ประกาศสำนักงานกองทุนน้ำมันเชื้อเพลิง
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของสำนักงานกองทุนน้ำมันเชื้อเพลิง พ.ศ. ๒๕๖๕

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ ตามความในมาตรา ๕ และ ๗ กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานภาครัฐ หรือโดยหน่วยงานภาครัฐมีความมั่นคงและเชื่อถือได้ และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานภาครัฐ พ.ศ. ๒๕๕๓ นั้น

เพื่อให้ระบบเทคโนโลยีสารสนเทศของสำนักงานกองทุนน้ำมันเชื้อเพลิง เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง และการถูกคุกคามจากภัยต่าง ๆ จึงเห็นสมควรกำหนดนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยกำหนดให้มีมาตรฐาน (Standard) แนวปฏิบัติ (Guideline) ขั้นตอนปฏิบัติ (Procedure) ให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศตามพระราชกฤษฎีกาฯ และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ฯ จึงออกประกาศไว้ ดังต่อไปนี้

๑. ประกาศนี้เรียกว่า “ประกาศสำนักงานกองทุนน้ำมันเชื้อเพลิง เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานกองทุนน้ำมันเชื้อเพลิง พ.ศ. ๒๕๖๕”

๒. นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มีวัตถุประสงค์ ดังต่อไปนี้

๒.๑ เพื่อให้เกิดความเชื่อมั่น และมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์ของหน่วยงาน ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล

๒.๒ เพื่อให้การกำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของหน่วยงาน มีความสอดคล้องตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙

๒.๓ เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีปฏิบัติ ให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับหน่วยงาน ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้ระบบเทคโนโลยีสารสนเทศของหน่วยงาน

๓. นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กำหนดประเด็นสำคัญ ดังต่อไปนี้

๓.๑ การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

๓.๑.๑ การเข้าถึงระบบสารสนเทศ ต้องตรวจสอบการอนุมัติสิทธิการเข้าถึงระบบและกำหนดรหัสผ่าน การลงทะเบียนผู้ใช้งานเพื่อให้ผู้ใช้มีสิทธิเท่านั้น ที่สามารถเข้าถึงระบบได้ รวมถึงมีการเก็บบันทึกข้อมูลการเข้าถึงระบบและข้อมูลจราจรทางคอมพิวเตอร์

๓.๑.๒ การบริหารจัดการการเข้าถึงข้อมูลของผู้ใช้งาน เพื่อบริหารจัดการการเข้าถึงสิทธิการเข้าถึงข้อมูลให้เหมาะสมตามระดับชั้นความลับของผู้ใช้งาน ทบทวนสิทธิการใช้งาน และตรวจสอบการละเมิดความปลอดภัย

๓.๑.๓ การบริหารจัดการการเข้าถึงระดับเครือข่าย ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อใช้งานอินเทอร์เน็ตต้องผ่านระบบรักษาความปลอดภัยที่องค์กรจัดสรรไว้ เช่น Firewall, IDS/IPS, Proxy, การตรวจสอบไวรัสคอมพิวเตอร์ เป็นต้น เพื่อให้ควบคุมและป้องกันภัยคุกคามได้อย่างเป็นระบบ

๓.๑.๔ การควบคุมการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารจากภายนอก (Remote Access) โดยการกำหนดสิทธิควบคุมพอร์ต (Port) ที่ใช้เข้าสู่ระบบอย่างรัดกุมและมีการแสดงตัวตนของผู้ใช้งาน (Identification) และการยืนยันตัวตน (Authentication)

๓.๒ การจัดทำระบบสารสนเทศและระบบสำรองข้อมูลสารสนเทศ โดยกำหนดระบบสารสนเทศหรือข้อมูลที่ต้องการสำรองเก็บไว้ เรียงลำดับตามความสำคัญพร้อมทั้งกำหนดผู้รับผิดชอบในการสำรองข้อมูล และจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานระบบสารสนเทศได้อย่างต่อเนื่อง

๓.๓ การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยจัดให้ผู้ตรวจสอบภายในของหน่วยงาน (Internal Audit) หรือ ผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Audit) อย่างน้อยปีละ ๑ ครั้ง เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

๔. กำหนดให้มีการเผยแพร่นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อสร้างความรู้ความเข้าใจให้กับผู้ใช้งาน ผ่านทางเว็บไซต์และระบบอินทราเน็ตของหน่วยงาน ทั้งนี้ เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยคุกคาม และผลกระทบจากความรู้เท่าไม่ถึงการณ์ หรือขาดความระมัดระวังในการใช้ระบบสารสนเทศ

๕. ให้มีการทบทวนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้เป็นปัจจุบันอย่างน้อยปีละ ๑ ครั้ง

๖. ผู้อำนวยการสำนักงานกองทุนน้ำมันเชื้อเพลิง เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นต่อข้อมูลสารสนเทศ ระบบสารสนเทศ ระบบเครือข่าย และสินทรัพย์ของหน่วยงานหรือของผู้หนึ่งผู้ใด อันเกิดจากความบกพร่อง ละเลย ฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๗. ให้ใช้แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่แนบท้ายประกาศนี้ ซึ่งสอดคล้องกับนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน

๘. ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันออกประกาศ เป็นต้นไป

ประกาศ ณ วันที่ ๗ เดือนมีนาคม พ.ศ. ๒๕๖๕

(นายวิศักดิ์ วัฒนศัพท์)
ผู้อำนวยการสำนักงานกองทุนน้ำมันเชื้อเพลิง

เอกสารแนบท้ายประกาศ
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของสำนักงานกองทุนน้ำมันเชื้อเพลิง

ว่าด้วยนิยาม

หน่วยงาน หมายถึง สำนักงานกองทุนน้ำมันเชื้อเพลิง

ผู้บริหารระดับสูงสุด หมายถึง ผู้อำนวยการสำนักงานกองทุนน้ำมันเชื้อเพลิง

สำนักนโยบายและยุทธศาสตร์ หมายถึง สำนักที่ควบคุมดูแลการให้บริการด้านเทคโนโลยีสารสนเทศและการสื่อสาร ให้คำปรึกษา พัฒนาปรับปรุง บำรุงรักษา ระบบคอมพิวเตอร์และเครือข่าย

ผู้อำนวยการ หมายถึง ผู้อำนวยการสำนักนโยบายและยุทธศาสตร์

กลุ่มงานบริหารสารสนเทศ หมายถึง ผู้ที่ได้รับมอบหมายจากผู้อำนวยการ ให้มีหน้าที่ในการประสานงานเกี่ยวกับการติดตาม ดูแลรักษาระบบคอมพิวเตอร์และเครือข่าย ตลอดจนการถ่ายทอดนโยบายและแนวทางปฏิบัติต่าง ๆ ของหน่วยงาน

ผู้ดูแลระบบ หมายถึง เจ้าหน้าที่ของบริษัทผู้ให้เช่าคอมพิวเตอร์และอุปกรณ์ที่เกี่ยวข้อง และเจ้าหน้าที่ของบริษัทที่รับจ้างบำรุงรักษาและซ่อมแซมแก้ไขระบบเว็บไซต์ของหน่วยงาน (Outsourcing) ซึ่งมีหน้าที่รับผิดชอบดูแลรักษาหรือจัดการระบบคอมพิวเตอร์และเครือข่ายให้หน่วยงาน

ผู้ใช้งาน หมายถึง บุคคลที่ได้รับอนุญาต (Authorized user) ให้สามารถเข้าใช้งานหรือดูแลรักษาระบบเทคโนโลยีสารสนเทศของหน่วยงาน โดยมีสิทธิและหน้าที่ขึ้นอยู่กับบทบาท (role)

สิทธิของผู้ใช้งาน หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใด ที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน

สินทรัพย์ หมายถึง ข้อมูล ระบบสารสนเทศ และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสาร หรือสิ่งใดก็ตามที่มีคุณค่าของหน่วยงาน เช่น อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์ เป็นต้น

การรักษาความมั่นคงปลอดภัย หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน

การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ หมายถึง การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์ และทางภายภาพ รวมทั้งการอนุญาตสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

ความมั่นคงปลอดภัยด้านสารสนเทศ หมายถึง การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (authenticity) ความรับผิด (accountability) การห้ามปฏิเสธความรับผิด (nonrepudiation) และความน่าเชื่อถือ (reliability)

เหตุการณ์ด้านความมั่นคงปลอดภัย หมายถึง กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิด การฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (unwanted or unexpected) ซึ่งอาจทำให้ระบบของหน่วยงานถูกบุกรุกหรือโจมตี

หน่วยงานภายนอก หมายถึง องค์กรหรือหน่วยงานที่หน่วยงานอนุญาตให้มีสิทธิในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่าง ๆ ของหน่วยงาน โดยจะได้รับสิทธิในการใช้งานตามอำนาจและต้องรับผิดชอบในการรักษาความลับของข้อมูล

รหัสผ่าน (Password) หมายถึง ตัวเลข ตัวอักษรที่เป็นตัวพิมพ์เล็กหรือตัวพิมพ์ใหญ่ ตัวอักขระพิเศษและสัญลักษณ์ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

ข้อมูลคอมพิวเตอร์ หมายถึง ข้อมูล ข้อความคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

ข้อมูลอิเล็กทรอนิกส์ หมายถึง ข้อความที่ได้สร้าง ส่ง รับ เก็บรักษา หรือประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์ เช่น วิธีการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ จดหมายอิเล็กทรอนิกส์ โทรเลข โทรพิมพ์หรือโทรสาร ดังนั้น เอกสารอิเล็กทรอนิกส์ จึงถือได้ว่าเป็นข้อมูลอิเล็กทรอนิกส์ และมีผลทำให้ต้องปฏิบัติตามหลักกฎหมายที่สำคัญ คือ

- ห้ามมิให้ปฏิเสธความมีผลผูกพันและการบังคับใช้ทางกฎหมายต่อข้อมูลอิเล็กทรอนิกส์ ต่อการลงลายมือชื่ออิเล็กทรอนิกส์ด้วยวิธีการตามที่กฎหมายกำหนด ข้อมูลอิเล็กทรอนิกส์ที่มีการรับ-ส่ง การเก็บรักษาและการรักษาสภาพเอกสารต้นฉบับตามวิธีการที่กฎหมายกำหนด
- เอกสารอิเล็กทรอนิกส์ที่อยู่ในรูปแบบของ อีเมล เว็บเพจ หรือสื่ออิเล็กทรอนิกส์อย่างอื่น สามารถเป็นพยาน หลักฐานในกระบวนการพิจารณาตามกฎหมายได้
- นิติกรรมบางอย่างที่กฎหมายระบุให้ต้องทำเป็นหนังสือ สามารถทำผ่านสื่ออิเล็กทรอนิกส์ รวมถึงการแสดงเจตนาในการทำนิติกรรมสัญญาผ่านสื่ออิเล็กทรอนิกส์สามารถมีผลใช้บังคับตามกฎหมาย

ระบบเครือข่าย (Network System) หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสาร หรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ของหน่วยงานได้ เช่น ระบบแลน (LAN) ระบบอินทราเน็ต (Intranet) ระบบอินเทอร์เน็ต (Internet)

- ระบบแลน (LAN) และระบบอินทราเน็ต (Intranet) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่าง ๆ ภายในหน่วยงานเข้าด้วยกันเป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน

- ระบบอินเทอร์เน็ต (Internet) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่าง ๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตทั่วโลก

ระบบสารสนเทศ (Information System) หมายถึง ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศระบบคอมพิวเตอร์และระบบเครือข่าย มาช่วยในการสร้างสารสนเทศ ที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุม การติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรมข้อมูลและสารสนเทศ เป็นต้น

พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร (Information Technology System Workspace) หมายถึง พื้นที่ที่หน่วยงานอนุญาตให้มีการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยแบ่งเป็น

- พื้นที่ทำงานทั่วไป (General working area) หมายถึง พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคล
- พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย (IT equipment or network area)
- พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data storage area)

เจ้าของข้อมูล หมายถึง ผู้ที่ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงานโดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น ๆ หรือได้รับผลกระทบโดยตรง หากข้อมูลเหล่านั้นเกิดสูญหาย

จดหมายอิเล็กทรอนิกส์ (e-mail) หมายถึง ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกัน โดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้ง ตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้

ชุดคำสั่งไม่พึงประสงค์ หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

เอกสารแนบท้ายประกาศ
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของสำนักงานกองทุนน้ำมันเชื้อเพลิง

สารบัญ

หมวดที่ ๑

การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

วัตถุประสงค์

เพื่อให้มีการควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานตามภารกิจและความมั่นคงปลอดภัย ในเรื่องการอนุญาตให้เข้าถึง การกำหนดสิทธิ ประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล ระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึง

ผู้รับผิดชอบ

๑. สำนักนโยบายและยุทธศาสตร์
๒. กลุ่มงานบริหารสารสนเทศ
๓. ผู้ดูแลระบบ

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชัน ๒.๕)

แนวทางปฏิบัติ

๑. การเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control)

๑.๑ ผู้ดูแลระบบ ต้องจำแนกกลุ่มทรัพยากรของระบบหรือการทำงาน โดยให้กำหนดกลุ่มผู้ใช้งานและสิทธิของกลุ่มผู้ใช้งาน

๑.๒ ผู้ดูแลระบบ ต้องกำหนดสิทธิการเข้าถึงข้อมูลและระบบสารสนเทศให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งาน และหน้าที่ความรับผิดชอบในการปฏิบัติงานของผู้ใช้งานระบบสารสนเทศ รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ดังนี้

(๑) กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจ

(๑.๑) กำหนดสิทธิของกลุ่มผู้ใช้งานในการเข้าถึงข้อมูลและระบบสารสนเทศให้เหมาะสมกับการใช้งาน ดังนี้

- สิทธิในการสร้างข้อมูล (Create)
- สิทธิในการอ่านข้อมูลหรือเรียกดูข้อมูล (Read)
- สิทธิในการเปลี่ยนแปลงหรือปรับปรุงข้อมูล (Modify/Update)
- สิทธิในการมอบหมายสิทธิในการดำเนินการแทน (Assign)
- สิทธิในการรับรองความถูกต้องครบถ้วนของข้อมูล (Approve/Authenticate)
- สิทธิในการรับรองการดำเนินการจัดทำ/แปลง (Approve/Authenticate)

(๑.๒) ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับพิจารณาอนุญาตจากผู้อำนวยการสำนักนโยบายและยุทธศาสตร์หรือผู้ที่ได้รับมอบหมาย

(๒) การแบ่งประเภทของข้อมูลและการจัดลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล ใช้แนวทางตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ ซึ่งระเบียบดังกล่าวเป็นมาตรการที่ละเอียด รอบคอบ ถือว่าเป็นแนวทางที่เหมาะสมในการจัดการเอกสาร

อิเล็กทรอนิกส์ และในการรักษาความปลอดภัยของเอกสารอิเล็กทรอนิกส์ โดยได้กำหนดกระบวนการและกรรมวิธีต่อเอกสารที่สำคัญไว้ ดังนี้

(๒.๑) ประเภทข้อมูลหรือรูปแบบของเอกสารอิเล็กทรอนิกส์ แบ่งได้ดังนี้

- ข้อมูลและสารสนเทศสนับสนุนการตัดสินใจของผู้บริหาร (Early Indicator) ได้แก่ ข้อมูลและสารสนเทศที่มีความสำคัญหรือจำเป็นเร่งด่วนที่ต้องติดตามอย่างใกล้ชิดเพื่อประกอบการตัดสินใจเชิงนโยบาย การกำหนดนโยบาย และการวางแผนของผู้บริหารระดับสูง
- ข้อมูลและสารสนเทศสนับสนุนเชิงยุทธศาสตร์ (Strategy Data) ได้แก่ ข้อมูลและสารสนเทศเชิงวิชาการเพื่อสนับสนุนการดำเนินงานตามพันธกิจและยุทธศาสตร์ของหน่วยงานให้บรรลุเป้าหมาย รวมทั้งข้อมูลที่เผยแพร่แก่ผู้รับบริการภายนอก
- ข้อมูลสารสนเทศเพื่อสนับสนุนการปฏิบัติงาน (Operation Data) ได้แก่ ข้อมูลและสารสนเทศเพื่อสนับสนุนการปฏิบัติงานทั่วไปของหน่วยงาน

(๒.๒) จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น ๓ ระดับ คือ

- ข้อมูลที่มีระดับความสำคัญมาก หมายถึง มีผลกระทบในระดับที่มีนัยสำคัญต่อการดำเนินงานตามวัตถุประสงค์ขององค์กร เช่น ข้อมูลฐานะกองทุนน้ำมันเชื้อเพลิง ประมาณการสภาพคล่องของกองทุนน้ำมันเชื้อเพลิง ข้อมูลด้านน้ำมันเชื้อเพลิง และระบบบัญชีของหน่วยงาน
- ข้อมูลที่มีระดับความสำคัญปานกลาง หมายถึง มีผลกระทบต่อการดำเนินภารกิจ เช่น ข้อมูลการรับ-จ่ายเงินกองทุนน้ำมันเชื้อเพลิง
- ข้อมูลที่มีระดับความสำคัญน้อย หมายถึง ไม่มีผลกระทบใด ๆ ต่อการดำเนินภารกิจ เช่น ประกาศ คำสั่ง ภายในหน่วยงาน

(๒.๓) จัดแบ่งลำดับชั้นความลับของข้อมูล

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

(๒.๔) จัดแบ่งระดับชั้นการเข้าถึง

- ระดับชั้นสำหรับผู้บริหาร
- ระดับชั้นสำหรับผู้ใช้งานทั่วไป
- ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย

(๒.๕) กำหนดเวลาการเข้าถึงระบบสารสนเทศ ดังนี้

- ข้อมูลที่เผยแพร่บนเว็บไซต์ (www.offo.or.th) สำหรับผู้ใช้งานภายนอก สามารถเข้าถึงได้ตลอดเวลา
- ระบบงานภายใน (Back Office) สำหรับผู้ใช้งานภายใน ตามที่หน่วยงานกำหนด

(๒.๖) กำหนดช่องทางการเข้าถึง สิทธิในการเข้าถึงข้อมูลและสามารถเข้าถึงได้เฉพาะข้อมูลที่ได้รับอนุญาตเท่านั้น โดยมีช่องทางการเข้าถึง ดังนี้

- ระบบเครือข่ายภายใน (Intranet)
- ระบบเครือข่ายอินเทอร์เน็ต (Internet)
- ระบบจดหมายอิเล็กทรอนิกส์ (E-Mail)

๑.๓ ผู้ดูแลระบบ ต้องจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศของหน่วยงาน และตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบสารสนเทศ

๑.๔ ผู้ดูแลระบบ ต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบสารสนเทศและการแก้ไขเปลี่ยนแปลงสิทธิต่าง ๆ เพื่อเป็นหลักฐานในการตรวจสอบ

๒. การบริหารจัดการ การเข้าถึงของผู้ใช้งาน (User Access Management)

๒.๑ สร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (Information security awareness training) โดยจัดให้มีการฝึกอบรมให้แก่ผู้ใช้งาน ประกอบด้วย

(๑) การกำหนดหลักสูตรการฝึกอบรมเกี่ยวกับการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (information security awareness training) ได้แก่ โครงการยกระดับความรู้ด้านดิจิทัลสู่ไทยแลนด์ ๔.๐ โครงการฝึกอบรมเพื่อความปลอดภัยในการเข้าใช้งานระบบสารสนเทศของหน่วยงาน เป็นต้น

(๒) ฝึกอบรมให้ความรู้ความเข้าใจกับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม โดยกำหนดให้บุคลากรของ สกนช. เข้าร่วมการอบรม online ของสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล (TDGA) ตามหลักสูตรที่เกี่ยวข้องอย่างน้อยกลุ่มงานละ ๒ หลักสูตร และผู้ดูแลระบบจะเป็นผู้อบรมให้ความรู้เกี่ยวกับความปลอดภัยในการใช้งานคอมพิวเตอร์และเครือข่าย ให้แก่ผู้ใช้งานภายในหน่วยงาน เป็นประจำอย่างน้อยปีละ ๑ ครั้ง

๒.๒ กลุ่มงานบริหารสารสนเทศ เป็นผู้กำหนดบัญชีผู้ใช้งาน (User Account) โดยมีขั้นตอนปฏิบัติสำหรับการลงทะเบียนผู้ใช้งาน (User registration) และการตัดออกจากทะเบียนของผู้ใช้งาน โดยต้องได้รับการพิจารณาอนุมัติอย่างเป็นลายลักษณ์อักษรจากผู้อำนวยการสำนักนโยบายและยุทธศาสตร์ หรือผู้ที่ได้รับมอบหมาย ครอบคลุมประเด็นดังต่อไปนี้

(๑) ให้ผู้ใช้งานแจ้งรายละเอียดเพื่อดำเนินการตามขั้นตอน

(๒) มีการระบุชื่อบัญชีผู้ใช้งานแยกกันเป็นรายบุคคลไม่ซ้ำซ้อนกัน

(๓) การกำหนดบัญชีผู้ใช้ (Username) จะกำหนดจากชื่อภาษาอังกฤษ ทั้งนี้ ต้องควบคุมมิให้มีการใช้งานบัญชีชื่อผู้ใช้ซ้ำซ้อนกัน

(๔) การกำหนดสิทธิที่เหมาะสมกับผู้ใช้งานตามความจำเป็นตามภารกิจ และสอดคล้องกับหน้าที่ความรับผิดชอบ

(๕) การยกเลิกเพิกถอนการอนุญาตให้เข้าถึงระบบสารสนเทศและการตัดออกจากทะเบียนของผู้ใช้งาน ให้กลุ่มงานบริหารกลาง แจ้งกลุ่มงานบริหารสารสนเทศ ทันที เมื่อมีผู้ใช้งาน เกษียณอายุ โอน ย้าย เปลี่ยนแปลงสังกัด ลาออก เพื่อทำการเปลี่ยนสิทธิหรือถอดถอนสิทธิของผู้ใช้งานออกจากระบบสารสนเทศทันทีที่ได้รับแจ้ง

(๖) มีการตรวจสอบและทบทวนบัญชีผู้ใช้งาน เป็นประจำทุกปี

๒.๓ มีการบริหารจัดการสิทธิของผู้ใช้งาน (User management) ดังนี้

(๑) ต้องจัดให้มีการควบคุมและจำกัดสิทธิในการใช้งานระบบตามความจำเป็นในการใช้งานเท่านั้น

(๒) กำหนดสิทธิการใช้ระบบสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (e-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้ดูแลระบบ รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

(๓) กรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้ หมายถึง ผู้ใช้ที่มีสิทธิสูงสุด ต้องมีการพิจารณาการควบคุมผู้ใช้ที่มีสิทธิพิเศษนั้นอย่างรัดกุมเพียงพอ และควรได้รับความเห็นชอบและอนุมัติจากผู้ดูแลระบบงานนั้น ๆ โดยมีการกำหนดระยะเวลาการใช้งาน และต้องระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง

๒.๔ การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User password management)

(๑) กำหนดให้รหัสผ่านต้องมีความยาวไม่น้อยกว่า ๘ ตัวอักษร โดยอาจจะมีการผสมกันระหว่างตัวเลข ตัวอักษรที่เป็นตัวพิมพ์เล็กหรือตัวพิมพ์ใหญ่ ตัวอักขระพิเศษและสัญลักษณ์

