าง ๆ และจำกัดสิทธิการเข้าถึงบันทึกเหล่านั้น ให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

๑.๘ ให้กลุ่มงานระบบฐานข้อมูลและเทคโนโลยีสารสนเทศกำหนดมาตรการควบคุมการใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย เพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอก ตามแนวทางดังต่อไปนี้

๑) บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่ายของสำนักงาน จะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุญาตจากผู้อำนวยการกลุ่มงานระบบฐานข้อมูลและเทคโนโลยีสารสนเทศ

๒) ผู้ดูแลระบบควบคุมช่องทางหรือพอร์ต (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม ต้องไม่เปิด Port ที่ใช้ทิ้งเอาไว้โดยไม่จำเป็น และช่องทางดังกล่าวจะต้องตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้วโดยอัตโนมัติ และจะเปิดให้ใช้ได้ต่อเมื่อมีการร้องขอที่จำเป็นเท่านั้น

๓) วิธีการใด ๆ ที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้จากระยะไกล ต้องได้รับการอนุญาตจากผู้อำนวยการกลุ่มงานระบบฐานข้อมูลและเทคโนโลยีสารสนเทศ

๔) การเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องแสดงหลักฐาน ระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับสำนักงานอย่างเพียงพอ

๕) การเข้าใช้งานระบบต้องผ่านการพิสูจน์ตัวตนจากระบบของสำนักงาน

๖) การเข้าสู่ระบบต้องมีการใช้มาตรการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน เช่น VPN (Virtual Private Network) เป็นต้น

๗) ผู้ดูแลระบบ ต้องกำหนดให้ผู้ใช้งานสามารถเชื่อมต่อกับระบบโมเด็มได้เพียงหนึ่งการเชื่อมต่อในขณะเวลาเดียวกัน

๘) ผู้ดูแลระบบจะต้องกำหนดพอร์ต (Port) ที่ใช้ในการเข้าสู่ระบบ และจะต้องตรวจสอบและติดตามการใช้งานเป็นประจำอย่างน้อยเดือนละ ๑ ครั้ง

๑.๙ ผู้ดูแลระบบ (System Administrator) ป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นหมายเลข (IP Address) ภายในระบบงานเครือข่ายภายของสำนักงาน เพื่อป้องกันไม่ให้บุคคลภายนอกสามารถทราบข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายได้ โดยทำการแบ่งแยกเป็น Public IP Address และ Private IP Address เพื่อแยกเครือข่ายย่อย และมีการ NAT (Network Address Translation) เพื่อทำการแปลงหมายเลขเครือข่าย

๒. ให้มีการทบทวนการทำงานของระบบเทคโนโลยีสารสนเทศภายหลังจากเปลี่ยนแปลงระบบปฏิบัติการ โดยปฏิบัติดังนี้

๒.๑ แจ้งให้ผู้ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศได้รับทราบเกี่ยวกับการเปลี่ยนแปลงระบบปฏิบัติการเพื่อให้บุคคลเหล่านั้นมีเวลาเพียงพอในการดำเนินการทดสอบและทบทวนก่อนที่จะดำเนินการเปลี่ยนแปลงระบบปฏิบัติการ

๒.๒ พิจารณาวางแผนดำเนินการเปลี่ยนแปลงระบบปฏิบัติการของระบบเทคโนโลยีสารสนเทศ รวมทั้งวางแผนด้านงบประมาณที่จำเป็นต้องใช้ ในกรณีที่สำนักงานต้องเปลี่ยนไปใช้ระบบปฏิบัติการใหม่

๓. การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก

๓.๑ ควรจัดให้มีการควบคุมโครงการพัฒนาซอฟต์แวร์โดยผู้รับจ้างจากภายนอก

๓.๒ ให้ระบุว่าใครจะเป็นผู้มีสิทธิในทรัพย์สินทางปัญญาสำหรับซอร์สโค้ด (Source code) ในการพัฒนาซอฟต์แวร์โดยผู้รับจ้างให้บริการจากภายนอก

๓.๓ ให้กำหนดเรื่องการสงวนสิทธิที่จะตรวจสอบด้านคุณภาพและความถูกต้องของซอฟต์แวร์ที่จะมีการพัฒนาโดยผู้ให้บริการภายนอก โดยระบุไว้ในสัญญาจ้างที่ทำกับผู้ให้บริการภายนอกนั้น

๓.๔ ให้มีการตรวจสอบโปรแกรมไม่ประสงค์ดี ในซอฟต์แวร์ต่าง ๆ ที่จะทำการติดตั้งก่อนดำเนินการติดตั้ง

๔. มาตรการควบคุมช่องโหว่ทางเทคนิค

๔.๑ กำหนดให้มีการจัดทำบัญชีของระบบสารสนเทศ เพื่อใช้สำหรับกระบวนการบริหารจัดการช่องโหว่ของระบบเหล่านั้น ประกอบด้วย ชื่อซอฟต์แวร์และเวอร์ชันที่ใช้งาน สถานที่ที่ติดตั้ง เครื่องที่ติดตั้ง ผู้ผลิตซอฟต์แวร์ และข้อมูลสำหรับติดต่อผู้ผลิตหรือผู้พัฒนาซอฟต์แวร์นั้น

๔.๒ กำหนดให้มีการจัดการกับช่องโหว่สำคัญของระบบสารสนเทศอย่างเหมาะสมโดยทันที

๔.๓ กระบวนการบริหารจัดการช่องโหว่ของระบบเทคโนโลยีสารสนเทศ ให้ผู้ดูแลระบบดำเนินการ ดังนี้

๑) มีการเฝ้าระวังและติดตาม ประเมินความเสี่ยงสำหรับช่องโหว่ของระบบสารสนเทศ รวมทั้งการประสานงานเพื่อให้ผู้ที่เกี่ยวข้องดำเนินการแก้ไขช่องโหว่ตามความเหมาะสม

๒) ให้กำหนดแหล่งข้อมูลข่าวสารเพื่อใช้ในการติดตามช่องโหว่ของระบบสารสนเทศของสำนักงาน กำหนดให้ผู้ที่เกี่ยวข้องดำเนินการประเมินความเสี่ยงเมื่อได้รับแจ้งหรือทราบเกี่ยวกับช่องโหว่นั้น

๔.๔ ปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้ใช้งานได้อย่างจำกัดระยะเวลาเท่าที่จำเป็น โดยต้องได้รับการอนุญาตจากผู้รับผิดชอบเป็นลายลักษณ์อักษร

๕. การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ (Log) โดยจะต้องเก็บรักษาข้อมูลของผู้ใช้งานเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ใช้บริการนับตั้งแต่เริ่มใช้บริการและต้องเก็บรักษาไว้เป็นเวลาไม่น้อยกว่าเก้าสิบวันนับตั้งแต่การใช้งานสิ้นสุดลง การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ (Log) ต้องใช้วิธีการที่มั่นคงปลอดภัย ดังต่อไปนี้

๕.๑ เก็บในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วนถูกต้องแท้จริง และระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้

๕.๒ มีระบบการเก็บรักษาความลับของข้อมูลที่จัดเก็บ และกำหนดชั้นความลับในการเข้าถึงข้อมูลดังกล่าว เพื่อรักษาความน่าเชื่อถือของข้อมูล และไม่ให้ผู้ดูแลระบบสามารถแก้ไขข้อมูลที่เก็บรักษาไว้ เว้นแต่ผู้ที่กำหนดให้สามารถเข้าถึงข้อมูลดังกล่าวได้ เช่น ผู้ตรวจสอบระบบเทคโนโลยีสารสนเทศของสำนักงาน (Internal IT Auditor) หรือบุคคลที่สำนักงานมอบหมาย

๕.๓ ในการเก็บข้อมูลจราจรนั้น ต้องสามารถระบุรายละเอียดผู้ใช้บริการเป็นรายบุคคลได้

๕.๔ เพื่อให้ข้อมูลจราจรมีความถูกต้องและนำมาใช้ประโยชน์ได้จริงผู้ให้บริการต้องตั้งนาฬิกาของอุปกรณ์บริการทุกชนิดให้ตรงกับเวลาอ้างอิงสากล (Stratum 0) โดยผิดพลาดไม่เกิน ๑๐ มิลลิวินาที

ส่วนที่ ๗
แนวปฏิบัติในการควบคุมการเข้าถึงเครือข่าย

วัตถุประสงค์

๑. เพื่อป้องกันการเข้าถึงเครือข่ายจากผู้ที่ไม่ได้รับอนุญาตและผู้ไม่ประสงค์ดี

๒. เพื่อให้เครือข่ายของสำนักงานมีความปลอดภัยและสามารถใช้งานได้อย่างมีประสิทธิภาพและต่อเนื่อง

ผู้รับผิดชอบ

๑. กองติดตามประเมินผลสิ่งแวดล้อม/กลุ่มงานระบบฐานข้อมูลและเทคโนโลยีสารสนเทศ

๒. ผู้ดูแลระบบสารสนเทศ

๓. ผู้ดูแลระบบ

๔. ผู้ใช้งาน

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชั่น ๒.๕) ประจำปี พ.ศ. ๒๕๕๐ ของศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕

แนวปฏิบัติ

การควบคุมการเข้าถึงเครือข่าย (Network access control) เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต ผู้ดูแลระบบสารสนเทศและผู้ดูแลระบบของหน่วยงานในสำนักงาน มีแนวปฏิบัติอย่างน้อยดังนี้

๑. การใช้งานบริการเครือข่าย ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้เฉพาะบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น โดยมีแนวปฏิบัติดังนี้

๑.๑ การใช้งานระบบเครือข่าย

๑) ผู้ใช้งานต้องไม่ใช้ระบบเครือข่ายสำนักงาน เพื่อแสวงหาประโยชน์ทางธุรกิจส่วนตัว หรือกระทำการใด ๆ ที่เป็นการขัดต่อกฎหมายหรือศีลธรรมอันดี

๒) ผู้ใช้งานต้องไม่ละเมิดต่อผู้อื่น คือ ต้องไม่อ่าน เขียน ลบ เปลี่ยนแปลงหรือแก้ไขข้อมูลหรือข้อความใด ๆ ในส่วนที่ไม่ใช่ของตน โดยไม่ได้รับอนุญาต รวมถึงการเผยแพร่ข้อความใด ๆ ที่ก่อให้เกิดความเสียหายหรือเสื่อมเสียแก่ผู้อื่น

๓) ผู้ใช้งานต้องเก็บรักษาบัญชีผู้ใช้งานและรหัสผ่านเป็นการเฉพาะบุคคลเท่านั้น จะโอนหรือจ่ายแจกสิทธิให้ผู้อื่นไม่ได้ และผู้ใช้งานต้องรับผิดชอบผลต่าง ๆ อันอาจจะเกิดขึ้นรวมถึงผลเสียต่างๆ ที่เกิดจากบัญชีผู้ใช้งานนั้น ๆ เว้นแต่พิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของบุคคลอื่น

๔) ผู้ใช้งานต้องปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ และกฎระเบียบที่เกี่ยวข้องอย่างเคร่งครัด

๑.๒ การใช้งานระบบเครือข่ายไร้สาย

๑) ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายภายในของสำนักงาน ต้องทำการลงทะเบียนกับผู้ดูแลเครือข่าย และต้องได้รับอนุญาตจากผู้อำนวยการกลุ่มงานระบบฐานข้อมูลและเทคโนโลยีสารสนเทศหรือผู้ดูแลเครือข่ายที่ได้รับมอบหมาย

๒) ผู้ดูแลเครือข่ายต้องเปลี่ยนค่ารหัสผู้ใช้และรหัสผ่านในการเข้าตั้งค่าการทำงานของอุปกรณ์ไร้สายที่ติดตั้งมาจากผู้ผลิต เพื่อป้องกันการโจมตี

๓) ผู้ดูแลเครือข่ายควรใช้ซอฟต์แวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ

๔) ผู้ดูแลเครือข่ายควรเปลี่ยนค่าชื่อบัญชีรายชื่อและรหัสผ่านในการเข้าสู่ระบบ สำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สาย และควรจะเลือกใช้ชื่อบัญชีรายชื่อและรหัสผ่านที่คาดเดาได้ยาก เพื่อป้องกันผู้โจมตีไม่ให้สามารถเดา หรือเจาะรหัสได้โดยง่าย

๕) ควรตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ เพื่อตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยที่เกิดขึ้นในระบบเครือข่ายไร้สาย และเมื่อตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติ ให้รายงานต่อผู้อำนวยการกลุ่มงานระบบฐานข้อมูลและเทคโนโลยีสารสนเทศทราบโดยทันที

๒. การยืนยันตัวบุคคลสำหรับผู้ใช้งาน (User authentication) จะต้องมีข้อปฏิบัติหรือกระบวนการให้มีการยืนยันตัวตน (Authentication) ก่อนที่จะอนุญาตให้ผู้ใช้งานสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของสำนักงานได้ ดังนี้ โดยผู้ใช้งานต้องแสดงตัวตนด้วย ชื่อผู้ใช้งานและรหัสผ่าน หรือ MAC Address ของอุปกรณ์ ทุกครั้ง

๓. การระบุอุปกรณ์บนระบบเครือข่าย (Equipment identification in networks)

๓.๑ ผู้ดูแลเครือข่ายจัดทำบัญชีของเครื่องคอมพิวเตอร์และอุปกรณ์เครือข่ายที่เชื่อมต่อกับเครือข่าย ประกอบไปด้วย รายละเอียดเครื่องคอมพิวเตอร์หรืออุปกรณ์ IP Address, MAC Address สถานที่ติดตั้ง และหมายเลขโทรศัพท์ติดต่อ

๓.๒ การติดตั้งและเชื่อมต่ออุปกรณ์เครือข่ายจะต้องได้รับการอนุมัติจากผู้บังคับบัญชา และได้รับความเห็นชอบจากกลุ่มงานระบบฐานข้อมูลและเทคโนโลยีสารสนเทศก่อนดำเนินการทุกครั้ง

