แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ
กรมเจ้าท่า

๑. บทนำ

๑.๑ หลักการ

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ ภาครัฐ พ.ศ. ๒๕๔๙ ในมาตรา ๕ “หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้” และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ กำหนดให้หน่วยงานของรัฐต้องต้องจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร นั้น

เพื่อใหระบบเทคโนโลยีสารสนเทศของกรมเจ้าท่าหรือตอไปนี้เรียกวา “กรม” เปนไปอยางเหมาะสมมีประสิทธิภาพมีความมั่นคงปลอดภัย และสามารถดำเนินงานไดอยางตอเนื่อง รวมทั้งปองกันปัญหาหาที่อาจจะเกิดขึ้นจากการใชงานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไมถูกตอง และการถูกคุกคามจากภัยตางๆ กรมจึงเห็นสมควรกำหนดนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศโดยกำหนดใหมีมาตรฐาน แนวปฏิบัติ ขั้นตอนปฏิบัติ ใหครอบคลุมดานการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ตามพระราชกฤษฎีกาฯ และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ฯ โดยมีวัตถุประสงคดังตอไปนี้

๑.๑. การจัดทำนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อใหเกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใชงานระบบเทคโนโลยีสารสนเทศและการสื่อสาร หรือเครือขายคอมพิวเตอรของกรมทำใหดำเนินงานไดอยางมีประสิทธิภาพและประสิทธิผล

๑.๒. เป็นบรรทัดฐานด้านความมั่นคงปลอดภัยในการดำเนินกิจการอันเกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศและการสื่อสาร

๑.๓. กำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร อางอิงตามมาตรฐาน ISO/IEC ๒๗๐๐๑ และมีการปรับปรุงอยางตอเนื่อง

๑.๔. นโยบายนี้จะตองทำการเผยแพรใหเจาหนาที่ทุกระดับในกรมไดรับทราบและเจาหนาที่ทุกคนจะตองถือปฏิบัติตามนโยบายนี้อยางเครงครัด

๑.๕. เพื่อกำหนดมาตรฐานแนวทางปฏิบัติและวิธีปฏิบัติใหผูบริหารเจาหนาที่ผูดูแลระบบ และบุคคลภายนอกที่ปฏิบัติงานใหกับกรมตระหนักถึงความสำคัญของการรักษาความมั่นคง ปลอดภัยในการใชงานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมในการดำเนินงานและปฏิบัติตามอยางเครงครัด

๑.๖. เพื่อใช้เป็นหลักในการพัฒนาและปรับปรุงคุณภาพด้านความมั่นคงปลอดภัยสารสนเทศ

๑.๗. นโยบายนี้ตองมีการดำเนินการตรวจสอบและประเมินนโยบายตามระยะเวลา ๑ ครั้งตอป

๒. องคประกอบของนโยบาย

คำนิยาม

ส่วนที่ ๑ การบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

ส่วนที่ ๒ การควบคุมการเขาออกหองควบคุมระบบคอมพิวเตอร์

ส่วนที่ ๓ การควบคุมการเขาถึงระบบเทคโนโลยีสารสนเทศ

ส่วนที่ ๔ การบริหารจัดการการเข้าถึงของผู้ใช้งาน

ส่วนที่ ๕ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน

ส่วนที่ ๖ การควบคุมการเข้าถึงและใช้บริการระบบเครือข่าย

ส่วนที่ ๗ การควบคุมการเข้าถึงระบบปฏิบัติการ

ส่วนที่ ๘ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ

ส่วนที่ ๙ การจัดทำระบบสำรองข้อมูล

ส่วนที่ ๑๐ การตรวจสอบและประเมินความเสี่ยง

ส่วนที่ ๑๑ นโยบายความมั่นคงปลอดภัยของการใช้งานอินเตอร์เน็ต

ส่วนที่ ๑๒ แนวทางการใชงานจดหมายอิเล็กทรอนิกส

ส่วนที่ ๑๓ ข้อตกลงการใชบริการจดหมายอิเล็กทรอนิกส

ส่วนที่ ๑๔ การควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ

ส่วนที่ ๑๕ นโยบายการรักษาความมั่นคงปลอดภัยของเครือข่ายไร้สาย (Wireless Policy)

การดำเนินการตอบสนองเหตุการณ์ความมั่นคงปลอดภัยทางระบบสารสนเทศ

องคประกอบของนโยบายการการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของกรมแตละสวนที่กลาวขางตนจะประกอบดวยวัตถุประสงครายละเอียดของมาตรฐาน (Standard) แนวทางปฏิบัติ (Guideline) และขั้นตอนวิธีการปฏิบัติ (Procedure) ในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของกรมเพื่อที่จะทำใหกรมมีมาตรการในการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศอยูในระดับที่ปลอดภัย ชวยลดความเสียหายตอการดำเนินงานทรัพย์สินบุคลากรของกรม ทำใหสามารถดำเนินงานไดอยางมั่นคงปลอดภัย นโยบายการเขาใชงานระบบเทคโนโลยีสารสนเทศของกรมนี้จัดเปนมาตรฐานดานความปลอดภัยในการใชงานระบบเทคโนโลยีสารสนเทศของกรม ซึ่งเจาหนาที่ของกรม และหนวยงานภายนอกตองปฏิบัติตามอยางเครงครัด

คำนิยาม

คำนิยามที่ใชในนโยบายนี้

๑. **กรม** หมายถึง กรมเจ้าท่า

๒. **การรักษาความมั่นคงปลอดภัย** หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมเจ้าท่า

๓. **ผู้ใชงาน** หมายถึง บุคคลที่ไดรับอนุญาต (Authorized user) ใหสามารถเขาใชงานบริหารหรือดูแลรักษา ระบบเทคโนโลยีสารสนเทศของกรมเจ้าท่าโดยมีสิทธิและหน้าที่ขึ้นอยูกับบทบาท (role)

- ผู้บริหารระดับสูงสุด (Chief Executive Office : CEO) หมายความว่า อธิบดีกรมเจ้าท่า
- ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Office :CIO) หมายความว่า รองอธิบดีกรมเจ้าท่าที่รับผิดชอบด้านเทคโนโลยีสารสนเทศ
- เจ้าหน้าที่ หมายความว่า ข้าราชการ พนักงานราชการ ลูกจ้างชั่วคราว ลูกจ้างประจำ
- บุคคลภายนอก หมายความว่า บุคคลที่กรมเจ้าท่าอนุญาตให้เข้ามาใช้ระบบเทคโนโลยีสารสนเทศของกรมเจ้าท่า ได้ชั่วคราวเพื่อประโยชน์ในการดำเนินงานของกรมเจ้าท่า ได้แก่ พนักงานหรือลูกจ้างบริษัทภายนอกที่เข้ามาติดต่อหรือดูแลรักษาระบบให้กับกรมเจ้าท่า หรือที่ปรึกษา หรือผู้ปฏิบัติงานตามสัญญาจ้าง

๔. **สิทธิของผู้ใช้งาน** หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใด ที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน

๕. **สินทรัพย์** หมายถึง ขอมูลระบบขอมูลและทรัพย์สินดานเทคโนโลยีสารสนเทศและการสื่อสาร หรือสิ่งใดก็ตามที่มีคุณค่าของหนวยงาน เชนอุปกรณระบบเครือขายซอฟตแวรที่มีลิขสิทธิเปนตน

๖. **การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ** หมายความว่า การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์ และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

๗. **ความมั่นคงปลอดภัยด้านสารสนเทศ** หมายถึง การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (authenticity) ความรับผิด (accountability) การห้ามปฏิเสธความรับผิด (non-repudiation) และความน่าเชื่อถือ (reliability)

๘. **ความมั่นคงปลอดภัยด้านการบริหารจัดการ** หมายถึง การกระทำในระดับบริหารโดยการจัดให้มีนโยบาย มาตรการ หลักเกณฑ์ หรือกระบวนการใดๆ เพื่อนำมาใช้ในกระบวนการคัดเลือก การพัฒนา การนำไปใช้งาน หรือการบำรุงรักษาทรัพย์สินสารสนเทศให้มีความมั่นคงปลอดภัย

๙. **ความมั่นคงปลอดภัยทางด้านกายภาพ** หมายถึง การจัดให้มีนโยบาย มาตรการหลักเกณฑ์ หรือกระบวนการใดๆ เพื่อนำมาใช้ในการป้องกันทรัพย์สินสารสนเทศ สิ่งปลูกสร้าง หรือทรัพย์สินอื่นใดจากการคุกคามของบุคคล ภัยธรรมชาติ อุบัติภัย หรือภัยทางกายภาพอื่น

๑๐. **เหตุการณ์ด้านความมั่นคงปลอดภัย** หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิด การฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

๑๑. **<u>สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด</u>** หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (unwanted or unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยคุกคาม

๑๒. **<u>หนวยงานภายนอก</u>** หมายถึง องคกรหรือหนวยงานที่กรมเจ้าท่าอนุญาตใหมีสิทธิในการเขาถึงและใชงานขอมูลหรือทรัพย์สินตางๆ ของหนวยงานโดยจะไดรับสิทธิในการใชงานตามอำนาจและตองรับผิดชอบในการรักษาความลับของขอมูล

๑๓. **<u>รหัสผาน</u>** (Password) หมายถึง ตัวอักษรหรืออักขระหรือตัวเลขที่ใชเปนเครื่องมือในการตรวจสอบยืนยันตัวบุคคลเพื่อควบคุมการเขาถึงขอมูลและระบบขอมูลในการรักษาความมั่นคงปลอดภัยของขอมูลและระบบเทคโนโลยีสารสนเทศ

๑๔. **<u>ขอมูลคอมพิวเตอร</u>** หมายถึง ขอมูลขอความคำสั่งชุดคำสั่งหรือสิ่งอื่นใดที่อยูในระบบคอมพิวเตอร ในสภาพที่ระบบคอมพิวเตอรอาจประมวลผลได และใหหมายความรวมถึงขอมูลอิเล็กทรอนิกส ตามกฎหมายวาดวยธุรกรรมทางอิเล็กทรอนิกส์

๑๕. **<u>ระบบเครือขาย</u>** (Network System) หมายถึง ระบบที่สามารถใชในการติดตอสื่อสารหรือการสงขอมูลและสารสนเทศระหวางระบบเทคโนโลยีสารสนเทศตางๆของกรมได เชนระบบแลน (LAN) ระบบอินทราเน็ต (Intranet) ระบบอินเตอรเน็ต (Internet)

- ระบบแลน (LAN) และระบบอินทราเน็ต (Intranet) หมายถึง ระบบเครือขายอิเล็กทรอนิกสที่เชื่อมตอ ระบบคอมพิวเตอรตางๆภายในหนวยงานเขาดวยกันเปนเครือขายที่มีจุดประสงค เพื่อการติดตอสื่อสารแลกเปลี่ยนขอมูลและสารสนเทศภายในหนวยงาน
- ระบบอินเตอรเน็ต (Internet) หมายถึง ระบบเครือขายอิเล็กทรอนิกสที่เชื่อมตอระบบเครือขายคอมพิวเตอรตางๆของหนวยงานเขากับเครือขายอินเตอรเน็ตทั่วโลก

๑๖. **<u>ระบบเทคโนโลยีสารสนเทศ</u>** (Information Technology System) หมายถึง ระบบงานของหนวยงานที่นำเอาเทคโนโลยีสารสนเทศระบบคอมพิวเตอรและระบบเครือขาย มาชวยในการสรางสารสนเทศที่หนวยงานสามารถนำมาใชประโยชนในการวางแผนบริหารการสนับสนุนการใหบริการการพัฒนา และควบคุมการติดตอสื่อสารซึ่งมีองคประกอบเชนระบบคอมพิวเตอรระบบเครือขายโปรแกรมขอมูลและสารสนเทศเปนตน

๑๗. **<u>พื้นที่ใชงานระบบเทคโนโลยีสารสนเทศและการสื่อสาร</u>** (Information System Workspace) หมายถึง พื้นที่ที่หนวยงานอนุญาตใหมีการใชงานระบบเทคโนโลยีสารสนเทศและการสื่อสารโดยแบงเปน

- พื้นที่ทำงานทั่วไป (General working area) หมายถึง พื้นที่ติดตั้งเครื่องคอมพิวเตอรสวนบุคคล
- พื้นที่ติดตั้งอุปกรณระบบเทคโนโลยีสารสนเทศหรือระบบเครือขาย (IT equipment or network area)
- พื้นที่จัดเก็บขอมูลคอมพิวเตอร (Data storage area)

๑๘. **<u>เจาของขอมูล</u>** หมายถึง ผูไดรับมอบอำนาจจากผูบังคับบัญชาใหรับผิดชอบขอมูลของระบบงานโดยเจาของขอมูลเปนผูรับผิดชอบขอมูลนั้นๆหรือไดรับผลกระทบโดยตรงหากขอมูลเหลานั้นเกิดสูญหาย

๑๙. **<u>จดหมายอิเล็กทรอนิกส</u>** (e-mail) หมายถึง ระบบที่บุคคลใชในการรับสงขอความระหวางกัน โดยผานเครื่องคอมพิวเตอรและเครือขายที่เชื่อมโยงถึงกันขอมูลที่สงจะเปนไดทั้ง ตัวอักษร ภาพถาย ภาพกราฟก ภาพเคลื่อนไหว และเสียง ผูสงสามารถสงขาวสารไปยังผูรับคนเดียวหรือหลายคนก็ได

