นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ องค์การอุตสาหกรรมป่าไม้

พ.ศ.๒๕๕๘

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
องค์การอุตสาหกรรมป่าไม้

๑. วัตถุประสงค์และขอบเขต

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ ในมาตรา ๕ “หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้” และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ.๒๕๕๓ กำหนดให้หน่วยงานของรัฐต้องจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร นั้น

เพื่อให้ระบบเทคโนโลยีสารสนเทศขององค์การอุตสาหกรรมป่าไม้หรือต่อไปนี้เรียกว่า “อ.อ.ป.” เป็นไปอย่างเหมาะสมมีประสิทธิภาพมีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง และการถูกคุกคามจากภัยต่างๆ อ.อ.ป.จึงเห็นสมควรกำหนดนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศโดยกำหนดให้มีมาตรฐาน แนวปฏิบัติ ขั้นตอนปฏิบัติ ให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ตามพระราชกฤษฎีกาฯ และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ฯ โดยมีวัตถุประสงค์ดังต่อไปนี้

๑.๑ การจัดทำนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสารเพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารหรือเครือข่ายคอมพิวเตอร์ขององค์การอุตสาหกรรมป่าไม้ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล

๑.๒ นโยบายนี้จะต้องทำการเผยแพร่ให้เจ้าหน้าที่ทุกระดับใน อ.อ.ป. ได้รับทราบและเจ้าหน้าที่ทุกคนจะต้องถือปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

๑.๓ เพื่อกำหนดมาตรฐานแนวทางปฏิบัติและวิธีปฏิบัติให้ผู้บริหาร เจ้าหน้าที่ผู้ดูแลระบบ และบุคคลภายนอกที่ปฏิบัติงานให้กับ อ.อ.ป. ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของ อ.อ.ป. ในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด

๒. องค์ประกอบของนโยบาย

คำนิยาม

ส่วนที่ ๑ การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ
ส่วนที่ ๒ การบริหารจัดการการเข้าถึงของผู้ใช้งาน
ส่วนที่ ๓ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน
ส่วนที่ ๔ การควบคุมการเข้าถึงและใช้บริการระบบเครือข่าย
ส่วนที่ ๕ การควบคุมการเข้าถึงระบบปฏิบัติการ
ส่วนที่ ๖ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ
ส่วนที่ ๗ การจัดทำระบบสำรองข้อมูล
ส่วนที่ ๘ การตรวจสอบและประเมินความเสี่ยง
ส่วนที่ ๙ การควบคุมการเข้าออกห้องควบคุมระบบคอมพิวเตอร์และการป้องกันความเสียหาย

ส่วนที่ ๑๐ การใช้งานคอมพิวเตอร์ส่วนบุคคล
ส่วนที่ ๑๑ การจัดเตรียมระบบเครือข่ายคอมพิวเตอร์
ส่วนที่ ๑๒ การบริหารระบบเครือข่ายคอมพิวเตอร์
ส่วนที่ ๑๓ การนำ Open Source Software มาใช้ในหน่วยงาน
ส่วนที่ ๑๔ การสร้างความตระหนักในเรื่องการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ
ส่วนที่ ๑๕ การกำหนดแบ่งอำนาจหน้าที่ผู้รับผิดชอบ
ส่วนที่ ๑๖ นโยบายความมั่นคงปลอดภัยการใช้งานอินเทอร์เน็ต
ส่วนที่ ๑๗ แนวทางการใช้งานจดหมายอิเล็กทรอนิกส์
ส่วนที่ ๑๘ ข้อตกลงการใช้บริการจดหมายอิเล็กทรอนิกส์

คำนิยาม

คำนิยามที่ใช้ในนโยบายนี้

“อ.อ.ป.” หมายถึง องค์การอุตสาหกรรมป่าไม้

“การรักษาความมั่นคงปลอดภัย” หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศขององค์การอุตสาหกรรมป่าไม้

“ผู้ใช้งาน” หมายถึง บุคคลที่ได้รับอนุญาต (Authorized user) ให้สามารถใช้งานบริหารหรือดูแลรักษาระบบเทคโนโลยีสารสนเทศขององค์การอุตสาหกรรมป่าไม้ โดยมีสิทธิและหน้าที่ขึ้นอยู่กับบทบาท (Role)

“สิทธิของผู้ใช้งาน” หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศของหน่วยงาน

“สินทรัพย์” หมายถึง ข้อมูลระบบ ข้อมูลทรัพย์สินด้านระบบเทคโนโลยีสารสนเทศหรือสิ่งใดก็ตามที่มีคุณค่าของหน่วยงาน เช่น อุปกรณ์ระบบเครือข่ายซอฟต์แวร์ที่มีลิขสิทธิ์ เป็นต้น

“การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ” หมายถึง การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานเครือข่ายระบบเทคโนโลยีสารสนเทศ ทั้งทางอิเล็กทรอนิกส์ และทางกายภาพ รวมทั้งการอนุญาตสำหรับบุคคลภายนอก ตลอดจนการกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

“ความมั่นคงปลอดภัยด้านสารสนเทศ” หมายถึง การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non-repudiation) และความน่าเชื่อถือ (Reliability)

“เหตุการณ์ด้านความมั่นคงปลอดภัย” หมายถึง กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่ให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

“สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด” หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or Unexpected) ซึ่งอาจทำให้ระบบถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยคุกคาม

“หน่วยงานภายนอก” หมายถึง องค์กรหรือหน่วยงานที่ อ.อ.ป. อนุญาตให้มีสิทธิ์ในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่างๆ ของหน่วยงาน โดยจะได้รับสิทธิ์ในการใช้งานตามอำนาจและต้องรับผิดชอบในการรักษาความลับของข้อมูล

“รหัสผ่าน” (Password) หมายถึง ตัวอักษรหรืออักขระ หรือตัวเลขที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคลเพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

“ข้อมูลคอมพิวเตอร์” หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดในระบบคอมพิวเตอร์ในสภาพที่มีระบบคอมพิวเตอร์ที่อาจประมวลผลได้ และให้ความหมายรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์

“ระบบเครือข่าย” (Network System) หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่างๆ ของ อ.อ.ป.ได้ เช่น ระบบแลน (LAN) อินทราเน็ต (Intranet) ระบบอินเทอร์เน็ต (Internet) เป็นต้น

- ระบบแลน (LAN) และระบบอินทราเน็ต (Intranet) หมายถึง ระบบเครือข่ายที่เชื่อมต่อระบบคอมพิวเตอร์ต่างๆ ภายในหน่วยงานเข้าด้วยกันเป็นเครือข่ายที่มีจุดประสงค์ เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน
- ระบบอินเตอร์เน็ต (Internet) หมายถึง ระบบเครือข่ายที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่างๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตทั่วโลก

“ระบบเทคโนโลยีสารสนเทศ” (Information System) หมายถึง ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการการพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ โปรแกรมข้อมูลและสารสนเทศ เป็นต้น

“พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ” (Information System Workspace) หมายถึง พื้นที่ที่หน่วยงานอนุญาตให้มีการใช้งานระบบเทคโนโลยีสารสนเทศ โดยแบ่งเป็น

- พื้นที่ทำงานทั่วไป (General Working Area) หมายถึง พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคลและคอมพิวเตอร์แบบพกพาที่ประจำโต๊ะทำงาน รวมถึงพื้นที่ทำงานของผู้ดูแลระบบ (System Administrator)
- พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย (IT Equipment or Network Area) หมายถึง พื้นที่ติดตั้งและจัดเก็บอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่ายและให้หมายความรวมถึงพื้นที่จัดเก็บข้อมูลคอมพิวเตอร์

“ห้องควบคุมระบบ” หมายถึง ห้องที่ติดตั้งและจัดวางระบบ Server อุปกรณ์เชื่อมต่อ และอุปกรณ์เครือข่าย

“จดหมายอิเล็กทรอนิกส์” (E-Mail) หมายถึง ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกัน โดยผ่านเครือข่ายคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้ง ตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลานคนก็ได้

“เจ้าหน้าที่ห้องควบคุมระบบ” หมายถึง หัวหน้าฝ่ายสารสนเทศ หัวหน้าส่วนสารสนเทศ ผู้ดูแลระบบคอมพิวเตอร์ ผู้ดูแลระบบเครือข่าย และผู้ดูแลระบบฐานข้อมูล

“ผู้บริหารระดับสูง” (Chief Executive Officer : CEO) หมายถึง ผู้อำนวยการองค์การอุตสาหกรรมป่าไม้

“ผู้บริหาร เทคโนโลยีสารสนเทศ ระดับสูง” (Chief Information Officer: CIO) หมายถึง รองผู้อำนวยการองค์การอุตสาหกรรมป่าไม้ที่มีหน้าที่ดูแลรับผิดชอบด้านเทคโนโลยีสารสนเทศ ซึ่งมีบทบาทหน้าที่และความรับผิดชอบในส่วนของการกำหนดนโยบายมาตรฐานการควบคุมดูแลการใช้งานระบบเทคโนโลยีสารสนเทศ

“คณะทำงานด้านเทคโนโลยีสารสนเทศและการสื่อสารของ อ.อ.ป.” หมายถึง คณะทำงานที่ อ.อ.ป. แต่งตั้งมา เพื่อดำเนินการด้านความปลอดภัยระบบคอมพิวเตอร์และเครือข่าย

ส่วนที่ ๑
การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ
(Access Control)

๑. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้รับอนุญาตเข้าถึงระบบเทคโนโลยีสารสนเทศของ อ.อ.ป. และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุกจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ที่จะสร้างความเสียหายแก่ข้อมูลหรือการทำงานของระบบเทคโนโลยีสารสนเทศให้หยุดชะงักและทำให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงานได้อย่างถูกต้อง

๒. กระบวนการหลักในการควบคุมการเข้าถึงระบบ

๒.๑ จัดทำบัญชีทรัพย์สินหรือทะเบียนทรัพย์สิน การจำแนกกลุ่มทรัพยากรของระบบหรือการทำงานโดยให้กำหนดกลุ่มผู้ใช้งานและสิทธิของกลุ่มผู้ใช้งาน

๒.๒ สถานที่ตั้งของระบบเทคโนโลยีสารสนเทศที่สำคัญต้องมีการควบคุมการเข้าออกที่รัดกุมและอนุญาตให้เฉพาะบุคคลที่ได้รับสิทธิและมีความจำเป็นผ่านเข้าใช้งานได้เท่านั้น

๒.๓ ผู้ดูแลระบบต้องกำหนดสิทธิการเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบเทคโนโลยีสารสนเทศ รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ผู้ใช้ระบบจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

๒.๔ ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายเท่านั้นที่สามารถแก้ไขเปลี่ยนแปลงสิทธิการเข้าถึงข้อมูลและระบบข้อมูลได้

๒.๕ ผู้ดูแลระบบควรจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงานและตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบข้อมูลสำคัญ

๒.๖ ผู้ดูแลระบบต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิต่างๆ และการผ่านเข้าออกสถานที่ตั้งของระบบของผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาต เพื่อเป็นหลักฐานในการตรวจหากมีปัญหาเกิดขึ้น

๓. การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

๓.๑ ผู้ดูแลระบบมีหน้าที่ในการตรวจสอบการอนุมัติและกำหนดสิทธิในการผ่านเข้าสู่ระบบให้แก่ผู้ใช้ในการขออนุญาตเข้าระบบงานนั้น จะต้องมีการทำเป็นเอกสารเพื่อขอสิทธิในการเข้าสู่ระบบและกำหนดให้มีการลงนามอนุมัติเอกสารดังกล่าวต้องมีการจัดเก็บไว้เป็นหลักฐาน

๓.๒ เจ้าของข้อมูลและเจ้าของระบบงานจะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่จำเป็นต้องรู้ตามหน้าที่งานเท่านั้น เนื่องจากการให้สิทธิเกินความจำเป็นในการใช้งานจะนำไปสู่ความเสี่ยงในการใช้งานเกินอำนาจหน้าที่ ดังนั้น การกำหนดสิทธิในการเข้าถึงระบบงานต้องกำหนดตามความจำเป็นขั้นต่ำเท่านั้น

๓.๓ ผู้ใช้งานจะต้องได้รับอนุญาตจากเจ้าหน้าที่ที่รับผิดชอบข้อมูลและระบบงานตามความจำเป็นต่อการใช้งานระบบเทคโนโลยีสารสนเทศ

๔. การบริหารจัดการการเข้าถึงของผู้ใช้

๔.๑ กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจ ดังนี้

(๑) กำหนดสิทธิของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง เช่น

- อ่านอย่างเดียว

- สร้างข้อมูล
- ป้อนข้อมูล
- แก้ไข
- อนุมัติ
- ไม่มีสิทธิ์

(๒) กำหนดเกณฑ์การระงับสิทธิ มอบอำนาจ ให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) ที่กำหนดไว้

(๓) ผู้ใช้งานที่ต้องการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของ อ.อ.ป.จะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาตจากหัวหน้าฝ่ายสารสนเทศหรือผู้ดูแลระบบที่ได้รับมอบหมาย

๔.๒ การลงทะเบียนใหม่ ผู้ดูแลระบบควรกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการ สำหรับการลงทะเบียนใหม่ เพื่อให้มีสิทธิต่างๆ ในการใช้งานตามความจำเป็น รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน เช่น เมื่อลาออกไปต้องทำภายใน ๒๔ ชั่วโมง หรือเมื่อเปลี่ยนตำแหน่งงานภายในต้องทำการภายใน ๗ วัน

๔.๓ กำหนดสิทธิการใช้ระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์ โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (e-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเตอร์เน็ต เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้ดูแลระบบเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

๔.๔ ผู้ใช้ต้องลงนามรับทราบสิทธิและหน้าที่เกี่ยวกับการใช้งานระบบเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษรและต้องปฏิบัติตามอย่างเคร่งครัด

๔.๕ การบริหารจัดการบัญชีรายชื่อผู้ใช้งาน (User Account) และรหัสผ่านของเจ้าหน้าที่

๔.๕.๑ ผู้ดูแลระบบที่รับผิดชอบงานนั้นๆ ต้องกำหนดสิทธิของเจ้าหน้าที่ในการเข้าถึงระบบเทคโนโลยีสารสนเทศแต่ละระบบรวมทั้งกำหนดสิทธิแยกตามหน้าที่ที่รับผิดชอบ ซึ่งมีแนวปฏิบัติตามที่กำหนดไว้ในเอกสาร “การบริหารจัดการการเข้าถึงของผู้ใช้งาน”

๔.๕.๒ การกำหนดการเปลี่ยนแปลงและยกเลิกรหัสผ่านต้องปฏิบัติตาม “การบริหารจัดการการเข้าถึงของผู้ใช้งาน”

๔.๕.๓ ควรกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันที เมื่อพ้นระยะเวลาดังกล่าว

๔.๕.๔ ควรมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ทุกครั้งหลังหมดความจำเป็นในการใช้งาน หรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานานก็ควรเปลี่ยนรหัสผ่านทุก ๓ เดือน เป็นต้น

๕. การจัดเก็บข้อมูล

๕.๑ อ.อ.ป.จัดแบ่งประเภทของข้อมูล ออกเป็น

๕.๑.๑ ข้อมูลสารสนเทศด้านการบริหาร เช่น ข้อมูลนโยบาย ข้อมูลบุคลากร ข้อมูลงบประมาณการเงินและบัญชี เป็นต้น

๕.๑.๒ ข้อมูลสารสนเทศด้านการบริหาร เช่น ข้อมูลจำนวนพื้นที่สวนป่า ข้อมูลผลผลิตไม้ เป็นต้น

๕.๒ อ.อ.ป.จัดแบ่งระดับความสำคัญของข้อมูลออกเป็น ๓ ระดับ คือ

๕.๒.๑ ข้อมูลที่มีความสำคัญมากที่สุด

๕.๒.๒ ข้อมูลที่มีระดับความสำคัญปานกลาง

๕.๒.๓ ข้อมูลที่มีระดับความสำคัญน้อย

๕.๓ อ.อ.ป.จัดแบ่งระดับความลับของข้อมูลออกเป็น ๔ ระดับ คือ

๕.๓.๑ ข้อมูลลับที่สุด หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด

๕.๓.๒ ข้อมูลลับมาก หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรง

๕.๓.๓ ข้อมูลลับ หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย

๕.๓.๔ ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

๕.๔ อ.อ.ป.จัดแบ่งระดับชั้นการเข้าถึงออกเป็น ๓ ระดับ คือ

๕.๔.๑ ระดับชั้นสำหรับผู้บริหาร

๕.๔.๒ ระดับชั้นสำหรับผู้ใช้งานทั่วไป

๕.๔.๓ ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมาย

๕.๕ การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

๕.๕.๑ ผู้ดูแลระบบกำหนดชั้นความลับของข้อมูล วิธีปฏิบัติในการจัดเก็บข้อมูลและวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภท ชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ

๕.๕.๒ เจ้าของข้อมูลจะต้องมีการสอบทานความเหมาะสมของสิทธิในการเข้าถึงข้อมูลของผู้ใช้งานเหล่านี้ อย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิต่างๆ ที่ให้ไว้ยังคงมีความเหมาะสม

๕.๕.๓ วิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน ผู้ดูแลระบบจะต้องกำหนดรายชื่อผู้ใช้งาน (User Account) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล

๕.๕.๔ การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล

๕.๕.๕ ควรมีการกำหนดให้เปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูลตามที่ระบุไว้ในเอกสาร “การบริหารจัดการการเข้าถึงของผู้ใช้งาน”

๕.๕.๖ ควรมีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของหน่วยงาน เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

ส่วนที่ ๒
การบริหารจัดการการเข้าถึงของผู้ใช้งาน
(User Access Management)

๑. วัตถุประสงค์

เพื่อควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้วและผ่านการฝึกอบรมหลักสูตรการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (Information Security Awareness Training) เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาตอย่างน้อย ดังนี้

๒. การลงทะเบียนผู้ใช้งาน (User Registration)

๒.๑ จัดทำแบบฟอร์มขอใช้ระบบงานสารสนเทศ และให้ผู้ใช้งานกรอกข้อมูลลงในแบบฟอร์ม เพื่อตรวจสอบสิทธิและดำเนินการตามขั้นตอนการลงทะเบียนผู้ใช้งาน

๒.๒ มีการระบุชื่อบัญชีผู้ใช้งานแยกกันเป็นรายบุคคล ไม่ซ้ำซ้อนกัน

๒.๓ การกำหนดชื่อผู้ใช้งาน (Username) จะกำหนดจากชื่อภาษาอังกฤษและตามด้วยตัวอักษรตัวแรกของนามสกุล หากซ้ำให้เพิ่มอักษรตัวที่สอง หรือจนกว่าจะไม่ซ้ำกับชื่อผู้ใช้งานคนอื่น

๒.๔ จำกัดการใช้งานบัญชีผู้ใช้งานแบบกลุ่มภายใต้บัญชีรายชื่อเดียวกัน และอนุญาตให้ใช้เท่าที่จำเป็น

๒.๕ มีการตรวจสอบและมอบหมายสิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ และ /หรือความต้องการทางธุรกิจ

๒.๖ จัดทำเอกสารแสดงถึงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งาน ซึ่งต้องลงนามรับทราบด้วย

๒.๗ มีการทำบันทึกและจัดเก็บข้อมูลการขออนุมัติเข้าใช้ระบบเทคโนโลยีสารสนเทศ

๒.๘ มีหลักเกณฑ์ในการอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศ และได้รับการพิจารณาอนุญาตจากหัวหน้าฝ่ายสารสนเทศหรือผู้ดูแลระบบที่ได้รับมอบหมาย

๒.๙ ผู้ดูแลระบบต้องมีการกำหนดการถอดถอนสิทธิการเข้าถึงระบบเทคโนโลยีสารสนเทศโดยทันทีเมื่อผู้ใช้งานหมดสภาพการเป็นผู้ปฏิบัติงาน อ.อ.ป.

