นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของสำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ (National Human Rights Commission of Thailand)

สารบัญ

ประกาศสำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ

เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของสำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ

.....

โดยพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ บัญญัติให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ประกอบกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดให้หน่วยงานของรัฐมีหน้าที่ดำเนินมาตรการป้องกัน รับมือ และลดความเสี่ยงภัยคุกคามทางไซเบอร์ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์มีความมั่นคงปลอดภัยและเชื่อถือได้

อาศัยอำนาจตามความในมาตรา ๕๓ แห่งพระราชบัญญัติประกอบรัฐธรรมนูญว่าด้วยคณะกรรมการสิทธิมนุษยชนแห่งชาติ พ.ศ. ๒๕๖๐ และมาตรา ๕ และมาตรา ๗ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ สำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติจึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศสำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ”

ข้อ ๒ ให้ยกเลิกประกาศสำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ เมื่อวันที่ ๓๐ กันยายน ๒๕๕๗

ข้อ ๓ ประกาศนี้ให้ใช้บังคับตั้งแต่บัดนี้เป็นต้นไป

ข้อ ๔ นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มีวัตถุประสงค์ดังต่อไปนี้

(๑) เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ของสำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ

(๒) เพื่อกำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยระบบสารสนเทศอ้างอิงตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ

(๓) เพื่อกำหนดมาตรฐาน แนวปฏิบัติและวิธีปฏิบัติ ให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับสำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติได้ถือปฏิบัติ

ข้อ ๕ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กำหนดประเด็นสำคัญ ดังต่อไปนี้

(๑) ให้มีการ...

(๑) ให้มีการเข้าถึงหรือควบคุมการใช้งานสารสนเทศและระบบเทคโนโลยีสารสนเทศของสำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ ได้แก่ ระบบสารสนเทศ ระบบเครือข่าย ระบบปฏิบัติการ โปรแกรมประยุกต์หรือแอพพลิเคชั่น เครื่องคอมพิวเตอร์ เครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์คอมพิวเตอร์ต่าง ๆ ให้มีความมั่นคงปลอดภัย

(๒) มีระบบสารสนเทศและระบบสำรองของสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งานและมีแผนเตรียมความพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้อย่างปกติอย่างต่อเนื่อง

(๓) มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ

ข้อ ๖ กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่หน่วยงานหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบาย และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยกำหนดให้ผู้บริหารระดับสูงสุดของหน่วยงานเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

ข้อ ๗ ให้สำนักและหน่วยงานในสังกัดสำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ ถือปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ ตามที่แนบท้ายประกาศนี้

ประกาศ ณ วันที่ ๒ มิถุนายน พ.ศ. ๒๕๖๖

(นายพิทักษ์พล บุณยมาลิก)
เลขาธิการคณะกรรมการสิทธิมนุษยชนแห่งชาติ

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของสำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ

๑. หลักการและเหตุผล

ตามความในมาตรา ๕ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการในทางอิเล็กทรอนิกส์กับหน่วยงานภาครัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ เพื่อให้ระบบสารสนเทศของสำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่าง ๆ สำนักงาน กสม. จึงเห็นควรกำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเพื่อเป็นเครื่องมือในการปฏิบัติงานและบริหารจัดการด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศและป้องกันภัยคุกคามต่าง ๆ

๒. วัตถุประสงค์

๒.๑ เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ของสำนักงาน กสม.

๒.๒ เพื่อกำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยระบบสารสนเทศ อ้างอิงตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ ของกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

๒.๓ เพื่อกำหนดมาตรฐาน แนวปฏิบัติและวิธีปฏิบัติ ให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับสำนักงาน กสม. ได้ถือปฏิบัติ

๓. นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๓.๑ ส่งเสริมและสนับสนุนการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้ตอบสนองต่อพันธกิจและนโยบายของสำนักงาน กสม.

๓.๒ มุ่งกำหนดแนวปฏิบัติ แนวทางแก้ไขหรือบทลงโทษตามความเหมาะสม หากละเมิดหรือฝ่าฝืนนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ รวมทั้งติดตามและตรวจสอบการดำเนินงานอย่างสม่ำเสมอเพื่อให้เป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

๓.๓ เน้นกำกับดูแลการดำเนินงานเพื่อบริหารจัดการให้ระบบสารสนเทศมีความถูกต้องสมบูรณ์และพร้อมใช้งานอยู่เสมอ

๓.๔ เผยแพร่ความรู้ความเข้าใจเพื่อสร้างความตระหนักให้บุคลากรที่เกี่ยวข้องในสำนักงาน กสม.

๓.๕ ติดตาม ตรวจสอบการดำเนินงานและปรับปรุงแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้สอดคล้องตามการเปลี่ยนแปลงของเทคโนโลยี

๔. แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

สำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติกำหนดขั้นตอนและกระบวนการที่เหมาะสมตามหลักมาตรฐานสากล สำหรับใช้งานระบบสารสนเทศโดยคำนึงถึงความถูกต้อง ครบถ้วน น่าเชื่อถือ เพื่อจะช่วยให้ระบบสารสนเทศมีสภาพพร้อมใช้งานและมีความปลอดภัย ลดความเสียหายต่อการดำเนินงาน ทรัพย์สิน บุคลากรของสำนักงาน กสม. จัดเป็นแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ซึ่งเจ้าหน้าที่ของสำนักงาน กสม. และหน่วยงานภายนอกที่เข้ามาใช้ระบบจะต้องปฏิบัติตามอย่างเคร่งครัด

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ประกอบด้วยส่วนต่าง ๆ ดังนี้

คำนิยาม

ส่วนที่ ๑ นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

ส่วนที่ ๒ นโยบายและแนวปฏิบัติในการเข้าถึงและควบคุมการใช้งานสารสนเทศ

ส่วนที่ ๓ นโยบายและแนวปฏิบัติในการสำรองและตรวจสอบประเมินความเสี่ยงด้านสารสนเทศ

ส่วนที่ ๔ นโยบายและแนวปฏิบัติในการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ส่วนที่ ๕ หน้าที่และความรับผิดชอบด้านสารสนเทศ

ภาคผนวก

คำนิยาม

คำนิยามที่ใช้ในนโยบายและแนวปฏิบัตินี้ ประกอบด้วย

๑. **สำนักงาน กสม.** หมายถึง สำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ

๒. **ผู้บริหารสูงสุด (Chief Executive Officer: CEO)** หมายถึง เลขาธิการคณะกรรมการสิทธิมนุษยชนแห่งชาติ เป็นผู้รับผิดชอบ กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๓. **ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกรม (Department Chief Information Officer: DCIO)** หมายถึง รองเลขาธิการที่ได้รับมอบหมายจากเลขาธิการคณะกรรมการสิทธิมนุษยชนแห่งชาติ ให้รับผิดชอบดูแลสำนักดิจิทัลสิทธิมนุษยชนของสำนักงาน กสม. หรือผู้มีอำนาจในด้านเทคโนโลยีสารสนเทศของสำนักงาน กสม. โดยมีหน้าที่และความรับผิดชอบในส่วนของการกำหนดนโยบาย มาตรฐานการควบคุมดูแลการใช้งานระบบเทคโนโลยีสารสนเทศ

๔. **ผู้อำนวยการสำนักดิจิทัลสิทธิมนุษยชน** หมายถึง ผู้อำนวยการสำนักดิจิทัลสิทธิมนุษยชนเป็นผู้ดูแลรับผิดชอบบริหารจัดการและมีอำนาจตัดสินใจงานของสำนักดิจิทัลสิทธิมนุษยชนของสำนักงาน กสม.

๕. **ความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security)** หมายความว่า การรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงาน กสม. เพื่อการธำรงไว้ซึ่งความลับ(Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศรวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non-Repudiation) และความน่าเชื่อถือ (Reliability) และหมายความรวมถึง การป้องกันทรัพย์สินสารสนเทศจากการเข้าถึง ใช้ เปิดเผย ขัดขวาง เปลี่ยนแปลงแก้ไข ทำสูญหาย ทำให้เสียหาย ถูกทำลายหรือล่วงรู้โดยมิชอบ

๖. **เหตุการณ์ด้านความมั่นคงปลอดภัย (information security event)** หมายถึง เหตุการณ์ที่เกิดขึ้นกับคอมพิวเตอร์และเครือข่ายขององค์กร หรือเหตุการณ์ที่สงสัยว่าจะเป็นจุดอ่อนหรือสร้างความเสียหายได้ในที่สุด ซึ่งส่งผลให้

- เกิดการหยุดชะงักต่อระบบงานสำคัญ
- เป็นการละเมิดนโยบายความมั่นคงปลอดภัยขององค์กร
- เป็นการละเมิดต่อกฎหมาย ระเบียบ ข้อบังคับ หรือข้อกำหนดต่าง ๆ ที่องค์กรต้องปฏิบัติตาม
- เกิดภาพลักษณ์ที่ไม่ดีต่อองค์กร หรือทำให้องค์กรสูญเสียชื่อเสียง (เช่น การไปโพสต์ข้อความพาดพิงถึงองค์กรในเว็บไซต์ภายนอก ซึ่งอาจก่อให้เกิดความเสียหายต่อชื่อเสียงขององค์กร เป็นต้น)

๗. **สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (information security incident)** หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (unwanted or unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

๘. **แนวทางปฏิบัติ (Guideline)** หมายถึง แนวทางที่ไม่ได้บังคับให้ปฏิบัติ แต่แนะนำให้ปฏิบัติตามเพื่อให้สามารถบรรลุเป้าหมายได้ง่ายขึ้น

๙. **ผู้ใช้งาน (User)** หมายถึง บุคคลที่ได้รับอนุญาต (Authorized user) ให้สามารถเข้าใช้งาน หรือบริหารจัดการ หรือดูแลรักษาระบบเทคโนโลยีสารสนเทศ หรือเครือข่ายอินเทอร์เน็ตของสำนักงาน กสม. โดยมีสิทธิและหน้าที่ขึ้นอยู่กับบทบาท (Role) ที่กำหนดในการเข้าถึงสารสนเทศของสำนักงาน ดังนี้

๙.๑ ผู้บริหาร หมายถึง คณะกรรมการสิทธิมนุษยชนแห่งชาติ เลขาธิการคณะกรรมการสิทธิมนุษยชนแห่งชาติ รองเลขาธิการคณะกรรมการสิทธิมนุษยชนแห่งชาติ ที่ปรึกษาสำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ ผู้ตรวจการสิทธิมนุษยชน ผู้อำนวยการสำนัก หัวหน้ากลุ่มงาน

๙.๒ ผู้ดูแลระบบ หมายถึง ผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาหรือจัดการระบบคอมพิวเตอร์แม่ข่าย ระบบเครือข่ายคอมพิวเตอร์ ระบบฐานข้อมูล และระบบสารสนเทศ

๙.๓ ผู้พัฒนาระบบ หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการพัฒนาระบบแอปพลิเคชัน

๙.๔ ผู้ดูแลครุภัณฑ์ หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้เป็นผู้ควบคุมดูแลพัสดุหรือทรัพย์สินของสำนักงานที่อยู่ในความครอบครองของหน่วยงานภายในให้อยู่ในสภาพที่พร้อมใช้งานได้ตลอดเวลา โดยมิให้เกิดการสูญหาย

๙.๕ เจ้าหน้าที่ หมายถึง ข้าราชการ พนักงานราชการ เลขานุการ/ผู้ช่วยเลขานุการ ประจำประธานกรรมการและกรรมการสิทธิมนุษยชนแห่งชาติ รวมถึงบุคคลอื่นใดของสำนักงาน กสม.

๙.๖ บุคคลภายนอก หมายความว่า บุคคลจากหน่วยงานภายนอกที่เข้ามาประชุม หรือปฏิบัติงานร่วมกับสำนักงาน กสม.

๑๐. **สิทธิของผู้ใช้งาน** หมายถึง สิทธิของผู้ใช้งานในการเข้าถึงระบบสารสนเทศของสำนักงาน กสม. ซึ่งกำหนดไว้ดังนี้

๑๐.๑ สิทธิทั่วไป หมายถึง สิทธิของผู้ใช้งาน (User) ที่สามารถใช้งานระบบสารสนเทศได้

๑๐.๒ สิทธิจำเพาะ หมายถึง สิทธิของผู้ใช้งาน (User) ที่สามารถนำเข้าข้อมูลและแก้ไขข้อมูลในระบบเฉพาะส่วนที่ตนเองได้รับมอบหมายเท่านั้น

๑๐.๓ สิทธิพิเศษ หมายถึง สิทธิสูงสุดของผู้ดูแลระบบ (Root) สามารถเข้าถึงข้อมูลในระบบได้ทั้งหมด

๑๑. **หน่วยงานภายนอก หมายถึง** องค์กรหรือหน่วยงานภายนอกที่ได้รับอนุญาตให้มีสิทธิในการเข้าถึงและใช้งานข้อมูลหรือสินทรัพย์ต่าง ๆ ของสำนักงาน กสม. โดยจะได้รับสิทธิในการใช้งานตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล

๑๒. **ข้อมูลคอมพิวเตอร์** หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึง ข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

๑๓. **สารสนเทศ (Information)** หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูล ซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่ายและสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ ได้

๑๔. **ระบบเทคโนโลยีสารสนเทศ (Information Technology System)** ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และ ระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุม

การติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูลและสารสนเทศ เป็นต้น

๑๕. โปรแกรม (Program) หมายถึง ชุดคำสั่งที่ใช้ในการควบคุมเครื่องอิเล็กทรอนิกส์หรือโปรแกรมคอมพิวเตอร์ที่มีชุดคำสั่งสำเร็จรูปรอการใช้งาน

๑๖. ระบบคอมพิวเตอร์ หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวปฏิบัติงานให้อุปกรณ์ หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

๑๗. ระบบเครือข่าย (Network System) หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสาร หรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ของสำนักงาน กสม. ได้แก่ ระบบ Intranet ระบบ Internet

๑๗.๑ ระบบอินทราเน็ต (Intranet) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่าง ๆ ภายในหน่วยงานเข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสาร แลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน

๑๗.๒ ระบบอินเทอร์เน็ต (Internet) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่าง ๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตทั่วโลก

๑๘. เว็บเบราว์เซอร์ (Web Browser) หมายถึง โปรแกรมสืบค้นข้อมูลทางอินเทอร์เน็ต เช่น Internet Explorer, Mozilla Firefox, Google Chrome เป็นต้น

๑๙. ห้องควบคุมระบบสารสนเทศ (Server room) หมายถึง ห้องควบคุมระบบเทคโนโลยีสารสนเทศและระบบรักษาความปลอดภัยเครือข่ายสารสนเทศของสำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ

๒๐. พื้นที่ใช้งานระบบสารสนเทศ (Information System Workspace) หมายถึง พื้นที่ที่หน่วยงานอนุญาตให้ใช้งานระบบสารสนเทศ โดยแบ่งเป็น

๒๐.๑ พื้นที่ทำงานทั่วไป (General working area) หมายถึง พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคลและคอมพิวเตอร์พกพาที่ประจำโต๊ะทำงาน

๒๐.๒ พื้นที่ห้องควบคุมระบบสารสนเทศ (Server room) หมายถึง พื้นที่ที่ติดตั้งและจัดเก็บอุปกรณ์ระบบสารสนเทศและระบบเครือข่าย

๒๐.๓ พื้นที่ใช้งานระบบเครือข่ายไร้สาย (Wireless LAN coverage area) หมายถึง พื้นที่ในการให้บริการระบบเครือข่ายไร้สาย

๒๑. เจ้าของข้อมูล หมายถึง ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงาน โดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น ๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย

๒๒. สินทรัพย์ หมายถึง ทรัพย์สิน หรือสิ่งใดก็ตามทั้งที่มีตัวตนและไม่มีตัวตน ที่มีคุณค่าสำหรับสำนักงาน อันได้แก่ ข้อมูล ระบบข้อมูล ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ ข้อมูลคอมพิวเตอร์และสินทรัพย์ด้านเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงาน เช่น อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ ระบบสารสนเทศ ตัวเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ เครื่องบันทึกข้อมูล อุปกรณ์ต่อพ่วง เป็นต้น

๒๓. การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ หมายถึง การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึง หรือใช้งานเครือข่าย หรือสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และ ทางกายภาพ รวมทั้งการอนุญาตสำหรับบุคคลภายนอก

๒๔. จดหมายอิเล็กทรอนิกส์ (E-mail) หมายถึง ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียว หรือหลายคนก็ได้ มาตรฐานที่ใช้ในการรับส่งข้อมูลชนิดนี้ เช่น SMTP, POP๓ และ IMAP เป็นต้น

๒๕. ชื่อผู้ใช้ (Username) หมายถึง ชุดของตัวอักษรหรือตัวเลขที่ถูกกำหนดขึ้น เพื่อใช้ในการลงบันทึกเข้า (Login) รวมถึงเพื่อใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายที่มีการกำหนดสิทธิ์การใช้งานไว้

๒๖. รหัสผ่าน (Password) หมายถึง ชุดของตัวอักษรหรืออักขระหรือตัวเลขที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคลเพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศ

๒๗. ลงบันทึกเข้า (Login) หมายถึง กระบวนการที่ผู้ใช้บริการต้องทำให้เสร็จสิ้นตามเงื่อนไขที่ตั้งไว้เพื่อเข้าใช้งานระบบคอมพิวเตอร์และระบบเครือข่าย ซึ่งปกติแล้วจะอยู่ในรูปแบบของการกรอกชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ให้ถูกต้อง

๒๘. ลงบันทึกออก (Logout) หมายถึง กระบวนการที่ผู้ใช้บริการทำเพื่อสิ้นสุดการใช้งานระบบคอมพิวเตอร์และระบบเครือข่าย

๒๙. ปรับปรุงข้อมูล (Update) หมายถึง ปรับให้เป็นปัจจุบันการปรับปรุงข้อมูลด้านต่าง ๆ ของระบบสารสนเทศให้ทันสมัยอยู่เสมอ

๓๐. โปรแกรมประสงค์ร้าย (Malware) หมายถึง โปรแกรมคอมพิวเตอร์หรือชุดคำสั่งที่ได้รับการออกแบบขึ้นมาโดยมีวัตถุประสงค์เพื่อก่อกวนหรือสร้างความเสียหายไม่ว่าโดยตรงหรือโดยอ้อมแก่ระบบคอมพิวเตอร์หรือระบบเครือข่าย เช่น ไวรัสคอมพิวเตอร์ (Computer Virus) หรือสปายแวร์ (Spyware) หรือหนอน (Worm) หรือม้าโทรจัน (Trojan horse) หรือฟิชชิง (Phishing) หรือจดหมายลูกโซ่ (Mass Mailing) เป็นต้น

๓๑. สื่อบันทึกพกพา หมายถึง สื่ออิเล็กทรอนิกส์ที่ใช้ในการบันทึกหรือจัดเก็บข้อมูล เช่น Flash Drive หรือ Handy Drive หรือ Thumb Drive หรือ External Hard disk หรือ Floppy disk เป็นต้น

๓๒. การตั้งค่าระบบ (Configuration) หมายถึง การกำหนดค่าที่ใช้งานของโปรแกรมหรือองค์ประกอบของเครื่องคอมพิวเตอร์ทั้งทางด้านฮาร์ดแวร์และซอฟต์แวร์

๓๓. เลขที่อยู่ไอพี (IP Address) หมายถึง ตัวเลขประจำเครื่องคอมพิวเตอร์ที่ต่ออยู่ในระบบเครือข่าย ซึ่งแต่ละเครื่องจะต้องไม่ซ้ำกัน โดยประกอบด้วย ชุดของตัวเลข ๔ ส่วนสำหรับ IPv๔ หรือ ๖ ส่วนสำหรับ IPv๖ ที่คั่นด้วยเครื่องหมายจุด (.)