๒๐. **<u>ชุดคำสั่งไมพึงประสงค</u>** หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นเกิดความเสียหายถูกทำลายถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติมขัดของหรือปฏิบัติงาน ไมตรงตามคำสั่งที่กำหนดไว

ส่วนที่ ๑
การบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ
(Information Security Management)

๑. วัตถุประสงค

เพื่อกำหนดผู้รับผิดชอบที่ชัดเจน ในการดูแลกรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดการเสียหาย หรืออันตรายใดๆ แก่กรมเจ้าท่า ในการหาแนวทาง ทบทวนแนวนโยบายและแนวปฏิบัติไปใช้ในการแก้ปัญหาที่เกิดขึ้น และนำไปสู่การปรับปรุงการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศให้มีคุณภาพต่อไป

๒. แนวทางในการบริหารจัดการ

๒.๑. ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Office : CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นจากการละเลยการควบคุม ความมั่นคงปลอดภัยสารสนเทศกรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใดๆ แก่กรมฯ หรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยจัดให้มีการประชุมคณะกรรมการพัฒนาบริหารจัดการระบบสารสนเทศ โดยผู้บริหารสารสนเทศระดับสูง และผู้อำนวยการสำนัก/ศูนย์/กลุ่ม เพื่อทำการทบทวนและทราบถึงแนวนโยบายและแนวปฏิบัติ การรักษาความมั่นคงปลอดภัยด้านสารสนเทศ อย่างน้อยปีละ๑ ครั้ง ส่วนผู้บริหารสารสนเทศระดับสูง (CIO) เป็นผู้กำกับดูแลรับผิดชอบด้านสารสนเทศของกรมเจ้าท่า

๒.๒. ทำความเข้าใจ และให้การสนับสนุนการปฏิบัติตามนโยบายความมั่นคงปลอดภัยสารสนเทศ โดยจัดให้มีการทำรายงานการประชุมผู้บริหารสารสนเทศและแจ้งเป็นแนวปฏิบัติให้เจ้าหน้าที่ผู้เกี่ยวข้องรับทราบและปฏิบัติตามอย่างเคร่งครัด

๒.๓. จัดให้มีการทบทวนปรับปรุงนโยบายและข้อปฏิบัติให้เป็นปัจจุบันอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง เพื่อให้สอดคล้องกับการเปลี่ยนแปลงและแนวโน้มของความเสี่ยงในอนาคตที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยทางด้านสารสนเทศของกรมเจ้าท่า

๒.๔. จัดให้มีการประเมินแนวปฏิบัติความมั่นคงปลอดภัยสารสนเทศ เพื่อนำไปปรับปรุงให้มีประสิทธิภาพในปีถัดไป

๒.๕. กำหนดนโยบายความมั่นคงปลอดภัยสารสนเทศต้องจัดทำเป็นลายลักษณ์อักษรตามวัตถุประสงค์ของขอบเขตงานที่ได้รับการอนุมัติจากผู้บริหารระดับสูงสุด (CEO) หรือผู้บริหารสารสนเทศระดับสูง (CIO) เพื่อประกาศใช้และถือปฏิบัติในกรมเจ้าท่า โดยให้มีผลบังคับใช้กับบุคลากรในทุกระดับชั้นของกรมเจ้าท่า ตลอดจนบุคคลภายนอกที่เกี่ยวข้องกับการใช้ข้อมูลและสินทรัพย์สารสนเทศของกรมเจ้าท่า

๒.๖. จัดให้มีทรัพยากรด้านบุคลากร งบประมาณ การบริหารจัดการ และวัตถุดิบที่พอเพียงต่อการบริหารจัดการด้านความมั่นคงปลอดภัยในแต่ละปีงบประมาณซึ่งรวมถึงแผนความมั่นคงปลอดภัยสารสนเทศที่จะดำเนินการในปีงบประมาณนั้นด้วย

๒.๗. จัดให้มีการอบรมให้ความรู้ เพื่อสร้างความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศให้กับข้าราชการ พนักงานราชการ และเจ้าหน้าที่ เพื่อสร้างความตระหนักและความเข้าใจภัยและ

ผลกระทบที่จะเกิดขึ้น จากการใช้ระบบงานสารสนเทศโดยไม่ระมัดระวังหรือไม่เท่าถึงการณ์ อย่างน้อยปีละ ๑ ครั้ง

๒.๘. จัดให้มีการตรวจสอบและประเมินความเสี่ยงในการปฏิบัติ ปีละ ๑ ครั้งและจัดให้มีการทำแผนการปรับปรุง เพื่อทบทวนหรือแก้ไขปัญหาที่พบ

๒.๙. จัดให้มีการอบรมให้ความรู้และซักซ้อมแผนฉุกเฉินภัยพิบัติของประเทศของระบบเทคโนโลยีสารสนเทศ (IT Contingence plan) อย่างน้อยปีละ ๑ ครั้ง

๒.๑๐. กำหนดหน้าที่ที่ต้องทบทวนปรับปรุงนโยบายและข้อปฏิบัติให้เป็นปัจจุบันอยู่เสมอ และกำหนดหน้าที่รับผิดชอบของบุคลากรที่เกี่ยวข้องด้านความมั่นคงปลอดภัยสารสนเทศ และแผนฉุกเฉินภัยพิบัติของระบบเทคโนโลยีสารสนเทศของกรมเจ้าท่า

๒.๑๑. ผู้บริหาร ต้องกำหนดและแบ่งแยกบริเวณพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารให้ชัดเจน โดยการกำหนดพื้นที่ดังกล่าวอาจแบ่งออกได้เป็น พื้นที่ทำงานทั่วไป (General working area) พื้นที่ทำงานของผู้ดูแลระบบ (System administrator area) พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศ (IT Equipment area) พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data storage area) และ พื้นที่ใช้งานเครือข่ายไร้สาย (Wireless LAN coverage area) เป็นต้น

ส่วนที่ ๒
การควบคุมการเขาออกหองควบคุมระบบคอมพิวเตอร์
(Computing System Control Room)

๑. วัตถุประสงค

เพื่อกำหนดเปนมาตรการควบคุมและปองกัน เพื่อการรักษาความมั่นคงปลอดภัยที่เกี่ยวของกับการเขาใชงาน หรือการเขาถึงห้องควบคุมระบบเครื่องคอมพิวเตอร์ อุปกรณ์เครือข่าย และระบบเทคโนโลยีสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ ระบบเทคโนโลยีสารสนเทศ ขอมูลซึ่งเปนทรัพย์สินที่มีคาและอาจจำเปนตองรักษาความลับโดยมาตรการนี้ จะมีผลบังคับใชกับผูใชซึ่งมีสวนเกี่ยวของกับการใชงานระบบเทคโนโลยีสารสนเทศของกรม

๒. การควบคุมการเขาออก

๒.๑. ภายในกรมมีการติดตั้งระบบควบคุมการเข้าออกอัตโนมัติ (Acess Control System) เพื่อควบคุมการเข้าออกห้องควบคุมเครื่องคอมพิวเตอร์แม่ข่าย โดยจำแนกและกำหนดพื้นที่การติดตั้งระบบควบคุมการเข้าออกอัตโนมัติ (Acess Control System) เป็น ๓ ส่วน โดยส่วนที่ ๑ เป็นการติดตั้งระบบควบคุมการเข้าออกอัตโนมัติ (Acess Control System) บริเวณทางเข้าศูนย์คอมพิวเตอร์ ส่วนที่ ๒ เป็นการติดตั้งระบบควบคุมการเข้าออกอัตโนมัติ (Acess Control System) ห้องควบคุมเครื่องคอมพิวเตอร์แม่ข่าย และส่วนที่ ๓ เป็นการติดตั้งระบบควบคุมการเข้าออกอัตโนมัติ (Acess Control System) ห้อง Facility เพื่อจุดประสงคในการควบคุมการเข้าออกของบุคคลภายนอก โดยใช้เทคโนโลยีระบบ Biometric Finger Scan และ Proximity Card

๒.๒. ภายในกรมมีการติดตั้งระบบกล้องวงจรปิด เพื่อจุดประสงคในการเฝาระวังควบคุมการรักษาความมั่นคงปลอดภัย จากผู้ที่ไมไดรับอนุญาตรวมทั้งปองกันความเสียหายอื่นๆที่อาจเกิดขึ้นได

๒.๓. ตองกำหนดสิทธิใหกับเจาหนาที่ใหสามารถมีมีสิทธิในการเขาถึงพื้นที่เพื่อปฏิบัติหนาที่ตามที่ไดรับมอบหมายประกอบดวย

๒.๓.๑. จัดทำ “ทะเบียนผูมีสิทธิเขาออกพื้นที่” เพื่อปฏิบัติหนาที่ตามสิทธิและหน้าที่ที่ไดรับมอบหมาย

๒.๓.๒. กำหนดผูมีหนาที่รับผิดชอบการบันทึกการเขา-ออก ดังกลาวโดยจัดทำเปนเอกสาร“บันทึกการเขาออกพื้นที่”

๒.๓.๓. จัดใหมีเจาหนาที่ทำหนาที่ตรวจสอบประวัติการเขาออกพื้นที่ใชงานระบบเทคโนโลยีสารสนเทศเปนประจำ และใหมีการปรับปรุงรายการผูมีสิทธิเขาออกพื้นที่ใชงานระบบสารสนเทศและการสื่อสาร ปละ ๑ ครั้ง เป็นอย่างน้อย

๒.๔. บุคคลภายนอกเขามาติดตอจะตองลงชื่ออนุญาตการเขาออกในแบบฟอรมการเขา-ออกใหถูกตองและจะตองอยูกับบุคคลที่มาติดตอตลอดเวลา

๒.๕. บุคคลอื่นที่ไม่มีหน้าที่เกี่ยวข้องขอเขาพื้นที่ หนวยงานเจาของพื้นที่ตองตรวจสอบเหตุผลและความจำเปนกอนที่จะอนุญาต

สวนที่ ๓
การควบคุมการเขาถึงระบบเทคโนโลยีสารสนเทศ
(Access Control)

๑. วัตถุประสงค

เพื่อกำหนดมาตรการควบคุมบุคคลที่ไมไดอนุญาตเขาถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมและปองกันการบุกรุกผานระบบเครือขายจากผูบุกรุกจากโปรแกรมชุดคำสั่งไมพึงประสงคที่จะสรางความเสียหายแกขอมูลหรือการทำงานของระบบเทคโนโลยีสารสนเทศและการสื่อสารใหหยุดชะงักและทำใหสามารถตรวจสอบติดตามพิสูจนตัวบุคคลที่เขาใชงานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรม ไดอยางถูกตอง

๒. กระบวนการหลักในการควบคุมการเขาถึงระบบ

๒.๑. สถานที่ตั้งของระบบเทคโนโลยีสารสนเทศ ที่สำคัญตองมีการควบคุมการเขาออกที่รัดกุมและอนุญาตใหเฉพาะบุคคลที่ไดรับสิทธิและมีความจำเปนผานเขาใชงานไดเทานั้น

๒.๒. ผูดูแลระบบตองกำหนดสิทธิการเขาถึงขอมูลและระบบขอมูลใหเหมาะสมกับการเขาใชงานของผูใชระบบและหนาที่ความรับผิดชอบของเจาหนาที่ในการปฏิบัติงานกอนเขาใชระบบเทคโนโลยีสารสนเทศและการสื่อสารรวมทั้งมีการทบทวนสิทธิการเขาถึงอยางสม่ำเสมอทั้งนี้ ผูใชระบบจะตองไดรับอนุญาตจากผูดูแลระบบตามความจำเปนในการใชงาน

๒.๓. ผูดูแลระบบหรือผูที่ไดรับมอบหมายเทานั้นที่สามารถแกไขเปลี่ยนแปลงสิทธิการเขาถึงขอมูลและระบบขอมูลได

๒.๔. ผูดูแลระบบควรจัดใหมีการติดตั้งระบบบันทึกและติดตามการใชงานระบบเทคโนโลยีสารสนเทศของกรมและตรวจตราการละเมิดความปลอดภัยที่มีตอระบบขอมูลสำคัญ

๒.๕. ผูดูแลระบบตองจัดใหมีการบันทึกรายละเอียดการเขาถึงระบบการแกไขเปลี่ยนแปลงสิทธิตางๆ และ การผานเขาออกสถานที่ตั้งของระบบของทั้งผูที่ไดรับอนุญาตและไมไดรับอนุญาตเพื่อเปนหลักฐานในการตรวจสอบหากมีปญหาเกิดขึ้น

๓. การควบคุมการเขาถึงระบบเทคโนโลยีสารสนเทศ

๓.๑. ผูดูแลระบบมีหนาที่ในการตรวจสอบการอนุมัติและกำหนดสิทธิในการผานเขาสูระบบใหแกผูใชในการขออนุญาตเขาระบบงานนั้นจะตองมีการทำเปนเอกสารเพื่อขอสิทธิในการเขาสูระบบและกำหนดใหมีการลงนามอนุมัติเอกสารดังกลาวตองมีการจัดเก็บไวเปนหลักฐาน

๓.๒. เจาของขอมูลและ เจาของระบบงาน จะอนุญาตใหผูใชงานเขาสูระบบเฉพาะในสวนที่จำเปนตองรูตามหนาที่งานเทานั้นเนื่องจากการให้สิทธิเกินความจำเปนในการใชงานจะนำไปสูความเสี่ยงในการใชงานเกินอำนาจหนาที่ดังนั้นการกำหนดสิทธิในการเขาถึงระบบงาน ตองกำหนดตามความจำเปนขั้นต่ำเทานั้น

