นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย ของระบบเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ (National Human Rights Commission of Thailand)

พ.ศ. ๒๕๕๗

ประกาศสำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร
สำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ

.....

ด้วยพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ ๒)พ.ศ. ๒๕๕๑ และพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ มาตรา ๕ กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานภาครัฐ หรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ และสำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติเป็นหน่วยงานที่มีการดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ที่จะต้องจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารด้วย

สำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติได้จัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อให้เป็นระบบที่มีความมั่นคงปลอดภัย ผู้เกี่ยวข้องเกิดความเชื่อมั่นในการใช้งาน โดยได้กำหนดแนวทางปฏิบัติให้ผู้บริหาร เจ้าหน้าที่ผู้ดูแลระบบและผู้ใช้งานระบบ ถือปฏิบัติ และให้มีการทบทวนปรับปรุงนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ ให้เป็นปัจจุบันอยู่เสมอ

ดังนั้น เพื่อให้นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ บรรลุวัตถุประสงค์ตามที่กำหนดไว้ จึงให้ส่วนต่างๆ ในสังกัดสำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ นำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร ไปใช้เป็นแนวทางในการปฏิบัติงานและถือปฏิบัติอย่างเคร่งครัดต่อไป รายละเอียดตามเอกสารแนบท้าย

จึงประกาศให้ทราบโดยทั่วกัน

ประกาศ ณ วันที่ ๑๐ กันยายน พ.ศ. ๒๕๕๗

(นายชาติชาย สุทธิกลม)
เลขาธิการคณะกรรมการสิทธิมนุษยชนแห่งชาติ

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย ของระบบเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ (National Human Rights Commission of Thailand)

พ.ศ. ๒๕๕๗

สารบัญ

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย ระบบเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ

๑. หลักการและเหตุผล

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ มาตรา ๕ กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเพื่อให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ หรือต่อไปนี้เรียกว่า “สำนักงาน กสม.” เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่าง ๆ สำนักงาน กสม. จึงเห็นสมควรกำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร ให้เป็นเครื่องมือในการปฏิบัติงานและบริหารจัดการให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและป้องกันภัยคุกคามต่างๆ

๒. วัตถุประสงค์

๒.๑ เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารและเครือข่ายคอมพิวเตอร์ของสำนักงาน กสม. ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล

๒.๒ เพื่อกำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร ซึ่งอ้างอิงตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ ของกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

๒.๓ เพื่อกำหนดมาตรฐาน แนวปฏิบัติและวิธีปฏิบัติ ให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับสำนักงาน กสม. ได้ถือปฏิบัติและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงาน กสม.

๒.๔ เน้นกำกับดูแลการดำเนินงานเพื่อบริหารจัดการให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารมีความถูกต้องสมบูรณ์พร้อมใช้งานอยู่เสมอและติดตามตรวจสอบการดำเนินงานปรับปรุงแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้สอดคล้องตามการเปลี่ยนแปลงของเทคโนโลยี

๓. นโยบายในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร

๓.๑ ส่งเสริมและสนับสนุนการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้ตอบสนองต่อพันธกิจและนโยบายขององค์กร

๓.๒. มุ่งกำหนดแนวปฏิบัติ แนวทางแก้ไขหรือบทลงโทษตามความเหมาะสมหากมีการละเมิดหรือฝ่าฝืนนโยบายในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารรวมทั้งติดตามและตรวจสอบการดำเนินงานอย่างสม่ำเสมอเพื่อให้เป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

๓.๓. เน้นกำกับดูแลการดำเนินงานเพื่อบริหารจัดการให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารมีความถูกต้องสมบูรณ์และพร้อมใช้งานอยู่เสมอ

๓.๔. เผยแพร่ความรู้ความเข้าใจเพื่อสร้างความตระหนักให้บุคลากรที่เกี่ยวข้องทั้งของหน่วยงานเองและของหน่วยงานที่เกี่ยวข้องตลอดจนส่งเสริมให้มีการศึกษาอย่างต่อเนื่อง

๓.๕. ติดตาม ตรวจสอบการดำเนินงานและปรับปรุงแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารให้สอดคล้องตามการเปลี่ยนแปลงของเทคโนโลยี

๔. แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร

สำนักงาน กสม. กำหนดขั้นตอนและกระบวนการที่เหมาะสมตามหลักมาตรฐานสากล สำหรับใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยคำนึงถึงความถูกต้อง ครบถ้วน น่าเชื่อถือ เพื่อจะช่วยให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารมีสภาพพร้อมใช้งานและมีความปลอดภัย ลดความเสียหายต่อการดำเนินงาน ทรัพย์สิน บุคลากรของสำนักงาน กสม.จัดเป็นมาตรฐานด้านความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงาน กสม. ซึ่งเจ้าหน้าที่ของสำนักงาน กสม. และหน่วยงานภายนอกที่เข้ามาใช้ระบบจะต้องปฏิบัติตามอย่างเคร่งครัด

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงาน กสม. ประกอบด้วยส่วนต่าง ๆ ดังนี้

นิยาม

ส่วนที่ ๑ นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

ส่วนที่ ๒ นโยบายและแนวปฏิบัติในการควบคุมการเข้าถึงและการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร

ส่วนที่ ๓ นโยบายและแนวปฏิบัติในการสำรองและตรวจสอบประเมินความเสี่ยงระบบเทคโนโลยีสารสนเทศและการสื่อสาร

ส่วนที่ ๔ นโยบายและแนวปฏิบัติในการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร

คำนิยาม

คำนิยามที่ใช้ในนโยบายและแนวปฏิบัตินี้ ประกอบด้วย

- **สำนักงาน กสม.** หมายถึง สำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ
- **ผู้บังคับบัญชา** หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของสำนักงาน กสม.
- **ศทส.** หมายถึง ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เป็นหน่วยงานที่ให้บริการด้านเทคโนโลยีสารสนเทศและการสื่อสาร ให้คำปรึกษา พัฒนาปรับปรุง บำรุงรักษา ระบบคอมพิวเตอร์และเครือข่ายภายในสำนักงาน กสม.
- **ผู้อำนวยการ ศทส.** หมายถึง ผู้ได้รับมอบหมายให้กำกับ ดูแล และบริหารจัดการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารของสำนักงาน กสม. ซึ่งมีบทบาทหน้าที่และความรับผิดชอบในส่วนของการกำหนดนโยบาย มาตรฐาน การควบคุมดูแลการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารและการสื่อสาร
- **การรักษาความมั่นคงปลอดภัย** หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงาน กสม.
- **แนวปฏิบัติ (Guideline)** หมายถึง แนวทางที่ไม่ได้บังคับให้ปฏิบัติ แต่แนะนำให้ปฏิบัติตามเพื่อให้สามารถบรรลุเป้าหมายได้ง่ายขึ้น
- **ผู้ใช้งาน (User)** หมายถึง บุคคลที่ใช้เครื่องคอมพิวเตอร์ในการเข้าระบบงานหรือเครือข่ายอินเตอร์เน็ตของสำนักงาน กสม. แบ่งได้ดังนี้
  - บุคลากรที่ปฏิบัติงานประจำของสำนักงาน กสม .ประกอบด้วย ผู้บริหารของสำนักงาน กสม.ข้าราชการ พนักงานราชการ
  - บุคลากรที่ปฏิบัติงานตามระยะเวลา เช่น พนักงานจ้างเหมา ลูกจ้างผู้ช่วยปฏิบัติงาน คณะอนุกรรมการต่าง ๆ
  - บุคคลากรที่ไม่เป็นไปตามข้อ ๑ และข้อ ๒ เช่น ผู้เข้าร่วมประชุม ผู้เข้าร่วมสัมมนา เจ้าหน้าที่เทคนิคของผู้รับจ้างเจ้าหน้าที่ตามสัญญาจ้างและเจ้าหน้าที่ตามโครงการต่าง ๆ ของสำนักงาน กสม.
- **สิทธิของผู้ใช้งาน** หมายถึง สิทธิของผู้ใช้งานในการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงาน กสม. ซึ่งกำหนดไว้ ดังนี้
  - สิทธิทั่วไป หมายถึงสิทธิของผู้ใช้งาน (User) ที่สามารถใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารได้
  - สิทธิจำเพาะ หมายถึง สิทธิของผู้ใช้งาน (User) ที่สามารถนำเข้าข้อมูลและแก้ไขข้อมูลในระบบเฉพาะส่วนที่ตนเองได้รับมอบหมายเท่านั้น
  - สิทธิพิเศษหมายถึง สิทธิสูงสุดของผู้ดูแลระบบ (Root) สามารถเข้าถึงข้อมูลในระบบได้ทั้งหมด

- **ผู้ดูแลระบบ (Administrator)** หมายถึง ผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบดูแลระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยแบ่งเป็น ๒ ส่วน คือ
  - ผู้ดูแลระบบฐานข้อมูล (Database Administrator) หมายถึง ผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่ดูแลรักษาหรือจัดการระบบฐานข้อมูล
  - ผู้ดูแลระบบคอมพิวเตอร์แม่ข่ายและระบบเครือข่าย (System Administrator and Network Administrator) หมายถึง ผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่ดูแลรักษาหรือจัดการระบบคอมพิวเตอร์แม่ข่ายและระบบเครือข่าย
- **หน่วยงานภายนอก** หมายถึง องค์กรหรือหน่วยงานภายนอกที่ได้รับอนุญาตให้มีสิทธิในการเข้าถึงและใช้งานข้อมูลหรือสินทรัพย์ต่าง ๆ ของหน่วยงาน โดยจะได้รับสิทธิในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล
- **ข้อมูลคอมพิวเตอร์** หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึง ข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์
- **สารสนเทศ (Information)** หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ ได้
- **โปรแกรม (Program)** หมายถึง ชุดคำสั่งที่ใช้ในการควบคุมเครื่องอิเล็กทรอนิกส์หรือโปรแกรมคอมพิวเตอร์ที่มีชุดคำสั่งสำเร็จรูปรอการใช้งาน
- **ระบบคอมพิวเตอร์** หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันโดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ
- **ระบบเครือข่าย (Network System)** หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศและการสื่อสารต่าง ๆ ของสำนักงาน กสม. ได้ เช่น ระบบ LAN ระบบ Intranet ระบบ Internet เป็นต้น
- **ระบบอินเทอร์เน็ต (Internet)** หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่าง ๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตทั่วโลก
- **ระบบเทคโนโลยีสารสนเทศและการสื่อสาร** หมายถึง ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูล และสารสนเทศ เป็นต้น