๓. การบริหารจัดการสิทธิของผู้ใช้งาน (User Management)

โดยแสดงรายละเอียดที่เกี่ยวกับการควบคุมและจำกัดสิทธิเพื่อให้สามารถเข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นๆ ที่เกี่ยวข้องกับการเข้าถึง ดังนี้

๓.๑ กำหนดสิทธิการใช้ระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์ โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต เป็นต้น โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้ดูแลระบบเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

๓.๒ ผู้ใช้ต้องลงนามรับทราบสิทธิและหน้าที่เกี่ยวกับการใช้งานระบบเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษรและต้องปฏิบัติตามอย่างเคร่งครัด

๓.๓ ผู้ดูแลระบบต้องจัดเก็บการมอบหมายสิทธิให้แก่ผู้ใช้งาน

๓.๔ กรณีมีความต้องให้สิทธิพิเศษต้องมีการควบคุมการใช้งานอย่างรัดกุม ทั้งนี้ในการพิจารณาว่าการควบคุมีความรัดกุมเพียงพอหรือไม่นั้น หน่วยงานจะใช้ปัจจัยต่อไปนี้ประกอบการพิจารณาในภาพรวม

๓.๔.๑ ควรได้รับความเห็นชอบจากผู้มีอำนาจหน้าที่

๓.๔.๒ ควรควบคุมสิทธิพิเศษการใช้งานอย่างเข้มงวด เช่น กำหนดให้มีการควบคุมการใช้งาน User ดังกล่าวในลักษณะ Dual Control โดยให้เจ้าหน้าที่ ๒ คนถือรหัสผ่านคนละครึ่ง หรือเก็บซอง Password ไว้ในตู้เซฟ เป็นต้น

๓.๔.๓ ควรมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

๓.๔.๔ ควรมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้าง

๓.๔.๕ ต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

๓.๕ ในกรณีที่มีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิพิเศษที่รับว่าเข้าถึงได้ถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

๔. การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management) โดยจัดทำกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม ดังนี้

๔.๑ ผู้ดูแลระบบกำหนดให้ผู้ใช้งานเปลี่ยนรหัสผ่านโดยทันที ภายหลังจากที่ได้รับรหัสผ่านชั่วคราว และควรเปลี่ยนรหัสผ่านที่มีความยากต่อการเดาโดยผู้อื่น

๔.๒ ผู้ดูแลระบบต้องให้ผู้ใช้งานลงนามเพื่อป้องกันการเปิดเผยข้อมูลรหัสผ่านของตน เช่น ลงนามในเอกสารเพื่อแสดงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งานในการเข้าถึงระบบเทคโนโลยีสารสนเทศของหน่วยงาน

๔.๓ ผู้ดูแลระบบกำหนดขั้นตอนปฏิบัติสำหรับการตั้งหรือเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัย

๔.๔ ผู้ดูแลระบบกำหนดรหัสผ่านชั่วคราว โดยกำหนดรหัสผ่านให้มีความยากต่อการเดาโดยผู้อื่น และควรกำหนดรหัสผ่านที่แตกต่างกัน

๔.๕ ผู้ดูแลระบบจัดส่งรหัสผ่านให้ผู้ใช้งาน โดยหลีกเลี่ยงการใช้อีเมล์เป็นช่องทางในการส่งและควรกำหนดให้ผู้ใช้งานตอบกลับจากที่ได้รับรหัสผ่านแล้ว

๕. การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Rights) มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบเทคโนโลยีสารสนเทศ ดังนี้

๕.๑ ผู้ดูแลระบบจะต้องดำเนินการทบทวนสิทธิการเข้าถึงระบบเทคโนโลยีสารสนเทศอย่างน้อยปีละ ๑ ครั้ง

๕.๒ ผู้ดูแลระบบทบทวนสิทธิสำหรับผู้ที่มีสิทธิในระดับสูง เช่น สิทธิในระดับผู้ดูแลระบบ ด้วยความถี่ที่มากกว่าผู้ใช้งานทั่วไป

๕.๓ ผู้ดูแลระบบทบทวนสิทธิตามรอบระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงใดๆ เช่น การเลื่อนตำแหน่ง ลดตำแหน่ง ย้ายหน่วยงาน หรือสิ้นสุดการจ้างงาน

๕.๔ ผู้ดูแลระบบต้องกำหนดให้มีการบันทึกการเปลี่ยนแปลงต่อบัญชีผู้ใช้งานที่มีสิทธิในระดับสูง เพื่อใช้ในการทบทวนในภายหลัง

ส่วนที่ ๓
การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน
(User Responsibilities)

๑. วัตถุประสงค์

เพื่อควบคุมและกำหนดมาตรการ การปฏิบัติงานของผู้ใช้งานให้เป็นไปตามหน้าที่ที่ได้รับมอบหมายที่เกี่ยวข้องกับข้อมูลสารสนเทศ และบังคับใช้กับผู้ที่ใช้งานระบบเทคโนโลยีสารสนเทศของ อ.อ.ป. เพื่อป้องกันการเข้าถึงข้อมูลโดยบุคคลอื่นและเปิดเผยข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต

๒. การใช้งานรหัสผ่าน (Password)

ผู้ใช้งานระบบเทคโนโลยีสารสนเทศควรปฏิบัติตามข้อกำหนดในการใช้งานรหัสผ่าน ดังนี้

๒.๑ รหัสผ่าน (Password) ควรมีความยาวไม่น้อยกว่า ๖ ตัวอักษร โดยอาจจะมีการผสมกันระหว่างตัวเลข ตัวอักษรที่เป็นตัวพิมพ์เล็กหรือตัวพิมพ์ใหญ่ ตัวอักขระพิเศษและสัญลักษณ์ต่างๆ ด้วย

๒.๒ ไม่ควรกำหนดรหัสผ่าน (Password) จากชื่อ หรือชื่อสกุลของผู้ใช้บริการ ชื่อบุคคลในครอบครัว บุคคลที่มีความสัมพันธ์กับตน หรือคำศัพท์ที่ใช้ในพจนานุกรม หรือจากหมายเลขโทรศัพท์

๒.๓ ควรทำการเปลี่ยนรหัสผ่าน (Password) เพื่อใช้งานเครื่องคอมพิวเตอร์ของหน่วยงานทุกๆ ๓ -๖ เดือน หรือเปลี่ยนรหัสผ่าน (Password) ทุกครั้งที่มีสัญญาณบอกเหตุว่าอาจรั่วไหล

๒.๔ ผู้ใช้บริการจะต้องเก็บรักษารหัสผ่าน (Password) สำหรับการใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายที่ได้มา โดยถือว่าเป็นความลับเฉพาะบุคคล และจะต้องไม่เปิดเผย หรือกระทำการใดให้ผู้อื่นทราบโดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

๒.๕ ผู้ใช้งานควรเปลี่ยนรหัสผ่านโดยทันทีเมื่อทราบว่ารหัสผ่านของตนอาจถูกเปิดเผยหรือล่วงรู้โดยผู้อื่น

๒.๖ ผู้ใช้งานควรตั้งรหัสผ่านที่มีความยาวเกินกว่าขั้นต่ำกำหนดไว้

๒.๗ ผู้ใช้งานควรหลีกเลี่ยงการตั้งรหัสผ่านที่ประกอบด้วยอักขระที่เรียงกัน เช่น ๑๒๓, abcd, กลุ่มของตัวอักขระที่เหมือนกัน เช่น ๑๑๑, aaa เป็นต้น

๒.๘ ผู้ใช้งานไม่ควรกำหนดให้ทำการบันทึกรหัสผ่านหรือจดจำรหัสผ่านของตนเองไว้ เพื่อความสะดวกของตนเองเมื่อทำการ Log in ในภายหลัง

๒.๙ ผู้ใช้งานไม่ควรใช้รหัสผ่านของตนร่วมกับผู้อื่น

๒.๑๐ ผู้ใช้งานควรหลีกเลี่ยงการใช้รหัสผ่านเดียวกันสำหรับระบบงานต่างๆ ที่ใช้งาน

๓. การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์

๓.๑ ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานออกจากระบบเทคโนโลยีสารสนเทศโดยทันทีเมื่อเสร็จสิ้นงาน เช่น ระบบงานเครื่องคอมพิวเตอร์ที่ใช้หรือเครื่องคอมพิวเตอร์แบบพกพา

๓.๒ ผู้ใช้งานควรล็อคอุปกรณ์ที่สำคัญเมื่อไม่ได้ใช้งานหรือปล่อยทิ้งไว้โดยไม่ได้ดูแลชั่วคราว

๓.๓ ผู้ดูแลระบบควรกำหนดให้พนักงานป้องกันผู้อื่นเข้าใช้เครื่องคอมพิวเตอร์หรือระบบเทคโนโลยีสารสนเทศของตนเอง โดยใส่รหัสผ่านให้ถูกต้องก่อนเข้าใช้งานเครื่องคอมพิวเตอร์

๔. การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear Desk and Clear Screen Policy)

๔.๑ ผู้ดูแลระบบต้องจัดให้มีการควบคุมการใช้งานสารสนเทศในระบบเทคโนโลยีสารสนเทศ ได้แก่ กำหนดสิทธิในการใช้งาน เช่น เขียน อ่าน ลบได้ เป็นต้น กำหนดกลุ่มของผู้ใช้ที่สามารถใช้งานได้ ตรวจสอบว่าสารสนเทศที่อนุญาตให้ใช้งานนั้นมีเฉพาะข้อมูลที่จำเป็นต้องใช้งาน

๔.๒ การแยกระบบเทคโนโลยีสารสนเทศที่มีความสำคัญสูง หัวหน้าฝ่ายสารเทศจะต้องแยกระบบเทคโนโลยีสารสนเทศที่มีความสำคัญหรือมีความเสี่ยงสูงไว้อีกบริเวณหนึ่ง เช่น การแบ่งระหว่างระบบที่เชื่อมต่ออินเทอร์เน็ตกับระบบอินทราเน็ตภายในที่ใช้งานในหน่วยงาน

๔.๓ การตัดเวลาการใช้งานเครื่องลูกข่าย ผู้ดูแลระบบต้องมีวิธีการตัดเวลาการใช้งานเครื่องลูกข่ายเมื่อเครื่องลูกข่ายนั้นไม่มีการใช้งานเป็นระยะเวลาหนึ่ง เช่น กลไกในการล็อคหน้าจอและต้องใช้รหัสผ่านในการเข้าสู่ระบบ

๔.๔ ต้องมีมาตรการรักษาความปลอดภัยข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของหน่วยงาน เช่น ส่งซ่อม หรือทำลายข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน

๕. การรักษาความปลอดภัยสื่อที่มีข้อมูลบันทึกอยู่

๕.๑ ติดป้ายชื่อไว้ที่สื่ออย่างชัดเจน แสดงชั้นความลับของข้อมูลที่เก็บ หากเป็นกรณีที่รวบรวมเก็บในกล่องหรือหีบห่อให้แสดงไว้ที่กล้องหรือหีบห่อนั้นๆ ด้วย

๕.๒ กำหนดบุคคลที่มีสิทธิ์ใช้งานและระดับการเข้าถึงสื่อบันทึกข้อมูลนั้นๆ

๕.๓ ต้องจัดเก็บไว้ในสถานที่และสภาวะแวดล้อมที่เหมาะสมปลอดภัย

๕.๔ ต้องจัดทำทะเบียนคุมไว้อย่างเป็นระเบียบและครบถ้วนสามารถตรวจสอบได้

๕.๕ กรณีสื่อบันทึกข้อมูลที่มีลักษณะสามารถถอดแยกได้ (Removable Computer Media) ให้ลบข้อมูลหรือทำลายสื่อที่มิได้ใช้งานทิ้งทันทีที่หมดความต้องการใช้งาน

๕.๖ ต้องกำหนดสิทธิ์ของบุคคลที่จะดำเนินการถอดแยกสื่อบันทึกข้อมูล

๕.๗ ในกรณีที่นำเครื่องคอมพิวเตอร์ไปตรวจซ่อม ต้องทำการสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน

๖. การทำลายสื่อบันทึกข้อมูล

การทำลายข้อมูลที่ถูกบันทึกอยู่ใน Disk, Hard Disk, Trumbdrive, External Hard Disk ที่เสื่อมสภาพหมดอายุการใช้งานให้ทุกหน่วยงานในสังกัดใช้โปรแกรม CClenner ในการทำลายข้อมูล ซึ่งเป็นโปรแกรมที่มีมาตรฐานการทำลายข้อมูลแบบ DOD 5220.22 M, NSA และ Gutmann

๗. การบริหารจัดการข้อมูล

๗.๑ การกำหนดชั้นความลับของข้อมูล วิธีปฏิบัติในการจัดเก็บข้อมูลแต่ละประเภทชั้นความลับ และวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ

๗.๒ การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะ ต้องได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น การใช้ SSL การใช้ VPN เป็นต้น

๗.๓ มีมาตรการควบคุมความถูกต้องของข้อมูลที่จัดเก็บ (Storage) นำเข้า (Input) ประมวลผล (Operate) และแสดงผล (Output) นอกจากนี้ในกรณีที่มีการจัดเก็บข้อมูลเดียวกันไว้หลายที่ (Distributed Database) หรือมีการจัดเก็บข้อมูลชุดข้อมูลที่มีความสัมพันธ์กัน ต้องมีการควบคุมให้ข้อมูลมีความถูกต้องครบถ้วนตรงกัน

ส่วนที่ ๔
การควบคุมการเข้าถึงและใช้บริการระบบเครือข่าย
(Network Access Control)

๑. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมป้องกันมิให้ผู้ที่ไม่ได้รับอนุญาตที่ไม่มีอำนาจหน้าที่เกี่ยวข้องในการปฏิบัติหน้าที่เข้าถึง ล่วงรู้ แก้ไข เปลี่ยนแปลงระบบเครือข่ายและการสื่อสารที่สำคัญซึ่งจะทำให้เกิดความเสียหายต่อข้อมูลและระบบเทคโนโลยีสารสนเทศของอ.อ.ป. โดยมีการกำหนดกระบวนการควบคุมการเข้าใช้งานเครือข่าย

๒. กระบวนการควบคุมการเข้าถึงและใช้บริการระบบเครือข่าย

๒.๑ ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบเทคโนโลยีสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

๒.๒ การใช้งานบริการเครือข่าย

๒.๒.๑ ห้ามผู้ใช้งานกระทำการใดๆ เกี่ยวกับข้อมูลที่เป็นการขัดต่อกฎหมายหรือศีลธรรมอันดีแห่งสาธารณะชน โดยผู้ใช้งานรับรองว่าหากมีการกระทำการใดๆ ดังกล่าว ย่อมถือว่าอยู่นอกเหนือความรับผิดชอบของ อ.อ.ป.

๒.๒.๒ อ.อ.ป.ไม่อนุญาตให้ผู้ใช้งานกระทำการใดๆ ที่เข้าข่ายลักษณะเพื่อการค้าหรือการแสวงหาผลกำไรผ่านเครื่องคอมพิวเตอร์และเครือข่าย เช่น การประกาศแจ้งความ การซื้อหรือการจำหน่ายสินค้า การนำข้อมูลไปซื้อขาย การรับบริการค้นหาข้อมูลโดยคิดค่าบริการ การให้บริการโฆษณาสินค้าหรือการเปิดบริการอินเทอร์เน็ตแก่บุคคลทั่วไปหรือแสวงหาผลกำไร

๒.๒.๓ ผู้ใช้งานต้องไม่ละเมิดสิทธิต่อผู้อื่น คือ ผู้ใช้งานจะต้องไม่อ่าน เขียน ลบ เปลี่ยนแปลงหรือแก้ไขใดๆ ในส่วนที่มิใช่ของตนเองโดยไม่ได้รับอนุญาต การบุกรุก (Hack) เข้าสู่บัญชีผู้ใช้งาน (User Account) ของผู้อื่น การเผยแพร่ข้อความใดๆ ที่ก่อให้เกิดความเสียหายเสื่อมเสียแก่ผู้อื่น การใช้ภาษาไม่สุภาพหรือการเขียนข้อความที่ทำให้ผู้อื่นเสียหาย ถือเป็นการละเมิดสิทธิของผู้อื่นทั้งสิ้น ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงฝ่ายเดียว อ.อ.ป.ไม่มีส่วนร่วมรับผิดชอบความเสียดายดังกล่าว

๒.๒.๔ ห้ามมิให้ผู้ใดเข้าใช้งานโดยมิได้รับอนุญาต การบุกรุกหรือพยายามบุกรุกเข้าสู่ระบบถือว่าเป็นการพยายามรุกล้ำเขตหวงห้ามของทางราชการ

๒.๒.๕ อ.อ.ป.ให้บัญชีผู้ใช้งาน (User Account) ที่เป็นการเฉพาะบุคคลเท่านั้น ผู้ใช้งานจะโอนหรือจ่ายแจกสิทธินี้ให้กับผู้อื่นไม่ได้

๒.๒.๖ บัญชีผู้ใช้งาน (User Account) ที่อ.อ.ป.ให้กับผู้ใช้งานนั้น ผู้ใช้งานต้องเป็นผู้รับผิดชอบผลต่างๆ อันอาจจะเกิดมีขึ้น รวมถึงผลเสียหายต่างๆ ที่เกิดจากบัญชีผู้ใช้งาน (User Account) นั้นๆ เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

๒.๓ การยืนยันตัวบุคคลสำหรับผู้ใช้ที่อยู่ภายนอกองค์กร (User Authentication for External Connections) ต้องมีการพิสูจน์ตัวตนสำหรับผู้ใช้งาน โดยต้องแสดงตัวตนด้วยชื่อผู้ใช้ พิสูจน์ยืนยันตัวตนด้วยการใช้รหัสผ่านในการเข้าสู่เครือข่าย

๒.๔ การระบุอุปกรณ์บนเครือข่าย (Equipment Identification in Networks)

๒.๔.๑ ผู้ดูแลระบบมีการเก็บบัญชีการขอเชื่อมต่อเครือข่าย ได้แก่ รายชื่อผู้ขอใช้บริการ รายละเอียดเครื่องคอมพิวเตอร์ที่ขอใช้บริการ IP Address และสถานที่ติดตั้ง

๒.๔.๒ กรณีอุปกรณ์ที่มีการเชื่อมต่อจากเครือข่ายภายนอก ต้องมีการระบุหมายเลขอุปกรณ์ว่าสามารถเข้าเชื่อมต่อกับเครือข่ายภายในได้หรือไม่สามารถเชื่อมต่อได้

๒.๔.๓ อุปกรณ์เครือข่ายต้องสามารถตรวจสอบ IP Address ของทั้งต้นทางและปลายทางได้

๒.๔.๔ ผู้ขอใช้บริการต้องกรอกแบบฟอร์ม “การขอเชื่อมต่อเครือข่าย” โดยดาวน์โหลดผ่านเว็บไซต์อ.อ.ป.อุตสาหกรรมป่าไม้ www.fio.co.th หัวข้อ ดาวน์โหลดแบบฟอร์มต่างๆ

๒.๕ การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection)

๒.๕.๑ ผู้ดูแลระบบต้องกำหนดการเปิด-ปิด พอร์ตของอุปกรณ์เครือข่ายเพื่อควบคุมการเข้าถึงต่อพอร์ตของอุปกรณ์เครือข่ายต่างๆ โดยจะปิดพอร์ตที่เสี่ยงที่ก่อให้เกิดความเสียหายต่อระบบเครือข่าย

๒.๕.๒ บุคคลภายนอกเข้ามาติดต่อหรือเข้ามาดำเนินการใดๆ ในห้องควบคุมระบบคอมพิวเตอร์จะต้องลงชื่ออนุญาตการเข้าออกใน “แบบฟอร์มการเข้า -ออกพื้นที่” ให้ถูกต้องและได้รับการอนุมัติจากหัวหน้าฝ่ายสารสนเทศก่อน ซึ่งจะต้องมีเจ้าหน้าที่อยู่กับบุคคลที่มาติดต่อตลอดเวลา

๒.๕.๓ บุคคลภายนอกเข้ามาดำเนินการบำรุงรักษา บริหารจัดการพอร์ตของอุปกรณ์เครือข่ายหรือจัดการผ่านระบบเครือข่ายต้องได้รับการอนุมัติจากผู้บังคับบัญชาตามลำดับชั้น

๒.๕.๔ ต้องยกเลิกหรือปิดพอร์ตและบริการบนอุปกรณ์เครือข่ายที่ไม่มีความจำเป็นในการใช้งาน

๒.๖ การแบ่งแยกเครือข่าย (Segregation in Networks) มีการระบุเกี่ยวกับการแบ่งแยกเครือข่ายสำหรับกลุ่มผู้ใช้งานต่างๆ โดยพิจารณาถึงความต้องการของผู้ใช้งานในการเข้าถึงระบบเครือข่าย ผลกระทบทางด้านความมั่นคง และระดับความสำคัญของข้อมูลบนเครือข่าย ดังนี้

๒.๖.๑ กลุ่มผู้ใช้งานพนักงานทั่วไป

๒.๖.๒ กลุ่มผู้ใช้งานของระบบเทคโนโลยีสารสนเทศ

๒.๖.๓ กลุ่มผู้ใช้งานบุคคลภายนอก

๒.๗ การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control)

๒.๗.๑ มีการตรวจสอบการเชื่อมต่อเครือข่าย

๒.๗.๒ จำกัดสิทธิ ความสามารถของผู้ใช้ในการเชื่อมต่อเข้าสู่เครือข่าย

๒.๗.๓ ระบุอุปกรณ์ เครื่องมือที่ใช้ควบคุมการเชื่อมต่อเครือข่าย

๒.๗.๔ มีระบบการตรวจจับผู้บุกรุกทั้งในระดับเครือข่าย และระดับเครื่องคอมพิวเตอร์แม่ข่าย

๒.๗.๕ ควบคุมไม่ให้มีการเปิดให้บริการบนเครือข่าย โดยไม่ได้รับอนุญาต

๒.๘ การควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control)

๒.๘.๑ ควบคุมไม่ให้มีการเปิดเผยแผนการใช้หมายเลขเครือข่าย (IP Address)

๒.๘.๒ กำหนดให้มีการแปลงหมายเลขเครือข่าย เพื่อแยกเครือข่ายย่อย

๒.๘.๓ กำหนดมาตรการบังคับใช้เส้นทางเครือข่าย สามารถเชื่อมเครือข่ายปลายทางผ่านช่องทางที่กำหนดไว้ หรือจำกัดสิทธิในการใช้บริการเครือข่าย