๓.๓. ผูใชงานจะตองไดรับอนุญาตจากเจาหนาที่ที่รับผิดชอบขอมูลและระบบงานตามความจำเปนตอการใชงานระบบเทคโนโลยีสารสนเทศ

๔. การบริหารจัดการการเขาถึงของผูใช

๔.๑. การลงทะเบียนเจาหนาที่ใหมของกรมควรกำหนดใหมีขั้นตอนปฏิบัติอยางเปนทางการ สำหรับการลงทะเบียนเจาหนาที่ใหมเพื่อใหมีสิทธิตางๆในการใชงานตามความจำเปนรวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใชงาน เชนเมื่อลาออกไปตองทำภายใน ๒๔ ชั่วโมงหรือ เมื่อเปลี่ยนตำแหนงงานภายในตองทำภายใน ๗ วัน

๔.๒. กำหนดสิทธิการใชระบบเทคโนโลยีสารสนเทศที่สำคัญ เชน ระบบคอมพิวเตอรโปรแกรมประยุกต (Application) จดหมายอิเล็กทรอนิกส (e-mail) ระบบอินเตอรเน็ต เปนตน โดยตองให้สิทธิเฉพาะการปฏิบัติงานในหนาที่และตองไดรับความเห็นชอบจากผูดูแลระบบเปนลายลักษณอักษร รวมทั้งตองทบทวนสิทธิดังกลาวอยางสม่ำเสมอ

๔.๓. ผูใชตองลงนามรับทราบสิทธิ และหนาที่เกี่ยวกับการใชงานระบบเทคโนโลยีสารสนเทศเปนลายลักษณอักษรและตองปฏิบัติตามอยางเครงครัด

๔.๔. การบริหารจัดการบัญชีรายชื่อผูใชงาน (User account) และรหัสผานของเจาหนาที่

๔.๔.๑.ผูดูแลระบบที่รับผิดชอบระบบงานนั้นๆตองกำหนดสิทธิของเจาหนาที่ในการเขาถึงระบบเทคโนโลยีสารสนเทศแตละระบบรวมทั้งกำหนดสิทธิแยกตามหนาที่ที่รับผิดชอบซึ่งมีแนวทางปฏิบัติตามที่กำหนดไวในเอกสาร“การบริหารจัดการการเข้าถึงของผู้ใช้งาน”

๔.๔.๒.การกำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผานตองปฏิบัติตาม“การบริหารจัดการการเข้าถึงของผู้ใช้งาน”

๔.๔.๓.กรณีมีความจำเปนตองให้สิทธิพิเศษกับผูใช หมายถึง ผูใชที่มีสิทธิสูงสุดตองมีการพิจารณาการควบคุมผูใชที่มีสิทธิพิเศษนั้นอยางรัดกุมเพียงพอโดยใชปจจัยตอไปนี้ประกอบการพิจารณา

๔.๔.๓.๑. ควรไดรับความเห็นชอบจากผูดูแลระบบงานนั้นๆ โดยนำเสนอผู้บังคับบัญชาอนุมัติ

๔.๔.๓.๒. ควรควบคุมการใชงานอยางเขมงวดเชน กำหนดให้ใชงานเฉพาะกรณีที่จำเปนเทานั้น

๔.๔.๓.๓. ควรกำหนดระยะเวลาการใชงานและระงับการใชงานทันที เมื่อพนระยะเวลาดังกลาว

๔.๔.๓.๔. ควรมีการเปลี่ยนรหัสผานอยางเครงครัด เชน ทุกครั้งหลังหมดความจำเปนในการใชงาน หรือในกรณีที่มีความจำเปนตองใชงานเปนระยะเวลานานก็ควรเปลี่ยนรหัสผานทุก ๓ เดือนเปนตน

๔.๕. การบริหารจัดการการเขาถึงขอมูลตามระดับชั้นความลับ

๔.๕.๑. ผูดูแลระบบตองกำหนดชั้นความลับของขอมูลวีธีปฏิบัติในการจัดเก็บขอมูลและวิธีปฏิบัติในการควบคุมการเขาถึงขอมูลแตละประเภทชั้นความลับทั้งการเขาถึงโดยตรงและการเขาถึงผานระบบงานรวมถึงวิธีการทำลายขอมูลแตละประเภทชั้นความลับ

๔.๕.๒. เจาของขอมูลจะตองมีการสอบทานความเหมาะสมของสิทธิในการเขาถึงขอมูลของผูใชงานเหลานี้ อยางนอยปละ ๑ ครั้ง เพื่อใหมั่นใจไดวาสิทธิตางๆ ที่ใหไวยังคงมีความเหมาะสม

๔.๕.๓. วิธีปฏิบัติในการควบคุมการเขาถึงขอมูลแตละประเภทชั้นความลับทั้งการเขาถึงโดยตรงและการเขาถึงผานระบบงานผูดูแลระบบตองกำหนดรายชื่อผูใชงาน (User account) และรหัสผาน (Password) เพื่อใชในการตรวจสอบตัวตนจริงของผูใชขอมูลในแตละชั้นความลับของขอมูล

๔.๕.๔. การรับสงขอมูลสำคัญผานเครือขายสาธารณะควรไดรับการเขารหัส (Encryption) ที่เปนมาตรฐานสากล

๔.๕.๕. ควรมีการกำหนดใหเปลี่ยนรหัสผานตามระยะเวลาที่กำหนดของระดับความสำคัญของขอมูลตามที่ระบุไวในเอกสาร“การบริหารจัดการการเข้าถึงของผู้ใช้งาน”

๔.๕.๖. ควรมีมาตรการรักษาความมั่นคงปลอดภัยของขอมูลในกรณีที่นำเครื่องคอมพิวเตอรออกนอกพื้นที่ของกรม เชน สงเครื่องคอมพิวเตอรไปตรวจซอม ควรสำรองและลบขอมูลที่เก็บอยูในสื่อ บันทึกกอน เปนตน

๕. การบริหารจัดการการเขาถึงระบบเครือขาย

๕.๑. ผูดูแลระบบตองมีการออกแบบระบบเครือขายตามกลุมของบริการระบบเทคโนโลยีสารสนเทศที่มีการใชงานกลุมของผูใช และกลุมของระบบสารสนเทศ เชน โซนภายใน (Internal zone) โซนภายนอก (External zone) เปนตน เพื่อทำใหการควบคุมและปองกันการบุกรุกได้อยาง เปนระบบ

๕.๒. ผูดูแลระบบตองมีวิธีการจำกัดสิทธิการใชงาน เพื่อควบคุมผูใชใหสามารถใชงานเฉพาะเครือขายที่ได รับอนุญาตเทานั้น

๕.๓. ผูดูแลระบบควรมีวิธีการจำกัดเสนทางการเขาถึงเครือขายที่มีการใชงานรวมกัน

๕.๔. ผูดูแลระบบควรจัดใหมีวิธีเพื่อจำกัดการใชเสนทางบนเครือขาย (Enforced path) จากเครื่องลูกขายไปยังเครื่องแมขายเพื่อไมใหผูใชสามารถใชเสนทางอื่นๆได กำหนดบุคคลที่รับผิดชอบในการกำหนดแกไขหรือเปลี่ยนแปลงคา parameter ตางๆของระบบ

๕.๕. ป้องกันเครือขายและอุปกรณตางๆที่เชื่อมตอกับระบบเครือขายอยางชัดเจนและควรทบทวนการกำหนดคา Parameter ตางๆอยางนอยปละครั้ง นอกจากนี้การกำหนดแกไขหรือเปลี่ยนแปลง คา parameter ควรแจงบุคคลที่เกี่ยวของใหรับทราบทุกครั้ง

๕.๖. ระบบเครือขายทั้งหมดของกรมที่มีการเชื่อมตอไปยังระบบเครือขายอื่นๆภายนอกกรม ควรเชื่อมตอผานอุปกรณปองกันการบุกรุกหรือโปรแกรมในการทำ Packet filtering เชน การใชไฟรวอล (firewall) หรือฮารดแวรอื่นๆ รวมทั้งตองมีความสามารถในการตรวจจับมัลแวร (Malware) ดวย

๕.๗. ตองมีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใชงานของบุคคลที่เขาใชงานระบบเครือขายของกรม ในลักษณะที่ผิดปกติผานระบบเครือขาย โดยมีการตรวจสอบการบุกรุกผานระบบเครือขายการใชงานในลักษณะที่ผิดปกติ และการแกไขเปลี่ยนแปลงระบบเครือขาย โดยบุคคลที่ไมมีอำนาจหน้าที่เกี่ยวของ

๕.๘. การเขาสูระบบงานเครือขายภายในกรมโดยผานทางอินเทอรเน็ต จำเปนตองมีการลอกอิน และตองมีการพิสูจนยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกตอง

๕.๙. IP address ภายในของระบบงานเครือขายภายในของกรม จำเปนตองมีการปองกันมิใหหนวยงานภายนอกที่เชื่อมตอสามารถมองเห็นได เพื่อเปนการปองกันไมใหบุคคลภายนอกสามารถรูขอมูลเกี่ยวกับโครงสรางของระบบเครือขายไดโดยงาย

๕.๑๐. ตองจัดทำแผนผังระบบเครือขาย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือขายภายใน และเครือขายภายนอกและอุปกรณตางๆ พรอมทั้งปรับปรุงใหเปนปจจุบันอยูเสมอ

๕.๑๑. การใชเครื่องมือตางๆ (Tools) เพื่อการตรวจสอบระบบเครือขายควรไดรับการอนุมัติจากผูดูแลระบบ และจำกัดการใชงานเฉพาะเทาที่จำเปน

๕.๑๒. การติดตั้งและการเชื่อมตออุปกรณเครือขายจะตองดำเนินการโดยเจาหน้าที่กลุ่มเทคโนโลยีสารสนเทศ สำนักแผนงานเทานั้น

๖. การบริหารจัดการระบบคอมพิวเตอรแมขาย

๖.๑. ควรกำหนดบุคคลที่รับผิดชอบในการดูแลระบบคอมพิวเตอรแมขาย (Server) ในการกำหนดแกไขหรือ เปลี่ยนแปลงคาตางๆของโปรแกรมระบบ (System Software) อยางชัดเจน

๖.๒. ตองมีขั้นตอนหรือวิธีปฏิบัติในการตรวจสอบระบบคอมพิวเตอรแมขายและในกรณีที่พบวามีการใชงาน หรือเปลี่ยนแปลงคาในลักษณะผิดปกติ จะตองดำเนินการแกไขรวมทั้งมีการรายงานโดยทันที

๖.๓. ตองเปดใชบริการ (Service) เทาที่จำเปนเทานั้นเชน Telnet ftp หรือ ping เปนตน ทั้งนี้หากบริการที่จำเปนตองใชมีความเสี่ยงตอระบบรักษาความปลอดภัยแลวตองมีมาตรการเพิ่มเติมดวย

๖.๔. ควรดำเนินการติดตั้งอัพเดทระบบซอฟตแวรใหเปนปจจุบันเพื่ออุดชองโหวตางๆของโปรแกรมระบบ (System Software) อยางสม่ำเสมอ เชน web server เปนตน

๖.๕. ควรมีการทดสอบโปรแกรมระบบ (System Software) เกี่ยวกับการรักษาความปลอดภัยและประสิทธิภาพ การใชงานโดยทั่วไปกอนติดตั้งและหลังจากการแกไขหรือบำรุงรักษา

๖.๖. การติดตั้งและการเชื่อมตอระบบคอมพิวเตอรแมขายจะตองดำเนินการโดยเจาหนาที่กลุ่มเทคโนโลยีสารสนเทศเท่านั้น

๗. การบริหารจัดการการบันทึกและตรวจสอบ

๗.๑. ควรกำหนดใหมีการบันทึกการทำงานของระบบคอมพิวเตอรแมขายและเครือขายบันทึกการปฏิบัติงานของผูใชงาน (Application logs) และบันทึกรายละเอียดของระบบปองกันการบุกรุก เชน บันทึกการเขาออกระบบ บันทึกการพยายามเขาสูระบบ บันทึกการใชงาน command line และ firewall log เปนตน เพื่อประโยชนในการใชตรวจสอบและตองเก็บบันทึกดังกลาวไวอยางนอย ๓ เดือน

๗.๒. ควรมีการตรวจสอบบันทึกการปฏิบัติงานของผูใชงานอยางสม่ำเสมอ

๗.๓. ตองมีมีวิธีการปองกันการแกไขเปลี่ยนแปลงบันทึกตางๆและจำกัดสิทธิการเขาถึงบันทึกเหลานั้นใหเฉพาะบุคคลที่เกี่ยวของเทานั้น

๘. การควบคุมการเขาใชงานระบบจากภายนอก

ตองกำหนดใหมีการควบคุมการใชงานระบบที่ ผูดูแลระบบไดติดตั้งไวภายในองคกรเพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอกโดยมีแนวทางปฏิบัติดังนี้

๘.๑. การเขาสูระบบระยะไกล (Remote access) สูระบบเครือขายของกรม ตองควบคุมบุคคลที่จะเขาสูระบบของกรม จากระยะไกลโดยกำหนดมาตรการการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเขาสูระบบภายใน

