นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของส่วนราชการในสังกัดสำนักการแพทย์ พ.ศ. ๒๕๖๖

สารบัญ **หน้า**

หมวดที่ ๑

ส่วนที่ ๑
แนวปฏิบัติในการกำหนดหน้าที่ความรับผิดชอบทางด้านสารสนเทศ

การกำหนดหน้าที่ความรับผิดชอบทางด้านสารสนเทศ ในกรณีระบบเทคโนโลยีสารสารเทศและการสื่อสารหรือข้อมูลสารสนเทศ เกิดความเสียหายหรืออันตรายใด ๆ ต่อหน่วยงาน หรือผู้ใดผู้หนึ่งอันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืน การปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานและป้องกันการเข้าถึงข้อมูลโดยบุคคลอื่น รวมถึงการเปิดเผยข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต โดยได้กำหนดบทบาทและความรับผิดชอบให้เป็นไปตามหน้าที่ที่ได้รับมอบหมาย ดังนี้

(๑) ผู้บริหารหน่วยงานสูงสุด เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นกับระบบเทคโนโลยีสารสนเทศและการสื่อสาร

(๒) CIO ของระบบเทคโนโลยีสารสนเทศ มีหน้าที่จัดทำและทบทวนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน โดยกำหนดมาตรการ และกำกับดูแลการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร ให้เป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน

(๓) ผู้ดูแลระบบ หรือผู้ที่ได้รับมอบหมายให้ปฏิบัติงานด้านสารสนเทศ เป็นผู้รับผิดชอบควบคุม ติดตาม และตรวจสอบการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร ให้เป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน

(๔) ผู้ใช้งาน เป็นผู้เข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน ตามสิทธิ์ที่ได้รับอนุญาต โดยให้ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ หน่วยงาน

<u>หน้าที่ความรับผิดชอบของผู้ดูแลระบบ</u>

(๑) จัดทำบัญชีทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสาร โดยระบุผู้รับผิดชอบในทรัพย์สินอย่างชัดเจน

(๒) บริหารจัดการทรัพย์สินที่ใช้สำหรับการให้บริการระบบคอมพิวเตอร์ และระบบเครือข่ายหลัก เพื่อป้องกันไม่ให้ทรัพย์สินเกิดความเสียหาย ใช้งานไม่ได้ หรือสูญหาย

(๓) เก็บรักษาอุปกรณ์ของระบบคอมพิวเตอร์และระบบเครือข่าย ในพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน และอนุญาตให้เข้าถึงได้เฉพาะผู้ดูแลระบบเท่านั้น

(๔) กำหนดสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน ตามที่ได้รับมอบหมาย โดยกำหนดสิทธิ์ให้ผู้ใช้งานสามารถใช้งานได้ตามภารกิจของผู้ใช้งาน และสามารถเข้าใช้ได้แต่เพียงงานที่ได้รับอนุญาตให้เข้าถึงเท่านั้น รวมทั้งดำเนินการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ

(๕) บริหารจัดการการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน ให้เป็นไปด้วยความเรียบร้อยและมีประสิทธิภาพ หากตรวจพบสิ่งผิดปกติให้รีบดำเนินการแก้ไข รวมทั้งป้องกันและบรรเทาความเสียหายที่อาจจะเกิดขึ้นในทันที ในกรณีที่สิ่งผิดปกติดังกล่าวเกิดขึ้นจากการใช้งานของผู้ใช้งานที่ไม่เป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน ให้รีบแจ้งผู้ใช้งานผู้นั้นให้ยุติการกระทำดังกล่าวในทันทีเพื่อป้องกันหรือบรรเทาความเสียหายที่จะเกิดขึ้นต่อหน่วยงาน ให้ผู้ดูแลระบบพิจารณาระงับการใช้งานของผู้ใช้งานดังกล่าวทันที

