นโยบายความมั่นคงปลอดภัยของระบบสารสนเทศ
กรมสนับสนุนบริการสุขภาพ ฉบับปรับปรุงปีงบประมาณ พ.ศ.๒๕๕๗

๑. วัตถุประสงค์และขอบเขต

เพื่อให้ระบบสารสนเทศของกรมสนับสนุนบริการสุขภาพ มีความมั่นคงปลอดภัยสามารถดำเนินงานได้อย่างต่อเนื่องป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานเครื่องมืออุปกรณ์เทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง และการถูกคุกคามจากภัยต่างๆ กรมสนับสนุนบริการสุขภาพจึงเห็นสมควรกำหนดนโยบายการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ โดยกำหนดให้มีมาตรฐาน (Standard) แนวปฏิบัติ (Guideline) ขั้นตอนการปฏิบัติ (Procedure) ให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศและป้องกันภัยคุกคามต่างๆ โดยมีวัตถุประสงค์ดังต่อไปนี้

๑.๑ การจัดทำนโยบายการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศเพื่อให้เกิดความเชื่อมั่นและมีความปลอดภัยในการใช้งานระบบสารสนเทศ หรือเครือข่ายคอมพิวเตอร์ของกรมสนับสนุนบริการสุขภาพ ทำให้ดำเนินงานได้อย่างปลอดภัย และ ต่อเนื่อง

๑.๒ กำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยระบบสารสนเทศ โดยอ้างอิงตามมาตรฐานสากลISO/IEC ๒๗๐๐๐๑ และที่ได้ปรับปรุงแก้ไขเพิ่มเติมในภายหน้า

๑.๓ นโยบายนี้จะต้องทำการเผยแพร่ให้เจ้าหน้าที่ทุกระดับในกรมสนับสนุนบริการสุขภาพได้รับทราบและเจ้าหน้าที่ทุกคนต้องปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

๑.๔ เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีปฏิบัติ ให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับกรมสนับสนุนบริการสุขภาพ ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศขององค์กรในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด

๒. องค์ประกอบของนโยบาย

หมวดที่ ๑ นโยบายหลัก

๑. การพิสูจน์ตัวตน
๒. การบริหารจัดการทรัพย์สิน
๓. การบริหารจัดการข้อมูลองค์กร
๔. การบริหารจัดการระบบสารสนเทศ
๕. การปฏิบัติตามกฎหมายและข้อบังคับ
๖. ซอฟต์แวร์และลิขสิทธิ์
๗. การป้องกันโปรแกรมไม่ประสงค์ดี

หมวดที่ ๒ นโยบายตามมาตรฐานสากล หน่วยงานในสังกัดกรมสนับสนุนบริการสุขภาพ ต้องดำเนินธุรกรรมทางอิเล็กทรอนิกส์ ให้เป็นไปในแนวทางของมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ ที่อ้างอิงตามมาตรฐาน ISO/IEC ๒๗๐๐๑ และ ที่ได้ปรับปรุงแก้ไขเพิ่มเติมในภายหน้า

หมวดที่ ๓ การแบ่งอำนาจหน้าที่ และ การดำเนินงานหน่วยงานส่วนกลาง และ หน่วยงานในส่วนภูมิภาค

องค์ประกอบของนโยบายการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของกรมสนับสนุนบริการสุขภาพ แต่ละส่วนที่กล่าวข้างต้นจะประกอบด้วยวัตถุประสงค์ รายละเอียดของมาตรฐาน (Standard) แนวทางปฏิบัติ (Guideline) และขั้นตอนวิธีการปฏิบัติ (Procedure) เพื่อจะทำให้กรมสนับสนุนบริการสุขภาพมีมาตรการในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศอยู่ในระดับที่ปลอดภัย ช่วยลดความเสียหายต่อการดำเนินงาน ทรัพย์สิน บุคลากร ของกรมสนับสนุนบริการสุขภาพ นโยบายการเข้าใช้งานระบบสารสนเทศของกรมสนับสนุนบริการสุขภาพนี้ จัดเป็นมาตรฐานด้านความปลอดภัยในการใช้งานระบบสารสนเทศของกรมสนับสนุนบริการสุขภาพ ซึ่งเจ้าหน้าที่ของกรมสนับสนุนบริการสุขภาพและหน่วยงานภายนอกจะต้องปฏิบัติตามอย่างเคร่งครัด

คำนิยาม

คำนิยามที่ใช้ในนโยบายนี้ ประกอบด้วย

- **องค์กร** หมายถึง กรมสนับสนุนบริการสุขภาพ
- **ผู้บังคับบัญชา** หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารงานของกรม
- **กลุ่มเทคโนโลยีสารสนเทศ สำนักบริหาร** หมายถึง หน่วยงานบริหาร จัดการ และ ดำเนินงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร เสนอแนะนโยบาย ให้คำปรึกษา พัฒนาปรับปรุง บำรุงรักษาระบบคอมพิวเตอร์และเครือข่ายของกรมสนับสนุนบริการสุขภาพ
- **หัวหน้ากลุ่มเทคโนโลยีสารสนเทศ** หมายถึง ผู้มีอำนาจในด้านเทคโนโลยีสารสนเทศและการสื่อสารของกรมสนับสนุนบริการสุขภาพ ซึ่งบทบาทหน้าที่และความรับผิดชอบในส่วนของการกำหนดนโยบายมาตรฐาน การควบคุมดูแลการใช้งานระบบสารสนเทศ
- **การรักษาความมั่นคงปลอดภัย** หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับระบบสารสนเทศของกรมสนับสนุนบริการสุขภาพ
- **มาตรฐาน** (Standard) หมายถึงบรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริงเพื่อให้ได้ตามวัตถุประสงค์หรือเป้าหมาย
- **วิธีการปฏิบัติ**(Procedure) หมายถึง รายละเอียดที่บอกขั้นตอนเป็นข้อๆ ที่ต้องนำมาปฏิบัติเพื่อให้ได้มาซึ่งมาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์
- **แนวทางปฏิบัติ**(Guideline) หมายถึงแนวทางที่ไม่ได้บังคับให้ปฏิบัติ แต่แนะนำให้ปฏิบัติตามเพื่อให้สามารถบรรลุเป้าหมายได้ง่ายขึ้น
- **ผู้ใช้** หมายถึง บุคคลที่ได้รับอนุญาต (Authorized User) ให้สามารถเข้าใช้งาน บริหาร หรือดูแลรักษาระบบสารสนเทศของกรมสนับสนุนบริการสุขภาพ โดยมีสิทธิและหน้าที่ขึ้นอยู่กับบทบาท ซึ่งกรมกำหนดไว้ดังนี้
    - ผู้บริหาร หมายถึง ผู้มีอำนาจบริหารในระดับสูงของกรม เช่น หัวหน้าหน่วยราชการ เป็นต้น
    - ผู้ดูแลระบบ (System Administrator) หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบและเครือข่ายคอมพิวเตอร์ซึ่งสามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์ เพื่อจัดการฐานข้อมูลเครือข่ายคอมพิวเตอร์
    - เจ้าหน้าที่ หมายถึง ข้าราชการ พนักงานราชการ ลูกจ้างประจำ ลูกจ้างชั่วคราว และพนักงานเจ้าหน้าบริการ
- **หน่วยงานภายนอก** หมายถึง องค์กรหรือหน่วยงานภายนอกที่กรมสนับสนุนบริการสุขภาพอนุญาตให้มีสิทธิในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่างๆ ของหน่วยงาน โดยจะได้รับสิทธิในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล
- **ข้อมูลคอมพิวเตอร์** หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์

- **สารสนเทศ** (Information) หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปตัวเลข ข้อความ หรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่ายและสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่นๆ
- **ระบบคอมพิวเตอร์** หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ
- **ระบบเครือข่าย** (Network System) หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบสารสนเทศต่างๆ ของกรมสนับสนุนบริการสุขภาพ ได้ เช่น ระบบ LAN , ระบบ Intranet ระบบ Internet เป็นต้น
    - ระบบ LAN และระบบ Intranet หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่างๆ ภายในหน่วยงานเข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน
    - ระบบ Internet หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่างๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตทั่วโลก
- ระบบสารสนเทศ(Information System) หมายถึง ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูลและสารสนเทศ เป็นต้น
- พื้นที่ใช้งานระบบสารสนเทศ(Information System Workspace) หมายถึง พื้นที่ที่หน่วยงานอนุญาตให้มีการใช้งานระบบสารสนเทศ โดยแบ่งเป็น
    - ห้องปฏิบัติงาน พื้นที่ทำงานทั่วไป (General working area) หมายถึง พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคล และคอมพิวเตอร์พกพา (Notebook) ที่ประจำโต๊ะทำงาน
    - พื้นที่ทำงานของผู้ดูแลระบบ (System administrator area)
    - พื้นที่ติดตั้งอุปกรณ์ระบบสารสนเทศหรือระบบเครือข่าย (IT equipment or network area)
    - พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data storage area)
    - พื้นที่ใช้งานระบบเครือข่ายไร้สาย (Wireless LAN coverage area)
- **เจ้าของข้อมูล** หมายถึง ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงานโดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้นๆ หรือ ได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย
- **ทรัพย์สิน** หมายถึง ข้อมูล ระบบข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน เช่นอุปกรณ์ระบบเครือข่าย ซอฟท์แวร์ที่มีลิขสิทธิ์ เป็นต้น
- **จดหมายอิเล็กทรอนิกส์**(e-mail) หมายถึง ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกัน โดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข่าวสาร ไปยังผู้รับคนเดียวหรือหลายคนก็ได้ มาตรฐานที่ใช้ในการรับส่งข้อมูลชนิดนี้ ได้แก่ SMTP , POP๓ และ IMAP เป็นต้น

- **รหัสผ่าน**(Password) หมายถึง ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศ
- **ชุดคำสั่งไม่พึงประสงค์** หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

หมวดที่ ๑

นโยบายหลัก

ข้อ ๑การพิสูจน์ตัวตน (Accountability, Identification and Authentication)

ผู้ใช้งานมีหน้าที่ในการป้องกันดูแลรักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) โดยผู้ใช้งานแต่ละคนต้องมีบัญชีชื่อผู้ใช้งาน (Username) ของตนเองห้ามใช้ร่วมกับผู้อื่นรวมทั้งห้ามทำการเผยแพร่แจกจ่ายทำให้ผู้อื่นล่วงรู้รหัสผ่าน (Password)

ข้อ ๒ การบริหารจัดการทรัพย์สิน (Assets Management)

ผู้ใช้งานต้องไม่เข้าไปในห้องคอมพิวเตอร์แม่ข่าย (Server) ที่เป็นเขตหวงห้ามโดยเด็ดขาดเว้นแต่ได้รับอนุญาตจากผู้ดูแลระบบ / ไม่นำอุปกรณ์หรือชิ้นส่วนใดออกจากห้องคอมพิวเตอร์แม่ข่าย (Server) เว้นแต่จะได้รับอนุญาตจากผู้ดูแลระบบ / ไม่นำเครื่องมือหรืออุปกรณ์อื่นใด เชื่อมเข้าเครือข่ายเพื่อการประกอบธุรกิจส่วนบุคคล / ไม่ใช้หรือลบแฟ้มข้อมูลของผู้อื่นไม่ว่ากรณีใดๆ / ไม่คัดลอกหรือทำสำเนาแฟ้มข้อมูลที่มีลิขสิทธิ์กำกับการใช้งานก่อนได้รับอนุญาต

ข้อ ๓ การบริหารจัดการข้อมูลองค์กร (Corporate Management)

ข้อมูลทั้งหลายที่อยู่ภายในทรัพย์สินของกรมสนับสนุนบริการสุขภาพ และ ที่อยู่ในทรัพย์สินที่ตั้งของสำนัก/กองในสังกัดกรมสนับสนุนบริการสุขภาพ ถือเป็นทรัพย์สินของกรมสนับสนุนบริการสุขภาพ ห้ามไม่ให้ทำการเผยแพร่เปลี่ยนแปลงทำซ้ำหรือทำลายโดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

ข้อ ๔ การบริหารจัดการระบบสารสนเทศ (IT Infrastructure Management)

ผู้ใช้งานจะไม่พัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆที่จะทำลายกลไกรักษาความปลอดภัยระบบ รวมทั้งการกระทำในลักษณะเป็นการแอบใช้รหัสผ่านการลักลอบทำสำเนาข้อมูลบุคคลอื่นหรือแกะรหัสผ่านของบุคคลอื่น / พัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆซึ่งทำให้ผู้ใช้มีสิทธิและลำดับความสำคัญในการครอบครองทรัพยากรระบบมากกว่าผู้ใช้อื่น / พัฒนาโปรแกรมใดที่จะทำซ้ำตัวโปรแกรมหรือแฝงตัวโปรแกรมไปกับโปรแกรมอื่นในลักษณะเช่นเดียวกับหนอนหรือไวรัสคอมพิวเตอร์ / พัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆที่จะทำลายระบบจำกัดสิทธิการใช้ (License)ซอฟต์แวร์ / นำเสนอข้อมูลที่ผิดกฎหมายละเมิดลิขสิทธิ์แสดงข้อความรูปภาพไม่เหมาะสมหรือ ขัดต่อศีลธรรมประเพณีอันดีงามของประเทศไทย

ข้อ ๕ การปฏิบัติตามกฎหมายและข้อบังคับ (Law and Compliance)

บรรดากฎหมายใดๆที่ได้ประกาศใช้ในประเทศไทยรวมทั้งกฎระเบียบของกรมสนับสนุนบริการสุขภาพถือเป็นสิ่งสำคัญที่ผู้ใช้งานต้องตระหนักและปฏิบัติตามอย่างเคร่งครัด และไม่กระทำความผิดนั้นดังนั้นหากผู้ใช้งานกระทำผิดตามกฎหมายดังกล่าวถือว่าความผิดนั้นเป็นความผิดส่วนบุคคลซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

ข้อ ๖ ซอฟต์แวร์และลิขสิทธิ์ (Software Licensing and intellectual property)

กรมสนับสนุนบริการสุขภาพ ให้ความสำคัญต่อทรัพย์สินทางปัญญาดังนั้นซอฟต์แวร์ที่อนุญาตให้ใช้งานมีลิขสิทธิ์ถูกต้องผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็นและ ห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์หากมีการตรวจสอบพบความผิดฐานละเมิดลิขสิทธิ์ ให้ถือว่าเป็นความผิดส่วนบุคคลผู้ใช้งานจะต้องรับผิดชอบแต่เพียงผู้เดียว

ข้อ ๗ การป้องกันโปรแกรมไม่ประสงค์ดี (Preventing MalWare)

คอมพิวเตอร์ของผู้ใช้งานได้ติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ (Anti virus) ตามที่กรมสนับสนุนบริการสุขภาพได้ประกาศให้ใช้เว้นแต่คอมพิวเตอร์นั้นเป็นเครื่องเพื่อการศึกษาพัฒนาระบบป้องกันโดยต้องได้รับอนุญาตจากผู้บังคับบัญชา / บรรดาข้อมูลไฟล์ซอฟต์แวร์หรือสิ่งอื่นใดที่ได้รับจากผู้ใช้งานอื่นต้องได้รับการตรวจสอบไวรัสคอมพิวเตอร์และโปรแกรมไม่ประสงค์ดีก่อนนำมาใช้งานหรือเก็บบันทึกทุกครั้ง

หมวดที่ ๒

นโยบายตามมาตรฐานสากล

ให้หน่วยงานในสังกัดกรมสนับสนุนบริการสุขภาพ ดำเนินธุรกรรมทางอิเล็กทรอนิกส์ เป็นไปในแนวทางของมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ ที่อ้างอิงตามมาตรฐาน ISO / IEC ๒๗๐๐๑ ที่มีใช้ในปัจจุบัน และ ที่จะได้พัฒนาเพิ่มเติมในภายหน้า โดยให้กลุ่มเทคโนโลยีสารสนเทศ สำนักบริหาร กรมสนับสนุนบริการสุขภาพ เป็นหน่วยงานหลักในการเสนอข้อพิจารณาดำเนินการเพื่อให้กรมสนับสนุนบริการสุขภาพให้ความเห็นชอบ

