



นโยบายและแนวปฏิบัติ
ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

กรมเจ้าท่า

ปีงบประมาณ พ.ศ. ๒๕๖๐

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ กรมเจ้าท่า

๑. บทนำ

๑.๑ หลักการ

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

เพื่อให้ระบบเทคโนโลยีสารสนเทศของกรมเจ้าท่าหรือต่อไปเรียกว่า “กรม” เป็นไปอย่างเหมาะสมมีประสิทธิภาพมีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง และการถูกคุกคามจากภัยต่างๆ กรมจึงเห็นสมควรกำหนดนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศโดยกำหนดให้มีมาตรฐาน แนวปฏิบัติ ขั้นตอนปฏิบัติ ให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ตามพระราชกฤษฎีกาฯ และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ฯ โดยมีวัตถุประสงค์ดังต่อไปนี้

- ๑.๑. การจัดทำนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร หรือเครือข่ายคอมพิวเตอร์ของกรมทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล
- ๑.๒. เป็นบรรทัดฐานด้านความมั่นคงปลอดภัยในการดำเนินกิจการอันเกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศและการสื่อสาร
- ๑.๓. กำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร อ้างอิงตามมาตรฐาน ISO/IEC ๒๗๐๐๑ และมีการปรับปรุงอย่างต่อเนื่อง
- ๑.๔. นโยบายนี้จะต้องทำการเผยแพร่ให้เจ้าหน้าที่ทุกระดับในกรมได้รับทราบและเจ้าหน้าที่ทุกคนจะต้องถือปฏิบัติตามนโยบายนี้อย่างเคร่งครัด
- ๑.๕. เพื่อกำหนดมาตรฐานแนวทางปฏิบัติและวิธีปฏิบัติให้ผู้บริหารเจ้าหน้าที่ผู้ดูแลระบบ และบุคคลภายนอกที่ปฏิบัติงานให้กับกรมตระหนักถึงความสำคัญของการรักษาความมั่นคง ปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด
- ๑.๖. เพื่อใช้เป็นหลักในการพัฒนาและปรับปรุงคุณภาพด้านความมั่นคงปลอดภัยสารสนเทศ
- ๑.๗. นโยบายนี้ต้องมีการดำเนินการตรวจสอบและประเมินนโยบายตามระยะเวลา ๑ ครั้งต่อปี

๒. องค์ประกอบของนโยบาย

คำนิยาม

- ส่วนที่ ๑ การบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ
- ส่วนที่ ๒ การควบคุมการเข้าออกห้องควบคุมระบบคอมพิวเตอร์
- ส่วนที่ ๓ การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ
- ส่วนที่ ๔ การบริหารจัดการการเข้าถึงของผู้ใช้งาน
- ส่วนที่ ๕ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน
- ส่วนที่ ๖ การควบคุมการเข้าถึงและใช้บริการระบบเครือข่าย
- ส่วนที่ ๗ การควบคุมการเข้าถึงระบบปฏิบัติการ
- ส่วนที่ ๘ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ
- ส่วนที่ ๙ การจัดทำระบบสำรองข้อมูล
- ส่วนที่ ๑๐ การตรวจสอบและประเมินความเสี่ยง
- ส่วนที่ ๑๑ นโยบายความมั่นคงปลอดภัยของการใช้งานอินเทอร์เน็ต
- ส่วนที่ ๑๒ แนวทางการใช้งานจดหมายอิเล็กทรอนิกส์
- ส่วนที่ ๑๓ ข้อตกลงการให้บริการจดหมายอิเล็กทรอนิกส์
- ส่วนที่ ๑๔ การควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ

การดำเนินการตอบสนองเหตุการณ์ความมั่นคงปลอดภัยทางระบบสารสนเทศ

องค์ประกอบของนโยบายการการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของกรมแต่ละส่วนที่กล่าวข้างต้นจะประกอบด้วยวัตถุประสงค์รายละเอียดของมาตรฐาน (Standard) แนวทางปฏิบัติ (Guideline) และขั้นตอนวิธีการปฏิบัติ (Procedure) ในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของกรมเพื่อที่จะทำให้กรมมีมาตรการในการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศอยู่ในระดับที่ปลอดภัย ช่วยลดความเสียหายต่อการดำเนินงานทรัพย์สินบุคลากรของกรม ทำให้สามารถดำเนินงานได้อย่างมั่นคงปลอดภัย นโยบายการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของกรมนี้จัดเป็นมาตรฐานด้านความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศของกรม ซึ่งเจ้าหน้าที่ของกรม และหน่วยงานภายนอกต้องปฏิบัติตามอย่างเคร่งครัด

คำนิยาม

คำนิยามที่ใช้ในนโยบายนี้

๑. **กรม** หมายถึง กรมเจ้าท่า
๒. **การรักษาความมั่นคงปลอดภัย** หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมเจ้าท่า
๓. **ผู้ใช้งาน** หมายถึง บุคคลที่ได้รับอนุญาต (Authorized user) ให้สามารถเข้าใช้งานบริหารหรือดูแลรักษา ระบบเทคโนโลยีสารสนเทศของกรมเจ้าท่าโดยมีสิทธิและหน้าที่ขึ้นอยู่กับบทบาท (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 ข้อมูลระบบข้อมูลและทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสาร หรือสิ่งใดก็ตามที่มีคุณค่าของหน่วยงาน เช่นอุปกรณ์ระบบเครือข่ายซอฟต์แวร์ที่มีลิขสิทธิ์ เป็นต้น
๖. **การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ** หมายความว่า การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์ และทางกายภาพ รวมทั้งการอนุญาตเช่นนั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมีขอบเอวได้ด้วยก็ได้
๗. **ความมั่นคงปลอดภัยด้านสารสนเทศ** หมายถึง การดำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (authenticity) ความรับผิดชอบ (accountability) การห้ามปฏิเสธความรับผิดชอบ (non-repudiation) และความน่าเชื่อถือ (reliability)
๘. **ความมั่นคงปลอดภัยด้านการบริหารจัดการ** หมายถึง การกระทำในระดับบริหารโดยการจัดให้มีนโยบาย มาตรการ หลักเกณฑ์ หรือกระบวนการใดๆ เพื่อนำมาใช้ในการกระบวนการคัดเลือก การพัฒนา การนำไปใช้งาน หรือการบำรุงรักษาทรัพย์สินสารสนเทศให้มีความมั่นคงปลอดภัย
๙. **ความมั่นคงปลอดภัยทางด้านกายภาพ** หมายถึง การจัดให้มีนโยบาย มาตรการหลักเกณฑ์ หรือกระบวนการใดๆ เพื่อนำมาใช้ในการป้องกันทรัพย์สินสารสนเทศ สิ่งปลูกสร้าง หรือทรัพย์สินอื่นใดจากการคุกคามของบุคคล ภัยธรรมชาติ อุบัติภัย หรือภัยทางกายภาพอื่น
๑๐. **เหตุการณ์ด้านความมั่นคงปลอดภัย** หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการ หรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิด การฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

๑๑. **สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด** หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (unwanted or unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยคุกคาม
๑๒. **หน่วยงานภายนอก** หมายถึง องค์กรหรือหน่วยงานที่กรมเจ้าท่าอนุญาตให้มีสิทธิในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่างๆ ของหน่วยงานโดยจะได้รับสิทธิในการใช้งานตามอำนาจและต้องรับผิดชอบในการรักษาความลับของข้อมูล
๑๓. **รหัสผ่าน** (Password) หมายถึง ตัวอักษรหรืออักขระหรือตัวเลขที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคลเพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ
๑๔. **ข้อมูลคอมพิวเตอร์** หมายถึง ข้อมูลข้อความคำสั่งชุดคำสั่งหรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์ ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์
๑๕. **ระบบเครือข่าย** (Network System) หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่างๆ ของกรมได้ เช่นระบบแลน (LAN) ระบบอินทราเน็ต (Intranet) ระบบอินเทอร์เน็ต (Internet)
- ระบบแลน (LAN) และระบบอินทราเน็ต (Intranet) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อ ระบบคอมพิวเตอร์ต่างๆภายในหน่วยงานเข้าด้วยกันเป็นเครือข่ายที่มีจุดประสงค์ เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน
 - ระบบอินเทอร์เน็ต (Internet) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อบริเวณเครือข่ายคอมพิวเตอร์ต่างๆของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตทั่วโลก
๑๖. **ระบบเทคโนโลยีสารสนเทศ** (Information Technology System) หมายถึง ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศระบบคอมพิวเตอร์และระบบเครือข่าย มาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผนบริหารการสนับสนุนการให้บริการการพัฒนา และควบคุมการติดต่อสื่อสารซึ่งมีองค์ประกอบเช่นระบบคอมพิวเตอร์ระบบเครือข่ายโปรแกรมข้อมูลและสารสนเทศเป็นต้น
๑๗. **พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร** (Information System Workspace) หมายถึง พื้นที่ที่หน่วยงานอนุญาตให้มีการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารโดยแบ่งเป็น
- พื้นที่ทำงานทั่วไป (General working area) หมายถึง พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคล
 - พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย (IT equipment or network area)
 - พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data storage area)
๑๘. **เจ้าของข้อมูล** หมายถึง ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงานโดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้นๆหรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย
๑๙. **จดหมายอิเล็กทรอนิกส์** (e-mail) หมายถึง ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกัน โดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกันข้อมูลที่ส่งจะเป็นได้ทั้ง ตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้