๘.๒. วิธีการใดๆก็ตามที่สามารถเขาถึงขอมูลหรือระบบขอมูลจากระยะไกลตองไดรับการอนุมัติจากหัวหน้ากลุ่มเทคโนโลยีสารสนเทศ หรือผู้อำนวยการ สำนักแผนงาน กอน และมีการควบคุมอยางเขมงวดกอนนำมาใช และผูใชตองปฏิบัติตามขอกำหนดของกรมในการเขาสูระบบและขอมูลอยางเครงครัด

๘.๓. การทำการให้สิทธิในการเขาสูระบบจากระยะไกลผูใชตองแสดงหลักฐานระบุเหตุผลหรือความจำเปนในการดำเนินงานกับองคกรอยางเพียงพอและตองไดรับอนุมัติจากผูมีอำนาจอยางเปนทางการ

๘.๔. ตองมีการควบคุม Port ที่ใชในการเขาสูระบบอยางรัดกุม

๘.๕. การอนุญาตให้ผู้ใช้เข้าสู่ระบบข้อมูลจากระยะไกลต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้นและไม่ควรเปิดพอร์ตทิ้งไว้โดยไม่จำเป็น ช่องทางดังกล่าวควรตัดการเชื่อมต่อเมื่อไม่ได้งานแล้ว และจะเปิดให้ใช้ได้ เมื่อมีการร้องขอที่จำเป็นเท่านั้น

๙. การพิสูจน์ตัวตนสำหรับผู้ใช้ที่อยู่ภายนอก

๙.๑. ผู้ใช้ระบบทุกคนเมื่อจะเข้าใช้งานระบบต้องผ่านการพิสูจน์ตัวตนจากระบบขององค์กรดังนี้

๙.๑.๑. แสดงชื่อผู้ใช้งาน (Username)

๙.๑.๒. ใส่รหัสผ่าน (Password)

ส่วนที่ ๔
การบริหารจัดการการเข้าถึงของผู้ใช้งาน
(User Access Management)

๑. วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการการเข้าถึงระบบเทคโนโลยีสารสนเทศของผู้ใช้งาน มิให้บุคคลที่ไม่มีหน้าที่ที่เกี่ยวข้องในการทำงานเข้าถึงระบบเทคโนโลยีสารสนเทศและเครือข่ายภายในโดยไม่ได้รับอนุญาต รวมทั้งจำกัดสิทธิในการใช้งานระบบเทคโนโลยีสารสนเทศ เพื่อให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรม

๒. การลงทะเบียนผู้ใช้งาน (User Registration)

๒.๑. จัดทำแบบฟอร์มการลงทะเบียนผู้ใช้งาน สำหรับระบบเทคโนโลยีสารสนเทศของกรม

๒.๒. ผู้ดูแลระบบต้องตรวจสอบบัญชีผู้ใช้งาน โดยเฉพาะผู้ที่ไม่มีการลงทะเบียนผู้ใช้งานมาก่อน

๒.๓. ผู้ดูแลระบบต้องตรวจสอบและให้สิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ

๒.๔. ผู้ดูแลระบบต้องกำหนดให้มีการแจกเอกสารหรือสิ่งที่แสดงเป็นลายลักษณ์อักษรให้แก่ผู้ใช้งานเพื่อแสดงถึงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งานในการเข้าถึงระบบเทคโนโลยีสารสนเทศ รวมทั้งกำหนดให้ผู้ใช้งานทำการลงนามในเอกสารดังกล่าวหลังจากที่ได้ทำความเข้าใจแล้ว

๒.๕. ผู้ดูแลระบบต้องกำหนดให้มีการถอดถอนสิทธิการเข้าถึงระบบเทคโนโลยีสารสนเทศโดยทันทีเมื่อผู้ใช้งานนั้นทำการลาออกหรือเปลี่ยนตำแหน่งงาน

๒.๖. การลงทะเบียนผู้ใช้งาน ผู้ดูแลระบบต้องทำการตรวจสอบหรือทบทวนบัญชีผู้ใช้งานทั้งหมด เพื่อป้องกันการเข้าถึงระบบเทคโนโลยีสารสนเทศโดยไม่ได้รับอนุญาต

๓. การบริหารจัดการสิทธิของผู้ใช้งาน (User Management)

๓.๑. ผู้ดูแลระบบต้องกำหนดสิทธิการใช้ระบบเทคโนโลยีสารสนเทศ โดยให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

๓.๒. ผู้ดูแลระบบต้องกำหนดระดับสิทธิในการเข้าถึงที่เหมาะสมสำหรับระบบเทคโนโลยีสารสนเทศ

๓.๓. ผู้ดูแลระบบต้องมอบหมายสิทธิควรมีความสอดคล้องกับนโยบายควบคุมการเข้าถึง

๓.๔. ผู้ดูแลระบบต้องจัดเก็บการมอบหมายสิทธิให้แก่ผู้ใช้งาน

๓.๕. กรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

๔. การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management)

๔.๑. ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานลงนามเพื่อป้องกันการเปิดเผยข้อมูลรหัสผ่านของตน เช่น ลงนามในเอกสารเพื่อแสดงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งานในการเข้าถึงระบบเทคโนโลยีสารสนเทศของกรม

๔.๒. ผู้ดูแลระบบต้องกำหนดขั้นตอนปฏิบัติสำหรับการตั้งหรือเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัย

๔.๓. ผู้ดูแลระบบต้องให้ผู้ใช้งานเปลี่ยนรหัสผ่านโดยทันที ภายหลังจากที่ได้รับรหัสผ่านชั่วคราว และควรเปลี่ยนรหัสผ่านที่มีความยากต่อการเดาโดยผู้อื่น

๔.๔. ผู้ดูแลระบบต้องกำหนดรหัสผ่านชั่วคราว โดยกำหนดรหัสผ่านให้มีความยากต่อการเดาโดยผู้อื่น และควรกำหนดรหัสผ่านที่แตกต่างกัน

๔.๕. ผู้ดูแลระบบต้องจัดส่งรหัสผ่านให้ผู้ใช้งาน โดยหลีกเลี่ยงการใช้อีเมล์เป็นช่องทางในการส่ง และควรกำหนดให้ผู้ใช้งานตอบกลับหลังจากที่ได้รับรหัสผ่านแล้ว

๕. การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review Of User Access Rights)

๕.๑. ผู้ดูแลระบบดำเนินการทบทวนสิทธิการเข้าถึงของผู้ใช้งาน ๑ ครั้ง / ปี เป็นอย่างน้อย

๕.๒. ผู้ดูแลระบบทบทวนสิทธิสำหรับผู้ที่มีสิทธิในระดับสูง เช่น สิทธิในระดับผู้ดูแลระบบ ด้วยความถี่ที่มากกว่าผู้ใช้งานทั่วไป

๕.๓. ผู้ดูแลระบบทบทวนสิทธิตามรอบระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงใดๆ เช่น การเลื่อนตำแหน่ง ลดตำแหน่ง ย้ายหน่วยงาน หรือสิ้นสุดการจ้างงาน

๕.๔. ผู้ดูแลระบบต้องกำหนดให้มีการบันทึกการเปลี่ยนแปลงต่อบัญชีผู้ใช้งานที่มีสิทธิในระดับสูง เพื่อใช้ในการทบทวนในภายหลัง

ส่วนที่ ๕
การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน
(User Responsibilities)

๑. วัตถุประสงค์

เพื่อควบคุมและกำหนดมาตรการ การปฏิบัติงานของผู้ใช้งานให้เป็นไปตามหน้าที่ที่ได้รับมอบหมายที่เกี่ยวข้องกับข้อมูลสารสนเทศ และบังคับใช้กับผู้ที่ใช้งานระบบเทคโนโลยีสารสนเทศของกรม เพื่อป้องกันการเข้าถึงข้อมูลโดยบุคคลอื่นและเปิดเผยข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต

๒. การใช้งานรหัสผ่าน (Password Use)

ผู้ใช้งานระบบเทคโนโลยีสารสนเทศควรปฏิบัติตามข้อกำหนดในการใช้งานรหัสผ่าน ดังนี้

๒.๑. ผู้ใช้งานควรตั้งรหัสผ่านที่ยากต่อการเดาโดยผู้อื่น

๒.๒. ผู้ใช้งานไม่เปิดเผยรหัสผ่านของตนเอง

๒.๓. ผู้ใช้งานควรจัดเก็บรหัสผ่านไว้ในสถานที่ที่มีความปลอดภัย

๒.๔. ผู้ใช้งานควรเปลี่ยนรหัสผ่านโดยทันทีเมื่อทราบว่ารหัสผ่านของตนอาจถูกเปิดเผยหรือล่วงรู้โดยผู้อื่น

๒.๕. ผู้ใช้งานควรตั้งรหัสผ่านที่มีความยาวเกินกว่าขั้นต่ำกำหนดไว้

๒.๖. ผู้ใช้งานควรตั้งรหัสผ่านที่มีเทคนิคที่ง่ายต่อการจดจำ

๒.๗. ผู้ใช้งานไม่ควรตั้งรหัสผ่านจากคำที่ปรากฏในพจนานุกรม

๒.๘. ผู้ใช้งานควรหลีกเลี่ยงการตั้งรหัสผ่านที่ประกอบด้วยอักขระที่เรียงกัน เช่น ๑๒๓ , abcd หรือกลุ่มของตัวอักขระที่เหมือนกัน เช่น ๑๑๑ , aaa เป็นต้น

๒.๙. ผู้ใช้งานควรเปลี่ยนรหัสผ่านตามรอบระยะเวลาที่กำหนด

๒.๑๐. ผู้ใช้งานควรเปลี่ยนรหัสผ่านโดยไม่ใช้รหัสผ่านเดิมที่เคยตั้งมาแล้ว

๒.๑๑. ผู้ดูแลระบบควรเปลี่ยนรหัสผ่านด้วยความถี่ที่มากกว่าผู้ใช้งานทั่วไป เช่น ทุกๆ ๓ เดือน สำหรับผู้ดูแล และ ๖ เดือน สำหรับผู้ใช้งานระบบ

๒.๑๒. ผู้ใช้งานควรเปลี่ยนรหัสผ่านชั่วคราวที่ได้รับโดยทันทีครั้งแรกที่ทำการล๊อคอินเข้าสู่ระบบงาน

๒.๑๓. ผู้ใช้งานไม่ควรกำหนดให้ทำการบันทึกรหัสผ่านหรือจดจำรหัสผ่านของตนเองไว้ เพื่อความสะดวกของตนเองเมื่อทำการล๊อคอินในภายหลัง

๒.๑๔. ผู้ใช้งานไม่ควรใช้รหัสผ่านของตนร่วมกับผู้อื่น

๒.๑๕. ผู้ใช้งานควรหลีกเลี่ยงการใช้รหัสผ่านเดียวกันสำหรับระบบงานต่างๆ ที่ใช้งาน

๓. การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์

๓.๑ ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานออกจากระบบเทคโนโลยีสารสนเทศโดยทันทีเมื่อเสร็จสิ้นงาน เช่น ระบบงาน เครื่องคอมพิวเตอร์ที่ใช้งาน หรือเครื่องโน๊ตบุ๊ก

๓.๒ ผู้ใช้งานควรล๊อคอุปกรณ์ที่สำคัญเมื่อไม่ได้ใช้งานหรือปล่อยทิ้งไว้โดยไม่ได้ดูแลชั่วคราว

๓.๓ ผู้ดูแลระบบควรกำหนดให้พนักงานป้องกันผู้อื่นเข้าใช้เครื่องคอมพิวเตอร์หรือระบบเทคโนโลยีสารสนเทศของตนโดยใส่รหัสผ่านได้ถูกต้องก่อนเข้าใช้งานเครื่องคอมพิวเตอร์

ส่วนที่ ๖
การควบคุมการเข้าถึงและใช้บริการระบบเครือข่าย
(Network Access Control)

๑. วัตถุประสงค

เพื่อกำหนดมาตรการควบคุมปองกันมิใหบุคคลที่ไมมีอำนาจหนาที่เกี่ยวของในการปฏิบัติหนาที่เขาถึงลวงรู แกไขเปลี่ยนแปลงระบบเครือข่ายและการสื่อสารที่สำคัญซึ่งจะทำใหเกิดความเสียหายต่อข้อมูลและระบบสารสนเทศของกรมโดยมีการกำหนดกระบวนการควบคุมการเขาใช้งานเครือข่ายที่แตกตางกันของกลุมเครือข่ายตางๆ ตามการแบ่งแยกเครือข่ายเป็น VLAN

๒. กระบวนการควบคุมการเข้าถึงและใช้บริการระบบเครือข่าย

๒.๑ การใช้งานบริการเครือข่าย

๒.๑. ห้ามผู้ใช้งานกระทำการใด ๆ เกี่ยวกับข้อมูลที่เป็นการขัดต่อกฎหมาย หรือศีลธรรมอันดีแห่งสาธารณชน โดยผู้ใช้งานรับรองว่าหากมีการกระทำการใด ๆ ดังกล่าว ย่อมถือว่าอยู่นอกเหนือความรับผิดชอบของกรม

๒.๒. กรม ไม่อนุญาตให้ผู้ใช้งานกระทำการใด ๆ ที่เข้าข่ายลักษณะเพื่อการค้าหรือการแสวงหาผลกำไรผ่านเครื่องคอมพิวเตอร์และ เครือข่าย เช่น การประกาศแจ้งความ การซื้อหรือการจำหน่ายสินค้า การนำข้อมูลไปซื้อขาย การรับบริการค้นหาข้อมูลโดยคิดค่าบริการ การให้บริการโฆษณาสินค้าหรือการเปิดบริการอินเทอร์เน็ตแก่บุคคลทั่วไปเพื่อ แสวงหากำไร