- **เว็บเบราว์เซอร์ (Web Browser)** หมายถึงโปรแกรมสืบค้นข้อมูลทางอินเตอร์เน็ต เช่น Internet Explorer, Mozilla Firefox, Google Chrome เป็นต้น
- **พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร (Information System Workspace)** หมายถึง พื้นที่ที่หน่วยงานอนุญาตให้มีการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยแบ่งเป็น
  - พื้นที่ทำงานทั่วไป (General working area) หมายถึง พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคล และคอมพิวเตอร์พกพาที่ประจำโต๊ะทำงาน
  - พื้นที่ห้องควบคุมระบบเทคโนโลยีสารสนเทศและการสื่อสาร (Server room) หมายถึง พื้นที่ที่ติดตั้งและจัดเก็บอุปกรณ์ระบบเทคโนโลยีสารสนเทศและระบบเครือข่าย
  - พื้นที่ใช้งานระบบเครือข่ายไร้สาย (Wireless LAN coverage area) หมายถึง พื้นที่ในการให้บริการระบบเครือข่ายไร้สาย
- **เจ้าของข้อมูล** หมายถึง ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงานโดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น ๆ หรือ ได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย
- **สินทรัพย์** หมายถึง ข้อมูล ระบบข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศของหน่วยงาน เช่น อุปกรณ์ระบบเครือข่าย ซอฟท์แวร์ที่มีลิขสิทธิ์ เครื่องคอมพิวเตอร์ของสำนักงานฯ เป็นต้น รวมถึง อุปกรณ์คอมพิวเตอร์ที่มีเลขครุภัณฑ์ทุกรายการ
- **การเข้าถึงหรือควบคุมการใช้งานระบบเทคโนโลยีสารสนเทศ** หมายถึง การอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งานเข้าถึง หรือใช้งานเครือข่ายหรือระบบเทคโนโลยีสารสนเทศและการสื่อสาร ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตสำหรับบุคคลภายนอก
- **ความมั่นคงปลอดภัยด้านสารสนเทศ** หมายถึง การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของสารสนเทศ ทั้งนี้ รวมถึงคุณสมบัติในด้านความถูกต้องแท้จริง (authenticity) ความรับผิด (accountability) การห้ามปฏิเสธความรับผิด (non-repudiation) และความน่าเชื่อถือ (reliability)
- **จดหมายอิเล็กทรอนิกส์ (E-mail)** หมายถึง ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ มาตรฐานที่ใช้ในการรับส่งข้อมูลชนิดนี้ ได้แก่ SMTP, POP๓ และ IMAP เป็นต้น
- **ชื่อผู้ใช้ (Username)** หมายถึง ชุดของตัวอักษรหรือตัวเลขที่ถูกกำหนดขึ้นเพื่อใช้ในการลงบันทึกเข้า (Login) เพื่อใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายที่มีการกำหนดสิทธิ์การใช้งานไว้

- **รหัสผ่าน (Password)** หมายถึง ชุดของตัวอักษรหรืออักขระหรือตัวเลขที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศและการสื่อสาร
- **ลงบันทึกเข้า (Login)** หมายถึง กระบวนการที่ผู้ใช้บริการต้องทำให้เสร็จสิ้นตามเงื่อนไขที่ตั้งไว้ เพื่อเข้าใช้งานระบบคอมพิวเตอร์และระบบเครือข่ายซึ่งปกติแล้วจะอยู่ในรูปแบบของการกรอกชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ให้ถูกต้อง
- **ลงบันทึกออก (Logout)** หมายถึง กระบวนการที่ผู้ใช้บริการทำเพื่อสิ้นสุดการใช้งานระบบคอมพิวเตอร์และระบบเครือข่าย
- **ปรับปรุงข้อมูล (Update)** หมายถึง ปรับให้เป็นปัจจุบันการปรับปรุงข้อมูลด้านต่าง ๆ ของระบบเทคโนโลยีสารสนเทศและการสื่อสารให้ทันสมัยอยู่เสมอ
- **โปรแกรมประสงค์ร้าย (Malware)** หมายถึง โปรแกรมคอมพิวเตอร์ชุดคำสั่งและ/หรือข้อมูลอิเล็กทรอนิกส์ที่ได้รับการออกแบบขึ้นมาโดยมีวัตถุประสงค์เพื่อก่อกวนหรือสร้างความเสียหายไม่ว่าโดยตรงหรือโดยอ้อมแก่ระบบคอมพิวเตอร์หรือระบบเครือข่าย เช่น ไวรัสคอมพิวเตอร์ (Computer Virus) หรือสปายแวร์ (Spyware) หรือหนอน (Worm) หรือม้าโทรจัน (Trojan horse) หรือฟิชชิง (Phishing) หรือจดหมายลูกโซ่ (Mass Mailing) เป็นต้น
- **สื่อบันทึกพกพา** หมายถึง สื่ออิเล็กทรอนิกส์ที่ใช้ในการบันทึกหรือจัดเก็บข้อมูลได้แก่ Flash Drive หรือ Handy Drive หรือ Thumb Drive หรือ External Hard disk หรือ Floppy disk เป็นต้น
- **การตั้งค่าระบบ (Configuration)** หมายถึง การกำหนดค่าที่ใช้งานของโปรแกรมหรือองค์ประกอบของเครื่องคอมพิวเตอร์ ทั้งทางด้านฮาร์ดแวร์และซอฟต์แวร์
- **เลขที่อยู่ไอพี (IP Address)** หมายถึง ตัวเลขประจำเครื่องคอมพิวเตอร์ที่ต่ออยู่ในระบบเครือข่ายซึ่งเลขนี้ของแต่ละเครื่องจะต้องไม่ซ้ำกันโดยประกอบด้วยชุดของตัวเลข ๔ ส่วนสำหรับ IPv๔ หรือ ๖ ส่วนสำหรับ IPv๖ ที่คั่นด้วยเครื่องหมายจุด (.)
- **อุปกรณ์กระจายสัญญาณ (Access Point)** หมายถึง อุปกรณ์ที่ทำหน้าที่กระจายสัญญาณในเครือข่ายไร้สาย
- **ค่าเริ่มต้น (Default)** หมายถึง ค่าที่เครื่องคอมพิวเตอร์หรือโปรแกรมได้กำหนดไว้ล่วงหน้าและนำไปใช้ได้โดยปริยายหากไม่มีการเปลี่ยนแปลงจากผู้ใช้บริการ
- **WPA (Wi-Fi Protected Access)** หมายถึง ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สายที่พัฒนาขึ้นมาใหม่ให้มีความปลอดภัยมากกว่าวิธีเดิมอย่าง WEP (Wired Equivalent Privacy)
- **ไฟร์วอลล์ (Firewall)** หมายถึง เทคโนโลยีป้องกันการบุกรุกจากบุคคลภายนอกเพื่อไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้ามาใช้ข้อมูลและทรัพยากรในเครือข่าย โดยอาจใช้ทั้งฮาร์ดแวร์และซอฟต์แวร์ในการรักษาความปลอดภัย

- **VPN (Virtual Private Network)** หมายถึง เครือข่ายคอมพิวเตอร์เสมือนที่สร้างขึ้นมาเป็นของส่วนตัว โดยในการรับส่งข้อมูลจริงจะทำโดยการเข้ารหัสเฉพาะแล้วรับ-ส่งผ่านเครือข่ายอินเทอร์เน็ตทำให้บุคคลอื่นไม่สามารถอ่านได้และมองไม่เห็นข้อมูลนั้นไปจนถึงปลายทาง
- **Web Server** หมายถึง เครื่องคอมพิวเตอร์ที่ติดตั้งโปรแกรมบริการเว็บและมีหน้าที่ให้บริการเว็บเพจต่าง ๆ
- **การพิสูจน์ยืนยันตัวตน (Authentication)** หมายถึง ขั้นตอนการรักษาความปลอดภัยในการเข้าใช้ระบบเป็นขั้นตอนในการพิสูจน์ตัวตนของผู้ใช้บริการระบบทั่วไป จะเป็นการพิสูจน์โดยใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password)
- **แผนผังระบบเครือข่าย (Network Diagram)** หมายถึง แผนผังซึ่งแสดงถึงการเชื่อมต่อของระบบเครือข่ายของหน่วยงาน
- **Command Line** หมายถึง บรรทัดที่ให้ผู้ใช้งานป้อนคำสั่งแบบข้อความเพื่อสั่งให้เครื่องคอมพิวเตอร์ทำงานตามต้องการ
- **Firewall Log** หมายถึง การบันทึกการสื่อสารทั้งหมดที่เกิดขึ้นไม่ว่าไฟร์วอลล์ (Firewall) จะอนุญาตให้เกิดการสื่อสารนั้นได้หรือไม่ก็ตามซึ่งสามารถนำมาใช้ในการวิเคราะห์เพื่อตรวจสอบประเภทของการสื่อสาร ปริมาณการสื่อสารนอกจากนั้นแล้วยังอาจจะสะท้อนให้เห็นจำนวนครั้งที่พยายามจะบุกรุกเข้ามาภายในหน่วยงาน
- **ข้อมูลจราจรทางคอมพิวเตอร์ (Log)** หมายถึง ข้อมูลที่เกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ซึ่งแสดงถึงแหล่งกำเนิดต้นทางปลายทางเส้นทางวันที่ปริมาณระยะเวลาและชนิดของบริการอื่นๆ ที่เกี่ยวข้องในการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น
- **เครือข่ายสังคมออนไลน์ (Social Network)** หมายถึง สังคมการติดต่อสื่อสารผ่านระบบเครือข่ายอิเล็กทรอนิกส์เช่น Facebook, Hi๕, Tagged, MySpace, Orkut, Vkontakte.ru, Friendster, Line, Instagram,Webboard Blog, กระดานข่าวหรือเว็บไซต์อื่นๆที่มีลักษณะการให้บริการใกล้เคียงกัน
- **ข้อมูลส่วนบุคคล** หมายถึง ข้อมูลส่วนตัวหรือส่วนของข้อมูลที่แสดงความเป็นตัวคุณ ไม่ว่าโดยตรงหรือโดยอ้อมเช่น ชื่อ- นามสกุล อายุ เพศ ที่อยู่ หรือ อีเมล์แอดเดรส และรายละเอียดการติดต่ออื่นๆ อาทิสถานที่ทำงาน และที่อยู่เป็นต้น

ส่วนที่ ๑
นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย ทางด้านกายภาพและสิ่งแวดล้อม

๑.๑ นโยบายการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Security)

วัตถุประสงค์ เพื่อกำหนดเป็นมาตรการในการควบคุมและป้องกันเพื่อการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงอาคาร สถานที่ และพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยพิจารณาตามความสำคัญของอุปกรณ์ระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้ง ข้อมูล ซึ่งเป็นทรัพย์สินที่มีค่าและอาจจำเป็นต้องรักษาความลับ โดยมาตรการนี้จะมีผลบังคับใช้กับผู้ใช้งาน (User) ทุกประเภท รวมทั้งหน่วยงานภายนอก ซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงาน กสม.