๓.๓ อุปกรณ์เครือข่ายต้องสามารถตรวจสอบ IP Address ของทั้งต้นทางและปลายทางได้

๓.๔ ผู้ขอใช้งานต้องทำหนังสือเป็นลายลักษณ์อักษรถึงผู้อำนวยการกลุ่มงานระบบฐานข้อมูลและเทคโนโลยีสารสนเทศ เรื่อง “การขอเชื่อมต่อเครือข่าย” และต้องได้รับการอนุมัติจากผู้บังคับบัญชาตามลำดับชั้น

๓.๕ ผู้ดูแลระบบสารสนเทศจัดทำแผนผังระบบเครือข่าย (Network Diagram) พร้อม IP Address และ MAC Address ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายใน เครือข่ายภายนอกและอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๔. การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote diagnostic and configuration port protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย

๔.๑ ผู้ดูแลระบบต้องกำหนดการเปิด–ปิด พอร์ตของอุปกรณ์เครือข่าย เพื่อควบคุมการเข้าถึงพอร์ตของอุปกรณ์เครือข่ายต่าง ๆ โดยจะปิดพอร์ตที่เสี่ยงที่จะก่อให้เกิดความเสียหายต่อระบบเครือข่าย

๔.๒ กำหนดบุคคลที่รับผิดชอบในการกำหนดแก้ไขหรือเปลี่ยนแปลงค่าตัวแปร (Parameter) ต่าง ๆ ของระบบเครือข่ายและอุปกรณ์ต่าง ๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจน และมีการทบทวนการกำหนดค่าตัวแปร (Parameter) ต่าง ๆ อย่างน้อยปีละ ๑ ครั้ง

๔.๓ บุคคลภายนอกที่เข้ามาติดต่อหรือเข้ามาดำเนินการใด ๆ ในห้องคอมพิวเตอร์แม่ข่าย ซึ่งควบคุมระบบเครือข่าย/ระบบสารสนเทศ จะต้องลงชื่อในแบบฟอร์มการเข้า-ออกพื้นที่ และได้รับการอนุมัติจากผู้อำนวยการกลุ่มงานระบบฐานข้อมูลและเทคโนโลยีสารสนเทศก่อน โดยต้องมีเจ้าหน้าที่กลุ่มงานระบบฐานข้อมูลและเทคโนโลยีสารสนเทศอยู่กับบุคคลที่มาติดต่อตลอดเวลา

๔.๔ บุคคลภายนอกที่เข้ามาดำเนินการบำรุงรักษา บริหารจัดการพอร์ตของอุปกรณ์เครือข่าย หรือบริหารจัดการผ่านระบบเครือข่าย ต้องได้รับการอนุมัติจากผู้อำนวยการกลุ่มงานระบบฐานข้อมูลและเทคโนโลยีสารสนเทศก่อนเข้าดำเนินการ

๔.๕ ให้ตรวจสอบและยกเลิกหรือปิดพอร์ตและบริการบนอุปกรณ์เครือข่ายที่ไม่มีความจำเป็นในการใช้งาน

๕. การแบ่งแยกเครือข่าย (Segregation in networks) ของสำนักงาน

๕.๑ แบ่งแยกเครือข่ายสำหรับกลุ่มผู้ใช้งาน ออกเป็น ๒ เครือข่าย คือ เครือข่ายสำหรับผู้ใช้งานภายใน และเครือข่ายสำหรับผู้ใช้งานภายนอก

๕.๒ พิจารณาแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศและกลุ่มของระบบสารสนเทศเพิ่มเติมตามความเหมาะสม

๖. การควบคุมการเชื่อมต่อทางเครือข่าย (Network connection control) ให้มีการควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างสำนักงาน ให้สอดคล้องกับแนวปฏิบัติในการควบคุมการเข้าถึง ดังนี้

๖.๑ ผู้ดูแลระบบตรวจสอบการเชื่อมต่อเครือข่าย โดยระบบเครือข่ายทั้งหมด ต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก เช่น Firewall หรืออุปกรณ์อื่น ๆ

๖.๒ ผู้ดูแลระบบต้องกำหนดสิทธิของผู้ใช้งานในการเชื่อมต่อเข้าสู่ระบบเครือข่าย

๖.๓ ผู้ดูแลระบบต้องระบุอุปกรณ์และเครื่องมือที่ใช้ควบคุมการเชื่อมต่อเครือข่าย

๖.๔ ห้ามมิให้มีการนำอุปกรณ์ที่ไม่ได้รับอนุญาตต่อเข้ากับระบบเครือข่าย

๖.๕ ผู้ดูแลระบบต้องควบคุมไม่ให้มีการเปิดให้บริการบนระบบเครือข่าย โดยไม่ได้รับอนุญาต

๖.๖ การเข้าสู่ระบบเครือข่ายไร้สาย ผู้ใช้งานต้องทำการลงทะเบียนกับผู้ดูแลระบบ และต้องได้รับการพิจารณาอนุญาตจากผู้อำนวยการระบบฐานข้อมูลและเทคโนโลยีสารสนเทศ ตามความจำเป็นในการใช้งาน

๖.๗ การเข้าสู่ระบบเครือข่ายภายในโดยผ่านอินเทอร์เน็ต ต้องมีการยืนยันตัวตนผ่านช่องทางที่ปลอดภัย

๖.๘ จำกัดการเข้าถึงเครือข่ายคอมพิวเตอร์ของหน่วยงานที่สามารถเข้าถึงได้จากภายนอก โดยให้สอดคล้องกับแนวปฏิบัติในการควบคุมการเข้าถึงและการใช้งานสารสนเทศ และแนวปฏิบัติในการควบคุมการใช้งานโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ

๗. การควบคุมการจัดเส้นทางบนเครือข่าย (Network routing control) ต้องควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์ และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับข้อปฏิบัติในการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ ดังนี้

๗.๑ ผู้ดูแลระบบควบคุมไม่ให้มีการเปิดเผยแผนผังการใช้หมายเลขเครือข่าย (IP Address)

๗.๒ ผู้ดูแลระบบกำหนดให้มีการแปลงหมายเลขเครือข่าย เพื่อแยกเครือข่ายย่อย

๗.๓ กำหนดผู้รับผิดชอบในการปรับปรุง แก้ไข หรือเปลี่ยนแปลงค่าระบบต่าง ๆ ของระบบเครือข่ายและอุปกรณ์ที่ใช้เชื่อมต่อกับระบบเครือข่าย และมีการทบทวนค่าระบบต่างๆ อย่างสม่ำเสมอ

๗.๔ ผู้ดูแลระบบต้องจำกัดเส้นทางการเข้าถึงเครือข่ายที่มีการใช้งานร่วมกัน และจำกัดสิทธิในการใช้บริการเครือข่าย เพื่อควบคุมให้ผู้ใช้งานสามารถใช้งานได้เฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

๘. การควบคุมการเข้าใช้งานระบบจากภายนอก (Remote access control)

๘.๑ การเข้าถึงระบบที่สำคัญ หรือระบบที่เกี่ยวข้องกับสารสนเทศสำคัญจากระยะไกล ต้องได้รับการพิสูจน์ตัวตนทุกครั้งก่อนใช้งาน

๘.๒ ห้ามใช้บริการระบบเครือข่าย หรือโพรโทคอล (Protocol) ที่ไม่มั่นคงปลอดภัยในการเข้าถึงระบบสารสนเทศจากระยะไกล

๘.๓ การเข้าสู่ระบบจากระยะไกล (Remote access) เพื่อเข้าสู่ระบบเครือข่ายคอมพิวเตอร์ของสำนักงาน ก่อให้เกิดช่องทางที่มีความเสี่ยงสูงต่อความปลอดภัยของข้อมูลและทรัพยากรของสำนักงาน จึงต้องกำหนดมาตรการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน และให้มีการกำหนดวิธีการตรวจสอบตัวตนที่เหมาะสมเพื่อควบคุมการเข้าถึงระบบสารสนเทศของหน่วยงานจากระยะไกล

๘.๔ การอนุญาตให้ผู้ใช้งานเข้าสู่ระบบจากระยะไกล ต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น และควรตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ได้ต่อเมื่อมีการร้องขอที่จำเป็นเท่านั้น

๘.๕ ก่อนทำการให้สิทธิในการเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับสำนักงานอย่างเพียงพอและต้องได้รับอนุมัติจากผู้อำนวยการกลุ่มงานระบบฐานข้อมูลและเทคโนโลยีสารสนเทศหรือผู้ดูแลระบบที่ได้รับมอบหมาย

๘.๖ มีการควบคุมการเข้าถึงช่องทางการดูแลระบบสารสนเทศ ทั้งทางกายภาพและการเชื่อมต่อผ่านคอมพิวเตอร์ สำหรับระบบสารสนเทศที่สามารถเข้าถึงจากระยะไกลได้ เช่น Remote diagnostic หรือ Configuration facility ของอุปกรณ์เครือข่ายคอมพิวเตอร์

ส่วนที่ ๘
แนวปฏิบัติในการควบคุมการเข้าถึงระบบปฏิบัติการ

วัตถุประสงค์

๑. เพื่อป้องกันการเข้าถึงระบบปฏิบัติการจากผู้ที่ไม่ได้รับอนุญาตและผู้ไม่ประสงค์ดี

๒. เพื่อให้ระบบปฏิบัติการของสำนักงานมีความปลอดภัยและสามารถใช้งานได้อย่างมีประสิทธิภาพและต่อเนื่อง

ผู้รับผิดชอบ

๑. กองติดตามประเมินผลสิ่งแวดล้อม/กลุ่มงานระบบฐานข้อมูลและเทคโนโลยีสารสนเทศ

๒. ผู้ดูแลระบบสารสนเทศ

๓. ผู้ดูแลระบบ

๔. ผู้ใช้งาน

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชั่น ๒.๕) ประจำปี พ.ศ. ๒๕๕๐ ของศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕

แนวปฏิบัติ

การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating system access control) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต มีแนวปฏิบัติดังนี้

๑. การกำหนดขั้นตอนการปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย โดยการยืนยันตัวตนที่มั่นคงปลอดภัย มีแนวปฏิบัติดังนี้

๑.๑ ผู้ใช้งานต้องกำหนดรหัสผ่านในการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์

๑.๒ ผู้ใช้งานต้องกำหนดรหัสผ่านที่มีคุณภาพ ตามที่ระบุไว้ในแนวปฏิบัติในการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน

๑.๓ ผู้ใช้งานต้องทำการล็อกหน้าจอหรือตั้งค่าการรักษาหน้าจอภาพ (Screen Saver) เมื่อไม่มีการใช้งานเครื่องคอมพิวเตอร์เป็นระยะเวลานาน และเมื่อกลับมาใช้งานต้องใส่รหัสผ่านเพื่อเข้าใช้งาน

๑.๔ ผู้ใช้ต้องทำการ Log off ออกจากระบบปฏิบัติการ หรือปิดเครื่องทันที เมื่อเลิกใช้งานหรือไม่อยู่ที่เครื่องเป็นเวลานาน

๑.๕ ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้งานรหัสผู้ใช้และรหัสผ่านของตนในการเข้าใช้เครื่องคอมพิวเตอร์ร่วมกัน

๑.๖ ซอฟต์แวร์ที่สำนักงานมีลิขสิทธิ์ ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความรับผิดชอบ และไม่ให้ผู้ใช้งานติดตั้งหรือใช้งานซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ หากตรวจพบถือเป็นความผิดส่วนบุคคล ผู้ใช้งานต้องเป็นผู้รับผิดชอบแต่เพียงผู้เดียว

๑.๗ ซอฟต์แวร์ที่กลุ่มงานระบบฐานข้อมูลและเทคโนโลยีสารสนเทศติดตั้งไว้ถือเป็นสิ่งจำเป็น ห้ามผู้ใช้งานทำการถอด ถอน เปลี่ยนแปลง แก้ไข ก่อนได้รับอนุญาต

๒. การระบุและยืนยันตัวบุคคลของผู้ใช้งาน (User Identification and Authentication) ต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจง ซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสมเพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง โดยมีแนวปฏิบัติ ดังนี้

๒.๑ ผู้ใช้งานต้องทำการแสดงและพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้อง ด้วยรหัสผู้ใช้และรหัสผ่านก่อนการเข้าใช้งานระบบสารสนเทศ หากการระบุและยืนยันตัวผู้ใช้งานมีปัญหา ต้องแจ้งให้ผู้ดูแลระบบทราบและแก้ไข

๒.๒ ผู้ใช้งานที่เป็นเจ้าของรหัสผู้ใช้งาน ต้องเป็นผู้รับผิดชอบในผลต่าง ๆ อันจะเกิดจากการใช้งานรหัสผู้ใช้งานของระบบสารสนเทศ เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

๓. การบริหารจัดการรหัสผ่าน (Password management system) ให้มีการใช้ระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (Interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ และเมื่อดำเนินการติดตั้งระบบแล้ว ให้ยกเลิกชื่อผู้ใช้งานหรือเปลี่ยนรหัสผ่านของผู้ใช้งานทุกชื่อที่ได้ถูกกำหนดไว้เริ่มต้น ซึ่งมาพร้อมกับการติดตั้งระบบโดยทันที โดยกำหนดให้มีการแจ้งเตือนแบบอัตโนมัติ ในกรณีต่อไปนี้

๓.๑ การแจ้งเตือนให้ผู้ใช้งานเปลี่ยนรหัสผ่าน ล่วงหน้าเป็นเวลา ๑ สัปดาห์ ก่อนถึงรอบระยะเวลาการเปลี่ยนรหัสผ่านที่กำหนดไว้ (๖ เดือน)

๓.๒ การแจ้งเตือนเมื่อผู้ใช้งานกรอกรหัสผ่านผิด และจะระงับการเข้าถึงระบบทันที เมื่อผู้ใช้งานกรอกรหัสผ่านผิด มากกว่า ๓ ครั้ง โดยผู้ใช้งานจะต้องแจ้งผู้ดูแลระบบเพื่อทำการยกเลิกการระงับการเข้าถึงระบบก่อน จึงจะสามารถเข้าใช้งานได้อีกครั้งหนึ่ง

๔. การใช้งานโปรแกรมอรรถประโยชน์ (Use of system utilities) ควรจำกัดและควบคุมการใช้งานโปรแกรมอรรถประโยชน์สำหรับโปรแกรมคอมพิวเตอร์ที่สำคัญ เนื่องจากการใช้งานโปรแกรมอรรถประโยชน์บางชนิดสามารถทำให้ผู้ใช้หลีกเลี่ยงมาตรการป้องกันทางด้านความมั่นคงปลอดภัยของระบบได้ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้ ให้ดำเนินการดังนี้