๓๔. อุปกรณ์กระจายสัญญาณ (Access Point) หมายถึง อุปกรณ์ที่ทำหน้าที่กระจายสัญญาณในเครือข่ายไร้สาย

๓๕. ค่าเริ่มต้น (Default) หมายถึง ค่าที่เครื่องคอมพิวเตอร์ หรือโปรแกรมได้กำหนดไว้ล่วงหน้าและนำไปใช้ได้โดยปริยาย หากไม่มีการเปลี่ยนแปลงจากผู้ใช้บริการ

๓๖. WPA (Wi-Fi Protected Access) หมายถึง ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สายที่พัฒนาขึ้นมาใหม่ ให้มีความปลอดภัยมากกว่าวิธีเดิมอย่าง WEP (Wired Equivalent Privacy)

๓๗. ไฟร์วอลล์ (Firewall) หมายถึง เทคโนโลยีป้องกันการบุกรุกจากบุคคลภายนอก เพื่อไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้ามาใช้ข้อมูลและทรัพยากรในเครือข่าย โดยอาจใช้ทั้งฮาร์ดแวร์และซอฟต์แวร์ในการรักษาความปลอดภัย

๓๘. VPN (Virtual Private Network) หมายถึง เครือข่ายคอมพิวเตอร์เสมือนที่สร้างขึ้นมาเป็นของส่วนตัว โดยในการรับส่งข้อมูลจริง จะทำโดยการเข้ารหัสเฉพาะแล้วรับ-ส่งผ่านเครือข่ายอินเทอร์เน็ต ทำให้บุคคลอื่นไม่สามารถอ่านได้และมองไม่เห็นข้อมูลนั้นไปจนถึงปลายทาง

๓๙. Web Server หมายถึง เครื่องคอมพิวเตอร์ที่ติดตั้งโปรแกรมบริการเว็บและมีหน้าที่ให้บริการเว็บเพจต่าง ๆ

๔๐. การพิสูจน์ยืนยันตัวตน (Authentication) หมายถึง ขั้นตอนการรักษาความปลอดภัยในการยืนยันตัวตนของผู้ใช้บริการก่อนใช้งาน โดยใช้ชื่อผู้ใช้ (Username) และ รหัสผ่าน (Password)

๔๑. แผนผังระบบเครือข่าย (Network Diagram) หมายถึง แผนผังซึ่งแสดงถึงการเชื่อมต่อของระบบเครือข่ายของหน่วยงาน

๔๒. Command Line หมายถึง บรรทัดที่ให้ผู้ใช้งานป้อนคำสั่งแบบข้อความเพื่อสั่งให้เครื่องคอมพิวเตอร์ทำงานตามต้องการ

๔๓. Firewall Log หมายถึง การบันทึกการสื่อสารทั้งหมดที่เกิดขึ้น ไม่ว่า Firewall จะอนุญาตให้เกิดการสื่อสารนั้นได้หรือไม่ก็ตาม ซึ่งสามารถนำมาใช้ในการวิเคราะห์เพื่อตรวจสอบประเภทของการสื่อสาร ปริมาณการสื่อสาร นอกจากนั้นแล้วยังอาจจะสะท้อนให้เห็นจำนวนครั้งที่พยายามจะบุกรุกเข้ามาภายในหน่วยงาน

๔๔. ข้อมูลจราจรทางคอมพิวเตอร์ (Log) หมายถึง ข้อมูลที่เกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิดต้นทาง-ปลายทาง/เส้นทาง/วันที่/ปริมาณ/ระยะเวลาและชนิดของบริการอื่น ๆ ที่เกี่ยวข้องในการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

๔๕. เครือข่ายสังคมออนไลน์ (Social Network) หมายถึง สังคมการติดต่อสื่อสารผ่านระบบเครือข่ายอิเล็กทรอนิกส์ เช่น Facebook, Tagged, MySpace, Orkut, Vkontakte.ru, Friendster, Line, Instagram, Webboard Blog, กระดานข่าวหรือเว็บไซต์อื่น ๆ ที่มีลักษณะการให้บริการใกล้เคียงกัน เป็นต้น

๔๖. ข้อมูลส่วนบุคคล หมายถึง ข้อมูลเกี่ยวกับสิ่งเฉพาะตัวของบุคคล เช่น ชื่อ-นามสกุล อายุ เพศ ที่อยู่ หรืออีเมล์แอดเดรส และรายละเอียดการติดต่ออื่น ๆ สถานที่ทำงานและที่อยู่ เป็นต้น

๔๗. DMZ Zone (Demilitarized Zone) หมายถึง พื้นที่ซึ่งทำหน้าที่เป็นส่วนเชื่อมระหว่าง Internet Zone และ Internal Zone ซึ่งเป็นพื้นที่ความปลอดภัยสูง การกำหนดพื้นที่ Demilitarized Zone เพื่อให้บุคคลภายนอกที่ได้รับอนุญาตสามารถติดต่อผ่านไปยัง Internal Zone ซึ่งเป็นพื้นที่จำกัดสิทธิ์และป้องกันไม่ให้บุคคลภายนอกบุกรุกเข้ามายัง Internal Zone โดยตรงเพื่อสร้างความปลอดภัยในเครือข่าย

๔๘. สถานการณ์ความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information Security Incident) หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or Unexpected) ซึ่งอาจทำให้ระบบของสำนักงาน กสม. ถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

๔๙. การรักษาความมั่นคงปลอดภัยไซเบอร์ หมายถึง มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ทั้งจากภายในและภายนอกประเทศ อันกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ

๕๐. ภัยคุกคามทางไซเบอร์ หมายถึง การกระทำ หรือการดำเนินการใด ๆ โดยมิชอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์ โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึง ที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

๕๑. ไซเบอร์ หมายถึง ข้อมูลและการสื่อสารที่เกิดจากการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต หรือโครงข่ายโทรคมนาคม รวมทั้งการให้บริการโดยปกติของดาวเทียมและระบบเครือข่ายที่คล้ายคลึงกัน ที่เชื่อมต่อกันเป็นการทั่วไป

๕๒. ประมวลแนวทางปฏิบัติ หมายถึง ระเบียบหรือหลักเกณฑ์ที่คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์กำหนด

๕๓. เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ หมายถึง เหตุการณ์ที่เกิดจากการกระทำหรือการดำเนินการใด ๆ ที่มิชอบ ซึ่งกระทำการผ่านทางคอมพิวเตอร์หรือระบบคอมพิวเตอร์ ซึ่งอาจเกิดความเสียหายหรือผลกระทบต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือความมั่นคงปลอดภัยไซเบอร์ของคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์

๕๔. มาตรการที่ใช้แก้ปัญหาเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ หมายถึง การแก้ไขปัญหาความมั่นคงปลอดภัยไซเบอร์โดยใช้บุคลากร กระบวนการ และเทคโนโลยี โดยผ่านคอมพิวเตอร์ ระบบคอมพิวเตอร์ โปรแกรมคอมพิวเตอร์ หรือบริการที่เกี่ยวกับคอมพิวเตอร์ใด ๆ เพื่อสร้างความมั่นใจและเสริมสร้างความมั่นคงปลอดภัยไซเบอร์ของคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์

ส่วนที่ ๑
นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

๑.๑ นโยบายในการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

วัตถุประสงค์ เพื่อกำหนดมาตรการควบคุมและป้องกันรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับเอกสาร สื่อบันทึกข้อมูล แฟ้มข้อมูล การเข้า-ออกพื้นที่ การนำอุปกรณ์/เครื่องคอมพิวเตอร์ออกนอกสถานที่ การทำลายเอกสารและสื่อบันทึกข้อมูล โดยมาตรการนี้จะมีผลบังคับใช้กับผู้ใช้งาน (User) ทุกประเภท รวมทั้งหน่วยงานภายนอก ซึ่งมีส่วนเกี่ยวข้องกับการเข้าถึงระบบสารสนเทศของสำนักงาน กสม.

๑.๒ แนวปฏิบัติ

การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อมเป็นการควบคุมไม่ให้สินทรัพย์สารสนเทศ อาทิ เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์หรือสารสนเทศ อยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ ดังนี้

๑.๒.๑ การควบคุมการเข้าถึงพื้นที่ทำงานทั่วไปของสำนักงาน กสม.

๑) สำนักงาน กสม. มีเวรยามรักษาอาคาร เพื่อป้องกันและตรวจสอบการเข้าสู่พื้นที่ของสำนักงาน กสม.

๒) บุคลากรที่ปฏิบัติงานในสำนักงาน กสม. จะต้องใช้บัตรประจำตัวเพื่อใช้ผ่านเข้าออกในพื้นที่ของสำนักงาน กสม.

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

๑.๒.๒ การควบคุมการเข้าถึงพื้นที่ห้องควบคุมระบบสารสนเทศ (Server room)

กำหนดให้ สำนักดิจิทัลสิทธิมนุษยชน เป็นผู้รับผิดชอบดูแลพื้นที่ห้องควบคุมระบบสารสนเทศ โดยมีหน้าที่ดังนี้

๑) จัดทำ “ทะเบียนเจ้าหน้าที่ผู้มีสิทธิเข้าออกพื้นที่” และกำหนดสิทธิให้กับเจ้าหน้าที่ผู้มีสิทธิในการเข้าถึงพื้นที่ห้องควบคุมระบบสารสนเทศ (Server room) เพื่อปฏิบัติงานตามหน้าที่ที่ได้รับมอบหมายและให้ทบทวนรายการผู้มีสิทธิถือบัตรเข้าออกพื้นที่ห้องควบคุมระบบสารสนเทศ (Server room) อย่างน้อยปีละ ๑ ครั้ง

๒) กำหนดระเบียบควบคุมการเข้า-ออกพื้นที่ห้องควบคุมระบบสารสนเทศ (Server room) และติดประกาศให้ทราบบริเวณหน้าห้องควบคุมระบบสารสนเทศ (Server room)

๓) ทำการบันทึกเวลาการผ่านเข้าออกห้องควบคุมระบบสารสนเทศ (Server room) และกำหนดผู้มีหน้าที่รับผิดชอบการบันทึกการเข้าออกดังกล่าว โดยจัดทำเป็นเอกสาร “บันทึกการผ่านเข้าออกพื้นที่ห้องควบคุมระบบสารสนเทศ (Server room) ของบุคคลภายนอก” เพื่อเป็นหลักฐานในการตรวจสอบ

๔) ควบคุมดูแลบุคคลภายนอกที่นำเครื่องคอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานระบบเครือข่ายมาใช้ภายในห้องควบคุมระบบสารสนเทศ (Server room) โดยจะต้องลงบันทึกในแบบฟอร์มการขออนุญาตตามที่กำหนดไว้ และตรวจเช็คอุปกรณ์ที่นำออกหลังจากเสร็จสิ้นการปฏิบัติงาน

๖) มีระบบสนับสนุนการทำงานระบบสารสนเทศของหน่วยงานที่จำเป็น ประกอบด้วย ระบบเครื่องปรับอากาศแบบควบคุมความชื้น ระบบสำรองไฟฟ้าอัตโนมัติ ระบบดับเพลิงอัตโนมัติด้วยก๊าช HFC ระบบตรวจจับการรั่วซึมของน้ำ ระบบกล้องวงจรปิด โดยต้องตรวจสอบหรือทดสอบระบบสนับสนุนเหล่านั้น

อย่างสม่ำเสมอ เพื่อให้มั่นใจได้ว่าระบบต่าง ๆ ทำงานตามปกติ และช่วยลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ รวมทั้งต้องดูแลให้สามารถใช้งานได้เป็นปกติ

๗) มีระบบแจ้งเตือนอัตโนมัติ เพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงานภายในห้องควบคุมระบบสารสนเทศ (Server room) ทำงานผิดปกติหรือหยุดการทำงาน ได้แก่ ระบบเครื่องปรับอากาศแบบควบคุมความชื้น ระบบสำรองไฟฟ้าอัตโนมัติ ระบบตรวจจับการรั่วซึมของน้ำ

๑.๒.๓ การนำอุปกรณ์/สินทรัพย์ของสำนักงาน กสม. ออกไปใช้นอกสำนักงาน กสม. (removal of property)

ให้ผู้อำนวยการสำนัก/หัวหน้ากลุ่มงาน มีหน้าที่ดูแลรักษาการนำอุปกรณ์/สินทรัพย์ของสำนักงาน กสม. ออกไปใช้นอกสำนักงาน กสม. โดยมีแนวปฏิบัติดังนี้

๑) ให้รับผิดชอบในการนำหรือเคลื่อนย้ายอุปกรณ์/สินทรัพย์ในหน่วยงานของตนออกไปใช้งานนอกสำนักงาน กสม.

๒) ให้กำหนดระยะเวลาของการนำอุปกรณ์/สินทรัพย์ออกไปใช้งานนอกสำนักงาน กสม.

๓) เมื่อมีการนำอุปกรณ์/สินทรัพย์ส่งคืน ให้ตรวจสอบว่าสอดคล้องกับระยะเวลาที่อนุญาตและตรวจสอบการชำรุดเสียหายของอุปกรณ์/สินทรัพย์ด้วย

๔) ให้บันทึกข้อมูลการนำอุปกรณ์/สินทรัพย์ของสำนักงาน กสม. ออกไปใช้งานนอกสำนักงาน กสม. เพื่อเอาไว้เป็นหลักฐานป้องกันการสูญหาย รวมทั้งบันทึกข้อมูลเมื่อนำอุปกรณ์/สินทรัพย์มาส่งคืน

ส่วนที่ ๒
นโยบายและแนวปฏิบัติในการเข้าถึงและควบคุมการใช้งานสารสนเทศ

๒.๑ นโยบายในการเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control)

วัตถุประสงค์ เพื่อกำหนดเป็นมาตรการในการป้องกันและควบคุมให้เกิดความปลอดภัยต่อระบบสารสนเทศของสำนักงาน กสม. โดยกำหนดแนวปฏิบัติสำหรับผู้เกี่ยวข้องในการบริหารจัดการและควบคุมการเข้าถึงระบบสารสนเทศ ระบบเครือข่าย ระบบเครือข่ายไร้สาย เครื่องคอมพิวเตอร์แม่ข่ายการใช้งานระบบปฏิบัติการ การใช้งานอินเทอร์เน็ต การใช้งานระบบจดหมายอิเล็กทรอนิกส์ การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล เพื่อป้องกันการบุกรุกผ่านระบบเครือข่ายหรือจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ที่จะสร้างความเสียหายแก่ข้อมูลหรือการทำงานของระบบสารสนเทศให้หยุดชะงัก รวมทั้งให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบสารสนเทศของสำนักงาน กสม. ได้อย่างถูกต้อง ครอบคลุมผู้ใช้งานที่ใช้งานขณะอยู่ภายในสำนักงาน และผู้ใช้งานที่ขอใช้งานขณะที่อยู่ภายนอกสำนักงาน

๒.๒ แนวปฏิบัติ

๒.๒.๑ การเข้าถึงและควบคุมการใช้งานสารสนเทศ

ผู้ดูแลระบบ หรือผู้ที่ได้รับมอบหมาย ต้องดำเนินการ ดังนี้

๑) กำหนดสิทธิการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ โดยต้องให้สิทธิเฉพาะผู้ที่เกี่ยวข้องกับข้อมูลและการปฏิบัติงานในหน้าที่เท่านั้น ทั้งนี้ ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายเท่านั้น ที่สามารถแก้ไขเปลี่ยนแปลงสิทธิการเข้าถึงสารสนเทศและระบบสารสนเทศได้

๒) ต้องทบทวนความเหมาะสมของสิทธิในการเข้าถึงของผู้ใช้งาน (review of user access rights) อย่างน้อยปีละ ๑ ครั้ง เพื่อทำการยกเลิก/เปลี่ยนแปลงสิทธิในการเข้าถึงของผู้ใช้งานระบบสารสนเทศ เมื่อมีผู้ลาออกหรือพ้นจากตำแหน่งหรือเปลี่ยนตำแหน่ง และเพื่อให้มั่นใจได้ว่าสิทธินั้น ๆ ยังคงมีความเหมาะสม ทั้งนี้ ให้สำนักบริหารกลางและสำนัก/กลุ่มงานที่บุคลากรสังกัด แจ้งผู้ดูแลระบบทราบ เพื่อทำการยกเลิกสิทธิการใช้งานต่อไป

๓) ต้องมีระบบบันทึกและติดตามการใช้งานระบบสารสนเทศของสำนักงาน กสม. (log File) และตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบข้อมูลสำคัญอย่างสม่ำเสมอ

๔) ต้องบันทึกรายละเอียดการเข้าถึงระบบจากบุคคลภายนอกและการเปิดสิทธิการใช้งานระบบต่าง ๆ ให้บุคคลภายนอก ได้แก่ การรีโมทระยะไกล และการเพิ่มรายชื่อผู้ใช้งานที่เป็นบุคคลภายนอกชั่วคราว

๕) การแบ่งประเภทของข้อมูล การจัดลำดับความสำคัญ ลำดับชั้นความลับของข้อมูลและสิทธิในการเข้าถึงการใช้งานสารสนเทศ กำหนดไว้ดังนี้

๕.๑) ประเภทของข้อมูลมีดังนี้

- ข้อมูลสารสนเทศทั่วไปตามพระราชบัญญัติข้อมูลข่าวสารของราชการ
- ข้อมูลที่มีความอ่อนไหว ได้แก่ ข้อมูลส่วนบุคคล ข้อมูลเงินเดือน ข้อมูลผู้ร้องเรียน เป็นต้น

๕.๒) จัดแบ่งลำดับชั้นความลับของข้อมูล ๔ ระดับ คือ

- ข้อมูลลับที่สุด หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด

- ข้อมูลลับมาก หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรง

- ข้อมูลลับ หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย

- ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

ทั้งนี้ ลำดับชั้นความลับของข้อมูล ให้อ้างอิงตามระบบงานสารบรรณของสำนักบริหารกลาง

๕.๓) จัดแบ่งระดับชั้นการเข้าถึง ดังนี้

- ระดับชั้นสำหรับผู้บริหาร สามารถเข้าถึงข้อมูลสารสนเทศต่าง ๆ ได้ทั้งหมด

- ระดับชั้นสำหรับผู้ดูแลระบบ หรือผู้ที่ได้มอบหมาย สามารถเข้าถึงข้อมูลได้ทุกประเภทตามที่ได้รับมอบหมาย

- ระดับชั้นสำหรับผู้ใช้งานทั่วไป สามารถเข้าถึงข้อมูลสารสนเทศที่เผยแพร่ทั่วไปได้

๕.๔) การกำหนดเวลาที่ได้เข้าถึง

- การเข้าถึงสารสนเทศในเวลาราชการ (๐๘.๓๐ – ๑๖.๓๐ น.)

- การเข้าถึงสารสนเทศในวันหยุดและนอกเวลาราชการ (นอกช่วงเวลา ๐๘.๓๐ – ๑๖.๓๐ น.)