๑. ข้อกำหนดหลักที่ ๑ นโยบายความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy)

๑.๑. ทิศทางการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Management Directions for Information Security)

๑.๑.๑ นโยบายความมั่นคงปลอดภัยสารสนเทศ (Policy of Information Security)

๑.๑.๑.๑. มีการกำหนดขอบเขตการรักษาความมั่นคงปลอดภัยแบ่งเป็น ๓ ระดับ ตามโครงสร้างสายการบังคับบัญชา คือ

๑.๑.๑.๑.๑ ระดับบริหาร ประกอบด้วย ผู้มีอำนาจบริหารในระดับสูงของกรม

๑.๑.๑.๑.๒ ระดับผู้ดูแลระบบ ประกอบด้วย เจ้าหน้าที่ ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่ในการดูแลรักษาระบบและเครือข่ายคอมพิวเตอร์ ซึ่งสามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์

๑.๑.๑.๑.๓ ระดับเจ้าหน้าที่ ประกอบด้วย

- ข้าราชการ
- พนักงานราชการ
- ลูกจ้างประจำ
- พนักงานจ้างเหมาบริการ

๑.๑.๑.๒. ผู้บริหารให้ความสำคัญเกี่ยวกับการรักษาความมั่นคงปลอดภัย

๑.๑.๑.๒.๑ การอนุมัติให้จัดทำระบบรักษาความมั่นคงปลอดภัยภายในกรม และ สำนักสนับสนุนบริการสุขภาพของกรม

๑.๑.๑.๒.๒ การสนับสนุนเพื่อให้การดำเนินงานด้านการรักษาความปลอดภัยเป็นไปอย่างมีประสิทธิภาพ

๑.๑.๑.๒.๓ การติดตามผลทุกไตรมาส หรือตามความเหมาะสม

๑.๑.๑.๒.๔ เผยแพร่และสื่อสารให้เจ้าหน้าที่ในสังกัดถือปฏิบัติ

๑.๑.๑.๓. มีการกำหนดหลักการ วัตถุประสงค์ และเป้าหมายในการรักษาความปลอดภัยอย่างชัดเจน

๑.๑.๑.๓.๑ ให้นำ พ.ร.บ.คอมพิวเตอร์ฯ มาบรรจุไว้ในภาคผนวกของประกาศฉบับนี้

๑.๑.๑.๓.๒ **หลักการ**

เพื่อให้กรมมีการบังคับใช้นโยบายการรักษาความมั่นคงปลอดภัยได้อย่างมีประสิทธิภาพ ในการเข้าถึงคอมพิวเตอร์ ระบบเครือข่ายและสารสนเทศให้ปราศจากภัย

คุกคามของเทคโนโลยีสมัยใหม่ รวมถึงโปรแกรมไม่ประสงค์ดี อุปกรณ์พกพาและความเป็นส่วนตัว

วัตถุประสงค์

เพื่อกำหนดทิศทางการบริหารจัดการและการสนับสนุนด้านความมั่นคงปลอดภัยของคอมพิวเตอร์และระบบเครือข่าย โดยให้สอดคล้องกับความต้องการ

เป้าหมาย

เพื่อให้กรมมีความมั่นคงและปลอดภัยในการเข้าถึงและการจัดการคอมพิวเตอร์ระบบเครือข่ายและสารสนเทศ

๑.๑.๑.๔. มีการกำหนดความรับผิดชอบของผู้ที่เกี่ยวข้องในการบริหารจัดการความมั่นคงปลอดภัยให้สำนักบริหารโดยกลุ่มเทคโนโลยีสารสนเทศมีหน้าที่รับผิดชอบในการบริหารจัดการความมั่นคงและปลอดภัยในการเข้าถึงและการจัดการคอมพิวเตอร์ระบบเครือข่ายและสารสนเทศ

๑.๑.๒. การทบทวนนโยบายสำหรับการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Review of the policies for information security)

๑.๑.๒.๑. การให้คำนิยามคำว่า “การรักษาความมั่นคงและปลอดภัยในการเข้าถึงและการจัดการคอมพิวเตอร์ระบบเครือข่ายและสารสนเทศ”

- “การรักษาความมั่นคง” หมายถึง สภาพความพร้อมในการใช้งาน และ ใช้งานได้อย่างต่อเนื่อง
- “การรักษาความปลอดภัย” หมายถึง ความถูกต้องสมบูรณ์ของข้อมูล การรักษาความลับของข้อมูล การจำกัดสิทธิ์ในการเข้าถึง และการระบุตัวตนผู้ใช้อย่างแม่นยำ

๑.๑.๒.๒. มีการทบทวนตามรอบระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญต่อกรม เพื่อให้นโยบายมีความเหมาะสม เพียงพอ และได้ผล

๑.๑.๒.๓. มีการทบทวนนโยบายทุก ๑ ปี นับจากวันที่ประกาศ หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญต่อกรม เพื่อให้นโยบายมีประสิทธิภาพอยู่เสมอ

๒. ข้อกำหนดหลักที่ ๒ โครงสร้างความมั่นคงปลอดภัยสารสนเทศ (Organization of Information Security)

๒.๑. โครงสร้างความมั่นคงปลอดภัย (Internal Organization)

๒.๑.๑. บทบาทหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ (Information security roles and responsibilities)

๒.๑.๑.๑. อธิบดีกรมสนับสนุนบริการสุขภาพแต่งตั้ง “คณะกรรมการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ” ในการเข้าถึงและการจัดการคอมพิวเตอร์ ระบบเครือข่ายและสารสนเทศ

๒.๑.๑.๒. ระบุอำนาจและหน้าที่ในทุกมิติของคณะกรรมการด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศให้ชัดเจนและครอบคลุม

๒.๑.๑.๓. มีการทบทวน หรือแก้ไขและเพิ่มเติม หรือแต่งตั้งคณะกรรมการ ทุก ๑ ปี นับจากวันที่ประกาศครั้งก่อน หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญต่อกรม เพื่อให้นโยบายมีความ

ทันสมัย ใช้งานได้จริง เหมาะสมกับวัฒนธรรมกรมและสอดคล้องกับกฎหมาย รวมถึงมาตรฐานอื่นๆ ที่เกี่ยวข้อง

๒.๑.๒. การแบ่งแยกหน้าที่ความรับผิดชอบ (Segregation of duties)

๒.๑.๒.๑. มีการกำหนดอำนาจหน้าที่ของ CSO ระดับกรมสนับสนุนบริการสุขภาพ และ CSO ระดับสำนักสนับสนุนบริการสุขภาพเขต

๒.๑.๒.๒. มีการกำหนดอำนาจหน้าที่ของคณะกรรมการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ ระดับกรม และ ระดับสำนักสนับสนุนบริการสุขภาพ โดยมี CSO ระดับกรม และ CSO ระดับสำนักสนับสนุนบริการสุขภาพ เป็นผู้นำคณะ

๒.๑.๒.๓. CSO ระดับกรม และ CSO ระดับสำนักสนับสนุนบริการสุขภาพ มีอำนาจและหน้าที่ดังนี้

๒.๑.๒.๓.๑. กำหนดความรับผิดชอบของเจ้าหน้าที่ภายใน

๒.๑.๒.๓.๒. กำหนดขั้นตอนในการอนุมัติการใช้งานอุปกรณ์

๒.๑.๒.๓.๓. กำหนดสิทธิ์การเข้าใช้งานในระบบเครือข่ายคอมพิวเตอร์

๒.๑.๓. การติดต่อกับหน่วยงานผู้มีอำนาจ (Contact with authorities)

๒.๑.๓.๑. CSO ทุกระดับ ต้องจัดให้มีการแต่งตั้งเจ้าหน้าที่ผู้มีหน้าที่รับผิดชอบในการประสานงาน

๒.๑.๓.๒. ผู้อำนวยการสำนักบริหาร มีหน้าที่จัดทำรายชื่อและมอบอำนาจให้เจ้าหน้าที่เพื่อติดต่อกับหน่วยงานอื่นๆ

๒.๑.๔. การติดต่อกับกลุ่มที่มีความสนใจเป็นพิเศษในเรื่องเดียวกัน (Contact with special interest groups)

๒.๑.๔.๑. ผู้อำนวยการสำนักบริหาร ต้องจัดทำรายชื่อและข้อมูลสำหรับการติดต่อกับหน่วยงานภายนอกทั้งภาครัฐและภาคเอกชนที่เกี่ยวข้อง

๒.๑.๔.๒. CSO ระดับกรม มีอำนาจในการตัดสินใจในการอนุญาตให้มีการติดต่อกับกลุ่มที่มีความสนใจเป็นพิเศษในเรื่องเดียวกัน

๒.๑.๕. ความมั่นคงปลอดภัยสารสนเทศกับการบริหารจัดการโครงการ (Information security in project management)

๒.๑.๕.๑. CSO ระดับกรม ต้องกำหนดนโยบายให้มีการตรวจสอบการบริหารจัดการและการดำเนินงานที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศ

๒.๑.๕.๒. ให้คณะกรรมการดำเนินการตรวจสอบการบริหารจัดการ และการปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยในการเข้าถึงคอมพิวเตอร์ ระบบเครือข่ายและสารสนเทศ

๒.๒. อุปกรณ์คอมพิวเตอร์แบบพกพา Digital device รวมถึงการปฏิบัติงานจากระยะไกล (Mobile devices and teleworking)

๒.๒.๑. นโยบายสำหรับอุปกรณ์คอมพิวเตอร์แบบพกพา (Mobile and Digital Device Policy)

๒.๒.๑.๑. สำนักบริหารแต่งตั้งผู้มีหน้าที่รับผิดชอบการอนุญาตสิทธิในการใช้อุปกรณ์คอมพิวเตอร์แบบพกพา และ Digital Device

๒.๒.๑.๒. มีการกำหนดสิทธิการเข้าถึงของ IMEI (Internal Mobile Equipment Identity) หรือ MAC Address สำหรับอุปกรณ์เครือข่ายคอมพิวเตอร์แบบพกพาและ Digital Device ที่ได้รับอนุญาต

๒.๒.๑.๓. มีหน้าที่บันทึกข้อมูลที่เกี่ยวข้องกับอุปกรณ์คอมพิวเตอร์แบบพกพาและ Digital Device เพื่อเป็นการพิสูจน์เครื่องที่ใช้งานจริงในระบบ

๒.๒.๑.๔. มีการจำกัดช่องทางการเข้าออกของระบบ เมื่อมีการใช้งานระบบเครือข่ายไร้สาย (Wireless Security) และมีการเชื่อมต่อจากภายนอก (Tunnel Routing Policy) ตามนโยบายของระบบเครือข่ายและสารสนเทศ

๒.๒.๒. การปฏิบัติงานจากระยะไกล (Telewoking)

๒.๒.๒.๑. ให้ผู้ใช้ขอรหัสการใช้งานเป็นครั้งคราวจากผู้มีหน้าที่รับผิดชอบ

๒.๒.๒.๒. ผู้มีหน้าที่รับผิดชอบกำหนดระยะเวลาในการใช้งาน

๒.๒.๒.๓. ในกรณีที่มีความจำเป็นขั้นสูงสุด ผู้รับผิดชอบสามารถอนุญาตให้ใช้งานได้ตามความเหมาะสม

๒.๒.๒.๔. กำหนดนโยบายการเชื่อมต่อ Inbound และ Outbound ให้รัดกุม โดยเรียงจาก Source Address, Destination Address, Service, Scheduled และ Security Feature

๒.๒.๒.๕. เมื่อมีการเชื่อมต่อการปฏิบัติงานระยะไกล สามารถตรวจสอบผู้ใช้งานพร้อมระบุตัวตนของผู้ใช้งาน รวมทั้งตรวจสอบสถานะและรายการเชื่อมต่อระบบได้

๓. ข้อกำหนดหลักที่ ๓ ความมั่นคงปลอดภัยสำหรับทรัพยากรบุคคล (Human Resource Security)

๓.๑. ก่อนการจ้างงาน (Prior to employment)

๓.๑.๑. ข้อกำหนดการตรวจสอบและอ้างอิงบริษัท (Screening)

๓.๑.๑.๑. ทุนจดทะเบียนต้องไม่น้อยกว่าร้อยละ ๒๐ ของวงเงินจ้าง ให้เป็นไปตามระเบียบสำนักนายกฯ ว่าด้วยพัสดุ

๓.๑.๑.๒. ประวัติ/รายละเอียด/ประเภท ต้องเป็นบริษัทที่ดำเนินกิจการตรงกับประเภทของงานซื้อ/จ้าง

๓.๑.๑.๓. ไม่อยู่ในระหว่างการพิจารณาคดีให้เป็นผู้ทิ้งงาน หรือเป็นผู้ทิ้งงาน หรือเป็นผู้กระทำผิดทางละเมิด

๓.๑.๑.๔. ส่งหลักฐาน การทดสอบตนของบริษัท ที่ถูกต้องตามกฎหมาย เกี่ยวกับเอกสารที่คัดสำเนาจากส่วนราชการ ไม่ปลอมแปลงเอกสาร

๓.๑.๑.๕. ประวัติการทำงาน หรือ ผลงานทางบริษัท ในสายงานที่ตรงกับการว่าจ้างตามที่กำหนด

๓.๑.๑.๖. ให้แสดงผลงานที่เคยเป็นที่ประจักษ์ของบริษัท หรือหากไม่มีให้แสดงผลงานของบุคคลกรที่เป็นผู้รับผิดชอบของงานจ้าง โดยบุคลากรนั้นต้องทำงานจนเสร็จสิ้นงานจ้าง

๓.๑.๑.๗. หลักประกันความเสียหายตามระเบียบสำนักนายกฯ ว่าด้วยพัสดุ

๓.๑.๑.๘. ต้องไม่เป็นบริษัทขายช่วง หรือซื้อช่วง การจ้าง/ซื้อ

๓.๑.๒. ข้อกำหนดการตรวจสอบของบุคลากรหรือทีมงานที่จะเข้ามาปฏิบัติงานในกรม (Term and Conditions of employment)

๓.๑.๒.๑. ระดับวุฒิการศึกษาอย่างน้อย ปริญญาตรี ในสาขาที่ตรงกับงานที่จ้างและประวัติการศึกษา

๓.๑.๒.๒. ใบรับรองหรือประกาศนียบัตร ของทีมงาน/บุคคล

๓.๑.๒.๓. ประวัติการทำงาน และประสบการณ์การทำงาน

๓.๑.๒.๔. ข้อมูลหลักฐานแสดงตัวตนของทีมงาน/บุคคล เช่นบัตรประชาชนหรือเอกสารระบุตัวบุคคล

๓.๑.๒.๕. ต้องมีผลงานเป็นที่ประจักษ์ ตรงกับประเภทงานจ้าง

๓.๒. ระหว่างการจ้างงาน (During employment)

ควรประกอบไปด้วย

- หน้าที่ความรับผิดชอบของผู้บริหาร (Management responsibilities)
- การสร้างความตระหนัก การให้ความรู้ และการฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศ (Information security awareness, education and training)
- กระบวนการทางวินัย (Disciplinary process)

๓.๒.๑. ขอบเขตการจ้างงานด้านการพัฒนาระบบสารสนเทศ

๓.๒.๑.๑. ข้อกำหนดในการพัฒนาระบบสารสนเทศ

๓.๒.๑.๑.๑. มีแผนงานในการดำเนินงานและนำเสนอต่อคณะกรรมการ

๓.๒.๑.๑.๒. มีการแต่งตั้งคณะกรรมการเปิดซอง/ตรวจรับ/คณะกรรมการTOR

๓.๒.๑.๑.๓. มีรายงานผลการศึกษาระบบเดิมและความต้องการผู้ใช้งาน

๓.๒.๑.๑.๔. มีการนำเสนอผลการวิเคราะห์ระบบและการออกแบบ

๓.๒.๑.๑.๕. ในการพัฒนาระบบ ต้องจัดทำให้สามารถเชื่อมโยงข้อมูลได้อย่างสมบูรณ์

๓.๒.๑.๑.๖. ระหว่างการพัฒนาระบบ ต้องมานำเสนอความก้าวหน้าเป็นระยะตามที่กรมกำหนด

๓.๒.๑.๑.๗. เมื่อพัฒนาระบบเสร็จสิ้น ต้องมีระบบการทดสอบหรือทดลองใช้งานจากผู้ใช้

๓.๒.๑.๑.๘. เมื่อขั้นตอนทดสอบระบบเสร็จสิ้นก่อนจะติดตั้งระบบขึ้นใช้งานจริงต้องมีการวิเคราะห์การทำงานของระบบ