(๒) ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

(๓) ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save password) สำหรับเครื่องคอมพิวเตอร์ลูกข่ายที่ใช้งาน

(๔) ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ซึ่งง่ายต่อการสังเกตเห็นของบุคคลอื่น

(๕) จะต้องเก็บรักษารหัสผ่านสำหรับการใช้งานเครื่องคอมพิวเตอร์และเครือข่ายที่ได้มาโดยถือว่าเป็นความลับเฉพาะบุคคล และจะต้องไม่เปิดเผยหรือกระทำการใดให้ผู้อื่นทราบรหัสผ่านดังกล่าว

(๖) ผู้ใช้งานที่เป็นเจ้าของรหัสผ่านต้องใช้งานอย่างระมัดระวัง ไม่เปิดเผยรหัสผ่านให้ผู้อื่นได้รับรู้ และต้องรับผิดชอบในกรณีที่เกิดความเสียหายขึ้นในทุกกรณี

(๗) ผู้ดูแลระบบ ต้องกำหนดรหัสผ่านของผู้ใช้งานแบบชั่วคราวที่ยากต่อการเดา และกำหนดให้ผู้ใช้งานทำการเปลี่ยนรหัสผ่านผู้ใช้ใหม่

(๘) ต้องมีการเปลี่ยนรหัสผ่านทุกรอบระยะเวลา ๓ เดือน ซึ่งขึ้นอยู่กับความสำคัญของระบบงาน

๒.๕ การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of user access rights)

(๑) ต้องจัดให้มีการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบเป็นประจำทุกปี

(๒) ผู้ดูแลระบบต้องมีการสอบทานและระงับการใช้งานบัญชีผู้ใช้งานที่ไม่ได้ใช้งานเกิน ๑ ปี และต้องจัดส่งรายชื่อของผู้ใช้งานที่ถูกระงับไปยังหัวหน้าส่วนงาน เพื่อยืนยันการยกเลิกการใช้งาน

๓. การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities)

๓.๑ การใช้งานรหัสผ่าน (Password use)

(๑) ผู้ใช้งานที่เป็นเจ้าของบัญชีผู้ใช้งาน (User Account) ต้องเป็นผู้รับผิดชอบในผลต่าง ๆ อันจะเกิดขึ้นจากการใช้บัญชีผู้ใช้บริการของเครื่องคอมพิวเตอร์และเครือข่ายเว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

(๒) ผู้ใช้งานจะต้องเก็บรักษาบัญชีผู้ใช้งาน (User Account) ไว้เป็นความลับและห้ามเปิดเผยต่อบุคคลอื่น ห้ามโอน จำหน่าย หรือจ่ายแจกให้แก่ผู้อื่นโดยมิได้รับอนุญาตจากผู้อำนวยการ

(๓) ผู้ใช้งาน ต้องเก็บรักษารหัสผ่านไว้เป็นความลับเฉพาะบุคคล ไม่เปิดเผยให้ผู้อื่นรับทราบ ผู้ใช้งานต้องไม่พิมพ์รหัสผ่านในลักษณะเปิดเผย เช่น พิมพ์รหัสผ่านต่อหน้าผู้ปฏิบัติงานคนอื่น และต้องรับผิดชอบในกรณีที่เกิดความเสียหายขึ้นในทุกกรณี

(๔) ผู้ใช้งาน ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

(๕) ผู้ใช้งานจะต้องเข้าระบบ (Log in) โดยใช้บัญชีผู้ใช้งาน (User Account) ของตนเองและทำการออกจากระบบ (Log out) ทุกครั้ง เมื่อสิ้นสุดการใช้งานหรือหยุดการใช้งานชั่วคราว

(๖) ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานป้องกันผู้อื่นเข้าใช้อุปกรณ์คอมพิวเตอร์หรือระบบสารสนเทศของตนเอง โดยใส่รหัสผ่านให้ถูกต้องก่อนเข้าใช้งานอุปกรณ์คอมพิวเตอร์

(๗) ผู้ดูแลระบบต้องกำหนดให้อุปกรณ์คอมพิวเตอร์ทุกเครื่องทำการตั้งเวลาพักหน้าจอ (Screen Saver) โดยตั้งเวลาอย่างน้อย ๑๐ นาที และมีการใช้รหัสในการเข้าถึงใหม่ทุกครั้ง

๓.๒ การควบคุมทรัพย์สินสารสนเทศและการใช้งานระบบคอมพิวเตอร์ (clear desk and clear screen policy)

(๑) ผู้ใช้งานต้องไม่คัดลอกหรือทำสำเนาแฟ้มข้อมูลที่มีลิขสิทธิ์กำกับการใช้งาน ก่อนได้รับอนุญาตและผู้ใช้งานต้องไม่ใช้ หรือลบแฟ้มข้อมูลของผู้อื่น ไม่ว่ากรณีใด ๆ

(๒) ผู้ใช้งานต้องไม่ทิ้งหรือปล่อยให้สินทรัพย์ที่มีความสำคัญ ได้แก่ เอกสาร สื่อบันทึกข้อมูล อยู่ในสถานที่ที่ไม่ปลอดภัย ที่สาธารณะ หรือถูกพบเห็นได้ง่าย โดยเก็บไว้ในตู้ที่มีการล็อคกุญแจ

(๓) ผู้ใช้งานต้องจัดเก็บสินทรัพย์ที่ตนใช้งานในที่ที่กำหนดไว้หลังใช้งานเสร็จเรียบร้อยแล้ว หากเป็นการใช้งานระบบสารสนเทศต้องทำการออกจากระบบทุกครั้ง

(๔) ผู้ใช้งานต้องทำลายข้อมูลสำคัญในอุปกรณ์สื่อบันทึกข้อมูล แฟ้มข้อมูล ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว และใช้เทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้ และพิจารณาวิธีการทำลายข้อมูลบนสื่อบันทึกข้อมูลแต่ละประเภท ดังนี้

ประเภทสื่อบันทึกข้อมูล	วิธีทำลาย
กระดาษ	ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร
Flash Drive	- ใช้การทำลายข้อมูลบน Flash Drive ตามมาตรฐาน DOD ๕๒๒๐.๒๒ M ของกระทรวงกลาโหมสหรัฐอเมริกา ซึ่งเป็นมาตรฐานการทำลายข้อมูลโดยการเขียนทับข้อมูลเดิมหลายรอบ - ใช้วิธีการทุบหรือบดให้เสียหาย
แผ่น CD/DVD	ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร
ฮาร์ดดิสก์	- ใช้การทำลายข้อมูลบนฮาร์ดดิสก์ตามมาตรฐาน DOD ๕๒๒๐.๒๒ M ของกระทรวงกลาโหมสหรัฐอเมริกา ซึ่งเป็นมาตรฐานการทำลายข้อมูลโดยการเขียนทับข้อมูลเดิมหลายรอบ - ใช้วิธีการทุบหรือบดให้เสียหาย

๓.๓ การนำการเข้ารหัสลับ มาใช้กับข้อมูลที่เป็นความลับ ผู้ใช้งานจะต้องปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ และต้องใช้วิธีการเข้ารหัสลับ (Encryption) ที่เป็นมาตรฐานสากล เช่น โพรโทคอล TLS ในการรับส่งข้อมูลผ่านเครือข่าย และ AES สำหรับข้อมูลที่จัดเก็บ

๔. การควบคุมการเข้าถึงระบบเครือข่าย (Network Access Control)

๔.๑ ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใด ๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์เชื่อมต่อกับระบบเครือข่ายของหน่วยงาน โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ

๔.๒ ผู้ดูแลระบบ ต้องควบคุมการเข้าถึงระบบเครือข่าย เพื่อบริหารจัดการระบบเครือข่ายได้อย่างมีประสิทธิภาพ ดังต่อไปนี้

(๑) ต้องจำกัดสิทธิการใช้งานเพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น

(๒) ต้องจำกัดเส้นทางการเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน

(๓) ต้องจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่าย เพื่อไม่ให้ผู้ใช้งานสามารถใช้เส้นทางอื่น ๆ ได้

(๔) ระบบเครือข่ายทั้งหมดของหน่วยงานที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกหน่วยงานต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก รวมทั้งต้องมีความสามารถในการตรวจจับโปรแกรมประสงค์ร้าย (Malware) ด้วย

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

(๖) การเข้าสู่ระบบเครือข่ายภายในหน่วยงาน โดยผ่านระบบอินเทอร์เน็ตจำเป็นต้องมีการลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่าน เพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนทุกครั้ง

(๗) ต้องป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็น IP Address ภายในของระบบเครือข่ายภายในหน่วยงาน

(๘) ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอกในภาพรวม

(๙) การระบุอุปกรณ์บนเครือข่าย

(๙.๑) ผู้ดูแลระบบมีการเก็บบัญชีการขอเชื่อมต่อเครือข่าย ได้แก่ รายชื่อผู้ขอใช้บริการ รายละเอียด เครื่องคอมพิวเตอร์ที่ขอใช้บริการ IP Address และสถานที่ติดตั้ง

(๙.๒) ผู้ดูแลระบบต้องจำกัดผู้ใช้งานที่สามารถเข้าใช้อุปกรณ์ได้

(๙.๓) กรณีอุปกรณ์ที่มีการเชื่อมต่อจากเครือข่ายภายนอก ต้องมีการระบุหมายเลขอุปกรณ์ว่าสามารถเข้าเชื่อมต่อกับเครือข่ายภายในได้หรือไม่

(๙.๔) อุปกรณ์เครือข่ายต้องสามารถตรวจสอบ IP Address ของต้นทางและปลายทางได้

(๙.๕) การเข้าใช้งานอุปกรณ์บนเครือข่ายต้องทำการพิสูจน์ตัวตนทุกครั้งที่ใช้อุปกรณ์

๔.๓ ผู้ดูแลระบบ ต้องบริหารควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server) และรับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนดแก้ไข หรือเปลี่ยนแปลงค่าต่าง ๆ ของซอฟต์แวร์ระบบ (Systems Software)

๔.๔ การจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้ตามแนวทาง พ.ร.บ.คอมพิวเตอร์ ๒๕๕๐

๔.๕ มีกำหนดมาตรการควบคุมการใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) จากผู้ใช้งานภายนอกหน่วยงาน เพื่อดูแลรักษาความปลอดภัยของระบบ ตามแนวทางปฏิบัติ ดังต่อไปนี้

(๑) บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) ของหน่วยงาน จะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษรเพื่อขออนุญาตจากหัวหน้าหน่วยงาน

(๒) มีการควบคุมช่องทาง (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

(๓) วิธีการใด ๆ ที่สามารถเข้าสู่ข้อมูล หรือระบบสารสนเทศได้จากระยะไกล ต้องได้รับการอนุญาตจากหัวหน้าหน่วยงาน

(๔) การเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องแสดงหลักฐาน ระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับหน่วยงานอย่างเพียงพอ

(๕) การเข้าสู่ระบบเครือข่ายภายในและระบบสารสนเทศในหน่วยงานจากระยะไกล ต้องมีการแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่าน เพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนทุกครั้ง

(๖) ผู้ดูแลระบบต้องกำหนดการเปิด-ปิด พอร์ตของอุปกรณ์เครือข่ายเพื่อควบคุมการเข้าถึงพอร์ตของอุปกรณ์เครือข่ายต่าง ๆ โดยจะปิดพอร์ตที่เสี่ยงที่จะก่อให้เกิดความเสียหายต่อระบบเครือข่ายคอมพิวเตอร์

(๗) ผู้ดูแลระบบต้องตรวจสอบและปิดพอร์ตของระบบหรืออุปกรณ์ที่ไม่มีความจำเป็นในการใช้งานอย่างสม่ำเสมออย่างน้อยสัปดาห์ละ ๒ ครั้ง