๒๐. ชุดคำสั่งไม่พึงประสงค์ หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นเกิดความเสียหายถูกทำลายถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติมขัดข้องหรือปฏิบัติงาน ไม่ตรงตามคำสั่งที่กำหนดไว้

ส่วนที่ ๑
การบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ
(Information Security Management)

๑. วัตถุประสงค์

เพื่อกำหนดผู้รับผิดชอบที่ชัดเจน ในการดูแลกรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดการเสียหาย หรืออันตรายใดๆ แก่กรมเจ้าท่า ในการหาแนวทาง ทบทวนนโยบายและแนวปฏิบัติไปใช้ในการแก้ปัญหาที่เกิดขึ้น และนำไปสู่การปรับปรุงการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศให้มีคุณภาพต่อไป

๒. แนวทางในการบริหารจัดการ

- ๒.๑. ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Office : CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นจากการละเลยการควบคุม ความมั่นคงปลอดภัยสารสนเทศกรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใดๆ แก่กรมฯ หรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยจัดให้มีการประชุมคณะกรรมการพัฒนาบริหารจัดการระบบสารสนเทศ โดยผู้บริหารสารสนเทศระดับสูง และผู้อำนวยการสำนัก/ศูนย์/กลุ่ม เพื่อทำการทบทวนและทราบดีถึงนโยบายและแนวปฏิบัติ การรักษาความมั่นคงปลอดภัยด้านสารสนเทศ อย่างน้อยปีละ ๑ 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 เพื่อสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศให้กับข้าราชการ พนักงานราชการ และเจ้าหน้าที่ เพื่อสร้างความตระหนักและความเข้าใจภัยและ

ผลกระทบที่จะเกิดขึ้น จากการใช้ระบบงานสารสนเทศโดยไม่ระมัดระวังหรือไม่เท่าถึงการณ์
อย่างน้อยปีละ ๑ ครั้ง

- ๒.๘. จัดให้มีการตรวจสอบและประเมินความเสี่ยงในการปฏิบัติ ปีละ ๑ ครั้งและจัดให้มีการทำแผนการ
ปรับปรุง เพื่อทบทวนหรือแก้ไขปัญหที่พบ
- ๒.๙. จัดให้มีการอบรมให้ความรู้และซักซ้อมแผนฉุกเฉินภัยพิบัติของประเทศของระบบเทคโนโลยี
สารสนเทศ (IT Contingence plan) อย่างน้อยปีละ ๑ ครั้ง
- ๒.๑๐. กำหนดหน้าที่ที่ต้องทบทวนปรับปรุงนโยบายและข้อปฏิบัติให้เป็นปัจจุบันอยู่เสมอ และกำหนด
หน้าที่รับผิดชอบของบุคลากรที่เกี่ยวข้องด้านความมั่นคงปลอดภัยสารสนเทศ และแผนฉุกเฉินภัย
พิบัติของระบบเทคโนโลยีสารสนเทศของกรมเจ้าท่า
- ๒.๑๑. ผู้บริหาร ต้องกำหนดและแบ่งแยกบริเวณพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร
ให้ชัดเจน โดยการกำหนดพื้นที่ดังกล่าวอาจแบ่งออกได้เป็น พื้นที่ทำงานทั่วไป (General working
area) พื้นที่ทำงานของผู้ดูแลระบบ (System administrator area) พื้นที่ติดตั้งอุปกรณ์ระบบ
เทคโนโลยีสารสนเทศ (IT Equipment area) พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data storage
area) และ พื้นที่ใช้งานเครือข่ายไร้สาย (Wireless LAN coverage area) เป็นต้น

ส่วนที่ ๒

การควบคุมการเข้าออกห้องควบคุมระบบคอมพิวเตอร์ (Computing System Control Room)

๑. วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการควบคุมและป้องกัน เพื่อการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการใช้งาน หรือการเข้าถึงห้องควบคุมระบบเครื่องคอมพิวเตอร์ อุปกรณ์เครือข่าย และระบบเทคโนโลยีสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ ระบบเทคโนโลยีสารสนเทศ ข้อมูลซึ่งเป็นทรัพย์สินที่มีค่าและอาจจำเป็นต้องรักษาความลับโดยมาตรการนี้ จะมีผลบังคับใช้กับผู้มีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศของกรม

๒. การควบคุมการเข้าออก

- ๒.๑. ภายในกรมมีการติดตั้งระบบควบคุมการเข้าออกอัตโนมัติ (Access Control System) เพื่อควบคุมการเข้าออกห้องควบคุมเครื่องคอมพิวเตอร์แม่ข่าย โดยจำแนกและกำหนดพื้นที่การติดตั้งระบบควบคุมการเข้าออกอัตโนมัติ (Access Control System) เป็น ๓ ส่วน โดยส่วนที่ ๑ เป็นการติดตั้งระบบควบคุมการเข้าออกอัตโนมัติ (Access Control System) บริเวณทางเข้าสู่ศูนย์คอมพิวเตอร์ ส่วนที่ ๒ เป็นการติดตั้งระบบควบคุมการเข้าออกอัตโนมัติ (Access Control System) ห้องควบคุมเครื่องคอมพิวเตอร์แม่ข่าย และส่วนที่ ๓ เป็นการติดตั้งระบบควบคุมการเข้าออกอัตโนมัติ (Access Control System) ห้อง Facility เพื่อจุดประสงค์ในการควบคุมการเข้าออกของบุคคลภายนอก โดยใช้เทคโนโลยีระบบ Biometric Finger Scan และ Proximity Card
- ๒.๒. ภายในกรมมีการติดตั้งระบบกล้องวงจรปิด เพื่อจุดประสงค์ในการเฝ้าระวังควบคุมการรักษาความมั่นคงปลอดภัย จากผู้ที่ไม่ได้รับอนุญาตรวมทั้งป้องกันความเสียหายอื่นๆที่อาจเกิดขึ้นได้
- ๒.๓. ต้องกำหนดสิทธิให้กับเจ้าหน้าที่ให้สามารถมีสิทธิในการเข้าถึงพื้นที่เพื่อปฏิบัติหน้าที่ตามที่ได้รับมอบหมายประกอบด้วย
 - ๒.๓.๑. จัดทำ “ทะเบียนผู้มีสิทธิเข้าออกพื้นที่” เพื่อปฏิบัติหน้าที่ตามสิทธิและหน้าที่ที่ได้รับมอบหมาย
 - ๒.๓.๒. กำหนดผู้มีหน้าที่รับผิดชอบการบันทึกการเข้า-ออก ดังกล่าวโดยจัดทำเป็นเอกสาร “บันทึกการเข้าออกพื้นที่”
 - ๒.๓.๓. จัดให้มีเจ้าหน้าที่ทำหน้าที่ตรวจสอบประวัติการเข้าออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศเป็นประจำ และให้มีการปรับปรุงรายการผู้มีสิทธิเข้าออกพื้นที่ใช้งานระบบสารสนเทศและการสื่อสาร ปีละ ๑ ครั้ง เป็นอย่างน้อย
- ๒.๔. บุคคลภายนอกเข้ามาติดต่อจะต้องลงชื่ออนุญาตการเข้าออกในแบบฟอร์มการเข้า-ออกให้ถูกต้อง และจะต้องอยู่กับบุคคลที่มาติดต่อตลอดเวลา
- ๒.๕. บุคคลอื่นที่ไม่มีหน้าที่เกี่ยวข้องขอเข้าพื้นที่ หน่วยงานเจ้าของพื้นที่ต้องตรวจสอบเหตุผลและความจำเป็นก่อนที่จะอนุญาต

ส่วนที่ ๓

การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

(Access Control)

๑. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้อนุญาตเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมและป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุกจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ที่จะสร้างความเสียหายแก่ข้อมูลหรือการทำงานของระบบเทคโนโลยีสารสนเทศและการสื่อสารให้หยุดชะงักและทำให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรม ได้อย่างถูกต้อง