๓.๒.๑.๑.๙. หลังการติดตั้งระบบที่พัฒนาขึ้นใช้งานจริง ต้องมีการรายงานประเมินผลการใช้งาน

๓.๒.๑.๑.๑๐. กรณีสิ้นสุดการจ้างต้องเปลี่ยนสิทธิการเข้าถึงระบบหรือคืนทรัพย์สินตามที่กรมกำหนด

๓.๒.๑.๒. ขอบเขตของการจ้างงานด้านระบบเครือข่ายและอุปกรณ์

๓.๒.๑.๒.๑. มีการแต่งตั้งคณะกรรมการเปิดซอง/ตรวจรับ/คณะกรรมการTOR

๓.๒.๑.๒.๒. มีรายงานการศึกษาวิเคราะห์และออกแบบพร้อมนำเสนอแผนงานไดอะแกรมการออกแบบระบบเครือข่ายต่อคณะกรรมการตรวจรับ

๓.๒.๑.๒.๓. นำเสนอผลการวิเคราะห์และแผนสำรอง กรณีที่อาจมีผลกระทบกับระบบเครือข่ายปัจจุบันที่ดำเนินงานต่อเนื่องเพื่อไม่ให้การดำเนินงานของกรมหยุดชะงัก

๓.๒.๑.๒.๔. หากระหว่างการดำเนินการติดตั้งหรือปรับปรุงระบบส่งผลกระทบความเสียหายต่อกรม บริษัทหรือผู้รับจ้างต้องรับผิดชอบเป็นเงินประกันตามความเสียหายทั้งหมด หรือตามข้อตกลงทางคณะกรรมการตรวจรับ

๓.๒.๑.๒.๕. ข้อมูลหรือทรัพย์สินด้านการพัฒนาหรือปรับปรุงระบบเครือข่าย ที่ถูกกำหนดเป็นความลับ ห้ามนำออกนอกกรมหรือห้ามสำรองข้อมูลเอกสารอื่นใด

๓.๓. การสิ้นสุดหรือการเปลี่ยนการจ้างงาน (Termination and change of employment)

๓.๓.๑. การสิ้นสุดหรือการเปลี่ยนแปลงหน้าที่ความรับผิดชอบของการจ้างงาน (Termination or change of employment responsibilities)

๓.๓.๑.๑. แนวทางปฏิบัติตามนโยบายความมั่นคงปลอดภัย

๓.๓.๑.๑.๑. ปฏิบัติงานตามขอบเขตและนโยบายความมั่นคงปลอดภัยที่กรมจ้าง/กำหนดไว้

๓.๓.๑.๑.๒. การเข้า-ออก กรมต้องมีระบบการลงทะเบียนการเข้า – ออกและกรณีต้องเข้าไปปฏิบัติงานใน Zone ต้องได้รับอนุญาตและอยู่ในความควบคุมของเจ้าหน้าที่ของกรม

๓.๓.๑.๑.๓. การปฏิบัติงานที่เกี่ยวข้อง หรือ ต้องมีการเปลี่ยนแปลงอันเกี่ยวกับทรัพย์สินของกรมต้องอยู่ในการดูแลควบคุมกำกับทางเจ้าหน้าที่กรมที่รับผิดชอบ

๓.๓.๑.๑.๔. ทรัพย์สินกรมที่สำคัญหรือเป็นความลับของกรม ห้ามนำออกนอกกรมโดยเด็ดขาด หรือสำรองข้อมูลไว้ที่อื่นนอกกรม

๓.๓.๑.๑.๕. ห้ามใช้งานโปรแกรมที่ไม่พึงประสงค์ ที่อาจก่อให้เกิดความเสียหายต่อกรม

๓.๓.๑.๒. แนวนโยบายความตระหนักรู้ด้านความมั่นคงปลอดภัยแก่บุคลากรของกรม

๓.๓.๑.๒.๑. ประกาศแจ้งนโยบายความมั่นคงปลอดภัย

๓.๓.๑.๒.๒. รวบรวมปัญหาเกี่ยวกับการใช้เครื่องมืออุปกรณ์และระบบที่เป็นช่องโหว่ส่งผลกระทบต่อระบบความมั่นคงปลอดภัยของกรม

๓.๓.๑.๒.๓. ประชาสัมพันธ์ให้เกิดความตระหนักรู้เกี่ยวกับความมั่นคงปลอดภัยต่อกรม

๓.๓.๑.๒.๔. จัดอบรมให้ความรู้การใช้งานระบบเทคโนโลยีสารสนเทศที่ถูกต้องและให้เกิดความตระหนักต่อระบบความมั่นคงปลอดภัย

๓.๓.๑.๒.๕. จัดทำมาตรการและบทลงโทษกรณีผู้ทำผิดนโยบายความมั่นคงปลอดภัยของกรม โดยควรได้รับการรับรองสนับสนุนจากผู้บริหารกรม

๓.๓.๑.๒.๖. ประเมินผลการถือปฏิบัติตามนโยบายความมั่นคงปลอดภัยที่ประกาศใช้

๓.๓.๑.๓. ข้อกำหนดสำหรับบุคลากรทั่วไปภายในกรม

๓.๓.๑.๓.๑. ห้ามนำโปรแกรม (Software) ที่ไม่เกี่ยวข้องกับการใช้งานตามมาตรฐานที่กรมกำหนดมาใช้ในกรม

๓.๓.๑.๓.๒. หากมีความประสงค์หรือความจำเป็นต้องใช้งานโปรแกรม (Software) ที่ไม่อยู่ในรายการมาตรฐานที่กรมกำหนด ให้ขออนุญาตเป็นลายลักษณ์อักษรและขอขึ้นทะเบียนจากผู้มีหน้าที่รับผิดชอบรับทราบก่อนทุกครั้ง ป้องกันการละเมิดลิขสิทธ์และความเสียหายของกรมอันเกิดจากการละเมิดลิขสิทธิ์การใช้ซอร์ฟแวร์อย่างไม่ถูกต้อง

๓.๓.๑.๓.๓. จัดทำคู่มือการใช้งานและการบำรุงรักษาเบื้องต้นให้กับบุคลากรทั่วไปกรมทราบในการปฏิบัติงานที่เกี่ยวข้องกับการใช้ระบบคอมพิวเตอร์

๓.๓.๑.๓.๔. การนำอุปกรณ์สำรองข้อมูลทุกประเภท เข้ามาใช้กับเครื่องคอมพิวเตอร์หรืออุปกรณ์ของกรม ต้องมีการตรวจสอบความปลอดภัยของตัวอุปกรณ์ก่อนใช้งานทุกครั้ง

๓.๓.๑.๓.๕. เครื่องคอมพิวเตอร์ทุกเครื่องที่ใช้ในกรมควรมีการเข้ารหัส ทั้งในส่วนระบบที่เป็น Workgroup และ Active Directory การเชื่อมต่อระบบของกรม

๓.๓.๑.๓.๖. หากเครื่องคอมพิวเตอร์มีปัญหาที่ไม่สามารถแก้ไขได้เองต้องแจ้งแผนกที่เกี่ยวข้องกับการบำรุงรักษาและปรับปรุงระบบคอมพิวเตอร์เท่านั้น

๓.๓.๑.๓.๗. บุคลากรต้องรับผิดชอบดูแลเครื่องคอมพิวเตอร์ที่ใช้งานของตนเองหากเกิดความเสียหายหรือสูญหายต้องรับผิดชอบตามมติ

๓.๓.๑.๓.๘. บุคลากรผู้ใช้งานไม่ควรเข้าเว็บไซต์ที่ก่อให้เกิดอันตรายหรือไม่เกี่ยวข้องกับการปฏิบัติงานหรือดาวน์โหลดข้อมูลอันก่อให้เกิดความเสียหายต่อระบบของกรม

๓.๓.๑.๔. ผู้ดูแลระบบการรักษาความมั่นคงปลอดภัยหรือเครือข่าย

๓.๓.๑.๔.๑. กรมต้องกำหนดโครงสร้างบทบาทหน้าที่ความรับผิดชอบของบุคลากรผู้ปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัย

๓.๓.๑.๔.๒. ต้องมีการกำหนดยุทธศาสตร์ด้านการดำเนินงานและปฏิบัติงานระบบคอมพิวเตอร์ ให้สอดคล้องกับความมั่นคงปลอดภัยของกรม

๓.๓.๑.๔.๓. ต้องมีการวางแผนการดำเนินงานด้านความมั่นคงปลอดภัยอย่างเป็นระบบโดยการตรวจสอบและควบคุมจากคณะกรรมการรักษาความมั่นคงปลอดภัย

๓.๓.๑.๔.๔. ต้องมีระบบการมอบหมายงานตามขอบเขตอำนาจหน้าที่ที่เหมาะสมต่อผู้ปฏิบัติงานด้านความมั่นคงปลอดภัย

๓.๓.๑.๔.๕. ต้องมีระบบการประเมินผลการดำเนินงานด้านความมั่นคงปลอดภัยและมีระบบแก้ไขปัญหาด้านความมั่นคงปลอดภัย

๔. ข้อกำหนดหลักที่ ๔ การบริหารจัดการทรัพยสิน (Asset Management)

๔.๑. หน้าที่ความรับผิดชอบต่อทรัพย์สิน (Responsibility for Assets)

๔.๑.๑. บัญชีทรัพย์สิน (Inventory of assets)

๔.๑.๑.๑. ให้หน่วยงานจัดทำทะเบียนบัญชีทรัพย์สิน (อุปกรณ์คอมพิวเตอร์-เครือข่ายและ software)

ประกอบด้วย ชื่ออุปกรณ์ หมายเลข ปีที่ได้รับ สถานที่ใช้งาน ผู้รับผิดชอบ

๔.๑.๑.๒. ให้หน่วยงานขึ้นทะเบียนทรัพย์สินที่ได้รับจัดสรรใหม่ทุกครั้ง

๔.๑.๑.๓. มีการตรวจสอบ ปรับปรุง ทบทวน ทะเบียนบัญชีทรัพย์สินอย่างน้อยปีละ ๑ ครั้ง

๔.๑.๒. ผู้ถือครองทรัพย์สิน (ownership of assets)

๔.๑.๒.๑. หน่วยงานต้องระบุรายชื่อผู้ใช้อุปกรณ์คอมพิวเตอร์-เครือข่ายและ software

๔.๑.๒.๒. มีการปรับปรุงรายชื่อผู้ใช้อุปกรณ์คอมพิวเตอร์เครือข่ายและ software ทุกครั้งเมื่อมีการ

เปลี่ยนแปลง / ทำหนังสือขอใช้ ระบุระยะเวลาในการใช้

๔.๑.๓. การใช้ทรัพย์สินอย่างเหมาะสม (Acceptable use of assets)

๔.๑.๓.๑. มีการจัดทำกฎ ระเบียบ หลักเกณฑ์การจัดสรรอุปกรณ์คอมพิวเตอร์ให้เหมาะสมกับภารกิจ
และบุคลากรและ มีการทบทวนปีละ ๑ ครั้ง

๔.๑.๓.๒. มีการจัดทำคู่มือการใช้งานอุปกรณ์คอมพิวเตอร์-เครือข่ายและ software รวมทั้งกำหนด
ขั้นตอนการดูแลรักษาเป็นรายอุปกรณ์

๔.๑.๓.๓. มีการจัดให้มีการตรวจสอบ บำรุงรักษา อุปกรณ์คอมพิวเตอร์ เครือข่ายและ software ให้มี
ความพร้อมใช้งานอย่างน้อยปีละ ๑ ครั้ง

๔.๑.๓.๔. มีการประกาศใช้ กฎ ระเบียบ หลักเกณฑ์ และคู่มือการใช้งานอุปกรณ์คอมพิวเตอร์ เครือข่าย และ software ให้ผู้ใช้

๔.๑.๔. การคืนทรัพย์สิน (Return of assets)

๔.๑.๔.๑. มีการกำหนดนโยบายให้ผู้ใช้ต้องคืนทรัพย์สินของกรมทั้งหมดที่กรมถือครอง เมื่อสิ้นสุด
การจ้างงาน หมดสัญญา สิ้นสุดข้อตกลงการจ้าง หรือทุกครั้งที่มีการเปลี่ยนแปลงกรม

๔.๒. การจัดชั้นความลับของสารสนเทศ (Information classification)

๔.๒.๑. ชั้นความลับของสารสนเทศ (Classification of information)

๔.๒.๑.๑. มีการการจัดหมวดหมู่ทรัพย์สินสารสนเทศ (Classification guidelines) แบ่งเป็น

- ฮาร์ดแวร์
- ซอฟแวร์
- ข้อมูลสารสนเทศ
- ผู้ใช้

๔.๒.๑.๒. หน่วยงานกำหนดชั้นความลับสารสนเทศ ได้แก่

- ปกติ ไม่กำหนดชั้นความลับ
- ลับ
- ลับมาก
- ลับที่สุด

๔.๒.๑.๓. มีการกำหนดระบบการเข้าถึงสารสนเทศตามระดับชั้นความลับสารสนเทศ

- ไม่ลับ คือ สามารถเผยแพร่ได้
- ลับ คือ ผู้ที่เกี่ยวข้องกับงาน
- ลับมาก คือ หัวหน้าฝ่าย/กลุ่ม
- ลับที่สุด คือ ผู้บริหารระดับสูง

๔.๒.๑.๔. มีการกำหนดมาตรการป้องกันอุปกรณ์สารสนเทศที่ใช้งานนอกกิจการ เช่น กำหนดให้มีการใส่รหัสผ่านก่อนการใช้อุปกรณ์ อุปกรณ์เหล่านั้นต้องลงทะเบียนก่อนเข้าสู่ระบบ

๔.๒.๒. การบ่งชี้สารสนเทศ (Labeling of information)

๔.๒.๒.๑. มีการกำหนดระเบียบหลักเกณฑ์และบทลงโทษในการใช้ระบบสารสนเทศตาม พรบ. ความมั่นคงปลอดภัย

๔.๒.๓. การจัดทรัพย์สิน (handling of assets)

๔.๒.๓.๑. มีการจัดทำป้ายชื่อตามทะเบียนบัญชีทรัพย์สิน และขั้นตอนการใช้งานติดที่อุปกรณ์คอมพิวเตอร์ทุกชิ้น

๔.๒.๓.๒. กิจการต้องมีมาตรการ ในการทำลายอุปกรณ์หรือสื่อบันทึกข้อมูลที่จัดเก็บข้อมูลสำคัญ เพื่อป้องกันการรั่วไหลของข้อมูล

๔.๒.๓.๓. มีการการควบคุมการเปลี่ยนแปลงหรือแก้ไขระบบสารสนเทศควรมีการทดสอบการใช้งานระบบใหม่ให้ถูกต้องเหมาะสมและมีการบันทึกการเปลี่ยนแปลงแก้ไขทุกครั้ง

๔.๓. การจัดสื่อบันทึกข้อมูล (Media Handing)

๔.๓.๑. การบริหารจัดสื่อบันทึกข้อมูลที่ถอดแยกได้ (Management of removable media)

๔.๓.๑.๑. กำหนดการจัดการเกี่ยวกับสื่อบันทึกข้อมูลที่ถอดแยกได้ ให้มีความสอดคล้องกับขั้นตอนการจัดชั้นความลับของสารสนเทศที่กรมกำหนดไว้

๔.๓.๒. การทำลายสื่อบันทึกข้อมูล (Disposal of media)

๔.๓.๒.๑. มีการกำจัดหรือทำลายทิ้งอย่างมั่นคงปลอดภัย เมื่อหมดความต้องการในการใช้งาน โดยปฏิบัติตามขั้นตอนปฏิบัติสำหรับการทำลายซึ่งกำหนดไว้อย่างเป็นทางการ