(๘) การขอใช้งานพอร์ตต้องได้รับอนุญาตจากผู้อำนวยการ หรือผ่านช่องทางที่กลุ่มงานบริหารสารสนเทศ จัดเตรียมไว้ให้

(๙) มีการบันทึกการเข้า-ออกพื้นที่บริเวณศูนย์ข้อมูลหลัก (Data Center) ห้ามบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าไปในศูนย์ข้อมูลหลัก (Data Center) หากจำเป็น ให้เจ้าหน้าที่ด้านเทคโนโลยีสารสนเทศ เป็นผู้รับผิดชอบนำพาเข้าไป

๔.๖ มีการแบ่งแยกเครือข่าย (Segregation in Networks) สำหรับกลุ่มผู้ใช้งาน โดยแบ่งออกเป็น ๒ เครือข่าย คือ

(๑) Internet แบ่งแยกเครือข่ายเป็นเครือข่ายย่อย ๆ ตามอาคารต่าง ๆ เพื่อควบคุมการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต

(๒) Intranet แบ่งเครือข่ายภายในและเครือข่ายภายนอก เพื่อความปลอดภัยในการใช้งานระบบสารสนเทศภายใน

๔.๗ ระบบเครือข่ายทั้งหมดที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกหน่วยงาน ต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือโปรแกรมในการทำ Packet filtering เช่น การใช้ไฟร์วอลล์ (Firewall) หรือฮาร์ดแวร์อื่น ๆ รวมทั้งต้องมีความสามารถในการตรวจจับมัลแวร์ (Malware) ด้วย

๔.๘ ต้องมีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานบุคคล ที่เข้าใช้งานระบบเครือข่ายของหน่วยงาน ในลักษณะที่ผิดปกติ โดยมีการตรวจสอบการบุกรุกผ่านระบบเครือข่าย การใช้งานในลักษณะที่ผิดปกติ และการแก้ไขเปลี่ยนแปลงระบบเครือข่าย โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

๔.๙ IP Address ของระบบเครือข่ายภายใน จำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายได้โดยง่าย

๕. การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

๕.๑ มีการกำหนดขั้นตอนการเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย ดังนี้

(๑) ผู้ดูแลระบบ ต้องจัดให้มีการควบคุมในการเข้าถึงระบบปฏิบัติการอย่างมั่นคงปลอดภัย โดยขั้นตอนการเข้าสู่ระบบ ต้องมีการเปิดเผยข้อมูลเกี่ยวกับระบบให้น้อยที่สุด เพื่อหลีกเลี่ยงผู้ใช้งานที่ไม่ได้รับอนุญาต

(๒) ต้องมีการกำหนดระยะเวลาสำหรับใช้ในการป้อนรหัสผ่าน โดยป้อนรหัสผ่านผิดได้ไม่เกิน ๓ ครั้ง

(๓) ต้องมีกำหนดให้ระบบแสดงข้อความเตือน “อนุญาตเฉพาะบุคคลที่เกี่ยวข้องเท่านั้นที่มีสิทธิเข้าใช้งาน”

(๔) จำกัดการเชื่อมต่อโดยตรงสู่ระบบปฏิบัติการผ่านทาน Command Line เนื่องจากอาจสร้างความเสียหายให้กับระบบได้

๕.๒ การระบุและยืนยันตัวตนของผู้ใช้งาน (User identification and authentication)

(๑) ผู้ดูแลระบบ ต้องจัดให้ผู้ใช้งานมีบัญชีผู้ใช้งานแต่ละบุคคลเพื่อใช้ในการพิสูจน์ตัวตนในการเข้าถึงระบบสารสนเทศ

(๒) ผู้ใช้งานระบบทุกคนเมื่อจะเข้าใช้งานระบบต้องผ่านการพิสูจน์ตัวตนจากระบบขององค์กร โดยแสดงชื่อผู้ใช้งาน (Username) ใส่รหัสผ่าน (Password) และทำการออกจากระบบ (Logout) ทุกครั้ง เมื่อสิ้นสุดการใช้งานหรือหยุดการใช้งานชั่วคราว

(๓) ในกรณีที่มีความจำเป็นต้องมีการใช้บัญชีผู้ใช้ร่วมกัน (Shared User ID) ต้องได้รับการอนุมัติจากผู้เป็นเจ้าของสารสนเทศ กลุ่มงานบริหารสารสนเทศ และผู้บังคับบัญชา นอกจากนี้กลุ่มงานบริหารสารสนเทศและผู้บังคับบัญชา ต้องพิจารณาการควบคุมอื่น ๆ เช่น ต้องกำหนดผู้รับผิดชอบ การดำเนินการใด ๆ อันเกิดจากการใช้งานบัญชีผู้ใช้นั้นและต้องมีการตรวจสอบการใช้งานดังกล่าวเป็นประจำอย่างน้อยปีละ ๒ ครั้ง

๕.๓ การบริหารจัดการรหัสผ่าน (Password management system)

(๑) ผู้ดูแลระบบ ต้องจัดให้มีการควบคุมรหัสผ่าน ดังต่อไปนี้

(๑.๑) บังคับให้มีการเปลี่ยนแปลงรหัสผ่านชั่วคราวในครั้งแรกของการเข้าสู่ระบบ และให้ผู้ใช้งานสามารถเลือกและเปลี่ยนแปลงรหัสผ่านของตนเอง พร้อมทั้งมีขั้นตอนในการยืนยันรหัสผ่าน

(๑.๒) ห้ามผู้ใช้กำหนดรหัสผ่านแบบไม่กำหนดค่า (Blank Password)

(๑.๓) ห้ามผู้ใช้ตั้งรหัสผ่านเหมือนชื่อผู้ใช้งาน

(๑.๔) ระบบมีการแจ้งเตือนให้ผู้ใช้งานเปลี่ยนรหัสผ่าน ๑ สัปดาห์ ก่อนถึงรอบระยะเวลาการเปลี่ยนรหัสผ่านที่กำหนดไว้

(๑.๕) ระบบมีการแจ้งเตือนเมื่อผู้ใช้งานกรอกรหัสผ่านผิด และจะระงับการเข้าถึงระบบทันทีเมื่อกรอกรหัสผ่านผิดเกิน ๓ ครั้ง โดยผู้ใช้งานต้องแจ้งผู้ดูแลระบบเพื่อทำการยกเลิกการระงับ

(๑.๖) ระบบมีการแจ้งเตือนให้ผู้ใช้งานทราบอย่างอัตโนมัติเมื่อเข้าสู่ระบบสำเร็จหรือเข้าสู่ระบบไม่สำเร็จ

(๑.๗) ระบบต้องไม่แสดงรหัสผ่านและจำนวนอักขระรหัสผ่านที่ผู้ใช้งานพิมพ์ในขณะเข้าสู่ระบบ โดยอาจมีการแสดงสัญลักษณ์แทนรหัสผ่านจริงในขณะผู้ใช้งานพิมพ์

(๑.๘) ต้องมีรูปแบบที่ป้องกันการจัดเก็บและส่งรหัสผ่าน เช่น Hashing เป็นต้น

(๒) ระบบปฏิบัติการ ฐานข้อมูล และแอปพลิเคชัน (Application) ที่เก็บบัญชีผู้ใช้งานและรหัสผ่านต้องมีการควบคุมอย่างเข้มงวด เพื่อให้เข้าถึงได้โดยผู้ดูแลระบบที่ได้รับอนุญาตเท่านั้น

(๓) เมื่อได้ดำเนินการติดตั้งระบบแล้ว ให้ยกเลิกชื่อผู้ใช้งานหรือเปลี่ยนรหัสผ่านของทุกชื่อผู้ใช้งานที่ได้ถูกกำหนดไว้เริ่มต้นที่มาพร้อมกับการติดตั้งระบบโดยทันที

๕.๔ การใช้งานโปรแกรมอรรถประโยชน์ (Use of system utilities)

(๑) ผู้อำนวยการ ต้องกำหนดความรับผิดชอบในการใช้โปรแกรมอรรถประโยชน์อย่างชัดเจน และสื่อสารให้ผู้เกี่ยวข้องทราบและถือปฏิบัติ

(๒) ผู้อำนวยการ ต้องมีการพิสูจน์ตัวตนและกำหนดสิทธิในการใช้งานโปรแกรมอรรถประโยชน์

(๓) จำกัดการเข้าถึงโปรแกรมอรรถประโยชน์ให้เฉพาะกลุ่มคนที่มีหน้าที่รับผิดชอบ

(๔) มีการบันทึกเหตุการณ์ (Log) การใช้งานโปรแกรมอรรถประโยชน์ และต้องมีการสอบทานจากผู้ดูแลระบบเป็นประจำทุกเดือน

(๕) ต้องทำการเพิกถอนหรือระงับโปรแกรมอรรถประโยชน์ที่ไม่จำเป็น

(๖) ไม่อนุญาตให้ผู้ใช้งานสามารถติดตั้งโปรแกรมคอมพิวเตอร์ที่สามารถใช้ในการตรวจสอบข้อมูลบนเครือข่ายคอมพิวเตอร์ได้

(๗) ไม่อนุญาตให้ผู้ใช้งานสามารถติดตั้งโปรแกรมคอมพิวเตอร์หรืออุปกรณ์อื่นใดเพิ่มเติมในเครื่องคอมพิวเตอร์ของหน่วยงาน เพื่อให้บุคคลอื่นสามารถใช้งานเครื่องคอมพิวเตอร์และเครือข่ายของหน่วยงานได้

๕.๕ การกำหนดเวลาการใช้งานระบบสารสนเทศ (Session time-out)

(๑) ผู้ดูแลระบบ ต้องกำหนด Session time-out ของระบบสารสนเทศที่ไม่มีการใช้งานภายในระยะเวลาที่กำหนด โดยการตัดการเชื่อมต่อกับแอปพลิเคชัน (Application) หรือเครือข่าย หากไม่มีการใช้งานเป็นเวลา ๑๐ นาทีโดยอัตโนมัติ ทั้งนี้ ถ้าระบบไม่สามารถตัดการเชื่อมต่อแบบอัตโนมัติต้องกำหนดให้ใช้โปรแกรมพักหน้าจอที่ต้องใส่รหัสผ่าน หรือกำหนดให้มีการล็อคหน้าจอ

(๒) ผู้ใช้งาน ต้องตั้งค่าให้มีโปรแกรมพักหน้าจอที่ต้องใส่รหัสผ่านสำหรับเครื่องคอมพิวเตอร์ส่วนบุคคล หรือเครื่องคอมพิวเตอร์แบบพกพา และเครื่องคอมพิวเตอร์แม่ข่าย ทั้งนี้ โปรแกรมพักหน้าจอ ต้องกำหนดให้ป้อนรหัสผ่านหลังจากมีการทิ้งเครื่องดังกล่าวไว้โดยไม่มีการใช้งานเป็นเวลา ๑๐ นาที

(๓) ผู้ใช้งาน จะต้องปิดเครื่องคอมพิวเตอร์ของหน่วยงานที่ตนเองครอบครองใช้งานอยู่เมื่อใช้งานประจำวันเสร็จสิ้น หรือเมื่อไม่มีการใช้งาน เว้นแต่เครื่องคอมพิวเตอร์นั้นเป็นเครื่องคอมพิวเตอร์แม่ข่าย (Server) ที่ต้องใช้งานตลอด ๒๔ ชั่วโมง

๕.๖ การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of connection time)

(๑) ผู้ดูแลระบบ ต้องจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศที่มีความสำคัญสูง เพื่อให้ผู้ใช้งานสามารถใช้งานได้นานที่สุดภายในระยะเวลา ๒ ชั่วโมงต่อการเชื่อมต่อ ๑ ครั้ง สำหรับระบบงานทั่วไป กำหนดให้เข้าใช้งานได้ในเวลาทำการของหน่วยงาน เท่านั้น