- การเข้าถึงในช่วงเวลาที่กำหนดตามคำสั่งการต่าง ๆ เป็นกรณีพิเศษ

๕.๕) ระยะเวลาการเข้าถึง ได้แก่

- ๑ วัน

- ๑ ปีงบประมาณ

- ตามที่ระบุ/ตามที่ร้องขอ

๕.๖) การกำหนดจำนวนช่องทางที่สามารถเข้าถึง

- ติดต่อด้วยตนเอง (เข้าถึงได้ในเวลาราชการ)

- ศูนย์ข้อมูลข่าวสาร (เข้าถึงได้ในเวลาราชการ)

- โทรศัพท์หรือโทรสาร (เข้าถึงได้ในเวลาราชการ)

- หนังสือหรือบันทึกข้อความ (เข้าถึงได้ในเวลาราชการ)

- ระบบเครือข่ายภายในสำนักงาน กสม. (เข้าถึงได้ทั้งในและนอกเวลาราชการ)

- ระบบอินทราเน็ต (เข้าถึงได้ทั้งในและนอกเวลาราชการ)

- ระบบอินเทอร์เน็ต (เข้าถึงได้ทุกช่วงเวลา)

- ระบบจดหมายอิเล็กทรอนิกส์ (เข้าถึงได้ทุกช่วงเวลา)

- เว็บไซต์ (เข้าถึงได้ทุกช่วงเวลาหรือในช่วงเวลาพิเศษที่กำหนด)

๕.๗) สิทธิในการเข้าถึงการใช้งานสารสนเทศของผู้ใช้งาน ดังนี้

- สิทธิในการอ่านอย่างเดียว

- สิทธิในการสร้าง/บันทึกข้อมูล

- สิทธิในการแก้ไขเปลี่ยนแปลงข้อมูล

- สิทธิในการลบข้อมูล

- สิทธิในการอนุญาตสิทธิให้บุคคลอื่น ๆ (admin)

๒.๒.๒ การบริหารจัดการการเข้าถึงและการใช้งานระบบสารสนเทศ

๒.๒.๒.๑ ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายต้องปฏิบัติ ดังนี้

๑) จัดทำแบบฟอร์มการลงทะเบียนผู้ใช้งานใหม่

๒) ต้องลงทะเบียนการเข้าถึงระบบสารสนเทศให้กับเจ้าหน้าที่ที่ปฏิบัติงานในสำนักงาน กสม. ทุกคน และจัดเก็บไว้เป็นหลักฐาน

๓) มีขั้นตอนการลงทะเบียนผู้ใช้งาน (User Registration) ดังนี้

๓.๑) ให้เจ้าหน้าที่ใหม่กรอกแบบฟอร์มเพื่อขอรหัสผ่านในการเข้าใช้งานระบบต่าง ๆ

๓.๒) ตรวจสอบบัญชีผู้ใช้งานว่าเคยลงทะเบียนผู้ใช้งานมาก่อนหรือไม่หรือมีชื่อในระบบอยู่แล้วหรือไม่

๓.๓) พิจารณาสิทธิที่ผู้ใช้งานจะได้รับอนุญาตให้เข้าสู่ระบบ โดยให้สิทธิเฉพาะในส่วนที่จำเป็นต้องรู้ตามหน้าที่งานเท่านั้น โดยกำหนดสิทธิในการเข้าถึงตามหน้าที่และความจำเป็นขั้นต่ำเท่านั้น เนื่องจากการให้สิทธิเกินความจำเป็นในการใช้งาน จะนำไปสู่ความเสี่ยงในการใช้งานเกินอำนาจหน้าที่

๓.๔) แจ้งรหัสผู้ใช้งานและรหัสผ่านแก่ผู้ใช้งาน โดยใส่ซองจดหมายปิดผนึก

๔) ให้ทบทวนรายชื่อผู้ใช้งาน เพื่อยกเลิกเพิกถอนการอนุญาตให้เข้าถึงระบบสารสนเทศสำหรับผู้ใช้งาน เมื่อบุคลากรไม่มีความจำเป็นต้องใช้งานระบบงานต่าง ๆ ได้แก่ ลาออกหรือเปลี่ยนตำแหน่งงาน ทั้งนี้ให้สำนักบริหารกลางและสำนัก/กลุ่มงานที่บุคลากรสังกัด ทบทวนความเหมาะสมของสิทธิในการเข้าถึงข้อมูลของผู้ใช้งานอย่างน้อยปีละ ๑ ครั้ง และแจ้งสำนักดิจิทัลสิทธิมนุษยชนทราบโดยเร็ว เพื่อทำการยกเลิกสิทธิการใช้งานต่อไป

๕) ให้คำแนะนำที่ถูกต้องเบื้องต้นในการใช้งานระบบสารสนเทศต่อผู้ใช้งานเกี่ยวกับระบบและโปรแกรมที่ไม่พึงประสงค์ หรือมีความเสี่ยงที่จะเป็นอันตรายต่อระบบสารสนเทศของสำนักงาน กสม.

๖) แจ้งตักเตือนผู้ใช้งานในกรณีใช้งานที่ก่อให้เกิดความเสี่ยงที่จะเป็นอันตรายต่อระบบสารสนเทศขึ้น และหากยังไม่ปรับปรุงแก้ไขให้เสนอผู้บริหารพิจารณาต่อไป

๗) การบริหารจัดการการเข้าถึงข้อมูลสารสนเทศที่เป็นความลับของสำนักงาน กสม. ดังนี้

๗.๑) กำหนดรายชื่อผู้ใช้งาน (User Account) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูล รวมทั้งกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

๗.๒) กำหนดสิทธิในการเข้าถึงข้อมูลสารสนเทศที่เป็นความลับของสำนักงาน กสม. ได้แก่ ข้อมูลส่วนบุคคล ข้อมูลทางการเงินและบัญชี รหัสผ่านการเข้าใช้งานระบบ ข้อมูลเรื่องร้องเรียน ข้อมูลภาคีเครือข่ายสิทธิมนุษยชนประเภทบุคคล เป็นต้น

๗.๓) ต้องควบคุมการเข้าถึงข้อมูลสารสนเทศแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

๗.๔) ให้รักษาความปลอดภัยของข้อมูลลับ ในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่เพื่อไปตรวจซ่อม โดยต้องสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน หรือถอดสื่อบันทึกข้อมูลออกก่อนนำไปส่งซ่อม

๗.๕) การจัดเก็บข้อมูล Username และ Password ลงใน Active Directory (AD) ถือเป็นความลับ จะต้องเข้ารหัสด้วยมาตรฐานสากล ใน field ของ Password ในฐานข้อมูล

๗.๖) การรับส่งข้อมูลสำคัญหรือข้อมูลที่เป็นความลับผ่านระบบเครือข่ายสาธารณะ ต้องได้รับการเข้ารหัส (Encryption) ที่ปลอดภัยเป็นมาตรฐานสากล ได้แก่ SSL, VPN หรือ XML Encryption เป็นต้น

๘) การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User password management) ดังนี้

๘.๑) การส่งมอบรหัสผ่าน (Password) ชั่วคราวให้กับผู้ใช้งาน ต้องทำด้วยวิธีการที่ปลอดภัยโดยใส่ซองปิดผนึกจดหมายและไม่ใช้บุคคลอื่นถือไปให้

๘.๒) ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันทีหลังจากได้รับรหัสผ่านชั่วคราว

๘.๓) ต้องใช้รหัสผ่าน (Password) ในการเข้าใช้งานระบบ

๘.๔) ไม่ตั้งรหัสผ่านเดียวกันสำหรับระบบงานต่าง ๆ ให้ผู้ใช้งาน

๙) ให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้เฉพาะที่ได้รับอนุญาตให้เข้าถึงเท่านั้น ได้แก่ ระบบทรัพยากรบุคคล (D-Pis) ระบบสารสนเทศเพื่อการรวบรวมข้อมูลสิทธิมนุษยชน ระบบสารบรรณ ระบบรับเรื่องร้องเรียน ระบบภาคีเครือข่ายสิทธิมนุษยชน ระบบอีเมล์สำนักงาน ระบบจัดเก็บข้อมูลข่าวเพื่อการติดตามและประเมินสถานการณ์สิทธิมนุษยชน ระบบเครือข่ายภายใน (Web Portal) และระบบสมุดโทรศัพท์

๒.๒.๒.๒ ผู้ใช้งาน ต้องปฏิบัติ ดังนี้

๑) เจ้าหน้าที่ใหม่ต้องกรอกแบบฟอร์มเพื่อขอสิทธิในการเข้าใช้งานระบบต่าง ๆ ตามความจำเป็น

๒) การใช้งานรหัสผ่าน (Password use) ผู้ใช้งานปฏิบัติ ดังนี้

๒.๑) ไม่บันทึกรหัสผ่านไว้ในโปรแกรมคอมพิวเตอร์ เพื่อช่วยในการจำรหัสผ่านของตน เช่น ในโปรแกรมเว็บเบราว์เซอร์จะต้องไม่ตั้งโปรแกรมช่วยจำรหัสผ่านไว้ เป็นต้น

๒.๒) ผู้ใช้งานต้องไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

๒.๓) ไม่จดหรือบันทึกรหัสผ่านไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นโดยบุคคลอื่น

๒.๔) รหัสผ่านถือเป็นข้อมูลลับ ห้ามให้ผู้อื่นยืมใช้รหัสผ่าน กรณีที่มีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่นเพื่อให้สามารถปฏิบัติงานแทนตนเองได้ หลังจากที่ทำงานนั้นเสร็จเรียบร้อยแล้ว ให้แจ้งผู้ดูแลระบบเพื่อเปลี่ยนรหัสผ่านโดยทันที

๒.๕) ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

๒.๖) ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบเปลี่ยนรหัสผ่าน หากสงสัยว่าบัญชีผู้ใช้งานหรือรหัสผ่านของตนถูกละเมิด

๓) การกำหนดและวิธีการเปลี่ยนรหัสผ่านที่มีคุณภาพ ดังนี้

๓.๑) หลีกเลี่ยงการใช้รหัสผ่านเดิมซ้ำ ๆ

๓.๒) ตั้งรหัสผ่านที่ยากต่อการคาดเดา

๓.๓) กำหนดรหัสผ่านให้มีตัวอักษรหรือตัวเลข อย่างน้อย ๘ ตัวอักษร

๓.๔) ไม่กำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเอง จากบุคคลในครอบครัวหรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน จากคำศัพท์ที่ใช้ในพจนานุกรมหรือหมายเลขโทรศัพท์

๓.๕) ไม่ตั้งรหัสผ่านจากอักขระที่เรียงกันหรือกลุ่มเหมือนกัน

๓.๖) ไม่ใช้คำในพจนานุกรม

๓.๗) กำหนดรหัสผ่านให้ประกอบด้วยตัวอักษรพิมพ์ใหญ่ พิมพ์เล็ก ตัวเลขและตัวอักขระพิเศษ อย่างน้อย ๑ ตัวอักขระ

๓.๘) ไม่ตั้งรหัสผ่านเป็นรูปแบบ (Pattern) ที่นิยมใช้กันทั่วไป

๒.๒.๓ การควบคุมการเข้าถึงเครือข่าย

๒.๒.๓.๑ สำนักดิจิทัลสิทธิมนุษยชน ต้องดำเนินการ ดังนี้

๑) กำหนดบุคคลที่รับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่า parameter ต่าง ๆ ของระบบเครือข่ายและอุปกรณ์ต่าง ๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจน และทบทวนการกำหนดค่า parameter ต่าง ๆ อย่างน้อยปีละ ๑ ครั้ง

๒) การใช้เครื่องมือต่าง ๆ (Tools) เพื่อตรวจสอบระบบเครือข่าย ต้องได้รับการอนุญาตจากผู้อำนวยการสำนักดิจิทัลสิทธิมนุษยชนเป็นลายลักษณ์อักษร

๒.๒.๓.๒ ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมาย ต้องดำเนินการ ดังนี้

๑) ให้ระบุอุปกรณ์บนเครือข่าย (Equipment identification in networks) เพื่อบ่งบอกว่าการเชื่อมต่อนั้นมาจากอุปกรณ์หรือสถานที่ที่ได้รับอนุญาตแล้ว ดังนี้

๑.๑) ผู้ขอใช้บริการต้องกรอกแบบฟอร์มเพื่อขอใช้บริการเชื่อมต่อเครือข่ายภายในสำนักงาน กสม.

๑.๒) อุปกรณ์เครือข่ายต้องสามารถตรวจสอบ IP Address ของทั้งต้นทางและปลายทางได้

๑.๓) ผู้ดูแลระบบต้องเก็บบัญชีผู้ขอใช้บริการเครือข่าย

๑.๔) ใช้ MAC Address และ IP Address ในการระบุอุปกรณ์บนเครือข่าย

๑.๕) ให้จัดทำทะเบียนสินทรัพย์อุปกรณ์ด้านเทคโนโลยีสารสนเทศ

๒) การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (remote diagnostic and configuration port protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ ดังนี้

๒.๑) ต้องกำหนดการเปิด–ปิด พอร์ตของอุปกรณ์เครือข่ายเพื่อควบคุมการเข้าถึงต่อพอร์ตของอุปกรณ์เครือข่ายต่าง ๆ โดยจะปิดพอร์ตที่เสี่ยงที่จะก่อให้เกิดความเสียหายต่อระบบเครือข่าย

๒.๒) บุคคลภายนอกเข้ามาดำเนินการบำรุงรักษา บริหารจัดการพอร์ตของอุปกรณ์เครือข่ายหรือบริหารจัดการผ่านระบบเครือข่าย ต้องได้รับการอนุญาตจากเจ้าหน้าที่สำนักดิจิทัลสิทธิมนุษยชนก่อน

๒.๓) ต้องยกเลิกหรือปิดพอร์ตและบริการบนอุปกรณ์เครือข่ายที่ไม่มีความจำเป็นในการใช้งาน

๓) ให้แบ่งแยกเครือข่าย (Segregation in networks) พื้นที่การทำงานของระบบเครือข่ายอย่างน้อย ๒ โซน คือ โซนภายใน (Internal Zone) และโซนภายนอก (External Zone) เพื่อควบคุมการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาตและป้องกันการบุกรุกทางเครือข่ายจากผู้ไม่หวังดี

๔) การควบคุมการเชื่อมต่อทางเครือข่าย (network connection control) ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกัน ดังนี้

๔.๑) ให้จำกัดสิทธิ์การใช้งาน เพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

๔.๒) ทำการตรวจสอบการเชื่อมต่อเครือข่าย และระบุอุปกรณ์/เครื่องมือที่ใช้ควบคุมการเชื่อมต่อเครือข่ายอย่างสม่ำเสมอ อย่างน้อยเดือนละ ๑ ครั้ง

๔.๓) ระบบเครือข่ายทั้งหมดของสำนักงาน กสม. ที่เชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกสำนักงาน กสม. ให้เชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก (Firewall) หรือโปรแกรมในการทำ Packet filtering

๔.๔) มีระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานระบบเครือข่ายของสำนักงาน กสม. ในลักษณะที่ผิดปกติ โดยต้องตรวจสอบการบุกรุกผ่านระบบเครือข่าย การแก้ไขเปลี่ยนแปลงระบบเครือข่ายโดยผู้บุกรุก

๔.๕) มีวิธีการจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องลูกข่ายไปยังเครื่องแม่ข่ายเพื่อไม่ให้ผู้ใช้สามารถใช้เส้นทางอื่นได้

๔.๖) จำกัดเส้นทางการเข้าถึงเครือข่ายที่ต้องใช้งานร่วมกัน

๕) การควบคุมการจัดเส้นทางบนเครือข่าย (network routing control) ต้องควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศดังนี้

๕.๑) กำหนดให้แปลงหมายเลขเครือข่าย เพื่อแยกเครือข่ายย่อย

๕.๒) กำหนดเส้นทางเครือข่าย เพื่อใช้เชื่อมต่อเครือข่ายระหว่างปลายทาง ผ่านช่องทางที่กำหนดไว้

๕.๓) ให้ตรวจสอบการเชื่อมต่อเข้าสู่เครือข่ายและจำกัดสิทธิความสามารถของผู้ใช้งานในการเชื่อมต่อเครือข่าย

๖) จำกัดระยะเวลาการเชื่อมต่อระบบเครือข่าย (Session Time-out) ในกรณีไม่มีการใช้งาน ๔๐ นาที ระบบจะตัดการเชื่อมต่อระบบเครือข่ายเมื่อผู้ใช้งานประสงค์จะเข้าใช้งานใหม่ ต้องพิสูจน์ยืนยันตัวตน (Authentication) อีกครั้ง เพื่อให้เกิดความปลอดภัย

๗) ต้องป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อระบบเครือข่ายสำนักงาน กสม. สามารถมองเห็นเลขที่อยู่ไอพี IP Address ภายใน (Local IP) ของระบบงานเครือข่ายภายในของสำนักงาน กสม. ได้ เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายและส่วนประกอบของเทคโนโลยีสารสนเทศได้โดยง่าย

๘) จัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับเครือข่ายภายใน เครือข่ายภายนอกและอุปกรณ์ต่าง ๆ พร้อมทั้งทบวนปรับปรุงให้เป็นปัจจุบันเสมออย่างน้อยปีละ ๑ ครั้ง

๒.๒.๓.๓ ผู้ใช้งานต้องดำเนินการ ดังนี้

๑) ทำการ Login เพื่อยืนยันตัวตน (Authentication) ก่อนเข้าสู่ระบบเครือข่ายของสำนักงาน กสม. โดยผ่านทางอินเทอร์เน็ตและเมื่อไม่ได้ใช้งานเกิน ๔๐ นาที ระบบจะตัดการเชื่อมต่อระบบเครือข่าย ให้ผู้ใช้งานทำการยืนยันตัวตน (Authentication) อีกครั้ง

๒) ผู้ใช้งานต้องเป็นผู้รับผิดชอบผลเสียหายต่าง ๆ อันอาจจะเกิดมีขึ้น จากบัญชีผู้ใช้งาน (User Account) ของตน เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

๒.๒.๔ การบริหารจัดการเครื่องคอมพิวเตอร์แม่ข่าย

๒.๒.๔.๑ สำนักดิจิทัลสิทธิมนุษยชนต้องดำเนินการดังนี้

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

๒) มีขั้นตอนหรือวิธีปฏิบัติในการตรวจสอบเครื่องคอมพิวเตอร์แม่ข่าย และในกรณีที่พบว่ามีการใช้งานหรือเปลี่ยนแปลงค่าในลักษณะผิดปกติ ต้องดำเนินการแก้ไข รวมทั้งการรายงานหรือแจ้งผู้อำนวยการสำนักดิจิทัลสิทธิมนุษยชนโดยทันที

๒.๒.๔.๒ ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมาย ต้องดำเนินการ ดังนี้

๑) เปิดใช้บริการ (Service) พื้นฐาน http และ https เท่านั้น หากจำเป็นใช้บริการนอกเหนือจากที่กำหนดให้พิจารณาเป็นกรณี ๆ ไป

๒) ดำเนินการติดตั้งและอัพเดทระบบซอฟต์แวร์ให้เป็นปัจจุบัน เพื่ออุดช่องโหว่ต่าง ๆ ของโปรแกรมระบบ (System Software)

๓) กำหนดให้บันทึกการทำงานของเครื่องคอมพิวเตอร์แม่ข่าย ดังนี้

๓.๑) บันทึกการปฏิบัติงานของผู้ใช้งาน (Application logs)

๓.๒) บันทึกการเข้าระบบ (Login logs)

๒.๒.๕ การบริหารจัดการการบันทึกและตรวจสอบการทำงานของระบบสารสนเทศ

ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายต้องดำเนินการ ดังนี้

๑) ต้องจัดเก็บบันทึกการทำงานของระบบคอมพิวเตอร์แม่ข่ายและเครือข่ายบันทึกการปฏิบัติงานของผู้ใช้งาน (Application logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก ได้แก่ บันทึกการเข้าออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน command line และ Firewall Log เพื่อให้เป็นไปตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม และเพื่อประโยชน์ในการตรวจสอบกรณีมีปัญหา โดยต้องเก็บบันทึกไว้อย่างน้อย ๙๐ วัน

๒) ต้องตรวจสอบบันทึกการทำงานตามข้อ ๑) อย่างสม่ำเสมอ

๓) จำกัดสิทธิในการเข้าถึงบันทึกการทำงานต่าง ๆ ตามข้อ ๑) เฉพาะผู้เกี่ยวข้องเท่านั้น เพื่อป้องกันการแก้ไขเปลี่ยนแปลงบันทึก

๔) ต้องกำหนดสิทธิ์ในการเข้าถึงข้อมูลแยกจากกันระหว่างผู้ดูแลระบบ (Admin) กับผู้ใช้งาน (User)

๒.๒.๖ การปฏิบัติงานจากภายนอกสำนักงาน กสม. (teleworking)