วิธีการทำลาย

กระดาษ	ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร
แผ่น CD/DVD	ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร
เทป	ใช้วิธีการทุบหรือบดให้เสียหาย หรือเผาทำลาย
ฮาร์ดดิสก์/Flash Drive	ใช้การทำลายข้อมูลบนฮาร์ดดิสก์ด้วยวิธีการฟอร์แม็ต (Low Level Format)

๔.๓.๓. การขนย้ายสื่อบันทึกข้อมูล (physical media transfer)

๔.๓.๓.๑. มีการป้องกันข้อมูลจากการถูกเข้าถึงโดยไม่ได้รับอนุญาต การนำไปใช้งานอย่างผิดวัตถุประสงค์ หรือความเสียหายในระหว่างที่นำส่งหรือขนย้ายสื่อบันทึกข้อมูลนั้น

๕. ข้อกำหนดหลักที่ ๕ การควบคุมการเข้าถึง (Access Control)

๕.๑. ความต้องการทางธุรกิจสำหรับการควบคุมการเข้าถึง (Business requirements of access control)

๕.๑.๑. นโยบายควบคุมการเข้าถึง (Access Control Policy)

๕.๑.๑.๑. มีการกำหนดผู้รับผิดชอบภายในกรมและร่วมกันพิจารณาออกนโยบายในการเข้าถึงระบบ และมีการประกาศใช้อย่างเป็นทางการ เช่น กำหนดสิทธิในการเข้าใช้งานในอุปกรณ์คอมพิวเตอร์, กำหนดสิทธิในการเข้าใช้งานระบบ

๕.๑.๒. การเข้าถึงเครือข่ายและบริการเครือข่าย (Access to networks and network services)

๕.๑.๒.๑. มีการลงทะเบียนสำหรับผู้ใช้งานใหม่โดยการยืนยันตัวตน

๕.๑.๒.๒. มีการกำหนดให้มีการพิจารณาสิทธิในการเข้าถึงข้อมูลของผู้ใช้โดยกำหนดระบบการเข้าถึงสารสนเทศตามระดับชั้นความลับสารสนเทศ,มีการทบทวนสิทธิ์การเข้าถึงข้อมูลของเจ้าหน้าที่เดิม

๕.๒. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User access management)

๕.๒.๑. การลงทะเบียนและการถอดถอนสิทธิผู้ใช้งาน (User registration and de-registration)

๕.๒.๑.๑. มีการลงทะเบียนสำหรับผู้ใช้และมีการปรับปรุงระบบข้อมูลผู้ใช้

๕.๒.๒. การจัดการสิทธิการเข้าถึงของผู้ใช้งาน (User access provisioning)

๕.๒.๒.๑. มีการกำหนดให้มีการพิจารณาสิทธิในการเข้าถึงข้อมูลของผู้ใช้โดยกำหนดระบบการเข้าถึงสารสนเทศตามระดับชั้นความลับสารสนเทศ,มีการทบทวนสิทธิ์การเข้าถึงข้อมูลของเจ้าหน้าที่เดิม

๕.๒.๓. การบริหารจัดการสิทธิการเข้าถึงตามระดับสิทธิ (Management of privileged access right)

๕.๒.๓.๑. มีการกำหนดระบบการเข้าถึงสารสนเทศตามระดับชั้นความลับสารสนเทศ

๕.๒.๓.๒. มีการกำหนดระดับสิทธิของการเข้าใช้งานด้านระบบคอมพิวเตอร์, ระบบเครือข่ายให้เหมาะสมกับผู้ใช้งานและผู้ดูแลระบบ

๕.๒.๔. การบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้งาน (Management of secret authentication information of users)

๕.๒.๔.๑. มีการมอบข้อมูลการพิสูจน์ตัวตนของผู้ใช้งานซึ่งเป็นข้อมูลลับ โดยมีการควบคุมผ่านกระบวนการบริหารจัดการที่เป็นทางการ

๕.๒.๕. การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of user access right)

๕.๒.๕.๑. มีการกำหนดให้เจ้าของทรัพย์สินต้องทบทวนสิทธิการเข้าถึงของผู้ใช้งานอย่างน้อยปีละ ๑ ครั้ง

๕.๒.๖. การถอดถอนหรือปรับปรุงสิทธิการเข้าถึง (Removal of adjustment of access rights)

๕.๒.๖.๑. มีการถอดถอนสิทธิการเข้าถึงของผู้ใช้เมื่อสิ้นสุดการจ้าง หรือมีการเปลี่ยนแปลงโอนย้าย

๕.๓. หน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities)

๕.๓.๑. การใช้ข้อมูลการพิสูจน์ตัวตนซึ่งเป็นข้อมูลลับ (Use of secret authentication information)

๕.๓.๑.๑. สร้างจิตสำนึกให้เกิดความตระหนักในระดับความลับของข้อมูล

๕.๓.๑.๒. มีการกำหนดให้เจ้าหน้าที่ ที่มีอุปกรณ์คอมพิวเตอร์กำหนดรหัสผ่านในการเข้าใช้งานอุปกรณ์นั้นๆ

๕.๔. การควบคุมการเข้าถึงระบบ (System and application access control)

๕.๔.๑. การจำกัดการเข้าถึงสารสนเทศ (Information access restriction)

๕.๔.๑.๑. มีการออกมาตรการการเข้าถึงระบบเครือข่ายโดยใช้ไอพีแอดเดรส

๕.๔.๑.๒. มีการสร้างระบบจัดเก็บ log ไฟล์ในการเข้าถึงเครือข่ายของกรม

๕.๔.๑.๓. มีการพิจารณาการเปิดเข้าใช้งาน port ของผู้ร้องขอใช้งานโดยกำหนดระยะเวลาในการใช้งานตามที่ผู้ดูแลระบบจะอนุญาต

๕.๔.๑.๔. มีการกำหนด vlan ในการเข้าใช้งานระบบเครือข่ายของกรมนั้นๆ

๕.๔.๑.๕. ถ้าไม่มีการใช้งานในระยะเวลาหนึ่ง ระบบจะดำเนินการตัดสัญญาณอินเตอร์เน็ต (session timeout) เพื่อนำสัญญาณไปให้ผู้ที่ร้องขอคนอื่นต่อไป

๕.๔.๑.๖. มีการจัดทำคู่มือขั้นตอนการใช้งาน

๕.๔.๑.๗. มีการกำหนดรหัสผ่านโดยผู้ดูแลระบบและจัดเก็บไว้ที่ผู้ดูแลระบบในรูปแบบแฟ้มเอกสารที่มีการปิดผนึกที่มิดชิด

๕.๔.๑.๘. มีการแยกประเภทของผู้ใช้งานและกำหนดการเข้าถึงข้อมูลในระดับชั้นต่าง เช่น ผู้บริหาร,ผู้ปฏิบัติงาน ฯลฯ

๕.๔.๑.๙. มีการกำหนดให้ผู้เข้ามาใช้งานขอรหัสผ่านเพื่อเข้าใช้งานระบบจากผู้ดูแลระบบ ซึ่งรหัสผ่านสามารถใช้ได้ในช่วงเวลาที่กำหนดไว้เท่านั้น

๕.๔.๒. ขั้นตอนการปฏิบัติสำหรับการล็อกอินเข้าระบบที่มีความมั่นคงปลอดภัย (Secure log-on procedures)

๕.๔.๒.๑. มีการกำหนดนโยบายควบคุมการเข้าถึง การเข้าถึงระบบต้องมีการควบคุมโดยผ่านทางขั้นตอนฏิบัติสำหรับการล็อกอินเข้าระบบที่มีความมั่นคงปลอดภัย

๕.๔.๓. ระบบบริหารจัดการรหัสผ่าน (Password management system)

๕.๔.๓.๑. มีระบบบริหารจัดการรหัสผ่านต้องมีปฏิสัมพันธ์กับผู้ใช้งานและบังคับการตั้งรหัสผ่านที่มีคุณภาพ เช่น รหัสผ่านมีความซับซ้อน คาดเดาได้ยาก เข้ารหัสในการจัดเก็บ

๕.๔.๔. การใช้โปรแกรมอรรถประโยชน์ (Use of privileged utility programs)

๕.๔.๔.๑. มีการควบการใช้โปรแกรม**อรรถประโยชน์**ในหน่วยงาน ผู้ใช้งานห้ามลง**โปรแกรมอรรถประโยชน์**ที่ไม่มีลิขสิทธิ์ถูกต้อง

๕.๔.๕. การควบคุมการเข้าถึงซอร์สโค้ดของโปรแกรม (Access Control to program source code)

๕.๔.๕.๑. มีการกำหนดระดับความปลอดภัยของเข้าใช้ซอร์สโค๊ดของโปรแกรมเป็นลำดับขั้นความปลอดภัยเพื่อป้องกันเกี่ยวกับข้อมลสูญหายหรือ มีซอร์สโค๊ดที่ไม่ได้รับการอัพเดตรายการแก้ไขเข้าไปอย่างถูกต้อง

๖. ข้อกำหนดหลักที่ ๖ การเข้ารหัสข้อมูล (Cryptography)

๖.๑. มาตรการเข้ารหัสข้อมูล (Cryptographic controls)

๖.๑.๑. นโยบายการใช้มาตรการเข้ารหัสข้อมูล (Policy on the use of cryptographic controls)

๖.๑.๑.๑. มีนโยบายการใช้มาตราการเข้ารหัสข้อมูลเพื่อป้องกันสารสนเทศ ต้องมีการจัดทำและปฏิบัติตามนโยบาย

๖.๑.๒. การบริหารจัดการกุญแจ (Key Management)

๖.๑.๒.๑. มีนโยบายการใช้งาน การป้องกัน และอายุการใช้งานของกุญแจ ต้องมีการจัดทำและปฏิบัติตามตลอดวงจรชีวิตของกุญแจ (Key Management)

๗. ข้อกำหนดหลักที่ ๗ ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and environmental security)

๗.๑.พื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัย (Secure areas)

๗.๑.๑.ขอบเขตหรือบริเวณโดยรอบทางกายภาพ (Physical security perimeter) กำหนดพื้นที่โดยตามการประเมินความเสี่ยงของกรม เพื่อจัดลำดับความเสี่ยงในการเข้าออกทางกายภาพ

๗.๑.๑.๒ความเสี่ยงสูง เช่น ห้อง Datacenter, ระบบฐานข้อมูล

๗.๑.๑.๓ความเสี่ยงปานกลาง ระบบเครือข่าย เช่น Wall Mount Rack และตู้ network ห้อง Datacenter

๗.๑.๑.๔ความเสี่ยงต่ำ ห้องปฏิบัติงาน, เครื่อง Client ณ จุดปฏิบัติงาน

๗.๑.๒.การควบคุมการเข้าออกทางกายภาพ (Physical entry controls)

พื้นที่ที่ต้องการรักษาความปลอดภัยต้องมีการป้องกันโดยมีการควบคุมการเข้าออกอย่างเหมาะสมตามการประเมินความเสี่ยงของกรม เพื่อจัดลำดับความเสี่ยงในการเข้าออกทางกายภาพดังนี้

๗.๑.๒.๑.ระดับความเสี่ยงสูง

- กั้นห้องให้เป็นสัดส่วนมั่นคงแข็งแรง
- มีระบบการรักษาความปลอดภัยในการเข้าออก สแกนนิ้วมือ หรือสแกนม่านตา
- กล้องวงจรปิดครอบคลุมพื้นที่ ๑๐๐ %
- กำหนดผู้รับผิดชอบและผู้ดูแลอุปกรณ์ทุกอย่าง
- มีระเบียบ มาตรการในการปฏิบัติการเข้าออกทางกายภาพ โดยเฉพาะการดำเนินการด้วยบุคคลภายนอกต้องมีเจ้าหน้าที่ติดตามตลอดเวลา
- มีเจ้าหน้าที่รักษาความปลอดภัย

๗.๑.๒.๒.ระดับความเสี่ยงปานกลาง

- กั้นห้องให้เป็นสัดส่วน
- กล้องวงจรปิดเฉพาะบางส่วนที่สำคัญ
- กำหนดผู้รับผิดชอบ
- เจ้าหน้าที่รักษาความปลอดภัย
- คีย์การ์ด
- ตำแหน่งการติดตั้งที่เหมาะสมของระบบ Network

๗.๑.๒.๓.ระดับความเสี่ยงต่ำ

- เจ้าหน้าที่รักษาความปลอดภัย (รปภ.)
- กำหนดผู้รับผิดชอบ
- กล้องวงจรปิด พื้นที่โดยรวม
- ตำแหน่งที่เหมาะสมสำหรับการใช้งานเครื่องคอมพิวเตอร์ลูกข่าย

๗.๑.๓. การรักษาความมั่นคงปลอดภัยสำหรับสำนักงาน ห้องทำงานและอุกกรณ์ (securing office,roomand facilities

- มีเจ้าหน้าที่รักษาความปลอดภัย (รปภ.)ควบคุมการเข้าออกบริเวณ
- อุปกรณ์ต่างๆที่เกี่ยวข้องกับงานระบบ ต้องติดตั้งในตู้เพื่อป้องกัน การทำลาย การปิดระบบ
- มีการกำหนดพื้นที่ในการปฏิบัติงานตามตำแหน่งหน้าที่ของผู้ดูแลระบบ

๗.๑.๔. การป้องกันภัยคุกคามจากภายนอกและสภาพแวดล้อม (protecting against external and environment threats)

- มีระบบเตือนภัยฉุกเฉิน กรณีไฟไหม น้ำท่วม
- มีอุปกรณ์ดับเพลิงตามมาตรฐาน
- มีระบบปรับอากาศและความคุมความชื้น
- แผน คู่มือ การซักซ้อม และการสรุปผล การป้องกันต่อภัยคุกคามจากภายนอกและสภาพแวดล้อม
- กรมมีแผนการใช้งานด้าน Disaster Recovery Site หรือระบบคอมพิวเตอร์สำรองเมื่อมีเหตุการณ์ด้านภัยพิบัติของสภาพแวดล้อมขึ้น

๗.๑.๕. การปฏิบัติงานในพื้นที่ที่ต้องการรักษาความมั่นคงปลอดภัย (Working is secure areas) ขั้นตอนปฏิบัติสำหรับการปฏิบัติการในพื้นที่

-ต้องรายงานการปฏิบัติงานและการตรวจสอบการปฏิบัติงาน เพื่อให้มั่นใจได้ว่ากากปฏิบัติงานถูกต้อง ครบถ้วน เป็นไปตามนโยบายและขั้นตอนการปฏิบัติงาน และอยู่ในกรอบอำนาจหน้าที่และความรับผิดชอบตามที่กำหนดไว้ นอกจากนี้ ในกรณีที่ได้ใช้บริการงานสนับสนุนด้านเทคโนโลยีสารสนเทศจากบุคคลภายนอกสำนักงาน ต้องมีระบบการตรวจสอบการปฏิบัติงานของบุคคลภายนอกอย่างรอบคอบและรัดกุมเพียงพอ เช่น มีการตรวจสอบบันทึกการทำงาน (log files) ของบุคคลภายนอก และกำหนดให้บุคคลภายนอกรายงานการปฏิบัติงาน เป็นต้น

๗.๑.๖. พื้นที่สำหรับรับส่งสิ่งของ (Delivery and loading areas)

- จุดหรือบริเวณที่สามารถเข้าถึงกรม เช่น พื้นที่สำหรับรับสิ่งของบริเวณอื่น ๆ ที่ไม่ได้รับอนุญาตสามารถเข้าถึงพื้นที่ของกรมได้ต้องมีการควบคุม และหากเป็นไปได้ จุดหรือบริเวณดังกล่าวควรแยกออกมาจากบริเวณที่มีอุปกรณ์ประมวลผลสารสนเทศ เพื่อหลีกเลี่ยงการเข้าถึงโดยไม่ได้รับอนุญาต

๗.๒. อุปกรณ์ (Equipment)

เพื่อป้องกันการสูญหาย การเสียหาย การขโมย หรือการเป็นอันตรายต่อสินทรัพย์และป้องกันการหยุดชะงักต่อการดำเนินงานของกรม

๗.๒.๑.การจัดตั้งและป้องกันอุปกรณ์ (Equipment sitting and protection)