ส่วนที่ ๕
การควบคุมการเข้าถึงระบบปฏิบัติการ
(Operating System Access Control)

๑. วัตถุประสงค์

เพื่อให้ผู้ใช้งานได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้ระบบปฏิบัติการ รวมทั้งทำความเข้าใจตลอดจนปฏิบัติตามอย่างเคร่งครัด อันจะเป็นการป้องกันทรัพยากรและข้อมูลของหน่วยงานให้มีความลับความถูกต้องและมีความพร้อมใช้งานอยู่เสมอ

๒. การกำหนดขั้นตอนการปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย

๒.๑ ผู้ใช้งานต้องกำหนดรหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ที่รับผิดชอบ

๒.๒ ผู้ใช้งานต้องตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ (Screen Saver) เพื่อทำการล็อคหน้าจอภาพเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้บริการต้องใส่รหัสผ่าน (Password) เพื่อเข้าใช้งาน

๒.๓ ก่อนการเข้าใช้ระบบปฏิบัติการต้องใส่ User และ Password ทุกครั้ง

๒.๔ ผู้ใช้งานไม่ควรอนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ของหน่วยงานร่วมกัน

๒.๕ ผู้ใช้งานต้องทำการลงบันทึกออก (Logout) ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

๓. การระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication)

๓.๑ การพิสูจน์ตัวตนสำหรับผู้ใช้งาน ผู้ดูแลระบบเทคโนโลยีสารสนเทศต้องให้มีการพิสูจน์ตัวตนสำหรับผู้ใช้งานเป็นรายบุคคลก่อนที่จะอนุญาตให้เข้าใช้งานระบบ

๓.๒ ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนใช้ระบบเทคโนโลยีสารสนเทศ เพื่อป้องกันผู้ไม่มีสิทธิ์เข้าใช้งานระบบเทคโนโลยีสารสนเทศ หากการระบุและยืนยันตัวตนของผู้ใช้งานมีปัญหา หรือเกิดความผิดพลาด ผู้ใช้งานแจ้งให้ผู้ดูแลระบบทำการแก้ไข

๓.๓ ผู้ใช้งานจะต้องเก็บรักษาบัญชีผู้ใช้บริการ (Account) ไว้เป็นความลับและห้ามเปิดเผยต่อบุคคลอื่น ห้ามโอน จำหน่าย หรือจ่ายแจกให้ผู้อื่น โดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

๓.๔ ผู้ใช้งานจะต้องลงบันทึกเข้า (Login) โดยใช้ชื่อบัญชีผู้ใช้บริการ (Account) ของตนเอง และทำการลงบันทึกออก (Logout) ทุกครั้ง เมื่อสิ้นสุดการใช้งานหรือหยุดการใช้งานชั่วคราว

๔. การบริหารจัดการรหัสผ่าน (Password Management System)

๔.๑ การบริหารจัดการรหัสผ่านของผู้ใช้ ผู้ดูแลระบบเทคโนโลยีสารสนเทศต้องบริหารจัดการรหัสผ่านของผู้ใช้ให้มีความมั่นคงปลอดภัย

๔.๒ วิธีการบริหารจัดการรหัสผ่านของผู้ใช้ให้มีความมั่นคงปลอดภัย กำหนดให้รหัสผ่านต้องมีมากกว่าหรือเท่ากับ ๘ ตัวอักษร (โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวพิมพ์ใหญ่ ตัวเลข และสัญลักษณ์เข้าด้วยกัน แต่ไม่ควรกำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเองหรือบุคคลในครอบครัว หรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ใช้ในพจนานุกรม

๔.๓ ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

๔.๔ ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password)

๔.๕ สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่ผู้ใช้ครอบครองอยู่ ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตของบุคคลอื่น ต้องให้ผู้ใช้ลงนามเพื่อเก็บรักษารหัสผ่านทั้งของ

ตนเองและของกลุ่มไว้เป็นความลับ กำหนดรหัสผ่านเริ่มต้นให้กับผู้ใช้ให้ยากต่อการเดาและการส่งมอบรหัสผ่านให้กับผู้ใช้ต้องเป็นไปอย่างปลอดภัย

๔.๖ ควรทำการเปลี่ยนรหัสผ่าน เพื่อใช้งานเครื่องคอมพิวเตอร์ของหน่วยงานทุก ๓ -๖ เดือนหรือเปลี่ยนรหัสผ่านทุกครั้งที่มีสัญญาณบอกเหตุว่าอาจรั่วไหล

๔.๗ การบริหารจัดการรหัสผ่าน ผู้ดูแลระบบเทคโนโลยีสารสนเทศควรมีระบบหรือวิธีการในการตรวจสอบคุณภาพของรหัสผ่านและวิธีการควบคุมดูแลให้ผู้ใช้เปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนด

๔.๘ กระบวนการในการเข้าสู่ระบบให้บริการอย่างมั่นคงปลอดภัย ผู้ดูแลระบบเทคโนโลยีสารสนเทศควรกำหนดกระบวนการในการเข้าสู่ระบบให้บริการ เพื่อใช้งานให้มีความมั่นคงปลอดภัย เช่น กำหนดให้ระบบให้บริการจะปฏิเสธการใช้งาน หากผู้ใช้พิมพ์รหัสผ่านผิดพลาดเกิน ๓ ครั้ง เป็นต้น

๕. การใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities)

การควบคุมการใช้งานโปรแกรมอรรถประโยชน์ ผู้ดูแลระบบกำหนดให้มีการควบคุมการใช้โปรแกรมอรรถประโยชน์สำหรับการเข้าระบบ เพื่อป้องกันการเข้าถึงโดยผู้ที่ไม่ได้รับอนุญาต ได้แก่

๕.๑ มีการพิสูจน์ตัวตนสำหรับผู้ใช้งาน

๕.๑.๑ ต้องแสดงตัวตนสำหรับผู้ใช้งาน

๕.๑.๒ ต้องพิสูจน์ยืนยันตัวตนด้วยการใช้รหัสผ่าน

๕.๒ การติดตั้งโปรแกรมอรรถประโยชน์เพื่อใช้งานร่วมกับระบบปฏิบัติการ

๕.๒.๑ ให้ทำการแยกโปรแกรมอรรถประโยชน์ออกจากโปรแกรมระบบงาน

๕.๒.๒ จำกัดการใช้งานโปรแกรมอรรถประโยชน์ให้เฉพาะผู้ที่ได้รับมอบหมายแล้วเท่านั้น

๕.๒.๓ ให้บันทึกรายละเอียดการเข้าใช้งานโปรแกรมอรรถประโยชน์ เช่น ใครเป็นผู้ใช้งาน

๕.๒.๔ หลีกเลี่ยงการติดตั้งโปรแกรมที่ละเมิดลิขสิทธิ์ ต้องใช้โปรแกรมที่ถูกต้องลิขสิทธิ์เท่านั้น

๕.๒.๕ ต้องติดตั้งโปรแกรมตามภารกิจและไม่ติดตั้งโปรแกรมที่ไม่เกี่ยวข้องกับการปฏิบัติงาน

๕.๓ จำกัดช่วงวันหรือช่วงเวลาในการอนุญาตให้เข้าสู่ระบบปฏิบัติการตามความจำเป็น

๕.๓.๑ จำกัดระยะเวลาการใช้งานระบบปฏิบัติการที่เชื่อมต่อ เช่น ตัดการเชื่อมต่อเมื่อใช้งานได้ระยะหนึ่งซึ่งได้กำหนดไว้ล่วงหน้า จำกัดการเชื่อมต่อระบบปฏิบัติการให้เป็นเฉพาะภายในระยะเวลาทำการ ให้ตรวจสอบยืนยันตัวตนใหม่ทุกช่วงเวลาที่กำหนด

๕.๓.๒ กำหนดการหมดเวลาการใช้งานระบบปฏิบัติการโดยมีกลไกในการยกเลิกการทำงาน เมื่อไม่ได้มีการใช้งานตามระยะเวลาที่กำหนด

๖. เมื่อมีการวางเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบเทคโนโลยีสารสนเทศนั้น (Session time-out)

๖.๑ ต้องกำหนดให้ระบบเทคโนโลยีสารสนเทศมีการตัดเวลาการใช้งานเครื่องลูกข่าย ผู้ดูแลระบบเทคโนโลยีสารสนเทศต้องมีวิธีการตัดเวลาการใช้งานเครื่องลูกข่าย เมื่อเครื่องลูกข่ายนั้นไม่ได้มีการใช้งานเป็นระยะเวลา ๑๐ นาที เช่น กลไกในการล็อคหน้าจอและต้องใช้รหัสผ่านในการเข้าสู่ระบบ

๖.๒ ต้องกำหนดให้ระบบเทคโนโลยีสารสนเทศตัดและหมดเวลาการใช้งานที่สั้นขึ้นสำหรับระบบเทคโนโลยีสารสนเทศหรือแอพพลิเคชั่นที่มีความเสี่ยงหรือมีความสำคัญสูง เช่น ระบบใบเสร็จรับเงิน เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๖.๓ ต้องกำหนดให้ระบบเทคโนโลยีสารสนเทศทำการล้างหน้าจอหลังจากที่ไม่มีกิจกรรมการใช้งานช่วงระยะเวลา ๑๐ นาที เพื่อป้องกันผู้อื่นเห็นข้อมูลบนหน้าจอ

๗. การจำกัดระยะเวลาการเชื่อมต่อระบบเทคโนโลยีสารสนเทศ (Limitation of Connection Time)

๗.๑ ต้องกำหนดให้ระบบเทคโนโลยีสารสนเทศจำกัดระยะเวลาการเชื่อมต่อสำหรับการใช้งานเพื่อให้ผู้ใช้งานสามารถใช้งานได้นานที่สุดภายในระยะเวลาที่กำหนดเท่านั้น โดยกำหนดให้ใช้งานได้ ๑ ชั่วโมงต่อการเชื่อมต่อหนึ่งครั้ง กำหนดให้ใช้งานได้เฉพาะในช่วงเวลาการทำงานของสำนักงานตามปกติเท่านั้น

๗.๒ ต้องกำหนดให้ระบบเทคโนโลยีสารสนเทศ เช่น ระบบงานที่มีความสำคัญสูง ระบบงานที่มีการใช้งานในสถานที่ที่มีความเสี่ยง (ในที่สาธารณะหรือพื้นที่ภายนอกองค์กร) เป็นต้น มีการจำกัดช่วงระยะเวลาการเชื่อมต่อ

๗.๓ ต้องกำหนดให้ระบบเทคโนโลยีสารสนเทศต้องมีการจำกัดช่วงระยะเวลาการใช้งาน มีการระบุและพิสูจน์ตัวตนเพื่อเข้าใช้งานใหม่ตามช่วงระยะเวลาที่กำหนดไว้ทุกๆ ๑ ชั่วโมง

ส่วนที่ ๖
การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ
(Application Information Access Control)

๑. วัตถุประสงค์

กำหนดขึ้นด้วยวัตถุประสงค์เพื่อป้องกันการใช้งานระบบเทคโนโลยีสารสนเทศโดยไม่ได้รับอนุญาต เข้าถึงระบบเทคโนโลยีสารสนเทศของอ.อ.ป. และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุกจาก โปรแกรมชุดคำสั่งไม่พึงประสงค์ที่จะสร้างความเสียหายแก่ข้อมูลหรือการทำงานของระบบเทคโนโลยี สารสนเทศให้หยุดชะงักและทำให้ และทำให้สามารถตรวจสอบติดตามพิสูจน์ตัวตนที่เข้าใช้งานระบบ เทคโนโลยีสารสนเทศของอ.อ.ป.ได้อย่างถูกต้อง

๒. การควบคุมการเข้าถึงสารสนเทศ

๒.๑ ให้สำนักวิจัยพัฒนาและสารสนเทศ กำหนดมาตรการควบคุมการเข้าใช้งานระบบเทคโนโลยี สารสนเทศของทั้งอ.อ.ป. เพื่อดูแลรักษาความปลอดภัย โดยที่บุคคลจากหน่วยงานภายนอกหรือบุคคลภายนอก ที่ต้องการสิทธิ์ในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของอ.อ.ป.จะต้องขออนุญาตจากหัวหน้าฝ่าย สารสนเทศหรือผู้ที่ได้รับมอบหมาย

๒.๒ ผู้ดูแลระบบ (System Administrator) กำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลให้ เหมาะสมกับการเข้าใช้งานของผู้ใช้งานระบบ และหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อน เข้าใช้ระบบเทคโนโลยีสารสนเทศ รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ

๒.๓ ผู้ดูแลระบบ (System Administrator) ควรจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งาน ระบบเทคโนโลยีสารสนเทศของหน่วยงาน และตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบข้อมูล

๒.๔ ผู้ดูแลระบบ (System Administrator) จัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไข เปลี่ยนแปลงสิทธิต่างๆ และการผ่านเข้า-ออกสถานที่ตั้งของระบบ ของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาต เพื่อเป็นหลักฐานในการตรวจสอบ

๓. การบริหารจัดการการเข้าถึงระบบเทคโนโลยีสารสนเทศ

๓.๑ ผู้ดูแลระบบ (System Administrator) กำหนดให้มีการลงทะเบียนบุคลากรใหม่ของอ.อ.ป. ควร กำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการ เพื่อให้มีสิทธิ์ต่างๆ ในการใช้งานตามความจำเป็น รวมทั้งขั้นตอน ปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน เช่น การลาออกหรือการเปลี่ยนตำแหน่งงานภายในอ.อ.ป. เป็นต้น

๓.๒ ผู้ดูแลระบบ (System Administrator) กำหนดให้มีการใช้งานระบบเทคโนโลยีสารสนเทศที่ สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-mail) ระบบ เครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงาน ในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ดังกล่าว อย่างสม่ำเสมอ

๓.๓ ผู้ดูแลระบบ (System Administrator) ต้องบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่านของ บุคลากรดังต่อไปนี้

๓.๓.๑ กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบลาออก หรือพ้นจากตำแหน่งหรือยกเลิกการใช้งาน

๓.๓.๒ ส่งมอบรหัสผ่าน (Password) ชั่วคราวให้กับผู้ใช้บริการด้วยวิธีการที่ปลอดภัย ควรหลีกเลี่ยง การใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (E-mail) ที่ไม่มีการป้องกันในการส่ง รหัสผ่าน (Password)

๓.๓.๓ ควรกำหนดให้ผู้ใช้บริการตอบยืนยันการได้รับรหัสผ่าน (Password)

๓.๓.๔ ควรกำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

๓.๓.๕ กำหนดชื่อผู้ใช้หรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

๓.๓.๖ ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชาโดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว หรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้างและต้องกำหนดให้รหัสผ่านของผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

๓.๔ ผู้ดูแลระบบ (System Administrator) ต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมทั้งวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้

๓.๔.๑ ควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

๓.๔.๒ กำหนดรายชื่อผู้ใช้ (User Name) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล

๓.๔.๓ ควรกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

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

๓.๔.๕ กำหนดการเปลี่ยนรหัสผ่าน (Password) ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

๓.๔.๖ กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของอ.อ.ป. เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

๔. ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อหน่วยงาน ดำเนินการดังนี้

๔.๑ ระบบเครือข่ายของอ.อ.ป. ในลักษณะที่ต้องวางผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกเข้าถึงได้นั้น ต้องให้มีการร้อยท่อสายสัญญาณต่างๆ เพื่อป้องกันการดักจับสัญญาณ การตัดสายสัญญาณเพื่อทำให้เกิดความเสียหายและป้องกันสัตว์ต่างๆ กัดสาย เช่น หนู เป็นต้น

๔.๒ ให้เดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซงรบกวนของสัญญาณซึ่งกันและกัน

๔.๓ จัดทำแผนผังสายสัญญาณสื่อสารต่างๆ ให้ครบถ้วนและถูกต้อง

๔.๔ ตู้ Rack ที่มีสายสัญญาณสื่อสารต่างๆปิดใส่สลักให้สนิท เพื่อป้องกันการเข้าถึงของบุคคลภายนอก

๕. การควบคุมอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอก

การป้องกันข้อมูลและทรัพย์สินด้านสารสนเทศที่อยู่ในเครื่องคอมพิวเตอร์ประเภทพกพาของผู้ใช้งานต้องมีวิธีการป้องกันข้อมูลและทรัพย์สินด้านสารสนเทศที่อยู่ในเครื่องคอมพิวเตอร์ประเภทพกพา (Notebook, Palmtops, Laptop) เช่น เมื่อปฏิบัติงานอยู่นอกสถานที่

๕.๑ ใส่รหัสผ่านป้องกันหน้าจอทุกเครื่อง

๕.๒ ใช้กุญแจล็อคเครื่องคอมพิวเตอร์แบบพกพา

๕.๓ เข้ารหัสข้อมูลที่สำคัญไว้

๖. การควบคุมการเข้าใช้งานระบบจากภายนอก

กำหนดให้มีการควบคุมการใช้งานระบบที่ผู้ดูแลระบบได้ติดตั้งภายในอ.อ.ป. เพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอก โดยมีแนวทางปฏิบัติดังนี้

๖.๑ การเข้าสู่ระบบจากระยะไกล (Remote Access) สู่ระบบเครือข่ายของอ.อ.ป.ต้องควบคุมบุคคลที่จะเข้าสู่ระบบของหน่วยงานจากระยะไกล โดยกำหนดมาตรการการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน

๖.๒ วิธีการใดๆก็ตามที่สามารถเข้าถึงข้อมูลหรือระบบข้อมูลจากระยะไกล ต้องได้รับการอนุมัติจากหัวหน้าฝ่ายสารสนเทศหรือผู้อำนวยการสำนักวิจัยพัฒนาและสารสนเทศ และมีการควบคุมอย่างเข้มงวดก่อนนำมาใช้และผู้ใช้ต้องปฏิบัติตามข้อกำหนดของ อ.อ.ป.ในการเข้าสู่ระบบและข้อมูลอย่างเคร่งครัด

๖.๓ การทำการให้สิทธิในการเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับ อ.อ.ป.อย่างเพียงพอและต้องได้รับการอนุมัติจากผู้มีอำนาจอย่างเป็นทางการ

๖.๔ มีการควบคุม Port ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

๖.๕ การอนุญาตให้ผู้ใช้งานเข้าสู่ระบบข้อมูลจากระยะไกลต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น และไม่ควรเปิด Port ทิ้งไว้โดยไม่มีความจำเป็น ควรตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้วและจะเปิดให้ใช้ได้เมื่อมีการร้องขอที่จำเป็นเท่านั้น

๗. การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)

๗.๑ ต้องมีการกำหนดมาตรการและการเตรียมการต่างๆ ที่จำเป็นก่อน ซึ่งรวมถึงการเตรียมการป้องกันทางกายภาพสำหรับสถานที่ที่จะอนุญาตการปฏิบัติงานของผู้ใช้งานจากระยะไกล ก่อนที่จะอนุญาตให้เริ่มปฏิบัติงานจากระยะไกล

๗.๒ ต้องมีการกำหนดมาตรการที่มีความมั่นคงปลอดภัยสำหรับระบบสื่อสารข้อมูลระหว่างสถานที่ที่จะมีการปฏิบัติงานจากระยะไกลและระบบงานต่างๆ ภายในองค์กร ก่อนที่จะอนุญาตให้เริ่มปฏิบัติงานจากระยะไกล

๗.๓ ต้องกำหนดมาตรการการรักษาความมั่นคงปลอดภัยทางกายภาพสำหรับสถานที่ที่จะมีการปฏิบัติงานของผู้ใช้งานจากระยะไกล (ซึ่งรวมถึงตึก อาคาร สำนักงาน และสิ่งแวดล้อมภายนอก) เพื่อป้องกันการขโมยอุปกรณ์ การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต และการเชื่อมต่อจากระยะไกลโดยผู้ไม่ประสงค์ดี เพื่อเข้าสู่ระบบงานของอ.อ.ป.

๗.๔ ต้องกำหนดให้ผู้ปฏิบัติงานจากระยะไกลไม่อนุญาตให้ครอบครัวหรือเพื่อนของตนเข้าถึงระบบเทคโนโลยีสารสนเทศภายในอ.อ.ป.ในสถานที่ดังกล่าว

๗.๕ ต้องมีการกำหนดมาตรการควบคุมสำหรับการใช้เครือข่ายจากที่บ้านเพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศของอ.อ.ป. รวมทั้งมาตรการควบคุมการใช้บริหารเครือข่ายไร้สายที่บ้าน

๗.๖ ต้องมีการตรวจสอบว่าอุปกรณ์เป็นของส่วนตัวซึ่งใช้ในการเข้าถึงระบบเทคโนโลยีสารสนเทศของอ.อ.ป.จากระยะไกลมีการป้องกันไวรัสและการใช้งานไฟร์วอลล์ตามที่อ.อ.ป.ต้องการ

๗.๗ ต้องมีการจัดเตรียมอุปกรณ์สำหรับการปฏิบัติงานจากระยะไกล การจัดเก็บข้อมูล และอุปกรณ์สื่อสารไว้ให้กับผู้ปฏิบัติงานจากระยะไกล

๗.๘ อ.อ.ป.ไม่อนุญาตให้ใช้งานอุปกรณ์ที่เป็นของส่วนตัวเพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศของอ.อ.ป.จากระยะไกล ถ้าอุปกรณ์ดังกล่าวไม่อยู่ภายใต้การควบคุมหรือดูแลโดยอ.อ.ป.