๔.๑ จำกัดสิทธิการเข้าถึง และกำหนดสิทธิอย่างรัดกุมในการอนุญาตให้ใช้โปรแกรมอรรถประโยชน์

๔.๒ กำหนดให้อนุญาตใช้งานโปรแกรมอรรถประโยชน์เป็นรายครั้งไป

๔.๓ ต้องจัดเก็บโปรแกรมอรรถประโยชน์แยกจากซอฟต์แวร์สำหรับระบบสารสนเทศ

๔.๔ เก็บบันทึกการเรียกใช้งานโปรแกรมเหล่านี้

๔.๕ กำหนดให้ถอดถอนโปรแกรมอรรถประโยชน์ที่ไม่จำเป็นออกจากระบบ

๔.๖ ห้ามใช้งานโปรแกรมที่ละเมิดลิขสิทธ์

๔.๗ ห้ามติดตั้งโปรแกรมโดยไม่ได้รับอนุญาต

๕. เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่ง ให้ยุติการใช้งานระบบสารสนเทศนั้น (session time-out)

๕.๑ กำหนดให้ระบบสารสนเทศ เช่น ระบบงาน อุปกรณ์เครือข่าย เป็นต้น ยุติการใช้งานเมื่อว่างเว้นจากการใช้งานเป็นเวลา ๓๐ นาทีเป็นอย่างน้อย หากเป็นระบบที่มีความเสี่ยงหรือความสำคัญสูง ให้กำหนดระยะเวลายุติการใช้งานระบบเมื่อว่างเว้นจากการใช้งานเป็นเวลา ๑๕ นาที ตามความเหมาะสม เพื่อป้องกันการเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต

๕.๒ ถ้าไม่มีการใช้งานระบบ ต้องทำการยกเลิกการใช้โปรแกรมประยุกต์และการเชื่อมต่อเข้าสู่ระบบโดยอัตโนมัติ

๖. การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of connection time) ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศหรือโปรแกรมที่มีความเสี่ยงหรือมีความสำคัญสูง ดังต่อไปนี้

๖.๑ กำหนดระยะเวลาในการเชื่อมต่อระบบสารสนเทศหรือแอปพลิเคชันที่มีความเสี่ยงหรือมีความสำคัญสูง โดยการระบุตัวตน และกำหนดระยะเวลาให้ใช้งานได้ ๑ ชั่วโมง ต่อการเชื่อมต่อหนึ่งครั้ง และกำหนดให้ใช้งานได้เฉพาะในช่วงเวลาการทำงานตามปกติของสำนักงานเท่านั้น

๖.๒ กำหนดระยะเวลาในการเชื่อมต่อระบบสารสนเทศที่ใช้ในการปฏิบัติงาน เมื่อผู้ใช้งานไม่มีการใช้งานระบบสารสนเทศ เกินกว่า ๑๕ นาที ระบบจะยุติการใช้งาน ผู้ใช้งานต้องทำการ Log in เข้าระบบเทคโนโลยีสารสนเทศอีกครั้ง

ส่วนที่ ๙
แนวปฏิบัติในการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ

วัตถุประสงค์

๑. เพื่อป้องกันการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศจากผู้ที่ไม่ได้รับอนุญาตและผู้ไม่ประสงค์ดี

๒. เพื่อให้การใช้งานโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศเป็นไปอย่างปลอดภัย

ผู้รับผิดชอบ

๑. กองติดตามประเมินผลสิ่งแวดล้อม/กลุ่มงานระบบฐานข้อมูลและเทคโนโลยีสารสนเทศ

๒. ผู้ดูแลระบบสารสนเทศ

๓. ผู้ดูแลระบบ

๔. ผู้ใช้งาน

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชั่น ๒.๕) ประจำปี พ.ศ. ๒๕๕๐ ของศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕

แนวปฏิบัติ

การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (application and information access control) มีแนวปฏิบัติอย่างน้อยดังนี้

๑. การจำกัดการเข้าถึงสารสนเทศ (Information access restriction) ผู้ดูแลระบบสารสนเทศ และผู้ดูแลระบบต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานสารสนเทศและฟังก์ชัน (Functions) ต่าง ๆ ของโปรแกรมประยุกต์หรือแอปพลิเคชัน ของผู้ใช้งานและบุคลากรฝ่ายสนับสนุน โดยให้กำหนดหลักเกณฑ์ในการจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานที่สอดคล้องตามแนวปฏิบัติในการควบคุมการเข้าถึงและการใช้งานสารสนเทศที่ได้กำหนดไว้ ดังนี้

๑.๑ การลงทะเบียนบุคลากรใหม่ของสำนักงาน ผู้ดูแลระบบสารสนเทศต้องกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการเพื่อให้มีสิทธิต่าง ๆ ในการใช้งานตามความจำเป็น รวมทั้งกำหนดให้มีขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน เช่น การลาออก หรือการเปลี่ยนตำแหน่งงานภายในสำนักงาน เป็นต้น

๑.๒ ผู้ดูแลระบบสารสนเทศต้องกำหนดสิทธิการใช้งานระบบสารสนเทศที่สำคัญ เช่น โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-mail) ระบบอินเทอร์เน็ต (Internet) ระบบเครือข่ายไร้สาย เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่ และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

๑.๓ ผู้ดูแลระบบต้องกำหนดระยะเวลาในการเชื่อมต่อระบบสารสนเทศ (Limitation of connection time) ที่ใช้ในการปฏิบัติงานระบบสารสนเทศต่าง ๆ เมื่อผู้ใช้งานไม่มีการใช้งานระบบสารสนเทศเกินกว่า ๑๕ นาที ระบบจะยุติการใช้งาน ผู้ใช้งานต้องทำการ Login เข้าระบบเทคโนโลยีสารสนเทศอีกครั้ง

๑.๔ ผู้รับผิดชอบระบบต้องบริหารจัดการการเข้าถึงข้อมูล ตามประเภทชั้นความลับในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบ ให้เป็นไปตามข้อกำหนดเกี่ยวกับการรักษาความลับข้อมูล

๑.๕ ผู้รับผิดชอบระบบมีมาตรการตรวจสอบข้อมูลที่นำออกจากระบบว่ามีความถูกต้องและสมบูรณ์ก่อนนำไปใช้งาน

๑.๖ ผู้รับจ้างพัฒนาระบบต้องลงนามในสัญญาการไม่เปิดเผยข้อมูลของสำนักงาน

๑.๗ ผู้ดูแลระบบต้องควบคุมการเข้าถึงข้อมูลของผู้รับจ้างพัฒนาระบบจากภายนอก ให้มีสิทธิเข้าถึงเฉพาะข้อมูลที่เกี่ยวข้อง และตรวจสอบการนำข้อมูลเข้าและออกจากระบบสารสนเทศของผู้รับจ้างพัฒนาระบบจากภายนอกทุกครั้ง

๑.๘ ผู้รับผิดชอบระบบต้องกำหนดให้ผู้รับจ้างจัดทำคู่มือการปฏิบัติงานและเอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอ

๑.๙ กำหนดให้ผู้รับจ้างรายงานผลการปฏิบัติงาน ปัญหาต่าง ๆ และแนวทางแก้ไข กำหนดให้มีขั้นตอนในการตรวจรับงานของผู้ให้บริการอย่างชัดเจน

๒. ระบบซึ่งไวต่อการรบกวน มีผลกระทบ และมีความสำคัญสูงต่อสำนักงาน จะต้องดำเนินการดังนี้

๒.๑ ระบบซึ่งไวต่อการรบกวน มีผลกระทบ และมีความสำคัญสูงต่อสำนักงาน เช่น ระบบบริหารการเงินการคลังภาครัฐแบบอิเล็กทรอนิกส์ (GFMIS) ระบบที่ใช้ในการปฏิบัติงานด้านการงบประมาณการบัญชี การจัดซื้อจัดจ้าง การเบิกจ่าย และการบริหารทรัพยากร ซึ่งดูแลรับผิดชอบโดยกรมบัญชีกลาง จะได้รับการแยกออกจากระบบงานอื่น ๆ ของสำนักงาน

๒.๒ ระบบซึ่งไวต่อการรบกวน ต้องมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ โดยมีพื้นที่ปฏิบัติงานแยกเป็นสัดส่วน และต้องมีการกำหนดสิทธิให้เฉพาะผู้ที่มีสิทธิใช้ระบบเท่านั้นที่สามารถเข้าไปปฏิบัติงานในพื้นที่ควบคุมดังกล่าว

๒.๓ ให้มีการควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ และการปฏิบัติงานภายนอกสำนักงาน (Moblie computing and teleworking) สำหรับระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อสำนักงาน

๓. การควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ ต้องกำหนดแนวปฏิบัติและมาตรการที่เหมาะสม เพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ดังนี้

๓.๑ เครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ที่เป็นทรัพย์สินของสำนักงาน ผู้ใช้งานต้องใช้งานอย่างมีประสิทธิภาพ และใช้เพื่องานของสำนักงานเท่านั้น

๓.๒ โปรแกรมที่ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์แบบพกพาของสำนักงาน ต้องเป็นโปรแกรมที่สำนักงานมีลิขสิทธิ์ถูกต้องตามกฎหมายเท่านั้น ห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้ง แก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๓.๓ ผู้ใช้งานต้องศึกษาและปฏิบัติตามคู่มือการใช้งานอย่างละเอียด เพื่อการใช้งานอย่างปลอดภัยและมีประสิทธิภาพ

๓.๔ ห้ามดัดแปลงแก้ไขส่วนประกอบต่าง ๆ ของเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ของสำนักงาน และต้องรักษาให้มีสภาพเดิมอยู่เสมอ

๓.๕ กรณีต้องการนำเครื่องคอมพิวเตอร์แบบพกพาหรืออุปกรณ์สื่อสารเคลื่อนที่ที่เป็นสินทรัพย์ของสำนักงานออกจากสำนักงาน ต้องได้รับอนุญาตจากผู้บังคับบัญชาก่อนทุกครั้ง

๔. การปฏิบัติงานจากภายนอกสำนักงาน (teleworking) ผู้ดูแลระบบสารสนเทศต้องกำหนดแนวปฏิบัติ แผนงาน และขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานจากหน่วยงานภายนอกสำนักงาน ดังนี้

๔.๑ ต้องมีการตรวจสอบว่าอุปกรณ์ที่เป็นของส่วนตัวซึ่งใช้ในการเข้าถึงระบบสารสนเทศของสำนักงานจากระยะไกล มีการป้องกันไวรัสและการใช้งานไฟร์วอลล์ตามที่กำหนด

๔.๒ ผู้ใช้งานจากระยะไกลทุกคนต้องผ่านการพิสูจน์ตัวตน เพื่อเพิ่มความปลอดภัย โดยจะต้องมีการตรวจสอบ เช่น รหัสผ่าน หรือวิธีการเข้ารหัสลับ เป็นต้น

๔.๓ ต้องกำหนดชนิดของงาน ชั่วโมงการทำงาน ชั้นความลับของข้อมูล ระบบงานและบริการต่าง ๆ ของสำนักงาน ที่อนุญาตและไม่อนุญาตให้ปฏิบัติงานจากระยะไกล

๔.๔ ต้องกำหนดขั้นตอนปฏิบัติสำหรับการขออนุมัติ การขอยกเลิก การกำหนดหรือปรับปรุงสิทธิการเข้าถึงระบบงาน และการคืนอุปกรณ์ที่ใช้ปฏิบัติงานจากระยะไกล

ส่วนที่ ๑๐
แนวปฏิบัติในการใช้งานระบบอินเทอร์เน็ต

วัตถุประสงค์

เพื่อให้การใช้งานระบบอินเทอร์เน็ต (Internet) ของสำนักงานเป็นไปอย่างมีประสิทธิภาพและปลอดภัย

ผู้รับผิดชอบ

๑. กองติดตามประเมินผลสิ่งแวดล้อม/กลุ่มงานระบบฐานข้อมูลและเทคโนโลยีสารสนเทศ

๒. ผู้ดูแลระบบสารสนเทศ

๓. ผู้ใช้งาน

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชั่น ๒.๕) ประจำปี พ.ศ. ๒๕๕๐ ของศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓

แนวปฏิบัติ

การควบคุมการใช้งานระบบอินเทอร์เน็ต (Internet) ของสำนักงานให้เป็นไปอย่างมีประสิทธิภาพและปลอดภัย มีแนวปฏิบัติดังนี้

๑. ผู้ใช้งานต้องเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานระบบอินเทอร์เน็ต (Internet) ผ่านระบบที่กำหนดไว้เท่านั้น เพื่อความปลอดภัยต่อระบบเครือข่ายของสำนักงาน

๒. ผู้ใช้งานต้องเข้าถึงแหล่งข้อมูลตามสิทธิที่ได้รับตามหน้าที่ความรับผิดชอบเพื่อประสิทธิภาพของระบบเครือข่ายและความปลอดภัยทางข้อมูลของสำนักงาน

๓. ผู้ใช้งานต้องไม่ใช้ระบบอินเทอร์เน็ต (Internet) ของสำนักงาน เพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล หรือเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับสำนักงาน เป็นต้น

๔. ห้ามผู้ใช้งานเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของสำนักงานที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต (Internet)

๕. ผู้ใช้งานต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากระบบอินเทอร์เน็ต (Internet) ซึ่งรวมถึงการดาวน์โหลดการอัพเดท (Update) โปรแกรมต่าง ๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์หรือสินทรัพย์ทางปัญญา

๖. ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ผู้ใช้งานต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของสำนักงาน

๗. ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ผู้ใช้งานต้องไม่เสนอความคิดเห็น หรือใช้ ข้อความที่ยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของสำนักงาน การทำลายความสัมพันธ์กับบุคคลากรของหน่วยงานอื่น ๆ

๘. หลังจากใช้งานระบบอินเทอร์เน็ต (Internet) เสร็จแล้ว ให้ผู้ใช้งานทำการปิดเว็บเบราเซอร์ทุกครั้ง เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น ๆ