๒.๓. ผู้ใช้งานจะต้องไม่ละเมิดต่อผู้อื่น คือ ผู้ใช้งานจะต้องไม่อ่าน เขียน ลบ เปลี่ยนแปลงหรือแก้ไขใด ๆ ในส่วนที่มิใช่ของตนโดยไม่ได้รับอนุญาต การบุกรุก (Hack) เข้าสู่บัญชีผู้ใช้งาน (User Account) ของผู้อื่น การเผยแพร่ข้อความใด ๆ ที่ก่อให้เกิดความเสียหายเสื่อมเสียแก่ผู้อื่น การใช้ภาษาไม่สุภาพหรือการเขียนข้อความที่ทำให้ผู้อื่นเสียหาย ถือเป็นการละเมิดสิทธิของผู้อื่นทั้งสิ้น ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงฝ่ายเดียว กรมฯ ไม่มีส่วนร่วมรับผิดชอบความเสียหายดังกล่าว

๒.๔. ห้ามมิให้ผู้ใดเข้าใช้งานโดยมิได้รับอนุญาต การบุกรุกหรือพยายามบุกรุกเข้าสู่ระบบถือว่าเป็นการพยายามรุกล้ำเขตหวงห้าม ของทางราชการ

๒.๕. กรม ให้บัญชีผู้ใช้งาน (User Account) เป็นการเฉพาะบุคคลเท่านั้น ผู้ใช้งานจะโอนหรือจ่ายแจกสิทธินี้ให้กับผู้อื่นไม่ได้

๒.๖. บัญชีผู้ใช้งาน (User Account) ที่กรมฯ ให้กับผู้ใช้งานนั้น ผู้ใช้งานต้องเป็นผู้รับผิดชอบผลต่างๆ อันอาจจะเกิดมีขึ้น รวมถึงผลเสียหายต่างๆที่เกิดจากบัญชีผู้ใช้งาน (User Account) นั้นๆ เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

๒.๒. ผูดูแลระบบหองควบคุมระบบเครือขายและเจาหนาที่กรมมีแนวทางปฏิบัติดังนี้

๒.๒.๑. ผูดูแลระบบหองควบคุมระบบเครือขายตองทำการกำหนดสิทธิบุคคลในการเขาออกหองควบคุม ระบบเครือขายโดยเฉพาะบุคคลที่ปฏิบัติหนาที่เกี่ยวของภายในและมีการบันทึก

“ทะเบียนผูมีสิทธิเขาออกพื้นที่” เชน เจาหนาที่ปฏิบัติงานคอมพิวเตอร (Computer Operator) เจาหนาที่ผูดูและระบบ (System Administrator) เปนตน

๒.๒.๒. สิทธิในการเขาออกหองตางๆภายในหองควบคุมระบบเครือขายของเจาหนาที่แตละคน ตองไดรับการอนุมัติจากหัวหน้ากลุ่มเทคโนโลยีและสารสนเทศ เปนลายลักษณอักษรโดยสิทธิของเจาหนาที่แตละคนขึ้นอยูกับหนาที่การปฏิบัติงานภายหองควบคุมระบบเครือขาย

๒.๒.๓. ผู้ดูแลระบบห้องควบคุมระบบเครือข่าย จัดเก็บลายนิ้วมือเจ้าหน้าที่ผ่านเครื่องจัดเก็บลายนิ้วมือ และบันทึกข้อมูลลงคีย์การ์ด เพื่อบันทึกประวัติการเข้า-ออก ห้องควบคุมระบบเครือข่ายของเจ้าหน้าที่

๒.๒.๔.กรณีเจาหนาที่ที่ไมมีหนาที่เกี่ยวของประจำมีความจำเปนตองเขาออกหองควบคุมระบบเครือขายตองทำการติดต่อผู้ดูแลระบบห้องควบคุมระบบเครือข่าย เพื่อเข้าห้องควบคุมระบบเครือข่าย พร้อมทั้งระบุเหตุผลการเข้าห้องควบคุมระบบเครือข่าย

๒.๒.๕. ผู้ดูแลระบบห้องควบคุมระบบเครือข่าย ต้องทำการแจ้งเจ้าหน้าที่ที่ไม่มีหน้าที่เกี่ยวข้องหลังจากดำเนินการเสร็จ ให้แจ้งผู้ดูแลระบบห้องควบคุมระบบเครือข่ายเพื่อตรวจสอบความเรียบร้อยและความถูกต้อง

๒.๓. ผู้ติดต่อจากหนวยงานภายนอกมีแนวทางปฏิบัติดังนี้

๒.๓.๑. ผู้ติดต่อจากหนวยงานภายนอกตองทำการติดต่อผู้ดูแลระบบห้องควบคุมระบบเครือข่าย เพื่อเข้าห้องควบคุมระบบเครือข่าย พร้อมทั้งระบุเหตุผลการเข้าห้องควบคุมระบบเครือข่าย

๒.๓.๒. ผู้ดูแลระบบห้องควบคุมระบบเครือข่าย ต้องทำการแจ้งผู้ติดต่อจากหน่วยงานภายนอกหลังจากดำเนินการเสร็จ ให้แจ้งผู้ดูแลระบบห้องควบคุมระบบเครือข่ายเพื่อตรวจสอบความเรียบร้อยและความถูกต้อง

ส่วนที่ ๗
การควบคุมการเข้าถึงระบบปฏิบัติการ
(Operating System Access Control)

๑. วัตถุประสงค์

เพื่อให้ผู้ใช้งาน ได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้ระบบปฏิบัติการ รวมทั้งทำความเข้าใจตลอดจนปฏิบัติตามอย่างเคร่งครัด อันจะเป็นการป้องกันทรัพยากรและข้อมูลของหน่วยงานให้มีความลับ ความถูกต้องและมีความพร้อมใช้งานอยู่เสมอ

๒. การกำหนดขั้นตอนการปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย

๒.๑. ผู้ใช้งานควรกำหนดรหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ที่รับผิดชอบ

๒.๒. ผู้ใช้งานควรตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ (Screen saver) เพื่อทำการล็อคหน้าจอภาพเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้บริการต้องใส่รหัสผ่าน (Password) เพื่อเข้าใช้งาน

๒.๓. ก่อนการเข้าใช้ระบบปฏิบัติการต้องใส่ User และ Password ทุกครั้ง

๒.๔. ผู้ใช้งานไม่ควรอนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ของหน่วยงานร่วมกัน

๒.๕. ผู้ใช้งานควรทำการลงบันทึกออก (Logout) ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

๓. การระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication)

๓.๑ ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนใช้ระบบเทคโนโลยีสารสนเทศ เพื่อป้องกันผู้ไม่มีสิทธิเข้าใช้งานระบบเทคโนโลยีสารสนเทศ หากการระบุและยืนยันตัวตนของผู้ใช้งานมีปัญหา หรือเกิดความผิดพลาด ผู้ใช้งานแจ้งให้ผู้ดูแลระบบทำการแก้ไข

๓.๒ ผู้ใช้งานที่เป็นเจ้าของบัญชีผู้ใช้บริการ (Account) ต้องเป็นผู้รับผิดชอบในผลต่าง ๆ อันจะเกิดขึ้นจากการใช้บัญชีผู้ใช้บริการ (Account) ของเครื่องคอมพิวเตอร์และระบบเครือข่าย เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

๓.๓ ผู้ใช้งานจะต้องเก็บรักษาบัญชีผู้ใช้บริการ (Account) ไว้เป็นความลับและห้ามเปิดเผยต่อบุคคลอื่น ห้ามโอน จำหน่าย หรือจ่ายแจกให้ผู้อื่น โดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

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

ส่วนที่ ๘
การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ
(Application Information Access Control)

๑. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ไดอนุญาตเขาถึงระบบสารสนเทศของกรม และปองกันการบุกรุกผานระบบเครือขายจากผูบุกรุกจากโปรแกรมชุดคำสั่งไมพึงประสงคที่จะสรางความเสียหายแกขอมูลหรือการทำงานของระบบเทคโนโลยีสารสนเทศและการสื่อสารใหหยุดชะงักและทำใหสามารถตรวจสอบติดตามพิสูจนตัวบุคคลที่เขาใชงานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรม ไดอยางถูกตอง

๒. การจำกัดการเข้าถึงสารสนเทศ (Information Access Control)

๒.๑. ผู้ดูแลระบบ (System Administrator) ต้องกำหนดการลงทะเบียนบุคลากรใหม่ของกรม ควรกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการเพื่อให้มีสิทธิต่างๆ ในการใช้งานตามความจำเป็น รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน เช่น การลาออก หรือการเปลี่ยนตำแหน่งงานภายในหน่วยงาน เป็นต้น

๒.๒. ผู้ดูแลระบบ (System Administrator) ต้องกำหนดสิทธิการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (e-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

๒.๓. ผู้ดูแลระบบ (System Administrator) ต้องบริหารจัดการสิทธิการใช้งานระบบและรหัสผ่านของบุคลากรดังต่อไปนี้

๒.๓.๑ กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบลาออก หรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน

๒.๓.๒ ส่งมอบรหัสผ่าน (Password) ชั่วคราวให้กับผู้ใช้บริการด้วยวิธีการที่ปลอดภัย ควรหลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (e-mail) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน (Password)

๒.๓.๓ กำหนดให้ผู้ใช้บริการตอบยืนยันการได้รับรหัสผ่าน (Password)

๒.๓.๔ กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

๒.๓.๕ กำหนดชื่อผู้ใช้หรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

๒.๓.๖ ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหนง และมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

๒.๔. ผู้ดูแลระบบ (System Administrator) ต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับ ในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้

๒.๔.๑ ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

๒.๔.๒ ต้องกำหนดรายชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล

๒.๔.๓ กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

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

๒.๔.๕ กำหนดการเปลี่ยนรหัสผ่าน (Password) ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

๒.๔.๖ กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของหน่วยงาน เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

ส่วนที่ ๙

การจัดทำระบบสำรองข้อมูล

๑.วัตถุประสงค์

เพื่อกำหนดข้อปฏิบัติการสำรองข้อมูลและกู้คืนระบบ โดยมีวัตถุประสงค์เพื่อให้ผู้ดูแลระบบคอมพิวเตอร์และเครือข่ายสามารถดำเนินการสำรองข้อมูล ได้อย่างถูกต้องและสามารถกู้คืนระบบได้ในกรณีที่จำเป็น

๒.แนวปฏิบัติงานการสำรองข้อมูลและระบบคอมพิวเตอร์

๒.๑. ผู้ดูแลระบบคอมพิวเตอร์ ต้องจัดให้มีการสำรองและทดสอบข้อมูลที่สำรองเก็บไว้อย่างสม่ำเสมอ และให้เป็นไปตามนโยบายการสำรองข้อมูลของกรม

๒.๒ การจัดทำบันทึกการสำรองข้อมูล (Operator logs) ผู้ดูแลระบบคอมพิวเตอร์ต้องทำบันทึกรายละเอียดการสำรองข้อมูล ได้แก่ เวลาเริ่มต้นและสิ้นสุด ชื่อผู้สำรอง ชนิดของข้อมูลที่บันทึก เป็นต้น

๒.๓ การรายงานข้อผิดพลาด (Fault logging) ผู้ดูแลระบบคอมพิวเตอร์ต้องทำรายงานข้อผิดพลาดจากการสำรองข้อมูลที่เกิดขึ้น รวมทั้งวิธีการที่ใช้แก้ไขด้วย

๒.๔ ให้ผู้ดูแลระบบคอมพิวเตอร์มอบหมายหน้าที่การสำรองข้อมูลแก่เจ้าหน้าที่คนอื่นไว้สำรองในกรณีที่ผู้ดูแลระบบคอมพิวเตอร์และ/หรือผู้ดูแลระบบเครือข่ายไม่สามารถปฏิบัติงานได้

๒.๕ ในกรณีที่พบปัญหาในการสำรองข้อมูลจนเป็นเหตุไม่สามารถดำเนินการอย่างสมบูรณ์ได้ให้ดำเนินการแก้ไขปัญหาและสรุปผลการแก้ไขปัญหาและรายงานต่อหัวหน้ากลุ่มเทคโนโลยีสารสนเทศ

๒.๖ ให้ผู้ดูแลระบบคอมพิวเตอร์และผู้ดูแลระบบเครือข่ายกำหนดชนิดและช่วงเวลาการสำรองข้อมูลตามความเหมาะสม พร้อมทั้งกำหนดสื่อที่ใช้เก็บข้อมูล โดยรูปแบบการสำรองข้อมูลมีสองชนิด คือ การสำรองข้อมูลแบบเต็ม (Full Backup) และการสำรองข้อมูลแบบส่วนต่าง (Incremental Backup)

๒.๗ การเข้ารหัสข้อมูลสำคัญในการสำรองข้อมูล (Encrypted backup) ผู้ดูแลระบบคอมพิวเตอร์ต้องจัดให้มีการเข้ารหัสข้อมูลสำรองที่สาคัญ โดยการใช้เทคโนโลยีการเข้ารหัสที่เหมาะสมเพื่อป้องกันมิให้ข้อมูลสำรองเหล่านั้นถูกเปิดเผย