๑.๒ แนวปฏิบัติ

๑.๒.๑ การเข้าถึงพื้นที่ทำงานทั่วไปของสำนักงาน กสม.

๑) สำนักงาน กสม. จัดให้มีเวรยาม รักษาอาคาร เพื่อป้องกันและตรวจสอบการเข้าสู่พื้นที่ของสำนักงาน กสม.

๒) บุคลากรที่ปฏิบัติงานในสำนักงาน กสม. จะต้องมีบัตรประจำตัวเพื่อผ่านเข้าออกในพื้นที่ของสำนักงาน กสม.

๓) บุคคลภายนอกหรือผู้มาติดต่อ ที่ต้องการเข้ามาภายในพื้นที่ทำงานทั่วไปของสำนักงาน กสม. จะต้องให้มีการแลกบัตรกับเจ้าหน้าที่รักษาความปลอดภัย และให้ผู้ติดต่อติดบัตรผู้ติดต่อ (Visitor) ตลอดเวลาที่อยู่ในสำนักงาน กสม.

๑.๒.๒ การเข้าถึงพื้นที่ห้องควบคุมระบบเทคโนโลยีสารสนเทศและการสื่อสาร (Server room)

กำหนดให้ ศทส. เป็นผู้รับผิดชอบดูแลพื้นที่ห้องควบคุมระบบเทคโนโลยีสารสนเทศและการสื่อสาร (Server room) มีหน้าที่ดังนี้

๑) กำหนดสิทธิให้กับเจ้าหน้าที่ให้สามารถมีสิทธิในการเข้าถึงพื้นที่ห้องควบคุมระบบเทคโนโลยีสารสนเทศและการสื่อสาร (Server room) เพื่อปฏิบัติหน้าที่ตามที่ได้รับมอบหมายอย่างครบถ้วน พร้อมจัดทำ “ทะเบียนผู้มีสิทธิเข้าออกพื้นที่” เพื่อใช้งานพื้นที่ห้องควบคุมระบบเทคโนโลยีสารสนเทศและการสื่อสาร (Server room)

๒) ทำการบันทึกเวลาการเข้าออกพื้นที่ใช้งานและกำหนดผู้มีหน้าที่รับผิดชอบการบันทึกการเข้าออกดังกล่าว โดยจัดทำเป็นเอกสาร “บันทึกการเข้าออกพื้นที่ห้องควบคุมระบบเทคโนโลยีสารสนเทศและการสื่อสาร (Server room) ของบุคคลภายนอก”

๓) จัดให้มีเจ้าหน้าที่ทำหน้าที่ตรวจสอบประวัติการเข้าออกพื้นที่ห้องควบคุมระบบเทคโนโลยีสารสนเทศและการสื่อสาร (Server room) และให้มีการปรับปรุงรายการผู้มีสิทธิถือบัตรเข้าออกพื้นที่ห้องควบคุมระบบเทคโนโลยีสารสนเทศและการสื่อสาร (Server room) อย่างน้อยปีละ ๑ ครั้ง

๔) กำหนดมาตรการควบคุมการเข้า-ออกพื้นที่ห้องควบคุมระบบเทคโนโลยีสารสนเทศและการสื่อสาร (Server room) และติดประกาศให้ทราบบริเวณหน้าห้องควบคุมระบบเทคโนโลยีสารสนเทศและการสื่อสาร (Server room)

๕) ควบคุมดูแลหน่วยงานภายนอกที่นำเครื่องคอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานระบบเครือข่าย มาใช้ภายในห้องควบคุมระบบเทคโนโลยีสารสนเทศและการสื่อสาร (Server room) โดยจะต้องลงบันทึกในแบบฟอร์มการขออนุญาตใช้งานเครื่องคอมพิวเตอร์หรืออุปกรณ์

๖) ให้มีระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน ประกอบด้วย ระบบเครื่องปรับอากาศแบบควบความชื้น ระบบสำรองไฟฟ้าอัตโนมัติ ระบบดับเพลิงอัตโนมัติด้วยก๊าซ HFC ระบบตรวจจับการรั่วซึมของน้ำ และอื่น ๆ ที่จำเป็น โดยต้องให้มีการตรวจสอบหรือทดสอบระบบสนับสนุนเหล่านั้นอย่างสม่ำเสมอให้มั่นใจได้ว่า ระบบทำงานตามปกติ และลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ พร้อมทั้งการดูแลให้สามารถใช้งานได้

๗) ให้มีระบบแจ้งเตือนเพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงานภายในห้องควบคุมระบบเทคโนโลยีสารสนเทศและการสื่อสาร (Server room) ทำงานผิดปกติหรือหยุดการทำงาน

๑.๒.๓ การนำสินทรัพย์ของสำนักงาน กสม. ออกนอกสำนักงาน กสม. (removal of property)

ให้ผู้อำนวยการสำนัก/กลุ่มงาน มีหน้าที่ดูแลรักษาการนำสินทรัพย์ของสำนักงาน กสม. กำหนดแนวปฏิบัติ ดังนี้

๑) ให้รับผิดชอบในการนำหรือเคลื่อนย้ายสินทรัพย์ในหน่วยงานของตนออกไปใช้งานนอกสำนักงานฯ

๒) ควรกำหนดระยะเวลาของการนำสินทรัพย์ออกไปใช้งานนอกสำนักงาน กสม.

๓) เมื่อมีการนำอุปกรณ์ส่งคืน ควรตรวจสอบว่าสอดคล้องกับระยะเวลาที่อนุญาต และตรวจสอบการชำรุดเสียหายของสินทรัพย์ด้วย

๔) ควรบันทึกข้อมูลการนำอุปกรณ์ของสำนักงาน กสม. ออกไปใช้งานนอกสำนักงาน กสม. เพื่อเอาไว้เป็นหลักฐานป้องกันการสูญหาย รวมทั้งบันทึกข้อมูลเมื่อนำอุปกรณ์มาส่งคืน

๕) เมื่อเครื่องคอมพิวเตอร์หมดอายุการใช้งานหรือเครื่องคอมพิวเตอร์ที่จะตัดจำหน่าย ต้องทำการลบทำลายข้อมูลการทำงานทั้งหมดในเครื่องออกไปและแจ้งให้ ศทส. ทราบ เพื่อตรวจสอบและล้างข้อมูลในเครื่องคอมพิวเตอร์ต่อไป

ส่วนที่ ๒
นโยบายและแนวปฏิบัติในการควบคุมการเข้าถึงและการใช้งาน ระบบเทคโนโลยีสารสนเทศและการสื่อสาร
(Access Control)

๒.๑ นโยบายการควบคุมการเข้าถึงและการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร

วัตถุประสงค์ เพื่อกำหนดเป็นมาตรการในการควบคุมและป้องกันเพื่อให้เกิดความปลอดภัยต่อระบบเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงาน กสม. โดยกำหนดแนวปฏิบัติสำหรับผู้เกี่ยวข้องเพื่อการควบคุมการเข้าถึง การบริหารจัดการการเข้าถึงระบบเทคโนโลยีสารสนเทศ ระบบเครือข่าย ระบบเครือข่ายไร้สาย เครื่องคอมพิวเตอร์แม่ข่าย การใช้งานระบบปฏิบัติการ การใช้งานอินเตอร์เน็ต การใช้งานระบบจดหมายอิเล็กทรอนิกส์ การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล เพื่อป้องกันการบุกรุกผ่านระบบเครือข่ายหรือจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ ที่จะสร้างความเสียหายแก่ข้อมูลหรือการทำงานของระบบเทคโนโลยีสารสนเทศและการสื่อสาร ให้หยุดชะงัก รวมทั้งให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงาน กสม. ได้อย่างถูกต้อง ครอบคลุมผู้ใช้งานที่ใช้งานขณะอยู่ภายในสำนักงาน และผู้ใช้งานที่ขอใช้งานขณะที่อยู่ภายนอกสำนักงาน

๒.๒ แนวปฏิบัติ

๒.๒.๑ การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร

ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมาย กำหนดแนวปฏิบัติที่ต้องดำเนินการ ดังนี้

๑) กำหนดกลุ่มผู้ใช้งานและสิทธิการเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอจัดทำบัญชีผู้ได้รับสิทธิใช้งานและมีการปรับปรุงข้อมูลให้มีความเป็นปัจจุบันอย่างสม่ำเสมอทั้งนี้ ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายเท่านั้นที่สามารถแก้ไขเปลี่ยนแปลงสิทธิการเข้าถึงข้อมูลและระบบข้อมูลได้

๒) ควรจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารชองสำนักงาน กสม. และตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบข้อมูลสำคัญ

๓) จัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบจากบุคคลภายนอก การเปิดสิทธิการใช้งานระบบต่าง ๆ ให้บุคคลภายนอก (เช่น การรีโมทระยะไกล การเพิ่มรายชื่อผู้ใช้งานที่เป็นบุคคลภายนอกชั่วคราว เป็นต้น) รวมทั้งการผ่านเข้าออกพื้นที่ห้องควบคุมระบบเทคโนโลยีสารสนเทศและการสื่อสาร (Server room) ของบุคคลภายนอกเพื่อเป็นหลักฐานในการตรวจสอบ