๗.๒.๑.๑. จัดสรรพื้นที่ในการติดตั้งอุปกรณ์ที่มีความสำคัญให้เข้าถึงยาก

๗.๒.๑.๒. การติดตั้งอุปกรณ์ต้องติดตั้งในตู้เก็บอุปรกรณ์ให้มิดชิด

๗.๒.๒.ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting Utilities)อุปกรณ์ต้องได้รับการป้องกันจากการล้นเหลวของกระแสไฟฟ้าและการหยุดชะงักอื่น ๆ ที่มีสาเหตุมาจากการล้มเหลวของระบบและอุปกรณ์สนับสนุนการทำงานต่าง ๆ

๗.๒.๒.๑ ความเสี่ยงสูง ต้องมีระบบสำรองไฟฟ้าทั้ง UPS และ เครื่องกำเนิดไฟฟ้า

๗.๒.๒.๒ ความเสี่ยงปานกลาง ต้องมีระบบสำรองไฟฟ้าUPS

๗.๒.๒.๓ความเสี่ยงต่ำมีระบบสำรองไฟฟ้าหรือไม่ก็ได้

๗.๒.๓.ความมั่นคงปลอดภัยของการเดินสายสัญญาณและสายสื่อสาร (Cabling Security)

๗.๒.๓.๑ ความเสี่ยงสูง การเดินสายต้องใช้สายป้องกันการรบกวนสัญญาณและการเข้าถึงสายสัญญาณ

๗.๒.๓.๓ ความเสี่ยงปานกลาง การเดินสายต้องป้องกันการเข้าถึงสายสัญญาณ

๗.๒.๓.๓ ความเสี่ยงต่ำใช้สายสัญญาณธรรมดา

๗.๒.๓.๔ ต้องมีแผนการตรวจสอบระบบการเดินสายไฟ สายเคเบิ้ล สายสื่อสาร

๗.๒.๔.การบำรุงรักษาอุปกรณ์ (Equipment maintenance)

๗.๒.๔.๑. ระบบที่มีความเสี่ยงสูงต้องบำรุงรักษาทุก ๑ เดือน

๗.๒.๔.๒. ระบบที่มีความเสี่ยงปานกลางต้องบำรุงรักษาทุก ๓ เดือน

๗.๒.๔.๓. ระบบที่มีความเสี่ยงต่ำต้องบำรุงรักษาทุก ๑๒ เดือน

๗.๒.๕.การนำทรัพย์สินของกรมออกนอกสำนักงาน (Removal of assets)

๗.๒.๕.๑ ทรัพย์สินที่มีความเสี่ยงสูงไม่ให้ออกนอกสถานที่

๗.๒.๕.๒ทรัพย์สินที่มีความเสี่ยงปานกลางและต่ำ มีระบบการควบคุมดูแลทรัพย์สิน การลงทะเบียนทรัพย์สิน /ครุภัณฑ์ แบบฟอร์มการยืม – คืนทรัพย์สิน

๗.๒.๖.ความมั่นคงปลอดภัยของอุปกรณ์และทรัพย์สินที่ใช้งานอยู่ภายนอกสำนักงาน (Security of equipment and assets off-premises)

๗.๒.๖.๑. กำหนดรหัสการเข้าถึงการใช้งานอุปกรณ์คอมพิวเตอร์

๗.๒.๖.๒. กำหนดผู้รับผิดชอบและดูแลอุปกรณ์

๗.๒.๖.๓. กำหนดผู้รับผิดชอบและดูแลอุปกรณ์ห้องแม่ข่าย

๗.๒.๖.๔. มีระบบป้องกันความปลอดภัย เช่น antivirus การกำหนดสิทธิ์ใช้งาน

๗.๒.๗.ความมั่นคงปลอดภัยสำหรับการกำจัดหรือทำลายอุปกรณ์ หรือการนำอุปกรณ์ไปใช้งานอย่างอื่น (Secure disposal or re-use of equipment)

๗.๒.๗.๑. มีการตรวจสอบการลบข้อมูลและทำลายสื่อบันทึกข้อมูลก่อนทิ้งอุปกรณ์

๗.๒.๘.อุปกรณ์ของผู้ใช้งานที่ทิ้งไว้โดยไม่มีผู้ดูแล (Unattended use equipment)

๗.๒.๘.๑. ผู้ใช้งานต้องมีการป้องกันอุปกรณ์ทุกครั้งที่ทิ้งไว้ในสถานที่หนึ่ง ณ ช่วงเวลาหนึ่งโดยไม่มีผู้ดูแลระบบ

๗.๒.๙.นโยบายโต๊ะทำงานปลอดเอกสารสำคัญและนโยบายการป้องกันหน้าจอคอมพิวเตอร์ (Clear desk and clear screen policy)

เอกสารกระดาษและสื่อบันทึกข้อมูลที่ถอดแยกได้ และป้องกันสารสนเทศในอุปกรณ์ประมวลผลสารสนเทศ เมื่อมีการนำมาใช้งาน ต้องทำเรื่องขออนุญาตการนำไปใช้งานงานและกำหนดระยะเวลาเริ่มใช้งาน ระบุระยะเวลาในการนำส่งคืน ระบุถึงการจัดเก็บในระยะเวลาการใช้งาน

๘. ข้อกำหนดหลักที่ ๘ ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operations Security)

๘.๑. ขั้นตอนการปฏิบัติงานและหน้าที่ความรับผิดชอบ (Operation Procedures and Responsibilities)

๘.๑.๑.มีการแบ่งมอบหมายและจัดแบ่งหน้าที่ความรับผิดชอบอย่างชัดเจนรวมทั้งมีขั้นตอนคู่มือการปฏิบัติงานที่เป็นลายลักษณ์อักษร (Documented operating procedures) และสามารถเข้าถึงได้โดยผู้ที่จำเป็นต้องใช้งานและมีระบบการควบคุมกำกับ ติดตามประเมินผลการปฏิบัติงานตามหน้าที่ความรับผิดชอบอย่างต่อเนื่อง

๘.๑.๒. การบริหารจัดการเปลี่ยนแปลง (Change management)

๘.๑.๒.๑. มีการกำหนดระดับชั้นของผู้ให้ข่าวสาร

๘.๑.๒.๒. การเปลี่ยนแปลงต่อกรม กระบวนการทางธุรกิจ อุปกรณ์ประมวลผลสารสนเทศและระบบที่มีผลต่อความมั่นคงปลอดภัยสารสนเทศ ต้องมีการควบคุมการดำเนินงาน

๘.๑.๓. การบริหารจัดการขีดความสามารถของระบบ (Capacity management)

๘.๑.๓.๑. มีการกำหนดหน้าที่ความรับผิดชอบของผู้ดูแลข้อมูล

๘.๑.๓.๒. มีการวางแผนการตรวจสอบประเมินขีดความสามารถของระบบและกำหนดค่าสูงสุดที่ยอมรับได้ของขีดความสามารถของระบบทั้งทางด้านอุปกรณ์ระบบคอมพิวเตอร์ และระบบเครือข่าย อย่างน้อยการประเมินค่า CPU, RAM, Storage, Network Utilization

๘.๑.๓.๓. ดำเนินการตรวจสอบประเมินขีดความสามารถของระบบดังระบุข้างต้น

๘.๑.๓.๔. ดำเนินการวิเคราะห์ ประมวลผล ขีดสมรรถนะของระบบเพื่อค้นหาสาเหตุและปัญหารวมทั้งแนวทางการแก้ไขอย่างเป็นระบบ รวมทั้ง ติดตาม ปรับปรุง และคาดการความต้องการเพิ่มเติมในอนาคตเพื่อให้ระบบมีประสิทธิภาพ

๘.๑.๓.๕. สรุปผลการบริหารจัดการขีดสมรรถนะของระบบ

๘.๑.๔. การแยกสภาพแวดล้อมสำหรับการพัฒนา การทดสอบ และการให้บริการออกจากกัน (Separation of development, testing and operational environments)

๘.๑.๔.๑. มีการสำรองข้อมูลก่อนการปรับปรุงแก้ไข เพื่อการพัฒนาการทดสอบและการให้บริการออกจากกัน

๘.๑.๔.๒. ต้องจัดทำการแยกระบบในการพัฒนาและระบบการตรวจสอบและระบบการให้บริการออกจากกันเพื่อลดความเสี่ยงของการเข้าถึงหรือการเปลี่ยนแปลงสำหรับการให้บริการโดยไม่ได้รับอนุญาต

๘.๒. การป้องกันโปรแกรมไม่ประสงค์ดี (Protection from Malware)

๘.๒.๑. มาตรการป้องกันโปรแกรมไม่ประสงค์ดี (Controls against malware)

๘.๒.๑.๑. มีระบบการตรวจจับ การป้องกัน และการกู้คืนข้อมูลจากผู้ที่ไม่ประสงค์ดี

๘.๒.๑.๒. มีการจัดอบรมเจ้าหน้าที่ให้ทราบถึงพฤติกรรมที่พึงประสงค์ต่อการใช้งานที่ถูกต้องปลอดภัย และไม่มีความเสี่ยง

๘.๒.๑.๓. มีการติดตั้งระบบป้องกันโปรแกรมที่ไม่ประสงค์ดีรวมทั้งตรวจสอบประสิทธิภาพให้สามารถป้องกันได้อย่างมีประสิทธิภาพ

๘.๒.๑.๔. ต้องมีการตรวจสอบประเมินผล มาตรการที่กำหนดไว้อย่างสม่ำเสมอเพื่อนำมาสู่การปรับปรุงความมั่นคงปลอดภัย

การสำรองข้อมูล (Backup)

๘.๒.๒. การสำรองข้อมูล (Information Backup)

๘.๓. การสำรองข้อมูลและระบบสารสนเทศ

๘.๔. ต้องสำรองข้อมูลสำคัญของกระบวนงานหลัก หรือข้อมูลที่สำคัญต่อการดำเนินงานของหน่วยงานทุกระดับ รวมถึงโปรแกรมระบบปฏิบัติการ (operating system) โปรแกรมระบบงานคอมพิวเตอร์ (application system) และชุดคำสั่งที่ใช้ทำงานให้ครบถ้วน ให้สามารถพร้อมใช้งานได้อย่างต่อเนื่อง

๘.๕. ต้องกำหนดขั้นตอนหรือวิธีปฏิบัติในการสำรองข้อมูลเพื่อเป็นแนวทางให้แก่ผู้ปฏิบัติงานโดยอย่างน้อยควรมีรายละเอียด ดังนี้(ตามแบบฟอร์ม ๑)

๘.๖. ข้อมูลที่ต้องสำรอง และความถี่ในการสำรอง

๘.๗. ประเภทสื่อบันทึก (media)

๘.๘. จำนวนที่ต้องสำรอง (copy)

๘.๙. รอบระยะเวลาการสำรอง (cycle)

๘.๑๐. ขั้นตอนและวิธีการสำรองโดยละเอียดรวมถึงผู้ที่มีหน้าที่และความรับผิดชอบในการสำรองข้อมูล

๘.๑๑. สถานที่สำรองข้อมูล ต้องมีระยะห่างในการจัดเก็บไม่น้อยกว่า ๒๐ กม. (ศูนย์ วศ. / ศูนย์ สช.) ที่อยู่ตามเขตปริมณฑล หรือในเขตพื้นที่กำหนด

๘.๑๒. วิธีการเก็บรักษาสื่อบันทึก เช่น สำรอง online /Hard copy

๘.๑๓. ต้องมีการบันทึกการปฏิบัติงาน (log book) เกี่ยวกับการสำรองข้อมูลของเจ้าหน้าที่เพื่อตรวจสอบความถูกต้องครบถ้วน และควรมีการตรวจสอบบันทึกดังกล่าวอย่างสม่ำเสมอ(ตามแบบฟอร์ม ๒)

๘.๑๔. ๒. การทดสอบข้อมูลสำรอง(กู้ระบบคืน)

๘.๑๕. ต้องทดสอบข้อมูลสำรองอย่างน้อยทุก ๔ เดือน เพื่อให้มั่นใจได้ว่าข้อมูล รวมทั้งโปรแกรมระบบต่างๆ ที่ได้สำรองไว้ มีความถูกต้องครบถ้วนและใช้งานได้

๘.๑๖. ต้องกำหนดขั้นตอนหรือวิธีปฏิบัติในการทดสอบและการนำข้อมูล/กู้ระบบคืนสำรองจากสื่อบันทึกมาใช้งาน (ตามแบบฟอร์ม ๓)

๘.๑๗. ๓.การเก็บรักษาข้อมูลสำรองและสื่อบันทึก

๘.๑๘. ต้องจัดเก็บสื่อบันทึกข้อมูลสำรอง พร้อมทั้งสำเนาขั้นตอนหรือวิธีปฏิบัติต่างๆ ไว้นอกสถานที่ โดยมีระยะห่างในการจัดเก็บไม่น้อยกว่า ๒๐ กม. (ศูนย์ วศ. / ศูนย์ สช.) ที่อยู่ตามเขตปริมณฑล หรือในเขตพื้นที่กำหนด เพื่อความปลอดภัยในกรณีที่สถานที่ปฏิบัติงานได้รับความเสียหาย โดยสถานที่ดังกล่าวต้องจัดให้มีระบบควบคุมการเข้าออก และระบบควบคุมสภาพแวดล้อมอย่างเหมาะสมด้วย

๘.๑๙. ในกรณีที่จำเป็นต้องจัดเก็บข้อมูลเป็นระยะเวลานาน ก็ต้องคำนึงถึงวิธีการนำข้อมูลกลับมาใช้งานในอนาคตด้วย เช่น ถ้าจัดเก็บข้อมูลในสื่อบันทึกประเภทใด ก็ต้องมีการเก็บอุปกรณ์และซอฟท์แวร์ที่เกี่ยวข้องสำหรับใช้อ่านสื่อบันทึกประเภทนั้นไว้ด้วยเช่นกัน เป็นต้น

๘.๒๐. ควรติดฉลากที่มีรายละเอียดชัดเจนไว้บนสื่อบันทึกข้อมูลสำรอง เพื่อให้สามารถค้นหาได้โดยเร็ว และเพื่อป้องกันการใช้งานสื่อบันทึกผิดพลาด

๘.๒๑. การขอใช้งานสื่อบันทึกข้อมูลสำรองควรได้รับอนุมัติจากผู้มีอำนาจ และควรจัดทำทะเบียนควบคุมการรับและส่งมอบสื่อบันทึกข้อมูลสำรอง โดยควรมีรายละเอียดเกี่ยวกับผู้รับ ผู้ส่ง ผู้อนุมัติ ประเภทข้อมูล และเวลา(ตามแบบฟอร์ม ๔)

๘.๒๒. ต้องกำหนดขั้นตอนการทำลายข้อมูลสำคัญและสื่อบันทึกที่ไม่ได้ใช้งานแล้ว ซึ่งรวมถึงข้อมูลสำคัญต่างๆ ในฮาร์ดดิสก์(ตามแบบฟอร์ม ๕)

๘.๒๓. การบันทึกข้อมูลล๊อกและการเฝ้าระวัง (Logging and Monitoring)

๘.๒๓.๑. การบันทึกข้อมูลล็อกแสดงเหตุการณ์ (Event logging)

๘.๒๓.๑.๑. มีการบันทึกการทำงานของระบบที่ไม่เป็นไปตามปกติ ความผิดพลาดในการทำงานของระบบ และเหตุการณ์ความมั่นคงปลอดภัย ต้องมีการบันทึกไว้ จัดเก็บและทบทวนอย่างสม่ำเสมอ รวมทั้งกำหนดวิธีการและระยะเวลาในการจัดเก็บให้สอดคล้องกับ พรบ. ว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ ปี ๕๐

๘.๒๓.๒. การป้องกันข้อมูลล็อก (Protection of log information)

๘.๒๓.๒.๑. อุปกรณ์บันทึกข้อมูลล็อกและข้อมูลล็อกต้องได้รับการป้องกันจากการเปลี่ยนแปลงแก้ไขและการเข้าถึงโดยไม่ได้รับอนุญาต

๘.๒๓.๒.๒. ต้องมีการตรวจสอบติดตามประเมินผลระบบการป้องกันข้อมูลล็อกที่มีประสิทธิภาพ