๒. กระบวนการหลักในการควบคุมการเข้าถึงระบบ

- ๒.๑. สถานที่ตั้งของระบบเทคโนโลยีสารสนเทศ ที่สำคัญต้องมีการควบคุมการเข้าออกที่รัดกุมและอนุญาตให้เฉพาะบุคคลที่ได้รับสิทธิและมีความจำเป็นผ่านเข้าใช้งานได้เท่านั้น
- ๒.๒. ผู้ดูแลระบบต้องกำหนดสิทธิการเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการใช้งานของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสารรวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอทั้งนี้ ผู้ใช้ระบบจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน
- ๒.๓. ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายเท่านั้นที่สามารถแก้ไขเปลี่ยนแปลงสิทธิการเข้าถึงข้อมูลและระบบข้อมูลได้
- ๒.๔. ผู้ดูแลระบบควรจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบเทคโนโลยีสารสนเทศของกรมและตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบข้อมูลสำคัญ
- ๒.๕. ผู้ดูแลระบบต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบการแก้ไขเปลี่ยนแปลงสิทธิต่างๆ และการผ่านเข้าออกสถานที่ตั้งของระบบของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาตเพื่อเป็นหลักฐานในการตรวจสอบหากมีปัญหาเกิดขึ้น

๓. การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

- ๓.๑. ผู้ดูแลระบบมีหน้าที่ในการตรวจสอบการอนุมัติและกำหนดสิทธิในการผ่านเข้าสู่ระบบให้แก่ผู้ใช้ในการขออนุญาตเข้าระบบงานนั้นจะต้องมีการทำเป็นเอกสารเพื่อขอสิทธิในการเข้าสู่ระบบและกำหนดให้มีการลงนามอนุมัติเอกสารดังกล่าวต้องมีการจัดเก็บไว้เป็นหลักฐาน
- ๓.๒. เจ้าของข้อมูลและ เจ้าของระบบงาน จะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่จำเป็นต้องรู้ตามหน้าที่งานเท่านั้นเนื่องจากการให้สิทธิเกินความจำเป็นในการใช้งานจะนำไปสู่ความเสี่ยงในการใช้งานเกินอำนาจหน้าที่ดังนั้นการกำหนดสิทธิในการเข้าถึงระบบงาน ต้องกำหนดตามความจำเป็นขั้นต่ำเท่านั้น
- ๓.๓. ผู้ใช้งานจะต้องได้รับอนุญาตจากเจ้าหน้าที่ที่รับผิดชอบข้อมูลและระบบงานตามความจำเป็นต่อการใช้งานระบบเทคโนโลยีสารสนเทศ

๔. การบริหารจัดการการเข้าถึงของผู้ใช้

- ๔.๑. การลงทะเบียนเจ้าหน้าที่ใหม่ของกรมควรกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการ สำหรับการลงทะเบียนเจ้าหน้าที่ใหม่เพื่อให้มีสิทธิต่างๆในการใช้งานตามความจำเป็นรวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน เช่นเมื่อลาออกไปต้องทำภายใน ๒๔ ชั่วโมงหรือ เมื่อเปลี่ยนตำแหน่งงานภายในต้องทำภายใน ๗ วัน
- ๔.๒. กำหนดสิทธิการในระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (e-mail) ระบบอินเทอร์เน็ต เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้ดูแลระบบเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ
- ๔.๓. ผู้ใช้ต้องลงนามรับทราบสิทธิ และหน้าที่เกี่ยวกับการใช้งานระบบเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษรและต้องปฏิบัติตามอย่างเคร่งครัด
- ๔.๔. การบริหารจัดการบัญชีรายชื่อผู้ใช้งาน (User account) และรหัสผ่านของเจ้าหน้าที่
 - ๔.๔.๑. ผู้ดูแลระบบที่รับผิดชอบระบบงานนั้นๆต้องกำหนดสิทธิของเจ้าหน้าที่ในการเข้าถึงระบบเทคโนโลยีสารสนเทศแต่ละระบบรวมทั้งกำหนดสิทธิแยกตามหน้าที่ที่รับผิดชอบซึ่งมีแนวทางปฏิบัติตามที่กำหนดไว้ในเอกสาร“การบริหารจัดการการเข้าถึงของผู้ใช้งาน”
 - ๔.๔.๒. การกำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่านต้องปฏิบัติตาม“การบริหารจัดการการเข้าถึงของผู้ใช้งาน”
 - ๔.๔.๓. กรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้ หมายถึง ผู้ใช้ที่มีสิทธิสูงสุดต้องมีการพิจารณาการควบคุมผู้ใช้ที่มีสิทธิพิเศษนั้นอย่างรัดกุมเพียงพอโดยใช้ปัจจัยต่อไปนี้ประกอบการพิจารณา
 - ๔.๔.๓.๑. ควรได้รับความเห็นชอบจากผู้ดูแลระบบงานนั้นๆ โดยนำเสนอผู้บังคับบัญชาอนุมัติ
 - ๔.๔.๓.๒. ควรควบคุมการใช้งานอย่างเข้มงวดเช่น กำหนดให้ใช้งานเฉพาะกรณีที่เป็นเท่านั้น
 - ๔.๔.๓.๓. ควรกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันที เมื่อพ้นระยะเวลาดังกล่าว
 - ๔.๔.๓.๔. ควรมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ทุกครั้งหลังหมดความจำเป็นในการใช้งาน หรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานานก็ควรเปลี่ยนรหัสผ่านทุก ๓ เดือน เป็นต้น
- ๔.๕. การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ
 - ๔.๕.๑. ผู้ดูแลระบบต้องกำหนดชั้นความลับของข้อมูลวิธีปฏิบัติในการจัดเก็บข้อมูลและวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงานรวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ
 - ๔.๕.๒. เจ้าของข้อมูลจะต้องมีการสอบถามความเหมาะสมของสิทธิในการเข้าถึงข้อมูลของผู้ใช้งานเหล่านี้ อย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิต่างๆ ที่ให้ไว้ยังคงมีความเหมาะสม
 - ๔.๕.๓. วิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงานผู้ดูแลระบบต้องกำหนดรายชื่อผู้ใช้งาน (User account) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล

- ๔.๕.๔. การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล
- ๔.๕.๕. ควรมีการกำหนดให้เปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูลตามที่ระบุไว้ในเอกสาร “การบริหารจัดการการเข้าถึงของผู้ใช้งาน”
- ๔.๕.๖. ควรมีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่น่าเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของกรม เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูลที่เก็บอยู่ในสื่อ บันทึกก่อน เป็นต้น

๕. การบริหารจัดการการเข้าถึงระบบเครือข่าย

- ๕.๑. ผู้ดูแลระบบต้องมีการออกแบบระบบเครือข่ายตามกลุ่มของบริการระบบเทคโนโลยีสารสนเทศที่มีการใช้งานกลุ่มของผู้ใช้ และกลุ่มของระบบสารสนเทศ เช่น โซนภายใน (Internal zone) โซนภายนอก (External zone) เป็นต้น เพื่อให้การควบคุมและป้องกันการบุกรุกได้อย่าง เป็นระบบ
- ๕.๒. ผู้ดูแลระบบต้องมีวิธีการจำกัดสิทธิการใช้งาน เพื่อควบคุมผู้ใช้ให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น
- ๕.๓. ผู้ดูแลระบบควรมีวิธีการจำกัดเส้นทางการเข้าถึงเครือข่ายที่มีการใช้งานร่วมกัน
- ๕.๔. ผู้ดูแลระบบควรจัดให้มีวิธีเพื่อกำหนดการใช้เส้นทางบนเครือข่าย (Enforced path) จากเครื่องลูกข่ายไปยังเครื่องแม่ข่ายเพื่อไม่ให้ผู้ใช้สามารถใช้เส้นทางอื่นๆได้ กำหนดบุคคลที่รับผิดชอบในการกำหนดแก้ไขหรือเปลี่ยนแปลงค่า parameter ต่างๆของระบบ
- ๕.๕. ป้องกันเครือข่ายและอุปกรณ์ต่างๆที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจนและควรทบทวนการกำหนดค่า Parameter ต่างๆอย่างน้อยปีละครั้ง นอกจากนี้การกำหนดแก้ไขหรือเปลี่ยนแปลง ค่า parameter ควรแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง
- ๕.๖. ระบบเครือข่ายทั้งหมดของกรมที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆภายนอกกรม ควรเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือโปรแกรมในการทำ Packet filtering เช่น การใช้ไฟร์วอลล์ (firewall) หรือฮาร์ดแวร์อื่นๆ รวมทั้งต้องมีความสามารถในการตรวจจับมัลแวร์ (Malware) ด้วย
- ๕.๗. ต้องมีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของกรม ในลักษณะที่ผิดปกติผ่านระบบเครือข่าย โดยมีการตรวจสอบการบุกรุกผ่านระบบเครือข่ายการใช้งานในลักษณะที่ผิดปกติ และการแก้ไขเปลี่ยนแปลงระบบเครือข่าย โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง
- ๕.๘. การเข้าสู่ระบบงานเครือข่ายภายในกรมโดยผ่านทางอินเทอร์เน็ต จำเป็นต้องมีการล็อกอิน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้อง
- ๕.๙. IP address ภายในของระบบงานเครือข่ายภายในของกรม จำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายได้โดยง่าย
- ๕.๑๐. ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายใน และเครือข่ายภายนอกและอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ
- ๕.๑๑. การใช้เครื่องมือต่างๆ (Tools) เพื่อการตรวจสอบระบบเครือข่ายควรได้รับการอนุมัติจากผู้ดูแลระบบ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