ส่วนที่ ๑๑
แนวปฏิบัติในการใช้งานเครือข่ายสังคมออนไลน์

วัตถุประสงค์

เพื่อให้การใช้งานระบบจดหมายอิเล็กทรอนิกส์ (E-mail) ของสำนักงานเป็นไปอย่างมีประสิทธิภาพและปลอดภัย

ผู้รับผิดชอบ

๑. กองติดตามประเมินผลสิ่งแวดล้อม/กลุ่มงานระบบฐานข้อมูลและเทคโนโลยีสารสนเทศ

๒. ผู้ดูแลระบบสารสนเทศ

๓. ผู้ใช้งาน

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชั่น ๒.๕) ประจำปี พ.ศ. ๒๕๕๐ ของศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓

แนวปฏิบัติ

การควบคุมการใช้งานสื่อสังคมออนไลน์ของสำนักงานให้เป็นไปอย่างมีประสิทธิภาพและปลอดภัย ให้ปฏิบัติตามแนวทางปฏิบัติในการใช้สื่อสังคมออนไลน์ที่สำนักงานกำหนดไว้ โดยมีแนวปฏิบัติดังนี้

๑. อนุญาตให้ใช้งานเครือข่ายสังคมออนไลน์ในรูปแบบและลักษณะตามที่หน่วยงานได้กำหนดไว้เท่านั้น

๒. ผู้ใช้งานเครือข่ายสังคมออนไลน์ต้องตระหนักถึงความปลอดภัยอยู่เสมอ และต้องปฏิบัติตามพระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. ๒๕๔๐ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ และที่แก้ไขเพิ่มเติม พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ตลอดจนกฎหมายอื่น ๆ ที่อาจเกี่ยวข้อง

๓. การใช้สื่อสังคมออนไลน์เพื่อเผยแพร่ข้อมูลเกี่ยวกับภารกิจหรือข้อมูลเกี่ยวกับองค์กร และหน่วยงานภายใน จะต้องได้รับความเห็นชอบจากผู้บังคับบัญชาก่อน

๔. ผู้ใช้งานต้องรับผิดชอบข้อความ รูปภาพ วิดีโอ และ/หรือความเห็นของตนเอง ที่เผยแพร่บนสื่อสังคมออนไลน์ ทั้งทางด้านสังคมและด้านกฎหมาย

๕. ผู้ใช้งานต้องรับผิดชอบหากเกิดความเสียหายใด ๆ ที่มีผลกระทบกับหน่วยงานจากการใช้งานเครือข่ายสังคมออนไลน์

๖. หากเกิดปัญหาจากการใช้งานเครือข่ายสังคมออนไลน์ที่อาจมีผลกระทบกับสำนักงาน ผู้ใช้งานต้องแจ้งต่อกลุ่มงานระบบฐานข้อมูลและเทคโนโลยีสารสนเทศโดยเร็วที่สุด เพื่อดำเนินการตามความเหมาะสม

ส่วนที่ ๑๒
แนวปฏิบัติในการใช้งานระบบจดหมายอิเล็กทรอนิกส์

วัตถุประสงค์

เพื่อให้การใช้งานระบบจดหมายอิเล็กทรอนิกส์ (E-mail) ของสำนักงานเป็นไปอย่างมีประสิทธิภาพและปลอดภัย

ผู้รับผิดชอบ

๑. กองติดตามประเมินผลสิ่งแวดล้อม/กลุ่มงานระบบฐานข้อมูลและเทคโนโลยีสารสนเทศ

๒. ผู้ดูแลระบบสารสนเทศ

๓. ผู้ใช้งาน

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชั่น ๒.๕) ประจำปี พ.ศ. ๒๕๕๐ ของศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓

แนวปฏิบัติ

การควบคุมการใช้งานจดหมายอิเล็กทรอนิกส์ (E-mail Policy) ของสำนักงานให้เป็นไปอย่างมีประสิทธิภาพและปลอดภัย มีแนวปฏิบัติดังนี้

๑. ผู้ดูแลระบบ มีแนวปฏิบัติดังนี้

๑.๑ กำหนดสิทธิในการใช้งานระบบจดหมายอิเล็กทรอนิกส์ของ สผ.

๑.๒ จัดทำบัญชีผู้ใช้งานและปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๑.๓ เก็บรักษาข้อมูลการขอใช้บริการจดหมายอิเล็กทรอนิกส์และรหัสผ่านของผู้ใช้แต่ละคนไว้เป็นความลับ

๒. ผู้ใช้งาน มีแนวปฏิบัติดังนี้

๒.๑ บุคลากรของสำนักงานที่ต้องการใช้งานจดหมายอิเล็กทรอนิกส์ของสำนักงาน จะต้องกรอกข้อมูลคำขอลงทะเบียนตามแบบฟอร์มการขอใช้บริการจดหมายอิเล็กทรอนิกส์กลางเพื่อการสื่อสารในภาครัฐ (mail.onep.go.th) ของสำนักงาน และยื่นต่อผู้ดูแลระบบเพื่อกำหนดสิทธิในการใช้งาน

๒.๒ เมื่อผู้ดูแลระบบกำหนดสิทธิในการใช้งาน และแจ้งยืนยันบัญชีผู้ใช้งานจดหมายอิเล็กทรอนิกส์ของ สำนักงานให้ทราบแล้ว เพื่อความปลอดภัยควรเปลี่ยนรหัสผ่าน (Password) ทันที

๒.๓ ควรเก็บข้อมูลรหัสผ่านไว้เป็นความลับ ไม่ควรเผยแพร่แก่บุคคลอื่น และไม่ควรตั้งค่าการจำรหัสผ่าน (Save password) แบบอัตโนมัติ

๒.๔ ควรใช้จดหมายอิเล็กทรอนิกส์ของสำนักงาน เพื่อการปฏิบัติงานที่เกี่ยวข้องกับภารกิจของสำนักงานเท่านั้น

๒.๕ ห้ามใช้จดหมายอิเล็กทรอนิกส์ของสำนักงานในการแสวงหาผลประโยชน์ทางธุรกิจ หรือผลประโยชน์ส่วนตัว

๒.๖ เจ้าของบัญชีผู้ใช้ต้องเป็นผู้รับผิดชอบต่อการกระทำใด ๆ ต่อจดหมายอิเล็กทรอนิกส์ของตน

๒.๗ ไม่ควรใช้บัญชีผู้ใช้ของบุคคลอื่นในสำนักงาน เพื่อรับ-ส่งจดหมายอิเล็กทรอนิกส์ เว้นแต่จะได้รับความยินยอมจากเจ้าของบัญชีผู้ใช้

๒.๘ การใช้งานจดหมายอิเล็กทรอนิกส์กลางของกอง/กลุ่มอิสระ/กลุ่มงาน ผู้ใช้จะต้องเป็นผู้ที่ได้รับมอบหมายจากผู้อำนวยการกอง/กลุ่มอิสระ/กลุ่มงาน เท่านั้น

๒.๙ ไม่ควรเปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์จากผู้ส่งที่ไม่รู้จัก

๒.๑๐ ควรตรวจสอบไฟล์เอกสารแนบของจดหมายอิเล็กทรอนิกส์ทุกครั้งก่อนทำการดาวน์โหลดและไม่ควรเปิดไฟล์เอกสารแนบหรือกดลิ้งค์จากผู้ส่งที่ไม่รู้จัก

๒.๑๑ ควรตรวจสอบความถูกต้องของไฟล์เอกสารที่จะแนบไปกับจดหมายอิเล็กทรอนิกส์ทุกครั้งก่อนส่ง

๒.๑๒ ห้ามส่งจดหมายอิเล็กทรอนิกส์ที่มีถ้อยคำหรือข้อความที่ไม่สุภาพ หรือมีข้อมูลที่เป็นความลับของทางราชการ ซึ่งอาจทำให้เกิดความเสื่อมเสียหรือเสียหายต่อสำนักงานได้

๒.๑๓ ห้ามส่งหรือส่งต่อจดหมายอิเล็กทรอนิกส์ที่มีไวรัสคอมพิวเตอร์ หรือโปรแกรมที่อาจเป็นอันตรายต่อเครื่องคอมพิวเตอร์หรือระบบเครือข่ายไปให้บุคคลอื่นโดยเจตนา

๒.๑๔ ห้ามส่งหรือส่งต่อจดหมายอิเล็กทรอนิกส์ลูกโซ่ หรือจดหมายอิเล็กทรอนิกส์ที่เข้าข่าย Spam อย่างเด็ดขาด

๒.๑๕ ห้ามส่งหรือส่งต่อจดหมายอิเล็กทรอนิกส์ที่เป็นการล่วงละเมิด ข่มขู่ สร้างความรำคาญต่อผู้อื่น หรือมีข้อความหรือเนื้อหาที่ผิดกฎหมาย หรือละเมิดศีลธรรม

๒.๑๖ ควรลงชื่อออก (log out) จากระบบทุกครั้ง หลังจากใช้งานจดหมายอิเล็กทรอนิกส์เสร็จสิ้น เพื่อป้องกันบุคคลอื่นเข้าใช้งานบัญชีผู้ใช้ของท่าน

ส่วนที่ ๑๓
แนวปฏิบัติในการใช้งานเครื่องคอมพิวเตอร์และเครื่องคอมพิวเตอร์แบบพกพาของสำนักงาน

วัตถุประสงค์

เพื่อให้การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพาของสำนักงานเป็นไปอย่างมีประสิทธิภาพและปลอดภัย

ผู้รับผิดชอบ

๑. กองติดตามประเมินผลสิ่งแวดล้อม/กลุ่มงานระบบฐานข้อมูลและเทคโนโลยีสารสนเทศ
๒. ผู้ดูแลระบบสารสนเทศ
๓. ผู้ใช้งาน

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชั่น ๒.๕) ประจำปี พ.ศ. ๒๕๕๐ ของศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓

แนวปฏิบัติ

การควบคุมการใช้งานเครื่องคอมพิวเตอร์และเครื่องคอมพิวเตอร์แบบพกพาของสำนักงานให้เป็นไปอย่างมีประสิทธิภาพและปลอดภัย มีแนวปฏิบัติดังนี้

๑. การใช้งานทั่วไป

๑.๑ ผู้ใช้งานต้องใช้เครื่องคอมพิวเตอร์และเครื่องคอมพิวเตอร์แบบพกพาที่เป็นทรัพย์สินของสำนักงานอย่างมีประสิทธิภาพ และใช้เพื่อการปฏิบัติงานของสำนักงานเท่านั้น

๑.๒ โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์และเครื่องคอมพิวเตอร์แบบพกพาของสำนักงาน ต้องเป็นโปรแกรมที่สำนักงานได้ลิขสิทธิ์ถูกต้องตามกฎหมาย และห้ามมิให้ผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๑.๓ ไม่อนุญาตให้ผู้ใช้งานทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์และเครื่องคอมพิวเตอร์แบบพกพาของสำนักงาน

๑.๔ การส่งเครื่องคอมพิวเตอร์และเครื่องคอมพิวเตอร์แบบพกพาของสำนักงานไปตรวจซ่อมจะต้องดำเนินการโดยเจ้าหน้าที่ของผู้รับจ้างในการบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้ทำสัญญากับสำนักงานเท่านั้น ยกเว้นในกรณีที่ไม่อยู่ในเงื่อนไขการบำรุงรักษาของสำนักงาน

๑.๕ ก่อนการใช้งานสื่อบันทึกพกพาต่าง ๆ ต้องมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัส

๑.๖ ไม่ควรเก็บข้อมูลสำคัญของสำนักงานไว้บนเครื่องคอมพิวเตอร์ที่ใช้งานอยู่

๑.๗ ไม่นำอาหารหรือเครื่องดื่มอยู่ใกล้บริเวณเครื่องคอมพิวเตอร์

๑.๘ ไม่วางสื่อแม่เหล็กไว้ใกล้หน้าจอเครื่องคอมพิวเตอร์หรือ Disk Drive

๑.๙ ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพา ควรใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพา เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน เช่น การตกจากโต๊ะทำงาน หรือหลุดมือ เป็นต้น

๑.๑๐ การใช้เครื่องคอมพิวเตอร์แบบพกพาเป็นระยะเวลานานเกินไป ในสภาพที่มีอากาศร้อนจัด ควรปิดเครื่องคอมพิวเตอร์เพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง

๑.๑๑ หลีกเลี่ยงการใช้นิ้วหรือของแข็ง เช่น ปลายปากกา กดสัมผัสหน้าจอ LCD ให้เป็นรอยขีดข่วนหรือทำให้จอ LCD ของเครื่องคอมพิวเตอร์แบบพกพาแตกเสียหายได้

๑.๑๒ ไม่วางของทับบนหน้าจอและแป้นพิมพ์

๑.๑๓ การเคลื่อนย้ายเครื่อง ขณะที่เครื่องเปิดใช้งานอยู่ ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น

๑.๑๔ ไม่ใช้หรือวางเครื่องคอมพิวเตอร์แบบพกพาใกล้สิ่งที่เป็นของเหลวหรือความชื้น เช่น อาหาร น้ำกาแฟ เครื่องดื่มต่าง ๆ เป็นต้น

๑.๑๕ ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย เช่น ควรล็อคเครื่องขณะที่ไม่ได้ใช้งาน และไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

๑.๑๖ ห้ามผู้ใช้งานทำการเปลี่ยนแปลงแก้ไขส่วนประกอบย่อย (Sub component) ที่ติดตั้งอยู่ภายในด้วยตนเอง

๒. การสำรองข้อมูลและการกู้คืนข้อมูลภายในเครื่อง

๒.๑ ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่น ๆ เช่น CD, DVD, External Hard Disk เป็นต้น

๒.๒ ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล และทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

ส่วนที่ ๑๔
แนวปฏิบัติในการจัดเก็บข้อมูลจราจรคอมพิวเตอร์

วัตถุประสงค์

เพื่อควบคุมจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (log) ของสำนักงานสำหรับการตรวจสอบในภายหลัง

ผู้รับผิดชอบ

๑. กองติดตามประเมินผลสิ่งแวดล้อม/กลุ่มงานระบบฐานข้อมูลและเทคโนโลยีสารสนเทศ

๒. ผู้ดูแลระบบสารสนเทศ

๓. ผู้ใช้งาน

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชั่น ๒.๕) ประจำปี พ.ศ. ๒๕๕๐ ของศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕

แนวปฏิบัติ

เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์ (log) มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้ มีแนวปฏิบัติ ดังนี้

๑. จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (log) ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วน ถูกต้อง แท้จริง ระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้ และข้อมูลที่ใช้ในการจัดเก็บ ต้องกาหนดชั้นความลับในการเข้าถึง

๒. ห้ามผู้ดูแลระบบแก้ไขข้อมูลที่เก็บรักษาไว้ ยกเว้นผู้ตรวจสอบระบบสารสนเทศของหน่วยงาน (IT auditor) หรือบุคคลที่หน่วยงานมอบหมาย

๓. กำหนดให้มีการบันทึกการทำงานของระบบบันทึกการปฏิบัติงานของผู้ใช้งาน (application logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้า – ออกระบบ บันทึกการพยายามเข้าสู่ระบบ เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกไว้อย่างน้อย ๙๐ วัน นับตั้งแต่การใช้งานสิ้นสุดลง

๔. ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่างๆ และจำกัดสิทธิการเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

ส่วนที่ ๑๕
แนวปฏิบัติในการพัฒนาและปรับปรุงระบบสารสนเทศให้มีความปลอดภัย

วัตถุประสงค์

เพื่อควบคุมการพัฒนาระบบสารสนเทศของสำนักงานให้เป็นไปอย่างมีประสิทธิภาพและปลอดภัย

ผู้รับผิดชอบ

๑. กองติดตามประเมินผลสิ่งแวดล้อม/กลุ่มงานระบบฐานข้อมูลและเทคโนโลยีสารสนเทศ

๒. ผู้ดูแลระบบสารสนเทศ

๓. ผู้ดูแลระบบ

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชั่น ๒.๕) ประจำปี พ.ศ. ๒๕๕๐ ของศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕

แนวปฏิบัติ

การควบคุมการพัฒนาและปรับปรุงระบบสารสนเทศของสำนักงานให้เป็นไปอย่างมีประสิทธิภาพและปลอดภัย ให้ปฏิบัติตามแนวทางการบริหารจัดการระบบสารสนเทศของสำนักงาน และแนวปฏิบัติดังนี้

๑. ผู้รับผิดชอบระบบต้องควบคุมให้ผู้พัฒนาระบบดำเนินการพัฒนา/ปรับปรุงระบบสารสนเทศเป็นไปอย่างปลอดภัย โดยมีแนวปฏิบัติดังนี้

๑.๑ กำหนดให้มีระบบป้องกันการบุกรุกระบบสารสนเทศที่พัฒนา/ปรับปรุงขึ้น

๑.๒ ตั้งรหัสผ่านที่มีความปลอดภัยสำหรับการเข้าถึงระบบ โดยปฏิบัติให้สอดคล้องกับแนวปฏิบัติในการตั้งและใช้งานรหัสผ่านของสำนักงาน

๑.๓ กรณีที่ข้อมูลในระบบ เป็นข้อมูลลับ ข้อมูลส่วนบุคคล หรือข้อมูลที่ใช้ภายในสำนักงานเท่านั้น ต้องมีการทดสอบเพื่อป้องกันการรั่วไหลของข้อมูล หรือให้มีการป้องกันมิให้ข้อมูลดังกล่าวออกไปสู่ภายนอกได้

๑.๔ ควบคุมการติดตั้งระบบไปยังเครื่องคอมพิวเตอร์แม่ข่าย โดยกำหนดให้เฉพาะผู้พัฒนาระบบ ผู้ดูแลระบบ หรือผู้ที่ได้รับมอบหมายจากผู้ดูแลระบบเท่านั้น เป็นผู้ดำเนินการติดตั้ง

๑.๕ กรณีที่เป็นการติดตั้งระบบสารสนเทศเพื่อทดแทนระบบเดิม ต้องกำหนดให้มีการสำรองข้อมูลที่จำเป็นที่เกี่ยวข้องกับระบบสารสนเทศนั้นไว้ด้วย

๑.๖ กรณีที่มีความจำเป็นต้องแปลงข้อมูลในระบบสารสนเทศเดิมไปยังระบบสารสนเทศที่พัฒนาหรือปรับปรุงขึ้น ต้องมีการตรวจสอบว่าข้อมูลที่มีการถ่ายโอนไปนั้นมีความถูกต้องและครบถ้วนหรือไม่

๑.๗ ติดตั้งโปรแกรมแก้ไขช่องโหว่ของซอฟแวร์ต่าง ๆ ในระบบ เช่น ซอฟต์แวร์ระบบปฏิบัติการ และระบบบริหารจัดการข้อมูล เป็นต้น เพื่อปรับปรุงหรือแก้ไขให้ระบบมีความสมบูรณ์และมั่นคงปลอดภัย

๑.๘ ตรวจสอบและปิดพอร์ตต่าง ๆ บนระบบ ที่ไม่มีความจำเป็นในการใช้งาน

๑.๙ ตรวจสอบเงื่อนไขของซอฟต์แวร์ที่จะทำการติดตั้งในระบบสารสนเทศที่พัฒนาหรือปรับปรุงขึ้น และจะต้องไม่เป็นการละเมิดลิขสิทธิ์ของผู้ผลิตซอฟต์แวร์นั้น

๑.๑๐ ตรวจสอบและลบบัญชีผู้ใช้งานในระบบที่ไม่ได้ใช้งานแล้ว ซึ่งรวมถึงบัญชีผู้ใช้งานต่าง ๆ ที่มากับซอฟต์แวร์เหล่านั้น

๑.๑๑ กำหนดให้ผู้พัฒนาระบบจัดส่งซอร์สโค้ด พร้อมคู่มือการดูแลระบบสำหรับเจ้าหน้าที่ดูแลระบบ ที่ครอบคลุมการเพิ่ม เปลี่ยนแปลง แก้ไข หรือการถอดถอนสิทธิของผู้ใช้งาน พร้อมทั้งอบรมการใช้งานแก่ผู้ดูแลระบบ

๒. ผู้รับผิดชอบระบบต้องมอบหมายเจ้าหน้าที่ทำหน้าที่ดูแลระบบ ผู้นำเข้าข้อมูล และผู้ตรวจสอบความถูกต้องของข้อมูลเป็นลายลักษณ์อักษร และแจ้งรายชื่อดังกล่าวให้กลุ่มงานระบบฐานข้อมูลและเทคโนโลยีสารสนเทศทราบ และหากมีการเปลี่ยนแปลงรายชื่อ ต้องแจ้งให้กลุ่มงานระบบฐานข้อมูลและเทคโนโลยีสารสนเทศทราบทุกครั้ง

๓. ผู้ดูแลระบบต้องจัดเก็บซอร์ดโค้ดสำหรับซอฟต์แวร์ของระบบสารสนเทศดังกล่าวไว้ในที่ที่ปลอดภัย และจำกัดให้เข้าถึงได้เฉพาะผู้ที่เกี่ยวข้องเท่านั้น

๔. ผู้ดูแลระบบต้องตรวจสอบการใช้งานระบบ และปรับปรุงเวอร์ชั่นของโปรแกรมที่ใช้ในการพัฒนาระบบสารสนเทศดังกล่าวให้เป็นปัจจุบัน เพื่อให้สามารถใช้งานได้อย่างต่อเนื่อง รวมทั้งกำหนดให้มีแผนการพัฒนาและบำรุงรักษาระบบเป็นระยะ ๆ

๕. หากไม่ได้ใช้งานหรือต้องการยกเลิกการใช้งานระบบสารสนเทศที่จัดทำแล้วเสร็จ ผู้รับผิดชอบระบบสารสนเทศต้องแจ้งให้กลุ่มงานระบบฐานข้อมูลและเทคโนโลยีสารสนเทศทราบทุกครั้ง

๖. หากระบบที่พัฒนาหรือปรับปรุงต้องมีการเชื่อมโยงและแลกเปลี่ยนข้อมูลกับระบบงานอื่นทั้งภายในและภายนอกสำนักงาน ต้องดำเนินการให้เป็นไปตามแนวปฏิบัติในการเชื่อมโยงระบบงานกับหน่วยงานภายนอก

ส่วนที่ ๑๖
แนวปฏิบัติในการสำรองข้อมูลสำคัญและการเตรียมรับมือกับเหตุฉุกเฉิน

วัตถุประสงค์

๑. เพื่อให้ระบบสารสนเทศของสำนักงานสามารถใช้ในการปฏิบัติงานและให้บริการได้อย่างต่อเนื่องและมีสภาพพร้อมใช้งานอยู่เสมอ

๒. เพื่อเตรียมพร้อมรับมือในกรณีเกิดเหตุฉุกเฉิน และป้องกันความเสียหายที่อาจเกิดขึ้นกับข้อมูลสำคัญของสำนักงาน

ผู้รับผิดชอบ

๑. กองติดตามประเมินผลสิ่งแวดล้อม/กลุ่มงานระบบฐานข้อมูลและเทคโนโลยีสารสนเทศ

๒. ผู้ดูแลระบบสารสนเทศ

๓. ผู้ดูแลระบบ

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชั่น ๒.๕) ประจำปี พ.ศ. ๒๕๕๐ ของศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕

แนวปฏิบัติ

การสำรองข้อมูลสำคัญและการเตรียมรับมือกับสถานการณ์ฉุกเฉิน มีแนวปฏิบัติดังนี้

๑. การกำหนดแนวทางปฏิบัติในการสำรองและกู้คืนข้อมูล ผู้ดูแลระบบสารสนเทศ และผู้ดูแลระบบมีแนวปฏิบัติดังนี้

๑.๑ คัดเลือกระบบงาน และระบบสารสนเทศ ที่มีความจำเป็นต้องสำรองข้อมูลไว้ให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ

๑.๒ กำหนดประเภทและชนิดของข้อมูลที่มีความจำเป็นต้องสำรองข้อมูลเก็บไว้ โดยอย่างน้อยต้องประกอบด้วย ข้อมูลในฐานข้อมูลของระบบ ข้อมูลสำหรับตัวระบบ เช่น ซอฟต์แวร์ระบบปฏิบัติการ และซอฟต์แวร์อื่นๆ ที่เกี่ยวข้อง เป็นต้น

๑.๓ กำหนดให้ผู้ดูแลระบบสารสนเทศและผู้ดูแลระบบแต่ละระบบเป็นผู้รับผิดชอบในการสำรองและกู้คืนข้อมูล

๑.๔ จัดทำแผนการสำรองและกู้คืนข้อมูล โดยกำหนดขั้นตอนของการสำรองข้อมูล การกู้คืนข้อมูลและความถี่ในการดำเนินงานที่เหมาะสม

๑.๕ คัดเลือกและจัดทำระบบสำรองข้อมูลที่เหมาะสมกับระบบงานและระบบสารสนเทศ

๑.๖ กำหนดรายละเอียดด้านฮาร์ดแวร์และซอฟต์แวร์ที่จำเป็นของระบบสำรองข้อมูล พร้อมทั้งจัดหาและติดตั้งตามความจำเป็น

๑.๗ กำหนดสถานที่และอุปกรณ์ในการสำรองข้อมูล เช่น เครื่องคอมพิวเตอร์ คอมพิวเตอร์แม่ข่าย หรือระบบคลาวด์ และควรนำข้อมูลที่สำรองไปเก็บไว้นอกสถานที่อย่างน้อย ๑ ชุด

๑.๘ ทำการสำรองข้อมูลตามแผนการสำรองและกู้คืนข้อมูลที่กำหนดไว้

๑.๙ ทำการตรวจสอบว่าการสำรองข้อมูลมีความถูกต้อง ครบถ้วน และเป็นไปตามที่กำหนดไว้หรือไม่

๑.๑๐ ทำการทดสอบการกู้คืนข้อมูลและระบบสารสนเทศที่สำรองไว้ อย่างน้อยปีละ ๑ ครั้ง รวมทั้งทดสอบว่า ระบบงานทั้งหมดสามารถใช้งานได้ตามปกติหรือไม่

๒. การจัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องประกอบด้วยหัวข้ออย่างน้อยดังนี้

๒.๑ การกำหนดหน้าที่และความรับผิดชอบของผู้ที่เกี่ยวข้อง โดยให้เจ้าหน้าที่กลุ่มงานระบบฐานข้อมูลและเทคโนโลยีสารสนเทศ กองติดตามประเมินผลสิ่งแวดล้อม เป็นผู้รับผิดชอบหลักในการดำเนินการ โดยให้รายงานต่อผู้อำนวยการกองติดตามประเมินผลสิ่งแวดล้อมเพื่อสั่งการให้เจ้าหน้าที่ที่เกี่ยวข้องดำเนินการต่อไป

๒.๒ การประเมินความเสี่ยงสำหรับระบบงานที่มีความสำคัญ และกำหนดมาตรการเพื่อลดความเสี่ยงเหล่านั้น เช่น ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว หรือการชุมนุมประท้วง เป็นต้น ที่ทำให้ไม่สามารถเข้ามาใช้ระบบงานได้ เป็นต้น

๒.๓ การกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูลและระบบสารสนเทศ รวมทั้งการกู้คืนข้อมูลที่สำรองไว้

๒.๔ การกำหนดช่องทางในการติดต่อสื่อสารกับผู้ให้บริการภายนอก เช่น ผู้ให้บริการเครือข่าย ผู้ดูแลเครือข่าย ผู้พัฒนาระบบ เป็นต้น เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อในกรณีเกิดเหตุฉุกเฉินต่าง ๆ

๒.๕ การจัดประชุมและแจ้งให้ผู้ที่เกี่ยวข้องทั้งหมดทราบรายละเอียดของแผน และเมื่อมีการปรับปรุงแผนใหม่จะต้องจัดประชุมและแจ้งให้ผู้ที่เกี่ยวข้องทราบ

๒.๖ การปรับปรุงแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง

๒.๗ การทดสอบสภาพความพร้อมใช้งานของระบบสารสนเทศ ระบบสำรองและกู้คืนข้อมูล และแผนเตรียมพร้อมกรณีฉุกเฉินอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง

ส่วนที่ ๑๗
แนวปฏิบัติในการเชื่อมโยงระบบงานกับหน่วยงานภายนอก

วัตถุประสงค์

เพื่อให้การเชื่อมโยงระบบงานของหน่วยงานกับระบบงานของหน่วยงานภายนอกเป็นไปอย่างปลอดภัย

ผู้รับผิดชอบ

๑. กองติดตามประเมินผลสิ่งแวดล้อม/กลุ่มงานระบบฐานข้อมูลและเทคโนโลยีสารสนเทศ

๒. ผู้ดูแลระบบสารสนเทศ

๓. ผู้ดูแลระบบ

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชั่น ๒.๕) ประจำปี พ.ศ. ๒๕๕๐ ของศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕

แนวปฏิบัติ

การควบคุมให้การเชื่อมโยงระบบงานของสำนักงานกับระบบงานของหน่วยงานภายนอกเป็นไปอย่างปลอดภัย ผู้ดูแลระบบสารสนเทศ และผู้ดูระบบ ร่วมกับผู้แทนของหน่วยงานภายนอก มีแนวปฏิบัติดังนี้

๑. หารือร่วมกันเพื่อประเมินความเสี่ยงของระบบงานและข้อมูลที่จะมีการแลกเปลี่ยนกันระหว่างสำนักงานกับหน่วยงานภายนอก

๒. กำหนดวิธีการและเทคนิคที่ใช้ในการเชื่อมโยง

๓. กำหนดผู้รับผิดชอบและสิทธิในการเข้าถึงระบบงานระหว่างหน่วยงานที่จะทำการเชื่อมโยง

๔. กำหนดมาตรการต่าง ๆ เพื่อป้องกันและแก้ไขปัญหาที่อาจเกิดขึ้นจากการเชื่อมโยงระบบงานและข้อมูล

๕. สำรองข้อมูลในระบบงานของทั้งสองหน่วยงานก่อนการเชื่อมโยง และกำหนดให้มีการสำรองข้อมูลเป็นระยะ ๆ ตามความเหมาะสม

๖. ติดตามการปฏิบัติตามข้อตกลงและ/หรือแนวทางที่กำหนดร่วมกันอย่างเข้มงวด

๗. ตรวจสอบและประเมินปัญหา/อุปสรรค และความเสี่ยงที่เกิดขึ้นอย่างสม่ำเสมอ เพื่อนำไปปรับปรุงให้สามารถเชื่อมโยงระบบได้อย่างมีประสิทธิภาพและปลอดภัยมากขึ้น

ส่วนที่ ๑๘
แนวปฏิบัติในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

วัตถุประสงค์

๑. เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศของสำนักงานอย่างสม่ำเสมอ

๒. เพื่อป้องกันและลดความเสี่ยงที่อาจจะเกิดขึ้นกับระบบสารสนเทศของสำนักงาน

ผู้รับผิดชอบ

๑. กองติดตามประเมินผลสิ่งแวดล้อม/กลุ่มงานระบบฐานข้อมูลและเทคโนโลยีสารสนเทศ

๒. ผู้ตรวจสอบภายใน (internal auditor)

๓. ผู้ดูแลระบบสารสนเทศ

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชั่น ๒.๕) ประจำปี พ.ศ. ๒๕๕๐ ของศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕

แนวปฏิบัติ

การป้องกันและลดความเสี่ยงที่อาจจะเกิดขึ้นกับระบบสารสนเทศของสำนักงาน มีแนวปฏิบัติดังนี้

๑. การระบุและประเมินความเสี่ยงด้านระบบสารสนเทศของสำนักงาน เพื่อนำไปจัดการความเสี่ยงให้อยู่ในระดับที่สำนักงานยอมรับได้ โดยผู้ดูแลระบบสารสนเทศมีแนวปฏิบัติดังนี้

๑.๑ ระบุความเสี่ยง โดยพิจารณาให้สอดคล้องกับแผนบริหารความเสี่ยงของสำนักงาน โดยมีหัวข้อดังต่อไปนี้

๑) ความเสี่ยงจากภัยพิบัติและสถานการณ์ฉุกเฉิน

๒) ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร

๓) ความเสี่ยงด้านระบบเครือข่าย

๔) ความเสี่ยงด้านข้อมูล

๕) ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์

๖) ความเสี่ยงด้านบุคลากร

๗) ความเสี่ยงด้านการบริหารจัดการ

๑.๒ ประเมินความเสี่ยง โดยคำนึงถึงองค์ประกอบดังต่อไปนี้

๑) โอกาสในการเกิดความเสี่ยง

๒) ความถี่ในการเกิดความเสี่ยง

๓) ความรุนแรงของผลกระทบที่เกิดจากความเสี่ยง

๔) ภัยคุกคามหรือสิ่งที่อาจก่อให้เกิดเหตุการณ์ที่ระบุ

๕) จุดอ่อนหรือช่องโหว่ที่อาจถูกใช้ในการก่อให้เกิดเหตุการณ์ที่ระบุ

๑.๓ จัดทำแผนการลดความเสี่ยงหรือกำหนดวิธีการลดความเสี่ยง และดำเนินการให้เป็นไปตามวิธีการที่กำหนดขึ้น

๑.๔ ตรวจสอบว่าวิธีการลดความเสี่ยงที่กำหนดไว้ สามารถลดความเสี่ยงได้ตามที่ต้องการหรือไม่ เพื่อนำไปปรับปรุงวิธีการลดความเสี่ยงให้เหมาะสม

๒. การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศของสำนักงาน มีแนวปฏิบัติดังนี้

๒.๑ กำหนดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศของสำนักงาน (Information security audit and assessment) อย่างน้อยปีละ ๑ ครั้ง

๒.๒ การตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการโดยผู้ตรวจสอบของหน่วยงาน (Internal auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External auditor)

ส่วนที่ ๑๙
แนวปฏิบัติในการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย

วัตถุประสงค์

เพื่อบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยที่เกิดขึ้นให้กลับเข้าสู่สภาวะปกติ

ผู้รับผิดชอบ

๑. กองติดตามประเมินผลสิ่งแวดล้อม/กลุ่มงานระบบฐานข้อมูลและเทคโนโลยีสารสนเทศ

๒. ผู้ดูแลระบบสารสนเทศ

๓. ผู้ดูแลระบบ

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชั่น ๒.๕) ประจำปี พ.ศ. ๒๕๕๐ ของศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕

แนวปฏิบัติ

กรณีเกิดเหตุการณ์ที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัย หรือมาตรการป้องกันที่ล้มเหลว หรือเกิดสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (unwanted or unexpected) ซึ่งอาจทำให้ระบบของสำนักงานถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม เมื่อได้รับแจ้งเกี่ยวกับเหตุการณ์ที่เกิดขึ้นจากผู้ใช้งานหรือผู้ที่เกี่ยวข้อง ผู้ดูแลระบบสารสนเทศและผู้ดูแลระบบ มีแนวปฏิบัติดังนี้

๑. ประเมินผลกระทบของเหตุการณ์ที่เกิดขึ้น ว่ามีระบบสารสนเทศ ระบบงาน หรือฐานข้อมูลใดบ้างที่ได้รับผลกระทบและเกิดความเสียหาย และแต่ละระบบได้ผลกระทบในระดับใด

๒. วิเคราะห์สาเหตุของปัญหาที่เกิดขึ้น และแก้ไขสถานการณ์ตามความจำเป็น เช่น กรณีการบุกรุกระบบ การโจมตีระบบ ด้วยโปรแกรมไวรัสคอมพิวเตอร์ หรือการถูกเข้ารหัสลับ เป็นต้น และความเสียหายที่เกิดขึ้น และประสานผู้ดูแลเครือข่าย หรือผู้ที่มีความเชี่ยวชาญ ช่วยเหลือในการแก้ไขปัญหา

๓. ป้องกันมิให้เกิดการโจมตีเพิ่มเติม และกู้คืนระบบและข้อมูลที่ถูกโจมตี

๔. แจ้งผู้รับผิดชอบระบบที่ถูกโจมตีทราบ เพื่อประสานผู้พัฒนาระบบในการติดตั้งระบบใหม่ และนำข้อมูลที่สำรองไว้เข้าสู่ระบบ

๕. ตรวจสอบช่องทางการโจมตี หรือการบุกรุก และปรับปรุงวิธีการป้องกัน และจัดการกับช่องโหว่ที่เกิดขึ้น เพื่อป้องกันมิให้เกิดเหตุการณ์ในลักษณะดังกล่าวขึ้นอีกในอนาคต

๖. รายงานให้ผู้บังคับบัญชาทราบเหตุการณ์ที่เกิดขึ้น พร้อมทั้งรายงานผลการแก้ไขปัญหาดังกล่าว

๗. ผู้ดูแลระบบสารสนเทศ ผู้ดูแลเครือข่าย ผู้ดูแลระบบ และผู้ที่เกี่ยวข้อง ร่วมกันกำหนดแผนงาน แนวทาง หรือวิธีปฏิบัติที่เหมาะสมเพื่อแก้ไขสาเหตุของปัญหาดังกล่าว รวมทั้งติดตามตรวจสอบอย่างสม่ำเสมอ

ส่วนที่ ๒๐
แนวปฏิบัติในการสร้างความตระหนักเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ

วัตถุประสงค์

๑. เพื่อสร้างความรู้ความเข้าใจเกี่ยวกับการใช้งานระบบสารสนเทศอย่างอย่างปลอดภัย

๒. เพื่อป้องกันการกระทำผิดเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศของผู้ใช้งาน

ผู้รับผิดชอบ

๑. กองติดตามประเมินผลสิ่งแวดล้อม/กลุ่มงานระบบฐานข้อมูลและเทคโนโลยีสารสนเทศ

๒. ผู้ดูแลระบบสารสนเทศ

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชั่น ๒.๕) ประจำปี พ.ศ. ๒๕๕๐ ของศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕

แนวปฏิบัติ

การสร้างความตระหนักเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อป้องกันการกระทำผิดเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศของผู้ใช้งาน มีแนวปฏิบัติดังนี้

๑. การให้ความรู้เกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศแก่ผู้ใช้งาน อย่างน้อยปีละ ๑ ครั้ง

๑.๑ จัดอบรม/ชี้แจงแนวปฏิบัติต่าง ๆ ภายใต้นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงาน โดยอาจใช้วิธีการเสริมเนื้อหาภายใต้นโยบายฯ ฉบับนี้เข้ากับหลักสูตรการอบรมอื่น ๆ ของสำนักงาน

๑.๒ จัดอบรมเกี่ยวกับกฎหมายและระเบียบต่าง ๆ ที่เกี่ยวข้องกับการใช้งานคอมพิวเตอร์และระบบสารสนเทศ และเรื่องอื่น ๆ ที่เกี่ยวข้องกับนโยบายฯ ฉบับนี้ อย่างสม่ำเสมอ

๒. การประชาสัมพันธ์และเผยแพร่ความรู้เกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ

๒.๑ จัดทำสื่อประชาสัมพันธ์แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงาน และ/หรือความรู้ทั่วไปเกี่ยวกับการใช้งานระบบสารสนเทศอย่างปลอดภัย ในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย

๒.๒ เผยแพร่ผ่านทางช่องทางต่าง ๆ ทั้งการทำหนังสือเป็นลายลักษณ์อักษร และแจ้งเวียนผ่านระบบสารบรรณอิเล็กทรอนิกส์ รวมทั้งประกาศในระบบอินทราเน็ตของ สผ.

ภาคผนวก

แนวทางการบริหารจัดการระบบสารสนเทศ
สำนักงานนโยบายและแผนทรัพยากรธรรมชาติและสิ่งแวดล้อม

วัตถุประสงค์

เพื่อให้การบริหารจัดการระบบสารสนเทศของสำนักงานนโยบายและแผนทรัพยากรธรรมชาติและสิ่งแวดล้อม (สผ.) เป็นไปด้วยความเรียบร้อยและมีประสิทธิภาพมากขึ้น

ขอบเขต

แนวปฏิบัตินี้ ครอบคลุมถึงการจัดทำระบบสารสนเทศทั้งหมดใน สผ. ได้แก่ เว็บไซต์, เว็บเพจ, เว็บแอปพลิเคชัน, โมบายแอปพลิเคชัน และฐานข้อมูล

ข้อปฏิบัติ

๑. ก่อนเสนอขอตั้งงบประมาณโครงการจัดทำ/พัฒนา/ปรับปรุงระบบสารสนเทศทุกประเภท กอง/กลุ่มอิสระ ต้องแจ้งให้กลุ่มงานระบบฐานข้อมูลและเทคโนโลยีสารสนเทศ กตป. ทราบ พร้อมทั้งส่ง (ร่าง) ข้อกำหนดขอบเขตของงาน (TOR) เพื่อนำเสนอคณะทำงานเทคโนโลยีสารสนเทศและการสื่อสาร สผ. พิจารณาให้ความเห็นชอบก่อนดำเนินการทุกครั้ง และปฏิบัติตามแนวทางดังนี้

(๑) กรณีที่เป็นเว็บไซต์ที่จัดทำขึ้นภายใต้โครงการ ขอให้จัดทำเป็นเว็บเพจแทนเว็บไซต์ และอยู่ภายใต้เว็บไซต์หลักของกอง/กลุ่มอิสระ

(๒) กรณีจัดทำฐานข้อมูล จะต้องระบุให้มีการจัดทำบัญชีข้อมูล (Data Catalog) และเมทาดาตา (Metadata) ไว้ด้วย

(๓) กรณีที่ไม่ได้จัดหาเครื่องคอมพิวเตอร์แม่ข่ายสำหรับระบบสารสนเทศไว้ และประสงค์จะจัดหาคอมพิวเตอร์แม่ข่ายดังกล่าว จะต้องแจ้งให้กลุ่มงานระบบฐานข้อมูลและสารสนเทศทราบล่วงหน้า

(๔) กรณีกอง/กลุ่มอิสระ จะเข้าดำเนินการใด ๆ กับเครื่องคอมพิวเตอร์แม่ข่าย จะต้องแจ้งรายละเอียดให้กลุ่มงานระบบฐานข้อมูลและเทคโนโลยีสารสนเทศ กตป. ทราบล่วงหน้า