๗.๙ อ.อ.ป.ต้องกำหนดชนิดของงานที่อนุญาตและไม่อนุญาตให้ทำสำหรับการปฏิบัติงานจากระยะไกลชั่วโมงการทำงานในสถานที่ดังกล่าว ชั้นความลับของข้อมูลที่อนุญาตให้ใช้งานได้ และระบบงานและบริการต่างๆ ของอ.อ.ป.ที่อนุญาตให้เข้าถึงได้จากระยะไกล

๗.๑๐ อ.อ.ป.ต้องกำหนดขั้นตอนปฏิบัติสำหรับการขออนุมัติและการยกเลิกการปฏิบัติงานจากระยะไกล การกำหนดหรือปรับปรุงสิทธิการเข้าถึงระบบงาน และการคืนอุปกรณ์ที่ใช้งานเมื่อมีการยกเลิกการปฏิบัติงาน

ส่วนที่ ๗
การจัดทำระบบสำรองข้อมูล
(Creating a Backup System)

๑. วัตถุประสงค์

เพื่อกำหนดข้อปฏิบัติการสำรองข้อมูลและกู้คืนระบบ โดยมีวัตถุประสงค์เพื่อให้ผู้ดูแลระบบสามารถดำเนินการสำรองข้อมูลได้อย่างถูกต้องและสามารถกู้คืนระบบได้ในกรณีที่จำเป็น

๒. แนวปฏิบัติการสำรองข้อมูลและระบบคอมพิวเตอร์

๒.๑ ผู้ดูแลระบบจัดให้มีการสำรองและทดสอบข้อมูลที่สำรองเก็บไว้อย่างสม่ำเสมออย่างน้อยปีละ ๑ ครั้ง รวมทั้งดำเนินการทดสอบว่าระบบงานทั้งหมดสามารถใช้งานได้หรือไม่

๒.๒ การจัดทำบันทึกการสำรองข้อมูล (Operator Logs) ผู้ดูแลระบบต้องทำบันทึกรายละเอียดการสำรองข้อมูล ได้แก่ เวลาเริ่มต้นและสิ้นสุด ชื่อผู้สำรอง ชนิดของข้อมูลที่บันทึก เป็นต้น

๒.๓ การรายงานข้อผิดพลาด (Fault Logging) ผู้ดูแลระบบต้องทำรายงานข้อผิดพลาดจากการสำรองข้อมูลที่เกิดขึ้น รวมทั้งวิธีการที่ใช้แก้ไขด้วย

๒.๔ ให้ผู้ดูแลระบบมอบหมายหน้าที่การสำรองข้อมูลแก่เจ้าหน้าที่คนอื่นไว้สำรองกรณีที่ผู้ดูแลระบบ / หรือผู้ดูแลระบบเครือข่ายไม่สามารถปฏิบัติงานได้

๒.๕ ในกรณีที่พบปัญหาในการสำรองข้อมูลจนเป็นเหตุไม่สามารถดำเนินการอย่างสมบูรณ์ได้ ให้ดำเนินการแก้ไขปัญหาและสรุปผลการแก้ไขปัญหาและรายงานต่อหัวหน้าฝ่ายสารสนเทศ

๒.๖ ให้ผู้ดูแลระบบกำหนดชนิดและช่วงเวลาการสำรองข้อมูลตามความเหมาะสม พร้อมทั้งกำหนดสื่อที่ใช้เก็บข้อมูล โดยรูปแบบการสำรองข้อมูลมี ๒ ชนิด คือ การสำรองข้อมูลแบบเต็ม (Full Backup) และการสำรองข้อมูลแบบส่วนต่าง (Incremental Backup)

๒.๗ การสำรองข้อมูลภายนอกสำนักงาน (Off-site Backup) ผู้ดูแลระบบจัดให้มีการสำรองข้อมูลภายนอกสำนักงานตามความเหมาะสมของหน่วยงาน เพื่อให้สามารถกู้ระบบกลับคืนได้อย่างรวดเร็ว และเพื่อป้องกันระบบจากการถูกโจมตีหรือความหายนะที่อาจเกิดขึ้น

๒.๘ การเข้ารหัสข้อมูลที่สำคัญในการสำรองข้อมูล (Encrypted Backup) ผู้ดูแลระบบจัดให้มีการเข้ารหัสข้อมูลที่สำรองที่สำคัญ โดยการใช้เทคโนโลยีการเข้ารหัสที่เหมาะสม เพื่อป้องกันมิให้ข้อมูลสำรองเหล่านั้นถูกเปิดเผย

๒.๙ นโยบายที่ต้องปฏิบัติเกี่ยวกับการสำรองข้อมูล (Backup Policy) ผู้ดูแลระบบต้องปฏิบัติตามขั้นตอนปฏิบัติ Backup Procedure โดยเคร่งครัด

๓. การปฏิบัติเกี่ยวกับสำรองข้อมูล

๓.๑ ผู้ดูแลระบบทำการสำรองข้อมูลแต่ละรายการ ตามความถี่ดังนี้

ที่	รายการ	ข้อมูลที่ต้องสำรอง	ความถี่ในการสำรองข้อมูล
๑	Mail Server	ค่า Configure	ก่อนและหลังการเปลี่ยนแปลง
		ข้อมูลใน Mail Box	๑ ครั้งต่อเดือน และนำสื่อบันทึกข้อมูลนั้นไปไว้นอกสถานที่
๒	Web Servers	ค่า Configure	ก่อนและหลังการเปลี่ยนแปลง
		ข้อมูลเผยแพร่บนเว็บไซต์	๑ ครั้งต่อเดือน และนำสื่อบันทึกข้อมูลนั้นไปไว้นอกสถานที่

๓	Database Servers	ค่า Configure	ก่อนและหลังการเปลี่ยนแปลง
			๑ ครั้งต่อเดือน และนำสื่อบันทึกข้อมูลนั้นไปไว้นอกสถานที่
๔	Firewall Servers	ค่า Configure	ก่อนและหลังการเปลี่ยนแปลง
		ข้อมูล Rule ของ Firewall	๑ ครั้งต่อเดือน และนำสื่อบันทึกข้อมูลนั้นไปไว้นอกสถานที่
๕	Server อื่นๆ	ค่า Configure	ก่อนและหลังการเปลี่ยนแปลง
		ข้อมูลบน Server อื่นๆ	๑ ครั้งต่อเดือน และนำสื่อบันทึกข้อมูลนั้นไปไว้นอกสถานที่
หมายเหตุ ทุกรายการที่ปรากฏในตารางจะใช้วิธี Back Up แบบ Full Backup			

๓.๒ ผู้ดูแลระบบควรตรวจสอบผลการสำรองข้อมูลด้วยตนเองว่าการ Back Up ตามรายละเอียดในตารางข้างต้นนั้นถูกต้องสมบูรณ์หรือไม่

๓.๓ กรณีที่สมบูรณ์ ผู้ดูแลระบบนำสื่อบันทึกข้อมูล Back Up ไปเก็บไว้นอกสำนักงานในสถานที่ที่ปลอดภัย

๓.๔ กรณีที่ไม่สมบูรณ์ ผู้ดูแลระบบต้องแก้ไขให้ Back Up สมบูรณ์และกลับไปทำการตรวจสอบทั้งหมดใหม่อีกครั้ง

๔. การกู้คืนระบบ

๔.๑ ในกรณีที่พบปัญหาที่อาจสร้างความเสียหายต่อระบบคอมพิวเตอร์และ /หรือระบบเครือข่ายจนเป็นเหตุทำให้ต้องดำเนินการกู้คืนระบบ ให้ผู้ดูแลระบบและ /หรือผู้ดูแลระบบเครือข่ายดำเนินการแก้ไขรายงานผลการแก้ไขพร้อมทั้งบันทึกและให้รายงานสรุปผลการปฏิบัติงานต่อหัวหน้าฝ่ายสารสนเทศ หรือผู้ที่ได้รับมอบหมายจากหัวหน้าฝ่ายสารสนเทศทราบ

๔.๒ ให้ใช้ข้อมูลทันสมัยที่สุด (Latest Update) ที่ได้สำรองไว้หรือตามความเหมาะสมเพื่อกู้คืนระบบ

๔.๓ หากความเสียหายที่เกิดขึ้นกับระบบคอมพิวเตอร์ หรือระบบเครือข่ายกระทบต่อการให้บริการหรือการใช้งานของผู้ใช้ระบบ ให้แจ้งผู้ใช้งานทราบทันที พร้อมทั้งรายงานความคืบหน้าการกู้คืนระบบเป็นระยะจนกว่าจะดำเนินการเสร็จสิ้นอย่างสมบูรณ์

๕. การจัดทำแผนเตรียมพร้อมกรณีฉุกเฉิน

การจัดทำแผนเตรียมพร้อมกรณีฉุกเฉิน (Continuity Management Policy) คณะกรรมการด้านเทคโนโลยีสารสนเทศและการสื่อสารขององค์กรต้องมอบหมายให้บุคลากรที่เกี่ยวข้องดำเนินการดังต่อไปนี้

๕.๑ กำหนดกระบวนการในการวางแผนรับมือกับเหตุภัยพิบัติสำหรับระบบที่มีความสำคัญสูง

๕.๒ กำหนดชนิดของภัยพิบัติที่มีผลต่อระบบที่มีความสำคัญสูงและจำเป็นต้องวางแผนรับมือ

๕.๓ ทำการประเมินความเสี่ยงที่มีผลทำให้ระบบที่มีความสำคัญสูง ติดขัดหรือไม่สามารถใช้งานได้อันเป็นผลมาจากภัยพิบัติที่กำหนดไว้

๕.๔ จัดทำแผนรับมือกับเหตุภัยพิบัติสำหรับระบบที่มีความสำคัญสูง

๕.๕ ทดสอบ /ประเมินและปรับปรุงแผนรับมือกับเหตุภัยพิบัติสำหรับระบบที่มีความสำคัญสูงอย่างน้อยปีละ ๑ ครั้ง

ส่วนที่ ๘
การตรวจสอบและประเมินความเสี่ยง
(Monitoring and Risk Assessment)

๑. วัตถุประสงค์

เพื่อแยกแยะและเตรียมความพร้อมภัยคุกคามใดๆ ที่จะส่งผลกระทบกับความมั่นคงปลอดภัยกับระบบเทคโนโลยีสารสนเทศของ อ.อ.ป. จึงจัดให้มีการตรวจสอบและประเมินความเสี่ยงต่อทรัพยากรสารสนเทศ เพื่อสร้างความมั่นใจว่าทรัพยากรสารสนเทศได้รับการปกป้องให้มีความมั่นคงปลอดภัยเพียงพอและมีประสิทธิภาพ ทรัพยากรสารสนเทศที่มีความเสี่ยงต่อภัยคุกคามสามารถลดหรือกำจัดได้

๒. แนวทางในการประเมินความเสี่ยง

๒.๑ กระบวนการในการบริหารจัดการกับความเสี่ยงของระบบฐานข้อมูลและสารสนเทศให้ปฏิบัติตามกระบวนการ PDCA ดังต่อไปนี้

๒.๑.๑ การกำหนดระบบบริหารจัดการความมั่นคงปลอดภัย (Plan)

- กำหนดขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัย โดยพิจารณาจากลักษณะการดำเนินงานของหน่วยงาน สถานที่ตั้ง ทรัพย์สิน และเทคโนโลยีที่หน่วยงานใช้งาน
- กำหนดนโยบายความมั่นคงปลอดภัยเพื่อให้ครอบคลุมตามขอบเขตที่กำหนดไว้
- กำหนดขั้นตอนปฏิบัติสำหรับการบริหารจัดการความเสี่ยงสำหรับทรัพย์สินสารสนเทศของหน่วยงาน
- ประเมินความเสี่ยง กำหนดทางเลือกในการจัดการกับความเสี่ยง และกำหนดมาตรการลดความเสี่ยง (ซึ่งสามารถนำมาตรการต่างๆ ในมาตรฐาน ISO/IEC ๒๗๐๐๑ มาใช้ในการลดความเสี่ยง)
- นำเสนอภาพความเสี่ยงโดยรวม และขออนุมัติสำหรับความเสี่ยงที่ยังหลงเหลืออยู่
- จัดทำเอกสาร Statement of Applicability

๒.๑.๒ การดำเนินการกับระบบบริหารจัดการความมั่นคงปลอดภัย (Do)

- จัดทำแผนการลดความเสี่ยง
- ปฏิบัติตามแผนการลดความเสี่ยงที่ได้กำหนดไว้
- กำหนดแผนการวัดความสัมฤทธิ์ผลของระบบบริหารจัดการความมั่นคงปลอดภัย เพื่อใช้ในการติดตามภาพรวมของการบริหารจัดการความมั่นคงปลอดภัยของหน่วยงาน
- จัดทำและดำเนินการตามแผนการอบรม และสร้างความตระหนักเพื่อให้ความรู้และสร้างความตระหนักแก่บุคลากรทั้งหมดที่อยู่ในขอบเขตเพื่อให้สามารถปฏิบัติหน้าที่ได้อย่างมีประสิทธิภาพ ประสิทธิผล รวมทั้งมีความมั่นคงปลอดภัย
- บริหารจัดการการดำเนินงานและการใช้ทรัพยากรต่างๆ ภายในขอบเขตเพื่อให้เป็นไปตามนโยบายความมั่นคงปลอดภัยของหน่วยงาน
- จัดทำขั้นตอนปฏิบัติ และ /หรือ กำหนดมาตรการที่จำเป็นสำหรับการติดตาม และบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย (Security Incident Management Procedures and controls) รวมทั้งกำหนดให้ผู้ที่เกี่ยวข้องให้ปฏิบัติตามโดยเคร่งครัด

๒.๑.๓ การเฝ้าระวังและทบทวนระบบบริหารจัดการความมั่นคงปลอดภัย (Check)

- ดำเนินการตามขั้นตอนปฏิบัติและมาตรการในการเฝ้าระวังและติดตาม (ที่กำหนดไว้ในนโยบายความมั่นคงปลอดภัย) เพื่อตรวจหาข้อผิดพลาดจากการประมวลผล, ตรวจหา

การละเมิดหรือความพยายามในการละเมิดความมั่นคงปลอดภัย, ตรวจหาเหตุการณ์ด้านความมั่นคงปลอดภัยที่เกิดขึ้น, ตรวจสอบว่าการดำเนินการจัดการกับเหตุการณ์การละเมิดความมั่นคงปลอดภัยที่ได้ดำเนินการไปแล้วได้ผลหรือไม่ เป็นต้น

- ดำเนินการทบทวนระบบบริหารจัดการความมั่นคงปลอดภัยอย่างสม่ำเสมอโดยอย่างน้อยนำสิ่งต่างๆ ดังนี้มาทบทวนด้วย เช่น ผลการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย, เหตุการณ์ด้านความมั่นคงปลอดภัยที่เกิดขึ้น, ผลจากการวัดความสัมฤทธิ์ผลของระบบบริหารจัดการความมั่นคงปลอดภัย, คำแนะนำและผลตอบกลับ (Feedback) จากผู้ที่เกี่ยวข้อง
- ดำเนินการทบทวนความสัมฤทธิ์ผลของระบบบริหารจัดการความมั่นคงปลอดภัยอย่างสม่ำเสมอโดยดูว่าแผนการวัดความสัมฤทธิ์ผลฯ เป็นไปตามเป้าหมายหรือตัวชี้วัดที่กำหนดไว้ในแผนหรือไม่
- ทบทวนผลการประเมินความเสี่ยงเป็นระยะๆ (เช่น ทุกๆ ๓-๖ เดือน) ทบทวนระดับความเสี่ยงที่ยังคงเหลืออยู่ และระดับความเสี่ยงที่ยอมรับได้ ตามการเปลี่ยนแปลงต่างๆ ที่เกิดขึ้นกับหน่วยงาน, เทคโนโลยีที่กรมใช้งาน, วัตถุประสงค์และกระบวนการทางธุรกิจของหน่วยงาน, ภัยคุกคามที่มีการระบุเพิ่มเติมหรือเปลี่ยนแปลง, ความสัมฤทธิ์ผลของมาตรการต่างๆ ที่หน่วยงานใช้งาน, เหตุการณ์ภายนอกต่างๆ เช่น การเปลี่ยนแปลงด้านกฎหมาย ระเบียบ ข้อบังคับ หรือสิ่งที่อยู่ในสัญญาจ้าง และการเปลี่ยนแปลงด้านสังคม เป็นต้น
- ดำเนินการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัยตามรอบระยะเวลาที่ได้กำหนดไว้
- บันทึกข้อมูลการดำเนินการและเหตุการณ์ต่างๆ ซึ่งอาจมีผลกระทบต่อความสัมฤทธิ์ผลหรือประสิทธิภาพของระบบบริหารจัดการความมั่นคงปลอดภัย ซึ่งประกอบด้วย การประชุมทบทวนด้านความมั่นคงปลอดภัยโดยผู้บริหาร ให้จัดทำรายงานการประชุมและแจ้งเวียนมติให้ผู้ที่เกี่ยวข้องได้รับทราบและปฏิบัติตาม การปฏิบัติตามนโยบายและขั้นตอนปฏิบัติต่างๆ ในนโยบายความมั่นคงปลอดภัยของหน่วยงาน ให้ผู้รับผิดชอบบันทึกหลักฐานการปฏิบัติตามนโยบายและขั้นตอนปฏิบัติเหล่านั้นไว้เพื่อให้สามารถตรวจสอบได้ในภายหลัง

๒.๑.๔ การทบทวนและปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัย (Act)

- ปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัยตามผลของการเฝ้าระวัง ติดตามและทบทวนระบบบริหารจัดการความมั่นคงปลอดภัย เช่น การปฏิบัติตามมติการประชุมทบทวนโดยผู้บริหาร การปรับปรุงนโยบายความมั่นคงปลอดภัย การจัดการหรือแก้ไขความไม่สอดคล้องกับนโยบายความมั่นคงปลอดภัย การกำหนดมาตรการเพิ่มเติมเพื่อลดการเกิดขึ้นของเหตุการณ์ด้านความมั่นคงปลอดภัยที่เคยเกิดขึ้นแล้ว การปฏิบัติตามแผนการลดความเสี่ยง การปฏิบัติตามแผนด้านความมั่นคงปลอดภัย การปฏิบัติตามคำแนะนำและผลตอบกลับจากผู้ที่เกี่ยวข้อง เป็นต้น
- แจ้งการปรับปรุงและการดำเนินการให้แก่ทุกหน่วยงานที่เกี่ยวข้องทราบ โดยให้รายละเอียดที่เพียงพอและเหมาะสมตรวจสอบว่าการปรับปรุงที่ได้ดำเนินการไปแล้วนั้นบรรลุผลตามที่ต้องการหรือไม่

๒.๒ การวางแผนระบบบริหารความเสี่ยงของระบบฐานข้อมูลและสารสนเทศ ต้องดำเนินการดังต่อไปนี้

๒.๒.๑ มีการบริหารความเสี่ยงเพื่อกำจัด ป้องกันหรือลดการเกิดความเสียหายในรูปแบบต่างๆ โดยสามารถฟื้นฟูระบบเทคโนโลยีสารสนเทศ และการสำรองและกู้คืนข้อมูลจากความเสียหาย (Backup and Recovery)

๒.๒.๒ มีการจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจจะเกิดกับระบบเทคโนโลยีสารสนเทศ (IT Contingency Plan)

๒.๒.๓ มีระบบการรักษาความมั่นคงปลอดภัย (Security) ของระบบฐานข้อมูล เช่น ระบบ Anti-Virus ระบบไฟฟ้าสำรอง เป็นต้น

๒.๒.๔ มีการกำหนดสิทธิให้ผู้ใช้ในแต่ละระดับ (Access Rights)

๒.๓ ตรวจสอบความเสี่ยงและประเมินความเสี่ยงด้านสารสนเทศที่อาจรุนแรงส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศนั้น ซึ่งกำหนดตรวจสอบและประเมินความเสี่ยงอย่างน้อยปีละ ๑ ครั้ง

๒.๔ ในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ผู้ตรวจสอบจากสำนักตรวจสอบภายในเป็นผู้ตรวจสอบความเสี่ยง เพื่อให้หน่วยงานของรัฐได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศของหน่วยงาน

๒.๕ ต้องมีการตรวจสอบและประเมินความเสี่ยงของระบบฐานข้อมูลและสารสนเทศเป็นประจำทุกปี โดยผู้ตรวจสอบจากสำนักตรวจสอบภายใน อ.อ.ป.อุตสาหกรรมป่าไม้ เป็นผู้ตรวจสอบ โดยใช้เกณฑ์คุณภาพการบริหารจัดการภาครัฐ (PMQA) ของสำนักงาน กพร. ในส่วนของ หมวด ๔ การวิเคราะห์และการจัดการความรู้ หัวข้อ IT ๖ ส่วนราชการต้องมีระบบบริหารความเสี่ยงของระบบฐานข้อมูลและสารสนเทศ กำหนดให้หน่วยงานต้องดำเนินการ ดังนี้

๒.๕.๑ แสดงการทบทวนนโยบายความมั่นคง

๒.๕.๒ แสดงผลการจัดทำนโยบายความมั่นคงปลอดภัยของอ.อ.ป.อย่างเป็นลายลักษณ์อักษร โดย CIO หรือ CEO เป็นผู้อนุมัติ

๒.๕.๓ แสดงผลการกำหนดหน้าที่ความรับผิดชอบของข้าราชการในการดำเนินงานทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศอ.อ.ป.