(๖) ติดตั้งและเปลี่ยนแปลงค่าต่างๆ ของระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงานที่ได้รับมอบหมายและทบทวนการกำหนดค่าต่างๆ อย่างน้อยไตรมาสละ ๑ ครั้ง

(๗) บริหารจัดการข้อมูลคอมพิวเตอร์หรือโปรแกรมคอมพิวเตอร์ที่เกี่ยวข้องกับการปฏิบัติงานของหน่วยงาน สำหรับเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ต่อพ่วงให้มีความปลอดภัยอยู่เสมอ

(๘) จัดเก็บข้อมูลการจราจรทางคอมพิวเตอร์ (Log File) ที่เกี่ยวข้องกับการให้บริการระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์สามารถระบุตัวผู้ใช้งานนับตั้งแต่เริ่มใช้งานและต้องเก็บรักษาไว้อย่างครบถ้วน ถูกต้องตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และประกาศกระทรวงไอซีที เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. ๒๕๕๐ และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐ (ฉบับที่ ๒)

(๙) ไม่ใช้อำนาจหน้าที่ของตนในการเข้าถึงข้อมูลของผู้ใช้งานที่ใช้งานระบบคอมพิวเตอร์ โดยไม่มีเหตุผลอันสมควร

(๑๐) ไม่เปิดเผยข้อมูลที่ได้มาจากการปฏิบัติหน้าที่ ซึ่งข้อมูลดังกล่าวเป็นข้อมูลที่ไม่เปิดเผยให้บุคคลหนึ่งบุคคลใดทราบโดยไม่มีเหตุผลอันสมควร

(๑๑) คืนทรัพย์สินของหน่วยงาน ที่เกี่ยวข้องกับการปฏิบัติหน้าที่ของตนในทันทีที่พ้นจากหน้าที่ และมอบให้ผู้บริหารของหน่วยงาน หรือผู้ที่ได้รับมอบหมายเพื่อทำการตรวจสอบการคืนทรัพย์สินดังกล่าวให้ถูกต้องและครบถ้วน

ส่วนที่ ๒
แนวปฏิบัติการเข้าถึงและควบคุมการใช้งานระบบสารสนเทศ
(Access control)

เพื่อควบคุมการเข้าถึงระบบสารสนเทศโดยกำหนดให้ผู้ที่ได้รับอนุญาตเท่านั้น และป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

๒.๑ หน่วยงานต้องจัดทำบัญชีทรัพย์สินหรือทะเบียนทรัพย์สินและจำแนกกลุ่มทรัพยากรของระบบหรือการทำงาน โดยจะต้องระบุเลขทรัพย์สินที่ชัดเจน และสามารถตรวจสอบสถานที่ติดตั้งได้

๒.๒ กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงและใช้งานระบบสารสนเทศ ดังนี้

(๑) กำหนดสิทธิของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง ให้กำหนดดังนี้

- อ่านอย่างเดียว
- สร้างข้อมูล
- ป้อนข้อมูล
- แก้ไข
- อนุมัติ
- ไม่มีสิทธิ

(๒) ผู้ใช้งานที่มีความประสงค์จะเข้าใช้งานระบบสารสนเทศของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาตจากผู้บังคับบัญชา

(๓) ผู้ดูแลระบบมีหน้าที่ทบทวน ตรวจสอบการอนุญาต และมีสิทธิร่วมกับเจ้าของระบบสารสนเทศหรือเจ้าของข้อมูล อย่างสม่ำเสมอ

(๔) บุคคลจากภายนอกหน่วยงาน ที่ต้องการจะเข้าถึงระบบสารสนเทศของหน่วยงานใดๆ หรือเข้าถึงข้อมูลใดๆ จะต้องขออนุญาตต่อหัวหน้าหน่วยงานเป็นลายลักษณ์อักษร