๘.๒๓.๓. ข้อมูลล็อกกิจกรรมของผู้ดูแลระบบและเจ้าหน้าที่ปฏิบัติการระบบ (Administrator and operator logs)

๘.๒๓.๓.๑. กิจกรรมของผู้ดูแลระบบและเจ้าหน้าที่ปฏิบัติการต้องมีการบันทึกไว้เป็นข้อมูลล็อก ข้อมูลดังกล่าวต้องมีการป้องกันและทบทวนอย่างสม่ำเสมอ

๘.๒๓.๔. การตั้งนาฬิกาให้ถูกต้อง (Clock Synchronization)

๘.๒๓.๔.๑. ต้องมีการกำหนดการตั้งนาฬิกาของระบบที่เกี่ยวข้องทั้งหมดภายในกรมหรือในขอบเขตหนึ่ง ต้องมีการตั้งค่าเวลาให้ตรงและถูกต้องเทียบกับแหล่งอ้างอิงเวลาที่มีความน่าเชื่อถือได้

๘.๒๓.๔.๒. ต้องมีการวางแผนและตรวจสอบการตั้งนาฬิกาให้ตรงและถูกต้อง

๘.๒๓.๔.๓. ต้องมีการสรุปประเมินผลการตรวจสอบการตั้งนาฬิกา

๘.๒๔. การควบคุมการติดตั้งซอร์ฟแวร์บนระบบให้บริการ (Control of operation software)

๘.๒๔.๑. การติดตั้งซอฟต์แวร์บนระบบให้บริการ (Installation of software on operation systems)

๘.๒๔.๑.๑. วิเคราะห์วางแผนการติดตั้งซอฟต์แวร์บนระบบการให้บริการเพื่อป้องกันความเสี่ยงต่อผลกระทบในการติดตั้งซอฟต์แวร์ระบบให้บริการที่อาจเกิดความล้มเหลว

๘.๒๔.๑.๒. มีขั้นตอนปฏิบัติสำหรับการควบคุมการติดตั้งซอฟต์แวร์บนระบบให้บริการต้องมีการปฏิบัติตามให้สอดคล้อง

๘.๒๔.๑.๓. สรุปวิเคราะห์ประเมินผล การติดตั้งซอฟต์แวร์ เพื่อนำไปสู่การปรับปรุงวางแผนการติดตั้งซอฟต์แวร์

๘.๒๕. การบริการจัดการช่องโหว่ทางเทคนิค (Technical Vulnerability Management)

๘.๒๕.๑. การบริหารจัดการช่องโหว่ทางเทคนิค (Management of technical vulnerabilities)

๘.๒๕.๑.๑. มีการบริหารจัดการช่องโหว่ทางเทคนิคของระบบที่ใช้งานต้องมีการติดตามอย่างทันกาล จุดอ่อนต่อช่องโหว่ดังกล่าวของกรมต้องมีการประเมิน และมาตราที่เหมาะสม เพื่อจัดการกับความเสี่ยงที่เกี่ยวข้อง

๘.๒๕.๒. การจำกัดการติดตั้งซอฟต์แวร์ (Restrictions on software installation)

๘.๒๕.๒.๑. มีกฎเกณฑ์ควบคุมการติดตั้งซอฟต์แวร์โดยผู้ใช้งานต้องมีการกำหนดและปฏิบัติตาม

๘.๒๕.๒.๒. มีการตรวจสอบช่องโหวทางเทคนิคอย่างสม่ำเสมอ รวมทั้งมีการวิเคราะห์สรุปประเมินผลเพื่อนำไปสู่การปรับปรุงอย่างเป็นระบบและต่อเนื่อง

๘.๒๖. สิ่งที่ต้องพิจารณาในการตรวจประเมินระบบ (Information Systems Audit Considerations)

๘.๒๖.๑. มาตรการการตรวจประเมินระบบ (Information systems audit controls)

๘.๒๖.๑.๑. ตรวจประเมินด้านความมั่นคงของระบบเพื่อให้ระบบพร้อมใช้งานได้อย่างต่อเนื่อง

๘.๒๖.๑.๒. ตรวจขีดความสามารถของระบบ

๘.๒๖.๑.๓. กำหนดค่าสูงสุดของขีดสรรถนะที่ควรเป็นอย่างน้อย ดังนี้

- CPU RAM HDD Bandwidth ไม่ควรเกินร้อยละ ๘๐
- Down time ไม่ควรเกิน ๑๘๐ นาที/ปี (การันตีค่า Service Availability = ๙๙.๙๖%)

๘.๒๖.๑.๔. รวบรวมข้อมูลการหยุดชะงักและขีดสมรรถนะของระบบ

๘.๒๖.๑.๕. ศึกษาวิเคราะห์กระบวนการในการเฝ้าระวังความพร้อมใช้งานของระบบ

๘.๒๖.๑.๖. นำข้อมูลมาวิเคราะห์ถึงความเสี่ยง สาเหตุและผลกระทบของเหตุการณ์ที่เกิดขึ้น

๘.๒๖.๑.๗. กำหนดแนวทางและมาตรการในการป้องกันเพื่อลดโอกาสการหยุดชะงักที่มีต่อการดำเนินงานของกรม

๘.๒๖.๑.๘. สุ่มตรวจคุณภาพข้อมูลรวมทั้งกระบวนการนำเข้าและการประมวลผลออก

- กำหนดเกณฑ์การตรวจสอบด้านคุณภาพข้อมูล

๘.๒๖.๑.๙. ศึกษากระบวนการในการนำเข้า จัดเก็บ ประมวลผลข้อมูล

๘.๒๖.๑.๑๐.วิเคราะห์ถึงความสี่ยง สาเหตุและผลกระทบของคุณภาพข้อมูลที่เกิดขึ้นในระบบ

๘.๒๖.๑.๑๑.กำหนดแนวทางและมาตรการในการป้องกันแก้ไข

๘.๒๖.๑.๑๒.กำหนดรายการข้อมูลที่เป็นความลับของกรมและระดับชั้นความลับ

๘.๒๖.๑.๑๓.ศึกษากระบวนการขั้นตอนวิธีการจัดเก็บข้อมูลที่เป็นความลับของกรม

๘.๒๖.๑.๑๔.วิเคราะห์ความเสี่ยงและสาเหตุผลการทบของโอกาสที่มีการเปลี่ยนแปลงแก้ไขข้อมูลที่เป็นความลับ

๘.๒๖.๑.๑๕.กำหนดแนวทางมาตรการในการแก้ไขป้องกัน

๙. ข้อกำหนดหลักที่ ๙ ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications security)

๙.๑. การบริหารจัดการความมั่นคงปลอดภัยของเครือข่าย (Network Security Management)

๙.๑.๑.มาตรการเครือข่าย (Network controls)

๙.๑.๑.๑. ออกมาตรการการเข้าถึงระบบเครือข่ายโดยใช้ไอพีแอดเดรส

๙.๑.๑.๒. สร้างระบบจัดเก็บ LOG ไฟล์ในการเข้าถึงเครือข่ายของกรม

๙.๑.๑.๓. พิจารณาการเปิดเข้าใช้งาน port ของผู้ร้องขอใช้งาน โดยกำหนดระยะเวลาในการเข้าใช้งานตามที่ผู้ดูแลระบบจะอนุญาต

๙.๑.๑.๔. มีการกำหนด Vlan ในการเข้าใช้งานระบบเครือข่ายของกรมนั้นๆ

๙.๑.๑.๕. ถ้าไม่มีการใช้งานในระยะเวลาหนึ่ง ระบบจะดำเนินการตัดสัญญาณอินเตอร์เน็ต (Session timeout) เพื่อนำสัญญาณไปให้ผู้ร้องขอคนอื่นต่อไป

๙.๑.๒.ความมั่นคงปลอดภัยสำหรับบริการเครือข่าย (Security of network services)

๙.๑.๒.๑. กำหนดขั้นตอนการใช้บริการข้อมูลของหน่วยงาน

๙.๑.๒.๒. การตรวจสอบการให้บริการ เพื่อวัดความพึงพอใจของผู้รับบริการ

๙.๑.๒.๓. มีการพัฒนาและปรับปรุงระบบสารสนเทศให้มีความทันสมัยและเป็นปัจจุบัน

๙.๑.๒.๔. มีการยืนยันตัวบุคคลที่แท้จริง

๙.๑.๒.๕. มีระบบตรวจสอบการเป็นบุคคลที่แท้จริง

๙.๑.๓.การแบ่งแยกเครือข่าย (Segregation in networks)

๙.๑.๓.๑. กำหนดผู้ดูแลระบบเครือข่าย

๙.๑.๓.๒. กำหนดสิทธิและการให้สิทธิแก่ผู้ใช้งานในระบบเครือข่าย

๙.๑.๓.๓. มีการแยกประเภทของผู้ใช้งานและกำหนดการเข้าถึงข้อมูลในระดับชั้นต่างๆ เช่น ผู้บริหาร, ผู้ปฏิบติงานตามตำแหน่ง แผนกหรือหน้าที่การงาน ฯลฯ

๙.๒. การถ่ายโอนสารสนเทศ (Information transfer)

๙.๒.๑.นโยบายและขั้นตอนปฏิบัติสำหกรับการถ่ายโอนสารสนเทศ (Information transfer policies and procedures)

๙.๒.๑.๑. กำหนดนโยบาย ขั้นตอนการปฏิบัติงาน และมาตรการรองรับ โดยผ่านช่องทางการสื่อสารทุกชนิด

๙.๒.๒.ข้อตกลงสำหรับการถ่ายโอนสารสนเทศ (Agreements on information transfer)

๙.๒.๒.๑. กำหนดให้ผู้เข้ามาใช้งานขอรหัสผ่านเพื่อเข้าใช้งานระบบจากผู้ดูแลระบบจากผู้ดูแลระบบ ซึ่งรหัสผ่านสามารถใช้ได้ในช่วงเวลาที่กำหนดไว้เท่านั้น

๙.๒.๒.๒. กำหนดข้อตกลง แนวทาง วิธีปฏิบัติ ระยะเวลา ของการถ่ายโอนสารสนเทศ

๙.๒.๒.๓. มีการบันทึก วันเวลาที่มีการถ่ายโอนสารสนเทศในระหว่างกรม

๙.๒.๒.๔. จำกัดการเข้าถึงสารสนเทศเมื่อมีการโอนย้ายเสร็จสิ้นแล้ว

๙.๒.๓.การส่งข้อความทางอิเล็กทรอนิกส์ (Electronic massaging)

๙.๒.๓.๑. กำหนดการใช้เมลล์อิเล็กทรอนิกส์ของกระทรวงไอซีที(mail.go.th) เฉพาะงานที่เกี่ยวข้องกับงานราชการ

๙.๒.๔.ข้อตกลงการรักษาความลับหรือไม่เปิดเผยความลับ (Confidentiality or non-disclosure agreements)

๙.๒.๔.๑. กำหนดผู้ดูแลหลักที่รับผิดชอบในข้อมูลที่สำคัญ

๙.๒.๔.๒. มีการกำหนดโทษในการรักษาความลับลากรไม่เปิดเผยความลับ

๑๐.ข้อกำหนดหลักที่ ๑๐ การจัดหา การพัฒนา และการบำรุงรักษาระบบ (System acquisition, development and maintenance)

๑๐.๑. ความต้องการด้านความมั่นคงปลอดภัยของระบบ (Security requirements of information systems)

๑๐.๑.๑. การวิเคราะห์และกำหนดความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ (Information security requirements analysis and specification)

ระบบสารสนเทศใหม่ ต้องมีการรักษาความปลอดภัย ที่สอดคล้องและสามารถเชื่อมโยงกับระบบเดิมได้ ระบบสารสนเทศเก่า จะต้องมีการป้องกันการเข้าใช้ server โดยอนุญาตให้เฉพาะบุคคลที่มีหน้าที่การทำงานโดยใช้การ login ด้วย user name และ password ของบุคคลนั้น และการยืนยันการเข้าใช้ว่าเป็นบุคคลไม่ใช่ program การ update ต่างๆต้องเป็นแบบ manual เท่านั้น

๑๐.๑.๒. ความมั่นคงปลอดภัยของบริการสารสนเทศบนเครือข่ายสาธารณะ (Securing application services on public networks)

สารสนเทศที่เกี่ยวข้องกับบริการสารสนเทศซึ่งมีการส่งผ่านเครือข่ายสาธารณะต้องได้รับการป้องกัน

-จากการเปลี่ยนแปลงข้อมูลบนเครือข่ายสาธารณะโดยการกำหนด user name และ password ของผู้เข้าถึงข้อมูล

-ข้อมูลต้องระบุได้ว่าบุคคลใดเป็นผู้สร้างข้อมูลและมีการสำเนา/สำรองข้อมูลทุกครั้งเพื่อสามารถย้อนดูข้อมูลเก่า ณ เวลานั้นได้

-การเปิดเผยข้อมูลบนเครือข่ายสาธารณะ ต้องได้รับการอนุญาตของผู้ดูแลระบบเท่านั้น

-ไม่อนุญาตให้แก้ไขข้อมูลใดๆ ที่ถูกสร้างขึ้น

๑๐.๑.๓. การป้องกันธุรกรรมของบริการสารสนเทศ (Protecting application services transactions)

สารสนเทศที่เกี่ยวข้องกับธุรกรรมของบริการสารสนเทศ ให้มีการตั้งระบบตอบกลับการส่งข้อมูลพร้อมทั้งมีการเข้ารหัสข้อมูลและมีการยืนยันตัวบุคคล

๑๐.๒. ความมั่นคงปลอดภัยสำหรับกระบวนการพัฒนาและสนับสนุน (Security in development and support processes)

๑๐.๒.๑. นโยบายการพัฒนาระบบให้มีความมั่นคงปลอดภัย (Secure development policy)

มีการแต่งตั้งผู้ดูแลควบคุมระบบซอฟต์แวร์ โดยให้กำหนดระยะเวลาอัพเดตซอฟต์แวร์ทุกๆ ๖ เดือน

๑๐.๒.๒. ขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงระบบ (System change control procedures)

แต่งตั้งคณะทำงานดูแลการเข้าใช้งานระบบ และตั้งข้อปฏิบัติในการเข้าใช้งาน

๑๐.๒.๓. การทบทวนทางเทคนิคต่อระบบหลังจากเปลี่ยนแปลงโครงสร้างพื้นฐานของระบบ (Technical review of applications after operating platform changes)

ทำการทดสอบระบบทุกครั้งเมื่อมีการเปลี่ยนแปลงโครงสร้าง

๑๐.๒.๔. การจำกัดการเปลี่ยนแปลงซอฟต์แวร์สำเร็จรูป (Restrictions on changes to software packages)

การใช้ซอฟต์แวร์ของผู้ผลิตจะใช้การแก้ไขโดยผ่านทาง firewall และกำหนดให้มีการupdate firewall ต่างๆ ให้เป็นแบบManual

๑๐.๒.๕. หลักการวิศวกรรมระบบด้านความมั่นคงปลอดภัย (Secure system engineering principles)

-มีคำสั่งจัดตั้งคณะกรรมการระบบด้านความมั่นคงปลอดภัย

-จัดทำแบบแปลนโครงสร้างทางวิศวกรรมและสามารถรองรับการแก้ไขเพิ่มเติมในอนาคตได้
-ตรวจทาน ปรับปรุง แก้ไขและทดสอบระบบทุก ๆ จุดและกระจายการออกแบบไปยังส่วนกลาง

๑๐.๒.๖. สภาพแวดล้อมของการพัฒนาระบบที่มีความมั่นคงปลอดภัย (Secure development environment)
-แต่งตั้งคณะกรรมการเพื่อศึกษาสภาพแวดล้อมของการพัฒนาระบบ
-จ้างบริษัทที่มีมาตรฐานเพื่อเข้ามาจัดทำระบบ

๑๐.๒.๗. การจ้างหน่วยงานภายนอกพัฒนาระบบ (Outsourced development)
-จัดบุคลากรสุ่มตรวจสอบซอฟแวร์