๒.๒.๖.๑ ผู้ดูแลระบบหรือผู้ได้รับมอบหมายต้องดำเนินการ ดังนี้

๑) กรณีเป็นบุคลากรของสำนักงาน กสม. ให้ติดต่อสำนักดิจิทัลสิทธิมนุษยชนเพื่อกรอกแบบฟอร์มขอรหัสผู้ใช้งานและรหัสผ่านเพื่อทำการเข้าสู่ระบบจากระยะไกลโดยผ่านระบบ VPN โดยต้องระบุเหตุผลหรือความจำเป็นในการใช้งาน

๒) กรณีเป็นบุคคลภายนอก (บริษัท/หน่วยงานภายนอก)

๒.๑) ให้บุคคลภายนอกติดต่อสำนักดิจิทัลสิทธิมนุษยชน เพื่อกรอกแบบฟอร์มขออนุญาตใช้งานพร้อมระบุเหตุผลหรือความจำเป็นในการใช้งาน

๒.๒) ต้องกำหนดให้ยืนยันตัวตน (User authentication for external connections) ด้วยชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ก่อนเข้าใช้งาน

๒.๓) กำหนดให้ใช้งานผ่านระบบ Remote Control หรือระบบ VPN

๓) ต้องดูแลตรวจสอบตลอดระยะเวลาที่มีการเข้าใช้จากภายนอกและปิดพอร์ตทันทีที่ไม่มีการเชื่อมต่อการใช้งาน

๔) ต้องควบคุมพอร์ต (Port) ที่ใช้ในการเข้าสู่จากภายนอกระบบอย่างรัดกุม

๒.๒.๖.๒ ผู้ใช้งานต้องดำเนินการ ดังนี้

๑) ขออนุญาตใช้งานระบบผ่านทางสำนักดิจิทัลสิทธิมนุษยชน โดยต้องระบุเหตุผลหรือความจำเป็นในการขอเข้าใช้งานทุกครั้ง

๒) ต้องพิสูจน์ยืนยันตัวตน (Authentication) โดยใช้รหัสผู้ใช้งานและรหัสผ่านที่กำหนดไว้ก่อนเข้าใช้งาน

๒.๒.๗ การควบคุมการเข้าถึงเครือข่ายไร้สาย (Wireless LAN Access Control)

๒.๒.๗.๑ ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายต้องดำเนินการ ดังนี้

๑) ต้องตรวจสอบสัญญาณอย่างน้อยทุก ๆ ๓ เดือน เพื่อทดสอบการทำงานและความแรงของสัญญาณ

๒) ต้องเปลี่ยนค่าชื่ออุปกรณ์ไร้สาย และรหัสผ่านในการเข้าตั้งค่าการทำงานของอุปกรณ์ไร้สาย โดยเลือกใช้ชื่อ Login และรหัสผ่านที่มีความคาดเดาได้ยาก เพื่อป้องกันผู้โจมตีไม่ให้สามารถเดาหรือเจาะรหัสได้โดยง่าย

๓) ต้องกำหนดค่าใช้ Web หรือ WPA ในการเข้ารหัสหรือข้อมูลระหว่าง Wireless LAN Client และ AP เพื่อให้ยากต่อการดักจับจะช่วยให้ปลอดภัยมากขึ้น

๔) ต้องแบ่ง Virtual Lan (VLAN) ระหว่างเครือข่ายไร้สายกับเครือข่ายภายในของสำนักงาน กสม. เพื่อความปลอดภัยในการใช้งาน

๕) ต้องตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยที่เกิดขึ้นในระบบเครือข่ายไร้สายเป็นประจำทุก ๓ เดือน

๖) ต้องกำหนดรหัสผู้ใช้และรหัสผ่านในการเข้าใช้งานเครือข่ายไร้สาย (Wireless LAN) ของสำนักงาน กสม. รวมถึงกำหนดระยะเวลาในการเข้าใช้งานให้กลุ่มบุคคลต่าง ๆ ดังนี้

๖.๑) ผู้ปฏิบัติงานในสำนักงาน กสม. สามารถใช้งานได้ตลอดเวลาจนกว่าจะลาออกหรือเกษียณอายุราชการ

๖.๒) บุคคลที่มีหน้าที่ดำเนินการตามสัญญาว่าจ้างหรือปฏิบัติงานตามที่ได้รับมอบหมายจากสำนักงาน หรือที่ปรึกษา หรือคณะอนุกรรมการ สามารถใช้ระบบเครือข่ายไร้สายได้ไม่จำกัดระยะเวลาจนกว่าจะสิ้นสุดสัญญาว่าจ้าง หรือสิ้นสุดภาระงานตามที่ได้รับมอบหมายหรือหมดวาระการเป็นกรรมการ/อนุกรรมการ

๖.๓) บุคคลภายนอก ที่เป็นผู้เข้าร่วมประชุม หารือ สัมมนาที่สำนักงาน กสม. จัดขึ้น สามารถใช้ระบบเครือข่ายไร้สายได้ต่อเนื่องไม่เกิน ๘ ชั่วโมง และจะสิ้นสุดการให้บริการในเวลา ๑๖.๓๐ น. ในกรณีพบความผิดปกติ หรือพบการใช้งานที่ผิดปกติให้ตักเตือนและบันทึกข้อมูลไว้เป็นหลักฐาน

๒.๒.๗.๓ ผู้ใช้งานต้องปฏิบัติ ดังนี้

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

๒) ผู้ใช้งานที่เป็นบุคคลภายนอกหรือผู้เข้าร่วมประชุมสัมมนา หากประสงค์ใช้งานระบบเครือข่ายไร้สาย (Wireless LAN) ของสำนักงาน กสม. ให้ติดต่อขอรับรหัสผ่านได้ที่สำนักดิจิทัลสิทธิมนุษยชน โดยผู้ขอใช้งานต้องระบุชื่อ – นามสกุล ในแบบฟอร์มขอใช้งานระบบเครือข่ายไร้สาย (Wireless LAN) ส่งให้สำนักดิจิทัลสิทธิมนุษยชนบันทึกเก็บไว้ด้วย

๒.๒.๘ การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์พกพา (Personal Computer and Notebook)

๒.๒.๘.๑ ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายต้องดำเนินการ ดังนี้

๑) ติดตั้งโปรแกรมลงบนเครื่องคอมพิวเตอร์ของสำนักงาน กสม. โดยต้องเป็นโปรแกรมที่สำนักงาน กสม. ได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย

๒) กำหนดชื่อเครื่องคอมพิวเตอร์ (Computer name) ของสำนักงาน กสม.

๓) ติดตั้งซอฟต์แวร์ป้องกันไวรัสในเครื่องคอมพิวเตอร์ของสำนักงาน กสม.

๒.๒.๘.๒ ผู้ใช้งานต้องควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear Desk and Clear Screen Policy) ในความรับผิดชอบของตน ไม่ให้อยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ไม่มีสิทธิ โดยปฏิบัติดังนี้

๑) ดูแลเครื่องคอมพิวเตอร์ในครอบครองของตนไม่ให้สูญหาย

๒) กำหนดรหัสผ่าน (Password) ในการเข้าใช้งานเครื่องคอมพิวเตอร์ที่ตนเองใช้งานอยู่

๓) ห้ามแก้ไขค่าการปรับปรุง Security Patch ของระบบปฏิบัติการและค่าพื้นฐานด้านความปลอดภัยของเครื่องคอมพิวเตอร์ที่ผู้ดูแลระบบตั้งไว้

๔) ห้ามลบ หรือปิดการใช้งานซอฟต์แวร์ป้องกันไวรัสที่สำนักงาน กสม. ติดตั้งไว้

๕) ห้ามทำการติดตั้งโปรแกรมละเมิดลิขสิทธิ์ในเครื่องคอมพิวเตอร์ของสำนักงาน กสม.

๖) ไม่เก็บข้อมูลที่เป็นความลับของสำนักงาน กสม. ไว้บนเครื่องคอมพิวเตอร์ของสำนักงาน กสม. ที่ใช้งานอยู่ หรือเก็บไว้บนเครื่องคอมพิวเตอร์พกพา (Notebook) ของสำนักงาน กสม.

๗) ไม่สร้าง Short-cut หรือปุ่มกดง่ายบน Desktop ที่เชื่อมต่อไปยังข้อมูลที่เป็นความลับของสำนักงาน กสม.

๘) ต้องตรวจสอบเพื่อหาไวรัสจากสื่อบันทึกข้อมูลต่าง ๆ เช่น สื่อบันทึกพกพา (Flash Drive) และ External Hard Disk เป็นต้น ก่อนใช้งาน

๙) ไม่ควรนำอาหารและเครื่องดื่มมารับประทานอยู่ใกล้บริเวณเครื่องคอมพิวเตอร์

๑๐) ไม่วางสื่อแม่เหล็กไว้ใกล้หน้าจอเครื่องคอมพิวเตอร์หรือฮาร์ดดิสก์

๑๑) การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ ผู้ใช้งานต้องปฏิบัติดังนี้

๑๑.๑) ต้อง log out ออกจากระบบเทคโนโลยีสารสนเทศหลังจากเสร็จสิ้นการใช้งานทันที

๑๑.๒) เมื่อไม่ได้ใช้งานเครื่องคอมพิวเตอร์หรืออยู่ที่โต๊ะคอมพิวเตอร์เกิน ๓๐ นาที ต้องออกจากระบบ (Logout) หรือ ปิดเครื่องคอมพิวเตอร์ หรือล็อคหน้าจอด้วยโปรแกรมถนอมหน้าจอ (Screen Saver)

๒.๒.๙ การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating system access control)

๒.๒.๙.๑ ผู้ดูแลระบบ หรือผู้ที่ได้รับมอบหมายต้องดำเนินการ ดังนี้

๑) ตรวจสอบและทำการตั้งค่าการปรับปรุง Security Patch ของระบบปฏิบัติการโดยอัตโนมัติเพื่อความปลอดภัยในการใช้งาน

๒) ทำการอัพเดทเว็บเบราว์เซอร์เพื่ออุดช่องโหว่ของเว็บเบราว์เซอร์และเพื่อความปลอดภัยในการใช้งานเว็บเบราว์เซอร์

๓) จำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection Time) สำหรับระบบสารสนเทศหรือโปรแกรมที่มีความเสี่ยงหรือความสำคัญสูง เพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้น โดยถ้าเว้นว่างจากการใช้งานเกิน ๑๕ นาที ระบบจะตัดการเชื่อมต่อ

๔) มีขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยแสดงวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย โดยมีแนวปฏิบัติ ดังนี้

๔.๑) ต้องควบคุมไม่ให้ระบบแสดงรายละเอียดสำคัญหรือความผิดพลาดต่าง ๆ ของระบบก่อนที่การเข้าสู่ระบบจะเสร็จสมบูรณ์

๔.๒) ระบบสามารถยุติการเชื่อมต่อจากเครื่องปลายทางได้ เมื่อพบการพยายามคาดเดารหัสผ่านจากเครื่องปลายทาง

๔.๓) ไม่อนุญาตให้เชื่อมต่อโดยตรงสู่ระบบปฏิบัติการผ่านทาง Command Line เนื่องจากอาจสร้างความเสียหายให้กับระบบได้

๕) การระบุและยืนยันตัวตนของผู้ใช้งาน (user identification and authentication) ต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสมเพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง ดังนี้

๕.๑) ผู้ใช้งานทุกคนต้องมีชื่อผู้ใช้งานของแต่ละบุคคล เพื่อใช้ในการพิสูจน์ตัวตนที่แตกต่างกัน

๕.๒) ผู้ใช้งานต้องทำการยืนยันตัวตนทุกครั้งเมื่อเข้าใช้งานระบบ โดยใช้ชื่อผู้ใช้งาน (User name) และรหัสผ่าน (Password) เพื่อป้องกันผู้ไม่มีสิทธิ์เข้าใช้งานระบบ

๖) มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ ดังนี้

๖.๑) การตั้งชื่อผู้ใช้งานและรหัสผ่าน ห้ามกำหนดชื่อผู้ใช้งานและรหัสผ่านเป็นตัวเดียวกัน

๖.๒) รหัสผ่านกำหนดให้มีตัวอักษรหรือตัวเลข อย่างน้อย ๘ ตัวอักษร

๒.๒.๑๐ การใช้งานอินเทอร์เน็ต (Use of the Internet) และเครือข่ายสังคมออนไลน์

๒.๒.๑๐.๑ ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายต้องดำเนินการ ดังนี้

๑) ต้องติดตั้งโปรแกรมตรวจสอบไวรัส (Virus scanning) เพื่อป้องกันไวรัสที่ติดมากับข้อมูลที่ส่งผ่านทางอินเทอร์เน็ตได้

๒) จัดให้มีระบบจัดการผู้ใช้งาน (Active Directory) เพื่อใช้ยืนยันตัวตนก่อนเข้าใช้งานอินเทอร์เน็ตของสำนักงาน กสม.

๓) กำหนดสิทธิให้กับผู้ใช้งานอินเทอร์เน็ตตามระยะเวลา ดังนี้

๓.๑) เวลาราชการ (๘.๓๐ – ๑๒.๐๐ น. , ๑๓.๐๐ – ๑๖.๓๐ น.) จะจำกัดการใช้งานแอปพลิเคชันบางประเภท เช่น YouTube เป็นต้น เพื่อไม่ให้มีกระทบกับการใช้งานอินเทอร์เน็ตโดยส่วนรวม หากมีความจำเป็นต้องใช้งาน ให้แจ้งสำนักดิจิทัลสิทธิมนุษยชนเพื่อเปิดการใช้งานเป็นกรณี ๆ ไป

๓.๒) เวลาอื่น ๆ นอกเหนือจากเวลาราชการ จะเปิดให้ใช้บริการตามปกติ ยกเว้นแอปพลิเคชัน ประเภท Peer to Peer (ได้แก่ Bit torrent และโปรแกรมดาว์นโหลดต่าง ๆ download manager) จะไม่เปิดให้ใช้งาน

๔) กรณีระบบได้แจ้งเตือนหรือระบบบล็อกการใช้งานอินเทอร์เน็ตของผู้ใช้งาน สำนักดิจิทัลสิทธิมนุษยชนจะดำเนินการตรวจสอบ/แก้ไข หากพบการใช้งานไม่เหมาะสม/ไม่ถูกต้อง จะแจ้งเตือนผู้ใช้งานให้ทราบโดยวาจาหรือลายลักษณ์อักษร

๒.๒.๑๐.๒ ผู้ใช้งานต้องปฏิบัติ ดังนี้

๑) ผู้ใช้งานต้องใส่รหัสผ่านเพื่อยืนยันตัวตน (Authentication) ก่อนเข้าใช้งานอินเทอร์เน็ต

๒) ต้องไม่ดาวน์โหลดโปรแกรมใช้งานใด ๆ ที่มีลิขสิทธิ์จากอินเทอร์เน็ตมาใช้งาน หากมีความจำเป็นต้องดาวน์โหลดต้องเป็นไปโดยไม่ละเมิดทรัพย์สินทางปัญญา

๓) ห้ามนำข้อมูลที่เป็นความลับของสำนักงาน กสม. สื่อสารผ่านทางอินเทอร์เน็ตของสำนักงาน กสม.

๔) ต้องตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนอินเทอร์เน็ตก่อนนำข้อมูลไปใช้งาน

๕) ต้องไม่ใช้อินเทอร์เน็ตของสำนักงาน กสม. เข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรมอันดีงาม เว็บไซต์ที่มีเนื้อหาสร้างความแตกแยก หรือบ่อนทำลายต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม เป็นต้น

<u>ทั้งนี้ การใช้งานอินเทอร์เน็ตในทางที่ผิด อาจถือว่าเป็นความผิดทางวินัยและอาจถูกดำเนินคดีตามกฎหมายทั้งทางแพ่งและอาญา</u>

๖) ไม่เผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันเป็นเท็จ ลักษณะอันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร ลักษณะอันเป็นความผิดเกี่ยวกับการก่อการร้าย ผ่านสื่ออินเทอร์เน็ตของสำนักงาน กสม.

๗) ไม่เผยแพร่หรือส่งต่อข้อมูลที่ไม่เหมาะสมทางศีลธรรม หรือลักษณะลามกอนาจาร ผ่านสื่ออินเทอร์เน็ตของสำนักงาน กสม.

๘) ไม่เผยแพร่หรือส่งต่อข้อมูลที่เป็นภาพของผู้อื่นและภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์ หรือวิธีการอื่นใด ซึ่งจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ผ่านสื่ออินเทอร์เน็ตของสำนักงาน กสม.

๙) ในการเสนอความคิดเห็นผ่านสื่ออินเทอร์เน็ต ต้องไม่ใช้ข้อความเชิงยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสีย ต่อชื่อเสียงของสำนักงาน กสม. หรือทำลายความสัมพันธ์กับเจ้าหน้าที่ของหน่วยงานอื่น ๆ

๑๐) ไม่ตั้งเว็บเบราว์เซอร์ให้จดจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Auto Save Password) ของอินเทอร์เน็ต

๑๑) ระมัดระวังการใช้งานเครือข่ายสังคมออนไลน์โดยไม่ใช้งานดังต่อไปนี้

๑๑.๑) การนำเสนอข้อมูลข่าวสารผ่านเครือข่ายสังคมออนไลน์ ต้องไม่เป็นการสร้างความเกลียดชังระหว่างคนในสังคม ไม่ยุยงให้เกิดความรุนแรง จนนำไปสู่ความขัดแย้งหรือความเสียหายขึ้นในสังคม

๑๑.๒) การนำเสนอข้อมูลข่าวสารของสำนักงานกสม. ต้องใช้หลักความถูกต้องและการใช้ภาษาที่เหมาะสม หลีกเลี่ยงการแสดงความคิดเห็นส่วนบุคคลในเรื่องที่เกี่ยวกับการดำเนินงานของสำนักงาน กสม. ในลักษณะที่อาจก่อให้เกิดความเข้าใจที่คลาดเคลื่อนจากความเป็นจริง

๑๑.๓) การเผยแพร่ข้อมูลข่าวสารผ่านเครือข่ายสังคมออนไลน์ ต้องไม่ละเมิดลิขสิทธิ์ของข้อมูล ภาพ หรือวีดิทัศน์ของผู้อื่น พึงตระหนักและรับรู้สิทธิ หรือลิขสิทธิ์ของบุคคล หรือองค์กรผู้เป็นเจ้าของข้อมูลเสมอ

๑๑.๔) ต้องมีความตระหนักในเรื่องความมั่นคงปลอดภัยอยู่เสมอและต้องรับผิดชอบหากเกิดความเสียหายใด ๆ ที่มีผลกระทบกับสำนักงาน กสม. จากการใช้งานเครือข่ายสังคมออนไลน์

๑๑.๕) ต้องไม่เปิดเผยข้อมูลที่สำคัญ ข้อมูลเฉพาะส่วนบุคคล หรือนำข้อมูลที่เป็นความลับของสำนักงาน กสม. สื่อสารผ่านทางอินเทอร์เน็ตของสำนักงาน กสม.