๒.๓ ข้อกำหนดด้านข้อมูลสารสนเทศ

(๑) ข้อมูลสารสนเทศของหน่วยงาน สามารถจำแนกประเภทได้ ดังนี้

- ข้อมูลสารสนเทศด้านการบริการ เช่น ข้อมูลระบบเว็บไซต์ของหน่วยงาน ข้อมูลระบบหนังสือเวียน ข้อมูลระบบจดหมายอิเล็กทรอนิกส์
- ข้อมูลสารสนเทศด้านการดำเนินการ เช่น ระบบ MIS
- ข้อมูลสารสนเทศด้านการให้บริการผู้ป่วย เช่น ระบบ e-Phis ระบบจัดเก็บเวชระเบียนผู้ป่วย ระบบ PACS

(๒) การจัดแบ่งระดับชั้นการเข้าถึงข้อมูลสารสนเทศแต่ละประเภท ดังนี้

- สามารถเข้าถึงได้เฉพาะผู้มีสิทธิ์สูงสุดในการบริหารจัดการระบบสารสนเทศ
- สามารถเข้าถึงได้เฉพาะผู้ใช้งานที่ได้รับอนุมัติสิทธิ์จากเจ้าของระบบงานหรือเจ้าของข้อมูลแล้วเท่านั้น
- สามารถเข้าถึงได้เฉพาะกลุ่มผู้ใช้งานที่เกี่ยวข้อง
- สามารถเข้าถึงได้โดยทุกกลุ่มผู้ใช้งานที่กำหนดไว้แล้ว

(๓) การกำหนดเวลาการเข้าถึง ดังนี้

- การเข้าถึงข้อมูลสารสนเทศในเวลาราชการ (๐๘.๐๐ – ๑๖.๐๐ น.)
- การเข้าถึงข้อมูลสารสนเทศนอกเวลาราชการ (นอกช่วงเวลา ๑๖.๐๐ – ๐๘.๐๐ น.)

- การเข้าถึงข้อมูลสารสนเทศในช่วงเวลาวันหยุดราชการ (วันหยุดราชการ และวันหยุด-นักขัตฤกษ์)
- การเข้าถึงข้อมูลสารสนเทศในช่วงเวลาพิเศษเป็นรายครั้ง (ระบุช่วงการเข้าถึงและจำนวนระยะเวลาการเข้าถึง)

(๔) การกำหนดจำนวนช่องทางที่สามารถเข้าถึงได้ ดังนี้

- ระบบการเชื่อมโยงภายในพื้นที่ระยะใกล้ (LAN) ในลักษณะมีเครื่องคอมพิวเตอร์ให้บริการและเครื่องคอมพิวเตอร์ใช้บริการ (Client Server)
- ระบบเครือข่ายภายใน (Intranet) ในลักษณะเครือข่ายเสมือนและมีการเข้ารหัส (SSL VPN)
- ระบบอินเทอร์เน็ต (Internet) ในลักษณะใช้โปรแกรมเว็บบราวเซอร์ (Web Base Application)

(๕) การรักษาความลับของข้อมูลสารสนเทศ

- ปฏิบัติตามระเบียบการรักษาความลับ ทางราชการ พ.ศ. ๒๕๔๔ เว้นแต่มีการประกาศไว้เป็นอย่างอื่น
- การรับส่งข้อมูลที่เป็นความลับผ่านเครือข่ายสารธารณะต้องมีการเข้ารหัสข้อมูลที่เป็นมาตรฐานสากลเพื่อดำเนินการป้องกันข้อมูลสารสนเทศให้ปลอดภัย และมีประสิทธิภาพ เช่น อัลกอริทึม RSA, Blowfish, IDEA, DES, 3DES เป็นต้น
- ความยาวของคีย์ในการเข้ารหัสต้องไม่น้อยกว่า ๕๖ บิตสำหรับการเข้ารหัสแบบสมมาตร (symmetric) และแบบอสมมาตร (asymmetric)

ส่วนที่ ๓
แนวปฏิบัติการบริหารจัดการการเข้าถึงของผู้ใช้งาน
(User access management)

แนวปฏิบัติในการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User access management) มีวิธีการปฏิบัติ ดังนี้

๓.๑ การลงทะเบียนผู้ใช้งาน (User registration)

มีการกำหนดขั้นตอนปฏิบัติในการลงทะเบียนผู้ใช้งาน ดังนี้

(๑) จัดทำแบบฟอร์มขอใช้ระบบงานสารสนเทศ และให้ผู้ใช้งานกรอกข้อมูลลงในแบบฟอร์ม เพื่อตรวจสอบสิทธิและดำเนินการตามขั้นตอนการลงทะเบียนผู้ใช้งาน โดยในแบบฟอร์มต้องระบุข้อมูลพื้นฐานอย่างน้อยดังนี้ ชื่อและนามสกุล ตำแหน่ง หน่วยงาน หมายเลขบัตรประจำตัวประชาชน
วัน เดือน ปีเกิด หมายเลขโทรศัพท์

(๒) ผู้ดูแลระบบตรวจสอบความถูกต้องของข้อมูลและตรวจสอบว่าเคยมีการการลงทะเบียนผู้ใช้งานมาก่อนหรือไม่ เพื่อดำเนินการต่อไป

(๓) ผู้ดูแลระบบต้องตรวจสอบและให้สิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ

(๔) ผู้ดูแลระบบพิจารณาอนุมัติชื่อผู้ใช้งานและรหัสผ่าน และแจ้งผลการอนุมัติ โดยแจ้งเป็นเอกสารหลักฐาน หรือแจ้งผ่านระบบส่งข้อความสั้น (sms) หรือแล้วแต่กรณีตามเหตุผลความจำเป็น

(๕) ผู้ดูแลระบบต้องจัดเก็บข้อมูลของการลงทะเบียนผู้ใช้งาน เพื่อเอาไว้ตรวจสอบในภายหลัง

(๖) การกำหนดชื่อผู้ใช้งาน (username) จะกำหนดจากชื่อภาษาอังกฤษและตามด้วยอักษร ตัวแรกของนามสกุล หากซ้ำ ให้เพิ่มอักษรตัวที่สอง หรือจนกว่าจะไม่ซ้ำกับชื่อผู้ใช้งานคนอื่น

๓.๒ การบริหารจัดการสิทธิของผู้ใช้งาน (User privilege management)

มีการกำหนดการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงดังนี้

(๑) ผู้ดูแลระบบต้องกำหนดสิทธิการใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน ให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่ และต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ โดยสามารถแบ่งสิทธิดังต่อไปนี้

(๑.๑) ระดับผู้ใช้งานที่ได้รับมอบหมายให้สามารถใช้งานตามภารกิจ ทุกคนจะมีสิทธิในการใช้งานระบบได้แก่

- ระบบระบบเครือข่ายภายใน (intranet)
- ระบบอินเทอร์เน็ต (internet)
- ระบบจดหมายอิเล็กทรอนิกส์ (e-mail)
- ระบบเครือข่ายเสมือนและมีการเข้ารหัส (SSL VPN)

(๑.๒) ระดับผู้บริหาร ได้แก่ ตำแหน่งประเภทบริหาร ตำแหน่งประเภทอำนวยการ ตำแหน่งประเภทหัวหน้าฝ่าย หรือตำแหน่งอื่นๆ ที่ได้รับมอบหมายให้สามารถใช้งานตามภารกิจ

(๑.๓) ระดับผู้ดูแลระบบจะได้รับสิทธิเพิ่มเติมจากสิทธิของผู้ใช้งานในการเข้าถึงระบบสารสนเทศดังนี้

- ระบบบริหารจัดการระบบเครือข่าย (network)
- ระบบบริหารจัดการระบบอินเทอร์เน็ต (internet)
- ระบบบริหารจัดการระบบจดหมายอิเล็กทรอนิกส์ (e-mail)