(๕) กรณีจัดทำเว็บแอปพลิเคชัน โมบายแอปพลิเคชันหรือฐานข้อมูลอื่นในลักษณะเดียวกัน จะต้องแจ้งรายละเอียดให้กลุ่มงานระบบฐานข้อมูลและเทคโนโลยีสารสนเทศทราบด้วย

๒. กอง/กลุ่มอิสระ ต้องมอบหมายเจ้าหน้าที่เพื่อทำหน้าที่ประสานงานกับกลุ่มงานระบบฐานข้อมูลและเทคโนโลยีสารสนเทศ กตป. เกี่ยวกับการจัดทำ/พัฒนา/ปรับปรุงระบบสารสนเทศตามข้อ ๑. จนกว่าการดำเนินการจะแล้วเสร็จ

๓. กอง/กลุ่มอิสระ ต้องมอบหมายเจ้าหน้าที่เพื่อทำหน้าที่ดูแลระบบสารสนเทศที่จัดทำขึ้น (Admin) ผู้นำเข้าข้อมูล และผู้ตรวจสอบความถูกต้องของข้อมูลเป็นลายลักษณ์อักษร รวมทั้งจะต้องปรับปรุงข้อมูลให้เป็นปัจจุบัน และตรวจสอบและปรับปรุงเวอร์ชั่นของโปรแกรมที่ใช้ในการพัฒนาระบบสารสนเทศดังกล่าวให้เป็นปัจจุบัน เพื่อให้สามารถใช้งานได้อย่างต่อเนื่อง รวมทั้งกำหนดให้มีแผนการพัฒนาและบำรุงรักษาระบบเป็นระยะ ๆ

๔. กอง/กลุ่มอิสระ ต้องจัดเก็บรายละเอียดของระบบสารสนเทศที่จัดทำขึ้นไว้ในที่ปลอดภัยและพร้อมใช้งาน และส่งข้อมูลอย่างน้อยดังต่อไปนี้ให้กลุ่มงานระบบฐานข้อมูลและเทคโนโลยีสารสนเทศ กตป. เพื่อนำไปใช้ในการบริหารจัดการต่อไป ดังนี้

(๑) ชื่อผู้ดูแลระบบ (Admin) ผู้นำเข้าข้อมูล และผู้ตรวจสอบความถูกต้องของข้อมูล พร้อมหมายเลขโทรศัพท์ และจดหมายอิเล็กทรอนิกส์ และหากมีการเปลี่ยนแปลงผู้ทำหน้าที่ดังกล่าว ต้องแจ้งให้กลุ่มงานระบบฐานข้อมูลและเทคโนโลยีสารสนเทศ กตป. ทราบทุกครั้ง

(๒) รายละเอียดของระบบสารสนเทศที่จัดทำขึ้น เช่น ชื่อของโปรแกรมและเวอร์ชั่นที่ใช้ในการพัฒนา และคู่มือการดูแลระบบ เป็นต้น

๕. หากไม่ได้ใช้งานหรือต้องการยกเลิกการใช้งานระบบสารสนเทศที่จัดทำแล้วเสร็จ กอง/กลุ่มอิสระ ต้องแจ้งให้ กลุ่มงานระบบฐานข้อมูลและเทคโนโลยีสารสนเทศ กตป. ทราบทุกครั้ง

๖. หากต้องมีการเชื่อมโยงและแลกเปลี่ยนข้อมูลกับระบบอื่น ทั้งภายในและภายนอก สผ. และ/หรือ การอนุญาตให้ใช้ฐานข้อมูล กอง/กลุ่มอิสระ ต้องแจ้งให้กลุ่มงานระบบฐานข้อมูลและเทคโนโลยีสารสนเทศ กตป. ทราบทุกครั้ง

แนวทางปฏิบัติในการใช้สื่อสังคมออนไลน์
สำนักงานนโยบายและแผนทรัพยากรธรรมชาติและสิ่งแวดล้อม

วัตถุประสงค์

เพื่อให้บุคลากรของ สผ. สามารถใช้สื่อสังคมออนไลน์ได้อย่างเหมาะสม และมีประสิทธิภาพ รวมทั้งไม่ก่อให้เกิดความเสียหาย ทั้งต่อตนเอง ผู้อื่น และองค์กร

ขอบเขต

แนวทางปฏิบัตินี้ ครอบคลุมการใช้สื่อสังคมออนไลน์ทุกชนิด รวมทั้งเว็บไซต์ ทั้งในประเทศและต่างประเทศที่ให้บริการในลักษณะสื่อสังคมออนไลน์ ทั้งการใช้งานผ่านเครือข่ายอินเทอร์เน็ตของ สผ. และเครือข่ายอื่น

คำนิยาม

- **สื่อสังคมออนไลน์** (Social Media & Social Network) หมายถึง สื่อดิจิทัลที่เป็นเครื่องมือในการปฏิบัติการทางสังคม (Social Tool) หรือที่ใช้เผยแพร่ข้อมูลและแสดงความคิดเห็นบนโลกออนไลน์ เพื่อใช้สื่อสารระหว่างกันในเครือข่ายทางสังคม (Social Network) ผ่านทางเว็บไซต์และโปรแกรมประยุกต์บนสื่อใด ๆ ที่มีการเชื่อมต่อกับอินเทอร์เน็ต โดยเน้นให้ผู้ใช้ทั้งที่เป็นผู้ส่งสารและผู้รับสารมีส่วนร่วม (Collaborative) อย่างสร้างสรรค์ ในการผลิตเนื้อหาขึ้นเอง (User-Generate Content: UGC) ในรูปของข้อมูล ภาพ และเสียง
- **ประเภทของสื่อสังคมออนไลน์** แบ่งเป็นกลุ่มหลักตามลักษณะของการนำมาใช้งานออกเป็น ๙ กลุ่ม ดังนี้

๑. Weblogs หรือ Blogs คือ สื่อส่วนบุคคลบนอินเทอร์เน็ตที่ใช้เผยแพร่ข้อมูล ข่าวสาร ความรู้ ข้อคิดเห็น บันทึกส่วนตัว โดยสามารถแบ่งปันให้บุคคลอื่น ๆ โดยผู้รับสารสามารถเข้าไปอ่าน หรือแสดงความคิดเห็นเพิ่มเติมได้ ตัวอย่างเช่น Exteen, Bloggang, Wordpress, Blogger, Blockdit เป็นต้น

๒. Social Networking หรือเครือข่ายทางสังคมในอินเทอร์เน็ต ใช้สำหรับเชื่อมต่อระหว่างบุคคล กลุ่มบุคคล เพื่อให้เกิดเป็นกลุ่มสังคม (Social Community) เพื่อร่วมกันแลกเปลี่ยนและแบ่งปันข้อมูลระหว่างกัน ตัวอย่างเช่น Facebook, Linkedin, MySpace, Instagram, Line, Messenger, Whatsapp เป็นต้น

๓. Micro Blogging และ Micro Sharing หรือ “บล็อกจิ๋ว” เป็นเว็บเซอร์วิสหรือเว็บไซต์ที่ให้บริการแก่บุคคลทั่วไป สำหรับให้ผู้ใช้บริการเขียนข้อความสั้นๆ เพื่อแสดงสถานะของตัวเองว่ากำลังทำอะไรอยู่ หรือแจ้งข่าวสารต่าง ๆ แก่กลุ่มเพื่อนในสังคมออนไลน์ ตัวอย่างเช่น Twitter

๔. Online Video เป็นเว็บไซต์ที่ให้บริการวิดีโอออนไลน์โดยไม่เสียค่าใช้จ่าย โดยผู้ใช้สามารถเลือกชมเนื้อหาได้ตามความต้องการ และยังสามารถเชื่อมโยงไปยังเว็บวิดีโออื่น ๆ ที่เกี่ยวข้องได้เป็นจำนวนมาก ตัวอย่างเช่น Youtube, MSN, Yahoo เป็นต้น

๕. Photo Sharing เป็นเว็บไซต์ที่เน้นให้บริการฝากรูปภาพ โดยผู้ใช้บริการสามารถอัพโหลดและดาวน์โหลดรูปภาพเพื่อนำมาใช้งานได้ ตัวอย่างเช่น Flickr, Photobucket, Express, Shutterstock, Pixabay เป็นต้น

๖. Wikis เป็นเว็บไซต์ที่มีลักษณะเป็นแหล่งข้อมูลหรือความรู้ (Data/Knowledge) ซึ่งผู้ใช้สามารถเขียนหรือแก้ไขข้อมูลได้อย่างอิสระ ตัวอย่างเช่น Wikipedia, Google Earth เป็นต้น

๗. Virtual Worlds คือ ใช้เพื่อสื่อสารระหว่างกันบนอินเทอร์เน็ตในลักษณะโลกเสมือนจริง (Virtual Reality) ซึ่งผู้ที่จะเข้าไปใช้บริการอาจจะต้องเสียค่าใช้จ่ายในการซื้อพื้นที่ เพื่อให้บุคคลในบริษัทหรือองค์กรได้มีช่องทางในการนำเสนอเรื่องราวต่าง ๆ ไปยังกลุ่มเครือข่ายผู้ใช้สื่อออนไลน์ ซึ่งอาจจะเป็นกลุ่มลูกค้า ผู้ที่เกี่ยวข้องกับธุรกิจของบริษัทหรือองค์กร ตัวอย่างเช่น Second life

๘. Crowd Sourcing เป็นหลักการขอความร่วมมือจากบุคคลในเครือข่ายสังคมออนไลน์ โดยสามารถจัดทำในรูปของเว็บไซต์ที่มีวัตถุประสงค์หลักเพื่อค้นหาคำตอบและวิธีการแก้ปัญหาต่าง ๆ โดยดึงความร่วมมือจากเครือข่ายทางสังคมมาช่วยตรวจสอบข้อมูล เสนอความคิดเห็น หรือให้ข้อเสนอแนะ ตัวอย่างเช่น Idea storm, Mystarbucks Idea เป็นต้น

๙. Podcasting หรือ Podcast คือ การบันทึกภาพและเสียงแล้วนำมาไว้ในเว็บเพจ เพื่อเผยแพร่ให้บุคคลภายนอกที่สนใจดาวน์โหลดเพื่อนำไปใช้งาน ตัวอย่างเช่น Dual Geek Podcast, Wiggly Podcast เป็นต้น

๑๐. Discuss / Review/ Opinion เป็นเว็บบอร์ดที่ผู้ใช้อินเทอร์เน็ตสามารถแสดงความคิดเห็น ตัวอย่างเช่น Epinions, Mouthshut, Yahoo!Answer, Pantip เป็นต้น

- **องค์กร** หมายถึง สำนักงานนโยบายและแผนทรัพยากรธรรมชาติและสิ่งแวดล้อม (สผ.)
- **หน่วยงานภายใน** หมายถึง กองและกลุ่มอิสระใน สผ.
- **ผู้ใช้งาน** หมายถึง บุคลากรภายใน สผ. ได้แก่ ข้าราชการ ลูกจ้างประจำ พนักงานราชการ พนักงานกองทุนสิ่งแวดล้อม พนักงานจ้างเหมา และลูกจ้างอื่นขององค์กร
- **ผู้มีส่วนได้ส่วนเสีย** หมายถึง บุคคลภายนอก เช่น ผู้รับบริการ ประชาชน นักเรียน นักศึกษา บุคคลทั่วไป หน่วยงานราชการ รัฐวิสาหกิจ องค์การมหาชน ภาคเอกชน องค์กรพัฒนาเอกชน องค์กรระหว่างประเทศ เป็นต้น
- **โพสต์** หมายถึง การนำข้อความตัวอักษร รูปภาพ หรือคลิปวิดีโอ เข้าสู่สังคมออนไลน์ เพื่อแสดงความคิดเห็น หรือเผยแพร่ข้อมูลข่าวสาร

แนวทางปฏิบัติ

แนวทางปฏิบัติทั่วไป

๑. การใช้งานสื่อสังคมออนไลน์ทุกประเภท จะต้องปฏิบัติตามแนวนโยบายขององค์กร รวมทั้งพระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. ๒๕๔๐ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ และที่แก้ไขเพิ่มเติม พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ตลอดจนกฎหมายอื่น ๆ ที่อาจเกี่ยวข้อง

๒. ผู้ใช้งานต้องรับผิดชอบข้อความ รูปภาพ วิดีโอ และ/หรือความเห็นของตนเอง ที่เผยแพร่บนสื่อสังคมออนไลน์ ทั้งทางด้านสังคม และด้านกฎหมาย

๓. กรณีมีบัญชีผู้ใช้ (Account) หลายบัญชี ควรแยกบัญชีผู้ใช้ (Account) ระหว่างการใช้เพื่อเรื่องส่วนตัว และเรื่องหน้าที่การงานออกจากกันอย่างชัดเจน

แนวทางปฏิบัติในการใช้งานในนามองค์กร

๑. การใช้สื่อสังคมออนไลน์เพื่อเผยแพร่ข้อมูลเกี่ยวกับภารกิจหรือข้อมูลเกี่ยวกับองค์กรและหน่วยงานภายใน จะต้องได้รับความเห็นชอบจากผู้อำนวยการกอง/ผู้อำนวยการกลุ่มงานโดยตรงก่อนดำเนินการ

๒. ข้อมูลหรือความเห็นที่เกี่ยวกับองค์กรที่นำไปเผยแพร่ จะต้องได้รับอนุญาตจากผู้มีหน้าที่เกี่ยวข้องแล้ว

๓. ห้ามเผยแพร่ข้อมูลที่เป็นทรัพย์สินทางปัญญา สถานะทางการเงิน และอื่น ๆ หรือข้อมูลที่ใช้ภายในองค์กร ก่อนได้รับอนุญาตอย่างเป็นทางการจากผู้บริหารหรือผู้ที่ได้รับมอบอำนาจจากผู้บริหาร

๔. หากต้องการสร้าง Page หรือ Account เพื่อเป็นช่องทางในการเผยแพร่ข้อมูลอย่างเป็นทางการของหน่วยงาน ต้องแจ้งให้ผู้อำนวยการกลุ่มงานระบบฐานข้อมูลและเทคโนโลยีสารสนเทศ กตป. และ/หรืองานประชาสัมพันธ์ขององค์กรทราบ และต้องแจ้งรายชื่อของผู้ดูแล (Admin) ของ Page หรือ Account นั้นให้กลุ่มงานระบบฐานข้อมูลและเทคโนโลยีสารสนเทศทราบ และ/หรืองานประชาสัมพันธ์ทราบด้วย และผู้ดูแล Page หรือ Account จะต้องมอบสิทธิ์ในการดูแล Page หรือ Account นั้น คืนแก่หน่วยงานเมื่อมีการโยกย้ายหรือเปลี่ยนแปลงตำแหน่ง หรือพ้นสภาพจากการเป็นบุคลากรของ สผ.