๒.๘ นโยบายที่ต้องปฏิบัติเกี่ยวข้องกับการสำรองข้อมูล (Backup Policy) ผู้ดูแลระบบคอมพิวเตอร์ต้องปฏิบัติตามขั้นตอนปฏิบัติ Backup Procedure โดยเคร่งครัด

การปฏิบัติเกี่ยวกับการสำรองข้อมูล

๑.๑ ผู้ดูแลระบบคอมพิวเตอร์และผู้ดูแลระบบเครือข่ายต้องทำการสำรองข้อมูลแต่ละรายการ ตามความถี่ดังนี้

	รายการ	ข้อมูลที่ต้องสำรอง	ความถี่ในการสำรองข้อมูล
	Web servers	ค่า configure	ก่อนและหลังการเปลี่ยนแปลง
		ข้อมูลเผยแพร่บนเว็บไซต์	๑ ครั้งต่อสัปดาห์
	Database servers	ค่า configure	ก่อนและหลังการเปลี่ยนแปลง

	รายการ	ข้อมูลที่ต้องสำรอง	ความถี่ในการสำรองข้อมูล
		ข้อมูลในฐานข้อมูลของระบบที่สาคัญ	๑ ครั้งต่อสัปดาห์
	Firewall , Proxy , IPS , DNS , CoreSwitch	ค่า configure	ก่อนและหลังการเปลี่ยนแปลง
		ข้อมูล Rule ของอุปกรณ์	๑ ครั้งต่อเดือน
	Server อื่น ๆ เช่น ระบบงานต่างๆ	ค่า configure	ก่อนและหลังการเปลี่ยนแปลง
		ข้อมูลบนเซิร์ฟเวอร์อื่น ๆ	๑ ครั้งต่อเดือน
หมายเหตุ ทุกรายการที่ปรากฏในตารางจะใช้วิธีแบคอัพแบบ Full Backup			

๑.๒ ผู้ดูแลระบบคอมพิวเตอร์ต้องตรวจสอบผลการสำรองข้อมูลด้วยตนเองว่าการแบคอัพ ตามรายละเอียด ในตารางข้างต้นนั้นถูกต้องสมบูรณ์หรือไม่

๓. การกู้คืนระบบ

๓.๑ ในกรณีที่พบปัญหาที่อาจสร้างความเสียหายต่อระบบคอมพิวเตอร์และ/หรือระบบ เครือข่ายจนเป็นเหตุทำให้ต้องดำเนินการกู้คืนระบบ ให้ผู้ดูแลระบบคอมพิวเตอร์และ/ หรือผู้ดูแลระบบเครือข่ายดำเนินการแก้ไข รายงานผลการแก้ไขพร้อมทั้งบันทึกและให้ รายงานสรุปผลการปฏิบัติงานต่อหัวหน้ากลุ่มเทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับมอบหมายจากหัวหน้ากลุ่มเทคโนโลยีสารสนเทศทราบ

๓.๒ ให้ใช้ข้อมูลทันสมัยที่สุด (Latest Update) ที่ได้สำรองไว้หรือตามความเหมาะสมเพื่อกู้คืนระบบ

๓.๓ หากความเสียหายที่เกิดขึ้นกับระบบคอมพิวเตอร์ หรือระบบเครือข่ายกระทบต่อการให้บริการ หรือการใช้งานของผู้ใช้ระบบ ให้แจ้งผู้ใช้งานทราบทันที พร้อมทั้งรายงาน ความคืบหน้าการกู้คืนระบบเป็นระยะ จนกว่าจะดำเนินการเสร็จสิ้นอย่างสมบูรณ์

๔. การจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ ที่อาจเกิดขึ้นกับระบบฐานข้อมูลและสารสนเทศ (IT Contingency Plan)

นโยบายเกี่ยวกับการจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ ที่อาจเกิดขึ้นกับระบบฐานข้อมูลและสารสนเทศ (IT Contingency Plan) ต้องมอบหมายให้บุคลากรที่เกี่ยวข้องดำเนินการดังต่อไปนี้

๔.๑ กำหนดกระบวนการในการวางแผนรับมือกับเหตุภัยพิบัติสาหรับระบบที่มีความสำคัญสูง

๔.๒ กำหนดชนิดของภัยพิบัติที่มีผลต่อระบบที่มีความสาคัญสูงและจำเป็นต้องวางแผนรับมือ

๔.๓ ทำการประเมินความเสี่ยงที่มีผลทำให้ระบบที่มีความสำคัญสูง ติดขัดหรือไม่สามารถใช้งานได้อันเป็นผลจากภัยพิบัติที่กำหนดไว้

๔.๔ จัดทำแผนรับมือกับเหตุภัยพิบัติสาหรับระบบที่มีความสำคัญสูง

๔.๕ ทดสอบ/ประเมินและปรับปรุงแผนรับมือกับเหตุภัยพิบัติสาหรับระบบที่มีความสาคัญสูง อย่างน้อยปีละ ๑ ครั้ง

ส่วนที่ ๑๐
การตรวจสอบและประเมินความเสี่ยง

๑.วัตถุประสงค์

เพื่อให้มีมาตรการในการควบคุมความเสี่ยงและป้องกันเหตุการณ์ที่อาจมีผลต่อความมั่นคงปลอดภัยด้านสารสนเทศ

๒.แนวปฏิบัติการประเมินความเสี่ยง

๒.๑. ระบุความเสี่ยงและเหตุการณ์ความเสี่ยงให้สอดคล้องตามแผนบริหารความเสี่ยงของกรม เพื่อการประเมินความเสี่ยงนั้น

๒.๒.๑ ระบบเทคโนโลยีสารสนเทศได้รับความเสียหาย เนื่องจากเจ้าหน้าที่หรือบุคลากรของหน่วยงาน (Human error), ไวรัสคอมพิวเตอร์ (Computer Virus), ระบบไฟฟ้าขัดข้อง, ความเสียหายจากเพลิงไหม้ , โจรกรรม และการขโมยอุปกรณ์คอมพิวเตอร์

๒.๒.๒ ระบบเทคโนโลยีสารสนเทศได้รับความเสียหาย เนื่องจากเจ้าหน้าที่หรือบุคลากรของหน่วยงาน (Human error)

๒.๒ กำหนดวิธีการในการประเมินความเสี่ยงและความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงนั้น

๒.๓ การประเมินความเสี่ยงให้คำนึงถึงองค์ประกอบดังต่อไปนี้

๒.๓.๑ ความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงที่ระบุ

๒.๓.๒ ภัยคุกคามหรือสิ่งที่อาจก่อให้เกิดเหตุการณ์ที่ระบุรวมถึงความเป็นไปได้ที่จะเกิดขึ้น

๒.๓.๓ จุดอ่อนหรือช่องโหว่ที่อาจถูกใช้ในการก่อให้เกิดเหตุการณ์ที่ระบุ

๒.๔ กำหนดมาตรการจัดการความเสี่ยง

๒.๔.๑ ดำเนินการทบทวนแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจจะเกิดขึ้นกับระบบสารสนเทศ (IT Contingency Plan)

๒.๔.๒ จัดทำหลักเกณฑ์นโยบายกฎระเบียบในการใช้เครื่องคอมพิวเตอร์และเครือข่ายของกรม

ส่วนที่ ๑๑
นโยบายความมั่นคงปลอดภัยของการใช้งานอินเตอร์เน็ต
(Internet Security Policy)

๑. วัตถุประสงค

เพื่อให้ผู้ใชรับทราบกฎเกณฑแนวทางปฏิบัติในการใชงานอินเทอรเน็ตอยางปลอดภัยและเปนการปองกันไมใหละเมิดพระราชบัญญัติวาดวยการกระทำผิดเกี่ยวกับคอมพิวเตอร เชน การสงขอมูล ขอความ คำสั่งชุดคำสั่งหรือสิ่งอื่นใดที่อยูในระบบคอมพิวเตอรแกบุคคลอื่นอันเปนการรบกวนการใชระบบคอมพิวเตอรของบุคคลอื่นโดยปกติสุขทำใหระบบคอมพิวเตอรของกรมถูกระงับชะลอขัดขวางหรือถูกรบกวนจนไมสามารถทำงานตามปกติได

๒. แนวทางปฏิบัติในการใชงานอินเทอรเน็ต

๒.๑. ผูดูแลระบบควรกำหนดเสนทางการเชื่อมตอระบบคอมพิวเตอรเพื่อการเขาใชงานอินเทอรเน็ตที่ตองเชื่อมตอผานระบบรักษาความปลอดภัยที่กรมจัดสรรไวเทานั้นเชน Proxy, Firewall, IPS-IDS เปนตน หามผูใชทำการเชื่อมตอระบบคอมพิวเตอรผานชองทางอื่น ยกเวนแตวามีเหตุผลความจำเปนและทำการขออนุญาตจากกลุ่มเทคโนโลยีและสารสนเทศ สำนักแผนงาน เปนลายลักษณอักษร

๒.๒. เครื่องคอมพิวเตอรสวนบุคคลและเครื่องคอมพิวเตอรแบบพกพา กอนทำการเชื่อมตออินเทอรเน็ต ผานเว็บเบราเซอร (Web browser) ตองมีการติดตั้งโปรแกรมปองกันไวรัสและทำการอุดชองโหวของระบบปฏิบัติการเว็บเบราเซอร

๒.๓. ผู้ใช้ หมั่น Update Patch และ HotFix อย่างสม่ำเสมอ โดยสามารถ Download patch และ HotFix ต่างๆ จาก Microsoft web site เพื่อแก้ปัญหาช่องโหว่

๒.๔. ในการรับสงขอมูลคอมพิวเตอรผานทางอินเทอรเน็ตจะตองมีการทดสอบไวรัส (Virus scanning) โดยโปรแกรมปองกันไวรัสกอนการรับสงขอมูลทุกครั้ง

๒.๕. ผูใช ตองไมใชเครือขายอินเทอรเน็ตของกรม เพื่อหาประโยชนในเชิงธุรกิจสวนตัวและทำการเขาสูเว็บไซตที่ไมเหมาะสมเชนเว็บไซตที่ขัดตอศีลธรรมเว็บไซตที่มีเนื้อหาที่ขัดตอชาติ ศาสนา พระมหากษัตริยหรือเว็บไซตที่เปนภัยตอสังคม เปนตน

๒.๖. ผูใชจะถูกกำหนดสิทธิในการเขาถึงแหลงขอมูลตามหนาที่ความรับผิดชอบ เพื่อประสิทธิภาพของเครือขายและความปลอดภัยทางขอมูลของกรม

๒.๗. ผูใช ตองไมเผยแพรขอมูลที่เปนการหาประโยชนสวนตัวหรือขอมูลที่ไมเหมาะสมทางศีลธรรม หรือขอมูลที่ละเมิดสิทธิของผู้อื่นหรือขอมูลที่อาจกอความเสียหายใหกับกรม

๒.๘. หามผูใช เปดเผยขอมูลสำคัญที่เปนความลับเกี่ยวกับงานของกรมที่ยังไมไดประกาศอยางเปนทางการ ผานอินเทอรเน็ต

๒.๙. ผูใชไมนำเขาขอมูลคอมพิวเตอรที่เปนภาพของผู้อื่นและภาพนั้นเปนภาพที่เกิดจากการสรางขึ้นตัดตอเติมหรือดัดแปลงดวยวิธีการทางอิเล็กทรอนิกสหรือวิธีการอื่นใดทั้งนี้จะทำใหผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่นถูกเกลียดชังหรือไดรับความอับอาย

๒.๑๐. หลังจากใชงานอินเทอรเน็ตเสร็จแลวใหทำการปดเว็บเบราเซอรเพื่อปองกันการเขาใชงานโดยบุคคลอื่น

ส่วนที่ ๑๒
แนวทางการใชงานจดหมายอิเล็กทรอนิกส
(Use of Electronic Mail)

๑. วัตถุประสงค

๑.๑ เพื่อให้การรับส่งข้อมูลข่าวสารด้วยจดหมายอิเล็กทรอนิกส์ของกรม สามารถสนับสนุนการปฏิบัติงานของกรมเจ้าท่า และการบริหารงานของกรมเจ้าท่า เป็นไปอย่างถูกต้อง สะดวก รวดเร็ว ทันสถานการณ์ มีประสิทธิภาพ และประสิทธิผล

๑.๒ เพื่อให้การติดต่อสื่อสารโดยการรับ-ส่งข้อมูลข่าวสารด้วยจดหมายอิเล็กทรอนิกส์ สำหรับบุคลากรของกรม และหน่วยงาน เป็นมาตรฐาน อยู่ในกรอบของกฎหมาย ระเบียบ คำสั่ง ข้อบังคับ ของกรมเจ้าท่า

๒. แนวทางปฏิบัติในการสงจดหมายอิเล็กทรอนิกส

๒.๑. ผูดูแลระบบตองกำหนดสิทธิการเขาถึงระบบจดหมายอิเล็กทรอนิกสของกรมใหเหมาะสมกับการเขาใชบริการของผูใชระบบและหนาที่ความรับผิดชอบของผูใชรวมทั้งมีการทบทวนสิทธิการเขาใชงานอยางสม่ำเสมอเชน การลาออกเปนตน

๒.๒. ผูดูแลระบบตองกำหนดสิทธิบัญชีรายชื่อผูใชรายใหมและรหัสผานสำหรับการใชงานครั้งแรกเพื่อใชในการตรวจสอบตัวตนจริงของผูใชระบบจดหมายอิเล็กทรอนิกสของกรม