๒.๒.๒ การบริหารจัดการการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร

๒.๒.๒.๑ ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมาย ต้องปฏิบัติดังนี้

๑) ต้องลงทะเบียนการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารให้กับเจ้าหน้าที่ที่ปฏิบัติงานในสำนักงาน กสม. ทุกคน

๒) การลงทะเบียนเจ้าหน้าที่ใหม่ ให้เจ้าหน้าที่ใหม่กรอกแบบฟอร์ม “การขอรหัสผ่านในการเข้าใช้งานระบบต่าง ๆ” เพื่อให้มีสิทธิต่าง ๆ ในการใช้งานตามความจำเป็น และจัดเก็บไว้เป็นหลักฐาน

๓) อนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่จำเป็นต้องรู้ตามหน้าที่งานเท่านั้น โดยควรกำหนดสิทธิในการเข้าถึงระบบงานต้องกำหนดตามความจำเป็นขั้นต่ำเท่านั้น เนื่องจาก การให้สิทธิเกินความจำเป็นในการใช้งาน จะนำไปสู่ความเสี่ยงในการใช้งานเกินอำนาจหน้าที่

๔) ให้ยกเลิกเพิกถอนการอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารสำหรับผู้ใช้งานทั่วไป เมื่อบุคลากรไม่มีความจำเป็นต้องใช้งานระบบต่าง ๆ ที่กำหนดให้เดิมแล้ว เช่น ลาออกไป หรือเปลี่ยนตำแหน่งงาน เป็นต้น ทั้งนี้ ให้สำนักบริหารกลางและสำนัก/กลุ่มงานที่บุคลากรสังกัด แจ้งผู้ดูแลระบบทราบโดยเร็วที่สุด เพื่อทำการยกเลิกสิทธิการใช้งานต่อไป

๕) ให้คำแนะนำที่ถูกต้องเบื้องต้นในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารต่อผู้ใช้งานเกี่ยวกับระบบและโปรแกรมที่ไม่พึงประสงค์หรือมีความเสี่ยงที่จะเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงาน กสม.

๖) แจ้งตักเตือนผู้ใช้งานในกรณีมีการใช้งานที่ก่อให้เกิดความเสี่ยงที่จะเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศและการสื่อสารขึ้น และหากยังไม่ปรับปรุงแก้ไข ให้เสนอผู้บริหารพิจารณาต่อไป

๗) ต้องบริหารจัดการการเข้าถึงข้อมูลที่เป็นความลับของสำนักงาน กสม. ดังนี้

- ต้องกำหนดสิทธิ์ในการเข้าถึงข้อมูลที่เป็นความลับของสำนักงาน กสม. ประกอบด้วย ข้อมูลส่วนบุคคล ข้อมูลทางการเงินและบัญชี รหัสผ่านการเข้าใช้งานระบบ ข้อมูลเรื่องร้องเรียน ข้อมูลภาคีเครือข่าย สิทธิมนุษยชนประเภทบุคคล

- ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

- ต้องกำหนดรายชื่อผู้ใช้งาน (User Account) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับข้อมูล รวมทั้งกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

- ควรกำหนดมาตรการให้สำนัก/กลุ่มงานต่างๆ ทบทวนความเหมาะสมของสิทธิในการเข้าถึงข้อมูลของผู้ใช้งานอย่างน้อยปีละ ๑ ครั้งและแจ้งให้ ศทส. ทราบ เพื่อให้มั่นใจได้ว่าสิทธินั้น ๆ ยังคงมีความเหมาะสม

- ควรกำหนดมาตรการรักษาความปลอดภัยของข้อมูล ในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่เพื่อไปตรวจซ่อม โดยควรทำการสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน หรือถอดสื่อบันทึกข้อมูลออกก่อนนำไปส่งซ่อม

๒.๒.๒.๒ ผู้ใช้งาน ต้องปฏิบัติดังนี้

๑) ต้องใช้รหัสผ่าน (password) ในการเข้าใช้งานเพื่อให้เกิดความปลอดภัย

๒) กำหนดรหัสผ่านให้มีความปลอดภัย โดยรหัสผ่านที่ดี ควรมีความยาวไม่น้อยกว่า ๘ ตัวอักษร โดยมีการผสมผสานกันระหว่างตัวอักษรที่เป็นตัวพิมพ์เล็ก ตัวพิมพ์ใหญ่ ตัวเลข และสัญลักษณ์เข้าด้วยกัน รวมถึง ไม่กำหนดรหัสผ่านจากคำศัพท์ที่ปรากฏในพจนานุกรม จากชื่อหรือนามสกุลผู้ใช้งาน จากหมายเลขโทรศัพท์

๓) ควรเก็บรักษารหัสผ่านของตนเองให้มีความมั่นคงปลอดภัย รหัสผ่านถือเป็นข้อมูลลับ ห้ามให้ผู้อื่นยืมใช้รหัสผ่าน กรณีที่มีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่นเพื่อให้สามารถปฏิบัติงานแทนตนเองได้ หลังจากที่ทำงานนั้นเสร็จเรียบร้อยแล้ว ควรทำการเปลี่ยนรหัสผ่านโดยทันที

๔) ไม่ควรบันทึกรหัสผ่านไว้ในโปรแกรมคอมพิวเตอร์เพื่อช่วยในการจำรหัสผ่านของตน (เช่น ในโปรแกรมเว็บบราวเซอร์จะสามารถเลือกให้โปรแกรมช่วยจำรหัสผ่านไว้ให้)

๕) ต้องไม่จดหรือบันทึกรหัสผ่านไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นโดยบุคคลอื่น

๖) ควรเปลี่ยนรหัสผ่านอย่างน้อยทุก ๖ เดือน เพื่อความปลอดภัย

๗) กรณีที่ผู้ใช้งานเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน ควรทำการ logout ทันที

๘) ให้แจ้งต่อผู้ดูแลระบบและทำการเปลี่ยนรหัสผ่านโดยทันที หากผู้ใช้งานสงสัยว่าบัญชีผู้ใช้งานหรือรหัสผ่านของตนถูกละเมิด

๒.๒.๒.๓ ผู้บริหารระดับสำนัก/กลุ่มงาน ต้องปฏิบัติดังนี้

๑) แจ้งชื่อผู้ลาออกหรือเปลี่ยนตำแหน่งข้าราชการต่อผู้ดูแลระบบทราบโดยเร็ว เพื่อทำการยกเลิก/เพิ่มสิทธิการใช้งานระบบงานต่อไป

๒) ทบทวนความเหมาะสมของสิทธิในการเข้าถึงข้อมูลของผู้ใช้งานอย่างน้อยปีละ ๑ ครั้งและแจ้งให้ ศทส. ทราบ เพื่อให้มั่นใจได้ว่าสิทธินั้นๆ ยังคงมีความเหมาะสม โดยเฉพาะข้อมูลที่เป็นความลับ

๒.๒.๓ การควบคุมการเข้าถึงระบบเครือข่าย

๒.๒.๓.๑ ศทส. ต้องดำเนินการดังนี้

๑) กำหนดบุคคลที่รับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่า parameter ต่าง ๆ ของระบบเครือข่ายและอุปกรณ์ต่าง ๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจน และควรมีการทบทวนการกำหนดค่า parameter ต่าง ๆ อย่างน้อยปีละครั้ง นอกจากนี้ การกำหนดแก้ไขหรือเปลี่ยนแปลงค่า parameter ต้องแจ้งผู้อำนวยการ ศทส. ผ่านแบบฟอร์มรายงานที่ ศทส. กำหนดขึ้นทุกครั้ง

๒) การใช้เครื่องมือต่าง ๆ (Tools) เพื่อตรวจสอบระบบเครือข่าย ต้องได้รับการอนุมัติจากผู้อำนวยการ ศทส. เป็นลายลักษณ์อักษร

๒.๒.๓.๒ ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมาย ต้องดำเนินการดังนี้

๑) กำหนดพื้นที่การทำงานของระบบเครือข่ายอย่างน้อย ๒ โซน คือ โซนภายใน (Internal Zone) และโซนภายนอก (External Zone) เพื่อให้การควบคุม และป้องกันการบุกรุกทำได้อย่างเป็นระบบ

๒) กำหนดวิธีการจัดการเส้นทางการเข้าถึงเครือข่ายที่มีการใช้งานร่วมกันโดยจัดทำเป็นเอกสารหรือคู่มือ และให้มีการรับรู้ร่วมกันระหว่างเจ้าหน้าที่ภายใน ศทส.

๓) ระบบเครือข่ายทั้งหมดของสำนักงาน กสม. ที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกสำนักงาน กสม. ควรเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือโปรแกรมในการทำ Packet filtering เช่น การใช้ Firewall หรือ Hardware อื่น ๆ ที่มีความสามารถในการตรวจสอบโปรแกรมประสงค์ร้าย (Malware) ด้วย

๔) มีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของสำนักงาน กสม. ในลักษณะที่ผิดปกติผ่านระบบเครือข่าย โดยมีการตรวจสอบการบุกรุกผ่านระบบเครือข่าย การแก้ไขเปลี่ยนแปลงระบบเครือข่ายโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

๕) ต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อระบบเครือข่ายสำนักงาน กสม. สามารถมองเห็นเลขที่อยู่ไอพี IP address ภายใน (Local IP) ของระบบงานเครือข่ายภายในของสำนักงาน กสม. ได้ เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายและส่วนประกอบของเทคโนโลยีสารสนเทศได้โดยง่าย

๖) จัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอย่างน้อยเดือนละ ๑ ครั้ง หรือทุกครั้งที่มีอุปกรณ์ใหม่เข้ามาติดตั้งเพิ่มเติม

๗) การพิสูจน์ตัวตนอุปกรณ์บนเครือข่าย (Equipment Identification in Networks) ต้องกำหนดให้อุปกรณ์บนเครือข่ายสามารถระบุและพิสูจน์ตัวตนเพื่อบ่งบอกว่าการเชื่อมต่อนั้นมาจากอุปกรณ์หรือสถานที่ที่ได้รับอนุญาตแล้ว

๘) ต้องจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้งานเพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

๙) ควรมีการจำกัดเส้นทางการเข้าถึงเครือข่ายที่มีการใช้งานร่วมกัน

๑๐) ควรจัดให้มีวิธีการจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องลูกข่ายไปยังเครื่องแม่ข่ายเพื่อไม่ให้ผู้ใช้สามารถใช้เส้นทางอื่นได้