๕.๑๒. การติดตั้งและการเชื่อมต่ออุปกรณ์เครือข่ายจะต้องดำเนินการโดยเจ้าหน้าที่กลุ่มเทคโนโลยีสารสนเทศ สำนักแผนงานเท่านั้น

๖. การบริหารจัดการระบบคอมพิวเตอร์แม่ข่าย

- ๖.๑. ควรกำหนดบุคคลที่รับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนดแก้ไข หรือ เปลี่ยนแปลงค่าต่างๆของโปรแกรมระบบ (System Software) อย่างชัดเจน
- ๖.๒. ต้องมีขั้นตอนหรือวิธีปฏิบัติในการตรวจสอบระบบคอมพิวเตอร์แม่ข่ายและในกรณีที่พบว่ามีการใช้ งาน หรือเปลี่ยนแปลงค่าในลักษณะผิดปกติ จะต้องดำเนินการแก้ไขรวมทั้งมีการรายงานโดยทันที
- ๖.๓. ต้องเปิดให้บริการ (Service) เท่าที่จำเป็นเท่านั้นเช่น Telnet ftp หรือ ping เป็นต้น ทั้งนี้หาก บริการที่จำเป็นต้องใช้มีความเสี่ยงต่อระบบรักษาความปลอดภัยแล้วต้องมีมาตรการเพิ่มเติมด้วย
- ๖.๔. ควรดำเนินการติดตั้งอัปเดตระบบซอฟต์แวร์ให้เป็นปัจจุบันเพื่ออุดช่องโหว่ต่างๆของโปรแกรมระบบ (System Software) อย่างสม่ำเสมอ เช่น web server เป็นต้น
- ๖.๕. ควรมีการทดสอบโปรแกรมระบบ (System Software) เกี่ยวกับการรักษาความปลอดภัยและ ประสิทธิภาพ การใช้งานโดยทั่วไปก่อนติดตั้งและหลังจากการแก้ไขหรือบำรุงรักษา
- ๖.๖. การติดตั้งและการเชื่อมต่อระบบคอมพิวเตอร์แม่ข่ายจะต้องดำเนินการโดยเจ้าหน้าที่กลุ่มเทคโนโลยี สารสนเทศเท่านั้น

๗. การบริหารจัดการการบันทึกและตรวจสอบ

- ๗.๑. ควรกำหนดให้มีการบันทึกการทำงานของระบบคอมพิวเตอร์แม่ข่ายและเครือข่ายบันทึกการ ปฏิบัติงานของผู้ใช้งาน (Application logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้าออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน command line และ firewall log เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย ๓ เดือน
- ๗.๒. ควรมีการตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอ
- ๗.๓. ต้องมีวิธีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่างๆและจำกัดสิทธิการเข้าถึงบันทึกเหล่านั้นให้ เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

๘. การควบคุมการเข้าใช้งานระบบจากภายนอก

ต้องกำหนดให้มีการควบคุมการใช้งานระบบที่ ผู้ดูแลระบบได้ติดตั้งไว้ภายในองค์กรเพื่อดูแลรักษา ความปลอดภัยของระบบจากภายนอกโดยมีแนวทางปฏิบัติดังนี้

- ๘.๑. การเข้าสู่ระบบระยะไกล (Remote access) เข้าสู่ระบบเครือข่ายของกรม ต้องควบคุมบุคคลที่จะเข้าสู่ ระบบของกรม จากระยะไกลโดยกำหนดมาตรการการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐาน การเข้าสู่ระบบภายใน
- ๘.๒. วิธีการใดๆก็ตามที่สามารถเข้าถึงข้อมูลหรือระบบข้อมูลจากระยะไกลต้องได้รับการอนุมัติจาก หัวหน้ากลุ่มเทคโนโลยีสารสนเทศ หรือผู้อำนวยการ สำนักแผนงาน ก่อน และมีการควบคุมอย่าง เข้มงวดก่อนนำมาใช้ และผู้ใช้ต้องปฏิบัติตามข้อกำหนดของกรมในการเข้าสู่ระบบและข้อมูลอย่าง เคร่งครัด
- ๘.๓. การทำการให้สิทธิในการเข้าสู่ระบบจากระยะไกลผู้ใช้ต้องแสดงหลักฐานระบุเหตุผลหรือความ จำเป็นในการดำเนินงานกับองค์กรอย่างเพียงพอและต้องได้รับอนุมัติจากผู้มีอำนาจอย่างเป็นทางการ
- ๘.๔. ต้องมีการควบคุม Port ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

๘.๕. การอนุญาตให้ผู้ใช้เข้าสู่ระบบข้อมูลจากระยะไกลต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้นและ
ไม่ควรเปิดพอร์ตทิ้งไว้โดยไม่จำเป็น ช่องทางดังกล่าวควรตัดการเชื่อมต่อเมื่อไม่ได้งานแล้ว และจะ
เปิดให้ใช้ได้ 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 เพื่อให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรม

๒. การลงทะเบียนผู้ใช้งาน (User Registration)

- ๒.๑. จัดทำแบบฟอร์มการลงทะเบียนผู้ใช้งาน สำหรับระบบเทคโนโลยีสารสนเทศของกรม
- ๒.๒. ผู้ดูแลระบบต้องตรวจสอบบัญชีผู้ใช้งาน โดยเฉพาะผู้ที่ไม่มีประวัติการลงทะเบียนผู้ใช้งานมาก่อน
- 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. ผู้ดูแลระบบต้องมอบหมายสิทธิความรับผิดชอบกับนโยบายควบคุมการเข้าถึง
- 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 โดยหลีกเลี่ยงการใช้อีเมลเป็นช่องทางในการส่ง 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 และบังคับใช้กับผู้ที่ใช้ระบบเทคโนโลยีสารสนเทศของกรม เพื่อป้องกันการเข้าถึงข้อมูลโดยบุคคลอื่นและเปิดเผยข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต

๒. การใช้งานรหัสผ่าน (Password Use)

ผู้ใช้งานระบบเทคโนโลยีสารสนเทศควรปฏิบัติตามข้อกำหนดในการใช้งานรหัสผ่าน ดังนี้

- ๒.๑. ผู้ใช้งานควรตั้งรหัสผ่านที่ยากต่อการเดาโดยผู้อื่น
- ๒.๒. ผู้ใช้งานไม่เปิดเผยรหัสผ่านของตนเอง
- ๒.๓. ผู้ใช้งานควรจัดเก็บรหัสผ่านไว้ในสถานที่ที่มีความปลอดภัย
- ๒.๔. ผู้ใช้งานควรเปลี่ยนรหัสผ่านโดยทันทีเมื่อทราบว่ารหัสผ่านของตนอาจถูกเปิดเผยหรือล่วงรู้โดยผู้อื่น
- ๒.๕. ผู้ใช้งานควรตั้งรหัสผ่านที่มีความยาวเกินกว่าขั้นต่ำที่กำหนดไว้
- 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. ผู้ใช้งานควรเปลี่ยนรหัสผ่านชั่วคราวที่ได้รับโดยทันทีครั้งแรกที่ทำการล็อกอินเข้าสู่ระบบงาน
- ๒.๑๓. ผู้ใช้งานไม่ควรกำหนดให้ทำการบันทึกหรือจดจำรหัสผ่านหรือจดจำรหัสผ่านของตนเองไว้ เพื่อความสะดวกของตนเองเมื่อทำการล็อกอินในภายหลัง
- ๒.๑๔. ผู้ใช้งานไม่ควรใช้รหัสผ่านของตนร่วมกับผู้อื่น
- ๒.๑๕. ผู้ใช้งานควรหลีกเลี่ยงการใช้รหัสผ่านเดียวกันสำหรับระบบงานต่างๆ ที่ใช้งาน