๒.๕.๔ แสดงระบบเทคโนโลยีสารสนเทศที่มีทั้งหมดในอ.อ.ป.

๒.๕.๕ แสดงระบบรักษาความมั่นคงและปลอดภัย(Security) ของระบบฐานข้อมูลและสารสนเทศ

๒.๕.๖ แสดงรายละเอียดแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจจะเกิดกับระบบฐานข้อมูลและสารสนเทศ (IT Contingency Plan)

๒.๕.๗ แสดงผลการปฏิบัติตามแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจจะเกิดกับระบบฐานข้อมูลและสารสนเทศ (IT Contingency Plan)

๒.๕.๘ แสดง Access Rights ที่ถูกต้องและทันสมัยได้อย่างน้อย ๑ ระบบ

ส่วนที่ ๙
การควบคุมการเข้าออกห้องควบคุมระบบคอมพิวเตอร์และการป้องกันความเสียหาย
(Computing System Control Room and Physical Security)

๑. วัตถุประสงค์

เพื่อการกำหนดมาตรการและแนวทางในการป้องกันอาคารและอุปกรณ์ในการสร้างห้องควบคุมระบบคอมพิวเตอร์และมาตรการในการใช้ห้องควบคุมระบบคอมพิวเตอร์ การควบคุมการเข้าออก การแบ่งสัดส่วนพื้นที่ และการกำหนดสิทธิผู้ผ่านเข้าออก

๒. การจัดแบ่งพื้นที่

๒.๑ ห้องควบคุมระบบแบ่งเป็นสองพื้นที่ ได้แก่ พื้นที่ควบคุม (Control Area) และพื้นที่จำกัดการเข้าถึง (Restricted Area)

๒.๒ พื้นที่ควบคุมเป็นพื้นที่ที่จัดไว้สำหรับการเยี่ยมชมหรือสังเกตการณ์ระบบ ส่วนพื้นที่จำกัดการเข้าถึงเป็นห้องที่มีระบบคอมพิวเตอร์และเครือข่ายติดตั้งอยู่

๓. การควบคุมการเข้าออก

๓.๑ ข้อปฏิบัติการเข้าไปในพื้นที่ควบคุม

๓.๑.๑ ไม่อนุญาตให้บุคคลใดเข้าไปในพื้นที่ควบคุม ยกเว้นเจ้าหน้าที่ห้องควบคุมระบบผู้บริหาร อ.อ.ป.หรือบุคคลที่ผู้บริหารอ.อ.ป.นำเข้าเยี่ยมชม

๓.๑.๒ บุคคลอื่นที่มีความจำเป็นในการปฏิบัติงานหรือการเข้าเยี่ยมชมในพื้นที่ควบคุม ต้องได้รับอนุญาตจากหัวหน้าฝ่ายสารสนเทศ และจะต้องมีเจ้าหน้าที่นำเยี่ยมชมอยู่ด้วยตลอดเวลา

๓.๑.๓ ในกรณีที่มีความจำเป็นเร่งด่วนหรือเหตุการณ์ฉุกเฉินอันอาจเป็นผลทำให้เกิดความเสียหายต่อทรัพย์สินของอ.อ.ป.จะอนุญาตให้เข้าไปในพื้นที่ควบคุมได้ โดยได้รับความเห็นชอบจากหัวหน้าฝ่ายสารสนเทศ

๓.๑.๔ ไม่อนุญาตให้นำอาหารหรือเครื่องดื่มเข้าไปในเขตพื้นที่ควบคุม

๓.๒ ข้อปฏิบัติการเข้าไปในพื้นที่จำกัดการเข้าถึง

๓.๒.๑ ไม่อนุญาตให้บุคคลใดเข้าไปในพื้นที่จำกัดการเข้าถึง ยกเว้นเจ้าหน้าที่ห้องควบคุมร

๓.๒.๒ หรือในกรณีที่บุคคลอื่นที่มีความจำเป็นเข้าไปปฏิบัติงานต้องได้รับอนุญาตจากหัวหน้าฝ่ายสารสนเทศ และจะต้องมีเจ้าหน้าที่รับผิดชอบอย่างน้อย ๑ คน เข้าไปร่วมปฏิบัติงานและประสานงานด้วยทุกครั้ง และให้บันทึกกิจกรรมการปฏิบัติงานทุกครั้ง

๓.๒.๓ หรือบุคคลที่ได้รับคำสั่งจากผู้บริหารให้เข้าปฏิบัติหน้าที่ในพื้นที่ควบคุมซึ่งต้องมีเจ้าหน้าที่รับผิดชอบอย่างน้อย ๑ คน เข้าไปร่วมปฏิบัติงานและประสานงานด้วยทุกครั้ง และให้บันทึกกิจกรรมการปฏิบัติงานทุกครั้ง

๓.๒.๔ ไม่อนุญาตให้บุคคลที่มีอายุต่ำกว่า ๑๕ ปี เข้าไปในพื้นที่จำกัดการเข้าถึง

๓.๒.๕ ไม่อนุญาตให้นำอาหารหรือเครื่องดื่มเข้าไปในพื้นที่จำกัดการเข้าถึง

๓.๒.๖ ไม่อนุญาตให้มีการเข้าเยี่ยมชมในพื้นที่จำกัดการเข้าถึง

๓.๒.๗ ในกรณีที่มีความจำเป็นเร่งด่วนหรือเหตุการณ์ฉุกเฉินอันอาจเป็นผลทำให้เกิดความเสียหายต่อทรัพย์สินจะอนุญาตให้เข้าไปในพื้นที่จำกัดการเข้าถึงได้โดยได้รับความเห็นชอบจากหัวหน้าฝ่ายสารสนเทศ

๔. การป้องกันความเสียหาย

๔.๑ ห้องควบคุมระบบคอมพิวเตอร์

๔.๑.๑ แยกอุปกรณ์ที่มีความสำคัญมากออกจากอุปกรณ์ที่ใช้งานทั่วไป โดยกำหนดลำดับความสำคัญของอุปกรณ์แต่ละชนิดไว้ เช่น Router, Switch, Server ฯลฯ

๔.๑.๒ จัดหา Rack ในการจัดเก็บอุปกรณ์ต่างๆ ที่เหมาะสมเพื่อสะดวกในการบำรุงรักษา

๔.๑.๓ ตำแหน่งของการวางอุปกรณ์ต่างๆ ไม่ควรวางใกล้ประตู หน้าต่าง เพื่อป้องกันอุบัติเหตุที่อาจเกิดขึ้น ไม่ควรวางอุปกรณ์ให้เครื่องปรับอากาศเป่าถูกโดยตรง เพื่อหลีกเลี่ยงความชื้น

๔.๑.๔ การจัดวางสาย Cable Network สายไฟฟ้าควรมีการเก็บสายให้เรียบร้อย เพื่อป้องกันการเดินสะดุด

๔.๑.๕ ติดประกาศบันทึกการบำรุงรักษา ชื่อและหมายเลขโทรศัพท์ของผู้ดูแลรับผิดชอบอุปกรณ์แต่ละชนิด

๔.๑.๖ ติดตั้งระบบรักษาความปลอดภัยในห้อง เช่น กล้อง CCTV ระบบการเข้าออกห้อง โดยระบบ Fingerprint Scan หรือ RFID เป็นต้น

๔.๒ ระบบป้องกันไฟไหม้

๔.๒.๑ ติดตั้งฉนวนกันไฟไหม้ที่ฝ้าเพดานและผนังกำแพง

๔.๒.๒ ต้องมีอุปกรณ์เตือนไฟไหม้ เช่น เครื่องตรวจจับควัน เครื่องตรวจจับความร้อน เป็นต้น เพื่อป้องกันหรือระงับเหตุไฟไหม้ได้ทันเวลา

๔.๒.๓ ห้องควบคุมระบบคอมพิวเตอร์ต้องมีระบบดับเพลิงอัตโนมัติ อย่างน้อยต้องมีถังดับเพลิงเพื่อใช้สำหรับการดับเพลิงในเบื้องต้น

๔.๓ ระบบป้องกันไฟฟ้าขัดข้อง

๔.๓.๑ มีระบบไฟฟ้าสำรองเพื่อป้องกันไฟฟ้าดับ เช่น ติดตั้งระบบเครื่องกำเนิดไฟฟ้าอัตโนมัติและระบบไฟฟ้าสำรอง เป็นต้น

๔.๓.๒ มีระบบป้องกันไฟฟ้าจากฟ้าผ่า

๔.๔ ระบบคอมคุมอุณหภูมิและความชื้น

๔.๔.๑ ควรตั้งอุณหภูมิเครื่องปรับอากาศและตั้งค่าความชื้นให้เหมาะสมกับคุณลักษณะ (Specification) ของระบบคอมพิวเตอร์ เนื่องจากระบบคอมพิวเตอร์อาจทำงานผิดปกติภายใต้สภาวะอุณหภูมิหรือความชื้นที่ไม่เหมาะสม

๔.๔.๒ ระบบปรับอากาศแบบควบคุมอุณหภูมิ (๕๐-๘๐ F) และความชื้น (๕๐-๘๐ %)

๔.๕ ระบบเตือนภัยน้ำรั่ว

ในกรณีที่มีการยกระดับพื้นของห้องควบคุมระบบคอมพิวเตอร์ เพื่อติดตั้งระบบปรับอากาศ รวมทั้งเดินสายไฟและสายเครือข่ายด้านล่าง ควรติดตั้งระบบเตือนภัยน้ำรั่วบริเวณที่มีท่อน้ำเพื่อป้องกันหรือระงับเหตุน้ำรั่วได้ทันเวลา นอกจากนี้ หากห้องควบคุมระบบคอมพิวเตอร์ตั้งอยู่ในสถานที่ที่มีความเสียต่อภัยน้ำรั่ว ควรหมั่นสังเกตว่ามีน้ำรั่วหรือไม่อย่างสม่ำเสมอ

๕. ข้อปฏิบัติการบำรุงรักษาห้องควบคุมระบบและระบบเครือข่าย

๕.๑ ตรวจสอบความพร้อมของระบบรักษาความปลอดภัยทุก ๓ เดือน

๕.๒ ร่างขั้นตอนแผนการดำเนินงานเมื่อเกิดกรณีฉุกเฉิน เช่น ไฟไหม้ หรือมีผู้บุกรุก เป็นต้น

๕.๓ มีการซ้อมการปฏิบัติงานเมื่อเกิดกรณีฉุกเฉินทุก ๖ เดือน

๕.๔ มีตารางการเข้าบำรุงรักษาอุปกรณ์ชัดเจน

ส่วนที่ ๑๐
การใช้งานคอมพิวเตอร์ส่วนบุคคล
(Using a Personal Computer)

การใช้งานเครื่องคอมพิวเตอร์ภายในหน่วยงานมีอยู่ในหลายหน่วยงานมีการเชื่อมต่อเครือข่ายภายในและภายนอกในระบบเครือข่ายแบบอินทราเน็ตและเครือข่ายอินเทอร์เน็ต ซึ่งอาจมีการติดไวรัสคอมพิวเตอร์หรือ malware ต่างๆ เครื่องคอมพิวเตอร์เหล่านี้อาจถูกโจมตีและเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต เพื่อให้การทำงานเป็นไปอย่างมีประสิทธิภาพ จึงต้องมีการกำหนดนโยบายการใช้คอมพิวเตอร์ส่วนบุคคล เพื่อให้มีความเข้าใจที่ตรงกันเกี่ยวกับการใช้งานคอมพิวเตอร์ส่วนบุคคลภายในหน่วยงาน

๑. วัตถุประสงค์

เพื่อให้มีการจัดการด้านความมั่นคงเป็นไปอย่างมีระบบ มีแบบแผนและสามารถจัดการแก้ปัญหาความปลอดภัยที่อาจจะเกิดขึ้นได้อย่างรวดเร็ว

๒. การจัดลำดับชั้นความมั่นคงของคอมพิวเตอร์ส่วนบุคคล คอมพิวเตอร์ส่วนบุคคล ลำดับชั้นความมั่นคงของคอมพิวเตอร์ส่วนบุคคลแบ่งเป็น ๓ ระดับ คือ ระดับที่ ๑ (ความมั่นคงสูงมาก) ระดับที่ ๒ (ความมั่นคงสูง) และระดับที่ ๓ (ความมั่นคงปกติ)

๒.๑ ระดับที่ ๑ (ความมั่นคงสูงมาก) คือ เครื่องคอมพิวเตอร์ส่วนบุคคลที่ใช้ปฏิบัติงานและมีการจัดเก็บบันทึกข้อมูลที่มีความสำคัญ หากข้อมูลเสียหายจะส่งผลกระทบต่อการดำเนินงานของอ.อ.ป. ได้แก่ เครื่องคอมพิวเตอร์ด้านการเงิน การบัญชี งานบุคคล งานสารบรรณและงานพัสดุหรืองานอื่นใดที่จะกำหนดเพิ่มเติมในภายหลัง

๒.๒ ระดับที่ ๒ (ความมั่นคงสูง) คือ เครื่องคอมพิวเตอร์ส่วนบุคคลที่ปฏิบัติงานเฉพาะด้าน เป็นเครื่องที่ใช้สำหรับการทดสอบงาน ได้แก่ เครื่องคอมพิวเตอร์ที่ใช้พัฒนาโปรแกรมดูระบบคอมพิวเตอร์และเครือข่ายและเครื่องคอมพิวเตอร์ของผู้บริหาร

๒.๓ ระดับที่ ๓ (ความมั่นคงปกติ) คือ เครื่องคอมพิวเตอร์ส่วนบุคคลที่ใช้ปฏิบัติงานทั่วไปและเครื่องคอมพิวเตอร์ให้บริการรวมถึงเครื่องคอมพิวเตอร์ส่วนบุคคล

๓. ข้อกำหนดด้านความมั่นคง

๓.๑ เครื่องคอมพิวเตอร์ส่วนบุคคลทุกเครื่องต้องมีรหัสผ่านประจำเครื่องสำหรับผู้ใช้งานและรหัสผ่านของผู้ดูแลระบบ

๓.๒ เครื่องคอมพิวเตอร์ส่วนบุคคลทุกเครื่องต้องมีการลงโปรแกรม Antivirus, Antispyware และ Firewall เป็นไปตามข้อกำหนดของฝ่ายสารสนเทศ

๓.๓ เครื่องคอมพิวเตอร์ส่วนบุคคลทุกเครื่องควรมีการป้องกันโดยใช้ Password ในระดับ BIOS เพื่อป้องกันการแก้ไขค่าติดตั้งเบื้องต้นประจำเครื่อง

๓.๔ เครื่องคอมพิวเตอร์ส่วนบุคคลทุกเครื่องควรลงโปรแกรมการบริหารการจัดการเครื่องคอมพิวเตอร์เพื่อป้องกันการติดตั้งโปรแกรมหรือการแก้ไขค่าติดตั้งประจำเครื่อง เช่น IP Address หรือเปลี่ยนแปลงสิทธิการใช้เครื่อง เป็นต้น

๓.๕ เครื่องคอมพิวเตอร์ส่วนบุคคลทุกเครื่องควรติดตั้งระบบพักหน้าจอ (Screen Saver) โดยกำหนดรหัสในการเข้าใช้

๓.๖ ห้ามผู้ใช้ที่ไม่ได้รับอนุญาตใช้งานคอมพิวเตอร์ที่มีความมั่นคงระดับที่ ๑ โดยเด็ดขาด หากมีความจำเป็นให้ผู้ใช้อื่นปฏิบัติงาน ผู้ใช้ประจำเครื่องจะต้องได้รับอนุญาตและเฝ้าระวังในระหว่างการใช้งาน

๓.๗ การเข้าถึงข้อมูลจะถูกจำกัดโดยผู้ดูแลระบบ ห้ามมิให้ผู้ใช้งานเข้าถึงข้อมูลที่ไม่ได้รับอนุญาต

๓.๘ การรักษาความลับของข้อมูลในเครื่องคอมพิวเตอร์จะเป็นความรับผิดชอบของผู้ใช้งานประจำเครื่องคอมพิวเตอร์นั้น

๓.๙ ห้ามนำเครื่องคอมพิวเตอร์ส่วนตัวมาใช้งานในความมั่นคงระดับที่ ๑

๓.๑๐ การใช้งานเครื่องคอมพิวเตอร์ส่วนตัวควรมีการดำเนินการตามข้อ ๕.๑ -๕.๕ เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นในระบบส่วนรวม

๔. ข้อปฏิบัติ

๔.๑ ข้อปฏิบัติการใช้งานสำหรับผู้ใช้

๔.๑.๑ ห้ามมิให้มีการเปิดระบบแชร์แฟ้มข้อมูลหรือโฟลเดอร์ระหว่างเครื่องคอมพิวเตอร์ส่วนบุคคล ยกเว้นได้รับอนุญาตจากผู้ดูแลระบบเป็นรายกรณี

๔.๑.๒ หากเครื่องคอมพิวเตอร์ส่วนบุคคลไม่สามารถทำงานได้ตามปกติ ผู้ใช้งานสามารถแจ้งผู้ดูแลระบบเพื่อแก้ปัญหาได้ ห้ามมิให้ผู้ใช้งานติดตั้ง ปรับแก้ และเปลี่ยนแปลง Hardware/Software ด้วยตนเอง ยกเว้นได้รับอนุญาตจากผู้ดูแลระบบเป็นรายกรณี

๔.๑.๓ ห้ามทำงานอื่นที่ไม่ได้รับมอบหมายในเครื่องที่มีความมั่นคงระดับ ๑

๔.๑.๔ ผู้ใช้งานต้องปฏิบัติตามคำแนะนำเมื่อผู้ดูแลระบบแจ้งให้เปลี่ยนรหัสผ่าน

๔.๑.๕ ไม่เปิดอ่าน E-Mail ที่ไม่มั่นใจว่าผู้ส่งเป็นผู้ใด เนื่องจากอาจมีโปรแกรมไวรัสคอมพิวเตอร์และโปรแกรมประเภท Malware ต่างๆ ติดมาพร้อมกับ E-Mail

๔.๑.๖ ห้ามติดตั้ง Software อื่นใดที่ไม่เกี่ยวข้องกับการทำงาน

๔.๑.๗ การติดตั้ง Software ที่ไม่เกี่ยวข้องกับการทำงานโดยตรงให้ติดต่อผู้ดูแลระบบ

๔.๑.๘ ตรวจสอบเครื่องคอมพิวเตอร์ว่ามีโปรแกรมไวรัสคอมพิวเตอร์หรือโปรแกรมประเภท Malware ในเครื่องหรือไม่

๔.๑.๙ ผู้ใช้งานประจำเครื่องมีหน้าที่สำรองข้อมูล และบำรุงรักษาเครื่องคอมพิวเตอร์ตามระยะเวลาที่กำหนด

๔.๑.๙.๑ เครื่องคอมพิวเตอร์ที่มีความมั่นคงระดับที่ ๑ ให้สำรองข้อมูลทุกวันโดยคำแนะนำจากผู้ดูแลระบบ

๔.๑.๙.๒ เครื่องคอมพิวเตอร์ที่มีความมั่นคงระดับที่ ๒ และ ๓ ให้สำรองข้อมูลทุกเดือน

๔.๑.๑๐ ในกรณีที่ข้อมูลเกิดความเสียหาย ให้ผู้ใช้งานประจำเครื่องกู้ข้อมูลตามคำแนะนำของผู้ดูแลระบบ ทั้งนี้หากเป็นเครื่องคอมพิวเตอร์ส่วนบุคคลที่มีความมั่นคงระดับที่ ๑ จะต้องดำเนินการโดยผู้ดูแลระบบ

๔.๑.๑๑ รายงานสิ่งผิดปกติที่เกิดขึ้นกับเครื่องคอมพิวเตอร์ส่วนบุคคลต่อผู้ดูแลระบบ

๔.๒ ข้อปฏิบัติการใช้งานของผู้ดูแลระบบ

๔.๒.๑ กำหนดรหัสผ่านให้กับเครื่องคอมพิวเตอร์ส่วนบุคคลทุกเครื่อง ผู้ดูแลระบบมีรหัสผ่านสองชุดเพื่อจัดการระบบ ชุดแรกเป็นรหัสผ่านที่ใช้ปกติ ชุดที่สองเป็นรหัสผ่านสำหรับการใช้งานกรณีฉุกเฉิน

๔.๒.๒ ติดตั้ง Software ต่างๆ ที่จำเป็นต่อการใช้งานให้พอเพียงต่อการใช้งานในแต่ละระดับ

๔.๒.๓ ทำการ Update โปรแกรมต่างๆ เช่นWindows, Antivirus, และ Antispyware ทุกสัปดาห์เพื่อให้ได้โปรแกรมที่ทันสมัยอยู่เสมอ