๑๑) มีการจำกัดระยะเวลาการเชื่อมต่อระบบเครือข่าย (Session Time-out) ในกรณีไม่มีการใช้งาน ๑๕ นาทีระบบจะตัดการเชื่อมต่อระบบเครือข่ายเมื่อผู้ใช้งานประสงค์จะเข้าใช้งานใหม่ ต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) อีกครั้ง เพื่อให้เกิดความปลอดภัย

๒.๒.๓.๓ ผู้ใช้งาน ต้องดำเนินการ Login และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เมื่อใช้งานเพื่อตรวจสอบความถูกต้องก่อนเข้าสู่ระบบงานเครือข่ายภายในสำนักงาน กสม. โดยผ่านทางอินเทอร์เน็ต และเมื่อใช้งานเกิน ๑๕ นาที ระบบจะตัดการเชื่อมต่อระบบเครือข่าย ให้ดำเนินการพิสูจน์ยืนยันตัวตน (Authentication) อีกครั้ง

๒.๒.๔ การบริหารจัดการเครื่องคอมพิวเตอร์แม่ข่าย

๒.๒.๔.๑ ศทส. ต้องดำเนินการดังนี้

๑) กำหนดบุคคลที่รับผิดชอบเครื่องคอมพิวเตอร์แม่ข่าย (Server) ในการแก้ไข หรือเปลี่ยนแปลงค่าต่าง ๆ ของโปรแกรมระบบ (System Software) อย่างชัดเจน ไม่น้อยกว่า ๒ คน

๒) มีขั้นตอนหรือวิธีปฏิบัติในการตรวจสอบเครื่องคอมพิวเตอร์แม่ข่าย และในกรณีที่พบว่ามีการใช้งานหรือเปลี่ยนแปลงค่าในลักษณะผิดปกติ ต้องดำเนินการแก้ไข รวมทั้งการรายงานหรือแจ้ง ผู้อำนวยการ ศทส. โดยทันที

๓) เปิดใช้บริการ (Service) เฉพาะ http และ https เท่านั้น หากจำเป็นใช้บริการนอกเหนือจากที่กำหนดต้องขออนุญาต ผู้อำนวยการ ศทส. เป็นรายกรณี

๒.๒.๔.๒ ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมาย ต้องดำเนินการอัพเดทระบบซอฟท์แวร์ให้เป็นปัจจุบัน อุดช่องโหว่ต่าง ๆ ของโปรแกรมระบบ (System Software) อย่างสม่ำเสมอ เช่น ใน Web Server เป็นต้น

๒.๒.๕ การบริหารจัดการการบันทึกและตรวจสอบการทำงานของระบบ

ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายต้องดำเนินการดังนี้

๑) ต้องมีการจัดเก็บบันทึกการทำงานของระบบคอมพิวเตอร์แม่ข่ายและเครือข่ายบันทึกการปฏิบัติงานของผู้ใช้งาน (Application logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้าออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน command line และ Firewall Log เป็นต้น เพื่อให้เป็นไปตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และใช้ประโยชน์ในการตรวจสอบกรณีมีปัญหา โดยต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย ๙๐ วัน

๒) มีการกำหนดสิทธิ์ในการเข้าถึงข้อมูลแยกจากกันระหว่างผู้ดูแลระบบ (Admin) กับผู้ใช้งาน (User)

๓) ควรมีการตรวจสอบบันทึกการทำงานอย่างคร่าวๆ ตามข้อ ๑) อย่างสม่ำเสมอ

๔) จำกัดสิทธิในการเข้าถึงบันทึกการทำงานต่างๆ ตามข้อ ๑) เฉพาะผู้เกี่ยวข้องเท่านั้น เพื่อป้องกันการแก้ไขเปลี่ยนแปลงบันทึก

๒.๒.๖ การควบคุมการเข้าใช้งานระบบจากภายนอกสำนักงาน กสม.

๒.๒.๖.๑ ผู้ดูแลระบบหรือผู้ได้รับมอบหมาย ต้องดำเนินการดังนี้

๑) กรณีเป็นบุคลากรของสำนักงาน กสม. ติดต่อ ศทส. เพื่อขอรหัสผู้ใช้งานและรหัสผ่านเพื่อทำการเข้าสู่ระบบจากระยะไกลโดยผ่านระบบ VPN โดยต้องระบุเหตุผลหรือความจำเป็นในการใช้งานและต้องได้รับอนุมัติจากผู้อำนวยการ ศทส.

๒) กรณีเป็นบุคคลภายนอก (บริษัท/หน่วยงานภายนอก) กำหนดให้ใช้งานผ่านระบบ Remote Control โดยต้องระบุเหตุผลหรือความจำเป็นในการใช้งานและต้องได้รับอนุมัติจากผู้อำนวยการ ศทส.

๓) ต้องดูแลตรวจสอบตลอดระยะเวลาที่มีการเข้าใช้จากภายนอกและปิดพอร์ตทันทีที่ไม่มีการเชื่อมต่อการใช้งาน

๔) กำหนดเวลาให้เปิดพอร์ตใช้งานต่อเนื่องกันไม่เกิน ๑๕ นาที (Limitation of Connection Time) เพื่อความปลอดภัยของระบบเครือข่ายข้อมูลภายในระบบงานต่างๆของสำนักงาน

๕) ต้องมีการควบคุมพอร์ต (Port) ที่ใช้ในการเข้าสู่จากภายนอกระบบอย่างรัดกุม

๒.๒.๖.๒ ผู้ใช้งาน ต้องดำเนินการดังนี้

๑) ขออนุญาตใช้งานระบบผ่านทาง ศทส. โดยต้องระบุเหตุผลหรือความจำเป็นในการขอเข้าใช้งานทุกครั้ง

๒) ต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) โดยใช้รหัสผู้ใช้งานและรหัสผ่านที่กำหนดไว้

๒.๒.๗ การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

๒.๒.๗.๑ ศทส. ต้องกำหนดตำแหน่งการวางอุปกรณ์ Access Point (AP) ให้เหมาะสมเป็นการควบคุมไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกไปนอกบริเวณที่ใช้งาน และมีการตรวจสอบสัญญาณอย่างน้อยทุก ๆ ๓ เดือน เพื่อป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้

๒.๒.๗.๒ ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมาย ต้องดำเนินการดังนี้

๑) เปลี่ยนค่าชื่ออุปกรณ์ไร้สาย และรหัสผ่านในการเข้าตั้งค่าการทำงานของอุปกรณ์ไร้สาย โดยควรเลือกใช้ชื่อ Login และรหัสผ่านที่มีความคาดเดาได้ยากเพื่อป้องกันผู้โจมตีไม่ให้สามารถเดาหรือเจาะรหัสได้โดยง่าย

๒) กำหนดค่าใช้ Web หรือ WPA ในการเข้ารหัสหรือข้อมูลระหว่าง Wireless LAN Client และ AP เพื่อให้ยากต่อการดักจับ จะช่วยให้ปลอดภัยมากขึ้น

๓) มีการแบ่ง Virtual Lan (VLAN) ระหว่างเครือข่ายไร้สายกับเครือข่ายภายในของสำนักงาน กสม. เพื่อความปลอดภัยในการใช้งาน

๔) ใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สาย เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยที่เกิดขึ้นในระบบเครือข่ายไร้สาย เป็นประจำทุกเดือน

๕) ต้องมีการกำหนดรหัสผู้ใช้และรหัสผ่านในการเข้าใช้งานเครือข่ายไร้สาย (Wireless LAN) ของสำนักงาน กสม. รวมถึง กำหนดระยะเวลาในการเข้าใช้งานให้กลุ่มบุคคลต่าง ๆ ดังนี้

- ผู้ปฏิบัติงานในสำนักงาน กสม. โดยให้สามารถใช้งานได้ตลอดเวลาจนกว่าจะลาออกหรือเกษียณอายุราชการ

- บุคคลที่มีหน้าที่ดำเนินการตามสัญญาว่าจ้าง หรือปฏิบัติงานตามที่ได้รับมอบหมายจากสำนักงานหรือที่ปรึกษา หรือคณะอนุกรรมการ สามารถใช้ระบบเครือข่ายไร้สายได้ไม่จำกัดระยะเวลา จนกว่าจะสิ้นสุดสัญญาว่าจ้าง หรือสิ้นสุดภาระงานตามที่ได้รับมอบหมายหรือหมดวาระการเป็นกรรมการ / อนุกรรมการ

- บุคคลภายนอก ที่เป็นผู้เข้าร่วมประชุม หารือ สัมมนาที่สำนักงานจัดขึ้น สามารถใช้ระบบเครือข่ายไร้สายได้ต่อเนื่องไม่เกิน ๘ ชั่วโมง และจะสิ้นสุดการให้บริการในเวลา ๑๖.๓๐ น. หลังจากนั้น ต้องดำเนินการตรวจสอบการใช้งาน หากพบความผิดปกติ หรือพบการใช้งานที่ผิดปกติให้ตักเตือนและบันทึกข้อมูลไว้เป็นหลักฐาน

๒.๒.๗.๓ ผู้ใช้งาน ต้องปฏิบัติดังนี้

๑) ห้ามนำอุปกรณ์ Wireless มาติดตั้งหรือเปิดใช้งานเองในหน่วยงาน ทั้งที่เป็น Access Point, Wireless Router, Wireless USB หรือ Wireless Card

๒) ผู้ใช้งานที่เป็นบุคคลภายนอก หากประสงค์ใช้งานระบบเครือข่ายไร้สาย (Wireless LAN) ของสำนักงาน กสม. ให้ติดต่อขอรับรหัสผ่านการใช้งานได้ที่ ศทส. หรือประสานผู้จัดประชุมในการติดต่อขอรหัสผ่านจาก ศทส. โดยต้องระบุชื่อ – นามสกุล ผู้ขอใช้งานให้ ศทส. บันทึกการใช้งานด้วย

๒.๒.๘ การใช้งานทั่วไปเครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์พกพา (Personal Computer and Notebook)

๒.๒.๘.๑ ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมาย ต้องดำเนินการดังนี้

๑) ติดตั้งโปรแกรมลงบนเครื่องคอมพิวเตอร์ของสำนักงาน กสม. โดยต้องเป็นโปรแกรมที่สำนักงาน กสม. ได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย

๒) กำหนดชื่อเครื่องคอมพิวเตอร์ (Computer name) ของสำนักงาน กสม.