๓. การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์

- ๓.๑. ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานออกจากระบบเทคโนโลยีสารสนเทศโดยทันทีเมื่อเสร็จสิ้นงาน เช่น ระบบงาน เครื่องคอมพิวเตอร์ที่ใช้งาน หรือเครื่องโน้ตบุ๊ก
- ๓.๒. ผู้ใช้งานควรล็อกอุปกรณ์ที่สำคัญเมื่อไม่ได้ใช้งานหรือปล่อยทิ้งไว้โดยไม่ได้ดูแลชั่วคราว
- ๓.๓. ผู้ดูแลระบบควรกำหนดให้พนักงานป้องกันผู้อื่นเข้าใช้เครื่องคอมพิวเตอร์หรือระบบเทคโนโลยีสารสนเทศของตนโดยใส่รหัสผ่านได้ถูกต้องก่อนเข้าใช้งานเครื่องคอมพิวเตอร์

ส่วนที่ ๖

การควบคุมการเข้าถึงและใช้บริการระบบเครือข่าย (Network Access Control)

๑. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องในการปฏิบัติหน้าที่เข้าถึงล่วงรู้ แก่ไขเปลี่ยนแปลงระบบเครือข่ายและการสื่อสารที่สำคัญซึ่งจะทำให้เกิดความเสียหายต่อข้อมูลและระบบสารสนเทศของกรมโดยมีการกำหนดกระบวนการควบคุมการเข้าใช้งานเครือข่ายที่แตกต่างกันของกลุ่มเครือข่ายต่างๆ 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 ในส่วนที่มีใช้ของตนโดยไม่ได้รับอนุญาต การบุกรุก (Hack) เข้าสู่บัญชีผู้ใช้งาน (User Account) ของผู้อื่น การเผยแพร่ข้อความใด ๆ ที่ก่อให้เกิดความเสียหายเสื่อมเสียแก่ผู้อื่น การใช้ภาษาไม่สุภาพหรือการเขียนข้อความที่ทำให้ผู้อื่นเสียหาย ถือเป็นการละเมิดสิทธิของผู้อื่นทั้งสิ้น ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงฝ่ายเดียว กรณฯ ไม่มีส่วนร่วมรับผิดชอบความเสียหายดังกล่าว
- ๒.๔. ห้ามมิให้ผู้ใดเข้าใช้งานโดยมิได้รับอนุญาต การบุกรุกหรือพยายามบุกรุกเข้าสู่ระบบถือว่าเป็นการพยายามรุกรานเขตหวงห้าม ของทางราชการ
- ๒.๕. กรม ให้บัญชีผู้ใช้งาน (User Account) เป็นการเฉพาะบุคคลเท่านั้น ผู้ใช้งานจะโอนหรือแจกสิทธินี้ให้กับผู้อื่นไม่ได้
- ๒.๖. บัญชีผู้ใช้งาน (User Account) ที่กรมฯ ให้กับผู้ใช้งานนั้น ผู้ใช้งานต้องเป็นผู้รับผิดชอบผลต่างๆ อันอาจจะเกิดขึ้น รวมถึงผลเสียหายต่างๆที่เกิดจากบัญชีผู้ใช้งาน (User Account) นั้นๆ เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

๒.๒ ผู้ดูแลระบบห้องควบคุมระบบเครือข่ายและเจ้าหน้าที่กรมมีแนวทางปฏิบัติดังนี้

- ๒.๒.๑. ผู้ดูแลระบบห้องควบคุมระบบเครือข่ายต้องทำการกำหนดสิทธิบุคคลในการเข้าออกห้องควบคุม ระบบเครือข่ายโดยเฉพาะบุคคลที่ปฏิบัติหน้าที่เกี่ยวข้องภายในและมีการบันทึก

- “ทะเบียนผู้มีสิทธิเข้าออกพื้นที่” เช่น เจ้าหน้าที่ปฏิบัติงานคอมพิวเตอร์ (Computer Operator) เจ้าหน้าที่ผู้ดูแลระบบ (System Administrator) เป็นต้น
- ๒.๒.๒. สิทธิในการเข้าออกห้องต่างๆภายในห้องควบคุมระบบเครือข่ายของเจ้าหน้าที่แต่ละคน ต้องได้รับการอนุมัติจากหัวหน้ากลุ่มเทคโนโลยีและสารสนเทศ เป็นลายลักษณ์อักษรโดยสิทธิของเจ้าหน้าที่แต่ละคนขึ้นอยู่กับหน้าที่การปฏิบัติงานภายในห้องควบคุมระบบเครือข่าย
- ๒.๒.๓. ผู้ดูแลระบบห้องควบคุมระบบเครือข่าย จัดเก็บลายนิ้วมือเจ้าหน้าที่ผ่านเครื่องจัดเก็บลายนิ้วมือ และบันทึกข้อมูลลงสื่ายกการ์ด เพื่อบันทึกประวัติการเข้า-ออก ห้องควบคุมระบบเครือข่ายของเจ้าหน้าที่
- ๒.๒.๔. กรณีเจ้าหน้าที่ที่ไม่มีหน้าที่เกี่ยวข้องประจำมีความจำเป็นต้องเข้าออกห้องควบคุมระบบเครือข่ายต้องทำการติดต่อผู้ดูแลระบบห้องควบคุมระบบเครือข่าย เพื่อเข้าห้องควบคุมระบบเครือข่าย พร้อมทั้งระบุเหตุผลการเข้าห้องควบคุมระบบเครือข่าย
- ๒.๒.๕. ผู้ดูแลระบบห้องควบคุมระบบเครือข่าย ต้องทำการแจ้งเจ้าหน้าที่ที่ไม่มีหน้าที่เกี่ยวข้องหลังจากดำเนินการเสร็จ ให้แจ้งผู้ดูแลระบบห้องควบคุมระบบเครือข่ายเพื่อตรวจสอบความเรียบร้อยและความถูกต้อง
- ๒.๓. ผู้ติดต่อจากหน่วยงานภายนอกมีแนวทางปฏิบัติดังนี้
- ๒.๓.๑. ผู้ติดต่อจากหน่วยงานภายนอกต้องทำการติดต่อผู้ดูแลระบบห้องควบคุมระบบเครือข่าย เพื่อเข้าห้องควบคุมระบบเครือข่าย พร้อมทั้งระบุเหตุผลการเข้าห้องควบคุมระบบเครือข่าย
- ๒.๓.๒. ผู้ดูแลระบบห้องควบคุมระบบเครือข่าย ต้องทำการแจ้งผู้ติดต่อจากหน่วยงานภายนอกหลังจากดำเนินการเสร็จ ให้แจ้งผู้ดูแลระบบห้องควบคุมระบบเครือข่ายเพื่อตรวจสอบความเรียบร้อยและความถูกต้อง

ส่วนที่ ๗
การควบคุมการเข้าถึงระบบปฏิบัติการ
(Operating System Access Control)

๑. วัตถุประสงค์

เพื่อให้ผู้ใช้งาน ได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้ระบบปฏิบัติการ รวมทั้งทำความเข้าใจตลอดจนปฏิบัติตามอย่างเคร่งครัด อันจะเป็นการป้องกันทรัพยากรและข้อมูลของหน่วยงานให้มีความลับ ความถูกต้องและมีความพร้อมใช้งานอยู่เสมอ

๒. การกำหนดขั้นตอนการปฏิบัติเพื่อการใช้งานที่มั่นคงปลอดภัย

- ๒.๑. ผู้ใช้งานควรกำหนดรหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ที่รับผิดชอบ
- ๒.๒. ผู้ใช้งานควรตั้งค่าการใช้งานโปรแกรมกั้นหน้าจอ (Screen saver) เพื่อทำการล๊อคหน้าจอเมื่อไม่มีการใช้งาน 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 หรือแจกจ่ายให้ผู้อื่น โดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา
- ๓.๔. ผู้ใช้งานจะต้องลงบันทึกเข้า (Login) โดยใช้บัญชีผู้ใช้บริการ (Account) ของตนเอง และทำการลงบันทึกออก (Logout) ทุกครั้ง เมื่อสิ้นสุดการใช้งานหรือหยุดการใช้งานชั่วคราว

ส่วนที่ ๘

การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application Information Access Control)

๑. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้อนุญาตเข้าถึงระบบสารสนเทศของกรม และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุกจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ที่จะสร้างความเสียหายแก่ข้อมูลหรือการทำงานของระบบเทคโนโลยีสารสนเทศและการสื่อสารให้หยุดชะงักและทำให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรม ได้อย่างถูกต้อง

๒. การจำกัดการเข้าถึงสารสนเทศ (Information Access Control)