- ระบบบริหารจัดการโครงการจัดระบบข้อมูลและข่ายงาน (MIS)
- ระบบบริหารจัดการระบบเครือข่ายไร้สาย (Wi-Fi)
- ระบบบริหารจัดการเครื่องแม่ข่าย (server)

(๑.๔) สำหรับบุคคลภายนอก เช่น นักศึกษาแพทย์ จะมีสิทธิเข้าถึงระบบดังนี้

- ระบบอินเทอร์เน็ต (internet) โดยมีการแบ่งแยกจากกลุ่มผู้ใช้งาน
- ระบบอื่นๆ ที่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากเจ้าของระบบสารสนเทศหรือเจ้าของข้อมูล

(๒) ผู้ดูแลระบบต้องกำหนดระดับสิทธิในการเข้าถึงที่เหมาะสมสำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน

(๓) ผู้ดูแลระบบต้องมอบหมายสิทธิ ให้มีความสอดคล้องกับแนวปฏิบัติในการควบคุมการเข้าถึงระบบสารสนเทศ

(๔) ผู้ดูแลระบบต้องจัดเก็บการมอบหมายสิทธิให้แก่ผู้ใช้งาน

(๕) กรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานให้มีสิทธิสูงกว่าปกติ จะต้องมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันที เมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และให้มีการกำหนดสิทธิพิเศษที่ได้รับด้วยว่าการเข้าถึงได้นั้นสามารถเข้าถึงได้ในระดับใดบ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

(๖) ผู้ใช้งานต้องรับทราบสิทธิและหน้าที่เกี่ยวกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร หน่วยงานและต้องปฏิบัติตามอย่างเคร่งครัด

๓.๓ การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User password management) ต้องมีการดำเนินการดังนี้

(๑) ผู้ดูแลระบบต้องกำหนดขั้นตอนปฏิบัติ สำหรับการตั้งหรือเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัย

(๒) การส่งมอบรหัสผ่านต้องกระทำโดยปลอดภัย อาจใส่ซองปิดผนึก หรือส่งมอบทางข้อความสั้นผ่านเครือข่ายโทรศัพท์มือถือ หรือแล้วแต่กรณี

(๓) ผู้ดูแลระบบต้องกำหนดรหัสผ่านชั่วคราว โดยกำหนดรหัสผ่านให้มีความยากต่อการเดาโดยผู้อื่น และ ควรกำหนดรหัสผ่านที่แตกต่างกัน

(๔) ผู้ดูแลระบบต้องให้ผู้ใช้งานเปลี่ยนรหัสผ่านโดยทันที ภายหลังจากที่ได้รับรหัสผ่านชั่วคราว และควร เปลี่ยนรหัสผ่านให้มีความยากต่อการเดาโดยผู้อื่น

(๕) ผู้ดูแลระบบสารสนเทศต้องกำหนดจำนวนครั้งที่ยินยอมให้ผู้ใช้งานใส่รหัสผ่านผิดพลาดได้ไม่เกิน ๓ ครั้ง

๓.๔ การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of user access rights) ต้องมีการดำเนินการดังนี้

(๑) ผู้ดูแลระบบดำเนินการทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อเกิดการเปลี่ยนแปลงสิทธิของผู้ใช้งาน อันได้แก่ ลาออก การย้ายหน่วยงาน เพื่อความถูกต้องและเป็นปัจจุบันของข้อมูลของผู้ใช้งาน

(๒) ผู้ดูแลระบบต้องดำเนินการตรวจสอบสิทธิและติดตามการใช้งานตามสิทธิที่ได้รับของแต่ละระบบ

(๓) ผู้ดูแลระบบต้องกำหนดให้มีการเพิกถอนสิทธิหรือระงับการใช้งานของแต่ละสิทธิแตกต่างกันไปตามหน้าที่ที่รับผิดชอบในแต่ละระบบ