๔.๒.๔ ทำการ Update บัญชีรายชื่อ ไวรัสคอมพิวเตอร์ทุกสัปดาห์ให้เครื่องคอมพิวเตอร์ทุกเครื่องอยู่ในสภาพพร้อมใช้งานและปราศจากโปรแกรมที่ไม่พึงประสงค์

๔.๒.๕ ทำการ Scan ไวรัสคอมพิวเตอร์และ Malware ทุกสัปดาห์

๔.๒.๖ ปิดระบบการให้บริการของระบบปฏิบัติการบางส่วนที่อาจะทำให้เป็นช่องทางในการเข้าจู่โจมของ Hacker และระบบการให้บริการที่ไม่เกี่ยวข้องกับการทำงานของผู้ใช้โดยตรง เช่น ปิดการให้บริการเว็บในระบบปฏิบัติการ Windows

๔.๒.๗ ผู้ดูแลระบบบันทึกรายงานผลการปฏิบัติงานเสนอต่อคณะกรรมการด้านความปลอดภัยสารสนเทศของอ.อ.ป. เมื่อมีเหตุการณ์ผิดปกติเกิดขึ้น เช่น การติดไวรัสคอมพิวเตอร์ที่เครื่องคอมพิวเตอร์ส่วนบุคคลในระดับความมั่นคงทุกระดับทันทีที่เกิดเหตุการณ์ขึ้น

๔.๒.๘ ผู้ดูแลระบบบันทึกรายงานผลการปฏิบัติงานเสนอต่อคณะกรรมการด้านความปลอดภัยสารสนเทศของอ.อ.ป. เมื่อทำการตรวจซ่อมบำรุงรักษาเครื่องคอมพิวเตอร์เป็นประจำทุกเดือน

๔.๒.๙ ผู้ดูแลระบบบันทึกผู้ใช้ที่ฝ่าฝืนข้อปฏิบัติด้านความมั่นคงเครื่องคอมพิวเตอร์ส่วนบุคคลของหน่วยงาน ให้คณะกรรมการด้านความปลอดภัยสารสนเทศของอ.อ.ป.รายงานต่อรองผู้อำนวยการองค์การอุตสาหกรรมป่าไม้ที่มีหน้าที่ดูแลรับผิดชอบด้านเทคโนโลยีสารสนเทศ (CIO)

ส่วนที่ ๑๑
การจัดเตรียมระบบเครือข่ายคอมพิวเตอร์
(Prepare the Computer Network)

๑. วัตถุประสงค์

เพื่อการกำหนดมาตรการและแนวทางในการติดตั้งอุปกรณ์เครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย การติดตั้ง Software ระบบปฏิบัติการ การติดตั้งโปรแกรมประยุกต์สำหรับใช้งานกับอุปกรณ์ รวมถึงการจัดเตรียมระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย การทดสอบอุปกรณ์ก่อนทำการติดตั้งในห้องปฏิบัติการ

๒. การเตรียมเอกสารก่อนการติดตั้ง

๒.๑ ผู้ดูแลระบบดำเนินการลงทะเบียนอุปกรณ์ทุกชิ้นกับผู้รับผิดชอบอุปกรณ์ โดยระบุคุณลักษณะที่สำคัญของอุปกรณ์ ระบบปฏิบัติการที่ใช้พร้อมรุ่น วันที่ติดตั้ง ชื่อผู้ติดตั้ง วัตถุประสงค์การใช้งานของอุปกรณ์ รวมถึงรายการโปรแกรมประยุกต์ที่ติดตั้งในอุปกรณ์อย่างชัดเจน

๒.๒ ผู้ดูแลระบบทำการรวบรวมเอกสารคุณลักษณะของอุปกรณ์ ทั้งที่เป็นสิ่งพิมพ์และโปรแกรมที่ใช้กับอุปกรณ์ เพื่อนำส่งไปยังผู้รับผิดชอบอุปกรณ์

๒.๓ ผู้ดูแลระบบจัดเตรียมแผนการติดตั้ง ระยะเวลา ผู้รับผิดชอบ และการรับมือในกรณีฉุกเฉิน

๒.๔ ผู้ดูแลระบบจัดเตรียมแผนผังทางกายภาพ (Layout) ที่ระบุตำแหน่งของอุปกรณ์ที่จะทำการติดตั้ง

๒.๕ ผู้ดูแลระบบจัดเตรียมแผนผังทางตรรกะของเครือข่าย (Network Logical Diagram) ที่ระบุการเชื่อมต่อของอุปกรณ์ที่ต้องการจะติดตั้ง

๒.๖ ผู้ดูแลระบบเตรียมเอกสารการติดตาม (Monitoring Chart) แบบที่เป็นการจดบันทึกด้วยกระดาษ หรือบันทึกด้วยระบบอิเล็กทรอนิกส์

๒.๗ ผู้ดูแลระบบเตรียมป้ายชื่ออุปกรณ์ ที่ใช้วัสดุ และมีรูปแบบการจัดพิมพ์ตามแบบที่ใช้ในห้องปฏิบัติงานติดตั้งให้เห็นชัดเจนบนตัวอุปกรณ์

๒.๘ ในกรณีต้องทำการใดๆ กับอุปกรณ์ที่กำลังทำหน้าที่ให้บริการอยู่ โดยเฉพาะกับอุปกรณ์ที่มีผลกระทบสูงต่อผู้ใช้งานและหน่วยงาน ต้องมีการแจ้งให้ผู้ใช้งานทราบล่วงหน้ารวมถึงทราบผลกระทบที่อาจเกิดขึ้น

๒.๙ มีหนังสือรับรองเห็นชอบอนุมัติในการติดตั้ง และแผนการติดตั้งจากหัวหน้าฝ่ายสารสนเทศก่อนดำเนินการเคลื่อนย้ายอุปกรณ์เข้าไปในห้องปฏิบัติงาน รวมทั้งก่อนมีการติดตั้งโปรแกรมใดๆ

๓. การทดสอบอุปกรณ์ และโปรแกรมก่อนการติดตั้ง

๓.๑ อุปกรณ์ต้องอยู่ในสภาพทางกายภาพสมบูรณ์พร้อมใช้งาน

๓.๒ อุปกรณ์ทุกชิ้นต้องผ่านการป้อนไฟเพื่อทดสอบว่าใช้งานได้ และไม่เกิดการลัดวงจร หรือมีความร้อนมาก จนอาจเป็นสาเหตุของไฟฟ้าลัดวงจรหรือไฟไหม้

๓.๓ ในกรณีที่เป็นการติดตั้งอุปกรณ์ใหม่ ผู้ดูแลระบบต้องทำการติดตั้งระบบปฏิบัติการโปรแกรมป้องกันไวรัส พร้อมทั้งโปรแกรมประยุกต์ที่จะใช้งานให้เสร็จสิ้น พร้อมทั้งทดสอบการทำงานให้สมบูรณ์ก่อนนำเข้าติดตั้ง

๓.๔ ในกรณีที่ต้องการติดตั้งโปรแกรมประยุกต์บนอุปกรณ์ที่กำลังใช้งาน

๓.๔.๑ จัดเตรียมอุปกรณ์ทดสอบที่ติดตั้งระบบปฏิบัติการ รุ่นของระบบปฏิบัติการและโปรแกรมประยุกต์ทั้งหมดเหมือนกับอุปกรณ์ที่กำลังใช้งาน

๓.๔.๒ ให้ผู้ดูแลระบบทำการทดลองติดตั้งโปรแกรมประยุกต์ดังกล่าวบนอุปกรณ์ทดสอบ เพื่อศึกษาถึงผลกระทบที่เกิดขึ้น

๓.๔.๓ เจ้าหน้าที่จัดทำรายงานสรุปผลการทดสอบ

๔. การทำงานขณะติดตั้งอุปกรณ์ และโปรแกรม

๔.๑ การเคลื่อนย้าย และการติดตั้งอุปกรณ์ ต้องเป็นไปตามนโยบายการควบคุมการเข้าออกห้องควบคุมระบบคอมพิวเตอร์และการป้องกันความเสียหาย

๔.๒ ผู้ดูแลระบบทำการบันทึก ชื่อบัญชีผู้ใช้ และรหัสผ่านของระบบ (Root User Name และ Password) ไว้ในที่ปลอดภัยตามนโยบายการรักษาความมั่นคงปลอดภัยและจัดเก็บรหัสลับของหน่วยงาน

๔.๓ การตั้งค่าทางเครือข่าย (Network Configuration) หมายเลข IP, Marking, Protocol การหาเส้นทาง การตั้งค่า LAN เสมือน และการตั้งค่าอื่นๆ ที่เกี่ยวกับเครือข่าย ต้องเป็นไปตามข้อกำหนดการใช้งานเครือข่ายของหน่วยงานเท่านั้น

๕. ภายหลังการติดตั้ง

๕.๑ ผู้ดูแลระบบทำการตรวจสอบติดตามการทำงานของอุปกรณ์ หรือโปรแกรมที่ติดตั้งและลงบันทึกในเอกสารการติดตาม (Monitoring Chart) ที่ได้เตรียมไว้ ทุกช่วงระยะเวลาที่กำหนด

๕.๒ ผู้ดูแลระบบจัดเตรียมรายงานการติดตั้ง ข้อเสนอแนะในการดูแลรักษา รวมถึงค่าใช้จ่ายในการดูแลรักษา เพื่อส่งให้กับหัวหน้าฝ่ายสารสนเทศรับทราบ

ส่วนที่ ๑๒
การบริหารระบบเครือข่ายคอมพิวเตอร์
(Computer Network Management)

๑. วัตถุประสงค์

เพื่อการกำหนดมาตรการและแนวทางในการบริหารระบบเครือข่าย ทั้งในด้าน Hardware และ Software ข้อกำหนดเกี่ยวกับการจัดการ IP Address การตรวจสอบระบบเครือข่าย การเข้าถึงระบบจากระยะไกล การซ่อมบำรุง และการดำเนินการเมื่อระบบขัดข้อง

๒. ขอบเขต

ครอบคลุมถึงอุปกรณ์เครือข่ายทุกชนิด ทั้งด้าน Hardware และ Software การเข้าถึงเครือข่าย และระบบสนับสนุนเครือข่ายที่เป็นสมบัติของฝ่ายสารสนเทศ สำนักวิจัยพัฒนาและสารสนเทศ ที่ติดตั้งและเปิดใช้งานเชื่อมต่อทั้งอย่างถาวรหรือชั่วคราวกับระบบเครือข่าย

๓. การจัดการ IP Address

๓.๑ การจัดสรร IP Address

๓.๑.๑ ผู้ดูแลระบบมีหน้าที่จัดสรร IP Address สำหรับหน่วยงานต่างๆ ของอ.อ.ป.

๓.๑.๒ หน่วยงานภายในสามารถยื่นเรื่องขออนุมัติต่อหัวหน้าฝ่ายสารสนเทศ เพื่อขอใช้ IP Address

๓.๑.๓ หน่วยงานภายในต้องระบุเหตุผลความจำเป็นที่ต้องการเพิ่มหรือลดจำนวน IP Address ในคำขออนุมัติ

๓.๑.๔ ผู้ดูแลระบบสามารถลดหรือเพิ่มจำนวน IP Address สำหรับหน่วยงานภายในได้ตามผลการพิจารณาคำขออนุมัติ และต้องแจ้งให้หน่วยงานนั้นๆ ทราบเป็นระยะเวลาไม่น้อยกว่า ๒ วันก่อนเริ่มใช้งานจริง

๓.๑.๕ หน่วยงานภายในต้องปฏิบัติตามนโยบายและข้อปฏิบัติต่างๆ ของอ.อ.ป.ที่เกี่ยวข้องกับการใช้งานเครือข่ายคอมพิวเตอร์อย่างเคร่งครัด

๓.๒ แนวทางการพิจารณาจัดสรร IP Address

๓.๒.๑ ผู้ดูแลระบบมีหน้าที่ประเมินปริมาณความต้องการใช้งาน IP Address ของหน่วยงานภายใน เพื่อประกอบการพิจารณาจัดสรร IP Address

๓.๒.๒ ผู้ดูแลระบบสามารถเสนอแนวทางการจัดสรรเพิ่มหรือลดจำนวน IP Address สำหรับอ.อ.ป. พร้อมทั้งระบุเหตุผลความจำเป็นต่อหัวหน้าฝ่ายสารสนเทศ

๓.๓ ข้อปฏิบัติสำหรับผู้ดูแลระบบ

๓.๓.๑ ผู้ดูแลระบบต้องประเมินการใช้งาน IP Address ของหน่วยงานภายในที่ได้รับการจัดสรรไปว่าได้ใช้งานอย่างมีประสิทธิภาพหรือไม่หลังจากการใช้งานจริง ๑ เดือน

๓.๓.๒ ผู้ดูแลระบบมีหน้าที่บันทึกข้อมูลการจัดสรร IP Address ในเอกสารข้อมูลการจัดสรร IP Address ทันที

๔. การตรวจสอบระบบเครือข่าย

๔.๑ ข้อปฏิบัติการตรวจสอบประจำวัน

๔.๑.๑ ผู้ดูแลระบบมีหน้าที่ตรวจสอบระบบคอมพิวเตอร์และเครือข่ายภายใต้ความรับผิดชอบเป็นประจำทุกวันทันทีที่มาปฏิบัติตามเวลาราชการ โดยกำหนดให้ตรวจสอบให้เสร็จสิ้นก่อนเวลา ๑๒.๐๐ น.

๔.๑.๒ ให้ผู้ดูแลระบบบันทึกผลการตรวจสอบแล้วรายงานต่อหัวหน้าฝ่ายสารสนเทศทุกวันหรือบันทึกผลการตรวจสอบในรูปแบบอื่นใดตามที่หัวหน้าฝ่ายสารสนเทศมอบหมาย

๔.๑.๓ ให้หัวหน้าฝ่ายสารสนเทศมอบหมายเจ้าหน้าที่สำรองตรวจสอบระบบประจำวัน ในกรณีที่ผู้ดูแลระบบไม่สามารถปฏิบัติงานได้

๔.๑.๔ ในกรณีที่ตรวจสอบแล้วพบปัญหา ให้ดำเนินการแก้ไขปัญหาและสรุปผลการแก้ไขปัญหาในรายงานการตรวจสอบประจำวัน

๔.๑.๕ ในกรณีที่ตรวจสอบพบปัญหาที่อาจสร้างความเสียหายอย่างรุนแรงทั้งในเวลาราชการและนอกเวลาราชการ ให้ผู้ดูแลระบบแจ้งหัวหน้าฝ่ายสารสนเทศเพื่อดำเนินการแก้ไข รายงานผลการแก้ไขพร้อมทั้งบันทึกในรายงานการตรวจสอบประจำวัน และให้หัวหน้าฝ่ายสารสนเทศรายงานสรุปผลการปฏิบัติงานต่อผู้อำนวยการสำนักวิจัยพัฒนาและสารสนเทศหรือผู้ที่ได้รับมอบหมาย

๔.๒ การตรวจสอบระบบคอมพิวเตอร์

๔.๒.๑ ตรวจสอบความคงอยู่และการให้บริการของระบบคอมพิวเตอร์ว่ายังสามารถให้บริการได้ตามปกติหรือไม่ โดยทดลองขอเข้าใช้บริการเสมือนเป็นผู้ขอใช้บริการตามปกติ โดยตรวจสอบระบบคอมพิวเตอร์แม่ข่ายหลักที่ให้บริการ

๔.๒.๒ ตรวจสอบการทำงานที่ผิดปกติของระบบคอมพิวเตอร์ทั้งหมดโดยพิจารณาจากหลักเกณฑ์ต่อไปนี้

- การทำงานของ Process
- ภาระงานหน่วยประมวลผลกลาง
- ปริมาณการใช้เนื้อที่ดิสก์ในพาร์ติชั่นต่างๆ
- ปริมาณการใช้หน่วยความจำหลัก
- แฟ้มบันทึกการทำงาน

๔.๒.๓ ตรวจสอบเครื่องคอมพิวเตอร์แม่ข่าย และระบบคอมพิวเตอร์แม่ข่ายอื่นๆ ที่มีความสำคัญ

๔.๓ การตรวจสอบระบบเครือข่าย

๔.๓.๑ ตรวจสอบความคงอยู่และการให้บริการของเส้นทางสื่อสารหลักว่ายังสามารถใช้งานได้ตามปกติหรือไม่

๔.๓.๒ ตรวจสอบความคงอยู่และการทำงานที่ผิดปกติของอุปกรณ์เครือข่ายหลักและระบบสนับสนุนการให้บริการ

๔.๓.๓ ตรวจสอบความคงอยู่และการให้บริการของ Router และการพิสูจน์ตัวจริง(Authentication)

๔.๓.๔ ตรวจสอบความคงอยู่และการให้บริการของ Access Point ในเครือข่ายไร้สาย

๔.๓.๕ ตรวจสอบสถิติและ /หรือข้อมูลที่เกี่ยวข้องทางสถิติของการใช้งานเครือข่ายว่ามีความผิดปกติหรือไม่ เช่น ปริมาณการใช้ช่องสัญญาณ เป็นต้น

๔.๓.๖ ตรวจสอบเครื่องคอมพิวเตอร์แม่ข่าย และเส้นทางเชื่อมโยงอื่นๆ ที่มีความสำคัญ

๕. การเข้าถึงระบบจากระยะไกล

๕.๑ ข้อปฏิบัติในการขอเข้าใช้ระบบจากระยะไกล

๕.๑.๑ ผู้ดูแลระบบมีหน้าที่จัดเตรียมระบบ เพื่อรองรับการเชื่อมต่อระยะไกล

๕.๑.๒ ผู้ใช้งานต้องยื่นเรื่องขอใช้งานผ่านหน่วยงาน เพื่อขออนุมัติต่อหัวหน้าฝ่ายสารสนเทศ

๕.๑.๓ ผู้ใช้งานต้องระบุเหตุผลความจำเป็นที่ต้องการใช้งาน

๕.๑.๔ ผู้ดูแลระบบต้องเป็นผู้ติดตามผลการพิจารณาคำขออนุมัติ และแจ้งให้ผู้ใช้งานนั้นๆ ทราบเป็นระยะเวลาไม่เกิน ๑ สัปดาห์

๕.๑.๕ ถ้าผลการพิจารณาอนุมัติ ผู้ดูแลระบบต้องเตรียมเอกสาร ขั้นตอนการติดตั้ง Software ที่จำเป็น และข้อมูลชื่อผู้ใช้ และรหัสผ่าน แก่ผู้ใช้งานพร้อมกับการแจ้งผล

๕.๑.๖ ผู้ใช้งานต้องปฏิบัติตามนโยบายและข้อปฏิบัติต่างๆ ของหน่วยงาน ที่เกี่ยวข้องกับการใช้งานเครือข่ายอย่างเคร่งครัด

๕.๒ ความปลอดภัยการใช้งาน

๕.๒.๑ ผู้ดูแลระบบมีหน้าที่เตรียมระบบความปลอดภัย ในการรองรับการเชื่อมต่อระยะไกล เช่น การเข้ารหัส การติดตั้งและใช้งานระบบ VPN เป็นต้น

๕.๒.๒ ผู้ดูแลระบบมีหน้าที่เตรียมเอกสารการใช้งาน และติดตั้งระบบความปลอดภัยให้พร้อมใช้งานได้ตลอดเวลา

๕.๒.๓ ผู้ดูแลระบบมี่หน้าที่กำหนดสิทธิในการเข้าถึงข้อมูลของผู้ใช้งานแต่ละคนตามความเหมาะสม เมื่อผู้ใช้เชื่อมต่อระบบจากระยะไกล พร้อมกับห้ามการเข้าใช้งานกับส่วนของเครือข่าย ระบบฐานข้อมูล หรือระบบที่มีความสำคัญสูง

๖. การซ่อมบำรุง

๖.๑ ข้อปฏิบัติการซ่อมบำรุงรักษาระบบ

๖.๑.๑ ผู้ดูแลระบบมีหน้าที่ซ่อมบำรุงรักษา แก้ไขข้อบกพร่อง เพิ่มขีดความสามารถ เพื่อให้ระบบเทคโนโลยีสารสนเทศทำงานและให้บริการได้ตามปกติ

๖.๑.๒ การซ่อมบำรุงใดๆ ที่เป็นเหตุให้ต้องหยุดระบบ ผู้ดูแลระบบต้องจัดทำแผนเพื่อขออนุมัติดำเนินการหรือเพื่อเสนอทราบจากหัวหน้าฝ่ายสารสนเทศหรือผู้ที่ได้รับมอบหมาย

๖.๑.๓ ในกรณีที่หยุดระบบมากกว่า ๑ ชั่วโมง ผู้ดูแลระบบต้องจัดทำแผนซ่อมบำรุงรักษาระบบโดยละเอียด เพื่อเสนอขออนุมัติก่อนดำเนินการล่วงหน้าไม่น้อยกว่า ๕ วันทำการ

๖.๑.๔ ในกรณีหยุดระบบโดยใช้เวลาน้อยกว่า ๑ ชั่วโมง ให้จัดทำแผนงานเพื่อเสนอทราบล่วงหน้าไม่น้อยกว่า ๕ วันทำการ