๑๐.๒.๘. การทดสอบด้านความมั่นคงปลอดภัยของระบบ (System security testing)
-มีการกำหนดผลลัพธ์ที่ต้องการในการทดสอบด้านความมั่นคงปลอดภัย

๑๐.๒.๙. การทดสอบเพื่อรับรองระบบ (System acceptance testing)
-จัดบุคลากรในการทดลองและประเมินผลการใช้งานของระบบ

๑๐.๓. ข้อมูลสำหรับการทดสอบ (Test data)

๑๐.๓.๑. การป้องกันข้อมูลสำหรับการทดสอบ (Protection of test data)
แยกระบบที่ทดสอบจากระบบที่ใช้งาน

๑๑.ข้อกำหนดหลักที่ ๑๑ ความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier relationships)

๑๑.๑. ความมั่นคงปลอดภัยสารสนเทศกับความสัมพันธ์กับผู้ให้บริการภายนอก (Information security in supplier relationships)

๑๑.๑.๑. นโยบายความมั่นคงปลอดภัยสารสนเทศด้านความสัมพันธ์กับผู้ให้บริการภายนอก (Information security policy for supplier relationships)
-จัดทำข้อกำหนด ข้อตกลง การเข้าถึงทรัพย์สินกับบริษัทที่ว่าจ้าง
-จัดทำนิติกรรมสัญญาเป็นลายลักษณ์อักษร

๑๑.๑.๒. การระบุความมั่นคงปลอดภัยในข้อตกลงการให้บริการของผู้ให้บริการภายนอก (Addressing security within supplier agreements)
-ต้องกำหนดสิทธิ์บุคคลของผู้ให้บริการภายนอกในการเข้าถึงข้อมูล การประมวลผล การจัดเก็บการสื่อสาร และการให้บริการโครงสร้างพื้นฐาน

๑๑.๑.๓. ห่วงโซ่การให้บริการเทคโนโลยีสารสนเทศและสื่อสารโดยผู้ให้บริการภายนอก (Information and communication technology supply chain)
-จัดทำรายละเอียดข้อตกลงเกี่ยวกับความเสี่ยงที่จะเกิดขึ้นทุกขั้นตอน
-ขั้นตอนห่วงโซ่ในการให้บริการเทคโนโลยีสารสนเทศสามารถตรวจสอบย้อนหลังได้

๑๑.๒. การบริหารจัดการการให้บริการโดยผู้ให้บริการภายนอก (Supplier service delivery management) ควบคุม กำกับดูแลเอกชน ให้รักษาความมั่นคงปลอดภัยและระยะเวลาที่ให้บริการตามสัญญา

๑๑.๒.๑. การติดตามและทบทวนบริการของผู้ให้บริการภายนอก (Monitoring and review of supplier services)

-หน่วยงาน ต้องมีบุคลากรติดตาม ทบทวน ตรวจสอบ ประเมินการให้บริการของเอกชน ระยะเวลาต่อสัปดาห์

-ทบทวนปัญหาที่เกิดขึ้น ในห้วงเวลาที่ให้บริการที่ผ่านมา

-ต้องมีแบบฟอร์มการตรวจประเมินการให้บริการอย่างชัดเจน

๑๑.๒.๒. การบริหารจัดการการเปลี่ยนแปลงบริการของผู้ให้บริการภายนอก (Managing changes to supplier services)

-จัดทำระดับความสำคัญของข้อมูลสารสนเทศ จัดเรียงเพื่อทบทวนการประเมินความเสี่ยงให้อยู่ในขั้นตอนและระยะเวลา

-กรณีที่ผู้ให้บริการภายนอกมีการเปลี่ยนแปลง ปรับปรุงนโยบาย ขั้นตอนปฏิบัติและมาตรการต่างๆ จะต้องแจ้งให้ผู้รับบริการทราบล่วงหน้าอย่างน้อย ๓ วันทำการ

- ขั้นตอนปฏิบัติและมาตราการต่าง ๆ ที่ไม่ได้กำหนด ให้แจ้งยกเลิกแจ้งให้ผู้รับบริการทราบล่วงหน้าอย่างน้อย ๓ วันทำการ

๑๒.ข้อกำหนดหลักที่ ๑๒ การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management)

๑๒.๑. การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศและการปรับปรุง (Management of information security incidents and improvements)

-มีการกำหนดวิธีปฏิบัติอย่างชัดเจน เมื่อมีเหตุการณ์ที่จะก่อให้เกิดความไม่ปลอดภัยสารสนเทศ

-เมื่อเกิดสถานการณ์ที่ไม่ปลอดภัยหรือมีจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัย ให้มีการรายงานต่อผู้ดูแลระบบ และผู้บังคับบัญชาให้ทราบทุกครั้ง

๑๒.๑.๑. หน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติ (Responsibilities and procedures)

๑๒.๑.๑.๑. มีการกำหนดเพื่อให้มีการตอบสนองอย่างรวดเร็ว ได้ผล และตามลำดับเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ

-มีการกำหนดผู้รับผิดชอบและหน้าที่รับผิดชอบอย่างชัดเจน

-มีมาตรการในการควบคุมกำกับดูแลผู้รับผิดชอบ เพื่อให้การปฏิบัติเป็นไปในทางเดียวกัน

๑๒.๑.๒. การรายงานสถานการณ์ความมั่นคงปลอดภัยสารสนเทศ (Reporting information security events)

๑๒.๑.๒.๑. มีการรายงานผ่านทางช่องทางการบริหารจัดการที่เหมาะสมและรายงานอย่างรวดเร็วที่สุดเท่าที่จะทำได้

- จัดทำการรายงานผ่านช่องทางที่สามารถแจ้งเตือนแก่ผู้ดูแลระบบทราบให้รวดเร็วมากที่สุด

-เมื่อมีสถานการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศเกิดขึ้น ให้ผู้ดูแลทำรายงานเสนอต่อผู้บังคับบัญชาในทันที

๑๒.๑.๓. การรายงานจุดอ่อนความมั่นคงปลอดภัยสารสนเทศ (Reporting information security weaknesses)

๑๒.๑.๓.๑. มีการทำกำหนดเกณฑ์เหตุการณ์อยู่ในระดับต่ำ

ผู้ดูแลระบบสารสนเทศของสำนัก/กอง สามารถแก้ไขเหตุการณ์ที่เกิดขึ้นเองได้ เช่น การติดไวรัส เป็นต้น และทำการรายงานเหตุการณ์ที่เกิดขึ้น ทุก ๆ ๑ เดือน ต่อผู้อำนวยการของสำนัก/กอง

๑๒.๑.๓.๒. มีการทำกำหนดเกณฑ์เหตุการณ์อยู่ในระดับกลาง

ผู้ดูแลระบบสารสนเทศของสำนัก/กอง แจ้งให้ผู้อำนวยการของสำนัก/กอง ทราบถึงเหตุการณ์ที่เกิดขึ้น หากเหตุการณ์ที่เกิดขึ้น สำนัก/กอง ประเมินความเสี่ยงแล้ว ให้สำนัก/กอง ทำการแจ้งเป็นลายลักษณ์อักษร แจ้งไปยัง สำนัก IT ของกรมฯ เพื่อให้สำนัก IT เข้ามาแก้ไขเหตุการณ์ที่เกิดขึ้น

๑๒.๑.๓.๓. มีการทำกำหนดเกณฑ์เหตุการณ์อยู่ในระดับสูง

ผู้ดูแลระบบสารสนเทศของสำนัก/กอง ต้องทำการแจ้งไปยังสำนัก IT กรมฯอย่างเร่งด่วน หากเหตุการณ์ที่เกิดขึ้น เป็นเหตุการณ์ร้ายแรง และเร่งด่วน เพื่อหาแนวทางในการแก้ไขปัญหา จากนั้นทำการสรุปปัญหาที่เกิดขึ้นกับระบบสารสนเทศของสำนัก/กอง ให้ผู้อำนวยการสำนัก/กอง และผู้บริหารระดับสูงทราบ

๑๒.๑.๔. การประเมินและตัดสินใจต่อสถานการณ์ความมั่นคงปลอดภัยสารสนเทศ (Assessment of and decision on information security events)

๑๒.๑.๔.๑. **<u>หัวหน้าระบบสารสนเทศ</u>** : ต้องกำหนดนโยบายให้กับบุคลากรและผู้ดูแลระบบในหน่วยงาน นั้น ๆ ปฏิบัติตามนโยบายที่วางไว้

-ผู้ดูแลระบบต้องกำหนดให้มีการเฝ้าระวังและรักษาอุปกรณ์ตรวจจับและป้องกันการบุกรุกระบบ เหตุการณ์ผิดปกติ และการแจ้งเตือนต่าง ๆ ที่อุปกรณ์ตรวจพบ จะถูกทำการวิเคราะห์ และหาสาเหตุของการบุกรุก ในระบบสารสนเทศของกรม เพื่อเป็นเครื่องมือสืบสวน หาบุคคลที่โจมตี บุกรุก หรือใช้ระบบในทางที่ผิด

๑๒.๑.๔.๒. **<u>ผู้ดูแลระบบ</u>** : ต้องกำหนดให้มีการเฝ้าระวังและรักษาอุปกรณ์ตรวจจับและป้องกันการบุกรุกระบบ เหตุการณ์ผิดปกติ และการแจ้งเตือนต่าง ๆ ที่อุปกรณ์ตรวจพบ

-ผู้ดูแลระบบต้องเก็บสถิติเกี่ยวกับความพยายามที่จะบุกรุกหรือโจมตีกรม เป็นเครื่องมือในการวัดประสิทธิภาพในการป้องกันภัยของระบบรักษาความปลอดภัยอื่น เช่น ไฟวอลล์เป็นต้น และเพื่อเป็นการป้องกันเครือข่ายคอมพิวเตอร์ภายในจากอันตราย ที่มาจากเครือข่ายคอมพิวเตอร์ภายนอก เช่น ผู้บุกรุก หรือ hacker รวมทั้ง ไวรัสประเภทต่าง ๆ

๑๒.๑.๔.๓. **<u>ผู้ดูแลระบบ</u>** : ผู้ดูแลระบบต้องมีการบริหารจัดการ การบุกรุกระบบ โดยต้องจัดลำดับความสำคัญของการบุกรุกจากผลกระทบที่เกิดขึ้นกับกรม

-ผู้ดูแลระบบต้องมีการบริหารจัดการ การบุกรุกระบบ โดยต้องจัดลำดับความสำคัญของการบุกรุกจากผลกระทบที่เกิดขึ้นกับกรม และจัดทำวิธีปฏิบัติที่ถูกต้อง ให้กับกรมเพื่อป้องกันเหตุการณ์ที่เกิดขึ้นซ้ำ

๑๒.๑.๕. การตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Response to information security incidents)

๑๒.๑.๕.๑. เหตุการณ์ความมั่นคงปลอดภัยสารสนเทศต้องได้รับการตอบสนองเพื่อจัดการกับปัญหาตามขั้นตอนปฏิบัติที่จัดทำไว้เป็นลายลักษณ์อักษร

-มีการจัดทำขั้นตอนการปฏิบัติอย่างชัดเจนในการแก้ไขปัญหาความมั่นคงปลอดภัยสารสนเทส

-กรณีเกิดปัญหาให้รายงานเหตุการณ์ต่อผู้บังคับบัญชาทุกครั้ง

๑๒.๑.๖. การเรียนรู้จากเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Learning from information security incidents)

๑๒.๑.๖.๑. ความรู้ที่ได้รับจากการวิเคราะห์และแก้ไขเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศต้องถูกนำมาใช้เพื่อลดโอกาสหรือผลกระทบของเหตุการณ์ความมั่นคงปลอดภัยที่จะเกิดขึ้นในอนาคต

-มีการแจ้งเวียนเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศที่เกิดขึ้น ให้เจ้าหน้าที่ภายในหน่วยงานทราบ

๑๒.๑.๗. การเก็บรวบรวมหลักฐาน (Collection of evidence)

๑๒.๑.๗.๑. กรมต้องกำหนดและประยุกต์ใช้ขั้นตอนปฏิบัติสำหรับการะบุ การรวบรวม การจัดหาและการจัดเก้บสารสนเทศซึ่งสามารถใช้เป็นหลักฐาน

-มีการเก็บหลักฐานด้านสารสนเทศในสถานที่ปลอดภัย มีข้อกำหนดและควบคุมการนำมาใช้เพื่อไม่ให้เกิดการสูญหาย

๑๓.ข้อกำหนดหลักที่ ๑๓ ประเด็นด้านความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ (Information security aspects of business continuity management)

๑๓.๑. ความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (information security continuity)

๑๓.๑.๑. การวางแผนความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (planning information security continuity)

๑๓.๑.๑.๑. ต้องสำรองข้อมูลสำคัญของกระบวนงานหลัก หรือข้อมูลที่สำคัญต่อการดำเนินงานของหน่วยงานทุกระดับ

-ต้องทดสอบข้อมูลสำรองอย่างน้อยทุก ๔ เดือน เพื่อให้มั่นใจได้ว่าข้อมูล รวมทั้งโปรแกรมระบบต่างๆ ที่ได้สำรองไว้ มีความถูกต้องครบถ้วนและใช้งานได้

๑๓.๑.๑.๒. ต้องกำหนดขั้นตอนหรือวิธีปฏิบัติในการสำรองข้อมูลเพื่อเป็นแนวทางให้แก่ผู้ปฏิบัติงานโดยอย่างน้อยควรมีรายละเอียด ดังนี้

๑๓.๑.๑.๒.๑. ข้อมูลที่ต้องสำรอง และความถี่ในการสำรอง

๑๓.๑.๑.๒.๒. ประเภทสื่อบันทึก (media)

๑๓.๑.๑.๒.๓. จำนวนที่ต้องสำรอง (copy)

๑๓.๑.๑.๒.๔. รอบระยะเวลาการสำรอง (cycle)

๑๓.๑.๑.๒.๕. ขั้นตอนและวิธีการสำรองโดยละเอียด รวมถึงผู้ที่มีหน้าที่และความรับผิดชอบในการสำรองข้อมูล

๑๓.๑.๑.๒.๖. สถานที่สำรองข้อมูล ต้องมีระยะห่างในการจัดเก็บไม่น้อยกว่า ๒๐ กม. (สบส.) ที่อยู่ตามเขตปริมณฑลหรือในเขตพื้นที่กำหนด

๑๓.๑.๑.๒.๗. ต้องมีการบันทึกการปฏิบัติงาน (log book) เกี่ยวกับการสำรองข้อมูลของเจ้าหน้าที่เพื่อตรวจสอบความถูกต้องครบถ้วน

๑๓.๑.๒. การปฏิบัติเพื่อเตรียมการสร้างความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Implementing information security continuity)

๑๓.๑.๒.๑. ต้องทดสอบข้อมูลสำรองอย่างน้อยทุก ๔ เดือน

๑๓.๑.๒.๒. ต้องกำหนดขั้นตอนหรือวิธีปฏิบัติในการทดสอบและการนำข้อมูล/กู้ระบบคืนสำรองจากสื่อบันทึกมาใช้งาน

๑๓.๑.๓. การตรวจสอบ การทบทวน และการประเมินความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Verify, review and evaluate information security continuity)

๑๓.๑.๓.๑. ต้องจัดเก็บสื่อบันทึกข้อมูลสำรอง พร้อมทั้งสำเนาขั้นตอนหรือวิธีปฏิบัติต่างๆ ไว้นอกสถานที่

๑๓.๑.๓.๒. ในกรณีที่จำเป็นต้องจัดเก็บข้อมูลเป็นระยะเวลานาน ก็ต้องคำนึงถึงวิธีการนำข้อมูลกลับมาใช้งานในอนาคตด้วย

๑๓.๑.๓.๓. ควรติดฉลากที่มีรายละเอียดชัดเจนไว้บนสื่อบันทึกข้อมูลสำรองเพื่อให้สามารถค้นหาได้โดยเร็ว,เพื่อป้องกันการใช้งานสื่อบันทึกผิดพลาด

๑๓.๑.๓.๔. มีการขอใช้งานสื่อบันทึกข้อมูลสำรองควรได้รับอนุมัติจากผู้มีอำนาจและควรจัดทำทะเบียนควบคุมการรับและส่งมอบสื่อบันทึกข้อมูลสำรอง