(๒) กรณี หากมีความจำเป็นต้องใช้งานนอกเวลาที่กำหนด ต้องขออนุมัติจากผู้อำนวยการ เท่านั้น

๖. การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชั่นและสารสนเทศ (Application and Information Access Control)

๖.๑ การจำกัดการเข้าถึงสารสนเทศ (Information access restriction)

(๑) ผู้ใช้งาน ต้องได้รับสิทธิการเข้าถึงเท่าที่จำเป็นต่อการปฏิบัติงาน โดยการให้สิทธิต้องพิจารณา ในเรื่องดังต่อไปนี้

(๑.๑) ความมั่นคงปลอดภัยทางตรรกะ (Logical Security) ภายในแอปพลิเคชัน (Application)

(๑.๒) การจำกัดไม่ให้ใช้ตัวเลือก (Options) ที่ไม่ได้รับอนุญาต

(๑.๓) การจำกัดการเข้าถึง Command Line

(๑.๔) การจำกัดการเข้าถึงข้อมูลและฟังก์ชันการใช้งานของแอปพลิเคชัน (Application) ที่ไม่เกี่ยวข้องกับหน้าที่ความรับผิดชอบ

(๑.๕) การจำกัดระดับสิทธิในการเข้าถึงไฟล์ เช่น อ่านอย่างเดียว เป็นต้น

(๑.๖) การควบคุมการแจกจ่ายหรือการเข้าถึงข้อมูลนำออกของระบบสารสนเทศ

(๒) ระบบควรรองรับการกำหนดสิทธิในการเข้าแบบกลุ่มได้

(๓) การควบคุม Outsource กรณีมีการจ้างเหมาพัฒนาระบบสารสนเทศของหน่วยงาน ดังนี้

(๓.๑) การกำหนดสิทธิการเข้าใช้งานระบบสารสนเทศ และพื้นที่ของหน่วยงาน

(๓.๒) การลงนามในสัญญา เรื่องหน้าที่ความรับผิดชอบ รวมถึงการไม่เปิดเผยข้อมูลของหน่วยงาน

(๓.๓) การกำหนดผู้รับผิดชอบต่อการควบคุมงาน เพื่อคอยกำกับดูแลการดำเนินงานต่าง ๆ ของ Outsource

๖.๒ การแยกระบบสารสนเทศที่มีความสำคัญสูง (Sensitive System Isolation) ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อหน่วยงาน ได้แก่ ระบบงานบัญชี จะต้องดำเนินการ ดังนี้

(๑) ผู้ดูแลระบบ ทำการแยกระบบซึ่งไวต่อการรบกวนออกจากระบบอื่น ๆ และมีการควบคุมสภาพแวดล้อมของระบบโดยเฉพาะ โดยกำหนดสิทธิให้เฉพาะผู้ที่มีสิทธิใช้ระบบเข้าไปปฏิบัติงานเท่านั้น

(๒) มีการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ และการปฏิบัติงานจากภายนอกหน่วยงาน (Mobile Computing and Teleworking) ที่เกี่ยวข้องกับระบบดังกล่าว

๖.๓ การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องกำหนดแนวปฏิบัติและมาตรการที่เหมาะสม เพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ดังนี้

(๑) การใช้งานอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ในที่สาธารณะ ห้องประชุม และพื้นที่ภายนอกอื่น ๆ ที่ไม่มีการป้องกัน ต้องป้องกันการเข้าถึงที่ไม่ได้รับอนุญาต เช่น กำหนดให้ต้องใช้

รหัสในการเข้าระบบเครือข่ายไร้สาย การไม่เปิดการเชื่อมต่อแบบไร้สายโดยไม่มีการเข้ารหัสลับข้อมูล เป็นต้น

(๒) ผู้ใช้งานอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ ชนิดที่รองรับการติดตั้งโปรแกรมป้องกันโปรแกรมประสงค์ร้ายได้ ต้องจัดให้มีโปรแกรมป้องกันโปรแกรมประสงค์ร้าย และต้องปรับปรุงให้โปรแกรมดังกล่าวทันสมัยอยู่เสมอ โดยผู้ดูแลระบบตรวจเช็ค update patch and Antivirus ทุกเดือน

(๓) ผู้ดูแลระบบ ต้องจัดให้มีการป้องกันการใช้อุปกรณ์สื่อสารเคลื่อนที่ในการเชื่อมต่อเครือข่าย โดยการใช้อุปกรณ์สื่อสารเคลื่อนที่เพื่อเชื่อมต่อผ่านเครือข่ายสาธารณะ ที่เป็นมาตรฐานสากล ด้วยเทคโนโลยี Virtual Private Networks (VPN) ซึ่งเป็นระบบเครือข่ายส่วนตัวเสมือน ใช้เทคนิคการเข้ารหัสข้อมูลที่อยู่บนระบบเครือข่าย

(๔) การดูแลอุปกรณ์สื่อสารเคลื่อนที่ ต้องมีการป้องกันในเรื่องดังต่อไปนี้

(๔.๑) มีการกำหนดและมอบหมายความรับผิดชอบในการดูแลอุปกรณ์สื่อสารเคลื่อนที่

(๔.๒) ผู้ใช้งาน ต้องนำอุปกรณ์สื่อสารเคลื่อนที่ติดตัวไปด้วยเสมอ เช่น ไม่ละทิ้งอุปกรณ์สื่อสารเคลื่อนที่ในรถยนต์ ห้องพักในโรงแรมหรือห้องประชุม เป็นต้น

(๔.๓) ผู้ใช้งาน ต้องจัดเก็บอุปกรณ์สื่อสารเคลื่อนที่ในกระเป๋าที่ปลอดภัยและเหมาะสม เพื่อป้องกันการกระแทก กันน้ำ หรือความชื้น เป็นต้น

(๔.๔) ผู้ใช้งาน ต้องสำรองข้อมูลของอุปกรณ์สื่อสารเคลื่อนที่อย่างสม่ำเสมอ และมีการเข้ารหัสลับข้อมูลที่สำรองอย่างเหมาะสม

(๕) กรณีนำเครื่องคอมพิวเตอร์และอุปกรณ์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์และเครือข่ายของหน่วยงาน ต้องได้รับอนุญาตจากผู้ดูแลระบบและปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

(๖) การเข้าสู่ระบบงานเครือข่ายภายในองค์กรโดยผ่านทางอินเทอร์เน็ต ต้องมีการลงทะเบียนเข้าใช้งานระบบและต้องมีการยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้อง

๖.๔ การปฏิบัติงานจากภายนอกหน่วยงาน (Teleworking) มีการกำหนดสิทธิการเข้าใช้งานโดยกำหนดค่าที่ Firewall และใช้เทคโนโลยี Virtual Private Networks (VPN) เพื่อป้องกันและเพิ่มความปลอดภัยของข้อมูล ต้องกำหนดแนวปฏิบัติ แผนงานและขั้นตอนปฏิบัติ ดังนี้

(๑) การปฏิบัติงานจากภายนอกสำนักงาน ต้องได้รับการอนุญาตจากผู้บังคับบัญชาอย่างเป็นลายลักษณ์อักษร โดยผู้บังคับบัญชา ต้องพิจารณาเงื่อนไขในการจัดเตรียมการ ดังต่อไปนี้

(๑.๑) ความมั่นคงปลอดภัยทางกายภาพ และสภาพแวดล้อมของการปฏิบัติงานจากภายนอกสำนักงาน

(๑.๒) ความมั่นคงปลอดภัยทางการสื่อสาร โดยยึดจากระดับความสำคัญ (Sensitivity) ของข้อมูลที่จะถูกเข้าถึงและส่งผ่านช่องทางการเชื่อมต่อสื่อสาร (Communication link) รวมถึงระดับความสำคัญ (Sensitivity) ของระบบภายในองค์กร

(๒) เอกสารที่เป็นความลับ ต้องจัดเก็บในบริเวณการทำงานและจัดเก็บในอุปกรณ์บรรจุภัณฑ์ที่ล็อคได้ โดยใช้หลักเกณฑ์การรักษาความลับเช่นเดียวกับสารสนเทศที่อยู่ในองค์กร

(๓) ผู้ใช้งาน ต้องมีการติดตั้งโปรแกรมป้องกันไวรัสและ Personal Firewall สำหรับอุปกรณ์ส่วนตัวที่ใช้เชื่อมต่อเครือข่ายจากภายนอก

(๔) ผู้บังคับบัญชาของผู้ใช้งาน ต้องประสานกับผู้ดูแลระบบ เพื่อทำการถอดถอนสิทธิในการเข้าถึงของผู้ใช้งานจากภายนอกองค์กร เมื่อเสร็จสิ้นการปฏิบัติงานที่ได้รับมอบหมาย

๗. การควบคุมการใช้อินเทอร์เน็ต (Internet)

๗.๑ ผู้ดูแลระบบ ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ต ที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่หน่วยงานจัดสรรไว้เท่านั้น เช่น Proxy, Firewall, IPS-IDS เป็นต้น ห้ามผู้ใช้งานทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น เช่น Dial-up Modem ยกเว้นแต่ว่ามีเหตุผลความจำเป็นและต้องทำการขออนุญาตจากหัวหน้าหน่วยงานเป็นลายลักษณ์อักษร

๗.๒ เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์พกพา ก่อนทำการเชื่อมต่ออินเทอร์เน็ต ผ่านเว็บเบราว์เซอร์ (Web browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัส และทำการอุดช่องโหว่ของระบบปฏิบัติการ

๗.๓ ในการรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเทอร์เน็ตจะต้องมีการทดสอบไวรัส (Virus scanning) โดยโปรแกรมป้องกันไวรัสก่อนการรับส่งข้อมูลทุกครั้ง

๗.๔ ไม่ใช้ระบบอินเทอร์เน็ต (Internet) ของหน่วยงาน เพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงของชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิของผู้อื่น หรือข้อมูลที่อาจก่อให้เกิดความเสียหายให้กับหน่วยงาน

๗.๕ ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของหน่วยงานที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต (Internet)

๗.๖ ระมัดระวังการดาวน์โหลด โปรแกรมใช้งานจากระบบอินเทอร์เน็ต (Internet) การอัปเดต (Update) โปรแกรมต่าง ๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์

๗.๗ ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของหน่วยงาน

๗.๘ ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ไม่เสนอความคิดเห็น หรือใช้ข้อความที่ยั่วยุให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของหน่วยงาน การทำลายความสัมพันธ์กับบุคลากรของหน่วยงานอื่น ๆ

๗.๙ ผู้ใช้งาน ไม่นำเข้าข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามก และไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเทอร์เน็ต

๗.๑๐ หลังจากใช้งานระบบอินเทอร์เน็ต (Internet) เสร็จแล้ว ให้ปิดเว็บเบราว์เซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น ๆ

๗.๑๑ หลังจากใช้งานระบบอินเทอร์เน็ตเสร็จแล้ว ให้ทำการออกจากระบบเพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น ๆ

๗.๑๒ ผู้ใช้งาน ต้องปฏิบัติตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์อย่างเคร่งครัด

๘. การควบคุมการใช้จดหมายอิเล็กทรอนิกส์ (E-Mail)

๘.๑ ในการลงทะเบียนบัญชีผู้ใช้งานจดหมายอิเล็กทรอนิกส์ (E-Mail) ต้องทำการกรอกข้อมูล ขอเข้าใช้บริการจดหมายอิเล็กทรอนิกส์ โดยยื่นคำขอกับกลุ่มงานบริหารสารสนเทศ