๖.๑.๕ ผู้ดูแลระบบต้องวางแผนงานและดำเนินการเพื่อสามารถประชาสัมพันธ์ให้ผู้ใช้งานที่ได้รับผลกระทบจากการหยุดระบบทราบเป็นเวลาไม่น้อยกว่า ๒ วัน นับจากวันประกาศถึงวันที่ต้องหยุดระบบ ยกเว้นในกรณีฉุกเฉินที่ต้องดำเนินการทันที เพื่อแก้ปัญหาความมั่นคงหรือความปลอดภัย โดยให้มีการประกาศข้อความผ่านทางระบบงานนั้นๆ ก่อนการหยุดระบบและ/หรือระหว่างการหยุดระบบ

๖.๑.๖ ผู้ดูแลระบบต้องจัดทำรายงานสรุปการดำเนินงานและเสนอหัวหน้าฝ่ายสารสนเทศ หรือผู้ที่ได้รับมอบหมายภายใน ๑ วัน หลังจากเสร็จสิ้นการหยุดระบบ

๖.๑.๗ การซ่อมบำรุงรักษาตามตารางเวลา ให้ผู้ดูแลระบบจัดทำแผนบำรุงรักษาระบบเสนอเพื่อขออนุมัติต่อหัวหน้าฝ่ายสารสนเทศไว้ล่วงหน้า

๖.๑.๘ กรณีเปิดให้บริการหลังจากหยุดระบบไม่เป็นไปตามแผนเกิน ๑ ชั่วโมง ให้แจ้งเหตุผลต่อหัวหน้าฝ่ายสารสนเทศหรือผู้ที่ได้รับมอบหมายจากหัวหน้าฝ่ายสารสนเทศทราบภายในวันถัดไป

๗. ข้อปฏิบัติเมื่อระบบคอมพิวเตอร์หรือเครือข่ายขัดข้อง

๗.๑ การแก้ไขปัญหา

๗.๑.๑ ให้ผู้ดูแลระบบวิเคราะห์ผลกระทบเบื้องต้นในกรณีที่ระบบคอมพิวเตอร์และ/หรือเครือข่ายขัดข้อง โดยพิจารณาแล้วกำหนดผลกระทบเป็นระดับปกติ ระดับปานกลาง หรือระดับสูง และรายงานต่อหัวหน้าฝ่ายสารสนเทศทราบทันที

๗.๑.๒ ให้เริ่มดำเนินการแก้ไขระบบคอมพิวเตอร์และเครือข่ายที่ขัดข้องหลังจากการวิเคราะห์ผลกระทบภายใน ๑ ชั่วโมง ในกรณีที่เป็นผลกระทบระดับปกติ ๓๐ นาที ในกรณีเป็นผลกระทบระดับปานกลาง และแก้ไขทันทีในกรณีที่เป็นผลกระทบระดับสูง โดยดำเนินการในเวลาราชการ ยกเว้นกรณีเร่งด่วนฉุกเฉินซึ่งผลกระทบอาจสร้างความเสียหายอย่างร้ายแรง ให้ดำเนินการโดยไม่เว้นวันหยุดราชการ

๗.๑.๓ ให้ผู้ดูแลระบบกำหนดแนวทางการแก้ปัญหา ขั้นตอน และตารางเวลาการปฏิบัติที่ชัดเจน โดยสรุปลักษณะปัญหา ผลกระทบที่เกิดขึ้นหรืออาจจะเกิดขึ้น หากมีความจำเป็นต้องได้รับความร่วมมือจากผู้มีส่วนเกี่ยวข้องอื่น ให้เรียกประชุมทีมงานพร้อมกันในคราวเดียว

๗.๑.๔ ให้ผู้ดูแลระบบที่ปฏิบัติงานดำเนินการแก้ปัญหาตามแนวทางที่กำหนดในข้อก่อนหน้านี้ และรายงานผลการปฏิบัติต่อหัวหน้าฝ่ายสารสนเทศทันทีที่ดำเนินการเสร็จสิ้น

๗.๑.๕ หากมีผลกระทบที่จำเป็นต้องแจ้งข่าวสารให้กับผู้ใช้งานทราบจะต้องตรวจสอบให้อย่างแน่ชัดและแจ้งให้ทราบทันที

๗.๑.๖ ในกรณีที่เป็นปัญหาที่ส่งผลกระทบระดับสูง ให้หัวหน้าฝ่ายสารสนเทศรายงานผลการปฏิบัติงานต่อผู้อำนวยการสำนักวิจัยพัฒนาและสารสนเทศหรือผู้ที่ได้รับมอบหมาย

๗.๒ ข้อคำนึงในการปฏิบัติงาน

๗.๒.๑ ระบบคอมพิวเตอร์และเครือข่ายมีความสำคัญต่อการให้บริการและการดำเนินงานของฝ่ายสารสนเทศ ดังนั้นจึงให้ผู้ปฏิบัติงานวิเคราะห์ความจำเป็นเร่งด่วนและผลกระทบที่อาจจะเกิดขึ้นและต้องให้ความสำคัญสูงต่อการปฏิบัติงานแก้ไขเมื่อระบบเกิดขัดข้อง

๗.๒.๒ หากเจ้าหน้าที่ผู้ใดไม่สามารถปฏิบัติงานได้ให้หัวหน้าฝ่ายสารสนเทศมอบหมายเจ้าหน้าที่เพื่อปฏิบัติหน้าที่แทนทันที เพื่อให้การดำเนินงานเป็นไปด้วยความถูกต้องและรวดเร็ว

๘. ข้อปฏิบัติเมื่อระบบจ่ายไฟฟ้าขัดข้อง

๘.๑ การแก้ไขปัญหา

๘.๑.๑ ให้ผู้ดูแลระบบวิเคราะห์ผลกระทบเบื้องต้นในกรณีที่ระบบคอมพิวเตอร์และ/หรือเครือข่ายขัดข้องเป็นระยะเวลานานเกินกว่าระบบสำรองไฟฟ้าจะจ่ายไฟฟ้าได้ โดยพิจารณาแล้วกำหนดผลกระทบเป็นระดับปกติ ระดับปานกลาง หรือระดับสูง และรายงานต่อหัวหน้าฝ่ายสารสนเทศทราบในทันที

๘.๑.๒ ให้ผู้ดูแลระบบดำเนินการตรวจสอบระบบไฟฟ้าและติดต่อผู้ที่เกี่ยวข้องกับปัญหาด้านไฟฟ้า โดยนำข้อมูลเพื่อวิเคราะห์ว่ามีระบบใดบ้างได้รับผลกระทบ กำหนดแนวทางการแก้ปัญหาด้านเครือข่ายและระบบคอมพิวเตอร์ ขั้นตอน และตารางเวลาการปฏิบัติ โดยสรุปลักษณะปัญหาผลกระทบที่เกิดขึ้นหรืออาจจะเกิดขึ้น หากมีความจำเป็นต้องได้รับความร่วมมือจากผู้มีส่วนเกี่ยวข้องอื่น ให้เรียกประชุมทีมงานพร้อมกันในคราวเดียว

๘.๑.๓ หากมีผลกระทบที่จำเป็นต้องแจ้งข่าวสารให้กับผู้ใช้งานทราบจะต้องตรวจสอบให้อย่างแน่ชัดและแจ้งให้ทราบทันที

๘.๑.๔ ให้ผู้ดูแลระบบที่ปฏิบัติงานดำเนินการแก้ปัญหาตามแนวทางที่กำหนดและรายงานผลการปฏิบัติต่อหัวหน้างานที่สังกัดทันทีที่ดำเนินการเสร็จสิ้น

๘.๑.๕ ในกรณีที่เป็นปัญหาที่ส่งผลกระทบระดับสูง ให้หัวน้าส่วนสารสนเทศรายงานผลการปฏิบัติงานต่อหัวหน้าฝ่ายสารสนเทศหรือผู้ที่ได้รับมอบหมาย

๘.๒ ข้อคำนึงในการปฏิบัติงาน

๘.๒.๑ ระบบคอมพิวเตอร์และเครือข่ายมีความสำคัญต่อการให้บริการและการดำเนินงานของฝ่ายสารสนเทศ ดังนั้นจึงให้ผู้ดูแลระบบวิเคราะห์ความจำเป็นเร่งด่วนและผลกระทบที่อาจจะเกิดขึ้นและต้องให้ความสำคัญสูงต่อการปฏิบัติงานแก้ไขเมื่อระบบไฟฟ้าเกิดขัดข้อง

๘.๒.๒ หากผู้ดูแลระบบผู้ใดไม่สามารถปฏิบัติงานใดให้หัวหน้าฝ่ายสารสนเทศมอบหมายผู้ดูแลระบบคนอื่นเพื่อปฏิบัติหน้าที่แทนทันที เพื่อให้การดำเนินงานเป็นไปด้วยความถูกต้องและรวดเร็ว

ส่วนที่ ๑๓
การนำ Open Source Software มาใช้ในหน่วยงาน

๑. บทนำ

ปัจจุบันปัญหาเรื่องการละเมิดลิขสิทธิ์ Software เป็นปัญหาใหญ่ในประเทศไทย ไม่ว่าจะเป็นผู้ใช้ทั่วไปหรือหน่วยงานบริษัทห้างร้านต่างๆ หน่วยงานที่ไม่ละเมิดลิขสิทธิ์ก็จะต้องแบกรับภาระการลงทุนซื้อ Software ลิขสิทธิ์ซึ่งจะมากน้อยก็แล้วแต่ขนาดความใหญ่ของหน่วยงาน ทางเลือกในหน่วยงานที่ใช้คือการนำ Open Source Software ซึ่งไม่มีค่าลิขสิทธิ์สามารถนำมาใช้ได้ฟรี ซึ่งสามารถลดภาระค่าใช้จ่ายให้แก่หน่วยงานได้เป็นอย่างมาก

๒. วัตถุประสงค์

๒.๑ เพื่อเปลี่ยนแปลงการใช้งาน Licensed Software เข้าสู่รูปแบบ Open Source Software

๒.๒ เพื่อลดปัญหาการละเมิดซอฟต์แวร์ที่มีลิขสิทธิ์ในประเทศไทย

๒.๓ เพื่อปรับองค์กรรูปแบบ Licensed Software เข้าสู่องค์กรรูปแบบ Open Source Software ตามนโยบายของกระทรวง ICT

๒.๔ สอดคล้องกับ พ.ร.บ.ลิขสิทธิ์ พ.ศ.๒๕๓๗

๓. แนวทางการนำมาใช้งาน

๓.๑ ผู้ดูแลระบบต้องทำความเข้าใจกับพนักงานทุกระดับ เริ่มตั้งแต่ระดับผู้ปฏิบัติงานเจ้าหน้าที่สนับสนุนทางเทคนิคจนถึงผู้บริหารระดับสูง เพื่อให้เข้าใจตรงกันว่าการนำ Open Source Software มาใช้งานนั้น ส่งผลดีต่อองค์กรอย่างไรบ้าง ไม่ว่าจะเป็นการช่วยลดค่าใช้จ่ายการซื้อ Software ลิขสิทธิ์ หรือการใช้ Software อย่างถูกต้องตามกฎหมาย เป็นต้น

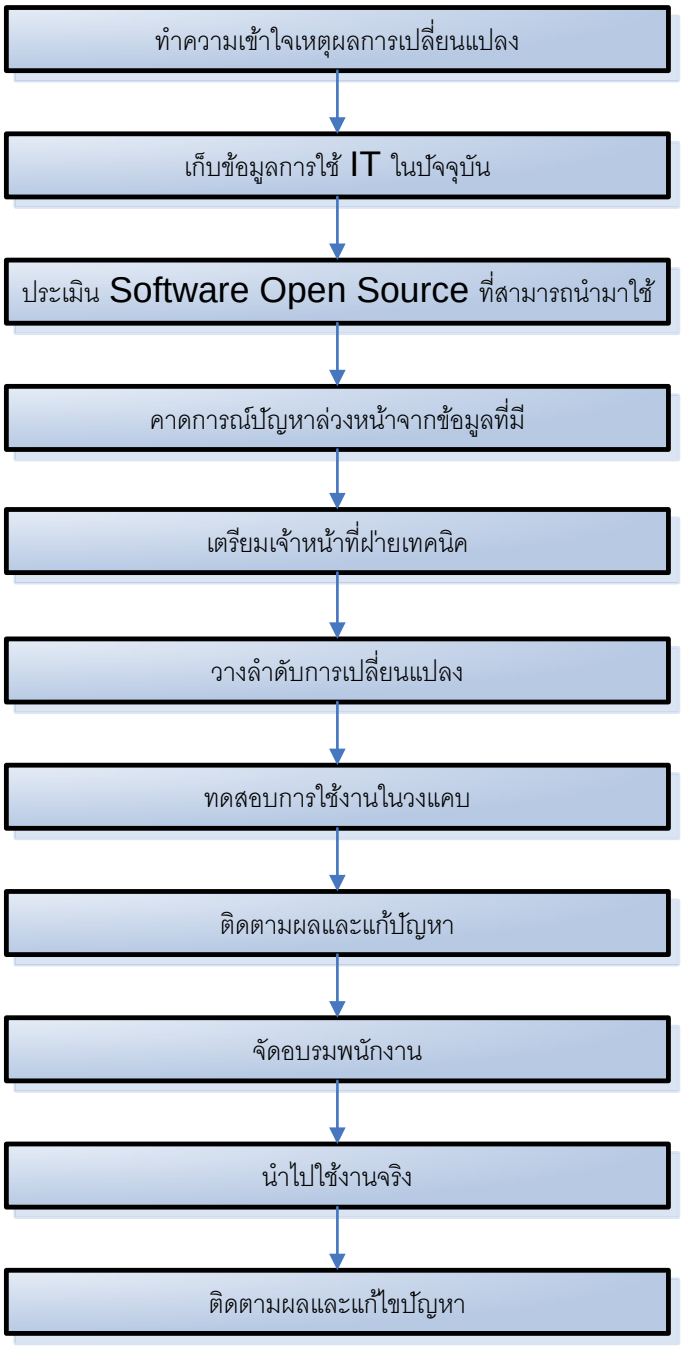
๓.๒ ผู้ดูแลระบบต้องเก็บข้อมูลการใช้ IT ในปัจจุบันในหน่วยงานก่อนว่าส่วนงานไหนสามารถนำ Open Source มาใช้งานได้บ้าง เพราะใช้ว่าหน่วยงานในองค์กรจะสามารถใช้ Software Open Source ได้ทั้งหมด เช่น Open Office ซึ่งจะนำมาใช้งานทดแทน Microsoft Office ได้ หากหน่วยงานต้องมีการแลกเปลี่ยนเอกสารกับบุคคลภายนอก การใช้ Open Office อย่างเต็มรูปแบบอาจจะไม่เหมาะสมนัก คงต้องควบคู่กันไป แต่หากเป็นหน่วยงานใช้เฉพาะเอกสารภายในก็สามารถใช้ Open Office ทดแทน Microsoft Office ได้เต็มรูปแบบ เป็นต้น

๓.๓ ผู้ดูแลระบบต้องคาดการณ์ปัญหาที่จะเกิดขึ้น และศึกษาข้อมูล Software ที่จะนำมาใช้งานว่ามีปัญหาด้านใดบ้าง เช่น ความเข้ากันได้กับข้อมูลที่มีอยู่เดิม ความยากในการใช้งาน เพราะ Software บางตัวอาจมีเมนูคำสั่งหรือหน้าจอการใช้งานต่างไปจากโปรแกรมเดิมที่ใช้งานอยู่ ซึ่งสามารถสร้างปัญหาให้กับผู้ใช้ได้พอสมควร

๓.๔ ผู้ดูแลระบบทำการประเมินต้นทุนในการเปลี่ยนแปลง มีการวัดผลด้วยว่าการนำ Open Source Software มาใช้งานนั้นมีความคุ้มค่ามากน้อยแค่ไหน เมื่อเทียบกับปัญหาที่เกิดขึ้น และมูลค่าเงินที่ประหยัดได้ หลังจากสรุปปัญหาและแนวทางการแก้ไขแล้ว ควรจัดให้มีการอบรมพนักงานได้ทราบข้อมูลเกี่ยวกับ Open Source Software ที่จะนำมาใช้งาน และเรียนรู้วิธีการใช้งาน รวมถึงแนวทางการแก้ไขเบื้องต้นด้วยตนเอง

๓.๕ ทดลองนำไปใช้งาน ในระยะเริ่มต้นของการนำ Open Source มาใช้งานในองค์กร ควรทดลองนำ Software Open Source ไปใช้งานในวงแคบ ซึ่งแนวทางที่องค์กรส่วนใหญ่เลือกใช้ก็คือเริ่มจากส่วนที่กระทบกับผู้ดูแลระบบและผู้ใช้น้อยที่สุดก่อน จากนั้นก็ค่อยพัฒนาไปยังส่วนอื่นๆ ที่กระทบกับผู้ใช้มากขึ้น โดยเลือกหน่วยงานหรือแผนกนำร่องขึ้นมาสักแผนกหนึ่งมาทดสอบ Software Open Source ที่ต้องการ มาติดตั้ง

กับระบบคอมพิวเตอร์ที่มีอยู่เดิม นำข้อมูลที่มีอยู่เดิมมาใช้งาน ศึกษาดูว่าเกิดปัญหาอะไรขึ้นบ้าง ไม่ว่าจะเป็นปัญหาทางเทคนิคหรือปัญหาจากผู้ใช้งานเอง จากนั้นทำการศึกษาแนวทางแก้ไขต่อไป จากนั้นควรมีการวัดผลด้วยว่า การนำ Software Open Source มาใช้งานนั้น มีความคุ้มค่ามากน้อยแค่ไหน เมื่อเทียบกับปัญหาที่เกิดขึ้น และมูลค่าที่ประหยัดได้ หลังจากสรุปปัญหาและแนวทางการแก้ไขเรียบร้อยแล้ว ควรจัดให้มีการอบรมพนักงานให้ทราบข้อมูลเกี่ยวกับ Software Open Source ที่จะนำมาใช้งานและเรียนรู้การใช้งาน รวมถึงแนวทางปัญหาเบื้องต้นด้วยตนเอง เพื่อให้การทำงานของแต่ละส่วนงานเป็นไปอย่างราบรื่น ในระยะแรกอาจจำเป็นต้องใช้งาน Software Open Source ควบคู่ไปกับโปรแกรมเดิมที่ใช้งานอยู่ เพื่อให้เกิดความชำนาญและลดปัญหาที่จะเกิดขึ้น ซึ่งอาจกำหนดระยะเวลาการใช้งานประมาณ ๑ -๓ เดือน จากนั้นจึงเริ่มทยอยนำโปรแกรมออกไป และนำ Software Open Source เข้ามาแทนที่อย่างเต็มรูปแบบต่อไป



แสดงแนวทางการนำ Software Open Source มาใช้งานในองค์กร

ส่วนที่ ๑๔
การสร้างความตระหนักในเรื่องการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ

๑. วัตถุประสงค์

เพื่อเผยแพร่แนวนโยบายและแนวปฏิบัติให้กับบุคลากรและบุคคลที่เกี่ยวข้องได้มีความรู้ความเข้าใจและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตลอดจนสามารถนำไปปฏิบัติได้อย่างถูกต้อง

๒. แนวปฏิบัติการสร้างความตระหนักในเรื่องการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ

๒.๑ จัดฝึกอบรมแนวปฏิบัติตามแนวนโยบายอย่างสม่ำเสมอ โดยการจัดฝึกอบรมโดยใช้วิธีการเสริมเนื้อหาแนวปฏิบัติตามแนวนโยบายเข้ากับหลักสูตรอบรมต่างๆ ตามแผนการฝึกอบรมของหน่วยงาน

๒.๒ จัดสัมมนาเพื่อเผยแพร่แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และสร้างความตระหนักถึงความสำคัญของการปฏิบัติให้กับบุคลากร โดยการจัดสัมมนามีแผนการดำเนินงานปีละไม่น้อยกว่า ๑ ครั้ง โดยจะจัดร่วมกับการสัมมนาที่เกี่ยวข้องกับด้านเทคโนโลยีสารสนเทศ และมีการเชิญวิทยากรจากภายนอกที่มีประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศมาถ่ายทอดความรู้

๒.๓ ติดประกาศประชาสัมพันธ์ ให้ความรู้เกี่ยวกับแนวปฏิบัติ ในลักษณะเกร็ดความรู้ หรือข้อระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย โดยมีการปรับเปลี่ยนเกร็ดความรู้อยู่เสมอ

๒.๔ ระดมการมีส่วนร่วมและลงสู่ภาคปฏิบัติด้วยการกำกับ ติดตาม ประเมินผล และสำรวจความต้องการของผู้ใช้บริการ