๑๑.๖) ไม่เปิดเผยข้อมูลที่เป็นความลับ ในการพูดคุยแลกเปลี่ยนกับชุมชนออนไลน์ รวมถึงการโพสต์ข้อความที่เกี่ยวข้องกับงานประจำเป็นสิ่งที่บุคคลสามารถกระทำได้ ถ้าไม่ขัดต่อหลักจรรยาบรรณองค์กร เว้นแต่ข้อมูลนั้นเป็นข้อมูลที่มีความสำคัญหรือเป็นความลับขององค์กร ซึ่งห้ามเปิดเผยโดยเด็ดขาดเช่น ข้อมูลส่วนบุคคลของบุคลากรสำนักงาน กสม. เป็นต้น

๑๑.๗) ไม่โพสต์ข้อความที่เป็นเท็จ หรือก่อให้เกิดความเข้าใจผิดและระบุที่มาของข้อมูลนั้นอย่างชัดเจน การโพสต์ข้อความใด ๆ ควรพิจารณาเนื้อหาอย่างรอบคอบและระมัดระวัง โดยเฉพาะการเปิดเผยข้อมูลส่วนบุคคล

๑๑.๘) ไม่ละเมิดกฎหมายลิขสิทธิ์และทรัพย์สินทางปัญญาของผู้อื่น รวมทั้งขององค์กรเอง ทั้งนี้ การอ้างอิงคำพูดหรือข้อมูลของผู้อื่น ควรใช้ข้อความที่คัดลอกมาสั้น ๆ เท่านั้น และควรระบุถึงที่มาของแหล่งข้อมูลหรือเจ้าของผลงานเสมอ การเชื่อมลิงค์ไปยังงานของเจ้าของข้อมูลถือเป็นการปฏิบัติที่เหมาะสมกว่าการคัดลอกข้อมูลมาใช้งาน

๒.๒.๑๑ การใช้งานจดหมายอิเล็กทรอนิกส์ (Electronic Mail)

๒.๒.๑๑.๑ ผู้ดูแลระบบ หรือผู้ที่ได้รับมอบหมายต้องดำเนินการ ดังนี้

๑) ต้องกำหนดรหัสผู้ใช้งานและรหัสผ่านให้กับผู้ใช้งาน

๒) การกำหนดรหัสผู้ใช้งานและรหัสผ่านสำหรับใช้งานครั้งแรก เป็นไปตามคู่มือระบบจดหมายอิเล็กทรอนิกส์ (E-mail)

๒.๒.๑๑.๒ ผู้ใช้งานต้องปฏิบัติ ดังนี้

๑) หลังจากผู้ใช้งานเข้าสู่ระบบในครั้งแรกแล้ว ให้เปลี่ยนรหัสผ่านเองโดยทันที รายละเอียดตามคู่มือจดหมายอิเล็กทรอนิกส์ (E-mail)

๒) หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้นแล้ว ต้องทำการ Logout ออกจากระบบ เพื่อป้องกันบุคคลอื่นเข้าใช้งานระบบจดหมายอิเล็กทรอนิกส์

๓) ตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ (Inbox) เป็นประจำและลบจดหมายที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้เนื้อที่ระบบจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจำนวนน้อยที่สุด

๔) ต้องระวังการเปิดข้อความที่ได้รับหรือส่งจดหมายอิเล็กทรอนิกส์ตอบกลับจากผู้ส่งที่ไม่รู้จัก

๕) ต้องตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์ หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัสก่อนใช้งานทุกครั้ง

๖) ห้ามใช้ระบบจดหมายอิเล็กทรอนิกส์ของสำนักงาน กสม. ในการสร้างความน่ารำคาญต่อผู้อื่น หรือละเมิดลิขสิทธิ์ หรือในเชิงผิดกฎหมาย หรือละเมิดศีลธรรม

๗) ห้ามส่งข้อความที่ไม่เหมาะสม ไม่สุภาพ หรือทำให้เกิดความแตกแยก ระหว่างสำนักงาน กสม. หรือส่งข้อมูลอันอาจทำให้สำนักงาน กสม. เสื่อมเสียชื่อเสียง ผ่านระบบจดหมายอิเล็กทรอนิกส์ของสำนักงาน กสม.

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

๒.๒.๑๒ การบริหารจัดการไฟร์วอลล์ (Firewall) และระบบการตรวจสอบผู้บุกรุก

๒.๒.๑๒.๑ สำนักดิจิทัลสิทธิมนุษยชน ต้องดำเนินการ ดังนี้

๑. กำหนดให้จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้าออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน command line บันทึก Application Log และบันทึก Firewall Log เป็นต้น เพื่อให้เป็นไปตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และประโยชน์ในการใช้ตรวจสอบ โดยต้องเก็บข้อมูลจราจรดังกล่าว ไว้อย่างน้อย ๙๐ วัน

๒.๒.๑๒.๒ ผู้ดูแลระบบ หรือผู้ที่ได้รับมอบหมายต้องดำเนินการ ดังนี้

๑) ติดตามและวิเคราะห์เหตุการณ์ด้านความมั่นคงปลอดภัยที่เกิดขึ้นในระบบเครือข่ายและพฤติกรรมของผู้ใช้

๒) ตรวจสอบการกำหนดค่าระดับความปลอดภัยไฟร์วอลล์และระบบการตรวจสอบผู้บุกรุกที่ใช้งานอยู่ในปัจจุบันอย่างน้อยทุก ๆ ๓ เดือน

๓) ต้องสำรองข้อมูลการกำหนดค่าต่าง ๆ ของอุปกรณ์ไฟร์วอลล์เป็นประจำทุก ๓ เดือน หรือทุกครั้งที่เปลี่ยนแปลงการตั้งค่า

๔) ตรวจสอบบันทึกของข้อมูลจราจรทางคอมพิวเตอร์ (Log) เพื่อป้องกันสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดคิด และตรวจสอบรายงานของไฟร์วอลล์ ดังต่อไปนี้

๔.๑) สถิติการป้องกันข้อมูลที่ส่งผ่านทางอินเทอร์เน็ต (block packet)

๔.๒) สถิติข้อมูลหมายเลข IP ที่ส่งผ่านทางอินเทอร์เน็ตที่ถูก block ว่ามาจากหมายเลข IP ใดของเครือข่ายใดบ้างและจำนวนการถูก block

๕) รายงานข้อมูลเมื่อเกิดความผิดปกติจากการบุกรุกหรือการถูกโจมตี ที่อาจจะก่อให้เกิดความไม่ปลอดภัยจากทั้งภายนอกและภายในต่อผู้อำนวยการสำนักดิจิทัลสิทธิมนุษยชนทันที เพื่อรับทราบและแนะนำแนวปฏิบัติ

๒.๒.๑๓ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application and Information Access Control)

ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายต้องดำเนินการ ดังนี้

๑) ต้องจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction) โดยจำกัดหรือควบคุมการเข้าถึงสารสนเทศและฟังก์ชัน (functions) ต่าง ๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชั่นของผู้ใช้งาน

๒) ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อหน่วยงาน จะต้องดำเนินการดังนี้

๒.๑) ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อองค์กร ได้แก่

- ระบบรับเรื่องร้องเรียน เป็นระบบงานหลักในการบริหารจัดการเรื่องร้องเรียนมีผลกระทบกับการดำเนินการแก้ไขข้อร้องเรียนของสำนักงาน กสม. สามารถเข้าถึงผ่านอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกองค์กรได้
- ระบบเว็บไซต์สำนักงาน กสม. เป็นระบบงานที่เผยแพร่ผลการดำเนินงานของคณะกรรมการสิทธิมนุษยชนแห่งชาติและสำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ สามารถเข้าถึงผ่าน อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกองค์กรได้

๒.๒) ระบบซึ่งไวต่อการรบกวน ต้องกำหนดรหัสผ่านให้เฉพาะผู้ที่มีสิทธิใช้ระบบเท่านั้น

๒.๓) ระบบซึ่งไวต่อการรบกวน ต้องแยกออกจากระบบอื่น โดยระบบต้องกำหนด DMZ Zone เป็นการเฉพาะผ่านอุปกรณ์ Firewall

๒.๔) ผู้ดูแลระบบต้องตรวจสอบและดูแลสภาพแวดล้อมภายในบริเวณหรือพื้นที่ที่มีระบบซึ่งไวต่อการรบกวน เพื่อป้องกันความเสียหายต่ออุปกรณ์ต่าง ๆ ได้แก่ ระบบควบคุมอุณหภูมิ ระบบตรวจจับความชื้นในห้องปฏิบัติการสารสนเทศ

๓) ต้องควบคุมอุปกรณ์สื่อสารเคลื่อนที่ (สมาร์ทโฟนและแท็บเล็ต) เพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์สื่อสารเคลื่อนที่ ดังนี้

๓.๑) ให้ติดต่อสำนักดิจิทัลสิทธิมนุษยชน เพื่อขออนุญาตใช้งานพร้อมระบุเหตุผลหรือความจำเป็นในการใช้งาน

๓.๒)กำหนดให้ยืนยันตัวตน (user authentication for external connections) ด้วยชื่อผู้ใช้งาน (username) และรหัสผ่าน (Password) ก่อนเข้าใช้งาน

๓.๓) กำหนดระยะเวลาในการใช้งาน โดยจำกัดระยะเวลาในการใช้งาน และต้องพิสูจน์ตัวตนเพื่อเข้าใช้งานใหม่ตามช่วงระยะเวลาที่กำหนดไว้ทุก ๆ ๔๐ นาที

๔) ต้องควบคุมการเข้าถึงจากผู้ให้บริการรายอื่น (IT Outsourcing) ดังนี้

๔.๑) ให้ติดต่อสำนักดิจิทัลสิทธิมนุษยชน เพื่อขออนุญาตใช้งานพร้อมระบุเหตุผลหรือความจำเป็นในการใช้งาน

๔.๒)กำหนดให้ยืนยันตัวตน (user authentication for external connections) ด้วยชื่อผู้ใช้งาน (username) และรหัสผ่าน (Password) ทุกครั้งก่อนเข้าใช้งาน

๔.๓) ผู้ให้บริการรายอื่น ต้องปฏิบัติงานด้วยความรัดกุมรอบคอบและรายงานผลหลังปฏิบัติงานให้ผู้ดูแลระบบทราบ

๔.๔) ต้องมีเจ้าหน้าที่ของสำนักดิจิทัลสิทธิมนุษยชนควบคุมดูแลการทำงานของผู้ให้บริการอย่างใกล้ชิด

๔.๕) หลังจากใช้งานเสร็จสิ้นแล้ว ผู้ดูแลระบบต้องลบรหัสผู้ขอเข้าใช้งาน หรือปิดบัญชีผู้ใช้งานทันที

๕) การทำลายเอกสาร สื่อบันทึกข้อมูลและข้อมูลอิเล็กทรอนิกส์

๕.๑) เครื่องคอมพิวเตอร์ เมื่อหมดอายุการใช้งานหรือตัดจำหน่าย แต่ละสำนัก/กลุ่มงานต้องทำการย้าย หรือลบข้อมูลทั้งหมดออกและต้องแจ้งให้ สำนักดิจิทัลสิทธิมนุษยชนทราบ เพื่อตรวจสอบและล้างข้อมูลในเครื่องคอมพิวเตอร์ก่อนส่งคืนพัสดุเพื่อทำลาย ทดแทน หรือจำหน่ายต่อไป

๕.๒) ฮาร์ดดิสก์ของสำนักดิจิทัลสิทธิมนุษยชน ต้องทำการฟอร์แมต (Format) ฮาร์ดดิสก์เพื่อป้องกันการกู้คืนข้อมูลในฮาร์ดดิสก์ โดยการใช้วิธีแบบเขียนทับซ้ำจำนวน ๑ ครั้ง สำหรับข้อมูลที่มีความลับระดับต่ำตามมาตรฐาน NIST ๘๐๐-๘๘ หรือแบบเขียนทับซ้ำจำนวน ๓ ครั้ง สำหรับข้อมูลที่มีความลับระดับปานกลาง ตามมาตรฐาน DoD ๕๒๒๐.๒๒- M หรือแบบเขียนทับซ้ำจำนวน ๗ ครั้ง สำหรับข้อมูลที่มีความลับระดับสูง มาตรฐาน NSA หรือตามมาตรฐานอื่น ๆ ที่เหมาะสม

๕.๓) แฟลชไดร์ฟ (Flash drive) ใช้วิธีทุบ หรือบดให้เสียหาย

๕.๔) กระดาษ ใช้วิธีเข้าเครื่องทำลายเอกสาร

๕.๕) แผ่นซีดี ใช้วิธีทุบทำลายให้เสียหาย

ส่วนที่ ๓
นโยบายและแนวปฏิบัติในการสำรองข้อมูลและตรวจสอบประเมินความเสี่ยงด้านสารสนเทศ

๓.๑ นโยบายในการสำรองข้อมูลและตรวจสอบประเมินความเสี่ยงด้านสารสนเทศ

วัตถุประสงค์ เพื่อให้มีการบริหารจัดการระบบสำรองข้อมูลระบบสารสนเทศ มีแผนกรณีฉุกเฉิน และเพื่อให้ระบบสามารถทำงานได้อย่างต่อเนื่อง รวมทั้งตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศ ซึ่งจะเป็นการป้องกันและลดระดับความเสี่ยงที่อาจจะเกิดขึ้นกับระบบสารสนเทศ รวมถึงกำหนดมาตรการในการควบคุมความเสี่ยงระบบสารสนเทศ

๓.๒ แนวปฏิบัติ

๓.๒.๑ การสำรองข้อมูล

ผู้ดูแลระบบ หรือผู้ที่ได้รับมอบหมายต้องดำเนินการ ดังนี้

๑) ต้องจัดทำทะเบียนระบบงานทั้งหมดของหน่วยงาน พร้อมพิจารณาคัดเลือกระบบงานที่จำเป็นต้องดำเนินการสำรองข้อมูล ขั้นตอนและความถี่ในการสำรองข้อมูลของแต่ละระบบ โดยระบบที่จะทำการสำรองข้อมูลต้องเป็นระบบที่มีความสำคัญ

๒) ต้องสำรองข้อมูลแบบเต็ม (Full Backup) และสำรองข้อมูลแบบส่วนต่าง (Incremental Backup) โดยกำหนดรูปแบบการสำรองข้อมูลให้เหมาะสมกับข้อมูลที่จะทำการสำรอง

๓) ต้องทำการสำรองข้อมูลระบบงานเก็บไว้เป็นประจำอย่างสม่ำเสมอ ตามแผนการสำรองข้อมูล

๔) ต้องตรวจสอบความสมบูรณ์ของข้อมูลที่สำรองและให้รทบทวนแผนการสำรองข้อมูลอย่างน้อยปีละ ๑ ครั้ง

๕) ต้องจัดทำขั้นตอนปฏิบัติ สำหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่ได้สำรองเก็บไว้

๖) ต้องทดสอบสภาพพร้อมใช้งานของระบบสำรองข้อมูล อย่างน้อยปีละ ๑ ครั้ง

๗) ต้องจัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ ระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลสำรองกับหน่วยงาน โดยห่างกันอย่างน้อย ๒๐ กม. เพื่อไม่ให้ส่งผลกระทบต่อข้อมูลที่จัดเก็บไว้นอกสถานที่นั้น ในกรณีที่เกิดภัยพิบัติกับหน่วยงาน เช่น ไฟไหม้ เป็นต้น

๓.๒.๒ การจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน

ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายต้องดำเนินการ ดังนี้

๑) จัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน (ในกรณีระบบหลักไม่สามารถใช้งานได้จากภัยพิบัติให้ไปใช้ระบบสำรอง (DR-Site))

๒) ทบทวนแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง

๓.๒.๓ การตรวจสอบประเมินความเสี่ยงด้านสารสนเทศ

สำนักดิจิทัลสิทธิมนุษยชน ต้องดำเนินการ ดังนี้

๑) ตรวจสอบ และประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (Information security audit and assessment) อย่างน้อยปีละ ๑ ครั้ง

๒) ตรวจสอบและประเมินความเสี่ยง โดยเจ้าหน้าที่ของสำนักดิจิทัลสิทธิมนุษยชน หรือผู้ตรวจสอบภายใน (Internal Auditor) หรือผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) เพื่อให้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

๓) ให้จัดทำแผนบริหารความเสี่ยง โดยต้องวิเคราะห์ความเสี่ยงและระบุความเสี่ยง เหตุการณ์ด้านความมั่นคงปลอดภัย กิจกรรมการบริหารความเสี่ยง จัดลำดับความเสี่ยง เป็นอย่างน้อย

ส่วนที่ ๔
นโยบายและแนวปฏิบัติในการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๔.๑. นโยบายการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

วัตถุประสงค์ เพื่อเผยแพร่นโยบายและแนวปฏิบัติให้กับบุคลากรของสำนักงาน กสม. ได้มีความรู้ความเข้าใจ ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และสามารถนำไปปฏิบัติได้อย่างถูกต้อง โดยการจัดทำคู่มือจัดฝึกอบรมการใช้งานด้านสารสนเทศและระบบคอมพิวเตอร์ให้แก่ผู้ใช้งาน

๔.๒ แนวปฏิบัติการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

สำนักดิจิทัลสิทธิมนุษยชน ต้องดำเนินการ ดังนี้

๑) จัดฝึกอบรมด้านระบบสารสนเทศ เพื่อเสริมสร้างความรู้ความเข้าใจด้านระบบสารสนเทศให้กับบุคลากรของสำนักงาน กสม. โดยอาจเชิญวิทยากรจากภายนอกที่มีประสบการณ์มาถ่ายทอดความรู้ให้ผู้ใช้งานของหน่วยงานทราบ หรือใช้วิธีเสริมเนื้อหาการสร้างความตระหนักการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเข้ากับหลักสูตรอบรมต่าง ๆ

๒) เผยแพร่นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยอาจใช้วิธีติดประกาศ การประชาสัมพันธ์ หรือการเผยแพร่ทางเว็บไซต์ หรือจัดทำคู่มือแนะนำเผยแพร่ทางเครือข่ายภายใน/เว็บไซต์ หรือให้คำแนะนำแก่ผู้ใช้งาน เป็นต้น

๓) ทบทวนปรับปรุงนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศจากการวิเคราะห์สถานการณ์ด้านความมั่นคงปลอดภัย ที่ไม่พึงประสงค์หรือไม่อาจคาดคิดในสำนักงาน กสม. ให้เป็นปัจจุบันอยู่เสมอ

ส่วนที่ ๕
หน้าที่และความรับผิดชอบด้านสารสนเทศ

๕.๑. นโยบายความรับผิดชอบด้านสารสนเทศ

วัตถุประสงค์ เพื่อกำหนดหน้าที่ความรับผิดชอบของผู้บริหารระดับสูงสุด (CEO) และผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (DCIO) และผู้อำนวยการสำนักฯ และผู้ดูแลระบบ และผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่และผู้ใช้งาน

๕.๒ แนวปฏิบัติของหน้าที่และความรับผิดชอบด้านสารสนเทศ

๕.๒.๑ ระดับนโยบาย

ระดับนโยบาย ประกอบด้วย ผู้บริหารระดับสูงสุดของสำนักงาน (CEO) ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (DCIO) และผู้อำนวยการสำนักดิจิทัลสิทธิมนุษยชนและหัวหน้ากลุ่มงาน

๑) ผู้บริหารระดับสูงสุดของสำนักงาน (Chief Executive Officer: CEO) มีหน้าที่เป็นผู้รับผิดชอบในการสั่งการตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้การสนับสนุนต่อการบริหารจัดการความมั่นคงปลอดภัยขององค์กร ให้นโยบาย กำกับดูแลและการเล็งเห็นถึงความสำคัญในหน้าที่และความรับผิดชอบด้านความมั่นคงปลอดภัยด้านสารสนเทศ

ในกรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่องละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ผู้บริหารระดับสูงของสำนักงาน (CEO) จะเป็นผู้รับผิดชอบต่อความเสี่ยงหรืออันตรายที่เกิดขึ้น

๒) ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (DCIO) มีหน้าที่ให้คำปรึกษา เรื่อง แนวนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๓) ผู้อำนวยการสำนักดิจิทัลสิทธิมนุษยชนและหัวหน้ากลุ่มงานเป็นผู้รับผิดชอบ ดังนี้

๓.๑) กำกับ ดูแล การปฏิบัติงานของผู้ปฏิบัติ ตลอดจนศึกษา ทบทวน วางแผน ติดตามการบริหารความเสี่ยง และระบบรักษาความปลอดภัยฐานข้อมูลและเทคโนโลยีสารสนเทศ

๓.๒) ควบคุม ดูแล รักษาความปลอดภัยระบบสารสนเทศและระบบฐานข้อมูล

๓.๓) วางแผน จัดทำ ทบทวน ติดตาม กำกับ ดูแล แผนสำรอง และแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

๕.๒.๒ ระดับปฏิบัติงาน

ระดับผู้ปฏิบัติงาน ประกอบด้วย ผู้ดูแลระบบ ผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่ และผู้ใช้งานเป็นผู้รับผิดชอบตามภารกิจ ดังนี้