ส่วนที่ ๔
แนวปฏิบัติการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities) เพื่อป้องกันการเข้าถึงและใช้งาน ระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน โดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้หรือการลักลอบทำสำเนาข้อมูลสารสนเทศและการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ มีแนวทางปฏิบัติดังนี้

๔.๑ การใช้งานรหัสผ่าน (Password Use) ผู้ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน ควรปฏิบัติตามข้อกำหนดในการใช้งานรหัสผ่าน ดังนี้

(๑) เปลี่ยนรหัสผ่านชั่วคราวทันทีเมื่อล็อกอินเข้าใช้งานระบบครั้งแรก

(๒) ควรกำหนดรหัสผ่าน ให้มีตัวอักษรจำนวนมากกว่าหรือเท่ากับ ๘ ตัวอักษร โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวเลข หรือสัญลักษณ์เข้าด้วยกัน

(๔) ไม่ตั้งรหัสผ่านจากอักขระที่เรียงกัน หรือกลุ่มเหมือนกัน

(๖) ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น หรือเก็บไว้ในระบบคอมพิวเตอร์

(๗) ต้องไม่กำหนดให้มีการบันทึกหรือช่วยจำรหัสผ่านส่วนบุคคล (save password)

(๘) ไม่ใช้รหัสผ่านของตนเองร่วมกับผู้อื่น

(๙) กรณีที่มีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่นเนื่องจากงาน หลังจากดำเนินการเรียบร้อย ให้ทำการเปลี่ยนรหัสผ่านโดยทันที

(๑๐) ควรมีการเปลี่ยนรหัสผ่านตามรอบระยะเวลาที่กำหนดไว้ หรือเปลี่ยนรหัสผ่านทันทีเมื่อทราบว่ารหัสผ่านอาจถูกเปิดเผยหรือล่วงรู้

(๑๑) หลีกเลี่ยงการใช้รหัสผ่านเดียวกันสำหรับระบบงานต่างๆ ที่ตนใช้งาน

(๑๒) หลีกเลี่ยงการใช้รหัสผ่านเดิม

(๑๓) ผู้ดูแลระบบต้องเปลี่ยนรหัสถี่กว่าผู้ใช้งานทั่วไป

๔.๒ การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ ต้องมีการดำเนินการดังนี้

(๑) ผู้ใช้งานและผู้ดูแลระบบต้องตั้งให้เครื่องคอมพิวเตอร์ล็อคหน้าจอหลังจากที่ไม่ได้ใช้งานเป็นเวลา ๓๐ นาที และต้องใส่รหัสผ่านให้ถูกต้องจึงจะสามารถเปิดหน้าจอได้

(๒) ผู้ใช้งานและผู้ดูแลระบบต้องล็อคอุปกรณ์และเครื่องคอมพิวเตอร์ที่สำคัญ เมื่อไม่ได้ถูกใช้งานหรือต้องปล่อยทิ้ง โดยไม่ได้ดูแลชั่วคราว

๔.๓ การควบคุมทรัพย์สินสารสนเทศและการใช้งานระบบคอมพิวเตอร์ (clear desk and clear screen policy) ต้องควบคุมไม่ให้ทรัพย์สินสารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์หรือสารสนเทศ อยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน ดังนี้

(๑) ผู้ใช้งานต้องป้องกันทรัพย์สินของหน่วยงานและควบคุมไม่ให้มีการทิ้งหรือปล่อยทรัพย์สินสารสนเทศ ที่สำคัญให้อยู่ในสถานที่ที่ไม่ปลอดภัย โดยให้ครอบคลุมเรื่องต่างๆ ประกอบด้วย

- การจัดการบริเวณล้อมรอบ
- การควบคุมการเข้า-ออก

- การจัดบริเวณการเข้าถึง การส่งผลิตภัณฑ์โดยบุคคลภายนอก
- การวางอุปกรณ์
- ระบบและอุปกรณ์สนับสนุนการทำงาน