ส่วนที่ ๑๕
การกำหนดแบ่งอำนาจหน้าที่ผู้รับผิดชอบ

การกำหนดแบ่ง อำนาจ หน้าที่มีวัตถุประสงค์เพื่อลดความเสี่ยงด้านโครงสร้างพื้นฐาน ซึ่งมีแนวทางปฏิบัติดังนี้ คือ ต้องแบ่งแยกบุคลากรที่ปฏิบัติหน้าที่ในส่วนการพัฒนาระบบงานออกจากบุคลากรที่ทำหน้าที่บริหารระบบ ซึ่งปฏิบัติงานอยู่ในส่วนระบบคอมพิวเตอร์ที่ใช้งานจริง และต้องจัดให้มีการระบุหน้าที่ความรับผิดชอบของแต่ละหน้าที่งาน และความรับผิดชอบของบุคลากรแต่ละคนภายในฝ่ายสารสนเทศอย่างชัดเจน เป็นลายลักษณ์อักษร ซึ่งควรจัดให้มีบุคลากรสำรองในงานที่มีความสำคัญ เพื่อให้สามารถทำงานทดแทนกันได้ในกรณีจำเป็น โดยกำหนดหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศเป็น ดังนี้

๑. ระดับนโยบาย

รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษาตลอดจน ติดตาม กำกับ ดูแล ควบคุม ตรวจสอบ เจ้าหน้าที่ในระดับปฏิบัติ รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นกรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใดๆ แก่หน่วยงานหรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ผู้รับผิดชอบ ได้แก่

รองผู้อำนวยการทำหน้าที่ (CIO)

ผู้อำนวยการสำนักที่รับผิดชอบดูแลงานระบบเทคโนโลยีสารสนเทศ

หัวหน้าฝ่ายที่รับผิดชอบดูแลงานระบบเทคโนโลยีสารสนเทศ

๒. ระดับปฏิบัติ

๒.๑ รับผิดชอบ กำกับ ดูแล การปฏิบัติงานของผู้ปฏิบัติ ตลอดจนศึกษา ทบทวน วางแผน ติดตามการบริหารความเสี่ยง และระบบรักษาความปลอดภัยฐานข้อมูลและเทคโนโลยีสารสนเทศ ผู้รับผิดชอบ ได้แก่

นาย ธนากร วิชัยกุล หัวหน้า ส่วนสารสนเทศ

นาย ปริญญา ร่มแสง หัวหน้า งานสารสนเทศ

๒.๒ รับผิดชอบในการดูแลบำรุงรักษา ระบบเครื่อง ระบบเครือข่าย ระบบฐานข้อมูล ความปลอดภัยของฐานข้อมูลและการสำเนาฐานข้อมูล

นายสันติ ภาคีทูล พนักงานส่วนสารสนเทศ

นางสาวนงค์รักษ์ ชำนาญ พนักงานส่วนสารสนเทศ

นางสาวกัลยาณี พลับสอาด พนักงานส่วนสารสนเทศ

นางสาวลมัยพร ดงเสือ พนักงานส่วนสารสนเทศ

นางสาวจารุวรรณ โพธิ์อินทร์ พนักงานส่วนสารสนเทศ

มีหน้าที่รับผิดชอบ ดังนี้

๑.) ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ส่วนที่ ๑ การควบคุมการเข้าถึงและใช้ระบบเครือข่าย

๒.) ควบคุมการเข้า -ออกห้องคอมพิวเตอร์แม่ข่าย (Server Room) ตามการกำหนดสิทธิการเข้าถึงห้องควบคุมระบบคอมพิวเตอร์

๓.) ดูแล ตรวจสอบ บำรุงรักษาอุปกรณ์ เครื่องคอมพิวเตอร์แม่ข่าย (Server Computer) และอุปกรณ์เชื่อมโยงเครือข่าย (Network) ของระบบการเชื่อมโยงเครือข่ายฐานข้อมูลทั้งหมด

๔.) ควบคุม ติดตาม ตรวจสอบ (Monitor) การเข้าใช้งานและการเข้าถึงระบบการทำงานของ Server ตามสิทธิการเข้าถึงระบบ

๕.) ทำการสำรองข้อมูลและเรียกคืนข้อมูล (Backup and Recovery) ตามกรอบระยะเวลาที่กำหนด

๖.) ป้องกันการถูกเจาะระบบ และปัญหาการถูกเจาะเข้าระบบฐานข้อมูลจากบุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาต

๗.) ดูแล ตรวจสอบ บำรุงรักษาอุปกรณ์ป้องกันการถูกเจาะระบบจากบุคคลภายนอก

๒.๓ รับผิดชอบในการรักษาความปลอดภัย ระบบเทคโนโลยีสารสนเทศ และระบบฐานข้อมูล

นายปริญญา ร่มแสง พนักงานส่วนสารสนเทศ

นางสาวนงค์รักษ์ ชำนาญ พนักงานส่วนสารสนเทศ

นางสาวกัลยาณี พลับสะอาด พนักงานส่วนสารสนเทศ

นางสาวจารุวรรณ โพธิ์อินทร์ พนักงานส่วนสารสนเทศ

มีหน้าที่รับผิดชอบ ดังนี้

๑.) ทบทวนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ส่วนที่ ๑-ส่วนที่ ๑๓

๒.) ประสานการปฏิบัติงานตามแผนป้องกันและแก้ไขปัญหาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ

๒.๔ รับผิดชอบในการรักษาความปลอดภัย ระบบอินเทอร์เน็ต

นางสาวนงค์รักษ์ ชำนาญ พนักงานส่วนสารสนเทศ

นางสาวกัลยาณี พลับสอาด พนักงานส่วนสารสนเทศ

นางสาวจารุวรรณ โพธิ์อินทร์ พนักงานส่วนสารสนเทศ

๒.๕ รับผิดชอบความปลอดภัยทั่วไป

นางสาวนงค์รักษ์ ชำนาญ พนักงานส่วนสารสนเทศ

นางสาวกัลยาณี พลับสอาด พนักงานส่วนสารสนเทศ

นางสาวละมัยพร ดงเสือ พนักงานส่วนสารสนเทศ

นางสาวจารุวรรณ โพธิ์อินทร์ พนักงานส่วนสารสนเทศ

ส่วนที่ ๑๖
นโยบายความมั่นคงปลอดภัยการใช้งานอินเทอร์เน็ต
(Internet Security Policy)

๑. วัตถุประสงค์

เพื่อให้ผู้ใช้รับทราบกฎเกณฑ์แนวทางปฏิบัติในการใช้งานอินเทอร์เน็ตอย่างปลอดภัยและเป็นการป้องกันไม่ให้ละเมิดพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ เช่น การส่งข้อมูล ข้อความ ชุดคำสั่งหรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์แก่บุคคลอื่นอันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุขทำให้ระบบคอมพิวเตอร์ของหน่วยงานถูกระงับชะลอขัดขวางหรือถูกรบกวนจนไม่สามารถทำงานตามปกติได้

๒. แนวทางปฏิบัติในการใช้งานอินเทอร์เน็ต

๒.๑ ผู้ดูแลระบบควรกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ตที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่ อ.อ.ป. จัดสรรไว้เท่านั้น เช่น Proxy, Firewall, IPS-IDS เป็นต้น ห้ามผู้ใช้ทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น ยกเว้นแต่ว่ามีเหตุผลความจำเป็นและทำการขออนุญาตจากฝ่ายสารสนเทศ สำนักวิจัยพัฒนาและสารสนเทศเป็นลายลักษณ์อักษร

๒.๒ เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพาก่อนทำการเชื่อมต่ออินเทอร์เน็ตผ่านเว็บบราวเซอร์ (Web Browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัสและทำการอุดช่องโหว่ของระบบปฏิบัติการเว็บบราวเซอร์

๒.๓ ในการรับส่งข้อมูลคอมพิวเตอร์ผ่านระบบอินเทอร์เน็ตจะต้องมีการทดสอบไวรัส (Virus Scanning) โดยโปรแกรมป้องกันไวรัสก่อนการรับส่งข้อมูลทุกครั้ง

๒.๔ ผู้ใช้ต้องไม่ใช้เครือข่ายอินเทอร์เน็ตของ อ.อ.ป. เพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัวและทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาที่ขัดต่อชาติ ศาสนา พระมหากษัตริย์หรือเว็บไซต์ที่เป็นภัยต่อสังคม เป็นต้น

๒.๕ ผู้ใช้จะถูกกำหนดสิทธิในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบ เพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยทางข้อมูลของหน่วยงาน

๒.๕ ผู้ใช้ต้องไม่เผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัวหรือข้อมูลที่ไม่เหมาะสมทางศีลธรรมหรือข้อมูลที่ละเมิดสิทธิของผู้อื่นหรือข้อมูลที่อาจก่อความเสียหายให้กับหน่วยงาน

๒.๖ ห้ามผู้ใช้เปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของ อ.อ.ป. ที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านอินเทอร์เน็ต

๒.๗ ผู้ใช้ไม่นำเข้าข้อมูลคอมพิวเตอร์ที่เป็นภาพของผู้อื่นและภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้นตัดต่อเติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ทั้งนี้จะทำให้ผู้อื่นนั้นเสียชื่อเสียงถูกดูหมิ่นถูกเกลียดชังหรือได้รับความอับอาย

๒.๘ หลังจากใช้งานอินเทอร์เน็ตเสร็จแล้วให้ทำการปิดเว็บบราวเซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น

ส่วนที่ ๑๗
แนวทางการใช้งานจดหมายอิเล็กทรอนิกส์
(Use of Electronic Mail)

๑. วัตถุประสงค์

๑.๑ เพื่อให้การรับส่งข้อมูลข่าวสารด้วยจดหมายอิเล็กทรอนิกส์ของ อ.อ.ป. สามารถสนับสนุนการปฏิบัติงานของ อ.อ.ป. และการบริหารงานของ อ.อ.ป.เป็นไปอย่างถูกต้อง สะดวก รวดเร็ว ทันสถานการณ์ มีประสิทธิภาพและประสิทธิผล

๑.๒ เพื่อให้การติดต่อสื่อสารโดยการรับ-ส่งข้อมูลข่าวสารด้วยจดหมายอิเล็กทรอนิกส์ สำหรับบุคลากรของ อ.อ.ป.เป็นมาตรฐาน อยู่ในกรอบของกฎหมาย ระเบียบ คำสั่ง ข้อบังคับของ อ.อ.ป.

๒. แนวทางปฏิบัติในการส่งจดหมายอิเล็กทรอนิกส์

๒.๑ ผู้ดูแลระบบต้องกำหนดสิทธิการเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของ อ.อ.ป. ให้เหมาะสมกับการเข้าใช้บริการของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของผู้ใช้รวมทั้งมีการทบทวนสิทธิการเข้าใช้งานอย่างสม่ำเสมอ เช่น การาลาออก เป็นต้น

๒.๒ ผู้ดูแลระบบต้องกำหนดสิทธิบัญชีรายชื่อผู้ใช้รายใหม่และรหัสผ่านสำหรับการใช้งานครั้งแรกเพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ระบบจดหมายอิเล็กทรอนิกส์ของ อ.อ.ป.

๒.๓ สำหรับผู้ใช้รายใหม่จะได้รับรหัสผ่านครั้งแรก (Default Password) ในการเข้าระบบจดหมายอิเล็กทรอนิกส์และเมื่อมีการเข้าสู่ระบบในครั้งแรกนั้นระบบจะต้องมีการบังคับให้เปลี่ยนรหัสผ่านโดยทันที

๒.๔ รหัสจดหมายอิเล็กทรอนิกส์เวลาใส่รหัสผ่านต้องไม่ปรากฏหรือแสดงรหัสผ่านออกมา แต่ต้องแสดงออกมาในรูปแบบของสัญลักษณ์แทนตัวอักษรนั้น เช่น “X” หรือ “O” ในการพิมพ์แต่ละตัวอักษร

๒.๕ ผู้ดูแลระบบควรกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิดได้ไม่เกิน ๓ ครั้ง

๒.๖ ผู้ดูแลระบบควรกำหนดให้ระบบจดหมายอิเล็กทรอนิกส์ควรมีการ Log Out ออกจากหน้าจอตัดการใช้งาน เมื่อผู้ใช้ไม่ได้ใช้งานระบบเป็นระยะเวลาตามที่กำหนดไว้ เช่น ๑๕ นาที เมื่อต้องการเข้าใช้งานต่อต้องใส่ชื่อผู้ใช้และรหัสผ่านอีกครั้ง

๒.๗ ผู้ใช้ไม่ควรตั้งค่าการใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) ของระบบจดหมายอิเล็กทรอนิกส์

๒.๘ ผู้ใช้ควรมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ควรเปลี่ยนรหัสผ่านทุก ๓-๖ เดือน

๒.๙ ผู้ใช้ควรระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์เพื่อไม่ให้เกิดความเสียหายต่อ อ.อ.ป. หรือละเมิดสิทธิ์ สร้างความรำคาญต่อผู้อื่นหรือผิดกฎหมายหรือละเมิดศีลธรรมและไม่แสวงหาประโยชน์หรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจจากการใช้จดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายของ อ.อ.ป.

๒.๑๐ ผู้ใช้ไม่ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-Mail Address) ของผู้อื่นเพื่ออ่านรับส่งข้อความยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้งานและให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานต่างๆ ในจดหมายอิเล็กทรอนิกส์ของตน

๒.๑๑ ผู้ใช้ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ของ อ.อ.ป.เพื่อการทำงานของ อ.อ.ป.เท่านั้น

๒.๑๒ หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้นควรทำการ Log Out ออกจากระบบทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าช้านจดหมายอิเล็กทรอนิกส์

๒.๑๓ ผู้ใช้ควรทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนทำการเปิดเพื่อทำการตรวจสอบไฟล์โดยใช้โปรแกรมป้องกันไวรัสเป็นการป้องกันในการเปิดไฟล์ที่เป็น Executable File เช่น .exe .com เป็นต้น

๒.๑๔ ผู้ใช้ไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

๒.๑๕ ผู้ใช้ไม่ควรใช้ข้อความที่ไม่สุภาพหรือรับส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสมอันอาจทำให้เสียชื่อเสียงของ อ.อ.ป.

๒.๑๖ ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์

๒.๑๗ ผู้ใช้ควรตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ของตนเองทุกวันและควรจัดเก็บแฟ้มข้อมูลและจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจำนวนน้อยที่สุด

๒.๑๘ ผู้ใช้ควรลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้เนื้อที่ระบบจดหมายอิเล็กทรอนิกส์

ส่วนที่ ๑๘
ข้อตกลงการใช้บริการจดหมายอิเล็กทรอนิกส์
(Terms of Use and Disclaimer)

๑. วัตถุประสงค์

๑.๑ เพื่อให้การรับส่งข้อมูลข่าวสารด้วยจดหมายอิเล็กทรอนิกส์ของ อ.อ.ป. สามารถสนับสนุนการปฏิบัติงานของหน่วยงานเป็นไปอย่างถูกต้อง สะดวก รวดเร็ว ทันสถานการณ์ มีประสิทธิภาพ

๑.๒ เพื่อให้การติดต่อสื่อสารโดยการรับ -ส่งข้อมูลข่าวสารด้วยระบบจดหมายอิเล็กทรอนิกส์สำหรับบุคลากรของหน่วยงานเป็นมาตรฐานอยู่ในกรอบของกฎหมาย ระเบียบ คำสั่ง ข้อบังคับ คำแนะนำ และมาตรการรักษาความปลอดภัยข้อมูลข่าวสารของ อ.อ.ป.

๒. ข้อตกลงและเงื่อนไขการใช้บริการจดหมายอิเล็กทรอนิกส์ของ อ.อ.ป.

๒.๑ ผู้ใช้บริการระบบจดหมายอิเล็กทรอนิกส์ของ อ.อ.ป.จะต้องไม่กระทำการอันละเมิดต่อกฎหมาย ระเบียบ คำสั่ง ข้อบังคับ คำแนะนำ อย่างน้อยดังต่อไปนี้

๒.๑.๑ พระราชบัญญัติกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐

๒.๑.๒ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.๒๕๔๔

๒.๑.๓ พระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ.๒๕๔๐

๒.๑.๔ ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.๒๕๔๔

๒.๑.๕ ระเบียบว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ.๒๕๑๗

๒.๑.๖ ระเบียบรักษาความปลอดภัยด้านการสื่อสาร พ.ศ.๒๕๒๕

๓. ข้อตกลงและเงื่อนไขการใช้บริการจดหมายอิเล็กทรอนิกส์ของอ.อ.ป.

๓.๑ หน่วยงาน/บุคคลผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ของอ.อ.ป.จะต้องใช้จดหมายอิเล็กทรอนิกส์ของอ.อ.ป. เพื่อผลประโยชน์ของทางราชการ

๓.๒ ห้ามใช้ระบบจดหมายอิเล็กทรอนิกส์ของอ.อ.ป. เพื่อการประกอบธุรกิจหรือแสวงหาผลประโยชน์ส่วนตน

๓.๓ ห้ามใช้บริการนี้ไปในการเผยแพร่ อ้างอิง พาดพิง ดูหมิ่น หรือการกระทำใดๆ ที่ก่อให้เกิดความเสียหายต่อสถาบัน ชาติ ศาสนา และพระมหากษัตริย์

๓.๔ ห้ามใช้ระบบจดหมายอิเล็กทรอนิกส์ขององค์กรในการประกอบอาชญากรรมทางคอมพิวเตอร์ หรือการกระทำการใดๆ ซึ่งผิดกฎหมาย คำสั่ง ระเบียบ ข้อบังคับ และมาตรการรักษาความปลอดภัย ข้อมูลความลับของทางราชการ

๓.๕ ห้ามใช้ระบบจดหมายอิเล็กทรอนิกส์ขององค์กร เพื่อการเผยแพร่ข้อมูลข่าวสารหรือภาพ เสียง ข้อความ ที่ไม่เหมาะสม หรือสร้างความเสื่อมเสียให้กับผู้อื่น

๓.๖ ห้ามใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-Mail Address) ไปแสดงข้อคิดเห็นส่วนตัวที่ส่งผลกระทบในทางลบหรือสร้างความเสื่อมเสียหรือเสียหายต่อบุคคลหรือ อ.อ.ป.

๓.๗ ห้ามกระทำการปลอมแปลงที่อยู่เป็นบุคคลอื่น (Impersonation)

๓.๘ ห้ามกระทำการที่สร้างปัญหาการใช้ทรัพยากรของระบบ เช่น

(๑) การสร้างจดหมายลูกโซ่ (Chain mail)

(๒) การส่งจดหมายจำนวนมาก (Spam mail)

(๓) การส่งจดหมายต่อเนื่อง (Letter bomb)

(๔) การส่งจดหมายเพื่อการแพร่กระจายไวรัสคอมพิวเตอร์

๓.๙ ห้ามผู้ใช้บริการกระทำการใดๆ ที่อาจจะนำมาซึ่งความเสื่อมเสีย หรือก่อให้เกิดความเสียหายแก่ระบบเครื่องแม่ข่ายจดหมายอิเล็กทรอนิกส์ของอ.อ.ป.

๓.๑๐ ผู้ใช้ต้องรักษารหัสผ่าน (Password) ส่วนบุคคลหรือหน่วยงานของจดหมายอิเล็กทรอนิกส์ไว้เป็นความลับ

๓.๑๑ การส่งข้อมูลข่าวสารอันเป็นความลับของทางราชการให้กับบุคคลหรือหน่วยงานที่ไม่เกี่ยวข้องกับราชการของอ.อ.ป.

๓.๑๒ การส่งข้อมูลข่าวสารที่เป็นความลับของทางราชการให้กับบุคคลหรือหน่วยงานนอกอ.อ.ป. จะต้องเข้ารหัสข้อมูลข่าวสารนั้นตามวิธีปฏิบัติและมาตรการรักษาความปลอดภัยข้อมูลข่าวสารตามที่อ.อ.ป. กำหนด

๓.๑๓ ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-Mail Address) และรหัสผ่าน (Password) ของหน่วยงานหรือบุคคลจะต้องเก็บรักษาไว้เป็นความลับ หากสงสัยว่ารั่วไหลจะต้องดำเนินการเปลี่ยนรหัสผ่านทันที โดยรหัสผ่านจะต้องกำหนดให้ยากแก่การคาดเดา (Strong Password)

๓.๑๔ ผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ของอ.อ.ป.หรือผู้รับผิดชอบที่อยู่จดหมายอิเล็กทรอนิกส์จะต้องศึกษาคู่มือการใช้งาน ระเบียบปฏิบัติ คำแนะนำ และข้อตกลงเงื่อนไขให้เข้าใจเพื่อใช้งานจดหมายอิเล็กทรอนิกส์ของอ.อ.ป.ได้อย่างถูกต้อง

๓.๑๕ กรณีได้รับการร้องเรียน ร้องขอ หรือพบเหตุอันไม่ชอบด้วยกฎหมาย ขอสงวนสิทธิ์ที่จะทำการยกเลิก หรือระงับบริการแก่สมาชิกนั้นๆ เป็นการชั่วคราวหรือเพื่อทำการสอบสวน และตรวจสอบหาสาเหตุของมูลเหตุนั้นๆ

๓.๑๖ การกระทำใดๆ ที่เกี่ยวกับการเผยแพร่ ทั้งในรูปแบบอีเมล์ และ/หรือโฮมเพจของผู้ใช้บริการ ให้ถือเป็นการกระทำที่อยู่ภายใต้ความรับผิดชอบของผู้ใช้บริการ ฝ่ายสารสนเทศ สำนักวิจัยพัฒนาและสารสนเทศไม่มีส่วนเกี่ยวข้องใดๆ