๑) ผู้ดูแลระบบ หรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่เป็นผู้รับผิดชอบ ดังนี้

๑.๑) ควบคุม ติดตาม และตรวจสอบการใช้งานระบบสารสนเทศให้สอดคล้องกับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๑.๒) ประสานการปฏิบัติงานตามแผนป้องกันและแก้ไขปัญหาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ

๑.๓) ควบคุม ดูแล รักษาความปลอดภัย และบำรุงรักษาระบบคอมพิวเตอร์ ระบบเครือข่ายระบบสารสนเทศ ห้องควบคุมระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย

๑.๔) ทำการสำรองข้อมูลและเรียกคืนข้อมูล (Backup and Recovery) ตามรอบระยะเวลาที่กำหนด

๑.๕) ป้องกันการถูกเจาะระบบ และแก้ไขปัญหาการถูกเจาะเข้าระบบฐานข้อมูลจากบุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาต

๑.๖) ปฏิบัติงานอื่น ๆ ตามที่ได้รับมอบหมายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงาน

๒) ผู้ใช้งานเป็นผู้เข้าถึงและใช้งานระบบสารสนเทศตามสิทธิที่ได้รับอนุญาต โดยให้ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้อย่างเคร่งครัด

ภาคผนวก
นโยบายและแผนปฏิบัติการอื่น ๆ ที่เกี่ยวข้อง

ภาคผนวก ก. แผนเตรียมความพร้อมกรณีฉุกเฉิน (IT Contingency Plan)
ภาคผนวก ข. นโยบายเว็บไซต์ของสำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ
ภาคผนวก ค. นโยบายการรักษาความมั่นคงปลอดภัยเว็บไซต์ของสำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ
ภาคผนวก ง. นโยบายการคุ้มครองข้อมูลส่วนบุคคลของเว็บไซต์สำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ
ภาคผนวก จ. นโยบายคุกกี้ของสำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ

ภาคผนวก ก. แผนเตรียมความพร้อมกรณีฉุกเฉิน (IT Contingency Plan)

๑. แนวปฏิบัติในการสำรองข้อมูลและระบบงาน

๑.๑ จัดทำทะเบียนระบบงานของสำนักงาน กสม. พร้อมจัดเรียงลำดับความสำคัญของระบบงาน

๑.๒ ผู้รับผิดชอบในการดำเนินการสำรองข้อมูลและระบบงาน คือ เจ้าหน้าที่สำนักดิจิทัลสิทธิมนุษยชน

๑.๓ กำหนดทะเบียนระบบที่ต้องดำเนินการสำรองดังนี้

ลำดับ	ระบบงาน	ความถี่	ความสำคัญ
๑	ระบบสารสนเทศเพื่อรวบรวมและบริการสารสนเทศด้านสิทธิมนุษยชน	ทุกวัน	๑
๒	ระบบสารบรรณอิเล็กทรอนิกส์	ทุกวัน	๑
๓	ระบบรับเรื่องร้องเรียน	ทุกวัน	๑
๔	ระบบบริการเครือข่ายภายใน (Web Portal)	ทุกวัน	๑
๕	ระบบฐานข้อมูลบัญชีรายชื่อและระบบยืนยันตัวตนผู้ใช้งาน (Active Directory & Authentication Systems & DNS Server)	ทุกวัน	๑
๖	ระบบให้บริการข้อมูลผ่านเครือข่าย (File Sharing Server)	ทุกวัน	๑
๗	ระบบเว็บไซต์สำนักงาน กสม.	ทุกวัน	๑
๘	ระบบเว็บไซต์ศูนย์สารสนเทศสิทธิมนุษยชน	ทุกวัน	๒
๙	ระบบภาคีเครือข่ายสิทธิมนุษยชน	ทุกวัน	๒
๑๐	ระบบอีเมล์สำนักงาน (Mail Server)	ทุกวัน	๒
๑๑	ระบบจัดเก็บข้อมูลข่าวเพื่อการติดตามและประเมินสถานการณ์สิทธิมนุษยชน	ทุกวัน	๒
๑๒	ระบบแอปพลิเคชันสำนักงานสิทธิมนุษยชนแห่งชาติ	ทุกวัน	๒
๑๓	ระบบสารสนเทศทรัพยากรบุคคล (D-Pis)	ทุกวัน	๓
๑๔	ระบบสมุดโทรศัพท์	ทุกวัน	๓
๑๕	ระบบแจ้งซ่อมคอมพิวเตอร์ออนไลน์	ทุกวัน	๓
๑๖	ระบบจองห้องประชุม	ทุกวัน	๓
๑๗	ระบบจัดการไฟล์ QR Code	ทุกวัน	๓

หมายเหตุ ความสำคัญของระบบงาน

ระดับความสำคัญ	ผลกระทบต่อผู้ใช้งาน
สูง (๑)	กระทบผู้ใช้งานเป็นส่วนใหญ่ ทำให้เกิดการหยุดชะงักงานโดยรวม
ปานกลาง (๒)	กระทบผู้ใช้งาน ทำให้เกิดการหยุดชะงักงานเล็กน้อย
น้อย (๓)	กระทบผู้ใช้งานเล็กน้อย ทำให้เกิดไม่สะดวกในการใช้งาน

๑.๔ ดำเนินการสำรองข้อมูลและระบบตามที่กำหนดไว้ พร้อมกับการตรวจสอบความสมบูรณ์ของการสำรองข้อมูลแต่ละครั้ง

๑.๕ รายงานผลการปฏิบัติงานตามสายงานการบังคับบัญชา

๑.๖ ทดสอบสภาพพร้อมใช้งานของระบบสำรองข้อมูล อย่างน้อยปีละ ๑ ครั้ง

๒. แนวปฏิบัติในการกู้คืนข้อมูลและระบบงาน

๒.๑ ผู้รับผิดชอบในการดำเนินการกู้คืนข้อมูลและระบบงาน คือ เจ้าหน้าที่สำนักดิจิทัลสิทธิมนุษยชน

๒.๒ ทดสอบการกู้คืนข้อมูลและระบบงาน อย่างน้อยปีละครั้ง

๒.๓ แจ้งผู้อำนวยการสำนักดิจิทัลสิทธิมนุษยชน ก่อนดำเนินการกู้คืนข้อมูล

๒.๔ ดำเนินการกู้คืนข้อมูลและระบบงาน

๒.๕ ตรวจสอบความสมบูรณ์ของข้อมูลและระบบที่ได้จากการกู้คืน

๒.๖ ทดสอบการปฏิบัติงานตามคู่มือข้อมูลและระบบงานที่กู้คืนแต่ละระบบหรือทั้งหมด

๒.๗ รายงานผลการปฏิบัติงานต่อผู้บังคับบัญชา

๓. การกำหนดหน้าที่และความรับผิดชอบของบุคลากร เมื่อเกิดเหตุฉุกเฉิน

๓.๑ กำหนดผู้รับผิดชอบ เมื่อเกิดเหตุฉุกเฉิน

๓.๑.๑ ผู้บริหารระดับสูงสุดของสำนักงาน (CEO)

๓.๑.๒ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (DCIO)

๓.๑.๓ ผู้อำนวยการสำนักดิจิทัลสิทธิมนุษยชน

๓.๑.๔ ผู้ประสานงานและบริหารกำกับดูแลระบบเครือข่ายและระบบสารสนเทศ

คือ หัวหน้ากลุ่มงานของสำนักดิจิทัลสิทธิมนุษยชน

๓.๑.๕ ผู้ดูแลระบบเครือข่ายและระบบสารสนเทศ (LAN Administrator and Staffs)

คือ เจ้าหน้าที่สำนักดิจิทัลสิทธิมนุษยชน

๓.๑.๖ บุคคลภายนอกที่เกี่ยวข้อง

๑) บริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด

๒) บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)

๓.๒ กำหนดหน้าที่ของบุคลากร เมื่อเกิดเหตุฉุกเฉิน

๓.๒.๑ ผู้บริหารระดับสูงสุดของสำนักงาน (CEO)

๑) กำหนดนโยบายให้สำนักดิจิทัลสิทธิมนุษยชน

๒) สั่งการ ให้คำปรึกษาและการสนับสนุนต่อการบริหารจัดการความมั่นคงปลอดภัยขององค์กร

๓.๒.๒ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (DCIO)

๑) กำหนดนโยบายให้สำนักดิจิทัลสิทธิมนุษยชน

๒) ให้คำปรึกษา กำกับดูแลผู้อำนวยการสำนักดิจิทัลสิทธิมนุษยชน

๓.๒.๓ ผู้อำนวยการสำนักดิจิทัลสิทธิมนุษยชน

๑) สั่งการให้ทุกหน่วยปฏิบัติการระงับเหตุฉุกเฉินที่เกิดขึ้น

๒) สั่งทำลายกุญแจอุปกรณ์สำนักงานเพื่อการระงับเหตุฉุกเฉิน

๓) วางแผนปฏิบัติงานเพื่อระงับเหตุฉุกเฉิน

๔) ประเมินสถานการณ์และสั่งการให้ปรับเปลี่ยนแผนฯตามความเหมาะสม

๕) รายงานข้อมูลและผลการปฏิบัติงานให้ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (DCIO) ทราบ

๓.๒.๔ ผู้ประสานงานและบริหารกำกับดูแลระบบเครือข่ายและระบบสารสนเทศ

๑) วิเคราะห์เหตุการณ์ด้านความมั่นคงปลอดภัย และสถานการณ์ด้านความมั่นคงปลอดภัยในที่เกิดเหตุแล้วแจ้งเหตุต่อผู้อำนวยการสำนักดิจิทัลสิทธิมนุษยชน

๒) สั่งการให้ใช้แผนปฏิบัติการฉุกเฉินขั้นต้นจนกว่าผู้อำนวยการสำนักดิจิทัลสิทธิมนุษยชนจะมาถึงที่เกิดเหตุหรือสั่งการใด ๆ

๓) ทำหน้าที่แทนผู้อำนวยการสำนักดิจิทัลสิทธิมนุษยชนตามที่ได้รับมอบหมาย หรือขณะที่ผู้อำนวยการสำนักดิจิทัลสิทธิมนุษยชนไม่อยู่ หรือไม่สามารถปฏิบัติหน้าที่ได้

๔) ประสานงานกับหน่วยงานที่เกี่ยวข้อง เช่น ไฟฟ้า ยานพาหนะ และดับเพลิง เป็นต้น

๕) วางแผนอัตรากำลังวัสดุอุปกรณ์และเครื่องมือที่จำเป็น

๖) ตรวจสอบความเสียหายของทรัพย์สินและอาคารที่เกิดเหตุ

๗) รายงานให้ผู้อำนวยการสำนักดิจิทัลสิทธิมนุษยชนทราบถึงสถานการณ์การดำเนินงานที่ได้กระทำไปแล้ว และรายงานสรุปเมื่อเสร็จสิ้นภารกิจ

๓.๒.๕ ผู้ดูแลระบบเครือข่ายและระบบสารสนเทศ (LAN Administrator and Staffs)

๑) ดำเนินการตามแผนและการสั่งการเพื่อป้องกันชีวิตทรัพย์สินและสิ่งแวดล้อมให้ได้รับความเสียหายน้อยที่สุด

๒) หลังจากเหตุการณ์ฉุกเฉินได้สงบลงแล้วให้รีบดำเนินการตรวจสอบวัสดุอุปกรณ์ที่ชำรุดเสียหายและรายงานให้ผู้อำนวยการสำนักดิจิทัลสิทธิมนุษยชนทราบ อุปกรณ์ที่ต้องตรวจสอบ ได้แก่

๒.๑) ทำการตรวจสอบระบบ Firewall

๒.๒) ทำการตรวจสอบ Virus, worm, Spy ware

๒.๓) ทำการตรวจสอบ UPS

๒.๔) ทำการตรวจสอบ Transaction log files

๒.๕) ทำการตรวจสอบการใช้งานข้อมูลระบบงานที่สำคัญ

๒.๖) ทำการตรวจสอบการเปลี่ยนแปลงของไฟล์ต่าง ๆ

๒.๗) ทำการตรวจสอบความถูกต้องของไฟล์ข้อมูล

๒.๘) ทำการตรวจสอบค่า Configuration ของระบบ

๓) เตรียมเครื่องมืออุปกรณ์ทั้งทางด้านฮาร์ดแวร์และซอฟต์แวร์ตลอดจนอุปกรณ์ที่เกี่ยวข้องเพื่อดำเนินการกู้คืนระบบโดยเร็ว

๔) ประสานงานกับที่ปรึกษาด้านเทคนิค

๕) ดำเนินการกู้คืนระบบและข้อมูลเพื่อให้สามารถใช้งานได้ตามปกติ

๓.๒.๖ ที่ปรึกษาด้านเทคนิค (เจ้าหน้าที่บริษัทที่รับจ้างบำรุงรักษาระบบ)

๑) ให้คำปรึกษาในเรื่องเกี่ยวกับระบบสารสนเทศและวิธีการจัดการในการระงับเหตุฉุกเฉินที่ปลอดภัยต่อชีวิตทรัพย์สินและสิ่งแวดล้อมมากที่สุด

๒) ให้คำปรึกษาวิธีการกู้คืนระบบสารสนเทศกลับคืนมาโดยเร็วหลังจากเหตุฉุกเฉินสงบแล้ว

๔. แนวปฏิบัติในกรณีเกิดสถานการณ์ฉุกเฉินจากภัยพิบัติ

๔.๑ กรณีเกิดไฟไหม้อาคารสถานที่

๑) รีบแจ้งให้ผู้อำนวยการสำนักดิจิทัลสิทธิมนุษยชนและสำนักบริหารกลางทราบโดยเร็วเพื่อประสานงานให้เจ้าหน้าที่บริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด แจ้งตำรวจดับเพลิงและหน่วยงานที่เกี่ยวข้องเข้ามาให้การช่วยเหลือโดยเร็ว

๒) ตัดการเชื่อมต่อระบบเครือข่ายโดยเร็ว แล้วปิดอุปกรณ์เครือข่ายและเครื่องคอมพิวเตอร์แม่ข่ายตามลำดับความสำคัญของการให้บริการ

๓) ถ้าไฟฟ้าดับ/ไฟฟ้าตก ให้ปิดเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายโดยพิจารณาตามลำดับความสำคัญของการให้บริการ ระยะเวลาที่ไฟฟ้าดับ และประสิทธิภาพของเครื่องสำรองไฟฟ้า

๔) ตัดระบบจ่ายไฟ ในกรณีไฟไหม้ ให้ใช้น้ำยาดับเพลิงฉีดควบคุมเพลิงโดยเร็ว

๕) ทำการรวบรวมโปรแกรมและแฟ้มข้อมูล, Hard Disk Backup, รายชื่อโปรแกรม, เอกสารที่เกี่ยวข้องกับระบบปฏิบัติการและโปรแกรม, สำเนาคู่มือต่าง ๆ ที่เกี่ยวข้องกับระบบสารสนเทศ ไปเก็บไว้ในสถานที่ปลอดภัย รวมถึงช่วยกันขนย้ายเครื่องคอมพิวเตอร์ไปไว้ในที่ปลอดภัย

๖) ประสานงานขอความช่วยเหลือกับผู้เชี่ยวชาญด้านระบบเครือข่ายโดยเร็วที่สุด

๗) ในกรณีที่อุปกรณ์ด้านฮาร์ดแวร์เสีย ให้รีบหาอุปกรณ์สำรอง หรือแจ้งให้บริษัทที่รับผิดชอบนำอุปกรณ์มาเปลี่ยนโดยเร็วที่สุด

๔.๒ กรณีเกิดภัยจากการจลาจล เป็นการก่อความไม่สงบที่มีลักษณะคล้ายสงครามการเมือง คือ มีมวลชนขนาดใหญ่รวมตัวกันเคลื่อนไหว เพื่อนำไปสู่การเปลี่ยนแปลง และไม่อาจควบคุมมวลชนที่มารวมตัวกันนั้นได้จนนำไปสู่การจลาจล สร้างความวุ่นวายสับสน และเกิดความเสียหายโดยเมื่อสถานการณ์พัฒนาสู่การจลาจลแล้วก็จะมีการปราบปรามจากเจ้าหน้าที่รัฐ

๑) เฝ้าติดตามข่าวจากแหล่งต่าง ๆ เช่น ตำรวจ นักข่าว โทรทัศน์ วิทยุ และหน่วยงานที่เกี่ยวข้อง

๒) จัดเตรียมกำลังเจ้าหน้าที่ วัสดุ อุปกรณ์ เครื่องมือเครื่องใช้ ระบบการสื่อสารยานพาหนะ เป็นต้น และมอบหมายหน้าที่ความรับผิดชอบในการปฏิบัติไว้ให้พร้อม

๓) ตรวจสอบระบบไฟฟ้า ให้อยู่ในสภาพที่พร้อมใช้งาน

๔) ตรวจเช็ดการทำงานกล้องวงจรปิดเพื่อรักษาความปลอดภัย

๕) ทำการสำรองข้อมูลในเครื่องคอมพิวเตอร์แม่ข่าย และจัดเก็บ Hard Disk External ที่สำรองข้อมูลไว้ในที่ปลอดภัย

๖) ปฏิบัติตามคำสั่งของผู้บังคับบัญชาอย่างเคร่งครัด

ภาคผนวก ข. นโยบายเว็บไซต์ของสำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ

๑. วัตถุประสงค์

เว็บไซต์สำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ (สำนักงาน กสม.) ได้จัดทำขึ้นเพื่อเผยแพร่ประชาสัมพันธ์ข้อมูล ข่าวสารและให้บริการที่เกี่ยวเนื่องกับสำนักงาน กสม. ในการใช้บริการเว็บไซต์ของผู้ใช้บริการจะอยู่ภายใต้เงื่อนไขและข้อกำหนดดังต่อไปนี้ ผู้ใช้บริการจึงควรศึกษาเงื่อนไข และข้อกำหนดการใช้เว็บไซต์ และ/เงื่อนไขและข้อตกลงอื่น ๆ ที่สำนักงาน กสม. ได้แจ้งให้ทราบบนเว็บไซต์โดยละเอียดก่อนการเข้าใช้บริการ ทั้งนี้ในการใช้บริการให้ถือว่าผู้ใช้บริการได้ตกลงที่จะปฏิบัติตามเงื่อนไขและข้อกำหนดการให้บริการ ที่กำหนดไว้นี้ หากผู้ใช้บริการไม่ประสงค์ที่จะผูกพันตามข้อกำหนดและเงื่อนไขการให้บริการ ขอความกรุณาท่านยุติการเข้าชมและใช้งานเว็บไซต์นี้ในทันที

๒. เงื่อนไขและข้อกำหนดการใช้งานเว็บไซต์

๒.๑ ผู้ใช้บริการอาจได้รับ เข้าถึง สร้าง ส่งหรือแสดงข้อมูล เช่น ไฟล์ข้อมูล ข้อความลายลักษณ์อักษร ซอฟต์แวร์คอมพิวเตอร์ ดนตรี ไฟล์เสียง หรือเสียงอื่น ๆ ภาพถ่าย วิดีโอ หรือรูปภาพอื่น ๆ โดยเป็นส่วนหนึ่งของบริการหรือโดยผ่านการใช้บริการ ซึ่งต่อไปนี้จะเรียกว่า “เนื้อหา”

๒.๒ เนื้อหาที่นำเสนอต่อผู้ใช้บริการ อาจได้รับการคุ้มครองโดยสิทธิในทรัพย์สินทางปัญญาของเจ้าของเนื้อหานั้น ผู้ใช้บริการไม่มีสิทธิเปลี่ยนแปลงแก้ไข จำหน่ายจ่ายโอนหรือสร้างผลงานต่อเนื่องโดยอาศัยเนื้อหาดังกล่าวไม่ว่าจะทั้งหมดหรือบางส่วน เว้นแต่ผู้ใช้บริการจะได้รับอนุญาตโดยชัดแจ้งจากเจ้าของเนื้อหานั้น