๓) ติดตั้งซอฟต์แวร์ป้องกันไวรัสในเครื่องคอมพิวเตอร์ของสำนักงาน กสม. ทุกเครื่อง

๒.๒.๘.๒ ผู้ใช้งาน ต้องปฏิบัติดังนี้

๑) ดูแลเครื่องคอมพิวเตอร์ในครอบครองของตนไม่ให้สูญหายและใช้เพื่องานของสำนักงาน กสม. เท่านั้น เนื่องจากเครื่องคอมพิวเตอร์ที่สำนักงาน กสม. อนุญาตให้ใช้งาน ถือเป็นทรัพย์สินของสำนักงาน กสม.

๒) ห้ามทำการลบหรือปิดการใช้งานซอฟต์แวร์ป้องกันไวรัสที่ทางสำนักงาน กสม. ติดตั้งไว้

๓) ห้ามทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ของสำนักงาน กสม. หากมีความจำเป็นต้องใช้งานให้แจ้ง ศทส. ทราบและดำเนินการให้

๔) ไม่เก็บข้อมูลที่เป็นความลับของสำนักงาน กสม. ไว้บนเครื่องคอมพิวเตอร์ของสำนักงานที่ใช้งานอยู่หรือเก็บไว้บนเครื่องคอมพิวเตอร์พกพาส่วนตัว (โน้ตบุ๊ก)

๕) ไม่สร้าง Short-cut หรือปุ่มกดง่ายบน Desktop ที่เชื่อมต่อไปยังข้อมูลที่เป็นความลับของสำนักงาน กสม.

๖) ต้องตรวจสอบเพื่อหาไวรัสจากสื่อต่าง ๆ เช่น สื่อบันทึกพกพา (Flash Drive) และ External Harddisk เป็นต้น ก่อนนำมาใช้งาน

๗) ไม่นำอาหารและ/หรือเครื่องดื่มมารับประทานอยู่ใกล้บริเวณเครื่องคอมพิวเตอร์

๘) ไม่วางสื่อแม่เหล็กไว้ใกล้หน้าจอเครื่องคอมพิวเตอร์หรือฮาร์ดดิสก์

๒.๒.๙ การควบคุมการเข้าถึงระบบปฏิบัติการเครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์พกพา (Personal Computer and Notebook)

๒.๒.๙.๑ ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมาย ต้องดำเนินการดังนี้

๑) ตรวจสอบและทำการตั้งค่าการปรับปรุง Security Patch ของระบบปฏิบัติการโดยอัตโนมัติเพื่อความปลอดภัยในการใช้งาน

๒) ทำการอัพเดทเว็บบราวเซอร์ เพื่ออุดช่องโหว่ของเว็บบราวเซอร์และเพื่อความปลอดภัยในการใช้งานเว็บบราวเซอร์

๒.๒.๙.๒ ผู้ใช้งาน ต้องปฏิบัติดังนี้

๑) ควรกำหนดรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการในเครื่องคอมพิวเตอร์ที่ตนเองใช้งานอยู่

๒) ควรตั้งการใช้งานโปรแกรมรักษาจอภาพ (Screen Saver) โดยตั้งเวลา ๑๐ – ๑๕ นาที เพื่อให้ทำการล็อคหน้าจอเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้งานต้องใส่รหัสผ่านใหม่เพื่อใช้งาน

๓) ไม่ควรให้ผู้อื่นใช้ชื่อผู้ใช้งาน (User name) และรหัสผ่าน (Password) ของตนเอง ในการเข้าใช้เครื่องคอมพิวเตอร์ แม้ว่าจะต้องใช้เครื่องคอมพิวเตอร์ร่วมกัน

๔) เมื่อไม่ได้ใช้งานเครื่องคอมพิวเตอร์ ต้องออกจากระบบ (Logout) หรือปิดเครื่องคอมพิวเตอร์หรือล็อคหน้าจอด้วยโปรแกรม Screen Saver

๕) ห้ามทำการแก้ไขค่าการปรับปรุง Security Patch ของระบบปฏิบัติการและค่าพื้นฐานของเครื่องคอมพิวเตอร์ที่ผู้ดูแลระบบตั้งไว้ให้

๒.๒.๑๐ การใช้งานอินเทอร์เน็ต (Use of the Internet)

๒.๒.๑๐.๑ ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมาย ต้องดำเนินการดังนี้

๑) ต้องติดตั้งโปรแกรมตรวจสอบไวรัส (Virus scanning) เพื่อป้องกันไวรัสที่ติดมากับข้อมูลที่ส่งผ่านทางอินเทอร์เน็ตได้

๒) กำหนดสิทธิให้กับผู้ใช้งานอินเตอร์เน็ต ตามระยะเวลาดังนี้

- เวลาราชการ ๘.๓๐ – ๑๒.๐๐ น. และ ๑๓.๐๐ – ๑๖.๓๐ น.จะมีการจำกัดการใช้งานบางประเภท เช่น YouTube เป็นต้น เพื่อไม่ให้มีกระทบกับการใช้งานอินเตอร์เน็ตโดยส่วนรวม หากมีความจำเป็นต้องใช้งาน ให้แจ้ง ศทส. เปิดการใช้งานเป็นกรณี ๆ ไป

- เวลาอื่น ๆ นอกเหนือจากเวลาราชการ จะเปิดให้ให้ใช้บริการตามปกติ

๓) กรณีระบบมีการแจ้งเตือนหรือบล็อกการใช้งานอินเตอร์เน็ตของผู้ใช้งาน ศทส. จะดำเนินการตรวจสอบการใช้งานของผู้ใช้งาน โดยมิต้องแจ้งให้ผู้ใช้งานทราบ หากพบการใช้งานไม่เหมาะสมจะมีการแจ้งเตือนต่อผู้ใช้งาน ทั้งนี้ ศทส. ต้องไม่นำข้อมูลส่วนบุคคลมาเปิดเผย หรือใช้ในทางที่เสื่อมเสียต่อผู้ใช้งาน

๔) จัดให้มีระบบจัดการผู้ใช้งาน (Active Directory) เพื่อใช้ยืนยันตัวบุคคลก่อนเข้าใช้งานอินเตอร์เน็ตของสำนักงาน กสม.

๒.๒.๑๐.๒ ผู้ใช้งาน ต้องปฏิบัติดังนี้

๑) ผู้ใช้งานต้องใส่รหัสผ่านเพื่อยืนยันตัวตน (Authentication) ก่อนเข้าใช้งานอินเทอร์เน็ต

๒) เมื่อใช้งานอินเทอร์เน็ตเสร็จแล้ว ให้ทำการออกจากระบบ (Log out) เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่นๆ

๓) ต้องไม่ดาวน์โหลดโปรแกรมใช้งานใดๆ ที่มีลิขสิทธิ์จากอินเทอร์เน็ต หากมีความจำเป็นต้องดาวน์โหลด ต้องเป็นไปโดยไม่ละเมิดทรัพย์สินทางปัญญา

๔) ห้ามนำข้อมูลที่เป็นความลับของสำนักงาน กสม. สื่อสารผ่านทางอินเทอร์เน็ตของสำนักงาน กสม.

๕) ต้องไม่ใช้อินเทอร์เน็ตของสำนักงาน กสม. เข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาสร้างความแตกแยกหรือบ่อนทำลายต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม เป็นต้น รวมถึงไม่เผยแพร่ข้อมูลที่ไม่เหมาะสมทางศีลธรรม หรือข้อมูลที่ละเมิดสิทธิของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับสำนักงาน กสม.

<u>ทั้งนี้ การใช้งานอินเตอร์เน็ตในทางที่ผิด อาจถือว่าเป็นความผิดทางวินัยและอาจถูกดำเนินคดีตามกฎหมายทั้งทางแพ่งและอาญา</u>

๖) ไม่นำเข้าข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันเป็นเท็จ ลักษณะอันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร ลักษณะอันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะลามกอนาจาร รวมถึง ไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านสื่ออินเทอร์เน็ตของสำนักงาน กสม.

๗) ไม่นำเข้าข้อมูลคอมพิวเตอร์ที่เป็นภาพของผู้อื่นและภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์ หรือวิธีการอื่นใด ซึ่งจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย

๘) ตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนอินเทอร์เน็ตก่อนนำข้อมูลไปใช้งาน

๙) ในการเสนอความคิดเห็นผ่านสื่ออินเตอร์เน็ต ต้องไม่ใช้ข้อความเชิงยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของสำนักงาน กสม. หรือทำลายความสัมพันธ์กับเจ้าหน้าที่ของหน่วยงานอื่นๆ

๑๐) ไม่ควรให้เว็บบราวเซอร์จดจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Auto Save Password) ของอินเตอร์เน็ต

๑๑) ระมัดระวังการใช้งานเครือข่ายสังคมออนไลน์ โดยไม่ใช่งานดังต่อไปนี้

- การนำเสนอข้อมูลข่าวสารผ่านเครือข่ายสังคมออนไลน์ ต้องไม่เป็นการสร้างความเกลียดชังระหว่างคนในสังคม ไม่ยุยงให้เกิดความรุนแรง จนนำไปสู่ความขัดแย้งหรือความเสียหายขึ้นในสังคม

- การนำเสนอข้อมูลข่าวสารของสำนักงาน กสม. ต้องใช้หลักความถูกต้องและการใช้ภาษาที่เหมาะสม หลีกเลี่ยงการแสดงความคิดเห็นส่วนบุคคลในเรื่องที่เกี่ยวกับการดำเนินงานของสำนักงาน กสม. ในลักษณะที่อาจก่อให้เกิดความเข้าใจที่คลาดเคลื่อนจากความเป็นจริง

- การเผยแพร่ข้อมูลข่าวสารผ่านเครือข่ายสังคมออนไลน์ ต้องไม่ละเมิดลิขสิทธิ์ของข้อมูล ภาพ หรือวีดีทัศน์ของผู้อื่น พึงตระหนักและรับรู้สิทธิหรือลิขสิทธิ์ของบุคคลหรือองค์กรผู้เป็นเจ้าของข้อมูลเสมอ

- ต้องมีความตระหนักเรื่องความมั่นคงปลอดภัยอยู่เสมอ และต้องรับผิดชอบหากเกิดความเสียหายใด ๆ ที่มีผลกระทบกับสำนักงาน กสม. จากการใช้งานเครือข่ายสังคมออนไลน์

๒.๒.๑๑ การใช้งานจดหมายอิเล็กทรอนิกส์ (Electronic Mail)

๒.๒.๑๑.๑ ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมาย ต้องดำเนินการดังนี้

๑) ต้องกำหนดรหัสผู้ใช้งานและรหัสผ่านให้กับผู้ใช้งานในกลุ่มบุคลากรที่ปฏิบัติงานประจำในสำนักงาน กสม.