- ๒.๑. ผู้ดูแลระบบ (System Administrator) ต้องกำหนดการลงทะเบียนบุคลากรใหม่ของกรม ควรกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการเพื่อให้มีสิทธิต่างๆ ในการทำงานตามความจำเป็น 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) เมื่อผู้ใช้งานระบบลาออกหรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน
 - ๒.๓.๒ ส่งมอบรหัสผ่าน (Password) ชั่วคราวให้กับผู้ใช้บริการด้วยวิธีการที่ปลอดภัย ควรหลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (e-mail) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน (Password)
 - ๒.๓.๓ กำหนดให้ผู้ให้บริการตอบยืนยันการได้รับรหัสผ่าน (Password)
 - ๒.๓.๔ กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง
 - ๒.๓.๕ กำหนดชื่อผู้ใช้หรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน
 - ๒.๓.๖ ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดบ้าง 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 ได้อย่างถูกต้องและสามารถกู้คืนระบบได้ในกรณีจำเป็น

๒.แนวปฏิบัติงานการสำรองข้อมูลและระบบคอมพิวเตอร์

- ๒.๑. ผู้ดูแลระบบคอมพิวเตอร์ ต้องจัดให้มีการสำรองและทดสอบข้อมูลที่สำรองเก็บไว้อย่างสม่ำเสมอ และให้เป็นไปตามนโยบายการสำรองข้อมูลของกรม
- ๒.๒ การจัดทำบันทึกการสำรองข้อมูล (Operator logs) ผู้ดูแลระบบคอมพิวเตอร์ต้องทำบันทึก รายละเอียดการสำรองข้อมูล ได้แก่ เวลาเริ่มต้นและสิ้นสุด ชื่อผู้สำรอง ชนิดของข้อมูลที่บันทึก เป็นต้น
- ๒.๓ การรายงานข้อผิดพลาด (Fault logging) ผู้ดูแลระบบคอมพิวเตอร์ต้องทำรายงานข้อผิดพลาดจากการสำรองข้อมูลที่เกิดขึ้น รวมทั้งวิธีการที่ใช้แก้ไขด้วย
- ๒.๔ ให้ผู้ดูแลระบบคอมพิวเตอร์มอบหมายหน้าที่การสำรองข้อมูลแก่เจ้าหน้าที่คนอื่นไว้สำรอง ในกรณีที่ผู้ดูแลระบบคอมพิวเตอร์และ/หรือผู้ดูแลระบบเครือข่ายไม่สามารถปฏิบัติงานได้
- ๒.๕ ในกรณีที่พบปัญหาในการสำรองข้อมูลจนเป็นเหตุไม่สามารถดำเนินการอย่างสมบูรณ์ได้ให้ดำเนินการแก้ไขปัญหาและสรุปผลการแก้ไขปัญหาและรายงานต่อหัวหน้ากลุ่มเทคโนโลยีสารสนเทศ
- ๒.๖ ให้ผู้ดูแลระบบคอมพิวเตอร์และผู้ดูแลระบบเครือข่ายกำหนดชนิดและช่วงเวลาการสำรองข้อมูลตามความเหมาะสม พร้อมทั้งกำหนดสื่อที่ใช้เก็บข้อมูล โดยรูปแบบการสำรองข้อมูลมีสองชนิด คือ การสำรองข้อมูลแบบเต็ม (Full Backup) และการสำรองข้อมูลแบบส่วนต่าง (Incremental Backup)
- ๒.๗ การเข้ารหัสข้อมูลสำคัญในการสำรองข้อมูล (Encrypted backup) ผู้ดูแลระบบคอมพิวเตอร์ต้องจัดให้มีการเข้ารหัสข้อมูลสำรองที่สำคัญ 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
		ข้อมูลในฐานข้อมูลของระบบที่สำคัญ	๑ ครั้งต่อสัปดาห์
	Firewall , Proxy , IPS , DNS , CoreSwitch	ค่า configure	ก่อนและหลังการเปลี่ยนแปลง
		ข้อมูล Rule ของอุปกรณ์	๑ ครั้งต่อเดือน
	Server อื่น ๆ เช่นระบบงานต่างๆ	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 กำหนดกระบวนการในการวางแผนรับมือกับเหตุภัยพิบัติสำหรับระบบที่มีความสำคัญสูง

๔.๒ กำหนดชนิดของภัยพิบัติที่มีผลต่อระบบที่มีความสำคัญสูงและจำเป็นต้องวางแผนรับมือ

๔.๓ ทำการประเมินความเสี่ยงที่มีผลทำให้ระบบที่มีความสำคัญสูง ติดขัดหรือไม่สามารถใช้งานได้ อันเป็นผลจากภัยพิบัติที่กำหนดไว้

๔.๔ จัดทำแผนรับมือกับเหตุภัยพิบัติสำหรับระบบที่มีความสำคัญสูง

๔.๕ ทดสอบ/ประเมินและปรับปรุงแผนรับมือกับเหตุภัยพิบัติสำหรับระบบที่มีความสำคัญสูง อย่างน้อยปีละ ๑ ครั้ง

ส่วนที่ ๑๐

การตรวจสอบและประเมินความเสี่ยง

๑.วัตถุประสงค์

เพื่อให้มีมาตรการในการควบคุมความเสี่ยงและป้องกันเหตุการณ์ที่อาจมีผลต่อความมั่นคงปลอดภัยด้านสารสนเทศ

๒.แนวปฏิบัติการประเมินความเสี่ยง

๒.๑. ระบุความเสี่ยงและเหตุการณ์ความเสี่ยงให้สอดคล้องตามแผนบริหารความเสี่ยงของกรม เพื่อการประเมินความเสี่ยงนั้น

๒.๒.๑ ระบบเทคโนโลยีสารสนเทศได้รับความเสียหาย เนื่องจากเจ้าหน้าที่หรือบุคลากรของหน่วยงาน (Human error), ไวรัสมัลแวร์ (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 ดำเนินการทบทวนแผนแก้ไขปัญหามาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดขึ้นกับระบบสารสนเทศ (IT Contingency Plan)

๒.๔.๒ จัดทำหลักเกณฑ์นโยบายกฎระเบียบในการใช้เครื่องคอมพิวเตอร์และเครือข่ายของกรม

ส่วนที่ ๑๑
นโยบายความมั่นคงปลอดภัยของการใช้งานอินเทอร์เน็ต
(Internet Security Policy)

๑. วัตถุประสงค์

เพื่อให้ผู้ใช้รับทราบกฎเกณฑ์แนวทางปฏิบัติในการใช้งานอินเทอร์เน็ตอย่างปลอดภัยและเป็นการป้องกันไม่ให้เกิดพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ เช่น การส่งข้อมูล ข้อความ คำสั่งชุดคำสั่งหรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์แก่บุคคลอื่นอันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุขทำให้ระบบคอมพิวเตอร์ของกรมถูกระงับชะลอขัดขวางหรือถูกรบกวนจนไม่สามารถทำงานตามปกติได้

๒. แนวทางปฏิบัติในการใช้งานอินเทอร์เน็ต

- ๒.๑. ผู้ดูแลระบบควรกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ตที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่กรมจัดสรรไว้เท่านั้นเช่น Proxy, Firewall, IPS-IDS เป็นต้น ห้ามผู้ใช้ทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น ยกเว้นแต่ว่ามีเหตุผลความจำเป็นและทำการขออนุญาตจากกลุ่มเทคโนโลยีและสารสนเทศ สำนักแผนงาน เป็นลายลักษณ์อักษร
- ๒.๒. เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา ก่อนทำการเชื่อมต่ออินเทอร์เน็ตผ่านเว็บเบราว์เซอร์ (Web browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัสและทำการอัปเดตช่องโหว่ของระบบปฏิบัติการเว็บเบราว์เซอร์
- ๒.๓. ผู้ใช้ หมั่น Update Patch และ HotFix อย่างสม่ำเสมอ โดยสามารถ Download patch และ HotFix ต่างๆ จาก Microsoft web site เพื่อแก้ปัญหาช่องโหว่
- ๒.๔. ในการรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเทอร์เน็ตจะต้องมีการทดสอบไวรัส (Virus scanning) โดยโปรแกรมป้องกันไวรัสก่อนการรับส่งข้อมูลทุกครั้ง
- ๒.๕. ผู้ใช้ ต้องไม่ใช้เครือข่ายอินเทอร์เน็ตของกรม เพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัวและทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสมเช่นเว็บไซต์ที่ขัดต่อศีลธรรมเว็บไซต์ที่มีเนื้อหาที่ขัดต่อชาติ ศาสนา พระมหากษัตริย์หรือเว็บไซต์ที่เป็นภัยต่อสังคม เป็นต้น
- ๒.๖. ผู้ใช้จะถูกกำหนดสิทธิในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบ เพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยทางข้อมูลของกรม
- ๒.๗. ผู้ใช้ ต้องไม่เผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัวหรือข้อมูลที่ไม่เหมาะสมทางศีลธรรมหรือข้อมูลที่ละเมิดสิทธิของผู้อื่นหรือข้อมูลที่อาจก่อความเสียหายให้กับกรม
- ๒.๘. ห้ามผู้ใช้ เปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของกรมที่ยังไม่ได้ประกาศอย่างเป็นทางการ ผ่านอินเทอร์เน็ต
- ๒.๙. ผู้ใช้ไม่นำเข้าข้อมูลคอมพิวเตอร์ที่เป็นภาพของผู้อื่นและภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้นตัดต่อเติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใดทั้งนี้จะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่นถูกเกลียดชังหรือได้รับความอับอาย
- ๒.๑๐. หลังจากใช้งานอินเทอร์เน็ตเสร็จแล้วให้ทำการปิดเว็บเบราว์เซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น