๒.๓ ผู้ใช้บริการอาจพบเนื้อหาที่ไม่เหมาะสม หรือหยาบคาย อันก่อให้เกิดความไม่พอใจ ภายใต้ความเสี่ยงของตนเอง

๒.๔ สำนักงาน กสม. ทรงไว้ซึ่งสิทธิในการคัดกรอง ตรวจทาน ทำเครื่องหมายเปลี่ยนแปลงแก้ไข ปฏิเสธ หรือลบเนื้อหาใด ๆ ที่ไม่เหมาะสมออกจากบริการ ซึ่งสำนักงาน กสม. อาจจัดเตรียมเครื่องมือในการคัดกรองเนื้อหาอย่างชัดเจน โดยไม่ขัดต่อกฎหมาย กฎ ระเบียบของทางราชการที่เกี่ยวข้อง

๒.๕ สำนักงาน กสม. อาจหยุดให้บริการเป็นการชั่วคราวหรือถาวร หรือยกเลิกการให้บริการแก่ผู้ใช้บริการรายใดเป็นการเฉพาะ หากการให้บริการดังกล่าวส่งผลกระทบต่อผู้ใช้บริการอื่น ๆ หรือขัดแย้งต่อกฎหมาย โดยไม่ต้องแจ้งให้ผู้ใช้บริการทราบล่วงหน้า

๒.๖ การหยุด หรือการยกเลิกบริการตามข้อ ๒.๕ ผู้ใช้บริการจะไม่สามารถเข้าใช้บริการ และเข้าถึงรายละเอียดบัญชีของผู้ใช้บริการ ไฟล์เอกสารใด ๆ หรือเนื้อหาอื่น ๆ ที่อยู่ในบัญชีของผู้ใช้บริการได้

๒.๗ ในกรณีที่สำนักงาน กสม. หยุดให้บริการเป็นการถาวร หรือยกเลิกบริการแก่ผู้ใช้บริการสำนักงาน กสม. มีสิทธิในการลบข้อมูลต่าง ๆ ที่อยู่ในบัญชีของผู้ใช้บริการได้ โดยไม่ต้องแจ้งให้ผู้ใช้บริการทราบล่วงหน้า

๓. สิทธิ หน้าที่ และความรับผิดชอบของผู้ใช้บริการ

๓.๑ ผู้ใช้บริการจะให้ข้อมูลเกี่ยวกับตนเอง เช่น ข้อมูลระบุตัวตนหรือรายละเอียดการติดต่อ ที่ถูกต้อง เป็นจริง และเป็นปัจจุบันเสมอแก่สำนักงาน กสม. อันเป็นส่วนหนึ่งของกระบวนการลงทะเบียนใช้บริการหรือการใช้บริการที่ต่อเนื่อง

๓.๒ ผู้ใช้บริการจะใช้บริการเว็บไซต์นี้ เพื่อวัตถุประสงค์ที่ได้รับอนุญาตตามข้อกำหนดของสำนักงาน กสม. และไม่ขัดต่อกฎหมาย กฎ ระเบียบ ข้อบังคับ หลักปฏิบัติที่เป็นที่ยอมรับโดยทั่วไป

๓.๓ ผู้ใช้บริการจะไม่เข้าใช้ หรือพยายามเข้าใช้บริการหนึ่งบริการใดโดยวิธีอื่น รวมถึงการใช้วิธีการอัตโนมัติ (การใช้สคริปต์) นอกจากช่องทางที่ (ชื่อหน่วยงาน/เว็บไซต์) จัดเตรียมไว้ให้ เว้นแต่ผู้ใช้บริการจะได้รับอนุญาตจากสำนักงาน กสม. โดยชัดแจ้งให้ทำเช่นนั้นได้

๓.๔ ผู้ใช้บริการจะไม่ทำ หรือมีส่วนร่วมในการขัดขวาง หรือรบกวนบริการของสำนักงาน กสม. รวมทั้งเครื่องแม่ข่ายและเครือข่ายที่เชื่อมต่อกับบริการ

๓.๕ ผู้ใช้บริการจะไม่ทำสำเนา คัดลอก ทำซ้ำ ขาย แลกเปลี่ยน หรือขายต่อบริการเพื่อวัตถุประสงค์ใด ๆ เว้นแต่ผู้ใช้บริการจะได้รับอนุญาตจากสำนักงาน กสม. โดยชัดแจ้งให้ทำเช่นนั้นได้

๓.๖ ผู้ใช้บริการมีหน้าที่ในการรักษาความลับของรหัสผ่านที่เชื่อมโยงกับบัญชีใด ๆ ที่ใช้ในการเข้าถึงบริการ

๓.๗ ผู้ใช้บริการจะเป็นผู้รับผิดชอบแต่เพียงผู้เดียวต่อบุคคลใด ๆ รวมถึงสำนักงาน กสม. ในความเสียหายอันเกิดจากการละเมิดข้อกำหนด

๔. การเชื่อมโยงกับเว็บไซต์อื่น ๆ

๔.๑ การเชื่อมโยงไปยังเว็บไซต์อื่นเป็นเพียงการให้บริการ เพื่ออำนวยความสะดวกแก่ผู้ใช้บริการเท่านั้น สำนักงาน กสม. มิได้มีส่วนเกี่ยวข้อง หรือมีอำนาจควบคุม รับรอง ความถูกต้อง ความน่าเชื่อถือ ตลอดจนความรับผิดชอบในเนื้อหาข้อมูลของเว็บไซต์นั้น ๆ และสำนักงาน กสม. ไม่รับผิดชอบต่อเนื้อหาใด ๆ ที่แสดงบนเว็บไซต์อื่นที่เชื่อมโยงมายังเว็บไซต์ของสำนักงาน กสม. หรือต่อความเสียหายใด ๆ ที่เกิดขึ้นจากการเข้าเยี่ยมชมเว็บไซต์ดังกล่าวการเชื่อมโยงมายังเว็บไซต์สำนักงาน กสม.

๔.๒ กรณีต้องการเชื่อมโยงมายังเว็บไซต์ของสำนักงาน กสม. ผู้ใช้บริการสามารถเชื่อมโยงมายังหน้าแรกของเว็บไซต์ของสำนักงาน กสม. โดยแจ้งความประสงค์เป็นหนังสือ แต่หากต้องการเชื่อมโยงมายังหน้าภายในของเว็บไซต์นี้จะต้องได้รับความยินยอมเป็นหนังสือจากสำนักงาน กสม. เท่านั้น และในการให้ความยินยอมดังกล่าว สำนักงาน กสม. ขอสงวนสิทธิที่จะกำหนดเงื่อนไขใด ๆ ไว้ด้วยก็ได้ ในการที่เว็บไซต์อื่นที่เชื่อมโยงมายังเว็บไซต์ของสำนักงาน กสม. จะไม่รับผิดชอบต่อเนื้อหาใด ๆ ที่แสดงบนเว็บไซต์ที่เชื่อมโยงมายังเว็บไซต์ของสำนักงาน กสม. หรือต่อความเสียหายใด ๆ ที่เกิดขึ้นจากการใช้เว็บไซต์เหล่านั้น

๕. การปฏิเสธความรับผิด

สำนักงาน กสม. จะไม่รับผิดต่อความเสียหายใด ๆ รวมถึง ความเสียหาย สูญเสียและค่าใช้จ่ายที่เกิดขึ้นไม่ว่าโดยตรง หรือโดยอ้อม ที่เป็นผลหรือสืบเนื่องจากการที่ผู้ใช้เข้าใช้เว็บไซต์นี้ หรือเว็บไซต์ที่เชื่อมโยงกับเว็บไซต์นี้ หรือต่อความเสียหาย สูญเสียหรือค่าใช้จ่ายที่เกิดจากความล้มเหลวในการใช้งาน ความผิดพลาด การละเว้น การหยุดชะงัก ข้อบกพร่อง ความไม่สมบูรณ์ คอมพิวเตอร์ไวรัส ถึงแม้ว่าสำนักงาน กสม. จะได้รับแจ้งว่าอาจจะเกิดความเสียหาย สูญเสียหรือค่าใช้จ่ายดังกล่าวขึ้น นอกจากนี้สำนักงาน กสม. ไม่รับผิดต่อผู้ใช้เว็บไซต์หรือบุคคลจากการเรียกร้องใด ๆ ที่เกิดขึ้นจากบนเว็บไซต์ หรือเนื้อหาใด ๆ ซึ่งรวมถึงการตัดสินใจหรือการกระทำใด ๆ ที่เกิดจากความเชื่อถือในเนื้อหาดังกล่าวของผู้ใช้เว็บไซต์ หรือในความเสียหายใด ๆ ไม่ว่าความเสียหายทางตรง หรือทางอ้อม รวมถึงความเสียหายอื่นใดที่อาจเกิดขึ้นได้ผู้ใช้บริการยอมรับและตระหนักดีว่าสำนักงาน กสม. จะไม่ต้องรับผิดชอบต่อการกระทำใดของผู้ใช้บริการทั้งสิ้น

๖. กรรมสิทธิ์และสิทธิในทรัพย์สินทางปัญญา

๖.๑ สำนักงาน กสม. หรือผู้ให้อนุญาตแก่สำนักงาน กสม. เป็นผู้มีสิทธิตามกฎหมายแต่เพียงผู้เดียวในกรรมสิทธิ์ ผลประโยชน์ทั้งหมด รวมถึงสิทธิในทรัพย์สินทางปัญญาใด ๆ ที่มีอยู่ในบริการซึ่งสำนักงาน กสม. หรือผู้ให้อนุญาตแก่สำนักงาน กสม. เป็นผู้จัดทำขึ้น ไม่ว่าสิทธิเหล่านั้นจะได้รับการจดทะเบียนไว้หรือไม่ก็ตาม

๖.๒ ผู้ใช้บริการจะต้องไม่เปิดเผยข้อมูลที่สำนักงาน กสม. กำหนดให้เป็นความลับ โดยไม่ได้รับความยินยอมเป็นลายลักษณ์อักษรล่วงหน้าจากสำนักงาน กสม.

๖.๓ ผู้ใช้บริการจะต้องไม่ใช้ชื่อทางการค้า เครื่องหมายการค้า เครื่องหมายการบริการ ตราสัญลักษณ์ ชื่อโดเมนของสำนักงาน กสม. โดยไม่ได้รับความยินยอมเป็นลายลักษณ์อักษรจากสำนักงาน กสม.

๗. กฎหมายที่ใช้บังคับ

การตีความ และการบังคับตามเงื่อนไขการให้บริการฉบับนี้ ให้เป็นไปตามกฎหมายไทย

ภาคผนวก ค. นโยบายการรักษาความมั่นคงปลอดภัยเว็บไซต์ ของสำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ

๑. มาตรการ และวิธีการรักษาความมั่นคงปลอดภัยเว็บไซต์

สำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ (สำนักงาน กสม.) ได้ตระหนักถึงความสำคัญในการรักษาความมั่นคงปลอดภัยเว็บไซต์ เพื่อปกป้องข้อมูลของผู้ใช้บริการจากการถูกทำลาย หรือบุกรุกจากผู้ไม่หวังดี หรือผู้ที่ไม่มีสิทธิ์ในการเข้าถึงข้อมูล จึงได้กำหนดมาตรการรักษาความมั่นคงปลอดภัยเว็บไซต์ โดยใช้มาตรฐานการรักษาความปลอดภัยของข้อมูลขั้นสูง ด้วยเทคโนโลยี Secured Socket Layer (SSL) ซึ่งเป็นเทคโนโลยีในการเข้าสู่ข้อมูลผ่านรหัสที่ระดับ ๑๒๘ bits (๑๒๘-bits Encryption) เพื่อเข้ารหัสข้อมูลที่ถูกส่งผ่านเครือข่ายอินเทอร์เน็ตในทุกครั้ง ที่มีการทำธุรกรรมทางการเงินผ่านเครือข่ายอินเทอร์เน็ตของสำนักงาน กสม. ทำให้ผู้ที่ดักจับข้อมูลระหว่างทางไม่สามารถนำข้อมูลไปใช้ต่อได้ โดยจะใช้การเข้ารหัสเป็นหลักในการรักษาความปลอดภัยของข้อมูล โดยผู้ใช้บริการสามารถสังเกตได้จากชื่อโปรโตคอลที่เป็น https://

๒. เทคโนโลยีเสริมที่นำมาใช้ในการรักษาความมั่นคงปลอดภัย

นอกจากมาตรการ และวิธีการรักษาความมั่นคงปลอดภัยโดยทั่วไปที่กล่าวข้างต้นแล้ว สำนักงาน กสม. ยังใช้เทคโนโลยีระดับสูงดังต่อไปนี้ เพื่อปกป้องข้อมูลส่วนตัวของท่าน

๒.๑ Firewall เป็นระบบซอฟท์แวร์ที่จะอนุญาตให้เฉพาะผู้ที่มีสิทธิ หรือผู้ที่สำนักงาน กสม. อนุมัติเท่านั้นจึงจะผ่าน Firewall เพื่อเข้าถึงข้อมูลได้

๒.๒ Scan Virus นอกจากเครื่องคอมพิวเตอร์ทุกเครื่องที่ให้บริการจะมีการติดตั้ง Software ป้องกัน Virus ที่มีประสิทธิภาพและ Update อย่างสม่ำเสมอแล้ว สำนักงาน กสม. ยังได้ติดตั้ง Scan Virus Software บนเครื่อง Server โดยเฉพาะอีกด้วย

๒.๓ Cookies เป็นไฟล์คอมพิวเตอร์เล็ก ๆ ที่จะทำการเก็บข้อมูลชั่วคราวที่จำเป็น ลงในเครื่องคอมพิวเตอร์ของผู้ขอใช้บริการ เพื่อความสะดวกและรวดเร็วในการติดต่อสื่อสาร อย่างไรก็ตาม สำนักงาน กสม. ตระหนักถึงความเป็นส่วนตัวของผู้ใช้บริการเป็นอย่างดี จึงหลีกเลี่ยงการใช้ Cookies แต่ถ้าหากมีความจำเป็น ต้องใช้ Cookies สำนักงาน กสม. จะพิจารณาอย่างรอบคอบและตระหนักถึงความปลอดภัย และความเป็นส่วนตัวของผู้ขอรับบริการเป็นหลัก

๒.๔ Auto Log off ในการใช้บริการของสำนักงาน กสม. หลังจากเลิกการใช้งานควร Log off ทุกครั้ง กรณีที่ผู้ใช้บริการลืม Log off ระบบจะทำการ Log off ให้โดยอัตโนมัติภายในเวลาที่เหมาะสมของแต่ละบริการ ทั้งนี้เพื่อความปลอดภัยของผู้ใช้บริการเอง

๓. ข้อแนะนำเกี่ยวกับการรักษาความมั่นคงปลอดภัย

แม้ว่าสำนักงาน กสม. จะมีมาตรฐานเทคโนโลยีและวิธีการทางด้านการรักษาความปลอดภัยอย่างสูง เพื่อช่วยมิให้มีการเข้าสู่ข้อมูลส่วนตัวหรือข้อมูลที่เป็นความลับของท่านโดยปราศจากอำนาจตามที่กล่าวข้างต้นแล้วก็ตาม แต่ก็เป็นที่ทราบกันอยู่โดยทั่วไปว่า ปัจจุบันนี้ยังมิได้มีระบบ รักษาความปลอดภัยใด ๆ ที่จะสามารถปกป้องข้อมูลของท่านได้อย่างเด็ดขาด จากการถูกทำลาย หรือถูกเข้าถึงโดยบุคคลที่ปราศจากอำนาจได้ ดังนั้นท่านจึงควรปฏิบัติตามข้อแนะนำเกี่ยวกับการรักษาความมั่นคงปลอดภัยดังต่อไปนี้ด้วย คือ

๓.๑ ระมัดระวังในการ Download Program จาก Internet มาใช้งาน ควรตรวจสอบ Address ของเว็บไซต์ให้ถูกต้องก่อน Login เข้าใช้บริการเพื่อป้องกันกรณีที่มีการปลอมแปลงเว็บไซต์

๓.๒ ควรติดตั้งระบบตรวจสอบไวรัส (Anti-Virus) ไว้ที่เครื่องและพยายามปรับปรุงให้โปรแกรมตรวจสอบไวรัสในเครื่องของท่านมีความทันสมัยอยู่เสมอ

๓.๓ ติดตั้งโปรแกรมประเภท Personal Firewall เพื่อป้องกันเครื่องคอมพิวเตอร์ จากการจู่โจมของผู้ไม่ประสงค์ดี เช่น Cracker หรือ Hacker

ภาคผนวก ง. นโยบายการคุ้มครองข้อมูลส่วนบุคคล ของเว็บไซต์สำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ

สำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ (สำนักงาน กสม.) ได้จัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคล ฉบับนี้ขึ้น เพื่อคุ้มครองข้อมูลส่วนบุคคลของผู้ใช้บริการทุกท่าน (Personal information) ที่ติดต่อเข้ามายังเว็บไซต์ของสำนักงาน กสม. ดังนี้

๑. การเก็บรวบรวมข้อมูลส่วนบุคคล

๑.๑ เพื่อความสะดวกในการให้บริการแก่ผู้ใช้บริการทุกท่านที่เข้ามาใช้บริการเว็บไซต์ของสำนักงาน กสม. จึงได้จัดเก็บรวบรวมข้อมูลส่วนบุคคลของท่านไว้ เช่น อีเมล์แอดเดรส (Email Address) ชื่อ (Name) ที่อยู่หรือที่ทำงาน (Home or Work Address) เขตไปรษณีย์ (ZIP Code) หรือหมายเลขโทรศัพท์ (Telephone Number) เป็นต้น ทั้งนี้ เป็นไปตามแบบฟอร์มในการเก็บรวบรวมข้อมูลส่วนบุคคลในกิจกรรมที่เกี่ยวข้อง

๑.๒ ในกรณีที่ท่านสมัคร (Sign Up) เพื่อสมัครสมาชิกหรือเพื่อใช้บริการอย่างใดอย่างหนึ่ง สำนักงาน กสม. จะเก็บรวบรวมข้อมูลส่วนบุคคลของท่านเพิ่มเติม ได้แก่ เพศ (Sex) อายุ (Gender) สิ่งที่โปรดปราน/ความชอบ (Preferences/Favorites) ความสนใจ (Interests) ทั้งนี้ เป็นไปตามแบบฟอร์มในการเก็บรวบรวมข้อมูลส่วนบุคคลในกิจกรรมที่เกี่ยวข้อง

๑.๓ นอกจากนั้น เพื่อสำรวจความนิยมในการใช้บริการ อันจะเป็นประโยชน์ในการนำสถิติไปใช้ในการปรับปรุงคุณภาพในการให้บริการของสำนักงาน กสม. จึงจำเป็นต้องจัดเก็บรวบรวมข้อมูลของท่านบางอย่างเพิ่มเติม ได้แก่ หมายเลขไอพี (IP Address) ชนิดของโปรแกรม ค้นผ่าน (Browser Type) โดเมนเนม (Domain Name) บันทึกหน้าเว็บ (web page) ของเว็บไซต์ที่ผู้ใช้เยี่ยมชม เวลาที่เยี่ยมชมเว็บไซต์ (Access Times) และเว็บไซต์ที่ผู้ใช้บริการเข้าถึงก่อนหน้านั้น (Referring Website Addresses)

๑.๔ สำนักงาน กสม. ขอแนะนำให้ท่านตรวจสอบนโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) ของเว็บไซต์อื่นที่เชื่อมโยงจากเว็บไซต์นี้เพื่อจะได้ทราบและเข้าใจว่าเว็บไซต์ดังกล่าวเก็บรวบรวม ใช้หรือดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลของท่านอย่างไร ทั้งนี้ สำนักงาน กสม. ไม่สามารถรับรองข้อความ หรือรับรองการดำเนินการใด ๆ ตามที่ได้มีการประกาศไว้ในเว็บไซต์ดังกล่าวได้และไม่ขอรับผิดชอบใด ๆ หากเว็บไซต์เหล่านั้น ไม่ได้ปฏิบัติการหรือดำเนินการใด ๆ ตามนโยบายการคุ้มครองข้อมูลส่วนบุคคลที่เว็บไซต์ดังกล่าวได้ประกาศไว้

๒.ระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคล

๒.๑ ในกรณีที่เป็นข้อมูลส่วนบุคคลที่ได้มีการเก็บรวบรวมตามกิจกรรมหรือบริการที่เกี่ยวข้องกับภารกิจของสำนักงาน กสม. จะมีระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคลตามระเบียบสำนักนายกรัฐมนตรีว่าด้วยงานสารบรรณหรือที่เกี่ยวข้อง

๒.๒ ในกรณีเป็นข้อมูลส่วนบุคคลที่อยู่ในลักษณะข้อมูลจราจรทางคอมพิวเตอร์จะมีระยะเวลาการเก็บรักษาตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม (ฉบับที่ ๒) พ.ศ. ๒๕๖๐

๓. การใช้ข้อมูลส่วนบุคคล

๓.๑ สำนักงาน กสม. จะใช้ข้อมูลส่วนบุคคลของท่านเพียงเท่าที่จำเป็น เช่น ชื่อ และที่อยู่ เพื่อใช้ในการติดต่อให้บริการ ประชาสัมพันธ์หรือให้ข้อมูลข่าวสารต่าง ๆ รวมทั้งสำรวจความคิดเห็นของท่าน ในกิจการหรือกิจกรรมของสำนักงาน กสม. เท่านั้น

๓.๒ สำนักงาน กสม. ขอรับรองว่าจะไม่นำข้อมูลส่วนบุคคลของท่านที่สำนักงาน กสม. ได้เก็บรวบรวมไว้ไปขายหรือเผยแพร่ให้กับบุคคลภายนอกโดยเด็ดขาด เว้นแต่จะได้รับอนุญาตจากท่านเท่านั้น

๓.๓ ในกรณีที่ สำนักงาน กสม. ได้ว่าจ้างหน่วยงานอื่นเพื่อให้ดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลของท่าน เช่น การจัดส่งพัสดุไปรษณีย์ การวิเคราะห์เชิงสถิติในกิจการหรือกิจกรรมของสำนักงาน กสม. เป็นต้น สำนักงาน กสม. จะกำหนดให้หน่วยงานที่ได้ว่าจ้างให้ดำเนินการดังกล่าว เก็บรักษาความลับ และความปลอดภัยของข้อมูลส่วนบุคคลของท่าน และกำหนดข้อห้ามมิให้มีการนำข้อมูลส่วนบุคคลดังกล่าวไปใช้นอกเหนือจากกิจกรรมหรือกิจการของสำนักงาน กสม.