๒.๓. สำหรับผูใชรายใหมจะไดรับรหัสผานครั้งแรก (default password) ในการผานเขาระบบจดหมายอิเล็กทรอนิกสและเมื่อมีการเขาสูระบบในครั้งแรกนั้นระบบจะตองมีการบังคับใหเปลี่ยนรหัสผานโดยทันที

๒.๔. รหัสจดหมายอิเล็กทรอนิกสเวลาใสรหัสผานตองไมปรากฏหรือแสดงรหัสผานออกมา แตตองแสดงออกมาในรูปแบบของสัญลักษณแทนตัวอักษรนั้นเชน ‘x’ หรือ ‘o’ ในการพิมพแตละตัวอักษร

๒.๕. ผูดูแลระบบควรกำหนดจำนวนครั้งที่ยอมใหผูใชงานใสรหัสผานผิดไดไมเกิน ๓ ครั้ง

๒.๖. ผูดูแลระบบควรกำหนดใหระบบจดหมายอิเล็กทรอนิกสควรมีการล็อกเอาทออกจากหนาจอตัดการใชงานผูใชเมื่อผูใชไมไดใชงานระบบเปนระยะเวลาตามที่กำหนดไวเชน ๑๕ นาที เมื่อตองการเขาใชงานตอตองใสชื่อผูใชและรหัสผานอีกครั้ง

๒.๗. ผูใชไมควรตั้งคาการใชโปรแกรมชวยจำรหัสผานสวนบุคคลอัตโนมัติ (save password) ของระบบจดหมายอิเล็กทรอนิกส

๒.๘. ผูใชควรมีการเปลี่ยนรหัสผานอยางเครงครัดเชนควรเปลี่ยนรหัสผานทุก ๓-๖ เดือน

๒.๙. ผูใช ควรระมัดระวังในการใชจดหมายอิเล็กทรอนิกสเพื่อไมใหเกิดความเสียหายตอกรม หรือ ละเมิดสิทธิ์ สรางความรำคาญตอผู้อื่นหรือผิดกฎหมายหรือละเมิดศีลธรรมและไมแสวงหาประโยชนหรืออนุญาตใหผู้อื่นแสวงหาผลประโยชนในเชิงธุรกิจจากการใชจดหมายอิเล็กทรอนิกสผานระบบเครือขายของกรม

๒.๑๐. ผูใชไมควรใชที่อยูจดหมายอิเล็กทรอนิกส (e-mail address) ของผู้อื่นเพื่ออานรับสงขอความยกเวนแตจะไดรับการยินยอมจากเจาของผูใชและใหถือวาเจาของจดหมายอิเล็กทรอนิกสเปนผูรับผิดชอบตอการใชงานตางๆในจดหมายอิเล็กทรอนิกสของตน

๒.๑๑. ผูใชควรใชที่อยูจดหมายอิเล็กทรอนิกสของกรมเพื่อการทำงานของกรมเทานั้น

๒.๑๒. หลังจากการใชงานระบบจดหมายอิเล็กทรอนิกสเสร็จสิ้นควรทำการล็อกเอาทออกจากระบบทุกครั้ง เพื่อปองกันบุคคลอื่นเขาใชงานจดหมายอิเล็กทรอนิกส

๒.๑๓. ผูใช ควรทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกสกอนทำการเปิดเพื่อทำการตรวจสอบไฟลโดยใชโปรแกรมปองกันไวรัสเปนการปองกันในการเปดไฟลที่เปน Executable file เชน .exe .com เป็นต้น

๒.๑๔. ผูใชไมเปดหรือสงตอจดหมายอิเล็กทรอนิกสหรือข่อความที่ไดรับจากผูสงที่ไมรูจัก

๒.๑๕. ผูใชไมควรใชขอความที่ไมสุภาพหรือรับสงจดหมายอิเล็กทรอนิกสที่ไมเหมาะสมขอมูลอันอาจทำใหเสียชื่อเสียงของกรมทำใหเกิดความแตกแยกระหวางกรมผานทางจดหมายอิเล็กทรอนิกส

๒.๑๖. ในกรณีที่ตองการสงขอมูลที่เปนความลับไมควรระบุความสำคัญของขอมูลลงในหัวขอจดหมายอิเล็กทรอนิกส

๒.๑๗. ผูใช ควรตรวจสอบตูเก็บจดหมายอิเล็กทรอนิกสของตนเองทุกวันและควรจัดเก็บแฟมขอมูลและจดหมายอิเล็กทรอนิกสของตนใหเหลือจำนวนนอยที่สุด

๒.๑๘. ผูใช ควรลบจดหมายอิเล็กทรอนิกสที่ไมตองการออกจากระบบเพื่อลดปริมาณการใชเนื้อที่ระบบจดหมายอิเล็กทรอนิกส

ส่วนที่ ๑๓

ข้อตกลงการใช้บริการจดหมายอิเล็กทรอนิกส์

(Terms of Use and Disclaimer)

๑. วัตถุประสงค์

๑.๑ เพื่อให้การรับส่งข้อมูลข่าวสารด้วยจดหมายอิเล็กทรอนิกส์ของกรม สามารถสนับสนุนการปฏิบัติงานของกรม เป็นไปอย่างถูกต้อง สะดวก รวดเร็ว ทันสถานการณ์ มีประสิทธิภาพ

๑.๒ เพื่อให้การติดต่อสื่อสารโดยการรับ-ส่งข้อมูลข่าวสารด้วยระบบจดหมายอิเล็กทรอนิกส์ สำหรับบุคลากรของ กรม และหน่วยงาน เป็นมาตรฐาน อยู่ในกรอบของกฎหมาย ระเบียบ คำสั่ง ข้อบังคับ คำแนะนำ และมาตรการรักษาความปลอดภัยข้อมูลข่าวสารของกรมเจ้าท่า

๒. ข้อตกลงและเงื่อนไขการใช้บริการจดหมายอิเล็กทรอนิกส์ของกรม

๒.๑ ผู้ใช้บริการระบบจดหมายอิเล็กทรอนิกส์ของกรม 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 ระเบียบว่าด้วยการรักษาความปลอดภัยแห่งชาติเกี่ยวกับการสื่อสาร พ.ศ.๒๕๒๕

๒.๑.๙ ข้อตกลง เงื่อนไขการใช้บริการที่กรม กำหนด

๓. ข้อตกลงและเงื่อนไขการใช้บริการจดหมายอิเล็กทรอนิกส์ของกรม

๓.๑ หน่วยงาน/บุคคลผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ของกรม จะต้องใช้จดหมายอิเล็กทรอนิกส์ของกรม เพื่อผลประโยชน์ของทางราชการ

๓.๒ ห้ามใช้ระบบจดหมายอิเล็กทรอนิกส์ของกรม เพื่อการประกอบธุรกิจ หรือแสวงหาผลประโยชน์ส่วนตน

๓.๓ ห้ามใช้บริการนี้ ไปในการเผยแพร่ อ้างอิง พาดพิง ดูหมิ่น หรือการกระทำใดๆ ที่ก่อให้เกิดความเสียหายต่อสถาบัน ชาติ ศาสนา และ พระมหากษัตริย์

๓.๔ ห้ามใช้ระบบจดหมายอิเล็กทรอนิกส์ของกรม ในการประกอบอาชญากรรมทางคอมพิวเตอร์ หรือการกระทำการใด ๆ ซึ่งผิดกฎหมาย คำสั่ง ระเบียบ ข้อบังคับ และมาตรการรักษาความปลอดภัยข้อมูล ข่าวสารลับของทางราชการ

๓.๕ ห้ามใช้ระบบจดหมายอิเล็กทรอนิกส์ของกรม เพื่อการเผยแพร่ข้อมูลข่าวสาร หรือภาพ เสียง ข้อความ ที่ไม่เหมาะสม หรือสร้างความเสื่อมเสียให้กับผู้อื่น

๓.๖ ห้ามใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-Mail Address) ไปแสดงข้อคิดเห็นส่วนตัวที่ส่งผลกระทบในทางลบ หรือสร้างความเสื่อมเสียหรือเสียหายต่อบุคคลหรือองค์กร

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 หรือก่อให้เกิดความเสียหายแก่ระบบเครื่องแม่ข่ายจดหมายอิเล็กทรอนิกส์ของ กรม

๓.๑๐ ผู้ใช้ต้องรักษารหัสผ่าน(Password) ส่วนบุคคล หรือหน่วยงานของจดหมายอิเล็กทรอนิกส์เป็นไว้เป็นความลับ

๓.๑๑ ห้ามส่งข้อมูลข่าวสารอันเป็นความลับของทางราชการให้กับบุคคลหรือหน่วยงานที่ไม่เกี่ยวข้องกับราชการของกรม

๓.๑๒ การส่งข้อมูลข่าวสารที่เป็นความลับของทางราชการให้กับบุคคลหรือหน่วยงานนอกกรมจะต้องเข้ารหัสข้อมูลข่าวสารนั้นตามวิธีปฏิบัติ และมาตรการรักษาความปลอดภัยข้อมูลข่าวสารตามที่กรม กำหนด

๓.๑๓ ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-Mail address) และรหัสผ่าน(Password) ของหน่วยหรือบุคคลจะต้องเก็บรักษาไว้เป็นความลับหากสงสัยว่ารั่วไหลจะต้องดำเนินการเปลี่ยนรหัสผ่านทันที โดยรหัสผ่านจะต้องกำหนดให้ยากแก่การคาดเดา (Strong Password)

๓.๑๔ ผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ กรมหรือผู้รับผิดชอบที่อยู่จดหมายอิเล็กทรอนิกส์จะต้องศึกษาคู่มือการใช้งาน ระเบียบปฏิบัติ คำแนะนำ และ ขอตกลงเงื่อนไขให้เข้าใจเพื่อใช้งานจดหมายอิเล็กทรอนิกส์ของกรม ได้อย่างถูกต้อง

๓.๑๕ กรณีได้รับการร้องเรียน ร้องขอ หรือพบเหตุอันไม่ชอบด้วยกฎหมาย ขอสงวนสิทธิ์ที่จะทำการยกเลิก หรือระงับบริการแก่สมาชิกนั้นๆ เป็นการชั่วคราวเพื่อทำการสอบสวน และตรวจสอบหาสาเหตุของมูลเหตุนั้นๆ

๓.๑๖ การกระทำใดๆ ที่เกี่ยวกับการเผยแพร่ ทั้งในรูปแบบของอีเมล์ และ/หรือโฮมเพจของผู้ใช้บริการ ให้ถือเป็นการกระทำที่อยู่ภายใต้ความรับผิดชอบของผู้ใช้บริการ กลุ่มเทคโนโลยีและสารสนเทศ สำนักแผนงาน ไม่มีส่วนเกี่ยวข้องใดๆ

สวนที่ ๑๔
การควบคุมหนวยงานภายนอกเขาถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร
(Third party access control)

๑. วัตถุประสงค

การใชบริการจากหนวยงานภายนอกอาจกอใหเกิดความเสี่ยงได เชนความเสี่ยงตอการเขาถึงขอมูล ความเสี่ยงตอการถูกแกไขขอมูลอยางไมถูกตองและการประมวลผลของระบบงานโดยไมไดรับอนุญาต เปนตนเพื่อใหการควบคุมหนวยงานภายนอกที่มีการเขาใชงานระบบเทคโนโลยีสารสนเทศและการสื่อสารขององคกรใหเปนไปอยางมั่นคงปลอดภัย และกำหนดแนวทางในการคัดเลือกควบคุมการปฏิบัติงานของหนวยงานภายนอก เชนการพัฒนาระบบการใชบริการของที่ปรึกษาการใชบริการดานระบบเทคโนโลยีสารสนเทศจากหนวยงานภายนอกเปนตน

๒. แนวทางปฏิบัติ

๒.๑. หัวหน้ากลุ่มเทคโนโลยีและสารสนเทศ สำนักแผนงาน ตองกำหนดใหมีการประเมินความเสี่ยงจากการเขาถึงระบบเทคโนโลยี สารสนเทศและการสื่อสารหรืออุปกรณที่ใชในการประมวลผลโดยหนวยงานภายนอกและกำหนดมาตรการรองรับหรือแกไขที่เหมาะสมกอนที่จะอนุญาตใหเขาถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารได

๒.๒. การควบคุมการเขาใชงานระบบเทคโนโลยีสารสนเทศและการสื่อสารของหนวยงานภายนอก

๒.๒.๑. บุคคลภายนอกที่ตองการสิทธิในการเขาใชงานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรม จะตองทำเรื่องขออนุญาตเปนลายลักษณอักษรเพื่อขออนุมัติจากหัวหน้ากลุ่มเทคโนโลยีและสารสนเทศ สำนักแผนงาน

๒.๒.๒. จัดทำเอกสารแบบฟอรมสำหรับใหหนวยงานภายนอกทำการระบุเหตุผลความจำเปนที่ตองเขาใชงานระบบเทคโนโลยีสารสนเทศและการสื่อสาร ซึ่งตองมีรายละเอียดอยางนอยดังนี้

- เหตุผลในการขอใช
- ระยะเวลาในการใช้
- การตรวจสอบความปลอดภัยของอุปกรณที่เชื่อมตอเครือขาย
- การตรวจสอบ MAC address ของเครื่องคอมพิวเตอรที่เชื่อมตอ
- การกำหนดการปองกันในเรื่องการเปดเผยขอมูล