ส่วนที่ ๑๒
แนวทางการใช้งานจดหมายอิเล็กทรอนิกส์
(Use of Electronic Mail)

๑. วัตถุประสงค์

- ๑.๑ เพื่อให้การรับส่งข้อมูลข่าวสารด้วยจดหมายอิเล็กทรอนิกส์ของกรม สามารถสนับสนุนการปฏิบัติงานของกรมเจ้าท่า และการบริหารงานของกรมเจ้าท่า เป็นไปอย่างถูกต้อง สะดวก รวดเร็ว ทันสถานการณ์ มีประสิทธิภาพ และประสิทธิผล
- ๑.๒ เพื่อให้การติดต่อสื่อสารโดยการรับ-ส่งข้อมูลข่าวสารด้วยจดหมายอิเล็กทรอนิกส์ สำหรับบุคลากรของกรม และหน่วยงาน เป็นมาตรฐาน อยู่ในกรอบของกฎหมาย ระเบียบ คำสั่ง ข้อบังคับ ของกรมเจ้าท่า

๒. แนวทางปฏิบัติในการส่งจดหมายอิเล็กทรอนิกส์

- ๒.๑. ผู้ดูแลระบบต้องกำหนดสิทธิการเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของกรมให้เหมาะสมกับการเข้าใช้บริการของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของผู้ใช้รวมทั้งมีการทบทวนสิทธิการเข้าใช้งานอย่างสม่ำเสมอเช่น การลาออกเป็นต้น
- ๒.๒. ผู้ดูแลระบบต้องกำหนดสิทธิบัญชีรายชื่อผู้ใช้อย่างใหม่และรหัสผ่านสำหรับการใช้งานครั้งแรกเพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ระบบจดหมายอิเล็กทรอนิกส์ของกรม
- ๒.๓. สำหรับผู้ใช้อย่างใหม่จะได้รับรหัสผ่านครั้งแรก (default password) ในการผ่านเข้าระบบจดหมายอิเล็กทรอนิกส์และเมื่อมีการเข้าสู่ระบบในครั้งแรกนั้นระบบจะต้องมีการบังคับให้เปลี่ยนรหัสผ่านโดยทันที
- ๒.๔. รหัสจดหมายอิเล็กทรอนิกส์เวลาใส่รหัสผ่านต้องไม่ปรากฏหรือแสดงรหัสผ่านออกมา แต่ต้องแสดงออกมาในรูปแบบของสัญลักษณ์แทนตัวอักษรนั้นเช่น 'x' หรือ 'o' ในการพิมพ์แต่ละตัวอักษร
- ๒.๕. ผู้ดูแลระบบควรกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิดได้ไม่เกิน ๓ ครั้ง
- ๒.๖. ผู้ดูแลระบบควรกำหนดให้ระบบจดหมายอิเล็กทรอนิกส์ควรมีการล็อกเข้าที่ออกจากหน้าจอตัดการใช้งานผู้ใช้เมื่อผู้ใช้ไม่ได้ใช้งานระบบเป็นระยะเวลาตามที่กำหนดไว้เช่น ๑๕ นาที เมื่อต้องการเข้าใช้งานต่อต้องใส่ชื่อผู้ใช้และรหัสผ่านอีกครั้ง
- ๒.๗. ผู้ใช้ไม่ควรตั้งค่าการใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ (save password) ของระบบจดหมายอิเล็กทรอนิกส์
- ๒.๘. ผู้ใช้ควรมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัดเช่นควรเปลี่ยนรหัสผ่านทุก ๓-๖ เดือน
- ๒.๙. ผู้ใช้ ควรระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์เพื่อไม่ให้เกิดความเสียหายต่อกรม หรือ ละเมิดสิทธิ์ สร้างความรำคาญต่อผู้อื่นหรือผิดกฎหมายหรือละเมิดศีลธรรมและไม่แสวงหาประโยชน์หรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจจากการใช้จดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายของกรม
- ๒.๑๐. ผู้ใช้ไม่ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (e-mail address) ของผู้อื่นเพื่ออ่านรับส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้และให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานต่างๆในจดหมายอิเล็กทรอนิกส์ของตน
- ๒.๑๑. ผู้ใช้ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ของกรมเพื่อการทำงานของกรมเท่านั้น

- ๒.๑๒. หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้นควรทำการล็อกเอาท์ออกจากระบบทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์
- ๒.๑๓. ผู้ใช้ ควรทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนทำการเปิดเพื่อทำการตรวจสอบไฟล์โดยใช้โปรแกรมป้องกันไวรัสเป็นการป้องกันในการเปิดไฟล์ที่เป็น Executable file เช่น .exe .com เป็นต้น
- ๒.๑๔. ผู้ใช้ไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก
- ๒.๑๕. ผู้ใช้ไม่ควรใช้ข้อความที่ไม่สุภาพหรือรับส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสมข้อมูลอันอาจทำให้เสียชื่อเสียงของกรมทำให้เกิดความแตกแยกระหว่างกรมผ่านทางจดหมายอิเล็กทรอนิกส์
- ๒.๑๖. ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์
- ๒.๑๗. ผู้ใช้ ควรตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ของตนเองทุกวันและควรจัดเก็บแฟ้มข้อมูลและจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจำนวนน้อยที่สุด
- ๒.๑๘. ผู้ใช้ ควรลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้เนื้อที่ระบบจดหมายอิเล็กทรอนิกส์

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.๒๕๓๗
- ๒.๑.๖ ระเบียบว่าด้วยการรักษาความปลอดภัยแห่งชาติเกี่ยวกับการสื่อสาร พ.ศ.๒๕๒๕
- ๒.๑.๗ ข้อตกลง เงื่อนไขการใช้บริการที่กรม กำหนด

๓. ข้อตกลงและเงื่อนไขการใช้บริการจดหมายอิเล็กทรอนิกส์ของกรม

- ๓.๑ หน่วยงาน/บุคคลผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ของกรม จะต้องใช้จดหมายอิเล็กทรอนิกส์ของกรม เพื่อผลประโยชน์ของทางราชการ
- ๓.๒ ห้ามใช้ระบบจดหมายอิเล็กทรอนิกส์ของกรม เพื่อการประกอบธุรกิจ หรือแสวงหาผลประโยชน์ส่วนตัว
- ๓.๓ ห้ามใช้บริการนี้ ไปในการเผยแพร่ อ้างอิง พาดพิง ดูหมิ่น หรือการกระทำใดๆ ที่ก่อให้เกิดความเสียหายต่อสถาบันชาติ ศาสนา และ พระมหากษัตริย์
- ๓.๔ ห้ามใช้ระบบจดหมายอิเล็กทรอนิกส์ของกรม ในการประกอบอาชญากรรมทางคอมพิวเตอร์ หรือการกระทำการใด ๆ ซึ่งผิดกฎหมาย คำสั่ง ระเบียบ ข้อบังคับ และมาตรการรักษาความปลอดภัยข้อมูล ข่าวสารลับของทางราชการ
- ๓.๕ ห้ามใช้ระบบจดหมายอิเล็กทรอนิกส์ของกรม เพื่อการเผยแพร่ข้อมูลข่าวสาร หรือภาพ เสียง ข้อความ ที่ไม่เหมาะสม หรือสร้างความเสียหายให้กับผู้อื่น
- ๓.๖ ห้ามใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-Mail Address) ไปแสดงความคิดเห็นส่วนตัวที่ส่งผลกระทบต่อในทางลบ หรือสร้างความเสียหายหรือเสียหายต่อบุคคลหรือองค์กร
- 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 ที่อาจจะนำมาซึ่งความเสียหาย หรือก่อให้เกิดความเสียหายแก่ระบบเครื่องแม่ข่ายจดหมายอิเล็กทรอนิกส์ของ กรม
- ๓.๑๐ ผู้ใช้ต้องรักษารหัสผ่าน(Password) ส่วนบุคคล หรือหน่วยงานของจดหมายอิเล็กทรอนิกส์เป็นไว้เป็นความลับ
- ๓.๑๑ ห้ามส่งข้อมูลข่าวสารอันเป็นความลับของทางราชการให้กับบุคคลหรือหน่วยงานที่ไม่เกี่ยวข้องกับการราชการของกรม
- ๓.๑๒ การส่งข้อมูลข่าวสารที่เป็นความลับของทางราชการให้กับบุคคลหรือหน่วยงานนอกกรม จะต้องเข้ารหัสข้อมูลข่าวสารนั้นตามวิธีปฏิบัติ 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 ทั้งในรูปแบบของอีเมลล์ และ/หรือโฮมเพจของผู้ใช้บริการ ให้ถือเป็นการกระทำที่อยู่ภายใต้ความรับผิดชอบของผู้ใช้บริการ กลุ่มเทคโนโลยี และสารสนเทศ สำนักแผนงาน ไม่มีส่วนเกี่ยวข้องใดๆ