๔. สิทธิในการควบคุมข้อมูลส่วนบุคคลของท่าน

เพื่อประโยชน์ในการรักษาความเป็นส่วนตัวของท่าน ท่านมีสิทธิเลือกที่จะให้มีการใช้หรือแชร์ข้อมูลส่วนบุคคลของท่าน หรืออาจเลือกที่จะไม่รับข้อมูลหรือสื่อทางการตลาดใด ๆ จากสำนักงาน กสม. ก็ได้โดยเลือกจากเมนู cookie บนหน้าเว็บไซต์ https://www.nhrc.or.th

๕. การรักษาความปลอดภัยสำหรับข้อมูลส่วนบุคคล

เพื่อประโยชน์ในการรักษาความลับและความปลอดภัยสำหรับข้อมูลส่วนบุคคลของท่าน สำนักงาน กสม. จึงได้กำหนดระเบียบภายในหน่วยงานเพื่อกำหนดสิทธิในการเข้าถึง หรือใช้ข้อมูลส่วนบุคคลของท่าน และเพื่อรักษาความลับและความปลอดภัยของข้อมูลตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงาน กสม. ทั้งนี้ ในกรณีที่ต้องให้ผู้ใช้งานเว็บไซต์กรอกข้อมูล ได้มีการจัดให้มี การใช้ Secure Socket Layer (SSL) protocol เพื่อรักษาความปลอดภัยในการใช้งานเว็บไซต์

๖. การใช้คุกกี้ (Cookies)

“คุกกี้” คือ ข้อมูลที่เว็บไซต์สำนักงาน กสม. ส่งไปยังโปรแกรมค้นผ่านเว็บไซต์ (Web browser) ของผู้ใช้บริการและเมื่อมีการติดตั้งข้อมูลดังกล่าวไว้ในระบบของท่านแล้ว หากมีการใช้ “คุกกี้” ก็จะทำให้เว็บไซต์สำนักงาน กสม.

สามารถบันทึกหรือจดจำข้อมูลของผู้ใช้บริการไว้ จนกว่าผู้ใช้บริการจะออกจากโปรแกรมค้นผ่านเว็บไซต์หรือจนกว่าผู้ใช้บริการจะทำการลบ “คุกกี้” นั้นเสีย หรือไม่อนุญาตให้ “คุกกี้” นั้น ทำงานอีกต่อไป

หากท่านเลือกใช้ “คุกกี้” แล้ว ท่านจะได้รับความสะดวกสบายในการท่องเว็บไซต์มากขึ้น เพราะ “คุกกี้” จะช่วยจดจำเว็บไซต์ที่ท่านแวะหรือเยี่ยมชม ทั้งนี้เว็บไซต์สำนักงาน กสม. จะนำข้อมูลที่ “คุกกี้” ได้บันทึกหรือเก็บรวบรวมไว้ไปใช้ในการวิเคราะห์เชิงสถิติ หรือในกิจกรรมอื่นของสำนักงาน กสม. เพื่อปรับปรุงคุณภาพการให้บริการของสำนักงาน กสม. ต่อไป

๗. การปรับปรุงนโยบายการคุ้มครองข้อมูลส่วนบุคคล

สำนักงาน กสม. อาจทำการปรับปรุงหรือแก้ไขนโยบายการคุ้มครองข้อมูลส่วนบุคคล โดยมิได้แจ้งให้ท่านทราบล่วงหน้า ทั้งนี้ เพื่อความเหมาะสมและมีประสิทธิภาพในการให้บริการ ดังนั้น สำนักงาน กสม. ขอแนะนำให้ผู้ใช้บริการอ่านนโยบายการคุ้มครองข้อมูลส่วนบุคคลทุกครั้งที่เยี่ยมชม หรือมีการใช้บริการจากเว็บไซต์ของสำนักงาน กสม.

๘. การปฏิบัติตามนโยบายคุ้มครองข้อมูลส่วนบุคคลและการติดต่อกับสำนักงาน กสม.

ในกรณีที่ท่านมีข้อสงสัย ข้อเสนอแนะ หรือข้อติชมใด ๆ เกี่ยวกับนโยบายการคุ้มครองข้อมูลส่วนบุคคล หรือการปฏิบัติตามนโยบายการคุ้มครองข้อมูลส่วนบุคคลฉบับนี้ สำนักงาน กสม. ยินดีที่จะตอบข้อสงสัย รับฟังข้อเสนอแนะและคำติชมทั้งหลาย อันจะเป็นประโยชน์ต่อการปรับปรุงการให้บริการของสำนักงาน กสม. ต่อไป โดยท่านสามารถติดต่อกับสำนักงาน กสม. ตามที่ปรากฏข้างล่างนี้

สำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ
ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา ๕ ธันวาคม ๒๕๕๐ อาคารรัฐประศาสนภักดี (อาคารบี) ชั้น ๗
เลขที่ ๑๒๐ ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ ๑๐๒๑๐ โทรศัพท์ ๐-๒๑๔๑-๓๘๐๐

ภาคผนวก จ. นโยบายคุกกี้ของสำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ

เมื่อท่านได้เข้าสู่เว็บไซต์สำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ (www.nhrc.or.th) ข้อมูลที่เกี่ยวข้องกับการเข้าสู่เว็บไซต์ของท่านจะถูกเก็บเอาไว้ในรูปแบบของคุกกี้ โดยนโยบายคุกกี้นี้จะอธิบายถึงความหมาย การทำงาน วัตถุประสงค์ รวมถึงการลบและการปฏิเสธการเก็บคุกกี้เพื่อความเป็นส่วนตัวของท่าน โดยการเข้าสู่เว็บไซต์นี้ถือว่าท่านได้อนุญาตให้บริษัทใช้คุกกี้ตามนโยบายคุกกี้ที่มีรายละเอียดดังต่อไปนี้

๑. คุกกี้คืออะไร

คุกกี้ คือ ไฟล์เล็ก ๆ เพื่อจัดเก็บข้อมูลการเข้าใช้งานเว็บไซต์ เช่น วันเวลา ลิงค์ที่คลิก หน้าที่เข้าชม เงื่อนไขการตั้งค่าต่าง ๆ โดยจะบันทึกลงไปในอุปกรณ์คอมพิวเตอร์ และ/หรือ เครื่องมือสื่อสารที่เข้าใช้งานของท่าน เช่น โน๊ตบุ๊ค แท็บเล็ต หรือ สมาร์ทโฟน ผ่านทางเว็บเบราว์เซอร์ในขณะที่ท่านเข้าสู่เว็บไซต์ โดยคุกกี้จะไม่ก่อให้เกิดอันตรายต่ออุปกรณ์คอมพิวเตอร์ และ/หรือ เครื่องมือสื่อสารของท่าน ในกรณีดังต่อไปนี้ ข้อมูลส่วนบุคคลของท่านอาจถูกจัดเก็บเพื่อใช้เพิ่มประสบการณ์การใช้งานบริการทางออนไลน์ โดยจะจำเอกลักษณ์ของภาษาและปรับแต่งข้อมูลการใช้งานตามความต้องการของท่าน เป็นการยืนยันคุณลักษณะเฉพาะตัว ข้อมูลความปลอดภัยของท่าน รวมถึงบริการที่ท่านสนใจ นอกจากนี้คุกกี้ยังถูกใช้เพื่อวัดปริมาณการเข้าใช้งานบริการทางออนไลน์ การปรับเปลี่ยนเนื้อหาตามการใช้งานของท่านโดยพิจารณาจากพฤติกรรมการเข้าใช้งานครั้งก่อน ๆ และ ณ ปัจจุบัน และอาจมีวัตถุประสงค์เพื่อการโฆษณาประชาสัมพันธ์

ทั้งนี้ท่านสามารถค้นหาข้อมูลเพิ่มเติมเกี่ยวกับคุกกี้ได้ที่ www.allaboutcookies.org

๒. สำนักงาน กสม. ใช้คุกกี้อย่างไร

สำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ (สำนักงาน กสม.) ใช้คุกกี้ เพื่อบันทึกการเข้าเยี่ยมชมและใช้งานเว็บไซต์ของท่าน โดยทำให้สามารถจดจำการใช้งานเว็บไซต์ของท่านได้ง่ายขึ้น และข้อมูลเหล่านี้จะถูกนำไปเพื่อปรับปรุงเว็บไซต์ของสำนักงาน กสม. ให้ตรงกับความต้องการของท่านมากยิ่งขึ้น เพื่ออำนวยความสะดวกให้เกิดความรวดเร็วในการใช้งานเว็บไซต์ของท่านและในบางกรณี สำนักงาน กสม. จำเป็นต้องให้บุคคลที่สามช่วยดำเนินการดังกล่าว ซึ่งอาจจะต้องใช้อินเตอร์เน็ตโปรโตคอลแอดเดรส (IP Address) และคุกกี้เพื่อวิเคราะห์ทางสถิติ ตลอดจนเชื่อมโยงข้อมูล และประมวลผลตามวัตถุประสงค์ เพิ่มประสิทธิภาพการใช้งานเว็บไซต์

๓. คุกกี้ที่สำนักงาน กสม. ใช้ อาจจะแบ่งได้ ๒ ประเภทตามการจัดเก็บ ดังนี้

Session Cookies เป็นคุกกี้ที่จะอยู่ชั่วคราวเพื่อจดจำท่านในระหว่างที่ท่านเข้าเยี่ยมชมเว็บไซต์ของสำนักงาน กสม. เช่น เฝ้าติดตามภาษาที่ท่านได้ตั้งค่าและเลือกใช้ เป็นต้น และจะมีการลบออกจากเครื่องคอมพิวเตอร์หรืออุปกรณ์ของท่าน เมื่อท่านออกจากเว็บไซต์หรือได้ทำการปิดเว็บเบราว์เซอร์

Persistent Cookie เป็นคุกกี้ที่จะอยู่ตามระยะเวลาที่กำหนดหรือจนกว่าท่านจะลบออก คุกกี้ประเภทนี้จะช่วยให้เว็บไซต์ของสำนักงาน กสม. จดจำท่านและการตั้งค่าต่าง ๆ ของท่านเมื่อท่านกลับมาใช้บริการเว็บไซต์อีกครั้ง ซึ่งจะช่วยให้ท่านเข้าใช้บริการเว็บไซต์ได้สะดวกรวดเร็วยิ่งขึ้น

๔. วัตถุประสงค์ในการใช้งานคุกกี้ที่สำนักงาน กสม. ใช้ มีรายละเอียดดังนี้

๔.๑ คุกกี้ที่มีความจำเป็น (Strictly Necessary Cookies)

คุกกี้ประเภทนี้มีความจำเป็นต่อการให้บริการเว็บไซต์ของสำนักงาน กสม. เพื่อให้ท่านสามารถเข้าใช้งานในส่วนต่าง ๆ ของเว็บไซต์ได้ รวมถึงช่วยจดจำข้อมูลที่ท่านเคยให้ไว้ผ่านเว็บไซต์ การปิด การใช้งานคุกกี้ประเภทนี้จะส่งผลให้ท่านไม่สามารถใช้บริการในสาระสำคัญของสำนักงาน กสม. ซึ่งจำเป็นต้องเรียกใช้คุกกี้ได้

๔.๒. คุกกี้เพื่อการวิเคราะห์และประเมินผลการใช้งาน (Performance Cookies)

คุกกี้ประเภทนี้ช่วยให้สำนักงาน กสม. ทราบถึงการปฏิสัมพันธ์ของผู้ใช้งานในการใช้บริการเว็บไซต์ของสำนักงาน กสม. รวมถึงหน้าเพจหรือพื้นที่ใดของเว็บไซต์ที่ได้รับความนิยม ตลอดจน การวิเคราะห์ข้อมูลด้านอื่น ๆ สำนักงาน กสม. ยังใช้ข้อมูลนี้เพื่อการปรับปรุงการทำงานของเว็บไซต์ และเพื่อเข้าใจพฤติกรรมของผู้ใช้งานมากขึ้น ถึงแม้ว่า ข้อมูลที่คุกกี้นี้เก็บรวบรวมจะเป็นข้อมูลที่ไม่สามารถระบุตัวตนได้ และนำมาใช้วิเคราะห์ทางสถิติเท่านั้น การปิดการใช้งานคุกกี้ประเภทนี้จะส่งผลให้สำนักงาน กสม. ไม่สามารถทราบปริมาณผู้เข้าเยี่ยมชมเว็บไซต์ และไม่สามารถประเมินคุณภาพการให้บริการได้

๔.๓ คุกกี้เพื่อการใช้งานเว็บไซต์ (Functional Cookies)

คุกกี้ประเภทนี้จะช่วยให้เว็บไซต์ของสำนักงาน กสม. จดจำตัวเลือกต่าง ๆ ที่ท่านได้ตั้งค่าไว้ และช่วยให้เว็บไซต์ส่งมอบคุณสมบัติและเนื้อหาเพิ่มเติมให้ตรงกับการใช้งานของท่านได้ เช่น จดจำ การเปลี่ยนแปลงการตั้งค่าขนาดฟอนต์หรือการตั้งค่าต่าง ๆ ของหน้าเพจซึ่งท่านสามารถปรับแต่งได้ การปิดการใช้งานคุกกี้ประเภทนี้อาจส่งผลให้เว็บไซต์ไม่สามารถทำงานได้อย่างสมบูรณ์

๕. ท่านจะจัดการคุกกี้ได้อย่างไร

บราวเซอร์ส่วนใหญ่จะมีการตั้งค่าให้มีการยอมรับคุกกี้เป็นค่าเริ่มต้น อย่างไรก็ตาม ท่านสามารถปฏิเสธการใช้งานหรือลบคุกกี้ในหน้าการตั้งค่าของบราวเซอร์ที่ท่านใช้งานอยู่ ทั้งนี้ หากท่านทำการปรับเปลี่ยนการตั้งค่าบราวเซอร์ของท่านอาจส่งผลกระทบต่อรูปแบบและการใช้งานบนหน้าเว็บไซต์ของเราได้ หากท่านประสงค์ที่จะทำการปรับเปลี่ยนการตั้งค่า ท่านสามารถตรวจสอบรายละเอียดเพิ่มเติมได้ตามลิงก์ที่ได้ระบุไว้ข้างล่าง

- Android (Chrome)
- Apple Safari
- Google Chrome
- Microsoft Edge
- Microsoft Internet Explorer
- Mozilla Firefox
- Opera
- Iphone or Ipad (Chrome)
- Iphone or Ipad (Safari)

ทั้งนี้ โปรดทราบว่า หากท่านเลือกที่จะปิดการใช้งานคุกกี้บนเบราว์เซอร์หรืออุปกรณ์ของท่าน อาจส่งผลกระทบกับการทำงานบางส่วนของเว็บไซต์ของ สพร. ที่ไม่สามารถทำงานหรือให้บริการได้เป็นปกติ

สำนักงาน กสม. จะไม่รับผิดชอบและไม่ได้มีความเกี่ยวข้องกับเว็บไซต์ รวมทั้งเนื้อหาในเว็บไซต์ต่าง ๆ ที่กล่าวมาข้างบน

สำหรับข้อมูลอื่น ๆ เพิ่มเติมในเรื่องนี้ ท่านสามารถเข้าไปอ่านได้ที่ https://www.aboutcookies.org/how-to-delete-cookies

๖. การเชื่อมโยงข้อมูลกับเว็บไซต์อื่น

เว็บไซต์ของสำนักงาน กสม. อาจมีการเชื่อมโยงไปยังเว็บไซต์หรือโซเชียลมีเดียของบุคคลภายนอก รวมถึงอาจมีการฝังเนื้อหาหรือวีดีโอที่มาจากโซเชียลมีเดีย เช่น YouTube หรือ Facebook เป็นต้น ซึ่งจะช่วยให้ท่านเข้าถึงเนื้อหาและสร้างการปฏิสัมพันธ์กับบุคคลอื่นบนโซเชียลมีเดียจากเว็บไซต์ของสำนักงาน กสม. ได้ ซึ่งเว็บไซต์หรือโซเชียลมีเดียของบุคคลภายนอกจะมีการกำหนดและตั้งค่าคุกกี้ขึ้นมาเอง โดยที่สำนักงาน กสม. ไม่สามารถควบคุมหรือรับผิดชอบต่อคุกกี้เหล่านั้นได้ และขอแนะนำให้ท่านควรเข้าไปอ่านและศึกษานโยบายหรือประกาศการใช้คุกกี้ของบุคคลภายนอกเหล่านั้นด้วย

๗. การเปลี่ยนแปลงนโยบายคุกกี้

ประกาศนี้อาจมีการปรับปรุงให้เหมาะสมและสอดคล้องกับสถานการณ์และตามการให้บริการจริง โดยสำนักงาน กสม. จะมีการแจ้งประกาศที่มีการปรับปรุงใหม่บนเว็บไซต์นี้ ดังนั้นสำนักงาน กสม. ขอแนะนำให้ท่านตรวจสอบให้แน่ใจว่าท่านได้เข้าใจการเปลี่ยนแปลงตามข้อกำหนดดังกล่าว

๘. ติดต่อสำนักงาน กสม.

ในกรณีที่ท่านมีคำถามเกี่ยวกับนโยบายคุกกี้ของเรา สามารถติดต่อสอบถามได้ที่อีเมล์ webmaster@nhrc.or.th หรือเบอร์โทรศัพท์ ๐-๒๑๔๑-๓๘๙๖