(๒) การป้องกันต้องมีความสอดคล้องกับเรื่องต่างๆ ดังนี้

- แนวทางการจัดหมวดหมู่สารสนเทศและการจัดการกับสารสนเทศ
- กฎหมาย ระเบียบ ข้อบังคับ หรือข้อกำหนดอื่นๆ
- วัฒนธรรมองค์กร

(๓) มีการกำหนดขอบเขตของการป้องกัน ดังนี้

- ลงชื่อออกจากระบบทันที เมื่อจำเป็นต้องปล่อยทิ้งโดยไม่มีผู้ดูแล
- จัดเก็บข้อมูลสำคัญในสถานที่ที่มีความปลอดภัย
- ล็อคเครื่องคอมพิวเตอร์ เมื่อไม่ได้ใช้งาน
- ป้องกันไม่ให้ผู้อื่นใช้อุปกรณ์ดังต่อไปนี้โดยไม่ได้รับอนุญาต ได้แก่ กล้องดิจิตอล เครื่องสำเนาเอกสาร เครื่องสแกนเอกสาร กล้องจากโทรศัพท์สมาร์ทโฟน เป็นต้น
- นำเอกสารออกจากเครื่องพิมพ์ทันทีที่พิมพ์งานเสร็จ

๔.๔ ผู้ใช้งานอาจนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับ ทางราชการ พ.ศ. ๒๕๔๔ มีแนวปฏิบัติ ดังนี้

(๑) ทำการประเมินความเสี่ยงเพื่อระบุระดับความสำคัญ และระดับความลับที่เหมาะสม สำหรับข้อมูลที่จำเป็นต้องป้องกัน

(๒) กำหนดหลักการทั่วไปสำหรับการป้องกันข้อมูลโดยใช้การเข้ารหัสข้อมูล

(๓) การจัดเก็บชื่อผู้ใช้งาน (username) และรหัสผ่าน (password) ของระบบสารสนเทศลงในฐานข้อมูลใดๆ จะต้องทำการ เข้ารหัสด้วย MD๕ ใน field ของ password ก่อนบันทึกลงในฐานข้อมูลทุกครั้ง

(๔) ต้องมีการเชื่อมต่อโดยการเข้ารหัส SSL ผ่านโปรโตคอล https สำหรับระบบสารสนเทศแบบ web application เพื่อเป็นการเข้ารหัสข้อมูลที่ส่งระหว่างบราว์เซอร์และเว็บเซิร์ฟเวอร์

(๕) กำหนดช่องทางการรับ – ส่งข้อมูลสำคัญหรือข้อมูลลับที่เหมาะสมกับหน่วยงานสำหรับช่องทางดังต่อไปนี้

- ระบบการสื่อสารข้อมูล ซึ่งรวมถึงระบบการเชื่อมโยงภายในพื้นที่ระยะใกล้ (LAN) และอินเทอร์เน็ต (internet)
- เครือข่ายไร้สายและอุปกรณ์เครือข่ายไร้สาย
- สื่อบันทึกข้อมูลที่สามารถถอดแยกได้ (จากตัวเครื่องคอมพิวเตอร์)

(๖) กำหนดวิธีการในการบริหารจัดการและการใช้งานกุญแจสำหรับการเข้ารหัสข้อมูล ดังนี้

- วิธีการป้องกันกุญแจที่ใช้สำหรับการเข้ารหัสข้อมูล
- วิธีการกู้คืนข้อมูลที่ถูกเข้ารหัสไว้ในกรณีที่กุญแจเกิดการสูญหายหรือถูกทำให้เสียหาย
- บทบาทและผู้มีหน้าที่รับผิดชอบที่เกี่ยวข้องกับการเข้ารหัสข้อมูล ประกอบด้วย ผู้ทำหน้าที่ควบคุมและดูแลกุญแจ การสร้างกุญแจ ผู้ทำหน้าที่ทำลาย ผู้ใช้งาน ผู้ทำหน้าที่จัดการกรณีกุญแจเกิดการสูญหาย