๕. หากพบเห็นการบิดเบือนข้อเท็จจริงหรือมีข้อความบน Social Media & Social Network หรือพบเห็นประเด็นขัดแย้งอื่น ๆ ที่เกี่ยวข้องกับองค์กร ที่อาจทำให้เกิดความเสื่อมเสียชื่อเสียงขององค์กร สามารถแจ้งให้กองติดตามประเมินผลสิ่งแวดล้อม/องค์กร ทราบโดยเร็วที่สุด เพื่อนำเสนอผู้บริหารพิจารณา ทั้งนี้ หลีกเลี่ยงการถกเถียงหรือโต้ตอบและพาดพิงไปยังผู้อื่น เพื่อนำเรียนผู้บังคับบัญชาทราบตามลำดับชั้นต่อไป

แนวทางปฏิบัติในการใช้งานส่วนบุคคล

๑. ไม่อนุญาตให้นำตราสัญลักษณ์ (logo) ชื่อเต็มและชื่อย่อขององค์กร ไว้ในรูปประกอบ profile ของตน

๒. ควรหลีกเลี่ยงการนำรูปบุคคลอื่น มาแสดงว่าเป็นรูปโปรไฟล์ของตนเอง และหลีกเลี่ยงโพสต์ภาพที่อาจทำให้เกิดความเข้าใจผิดเกี่ยวกับความเชื่อทางศาสนาการเมือง และสถาบันพระมหากษัตริย์

๓. ควรโพสต์หรือแสดงความคิดเห็นด้วยข้อความที่สุภาพ งดเว้นการใช้ถ้อยคำและภาษาที่อาจเป็นการดูหมิ่น ยุยง ท้าทาย รวมทั้งหลีกเลี่ยงการกล่าวถึง พาดพิง หรือก่อให้เกิดความเสียหายต่อบุคคล องค์กร และ/หรือหน่วยงานอื่น และในกรณีที่บุคคลอื่นมีความคิดเห็นที่แตกต่าง พึงงดเว้นการโต้ตอบด้วยถ้อยคำที่รุนแรง

๔. งดเว้นการเผยแพร่ข้อความหรือความคิดเห็นที่ละเมิดทรัพย์สินทางปัญญาของผู้อื่นหรือละเมิดสิทธิส่วนบุคคล รวมทั้งความคิดเห็นที่อาจกระตุ้นหรือนำไปสู่การโต้แย้งที่รุนแรง เช่น เรื่องเกี่ยวกับการเมืองหรือศาสนา

๕. งดเว้นการแสดงสัญลักษณ์พรรคการเมือง กลุ่มผู้ชุมนุมทางสังคมและการเมือง กลุ่มลัทธิทางศาสนา และสัญลักษณ์อื่น ๆ ที่อาจก่อให้เกิดความขัดแย้ง รวมทั้งภาพลามกอนาจาร ภาพความรุนแรงในสังคม ภาพการดื่มสุราหรือเสพยาเสพติด ภาพการเล่นการพนัน และการกระทำความผิดทางกฎหมายในลักษณะอื่น ๆ

๖. งดเว้นการส่งต่อข้อมูลที่เป็นเท็จ ข่าวลือ ข่าวไม่ปรากฏที่มา หรือข้อมูลที่เป็นเพียงการคาดเดา รวมทั้งข้อมูลที่กระทบต่อสิทธิ ความเป็นส่วนตัว และศักดิ์ศรีความเป็นมนุษย์

๗. หากต้องการกล่าวอ้างถึงข้อมูลที่สนับสนุนข้อความของตน ควรอ้างอิงแหล่งที่มาของข้อมูลนั้นอย่างชัดเจน

๘. การเผยแพร่ข้อมูล หรือแสดงความเห็นที่อาจทำให้เข้าใจว่าเป็นความเห็นขององค์กร ต้องมีการแสดงข้อความจำกัดความรับผิดชอบ (Disclaimer) ว่า เป็นความเห็นส่วนตัว มิใช่ความเห็นขององค์กร หรือหน่วยงานที่ตนสังกัด

๙. หากการเผยแพร่ข้อมูลหรือการแสดงความคิดเห็นผ่านสื่อสังคมออนไลน์ เกิดความผิดพลาดจนก่อให้เกิดความเสียหายต่อบุคคลหรือหน่วยงานอื่น ต้องดำเนินการแก้ไขข้อความที่มีปัญหาโดยทันที พร้อมทั้งแสดงถ้อยคำขอโทษต่อบุคคลหรือหน่วยงานที่ได้รับความเสียหาย

แนวทางการบริหารจัดการเฟซบุ๊กหลักของ สผ.

๑. กอง/กลุ่มอิสระมอบหมายเจ้าหน้าที่เพื่อกำหนดสิทธิ์เป็นผู้โพสต์ในเฟซบุ๊กหลักของ สผ. หน่วยงานละไม่เกิน ๒ คน เพื่อร่วมกับ สลก./กลุ่มงานอำนวยการและประชาสัมพันธ์ (กอป.) ทำหน้าที่บริหารจัดการเฟซบุ๊ก

๒. ให้ สลก./กอป. ตั้งกลุ่มไลน์สำหรับผู้ดูแลเฟซบุ๊กหลักของ สผ. เพื่อใช้แจ้งข้อมูล/หารือเกี่ยวกับการบริหารจัดการเฟซบุ๊ก

๓. เนื้อหาที่โพสต์ ขอให้คัดเลือกเฉพาะข้อมูลที่สำคัญ เช่น การจัดประชุม/กิจกรรม บทความและองค์ความรู้ รวมถึงการนำเสนอคลิปวีดิโอ และ infographic ต่าง ๆ

๔. เรื่องที่โพสต์ต้องได้รับความเห็นชอบจาก ผอ.กอง/กลุ่มอิสระ ก่อนทุกครั้ง

๕. ช่วงเวลาในการโพสต์ ขอให้อยู่ระหว่างเวลา ๐๙.๐๐ - ๑๘.๐๐ น.

๖. การโพสต์ในเฟซบุ๊กหลักของ สผ. ท้ายเรื่องที่ลงประชาสัมพันธ์ ขอให้เจ้าหน้าที่ที่ได้รับมอบหมายปฏิบัติดังนี้

๖.๑ พิมพ์ข้อความ “จัดทำและประชาสัมพันธ์โดย (ระบุชื่อกอง/กลุ่มอิสระ)” เช่น จัดทำและประชาสัมพันธ์โดยสำนักงานเลขานุการกรม

๖.๒ พิมพ์เครื่องหมาย hashtag “#(ระบุชื่อกอง/กลุ่มอิสระ)” เช่น #สำนักงานเลขานุการกรม

๗. กรณีที่มีการสอบถาม/ข้อมูล ขอให้กอง/กลุ่มอิสระที่มีการดำเนินงานเกี่ยวข้องกับประเด็นนั้น ๆ เป็นผู้ตอบ

๘. กรณีผู้โพสต์มีความประสงค์จะร้องเรียน ขอให้แจ้งผู้โพสต์ให้ร้องเรียนไปที่ http://e-petition.onep.go.th/ เพื่อเข้าสู่ระบบรับแจ้งเรื่องร้องเรียนอย่างเป็นทางการของ สผ. ต่อไป

นโยบายการรักษาความมั่นคงปลอดภัยในการใช้งานจดหมายอิเล็กทรอนิกส์ (E-mail)
สำนักงานนโยบายและแผนทรัพยากรธรรมชาติและสิ่งแวดล้อม

๑. วัตถุประสงค์

เพื่อกำหนดแนวทางปฏิบัติในการใช้งานจดหมายอิเล็กทรอนิกส์ (E-mail) ของสำนักงานนโยบายและแผนทรัพยากรธรรมชาติและสิ่งแวดล้อม (สผ.) ให้เป็นไปอย่างเหมาะสมและปลอดภัย

๒. คำนิยาม

“ผู้ดูแลระบบ” หมายถึง เจ้าหน้าที่กลุ่มงานระบบฐานข้อมูลและเทคโนโลยีสารสนเทศ กองติดตามประเมินผลสิ่งแวดล้อม ที่ได้รับมอบหมายให้ทำหน้าที่ดูแลระบบจดหมายอิเล็กทรอนิกส์ (E-mail) ของ สผ.

“ผู้ใช้” หมายถึง บุคลากรของ สผ. ที่ลงทะเบียนใช้งานระบบจดหมายอิเล็กทรอนิกส์ (E-mail) ของ สผ. (mail.onep.go.th)

๓. แนวทางปฏิบัติ

๓.๑ แนวทางปฏิบัติสำหรับผู้ดูแลระบบ

๓.๑.๑ กำหนดสิทธิในการใช้งานระบบจดหมายอิเล็กทรอนิกส์ของ สผ.

๓.๑.๒ จัดทำบัญชีผู้ใช้งานและปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๓.๑.๓ เก็บรักษาข้อมูลการขอใช้บริการจดหมายอิเล็กทรอนิกส์และรหัสผ่านของผู้ใช้แต่ละคนไว้เป็นความลับ

๓.๒ แนวทางปฏิบัติสำหรับผู้ใช้

๓.๒.๑ บุคลากรของ สผ. ที่ต้องการใช้งานจดหมายอิเล็กทรอนิกส์ของ สผ. จะต้องกรอกข้อมูลคำขอลงทะเบียนตามแบบฟอร์มการขอใช้บริการจดหมายอิเล็กทรอนิกส์กลางเพื่อการสื่อสารในภาครัฐ (mail.onep.go.th) ของ สผ. และยื่นต่อผู้ดูแลระบบเพื่อกำหนดสิทธิในการใช้งาน

๓.๒.๒ เมื่อผู้ดูแลระบบกำหนดสิทธิในการใช้งาน และแจ้งยืนยันบัญชีผู้ใช้งานจดหมายอิเล็กทรอนิกส์ของ สผ. ให้ทราบแล้ว เพื่อความปลอดภัยควรเปลี่ยนรหัสผ่าน (Password) ทันที

๓.๒.๓ ควรเก็บข้อมูลรหัสผ่านไว้เป็นความลับ ไม่ควรเผยแพร่แก่บุคคลอื่น และไม่ควรตั้งค่าการจำรหัสผ่าน (Save password) แบบอัตโนมัติ

๓.๒.๔ ควรใช้จดหมายอิเล็กทรอนิกส์ของ สผ. เพื่อการปฏิบัติงานที่เกี่ยวข้องกับภารกิจของ สผ. เท่านั้น

๓.๒.๕ ห้ามใช้จดหมายอิเล็กทรอนิกส์ของ สผ. ในการแสวงหาผลประโยชน์ทางธุรกิจหรือผลประโยชน์ส่วนตัว

๓.๒.๖ เจ้าของบัญชีผู้ใช้ต้องเป็นผู้รับผิดชอบต่อการกระทำใด ๆ ต่อจดหมายอิเล็กทรอนิกส์ของตน

๓.๒.๗ ไม่ควรใช้บัญชีผู้ใช้ของบุคคลอื่นใน สผ. เพื่อรับ-ส่งจดหมายอิเล็กทรอนิกส์ เว้นแต่จะได้รับความยินยอมจากเจ้าของบัญชีผู้ใช้

๓.๒.๘ การใช้งานจดหมายอิเล็กทรอนิกส์กลางของกอง/กลุ่มอิสระ/กลุ่มงาน ผู้ใช้จะต้องเป็นผู้ที่ได้รับมอบหมายจากผู้อำนวยการกอง/กลุ่มอิสระ/กลุ่มงาน เท่านั้น

๓.๒.๙ ไม่ควรเปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์จากผู้ส่งที่ไม่รู้จัก

๓.๒.๑๐ ควรตรวจสอบไฟล์เอกสารแนบของจดหมายอิเล็กทรอนิกส์ทุกครั้งก่อนทำการดาวน์โหลด และไม่ควรเปิดไฟล์เอกสารแนบหรือกดลิ้งค์จากผู้ส่งที่ไม่รู้จัก

๓.๒.๑๑ ควรตรวจสอบความถูกต้องของไฟล์เอกสารที่จะแนบไปกับจดหมายอิเล็กทรอนิกส์ทุกครั้งก่อนส่ง

๓.๒.๑๒ ห้ามส่งจดหมายอิเล็กทรอนิกส์ที่มีถ้อยคำหรือข้อความที่ไม่สุภาพ หรือมีข้อมูลที่เป็นความลับของทางราชการ ซึ่งอาจทำให้เกิดความเสื่อมเสียหรือเสียหายต่อ สผ. ได้

๓.๒.๑๓ ห้ามส่งหรือส่งต่อจดหมายอิเล็กทรอนิกส์ที่มีไวรัสคอมพิวเตอร์ หรือโปรแกรมที่อาจเป็นอันตรายต่อเครื่องคอมพิวเตอร์หรือระบบเครือข่ายไปให้บุคคลอื่นโดยเจตนา

๓.๒.๑๔ ห้ามส่งหรือส่งต่อจดหมายอิเล็กทรอนิกส์ลูกโซ่ หรือจดหมายอิเล็กทรอนิกส์ที่เข้าข่าย Spam อย่างเด็ดขาด

๓.๒.๑๕ ห้ามส่งหรือส่งต่อจดหมายอิเล็กทรอนิกส์ที่เป็นการล่วงละเมิด ข่มขู่ สร้างความรำคาญต่อผู้อื่น หรือมีข้อความหรือเนื้อหาที่ผิดกฎหมาย หรือละเมิดศีลธรรม

๓.๒.๑๖ ควรลงชื่อออก (log out) จากระบบทุกครั้ง หลังจากใช้งานจดหมายอิเล็กทรอนิกส์เสร็จสิ้น เพื่อป้องกันบุคคลอื่นเข้าใช้งานบัญชีผู้ใช้ของท่าน