๘.๒ รหัสจดหมายอิเล็กทรอนิกส์ เวลาใส่รหัสผ่านต้องไม่ปรากฏหรือแสดงรหัสผ่านออกมา แต่ต้องแสดงออกมาในรูปของสัญลักษณ์แทนตัวอักษรนั้น เช่น “X” หรือ “O” ในการพิมพ์แต่ละตัวอักษร

๘.๓ เมื่อได้รับรหัสผ่าน (Password) และเมื่อมีการเข้าสู่ระบบในครั้งแรกนั้น ให้เปลี่ยนรหัสผ่าน โดยทันที

๘.๔ ผู้ดูแลระบบ ต้องกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิดได้ เช่น ไม่เกิน ๓ ครั้ง

๘.๕ ไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์

๘.๖ เปลี่ยนรหัสผ่าน ทุก ๖ เดือน

๘.๗ ไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-Mail Address) ของผู้อื่น เพื่ออ่านหรือรับหรือส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้งาน และให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์ เป็นผู้รับผิดชอบต่อการใช้งานนั้น

๘.๘ หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์ เสร็จสิ้น ต้องลงบันทึกออก (Logout) ทุกครั้ง

๘.๙ การส่งข้อมูลที่เป็นความลับ ไม่ควรระบุความสำคัญของข้อมูลในหัวข้อจดหมายอิเล็กทรอนิกส์ เว้นเสียแต่ว่าจะใช้วิธีการเข้ารหัสลับข้อมูล E-Mail ที่หน่วยงานกำหนดไว้ ให้ใช้ความระมัดระวังในการระบุชื่อที่อยู่ E-Mail ของผู้รับให้ถูกต้องเพื่อป้องกันการส่งผิดตัวผู้รับ

๘.๑๐ ห้ามส่ง E-Mail ที่มีลักษณะเป็นจดหมายขยะ (Spam Mail)

๘.๑๑ ห้ามส่ง E-Mail ที่มีลักษณะเป็นจดหมายลูกโซ่ (Chain Letter)

๘.๑๒ ห้ามส่ง E-Mail ที่มีลักษณะเป็นการละเมิดต่อกฎหมาย หรือสิทธิของบุคคลอื่น

๘.๑๓ ห้ามส่ง E-Mail ที่มีไวรัสไปให้กับบุคคลอื่นโดยเจตนา

๘.๑๔ ให้ระบุชื่อของผู้ส่งใน E-Mail ทุกฉบับที่ส่งไป

๘.๑๕ ให้ทำการสำรองข้อมูล E-Mail ตามความจำเป็นอย่างสม่ำเสมอ (แม้ว่าหน่วยงานจะทำการสำรองข้อมูล E-Mail ไว้ให้แต่ก็เพียงช่วงระยะเวลาหนึ่งเท่านั้น ดังนั้น E-Mail ที่เก่ามาก ๆ และจำเป็นต้องใช้งานจึงมีความจำเป็นต้องสำรองเก็บไว้ด้วยตนเอง)

๘.๑๖ ผู้ใช้งานต้องทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนการเปิด เพื่อตรวจสอบไฟล์โดยใช้โปรแกรมป้องกันไวรัส เป็นการป้องการในการเปิดไฟล์ที่เป็น Executable file เช่น .exe เป็นต้น

๘.๑๗ ผู้ใช้งานต้องไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

๘.๑๘ ผู้ใช้งานต้องไม่ใช้ข้อความที่ไม่สุภาพ หรือรับส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสม ข้อมูลอันอาจทำให้เสียชื่อเสียงของหน่วยงาน ทำให้เกิดความแตกแยกระหว่างหน่วยงาน ผ่านทางจดหมายอิเล็กทรอนิกส์

๘.๑๙ ผู้ใช้งานต้องตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ของตนเองทุกวัน และควรจัดเก็บแฟ้มข้อมูลและจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจำนวนน้อยที่สุด และควรลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้เนื้อที่ระบบจดหมายอิเล็กทรอนิกส์

๙. การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล

๙.๑ แนวทางปฏิบัติการใช้งานทั่วไป

(๑) เครื่องคอมพิวเตอร์ที่หน่วยงานอนุญาตให้ใช้งาน เป็นสินทรัพย์ของหน่วยงานเพื่อใช้ในงานของหน่วยงาน

(๒) โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ส่วนบุคคลของหน่วยงาน ต้องเป็นโปรแกรมที่หน่วยงานได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้น ห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

(๓) ไม่อนุญาตให้ผู้ใช้งานทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ของหน่วยงาน

(๔) การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ส่วนบุคคลตรวจซ่อม จะต้องดำเนินการโดยเจ้าหน้าที่ของหน่วยงานหรือผู้รับจ้างเหมาบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้ทำสัญญากับหน่วยงานเท่านั้น

(๕) ก่อนการใช้งานสื่อบันทึกพกพาต่าง ๆ ต้องมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัส

(๖) ผู้ใช้งาน มีหน้าที่และรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์

(๗) ปิดเครื่องคอมพิวเตอร์ส่วนบุคคลที่ตนเองครอบครองใช้งานอยู่เมื่อใช้งานประจำวันเสร็จสิ้น หรือเมื่อมีมีการยุติการใช้งานเกินกว่า ๑ ชั่วโมง

(๘) ทำการตั้งค่า Screen Saver ของเครื่องคอมพิวเตอร์ที่ตนเองรับผิดชอบให้มีการล็อคหน้าจอหลังจากที่ไม่ได้ใช้งานเกินกว่า ๓๐ นาที เพื่อป้องกันบุคคลอื่นมาใช้งานที่เครื่อง

(๙) ห้ามนำเครื่องคอมพิวเตอร์ส่วนตัวที่เจ้าหน้าที่เป็นเจ้าของมาใช้กับระบบเครือข่ายของหน่วยงาน ยกเว้นจะได้รับการตรวจสอบจากผู้ดูแลระบบของหน่วยงานก่อนการใช้งาน

๙.๒ การใช้รหัสผ่าน ให้ผู้ใช้งานปฏิบัติตามแนวทางการบริหารจัดการรหัสผ่านที่ระบุไว้ในหัวข้อ “การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน”

๙.๓ การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)

(๑) ผู้ใช้งาน ต้องตรวจสอบหาไวรัสจากสื่อต่าง ๆ เช่น Flash Drive และ Data Storage อื่น ๆ ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์

(๒) ผู้ใช้งาน ต้องตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัส ก่อนใช้งาน

(๓) ผู้ใช้งาน ต้องตรวจสอบข้อมูลคอมพิวเตอร์ใดที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ซึ่งมีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

๙.๔ การสำรองข้อมูลและการกู้คืน

(๑) ผู้ใช้งาน ต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่น ๆ เช่น CD, DVD , External Hard disk เป็นต้น

(๒) ผู้ใช้งาน มีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

(๓) ผู้ใช้งาน ต้องประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้บน Hard Disk ไม่ควรจะเป็นข้อมูลสำคัญเกี่ยวข้องกับการทำงาน เพราะหาก Hard Disk เสีย ก็ไม่กระทบต่อการดำเนินงานของหน่วยงาน

๑๐.การใช้งานเครื่องคอมพิวเตอร์แบบพกพา

๑๐.๑ แนวทางปฏิบัติการใช้งานทั่วไป

(๑) เครื่องคอมพิวเตอร์แบบพกพาที่หน่วยงานอนุญาตให้ใช้งาน เป็นสินทรัพย์ของหน่วยงานเพื่อใช้ในงานของหน่วยงาน

(๒) โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์แบบพกพาของหน่วยงาน ต้องเป็นโปรแกรมที่หน่วยงานได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้น ห้ามผู้ใช้งานคัดลอกโปรแกรม

ต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

(๓) ไม่ดัดแปลงแก้ไขส่วนประกอบต่าง ๆ ของคอมพิวเตอร์และรักษาให้มีสภาพเดิม

(๔) ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพา ควรใส่กระเป๋าเฉพาะสำหรับเครื่อง เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน

(๕) หลีกเลี่ยงการใช้นิ้วหรือของแข็ง เช่น ปลายปากกา กดสัมผัสหน้าจอ LCD ให้เป็นรอยขีดข่วน หรือทำให้จอ LCD ของเครื่องแตกเสียหาย

(๖) ไม่วางของทับบนหน้าจอและแป้นพิมพ์

(๗) การเคลื่อนย้ายเครื่องขณะที่เครื่องเปิดใช้งานอยู่ ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น

๑๐.๒ ความปลอดภัยทางด้านกายภาพ

(๑) ผู้ใช้งาน มีหน้าที่รับผิดชอบในการป้องกันการสูญหาย เช่น ควรล็อคเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

(๒) ผู้ใช้งาน ไม่เก็บหรือใช้งานคอมพิวเตอร์พกพาในสถานที่ที่มีความร้อน/ความชื้น/ฝุ่นละอองสูง และต้องระวังป้องกันการตกกระทบ

๑๐.๓ การควบคุมการเข้าถึงระบบปฏิบัติการ

(๑) ผู้ใช้งาน ต้องกำหนดชื่อผู้ใช้งาน (User Name) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการของเครื่อง

(๒) ผู้ใช้งาน ต้องกำหนดรหัสผ่านให้มีคุณภาพดีอย่างน้อยตามที่ระบุไว้ในเอกสาร “การบริหารจัดการสิทธิการใช้งานระบบและรหัสผ่าน”

(๓) ผู้ใช้งาน ต้องตั้งการใช้งานโปรแกรมรักษาจอภาพ (Screen Saver) โดยตั้งเวลาประมาณ ๑๕ นาที ให้ทำการล็อคหน้าจอเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานต้องใส่รหัสผ่าน

(๔) ผู้ใช้งาน ต้องทำการ Log out ออกจากระบบทันทีเมื่อเลิกใช้งาน หรือไม่อยู่ที่หน้าจอเป็นเวลานาน

๑๐.๔ การใช้รหัสผ่าน ให้ผู้ใช้งานปฏิบัติตามแนวทางการบริหารจัดการรหัสผ่านที่ระบุไว้ในเอกสารหัวข้อ “การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน”

๑๐.๕ การสำรองข้อมูลและการกู้คืน

(๑) ผู้ใช้งาน ต้องทำการสำรองข้อมูลจากเครื่อง โดยวิธีการและสื่อต่าง ๆ เพื่อป้องกันการสูญหายของข้อมูล

(๒) ผู้ใช้งาน ต้องจัดเก็บรักษาสื่อสำรองข้อมูล (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล

(๓) แผ่นสื่อสำรองข้อมูลต่าง ๆ ที่เก็บข้อมูลไว้ จะต้องทำการทดสอบการกู้คืนอย่างสม่ำเสมอ

(๔) แผ่นสื่อสำรองข้อมูลที่ไม่ได้ใช้งานแล้ว ต้องทำลายไม่ให้สามารถนำไปใช้งานได้อีก

(๕) ผู้ใช้งาน ต้องประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้บน Hard Disk ไม่ควรจะเป็นข้อมูลสำคัญเกี่ยวข้องกับการทำงาน เพราะหาก Hard Disk เสียไป ก็ไม่กระทบต่อการดำเนินงานของหน่วยงาน

๑๑.การจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log)

๑๑.๑ จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วน ถูกต้อง แท้จริง ระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้ และข้อมูลที่ใช้ในการจัดเก็บ ต้องกำหนดชั้นความลับในการเข้าถึง

๑๑.๒ ห้ามแก้ไขข้อมูลจราจรคอมพิวเตอร์ (Log) ที่เก็บรักษาไว้

๑๑.๓ กำหนดให้มีการบันทึกการทำงานของระบบบันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้า – ออกระบบ บันทึกการพยายามเข้าสู่ระบบ เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกไว้อย่างน้อย ๙๐ วัน นับตั้งแต่การใช้งานสิ้นสุดลง โดยปฏิบัติตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

๑๑.๔ ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่าง ๆ และจำกัดสิทธิการเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