๑๓.๑.๓.๕. ต้องกำหนดขั้นตอนการทำลายข้อมูลสำคัญและสื่อบันทึกที่ไม่ได้ใช้งานแล้ว ซึ่งรวมถึงข้อมูลสำคัญต่างๆ ในฮาร์ดดิสก์

๑๓.๒. การเตรียมการอุปกรณ์ประมวลผลสำรอง (Redundancies)

๑๓.๒.๑. สภาพความพร้อมใช้ของอุปกรณ์ประมวลผลสารสนเทศ (Availability of information processing facilities)

๑๓.๒.๑.๑. มีการจัดลำดับความสำคัญของระบบงาน/กระบวนงาน ความสัมพันธ์ของแต่ละระบบงาน และระยะเวลาในการกู้แต่ละระบบงานด้วยการประเมินความเสี่ยง (Risk Assessment) และ/หรือการประเมินผลกระทบของกระบวนงานหลัก

๑๓.๒.๑.๒. มีการกำหนดสถานการณ์หรือลำดับความรุนแรงของปัญหา

๑๓.๒.๑.๓. มีขั้นตอนการแก้ไขปัญหาโดยละเอียดในแต่ละสถานการณ์

๑๓.๒.๑.๔. มีการกำหนดเจ้าหน้าที่รับผิดชอบ และผู้มีอำนาจในการตัดสินใจ

๑๓.๒.๑.๕. มีรายละเอียดของอุปกรณ์ที่จำเป็นต้องใช้ในกรณีฉุกเฉินของแต่ละระบบงาน

๑๓.๒.๑.๖. หน่วยงานที่เป็นหน่วยสำรองข้อมูลหรือจัดเก็บข้อมูลก็ต้องระบุรายละเอียดเกี่ยวกับศูนย์คอมพิวเตอร์สำรองให้ชัดเจน

๑๓.๒.๑.๗. มีการทบทวนหรือปรับปรุงแผนฉุกเฉินให้เป็นปัจจุบันอยู่เสมอ (ทุก ๔ เดือน) และเก็บแผนฉุกเฉินไว้ในสถานที่มั่นคงปลอดภัย

๑๓.๒.๑.๘. ทดสอบการปฏิบัติตามแผนฉุกเฉินอย่างน้อยปีละ ๒ ครั้ง โดยต้องเป็นการทดสอบในลักษณะการจำลองสถานการณ์จริง

๑๓.๒.๑.๙. ต้องสื่อสารแผนฉุกเฉินให้บุคคลที่เกี่ยวข้องทุกระดับได้รับทราบเฉพาะเท่าที่จำเป็น และควรป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องได้รับทราบ

๑๓.๒.๑.๑๐.กรณีที่เกิดเหตุการณ์ฉุกเฉิน ควรมีการบันทึกรายละเอียดของเหตุการณ์ สาเหตุของปัญหา และวิธีการแก้ไขปัญหาไว้ด้วย

๑๔.ข้อกำหนดหลักที่ ๑๔ ความสอดคล้อง (Compliance)

๑๔.๑. ความสอดคล้องกับความต้องการด้านกฎหมายและในสัญญาจ้าง (Compliance with legal and contractual requirements)

๑๔.๑.๑. การระบุกฎหมายและความต้องการในสัญญาจ้างที่เกี่ยวข้อง (Identification of applicable legislation and contractual requirements)

-จัดทำข้อกำหนดกฎหมาย ระเบียบข้อบังคับ และสัญญาจ้างอย่างเคร่งครัด

-มีการศึกษา ทบทวนข้อกำหนดกฎหมาย ระเบียบข้อบังคับ และสัญญาจ้างทุกๆ๑ ปีโดยคณะกรรมการ

๑๔.๑.๑.๑. มีการปฏิบัติตามข้อกำหนดทางกฎหมายเทคโนโลยีสารสนเทศ เพื่อป้องกันมิให้เจ้าหน้าที่ของกรมสนสังกัดกรมสนับสนุนบริการสุขภาพละเมิดข้อกำหนดของกฎหมาย

-จัดทำประกาศให้สำนัก/กอง ใน กรมสนับสนุนบริการสุขภาพ ต้องปฏิบัติตามข้อกำหนดทางกฎหมายเทคโนโลยีสารสนเทศ เพื่อป้องกันมิให้เจ้าหน้าที่ของกรมสนสังกัดกรมสนับสนุนบริการสุขภาพละเมิดข้อกำหนดของกฎหมาย

๑๔.๑.๑.๒. มีการการทำนิติกรรมสัญญาทางด้านเทคโนโลยีสารสนเทศต้องส่งให้นิติกรตรวจสอบดูความถูกต้องของสัญญาให้เป็นไปตามที่กฎหมายกำหนด

-การทำนิติกรรมสัญญาทางด้านเทคโนโลยีสารสนเทศต้องส่งให้นิติกรตรวจสอบดูความถูกต้องของสัญญาให้เป็นไปตามที่กฎหมายกำหนด เพื่อป้องกันความผิดพลาด หรือหลีกเลี่ยงการละเมิดข้อกำหนดทางกฎหมาย

๑๔.๑.๑.๓. มีการจัดตั้งคณะกรรมการจัดทำข้อกำหนดทางกฎหมายเทคโนโลยีสารสนเทศของกรมสนับสนุนบริการเพื่อรวมข้อกำหนดที่มีผลทางกฎหมายด้านระเบียบ

ให้มีการจัดตั้งคณะกรรมการจัดทำข้อกำหนดทางกฎหมายเทคโนโลยีสารสนเทศของกรมสนับสนุนบริการ เพื่อรวมข้อกำหนดที่มีผลทางกฎหมาย ด้านระเบียบ

- ระเบียบการใช้คอมพิวเตอร์
- ระเบียบการใช้ soft ware ที่ถูกต้องตามกฎหมาย
- การกำหนดสิทธิและการให้สิทธิในการเข้าถึงข้อมูล
- การป้องกันความปลอดภัยของข้อมูล และ ระบบต่างๆ อุปกรณ์ต่างๆ ทางด้านเทคโนโลยีสารสนเทศ
- การกำหนดแนวทางการใช้ข้อมูล
- การป้องกันข้อมูลส่วนตัว ฯลฯ

เพื่อจัดทำเป็นประกาศกรมสนับสนุนบริการสุขภาพ ทำเป็นนโยบายมาตรฐาน ความปลอดภัยมั่นคงของกรมฯ ให้เป็นแนวทางในการปฏิบัติเดียวกัน

๑๔.๑.๒. สิทธิในทรัพย์สินทางปัญญา (Intellectual property rights)

สิทธิในทรัพย์สินทางปัญญาและการใช้ผลิตภัณฑ์ที่มีกรรมสิทธิ์ต้องทำตามขั้นตอนกฎหมาย ข้อบังคับ และสัญญาจ้างเอกชน

๑๔.๑.๒.๑. มีขั้นตอนการปฏิบัติที่เหมาะสม เพื่อให้มั่นใจว่ามีความสอดคล้องกับความต้องการของกฎหมาย ระเบียบข้อบังคับ และสัญญาจ้าง ที่ว่าด้วยเรื่องสิทธิในทรัพย์สินทางปัญญาและการใช้ผลิตภัณฑ์ซอฟต์แวร์ที่มีกรรมสิทธิ

-มีสัญญาข้อตกลงระหว่างผู้ให้บริการกับผู้ใช้บริการอย่างชัดเจนในการใช้งานซอฟต์แวร์ที่มีลิขสิทธิ์

๑๔.๑.๓. การป้องกันข้อมูล (Protection of records)

หน่วยงานที่ทำสัญญาจ้างกับเอกชน ให้เอกชนอย่านำข้อมูลของกรมไปเผยแผ่ ทำหาย หรือทำลาย ปลอมแปลง โดยไม่ได้รับจากองค์ ให้เอกชนทำสัญญาจ้างและกฎหมาย ระเบียบข้อบังคับ

๑๔.๑.๓.๑. มีแนวทางปฏิบัติการป้องกันจากการสูญหาย การถูกทำลาย การปลอมแปลง การเข้าถึงโดยไม่ได้รับอนุญาต และการเผยแพร่โดยไม่ได้รับอนุญาต โดยสอดคล้องกับความต้องการของกฎหมาย ระเบียนข้อบังคับ สัญญาจ้าง และความต้องการทางธุรกิจ

-ในการเข้าออกห้องเก็บข้อมูลต้องมีระบบรักษาความปลอดภัยอย่างเข้มงวด

-มีการเก็บสำรองข้อมูลและกำหนดสิทธิการเข้าถึงข้อมูลด้วยusernameและpassword

๑๔.๑.๔. **ความเป็นส่วนตัวและการป้องกันข้อมูลส่วนบุคคล (Privacy and protection of personal** identifiable information)

๑๔.๑.๔.๑. มีการดำเนินการสอดคล้องกฎหมายและระเบียบข้อบังคับที่เกี่ยวข้อง เพื่อป้องกันข้อมูลส่วนบุคคลและความเป็นส่วนตัว

-ข้อมูลส่วนตัวต้องมีการเข้ารหัสหรือขออนุญาตจากเจ้าของเรื่อง ให้เป็นไปตามข้อบังคับ

-ข้อมูลที่เป็นส่วนบุคคล เจ้าของข้อมูลสามารถกำหนดวิธีการเข้ารหัสได้ด้วยตัวเอง

๑๔.๑.๕. ระเบียบข้อบังคับสำหรับมาตรการเข้ารหัสข้อมูล (Regulation of cryptographic controls)

มีมาตรการควบคุม ขั้นตอนการเข้าถึงฐานข้อมูลในแต่ละระดับชั้นความสำคัญ

๑๔.๑.๕.๑. มีการการตรวจประเมิน ให้คณะกรรมการจัดทำข้อกำหนด จัดทำมาตรฐานการตรวจสอบประเมินระบบสารสนเทศ

๑๔.๒. การทบทวนความมั่นคงปลอดภัยสารสนเทศ (Information security reviews)

๑๔.๒.๑. การทบทวนอย่างอิสระด้านความมั่นคงปลอดภัยสารสนเทศ (Independent review of information security)

-เมื่อมีการเปลี่ยนแปลงกรม คณะทำงานสามารถประชุมเพื่อทบทวนมาตรการ ขั้นตอนความมั่นคงปลอดภัยได้ตลอดเวลา

๑๔.๒.๑.๑. มีวิธีการในการบริหารจัดการความมั่งคงปลอดภัยสารสนเทศและการปฏิบัติของกรม ต้องมีการทบทวนอย่างอิสระตามรอบระยะเวลาที่กำหนดไว้ หรือมีการเปลี่ยนแปลงกรมที่มากเกิดขึ้น

๑๔.๒.๒. ความสอดคล้องกับนโยบายและมาตรฐานด้านความมั่นคงปลอดภัย (Compliance with security policies and standards)

-กำหนดให้ผู้ใช้มีขั้นตอนการปฏิบัติตามนโยบายและมาตรฐานความมั่นคงปลอดภัย

๑๔.๒.๒.๑. มีการดำเนินทบทวนความสอดคล้องอย่างสม่ำเสมอของการประมวลผลสารสนเทศและขั้นตอนปฏิบัติที่อยู่ภายใต้ความรับผิดชอบของตนเอง โดยเทียบกับนโยบาย มาตรฐานและความต้องการด้านความมั่นคงปลอดภัย

๑๔.๒.๓. การทบทวนความสอดคล้องทางเทคนิค (Technical compliance review)

-มีการดูแลบำรุงรักษาซอฟต์แวร์ ฮาร์ดแวร์ที่ใช้ในกรม ภายใต้กฎระเบียบข้อบังคับ ทุกๆ๓ เดือน

๑๔.๒.๓.๑. ระบบที่ใช้งานอยู่ต้องมีการทบทวนอย่างสม่ำเสมอ เพื่อพิจารณาความสอดคล้องกับนโยบายและมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศของกรม

หมวดที่ ๓

การแบ่งมอบหน้าที่ และ การดำเนินงานของหน่วยงานส่วนกลาง และ หน่วยงานส่วนภูมิภาค ของกรมสนับสนุนบริการสุขภาพ

เพื่อให้การดำเนินงานรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ กรมสนับสนุนบริการสุขภาพ เป็นไปตามนโยบาย และ หน่วยงานในสังกัดกรมสนับสนุนบริการสุขภาพ สามารถปฏิบัติได้อย่างถูกต้อง จึงให้ปฏิบัติดังนี้

ข้อ ๑ หัวหน้าส่วนราชการในส่วนกลาง และ ส่วนภูมิภาค สังกัดกรมสนับสนุนบริการสุขภาพ เป็นผู้มีหน้าที่ควบคุม กำกับ การดำเนินงานของเจ้าหน้าที่ที่เกี่ยวข้องกับธุรกรรมทางอิเล็กทรอนิกส์ ให้ปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

ข้อ ๒ การดำเนินงานตามมาตรฐาน ISO๒๗๐๐๑ ให้หน่วยงานต่างๆ ดำเนินการดังนี้

๒.๑ กลุ่มเทคโนโลยีสารสนเทศ สำนักบริหาร เป็นหัวหน้าเจ้าหน้าที่ในการกำกับ ติดตาม เสนอแนะ กำหนดแนวทางปฏิบัติเพื่อให้เป็นไปในนโยบายและ ปฏิบัติหน้าที่หัวหน้าสำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ กรมสนับสนุนบริการสุขภาพ

๒.๒ ให้กลุ่มเทคโนโลยีสารสนเทศ สำนักบริหาร ดำเนินการพัฒนาสมรรถนะบุคลากรด้าน ISO๒๗๐๐๑ ให้กับเจ้าหน้าที่ผู้มีหน้าที่เกี่ยวข้องในทุกหน่วยงาน และ การออกข้อกำหนดหลัก- ข้อกำหนดย่อย ให้เป็นภาระหน้าที่ของคณะกรรมการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ ที่กรมสนับสนุนบริการสุขภาพประกาศแต่งตั้ง ทั้งนี้กรรมการทุกตำแหน่งต้องมีความรู้ ความเข้าใจด้าน ISO๒๗๐๐๑ โดยความเห็นชอบของที่ปรึกษาคณะกรรมการฯ

๒.๓ ให้กลุ่มเทคโนโลยีสารสนเทศ สำนักบริหาร ดำเนินการจัดทำทะเบียนทรัพย์สินด้านเทคโนโลยีสารสนเทศทั้งหมดของกรมฯ และ หน่วยงานในสังกัดกรมฯ โดยทุกหน่วยงาน จัดเจ้าหน้าที่ร่วมให้ข้อมูลดำเนินการ

๒.๔ ให้หน่วยนำร่องดำเนินงานรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ ให้ผ่านการรับรองระดับผู้เชี่ยวชาญภายในปีงบประมาณ พ.ศ. ๒๕๕๘ และ ให้หน่วยงานต่างๆ ศึกษาเรียนรู้เพื่อให้ผ่านรับรองครบทุกหน่วยงานภายในปีงบประมาณ พ.ศ. ๒๕๖๐

๒.๕ บรรดากิจกรรมใดที่ยังไม่มีข้อกำหนดในทางปฏิบัติใดให้กลุ่มเทคโนโลยีสารสนเทศ สำนักบริหาร เป็นผู้ออกข้อกำหนด โดยความเห็นชอบของที่ปรึกษาคณะกรรมการฯ และ เสนอให้กรมสนับสนุนบริการสุขภาพประกาศใช้

ผู้เสนอ

.....

(นางชมบุญ โค้วสมจีน)

นักจัดการงานทั่วไปชำนาญการพิเศษ

รักษาราชการแทนผู้อำนวยการสำนักบริหาร

วันที่...../...../.....

ผู้ให้ความเห็นชอบ

.....

(นายธเรศ กรัษนัยรวิวงค์)

รองอธิบดีกรมสนับสนุนบริการสุขภาพ

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง

ประจำกรมสนับสนุนบริการสุขภาพ

วันที่...../...../.....

ผู้อนุมัติ

.....

(นาวาอากาศตรี บุญเรือง ไตรเรืองวรวัฒน์)

อธิบดีกรมสนับสนุนบริการสุขภาพ

วันที่...../...../.....