๒.๒.๓. หนวยงานภายนอกที่ทำงานใหกับกรม ทุกหนวยงานไมวาจะทำงานอยูภายในกรม หรือนอกสถานที่จำเปนตองลงนามในสัญญาการไมเปดเผยขอมูลของกรม โดยสัญญาตองจัดทำใหเสร็จกอนให้สิทธ์ในการเขาสูระบบเทคโนโลยีสารสนเทศ

๒.๒.๔. กรมควรพิจารณาการเขาไปประเมินความเสี่ยงหรือจัดทำการควบคุมภายในของหนวยงานภายนอกทั้งนี้ ขึ้นอยูกับความสำคัญของระบบเทคโนโลยีสารสนเทศและการสื่อสาร ที่เขาไปปฏิบัติงาน

๒.๒.๕. เจาของโครงการซึ่งรับผิดชอบตอโครงการที่มีการเขาถึงขอมูลโดยหนวยงานภายนอกตองกำหนดการเขาใชงานเฉพาะบุคคลที่จำเปนเทานั้นและใหหนวยงานภายนอกลงนามในสัญญาไมเปดเผยขอมูล

๒.๒.๖. สำหรับโครงการขนาดใหญหนวยงานภายนอกที่สามารถเขาถึงขอมูลที่มีความสำคัญของกรมผูดูแลระบบตองควบคุมการปฏิบัติงานนั้นๆใหมีความมั่นคงปลอดภัยทั้ง ๓ ดานคือ การรักษาความลับ (Confidentiality) การรักษาความถูกตองของขอมูล (Integrity) และการรักษาความ พรอมที่จะใหบริการ (Availability)

๒.๒.๗. กรมมีสิทธิ์ในการตรวจสอบตามสัญญาการใชงานระบบเทคโนโลยีสารสนเทศและการสื่อสารเพื่อใหมั่นใจไดวากรมสามารถควบคุมการใชงานได่อยางทั่วถึงตามสัญญานั้น

๒.๒.๘. ควรดำเนินการใหผูใหบริการหนวยงานภายนอกจัดทำแผนการดำเนินงานคูมือการปฏิบัติงานและเอกสารที่เกี่ยวของรวมทั้งมีการปรับปรุงใหทันสมัยอยูเสมอเพื่อควบคุมหรือตรวจสอบการใหบริการของผูใหบริการไดอยางเขมงวดเพื่อใหมั่นใจไดวาเปนไปตามขอบเขต ที่ได กำหนดไว

สวนที่ ๑๕
นโยบายการรักษาความมั่นคงปลอดภัยของเครือข่ายไร้สาย
(Wireless Policy)

๑. วัตถุประสงค

เพื่อกำหนดมาตรฐานการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN) โดยการ กำหนดสิทธิ์ของผู้ใช้ในการเข้าถึงระบบให้เหมาะสมตามหน้าที่ความรับผิดชอบในการปฏิบัติงาน รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ ผู้ใช้ระบบต้องผ่านการพิสูจน์ตัวตนจริงจากระบบว่าได้รับอนุญาตจากผู้ดูแลระบบ เพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบเครือข่ายไร้สาย

๒. แนวทางปฏิบัติ

๑. ผู้ดูแลระบบเครือข่ายไร้สายมีหน้าที่ความรับผิดชอบที่ต้องปฏิบัติ ดังนี้

๑.๑. เครือข่ายของกรมเจ้าท่าเป็นสมบัติของกรมเจ้าท่า ห้ามผู้ใดเข้าใช้งานโดยมิได้รับอนุญาต การบุกรุกหรือพยายามบุกรุกเข้าสู่ระบบถือว่าเป็นการพยายามรุกล้ำเขตหวงห้าม ต้องได้รับโทษจากทางกรมเจ้าท่าและรับโทษตามกฎหมาย

๑.๒. ผู้ดูแลระบบต้องวางตัวกระจายสัญญาณไร้สาย Access Point ในตำแหน่งที่เหมาะสม โดยไม่ให้รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายของกรมเจ้าท่า

๑.๓. การติดตั้งระบบเครือข่ายไร้สาย (Wireless) ต้องติดตั้งโดยการแยกเครือข่ายไร้สายออกจากระบบเครือข่ายภายใน LAN เพื่อป้องกันการเข้าถึงจากบุคคลภายนอก

๑.๔. การกำหนดการเข้าถึงระบบเครือข่ายไร้สาย ต้องแบ่งแยกการใช้งานให้แตกต่างกันตามความจำเป็นของผู้ใช้งาน และกำหนดรหัสการเข้าใช้งานตามวัตถุประสงค์ของการใช้งาน

๑.๕. ให้กำหนดรายการ MAC Address ที่สามารถเข้าใช้ Access Point ได้เฉพาะเครื่องคอมพิวเตอร์ที่อนุญาตเท่านั้น และตามชื่อผู้ใช้ (Username) และ รหัสผ่าน (Password) ที่กำหนดไว้เท่านั้น

๑.๖. ให้เปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่ามาจากโรงงานผู้ผลิต และต้องปิดคุณสมบัติการ Auto Broadcast SSID ของตัว Access Point ด้วย

๑.๗. ผู้ดูแลระบบต้องควบคุมดูแลไม่ให้บุคคลหรือหน่วยงานภายนอกที่ไม่ได้รับ อนุญาต ใช้งานระบบเครือข่ายไร้สายในการเข้าสู่ระบบอินทราเน็ต (Intranet) และฐานข้อมูลภายในต่างๆ ของหน่วยงาน

๑.๘. ผู้ดูแลระบบควรใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของ ระบบเครือข่ายไร้สายเพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้น ในระบบเครือข่ายไร้สาย และจัดส่งรายงานผลการตรวจสอบทุก ๓ เดือน และ ในกรณีที่ตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติให้ผู้ดูแล ระบบรายงานให้ผู้อำนวยการสำนักแผนงานทราบทันที

๒. ผู้ใช้งานระบบเครือข่ายไร้สายกรมเจ้าท่ามีหน้าที่ความรับผิดชอบที่ต้องปฏิบัติ ดังนี้

๒.๑. ห้ามผู้ใช้งาน นำอุปกรณ์ Wireless มาติดตั้งหรือเปิดใช้งานเองในหน่วยงาน ไม่ว่าจะเป็น Access point, Wireless Router, Wireless USB client หรือ Wireless card

๒.๒. กรมเจ้าท่าให้บัญชีผู้ใช้งานเป็นการเฉพาะบุคคลเท่านั้น ผู้ใช้งานจะโอน จำหน่าย หรือจ่ายแจกสิทธินี้ให้กับผู้อื่นไม่ได้

๒.๓. บัญชีผู้ใช้งานที่กรมเจ้าท่าให้กับผู้ใช้งานนั้น ผู้ใช้งานต้องเป็นผู้รับผิดชอบผลต่างๆ อันอาจจะเกิดมีขึ้น รวมถึงผลเสียหายต่างๆ ที่เกิดจากบัญชีผู้ใช้งานนั้นๆ เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

๒.๔. ห้ามผู้ใช้งานปฏิบัติการใดๆ เกี่ยวกับข้อมูลข่าวสารที่เป็นการขัดต่อกฎหมายหรือศีลธรรมอันดีแห่งสาธารณชน โดยผู้ใช้งานรับรองว่าหากมีการกระทำการใดๆ ดังกล่าวย่อมถือว่าอยู่นอกเหนือความรับผิดชอบของกรมเจ้าท่า

๒.๕. กรมเจ้าท่าไม่อนุญาตให้ผู้ใช้งานทำการใดๆ ที่เข้าข่ายลักษณะเพื่อการค้าหรือการแสวงหาผลกำไร ผ่านเครื่องคอมพิวเตอร์และเครือข่าย เช่น การประกาศแจ้งความ การซื้อหรือการจำหน่ายสินค้า การนำข้อมูลไปซื้อขาย การรับบริการค้นหาข้อมูลโดยคิดค่าบริการ การให้บริการโฆษณาสินค้า หรือการเปิดบริการอินเทอร์เน็ตแก่บุคคลทั่วไปเพื่อแสวงหากำไร

๒.๖. ผู้ใช้งานจะต้องไม่อ่าน, เขียน, ลบ, เปลี่ยนแปลงหรือแก้ไขใดๆ ในส่วนที่มิใช่ของตนโดยไม่ได้รับอนุญาต การบุกรุก (hack) เข้าสู่บัญชีผู้ใช้งาน (user account) ของผู้อื่น หรือพัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ ที่จะทำลายกลไกรักษาความปลอดภัย รวมไปถึงเข้าสู่เครื่องคอมพิวเตอร์ของหน่วยงานในกรมเจ้าท่าหรือหน่วยงานอื่นๆ การเผยแพร่ข้อความใดๆ ที่ก่อให้เกิดความเสียหายเสื่อมเสียแก่ผู้อื่น การใช้ภาษาไม่สุภาพหรือการเขียนข้อความที่ทำให้ผู้อื่นเสียหาย ถือเป็นการละเมิดสิทธิของผู้อื่นทั้งสิ้น ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงฝ่ายเดียว กรมเจ้าท่าไม่มีส่วนร่วมรับผิดชอบความเสียหายดังกล่าว

๒.๗. ผู้ใช้งานต้องยอมรับอย่างไม่มีเงื่อนไข ในการรับทราบกฎระเบียบ หรือนโยบายต่างๆ ที่กรมเจ้าท่ากำหนดขึ้น โดยจะอ้างว่าไม่ทราบกฎระเบียบ หรือนโยบายของกรมเจ้าท่ามิได้

๒.๘. กรมเจ้าท่าทรงไว้ซึ่งสิทธิที่จะปฏิเสธการเชื่อมต่อและ/หรือการใช้งาน และทรงไว้ซึ่งสิทธิที่จะยกเลิกหรือระงับการเชื่อมต่อและ/หรือการใช้งานใดๆ ของผู้ใช้งานที่ล่วงละเมิดหรือพยายามจะล่วงละเมิดกฎระเบียบนี้ของกรมเจ้าท่าโดยไม่มีการแจ้งให้ทราบก่อนล่วงหน้า

การดำเนินการตอบสนองเหตุการณ์ความมั่นคงปลอดภัยทางระบบสารสนเทศ

๑. ระบบป้องกันผู้บุกรุก

แผนดำเนินการรายวัน

๑. **ดำเนินการตรวจสอบไฟล์ล็อกหรือรายงานของระบบป้องกันการบุกรุก** สิ่งที่ทำการตรวจสอดังต่อไปนี้

๑.๑ การโจมตีเกิดขึ้นมากน้อยเพียงใด การโจมตีประเภทใดเกิดขึ้นเป็นจำนวนมาก

๑.๒ ลักษณะของการโจมตีที่เกิดขึ้นมีรูปแบบที่สามารถคาดเดาได้หรือไม่

๑.๓ ระดับความรุนแรงมากน้อยเพียงใด

๑.๔ หมายเลขไอพีของเครือข่ายที่เป็นผู้โจมตี

๒. ระบบไฟร์วอลล์

๑. ดำเนินการตรวจสอบกฎ (Rule) ของระบบป้องกันการบุกรุก อย่างน้อยเดือนละ ๑ ครั้ง

๒. ดำเนินการตรวจสอบบันทึกของไฟล์ล็อก (Log File) และรายงานของไฟล์วอลล์ สิ่งที่ต้องตรวจสอบมีดังต่อไปนี้

๒.๑ Packet ที่ไฟล์วอลล์ได้ทำการ Block

๒.๒ ลักษณะของ Packet ที่ถูก Block

๒.๓ Packet ของหมายเลขไอพี ของเครือข่ายใดถูก Block เป็นจำนวนมาก

๓. กรณีตรวจพบการโจมตีระบบหรือเหตุการณ์ละเมิดความปลอดภัยระบบสารสนเทศให้แจ้งหัวหน้ากลุ่มเทคโนโลยีสารสนเทศ เพื่อตัดสินใจดำเนินการแก้ไขปัญหา

๓. ระบบป้องกันภัยคุกคามทางอินเตอร์เน็ต

ภัยคุกคามทางอินเตอร์เน็ตหรือมัลแวร์ (Malware) ประกอบด้วย ไวรัส หนอนอินเตอร์เน็ต โทรจัน รวมถึงสปายแวร์

แผนดำเนินการรายวัน/รายสัปดาห์/รายเดือน

๑. ดำเนินการตรวจสอบไฟล์ล็อกและรายงานของอุปกรณ์ที่เกี่ยวข้องกับระบบป้องกันภัยคุกคามทางอินเตอร์เน็ต สิ่งที่ควรตรวจสอบมีดังนี้

๑.๑ มัลแวร์ประเภทใดถูกพบเป็นจำนวนมาก

๑.๒ มัลแวร์ถูกส่งมาจากเครือข่ายใด และถูกส่งไปยังที่ใด

๑.๓ มีการส่งมัลแวร์จากเครือข่ายภายในกรม ไปยังภายนอกหรือไม่

๒. ศึกษาหาวิธีแก้ไขเครื่องคอมพิวเตอร์ที่ติดมัลแวร์ โดยเฉพาะมัลแวร์ประเภทที่ตรวจพบว่ากระจายอยู่ในเครือข่ายของกรม

๓. ตรวจสอบพบว่าเครื่องคอมพิวเตอร์ภายในเครือข่ายติดมัลแวร์หรือส่งมัลแวร์ออกไปข้างนอก ควรระงับการเชื่อมต่อของเครื่องที่ติดมัลแวร์กับระบบเครือข่าย แล้วทำการแก้ไขเครื่องนั้นทันที