ส่วนที่ ๑๔

การควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร (Third party access control)

๑. วัตถุประสงค์

การใช้บริการจากหน่วยงานภายนอกอาจก่อให้เกิดความเสี่ยงได้ เช่น ความเสี่ยงต่อการเข้าถึงข้อมูล ความเสี่ยงต่อการถูกแก้ไขข้อมูลอย่างไม่ถูกต้องและการประมวลผลของระบบงานโดยไม่ได้รับอนุญาต เป็นต้น เพื่อให้การควบคุมหน่วยงานภายนอกที่มีการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กรให้เป็นไปอย่างมั่นคงปลอดภัย และกำหนดแนวทางในการคัดเลือกควบคุมการปฏิบัติงานของหน่วยงานภายนอก เช่น การพัฒนาระบบการใช้บริการของที่ปรึกษาการใช้บริการด้านระบบเทคโนโลยีสารสนเทศจากหน่วยงานภายนอก เป็นต้น

๒. แนวทางปฏิบัติ

๒.๑. หัวหน้ากลุ่มเทคโนโลยีและสารสนเทศ สำนักแผนงาน ต้องกำหนดให้มีการประเมินความเสี่ยงจากการเข้าถึงระบบเทคโนโลยี สารสนเทศและการสื่อสารหรืออุปกรณ์ที่ใช้ในการประมวลผลโดยหน่วยงานภายนอกและกำหนดมาตรการรองรับหรือแก้ไขที่เหมาะสมก่อนที่จะอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารได้

๒.๒. การควบคุมการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงานภายนอก

๒.๒.๑. บุคคลภายนอกที่ต้องการสิทธิในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรม จะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษรเพื่อขออนุมัติจากหัวหน้ากลุ่มเทคโนโลยีและสารสนเทศ สำนักแผนงาน

๒.๒.๒. จัดทำเอกสารแบบฟอร์มสำหรับให้หน่วยงานภายนอกทำการระบุเหตุผลความจำเป็นที่ต้องใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร ซึ่งต้องมีรายละเอียดอย่างน้อยดังนี้

- เหตุผลในการขอใช้
- ระยะเวลาในการใช้
- การตรวจสอบความปลอดภัยของอุปกรณ์ที่เชื่อมต่อเครือข่าย
- การตรวจสอบ MAC address ของเครื่องคอมพิวเตอร์ที่เชื่อมต่อ
- การกำหนดการป้องกันในเรื่องการเปิดเผยข้อมูล

๒.๒.๓. หน่วยงานภายนอกที่ทำงานให้กับกรม ทุกหน่วยงานไม่ว่าจะทำงานอยู่ภายในกรม หรือนอกสถานที่จำเป็นต้องลงนามในสัญญาการไม่เปิดเผยข้อมูลของกรม โดยสัญญาต้องจัดทำให้เสร็จก่อนให้สิทธิในการเข้าสู่ระบบเทคโนโลยีสารสนเทศ

๒.๒.๔. กรมควรพิจารณาการเข้าไปประเมินความเสี่ยงหรือจัดทำกรควบคุมภายในของหน่วยงานภายนอกทั้งนี้ ขึ้นอยู่กับความสำคัญของระบบเทคโนโลยีสารสนเทศและการสื่อสาร ที่เข้าไปปฏิบัติงาน

๒.๒.๕. เจ้าของโครงการซึ่งรับผิดชอบต่อโครงการที่มีการเข้าถึงข้อมูลโดยหน่วยงานภายนอกต้องกำหนดการเข้าใช้งานเฉพาะบุคคลที่จำเป็นเท่านั้นและให้หน่วยงานภายนอกลงนามในสัญญาไม่เปิดเผยข้อมูล

- ๒.๒.๖. สำหรับโครงการขนาดใหญ่หน่วยงานภายนอกที่สามารถเข้าถึงข้อมูลที่มีความสำคัญของกรม ผู้ดูแลระบบต้องควบคุมการปฏิบัติงานนั้นๆให้มีความมั่นคงปลอดภัยทั้ง ๓ ด้านคือ การรักษาความลับ (Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity) และ การรักษาความ พร้อมที่จะให้บริการ (Availability)
- ๒.๒.๗. กรมมีสิทธิในการตรวจสอบตามสัญญาการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อให้มั่นใจได้ว่ากรมสามารถควบคุมการใช้งานได้อย่างทั่วถึงตามสัญญานั้น
- ๒.๒.๘. ควรดำเนินการให้ผู้ให้บริการหน่วยงานภายนอกจัดทำแผนการดำเนินงานคู่มือการปฏิบัติงาน และเอกสารที่เกี่ยวข้องรวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอเพื่อควบคุมหรือตรวจสอบ การให้บริการของผู้ให้บริการได้อย่างเข้มงวดเพื่อให้มั่นใจได้ว่าเป็นไปตามขอบเขต ที่ได้ กำหนดไว้

การดำเนินการตอบสนองเหตุการณ์ความมั่นคงปลอดภัยทางระบบสารสนเทศ

๑. ระบบป้องกันผู้บุกรุก

แผนดำเนินการรายวัน

๑. ดำเนินการตรวจสอบไฟล์ล็อกหรือรายงานของระบบป้องกันการบุกรุก สิ่งที่ทำตรวจสอบดังต่อไปนี้

- 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) และรายงานของไฟร์วอลล์ สิ่งที่ต้องตรวจสอบมีดังต่อไปนี้
 - ๒.๑ Packet ที่ไฟร์วอลล์ได้ทำการ Block
 - ๒.๒ ลักษณะของ Packet ที่ถูก Block
 - ๒.๓ Packet ของหมายเลขไอพี ของเครือข่ายใดถูก Block เป็นจำนวนมาก
๓. กรณีตรวจพบการโจมตีระบบหรือเหตุการณ์ละเมิดความปลอดภัยระบบสารสนเทศให้แจ้งหัวหน้ากลุ่มเทคโนโลยีสารสนเทศ เพื่อตัดสินใจดำเนินการแก้ไขปัญหา

๓. ระบบป้องกันภัยคุกคามทางอินเทอร์เน็ต

ภัยคุกคามทางอินเทอร์เน็ตหรือมัลแวร์ (Malware) ประกอบด้วย ไวรัส หนอนอินเทอร์เน็ต โทรจัน รวมถึงสปายแวร์

แผนดำเนินการรายวัน/รายสัปดาห์/รายเดือน

๑. ดำเนินการตรวจสอบไฟล์ล็อกและรายงานของอุปกรณ์ที่เกี่ยวข้องกับระบบป้องกันภัยคุกคามทางอินเทอร์เน็ต สิ่งที่ต้องตรวจสอบมีดังนี้
 - ๑.๑ มัลแวร์ประเภทใดถูกพบเป็นจำนวนมาก
 - ๑.๒ มัลแวร์ถูกส่งมาจากเครือข่ายใด และถูกส่งไปยังที่ใด
 - ๑.๓ มีการส่งมัลแวร์จากเครือข่ายภายในกรม ไปยังภายนอกหรือไม่
๒. ศึกษาหาวิธีแก้ไขเครื่องคอมพิวเตอร์ที่ติดมัลแวร์ โดยเฉพาะมัลแวร์ประเภทที่ตรวจพบว่ากระจายอยู่ในเครือข่ายของกรม
๓. ตรวจสอบพบว่าเครื่องคอมพิวเตอร์ภายในเครือข่ายติดมัลแวร์หรือส่งมัลแวร์ออกไปข้างนอก ควรระงับการเชื่อมต่อของเครื่องที่ติดมัลแวร์กับระบบเครือข่าย แล้วทำการแก้ไขเครื่องนั้นทันที