หมวดที่ ๒

ระบบสารสนเทศ และระบบการสำรองข้อมูล

วัตถุประสงค์

เพื่อให้มีการพิจารณาคัดเลือกและจัดทำระบบสำรองให้อยู่ในสภาพพร้อมใช้งาน ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง กำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉินอย่างสม่ำเสมอ

ผู้รับผิดชอบ

๑. สำนักนโยบายและยุทธศาสตร์
๒. กลุ่มงานบริหารสารสนเทศ
๓. ผู้ดูแลระบบ

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชัน ๒.๕)

แนวทางปฏิบัติ

๑. พิจารณาคัดเลือกและจัดทำระบบสำรองให้อยู่ในสภาพพร้อมใช้งาน

๑.๑ กำหนดขั้นตอนการจัดทำระบบสำรองข้อมูล ดังนี้

(๑) สำรวจเครื่องแม่ข่ายของระบบงานต่าง ๆ

(๒) วิเคราะห์ความสำคัญของข้อมูลระบบงานต่าง ๆ

(๓) สำรองข้อมูลในลักษณะรายงาน รายสัปดาห์ เพื่อป้องกันการสูญหายของข้อมูล

(๔) กำหนดรูปแบบการสำรองข้อมูล

- ระบบงานทั่วไป ทำการสำรองข้อมูลแบบเต็มระบบ (Full Backup) เป็นประจำทุกวัน

- ระบบฐานข้อมูล กำหนดให้ทำการสำรองข้อมูลแบบเต็มระบบ (Full Backup) รายสัปดาห์ และให้ทำการสำรองข้อมูลแบบบางส่วนที่เพิ่มขึ้น (Incremental Backup) รายวัน

๑.๒ เก็บข้อมูลที่บันทึกการใช้งานเครื่องคอมพิวเตอร์แม่ข่าย และเครือข่ายคอมพิวเตอร์ (Log file) ย้อนหลังไม่น้อยกว่าเก้าสิบวัน ไว้ในหน่วยความจำเครื่องคอมพิวเตอร์อย่างน้อย ๑ เครื่อง ซึ่งแยกต่างหากจากเครื่องคอมพิวเตอร์แม่ข่าย

๑.๓ ผู้ดูแลระบบ จัดทำบันทึกการสำรองข้อมูล (Operator logs) โดยมีรายละเอียดการสำรองข้อมูล ได้แก่ เวลาเริ่มต้นและสิ้นสุด ชื่อผู้สำรองข้อมูล ชนิดของข้อมูลที่บันทึก เป็นต้น

๑.๔ จัดเก็บข้อมูลที่สำรองในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูล และผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน ข้อมูลที่สำรองจัดเก็บไว้ในสถานที่เก็บข้อมูลสำรองซึ่งติดตั้งอยู่ที่สถานที่อื่น และต้องมีการทดสอบสื่อเก็บข้อมูลสำรองเป็นประจำทุกเดือน

๑.๕ ผู้ดูแลระบบ จัดทำรายงานข้อผิดพลาดจากการสำรองข้อมูลที่เกิดขึ้น รวมทั้งวิธีการแก้ไขด้วย

๑.๖ ผู้ดูแลระบบ มอบหมายหน้าที่การสำรองข้อมูลแก่เจ้าหน้าที่คนอื่นไว้สำรอง ในกรณีที่ผู้ดูแลระบบไม่สามารถปฏิบัติงานได้

๑.๗ ในกรณีที่พบปัญหาในการสำรองข้อมูลจนเป็นเหตุไม่สามารถดำเนินการอย่างสมบูรณ์ได้ ให้ดำเนินการแก้ไขปัญหาและสรุปผลการแก้ไขปัญหา รายงานต่อผู้อำนวยการ

๑.๘ จัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ ระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลสำรองกับหน่วยงานควรห่างกันเพียงพอเพื่อไม่ให้ส่งผลกระทบต่อข้อมูลที่จัดเก็บไว้นอกสถานที่ในกรณีที่เกิดภัยพิบัติกับหน่วยงาน เช่น ไฟไหม้ เป็นต้น

๑.๙ ดำเนินการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรองที่ใช้จัดเก็บข้อมูลนอกสถานที่

๑.๑๐ ทดสอบบันทึกข้อมูลสำรองเป็นประจำทุกเดือน เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ

๑.๑๑ จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่ได้สำรองเก็บไว้

๑.๑๒ ตรวจสอบและทดสอบประสิทธิภาพและประสิทธิผลของขั้นตอนปฏิบัติในการกู้คืนข้อมูลเป็นประจำทุกเดือน

๑.๑๓ กำหนดให้มีการใช้งานการเข้ารหัสลับข้อมูลกับข้อมูลลับที่ได้สำรองเก็บไว้

๑.๑๔ มีระบบสำรองกระแสไฟฟ้า (UPS)

๑.๑๕ ผู้ดูแลระบบ ทำการทดสอบความพร้อมของระบบสำรองอย่างน้อยปีละ ๑ ครั้ง

๒. การกู้คืนระบบ

๒.๑ ในกรณีที่พบปัญหาที่อาจสร้างความเสียหายต่อระบบคอมพิวเตอร์ และ/หรือ ระบบเครือข่าย จนเป็นเหตุทำให้ต้องดำเนินการกู้คืนระบบ ให้ผู้ดูแลระบบคอมพิวเตอร์ และ/หรือ ผู้ดูแลระบบเครือข่าย ดำเนินการแก้ไข รายงานผลการแก้ไขพร้อมทั้งบันทึกและให้รายงานสรุปผลการปฏิบัติงานต่อผู้อำนวยการ หรือผู้ที่ได้รับมอบหมายจากผู้อำนวยการ ทราบ

๒.๒ ให้ใช้ข้อมูลทันสมัยที่สุด (Latest Update) ที่ได้สำรองไว้หรือตามความเหมาะสมเพื่อกู้คืนระบบ

๒.๓ หากความเสียหายที่เกิดขึ้นกับระบบคอมพิวเตอร์หรือระบบเครือข่าย กระทบต่อการให้บริการหรือการใช้งานของผู้ใช้ระบบ ให้แจ้งผู้ใช้งานทราบทันที พร้อมทั้งรายงานความคืบหน้าการกู้คืนระบบเป็นระยะจนกว่าจะดำเนินการเสร็จสิ้นอย่างสมบูรณ์

๓. การจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ ที่อาจเกิดขึ้นกับระบบฐานข้อมูลและสารสนเทศ (IT Contingency Plan)

นโยบายเกี่ยวกับการจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ ที่อาจเกิดขึ้นกับระบบฐานข้อมูลและสารสนเทศ (IT Contingency Plan) ต้องมอบหมายให้บุคลากรที่เกี่ยวข้องตามที่ระบุในแผนฯ ดำเนินการ ดังต่อไปนี้

๓.๑ กำหนดกระบวนการในการวางแผนรับมือกับเหตุภัยพิบัติสำหรับระบบที่มีความสำคัญสูง

๓.๒ กำหนดชนิดของภัยพิบัติที่มีผลต่อระบบที่มีความสำคัญสูง และจำเป็นต้องวางแผนรับมือ

๓.๓ ทำการประเมินความเสี่ยงที่มีผลทำให้ระบบที่มีความสำคัญสูงติดขัดหรือไม่สามารถทำงานได้ อันเป็นผลมาจากภัยพิบัติที่กำหนดไว้

๓.๔ จัดทำแผนรับมือกับเหตุภัยพิบัติสำหรับระบบที่มีความสำคัญสูง

๓.๕ ทดสอบ/ประเมิน และปรับปรุงแผนรับมือกับเหตุภัยพิบัติสำหรับระบบที่มีความสำคัญสูง อย่างน้อยปีละ ๑ ครั้ง

หมวดที่ ๓
การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

วัตถุประสงค์

เพื่อให้มีการควบคุมการตรวจประเมินระบบสารสนเทศ และการควบคุมเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศอย่างเหมาะสม

ผู้รับผิดชอบ

๑. สำนักนโยบายและยุทธศาสตร์
๒. กลุ่มงานบริหารสารสนเทศ
๓. ผู้ดูแลระบบ
๔. ผู้ตรวจสอบภายในหน่วยงาน (Internal Auditor) หรือ ผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor)

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชัน ๒.๕)

แนวทางปฏิบัติ

๑. การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ (Information security audit and assessment)

๑.๑ แต่งตั้งคณะทำงานบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อจัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร และแผนป้องกันและแก้ไขปัญหาจากภัยพิบัติต่อระบบสารสนเทศ

๑.๒ จัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร และแผนป้องกันและแก้ไขปัญหาจากภัยพิบัติต่อระบบสารสนเทศ และกำหนดผู้รับผิดชอบและขั้นตอนการปฏิบัติ

๑.๓ คณะทำงานบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร มีการทบทวนและปรับปรุงแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง

๑.๔ มีการตรวจสอบและประเมินความเสี่ยงโดยผู้ตรวจสอบภายในหน่วยงาน (Internal Auditor) หรือ ผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor)

๒. แนวปฏิบัติการประเมินความเสี่ยง

๒.๑ กระบวนการในการบริหารจัดการกับความเสี่ยงของระบบฐานข้อมูลและสารสนเทศ ให้ปฏิบัติตามกระบวนการในวงจรการบริหารงานคุณภาพ (PDCA) ดังต่อไปนี้

(๑) การกำหนดระบบบริหารจัดการความมั่นคงปลอดภัย (Plan)

(๒) การดำเนินการกับระบบบริหารจัดการความมั่นคงปลอดภัย (Do)

(๓) การเฝ้าระวังและทบทวนระบบบริหารจัดการความมั่นคงปลอดภัย (Check)

(๔) การทบทวนและปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัย (Act)

๒.๒ การวางแผนระบบบริหารความเสี่ยงของระบบฐานข้อมูลและสารสนเทศ ต้องดำเนินการดังต่อไปนี้

(๑) มีการบริหารความเสี่ยงเพื่อกำจัด ป้องกันหรือลดการเกิดความเสียหายในรูปแบบต่าง ๆ โดยสามารถฟื้นฟูระบบสารสนเทศ และการสำรองและการกู้คืนข้อมูล (Backup and Recovery)

(๒) มีการจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจจะเกิดกับระบบสารสนเทศ (IT Contingency Plan)

(๓) มีระบบรักษาความมั่นคงและปลอดภัย (Security) ของระบบฐานข้อมูล เช่น ระบบ Anti-Virus ระบบไฟฟ้าสำรอง เป็นต้น

(๔) มีการกำหนดสิทธิให้ผู้ใช้ในแต่ละระดับ (Access Rights)

๒.๓ ต้องมีการทบทวนระบบบริหารความเสี่ยงของระบบฐานข้อมูลและสารสนเทศเป็นประจำทุกปี อย่างน้อยปีละ ๑ ครั้ง

๒.๔ มีมาตรการในการตรวจประเมินระบบสารสนเทศ อย่างน้อย ดังนี้

(๑) ควรกำหนดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้แบบอ่านได้อย่างเดียว

(๒) ในกรณีที่จำเป็นต้องเข้าถึงข้อมูลในแบบอื่น ๆ ให้สร้างสำเนาสำหรับข้อมูลนั้น เพื่อให้ผู้ตรวจสอบใช้งาน รวมทั้งควรทำลายหรือลบโดยทันทีที่ตรวจสอบเสร็จ หรือต้องจัดเก็บไว้โดยมีการป้องกันเป็นอย่างดี

(๓) ควรกำหนดให้มีการระบุและจัดสรรทรัพยากรที่จำเป็นต้องใช้ในการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย

(๔) ในกรณีที่มีเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ ควรกำหนดให้แยกการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบออกจากระบบให้บริการจริง หรือระบบที่ใช้ในการพัฒนา และมีการจัดเก็บป้องกันเครื่องมือนั้นจากการเข้าถึงโดยไม่ได้รับอนุญาต

หมวดที่ ๔

การกำหนดหน้าที่ความรับผิดชอบของผู้ปฏิบัติงาน

วัตถุประสงค์

เพื่อกำหนดหน้าที่และแนวปฏิบัติของผู้ปฏิบัติงาน ตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย ในการบริหารจัดการ กำกับ ดูแลเครื่องคอมพิวเตอร์และระบบเครือข่ายให้สามารถใช้งานได้ดีอยู่เสมอ รวมทั้งสอดส่องดูแลการใช้งานของผู้ใช้บริการให้เป็นไปตามนโยบาย

ผู้รับผิดชอบ

๑. ผู้อำนวยการสำนักงานกองทุนน้ำมันเชื้อเพลิง
๒. สำนักนโยบายและยุทธศาสตร์
๓. กลุ่มงานบริหารสารสนเทศ
๔. ผู้ดูแลระบบ

แนวทางปฏิบัติ

๑. **ระดับนโยบาย** ผู้รับผิดชอบ ได้แก่ ผู้อำนวยการสำนักงานกองทุนน้ำมันเชื้อเพลิง มีหน้าที่ดังต่อไปนี้
   (๑) รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตาม กำกับ ดูแล ควบคุมตรวจสอบเจ้าหน้าที่ในระดับบริหาร
   (๒) รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นกรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๒. **ระดับบริหาร** ผู้รับผิดชอบ ได้แก่ ผู้อำนวยการสำนักนโยบายและยุทธศาสตร์ / หัวหน้ากลุ่มงานบริหารสารสนเทศ มีหน้าที่ดังต่อไปนี้
   (๑) รับผิดชอบ กำกับ ดูแลการปฏิบัติงานของผู้ปฏิบัติ ตลอดจนศึกษา ทบทวน วางแผน ติดตามการบริหารความเสี่ยง และระบบรักษาความปลอดภัยฐานข้อมูลและเทคโนโลยีสารสนเทศ
   (๒) รับผิดชอบในการควบคุม ดูแล รักษาความปลอดภัย ระบบสารสนเทศและระบบฐานข้อมูล

๓. **ระดับปฏิบัติ** ผู้รับผิดชอบ ได้แก่ ผู้ดูแลระบบ หรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่ทางสารสนเทศ เช่น นักวิชาการคอมพิวเตอร์ เจ้าหน้าที่คอมพิวเตอร์ มีหน้าที่ดังต่อไปนี้
   ๓.๑ กำหนดรหัสผ่านสำหรับเครื่องคอมพิวเตอร์แม่ข่ายในการใช้งานระดับ BIOS (Basic Integrated Operating System) ระดับปฏิบัติการและเครือข่ายคอมพิวเตอร์
   ๓.๒ ดูแลรักษาเครื่องคอมพิวเตอร์และเครือข่ายของหน่วยงาน
   ๓.๓ ติดตั้งเครื่องคอมพิวเตอร์และเครือข่ายของหน่วยงาน ระบบการเข้ารหัสลับข้อมูลอัตโนมัติ ระบบป้องกันและตรวจจับการบุกรุก ระบบป้องกันและกำจัดโปรแกรมประสงค์ร้าย รวมทั้งอุปกรณ์และระบบอื่นใดที่จำเป็นต่อการใช้เครื่องคอมพิวเตอร์และเครือข่าย เพื่อให้สามารถใช้งานได้อย่างมั่นคง
   ๓.๔ ตรวจสอบดูแลการใช้งานเครื่องคอมพิวเตอร์และเครือข่าย ให้เป็นไปด้วยความเรียบร้อยและมีประสิทธิภาพ หากตรวจพบสิ่งผิดปกติเกี่ยวกับการใช้งานเครื่องคอมพิวเตอร์และเครือข่ายให้รีบดำเนินการแก้ไข รวมทั้งป้องกันและบรรเทาความเสียหายที่อาจเกิดขึ้นในทันที

๓.๕ ติดตั้งและปรับปรุงโปรแกรมคอมพิวเตอร์สำหรับแก้ไขข้อบกพร่องของเครื่องคอมพิวเตอร์และเครือข่ายที่เกี่ยวกับความมั่นคง (Server pack หรือ Security patch) ให้มีความมั่นคงในการใช้งานและทันสมัยอยู่เสมอ

๓.๖ ตรวจสอบความมั่นคงในการใช้งานเครื่องคอมพิวเตอร์แม่ข่าย และเครือข่ายคอมพิวเตอร์ทุกเดือน

๓.๗ เปลี่ยนรหัสผ่านสำหรับการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย และเครือข่ายคอมพิวเตอร์ทุก ๖ เดือน หรือเมื่อมีความจำเป็นเพื่อความมั่นคงในการใช้งาน

๓.๘ สำรองข้อมูลที่มีความสำคัญแบบสมบูรณ์ (Full back-up) อย่างน้อยเดือนละ ๑ ครั้ง

๓.๙ ลบข้อมูลคอมพิวเตอร์หรือโปรแกรมคอมพิวเตอร์แม่ข่ายอย่างถาวร หรือทำลายข้อมูลที่เกี่ยวข้องกับการปฏิบัติงานของหน่วยงานบนเครื่องคอมพิวเตอร์และเครือข่าย เมื่อหมดความจำเป็นในการใช้งาน หรือเมื่อหมดสัญญาเช่า

๓.๑๐ เก็บข้อมูลที่บันทึกการใช้งานเครื่องคอมพิวเตอร์แม่ข่ายและเครือข่ายคอมพิวเตอร์ (Log File) ย้อนหลังไม่น้อยกว่าเก้าสิบวัน ไว้ในหน่วยความจำเครื่องคอมพิวเตอร์อย่างน้อย ๑ เครื่อง ซึ่งแยกต่างหากจากเครื่องคอมพิวเตอร์แม่ข่าย

๓.๑๑ ดูแลรักษาและตรวจสอบช่องทางการสื่อสาร (Communication port) ของเครือข่ายคอมพิวเตอร์อยู่เสมอ และปิดช่องทางการสื่อสาร (Communication port) ของเครือข่ายคอมพิวเตอร์ที่ไม่มีความจำเป็นต้องใช้งานในทันที

๓.๑๒ ดูแลรักษาและปรับปรุงบัญชีผู้ใช้บริการอินทราเน็ต หรือบัญชีจดหมายอิเล็กทรอนิกส์ให้ถูกต้องและเป็นปัจจุบันอยู่เสมอ โดยให้ยกเลิกสิทธิการใช้งานของผู้ใช้บริการที่พ้นสภาพการเป็นผู้ใช้บริการ

๓.๑๓ ฝึกอบรมและให้ความรู้แก่ผู้ใช้บริการเกี่ยวกับหน้าที่และวิธีปฏิบัติตามระเบียบ

๓.๑๔ เสนอรายงานการให้บริการและการใช้งานระบบคอมพิวเตอร์ รวมทั้งความเห็นและข้อสังเกตต่อผู้อำนวยการ โดยเสนอผ่านผู้บังคับบัญชาที่เหนือขึ้นไป เพื่อทราบหรือเพื่อพิจารณาสั่งการเกี่ยวกับการปรับปรุงประสิทธิภาพและการบริหารระบบคอมพิวเตอร์

๓.๑๕ ตั้งสัญญาณนาฬิกาของเครื่องคอมพิวเตอร์และเครือข่ายให้ตรงกับเวลามาตรฐานสากลจากเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการเวลา ตามที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม กำหนดไว้

๓.๑๖ การใช้ระบบการสื่อสารข้อมูลของเครือข่ายคอมพิวเตอร์แบบไร้สาย ผู้ดูแลระบบต้องดำเนินการดังต่อไปนี้

(๑) ใช้เทคโนโลยีการรักษาความมั่นคงของระบบการสื่อสารข้อมูลของเครือข่ายคอมพิวเตอร์แบบไร้สายที่ต้องมีการเข้ารหัสลับข้อมูลในการสื่อสารระหว่างเครื่องคอมพิวเตอร์และอุปกรณ์ที่ใช้ในการส่งและรับสัญญาณของเครือข่ายคอมพิวเตอร์แบบไร้สายซึ่งมีมาตรฐานของเทคโนโลยีไม่ต่ำกว่า WPA (Wi-Fi Protected Access)

(๒) ใช้เครื่องคอมพิวเตอร์และอุปกรณ์ที่ใช้ในการส่งและรับสัญญาณของเครือข่ายคอมพิวเตอร์ไร้สาย ซึ่งมีกลไกการตรวจสอบพิสูจน์ตัวตนของผู้ใช้บริการ (User Authentication) ที่มีความมั่นคง เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตสามารถเข้าใช้งานเครือข่ายคอมพิวเตอร์ไร้สายได้ และต้องสนับสนุนการส่งและรับข้อมูลและรหัสลับของผู้ใช้บริการด้วยโปรโตคอล IEEE ๘๐๒.๑x ไปยัง RADIUS Server (Remote Authentication Dial-In User Service Server) ที่ติดตั้งไว้เพื่อทำหน้าที่ตรวจสอบพิสูจน์ตัวตนของผู้ใช้บริการจากฐานข้อมูลผู้ใช้บริการที่ได้รับอนุญาตให้ใช้งาน

(๓) ติดตั้งใช้งานระบบเก็บบันทึกการใช้งานเครือข่ายคอมพิวเตอร์แบบไร้สายและทำการตรวจสอบบันทึกการใช้งานดังกล่าวอย่างสม่ำเสมอ เพื่อตรวจสอบการใช้งานเครือข่ายคอมพิวเตอร์แบบไร้สาย และจัดส่งรายงานผลการตรวจสอบเป็นรายเดือนไปให้หัวหน้าผู้ดูแลระบบทราบด้วย และในกรณีที่ตรวจสอบพบการใช้งานเครือข่ายคอมพิวเตอร์แบบไร้สายที่ผิดปกติ ให้หัวหน้าผู้ดูแลระบบรายงานผู้อำนวยการทราบทันที

(๔) ควบคุมดูแลให้ผู้ใช้บริการที่ใช้งานเครือข่ายคอมพิวเตอร์แบบไร้สาย ไม่ให้ใช้งานช่องรับและส่งสัญญาณทางอินฟราเรด และอุปกรณ์เชื่อมต่อด้วยเทคโนโลยีแบบไร้สาย (Bluetooth) ในขณะที่กำลังใช้งานเครือข่ายคอมพิวเตอร์แบบไร้สาย เพื่อป้องกันการรั่วไหลของข้อมูล

(๕) ติดตั้งและใช้งานระบบตรวจจับผู้บุกรุก (Intrusion Detection System) เช่น Personal Firewall ประเภทต่าง ๆ เป็นต้น

(๖) ติดตั้งและใช้งานโปรแกรมคอมพิวเตอร์สำหรับป้องกันและกำจัดโปรแกรมประสงค์ร้าย รวมทั้งทำการปรับปรุงให้ทันสมัยอยู่เสมอ

(๗) ควบคุมดูแลไม่ให้ผู้ใช้บริการใช้งานเครือข่ายคอมพิวเตอร์แบบไร้สาย ในการเข้าสู่ระบบเครือข่ายคอมพิวเตอร์ของหน่วยงาน เช่น ระบบอินทราเน็ต (Intranet) ระบบสารบรรณอิเล็กทรอนิกส์ ระบบบริหารทรัพยากรบุคคล และฐานข้อมูลต่าง ๆ ของหน่วยงาน เป็นต้น

(๘) ปฏิบัติหน้าที่อื่นใดที่เกี่ยวข้องกับการให้บริการเครื่องคอมพิวเตอร์แม่ข่าย ตามที่ผู้อำนวยการมอบหมาย