๒) สำหรับผู้ที่เข้ามาปฏิบัติงานใหม่ ให้กำหนดรหัสผู้ใช้งานและรหัสผ่านให้ทันทีที่ได้รับแจ้งจากหน่วยงานต้นสังกัด

๓) การกำหนดรหัสผู้ใช้งานและรหัสผ่านสำหรับใช้งานครั้งแรก เป็นไปตามคู่มือผู้ดูแลระบบจดหมายอิเล็กทรอนิกส์ (E-mail)

๒.๒.๑๑.๒ ผู้ใช้งาน ต้องปฏิบัติดังนี้

๑) หลังจากผู้ใช้งานเข้าสู่ระบบในครั้งแรกแล้ว ควรเปลี่ยนรหัสผ่านเองโดยทันทีรายละเอียดตามคู่มือการเปลี่ยนรหัสผ่านจดหมายอิเล็กทรอนิกส์

๒) ห้ามใช้ระบบจดหมายอิเล็กทรอนิกส์ของสำนักงาน กสม.ในการสร้างความเสียหายต่อสำนักงาน กสม. หรือละเมิดลิขสิทธิ์ หรือสร้างความน่ารำคาญต่อผู้อื่น หรือในเชิงผิดกฎหมาย หรือละเมิดศีลธรรม

๓) ต้องใช้จดหมายอิเล็กทรอนิกส์ของสำนักงาน กสม. เพื่อการทำงานของสำนักงาน กสม. เท่านั้น และหลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้นแล้ว ต้องทำการ Logout ออกจากระบบทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานระบบจดหมายอิเล็กทรอนิกส์

๔) ต้องตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัสก่อนใช้งานทุกครั้ง

๕) ต้องระวังการเปิดข้อความที่ได้รับ หรือส่งจดหมายอิเล็กทรอนิกส์ตอบกลับจากผู้ส่งที่ไม่รู้จัก

๖) ห้ามส่งข้อความที่ไม่เหมาะสม ไม่สุภาพ หรือทำให้เกิดความแตกแยกระหว่างสำนักงาน กสม. หรือส่งข้อมูลอันอาจทำให้สำนักงาน กสม. เสียชื่อเสียง ผ่านระบบจดหมายอิเล็กทรอนิกส์ของสำนักงาน กสม.

๗) ควรตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ของตนเอง (Inbox) เป็นประจำทุกวัน และลบจดหมายที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้เนื้อที่ระบบจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจำนวนน้อยที่สุด

๘) ต้องไม่ใช้บัญชีจดหมายอิเล็กทรอนิกส์ (Account E-mail) ของสำนักงาน กสม. ในการลงทะเบียนหรือประกาศข้อมูลใดๆ ทางเครือข่ายสังคมออนไลน์ เว้นแต่เป็นการปฏิบัติงานตามหน้าที่ที่ได้รับมอบหมายจากสำนักงาน กสม.

๒.๒.๑๒ การบริหารจัดการไฟร์วอลล์ และระบบการตรวจสอบผู้บุกรุก

๒.๒.๑๒.๑ ศทส. ต้องดำเนินการกำหนดให้มีการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้าออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน command line บันทึก Application Log และบันทึก Firewall Log เป็นต้น เพื่อให้เป็นไปตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และประโยชน์ในการใช้ตรวจสอบ โดยต้องเก็บข้อมูลจราจรดังกล่าว ไว้อย่างน้อย ๙๐ วัน

๒.๒.๑๒.๒ ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมาย ต้องดำเนินการดังนี้

๑) ติดตามและวิเคราะห์เหตุการณ์ที่เกิดขึ้นในระบบเครือข่ายและพฤติกรรมของผู้ใช้

๒) ตรวจสอบการกำหนดค่าระดับความปลอดภัยไฟร์วอลล์และระบบการตรวจสอบผู้บุกรุกที่ใช้งานอยู่ในปัจจุบันอย่างน้อยทุก ๆ ๓ เดือน

๓) มีการสำรองข้อมูลการกำหนดค่าต่าง ๆ ของอุปกรณ์ไฟร์วอลล์เป็นประจำทุกเดือนหรือทุกครั้งที่มีการเปลี่ยนแปลงการตั้งค่า

๔) ตรวจสอบบันทึกของข้อมูลจราจรทางคอมพิวเตอร์ (Log) และรายงานของไฟร์วอลล์ สิ่งที่ควรตรวจสอบมีดังต่อไปนี้

- สถิติข้อมูลที่ไฟร์วอลล์ได้ทำการป้องกันข้อมูลที่ส่งผ่านทางอินเตอร์เน็ต (block packet)
- สถิติข้อมูลหมายเลขไอพีที่ส่งผ่านทางอินเตอร์เน็ตที่ถูก block มาจากหมายเลขไอพีใดของเครือข่ายใดบ้างและจำนวนการถูก block

๕) รายงานข้อมูลเมื่อเกิดความผิดปกติจากการบุกรุกหรือการถูกโจมตีที่อาจจะก่อให้เกิดความไม่ปลอดภัยจากทั้งภายนอกและภายในต่อผู้อำนวยการ ศทส. ทันทีเพื่อรับทราบและแนะนำแนวปฏิบัติ

ส่วนที่ ๓
นโยบายและแนวปฏิบัติในการสำรองข้อมูล

๓.๑ นโยบายในการสำรองข้อมูล

วัตถุประสงค์ เพื่อให้มีการบริหารจัดการระบบสำรองข้อมูลระบบเทคโนโลยีสารสนเทศและการสื่อสาร มีแผนกรณีฉุกเฉินเพื่อให้สามารถทำงานได้อย่างต่อเนื่อง รวมทั้งมีการตรวจสอบและเมินความเสี่ยงของระบบเทคโนโลยีสารสนเทศและการสื่อสาร ซึ่งจะเป็นการป้องกันและลดระดับความเสี่ยงที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมถึงกำหนดมาตรการในการควบคุมความเสี่ยงด้านสารสนเทศ โดยต้องมีการทบทวนนโยบายและแนวปฏิบัติอย่างน้อยปีละ ๑ ครั้ง

๓.๒. แนวปฏิบัติ

๓.๒.๑ การสำรองข้อมูล

ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมาย ต้องดำเนินการดังนี้

๑) ต้องมีการจัดทำทะเบียนข้อมูลและระบบงานทั้งหมดของหน่วยงาน พร้อมกำหนดระบบสารสนเทศที่จะต้องดำเนินการสำรองข้อมูล ขั้นตอนและความถี่ในการสำรองข้อมูลของแต่ละระบบ

๒) ต้องกำหนดการสำรองข้อมูลแบบเต็ม (Full Backup) และสำรองข้อมูลแบบส่วนต่าง (Incremental Backup) รวมถึง รูปแบบการสำรองข้อมูลให้เหมาะสมกับข้อมูลที่จะทำการสำรอง

๓) ต้องทำการสำรองข้อมูลระบบงานเก็บไว้เป็นประจำอย่างสม่ำเสมอตามแผนการสำรองข้อมูล

๔) ต้องทำการตรวจสอบความสมบูรณ์ของข้อมูลที่สำรอง และให้มีการทบทวนแผนการสำรองข้อมูล อย่างน้อยปีละ ๑ ครั้ง

๕) ต้องจัดทำขั้นตอนปฏิบัติ สำหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่ได้สำรองเก็บไว้

๖) ต้องจัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ ระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลสำรองกับหน่วยงาน ควรห่างกันอย่างน้อย ๒๐ กม. เพื่อไม่ให้ส่งผลกระทบต่อข้อมูลที่จัดเก็บไว้นอกสถานที่นั้น ในกรณีที่เกิดภัยพิบัติกับหน่วยงาน เช่น ไฟไหม้ เป็นต้น

๓.๒.๒ การจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน

ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมาย ต้องดำเนินการดังนี้

๓.๒.๒.๑ มีการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน (ในกรณีระบบหลักไม่สามารถใช้งานได้จากภัยพิบัติ ให้ไปใช้ระบบสำรอง (DR-Site)) โดยมีรายละเอียดอย่างน้อยดังนี้

๑) มีการกำหนดหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด

๒) มีการประเมินความเสี่ยงระบบงาน และกำหนดมาตรการเพื่อลดความเสี่ยงเหล่านั้น เช่น ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว การชุมนุมประท้วง ทำให้ไม่สามารถเข้ามาใช้ระบบงานได้ เป็นต้น

๓) มีการกำหนดขั้นตอนการปฏิบัติในการกู้คืนระบบสารสนเทศ

๔) มีกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูล และมีการทดสอบกู้คืนข้อมูลที่สำรองไว้

๕) มีการกำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอก เช่น ผู้ให้บริการเครือข่าย ฮาร์ดแวร์ ซอฟต์แวร์ เป็นต้น เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อ

๓.๒.๒.๒ มีการทบทวนและทดสอบตามแผนเตรียมความพร้อมกรณีฉุกเฉินและระบบสำรองข้อมูล อย่างน้อยปีละ ๑ ครั้ง

๓.๒.๓ การตรวจสอบประเมินความเสี่ยงระบบเทคโนโลยีสารสนเทศและการสื่อสาร

ศทส. ต้องดำเนินการดังนี้

๑) ตรวจสอบ และประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (information security audit and assessment) อย่างน้อยปีละ ๑ ครั้ง พร้อมจัดทำรายงานพร้อมข้อเสนอแนะ

๒) ตรวจสอบและประเมินความเสี่ยง ที่ดำเนินการโดยเจ้าหน้าที่ของ ศทส. หรือผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยจากภายนอก (external auditor) เพื่อให้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

๓) มีการจัดทำแผนบริหารความเสี่ยง โดยต้องมีการวิเคราะห์ความเสี่ยงและระบุความเสี่ยง กิจกรรมการ บริหารความเสี่ยง จัดลำดับความเสี่ยง เป็นอย่างน้อย

๔) ให้มีการทบทวนกระบวนการบริหารจัดการความเสี่ยง อย่างน้อยปีละ ๑ ครั้ง

ส่วนที่ ๔

นโยบายและแนวปฏิบัติในการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัย ระบบเทคโนโลยีสารสนเทศและการสื่อสาร

๔.๑. นโยบายในการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร

วัตถุประสงค์ เพื่อเผยแพร่นโยบายและแนวปฏิบัติให้กับบุคลากรและบุคคลที่เกี่ยวข้อง ได้มีความรู้ความเข้าใจและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตลอดจนสามารถนำไปปฏิบัติได้อย่างถูกต้องโดยการจัดทำคู่มือ จัดฝึกอบรมการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารและระบบคอมพิวเตอร์ให้แก่ผู้ใช้งานเป็นระยะ ๆ

๔.๒ แนวปฏิบัติในการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร

๔.๒.๑ ผู้บริหารระดับสูงของสำนักงาน (Chief Information Officer: CEO) มีหน้าที่เป็นผู้รับผิดชอบในการสั่งการตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสารและการสื่อสาร ให้การสนับสนุนต่อการบริหารจัดการความมั่นคงปลอดภัยขององค์กร ให้นโยบายกำกับดูแลและการเล็งเห็นถึงความสำคัญในหน้าที่และความรับผิดชอบด้านความมั่นคงปลอดภัย

๔.๒.๒ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer: CIO) มีหน้าที่ให้คำปรึกษา เรื่อง แนวนโยบายเรื่องการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร

๔.๒.๓ ศทส. ต้องดำเนินการดังนี้

๑) ทำการจัดฝึกอบรมด้านเทคโนโลยีสารสนเทศและการสื่อสารประจำปี เพื่อเสริมสร้างความรู้ความเข้าใจด้านเทคโนโลยีสารสนเทศและการสื่อสารให้กับบุคลากรของสำนักงาน กสม. โดยแทรกเนื้อหาการสร้างความตระหนักเรื่องการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารในการฝึกอบรมด้วย

๒) ให้ความรู้เกี่ยวกับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยอาจใช้วิธีติดประกาศ การประชาสัมพันธ์ หรือการเผยแพร่ทางเว็บไซต์หรือจัดทำคู่มือการใช้งานระบบต่าง ๆ เป็นต้น

ภาคผนวก

แผนรับสถานการณ์ฉุกเฉิน
จากภัยพิบัติระบบเทคโนโลยีสารสนเทศ (IT Contingency Plan)

๑. แนวทางปฏิบัติในการสำรองข้อมูลและระบบงาน

๑.๑ จัดทำเอกสารทะเบียนระบบงานทั้งหมดของสำนักงาน กสม. พร้อมจัดลำดับความสำคัญของเอกสาร

๑.๒ กำหนดผู้รับผิดชอบในการดำเนินการสำรองข้อมูลและระบบงาน

๑.๓ กำหนดรายละเอียดของรายการข้อมูลที่ต้องดำเนินการสำรองและความถี่

ลำดับ	ระบบงาน	ความถี่
๑	ระบบห้องสมุด	ทุกสัปดาห์ (ส-อา)
๒	ระบบเครือข่ายสิทธิมนุษยชน	ทุกสัปดาห์ (ส-อา)
๓	ระบบสารสนเทศเพื่อการรวบรวมข้อมูลสิทธิมนุษยชน	ทุกสัปดาห์ (ส-อา)
๔	ระบบสารบรรณ	ทุกสัปดาห์ (ส-อา)
๕	ระบบสำนักวินิจฉัยและคดี	ทุกสัปดาห์ (ส-อา)
๖	ระบบรับเรื่องร้องเรียน	ทุกสัปดาห์ (ส-อา)
๗	ระบบเว็บไซต์	ทุกสัปดาห์ (ส-อา)
๘	ระบบอีเมล์สำนักงาน	ทุกสัปดาห์ (ส-อา)

๑.๔ ดำเนินการสำรองข้อมูลและระบบตามที่กำหนดไว้พร้อมกับการตรวจสอบความสมบูรณ์ของการสำรองแต่ละครั้ง

๑.๕ รายงานผลการปฏิบัติงานตามสายงานการบังคับบัญชา

๒. แนวทางปฏิบัติในการกู้คืนข้อมูลและระบบงาน

๒.๑ กำหนดผู้รับผิดชอบในการดำเนินการกู้คืนข้อมูลและระบบงาน

๒.๒ ทดสอบการกู้คืนข้อมูลและระบบงาน ปีละครั้ง

๒.๕ แจ้งผู้บังคับบัญชาศูนย์ก่อนดำเนินการกู้คืนข้อมูล

๒.๕ ดำเนินการกู้คืนข้อมูลและระบบงาน

๒.๖ ตรวจสอบความสมบูรณ์ของข้อมูลและระบบที่ได้จากการกู้คืน

๒.๗ ทดสอบการปฏิบัติงานตามคู่มือข้อมูลและระบบงานที่กู้คืนแต่ละระบบหรือทั้งหมด

๒.๘ รายงานผลการปฏิบัติงานต่อผู้บังคับบัญชาศูนย์

๓. การจัดสายการบังคับบัญชา (Lines of authority) เมื่อเกิดเหตุฉุกเฉิน

๓.๑ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer: CIO)

๑) กำหนดนโยบายให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๒) ให้คำปรึกษาแก่ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๓.๒ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๑) สั่งการให้ทุกหน่วยปฏิบัติการระงับเหตุฉุกเฉินที่เกิดขึ้น

๒) สั่งทำลายกุญแจอุปกรณ์สำนักงานเพื่อการระงับเหตุฉุกเฉิน

๓) วางแผนปฏิบัติงานเพื่อระงับเหตุฉุกเฉิน

๔) ประเมินสถานการณ์และสั่งการให้ปรับเปลี่ยนแผนฯตามความเหมาะสม

๕) รายงานข้อมูลและผลการปฏิบัติงานให้ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) ทราบ

๓.๓ ผู้ประสานงานและบริหารกำกับดูแลระบบเครือข่ายและระบบสารสนเทศ

๑) วิเคราะห์สถานการณ์ในที่เกิดเหตุแล้วแจ้งเหตุต่อผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๒) สั่งการให้ใช้แผนปฏิบัติการฉุกเฉินขั้นต้นจนกว่าผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารจะมาถึงที่เกิดเหตุหรือสั่งการใดๆ

๓) ทำหน้าที่แทนผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารตามที่ได้รับมอบหมายหรือขณะที่ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารไม่อยู่หรือไม่สามารถปฏิบัติหน้าที่ได้

๔) ประสานงานกับหน่วยงานที่เกี่ยวข้องเช่นไฟฟ้ายานพาหนะและดับเพลิงเป็นต้น

๕) วางแผนอัตรากำลังวัสดุอุปกรณ์และเครื่องมือที่จำเป็น

๖) ตรวจสอบความเสียหายของทรัพย์สินและอาคารที่เกิดเหตุ

๗) รายงานให้ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารทราบถึงสถานการณ์การดำเนินงานที่ได้กระทำไปแล้วและรายงานสรุปเมื่อเสร็จสิ้นภารกิจ

๓.๔ ผู้ดูแลระบบเครือข่ายและระบบสารสนเทศ (LAN Administrator and Staffs)

๑) ดำเนินการตามแผนและการสั่งการเพื่อป้องกันชีวิตทรัพย์สินและสิ่งแวดล้อมให้ได้รับความเสียหายน้อยที่สุด

๒) หลังจากเหตุการณ์ฉุกเฉินได้สงบลงแล้วให้รีบดำเนินการตรวจสอบวัสดุอุปกรณ์ที่ชำรุดเสียหายแล้วรายงานให้ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารทราบ อุปกรณ์ที่ต้องตรวจสอบได้แก่

- ทำการตรวจสอบระบบ firewall
- ทำการตรวจสอบ virus, worm, spy ware
- ทำการตรวจสอบ UPS
- ทำการตรวจสอบ Transaction log files
- ทำการตรวจสอบการใช้งานข้อมูลระบบงานที่สำคัญ
- ทำการตรวจสอบการเปลี่ยนแปลงของไฟล์ต่างๆ
- ทำการตรวจสอบความถูกต้องของไฟล์ข้อมูล
- ทำการตรวจสอบค่า Configuration ของระบบ

๓) เตรียมเครื่องมืออุปกรณ์ทั้งทางด้าน Hardware และ software ตลอดจนอุปกรณ์ที่เกี่ยวข้องเพื่อดำเนินการกู้คืนระบบโดยเร็ว

๔) ประสานงานกับที่ปรึกษาด้านเทคนิค

๕) ดำเนินการกู้คืนระบบและข้อมูลเพื่อให้สามารถใช้งานได้ตามปกติ

๓.๕ ที่ปรึกษาด้านเทคนิค (เจ้าหน้าที่บริษัทที่รับจ้างบำรุงรักษาระบบ)

๑) ให้คำปรึกษาในเรื่องเกี่ยวกับระบบสารสนเทศและวิธีการจัดการในการระงับเหตุฉุกเฉินที่ปลอดภัยต่อชีวิตทรัพย์สินและสิ่งแวดล้อมมากที่สุด

๒) ให้คำปรึกษาวิธีการกู้คืนระบบสารสนเทศกลับคืนมาโดยเร็วหลังจากเหตุฉุกเฉินสงบแล้ว

๓.๖ หัวหน้าหน่วยงานที่เกิดเหตุ (On-site manager)

๑) แจ้งเหตุฉุกเฉินเคลื่อนย้ายทรัพย์สินตนเองและผู้อื่นออกจากที่เกิดเหตุโดยเร็ว

๒) ให้รายละเอียดเกี่ยวกับสถานที่เกิดเหตุแก่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๓) นำทรัพย์สินที่ขนย้ายออกมาเก็บเข้าที่โดยต้องตรวจสภาพและสอบทานบัญชีทรัพย์สินที่จัดทำขึ้นมาและทำรายงานเสนอผู้บังคับบัญชาตามลำดับขั้น