(๗) ระบุข้อมูลเกี่ยวกับการเข้ารหัสข้อมูลที่เป็นความลับหรือวิธีการรักษาความลับของข้อมูล ดังนี้

- ต้องแสดงชั้นความลับบนไฟล์ข้อมูลลับ และแสดงชั้นความลับกับทุกหน้าของไฟล์ดังกล่าว
- ป้องกันไฟล์ข้อมูลลับที่จัดเก็บไว้ในเครื่องคอมพิวเตอร์ด้วยการใช้การเข้ารหัสข้อมูลตามมาตรฐานที่หน่วยงานกำหนด
- ป้องกันไฟล์ข้อมูลลับที่จัดเก็บไว้ในเครื่องคอมพิวเตอร์ที่ตนเองใช้งาน โดยการกำหนดรหัสผ่าน สำหรับไฟล์ที่มีการใช้งาน

(๘) ห้ามแชร์ (share) ไฟล์ข้อมูลลับบนเครือข่ายของหน่วยงานเพื่ออนุญาตให้ผู้อื่นเข้าถึงได้

(๙) ตรวจสอบการทำงานของระบบป้องกันไวรัสอย่างสม่ำเสมอ ในเครื่องคอมพิวเตอร์ที่ใช้ในการจัดเตรียมไฟล์ข้อมูลว่ามีการทำงานป้องกันไวรัสตามปกติหรือไม่

(๑๐) ตรวจสอบการทำงานของเครื่องคอมพิวเตอร์ที่ตนเองใช้งาน ว่ามีการติดตั้งโปรแกรมแก้ไขช่องโหว่ ของซอฟต์แวร์ในเครื่องตามปกติหรือไม่

(๑๑) ดำเนินการสำรองไฟล์ข้อมูลลับในเครื่องคอมพิวเตอร์ที่ตนเองใช้งานอย่างสม่ำเสมอหรือตามความจำเป็น

๔.๕ การทำลายสื่อข้อมูลอิเล็กทรอนิกส์

ประเภทสื่อบันทึก	วิธีการดำเนินการ
แผ่นซีดี/ดีวีดี	ทำการย่อย/ตัด เพื่อทำลายแผ่นซีดี/ดีวีดี
เทป DDS, DAT, LTO	ต้องลบข้อมูลทั้งม้วนเทป (Erase) ผ่าน Tape Device ก่อนการทำลายม้วนเทป
ข้อมูลอิเล็กทรอนิกส์ที่จัดเก็บในฮาร์ดดิสก์ (Hard Disk) หรือ Memory Devices เช่น USB flash drive, SD cards	ทำลายข้อมูลโดยใช้เทคโนโลยีซอฟต์แวร์ Wiping หรือโปรแกรมลบไฟล์ถาวร และไม่สามารถกู้คืนได้

ส่วนที่ ๕
แนวปฏิบัติการควบคุมการเข้าถึงเครือข่าย
(Network access control)

แนวปฏิบัติในการควบคุมการเข้าถึงระบบเครือข่าย (Network access control) เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต มีดังต่อไปนี้

๕.๑ การใช้งานเครือข่าย

(๑) ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

(๒) ผู้ใช้งานระบบเครือข่ายต้องพิสูจน์ยืนยันตัวตน (Authentication) ทุกครั้งที่ใช้ระบบ

(๓) ห้ามเปิดหรือใช้งานโปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยง เว้นแต่จะได้รับ อนุญาตจากผู้ดูแลระบบ

(๔) ห้ามเปิดหรือใช้งานโปรแกรมออนไลน์ทุกประเภท เพื่อความบันเทิง ในระหว่างปฏิบัติงาน

(๕) การใช้งานอินเทอร์เน็ตจะถูกบันทึกการใช้งานไว้เป็นเวลา ๙๐ วัน ตาม พ.ร.บ.กระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และ พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐ (ฉบับที่ ๒)

(๖) ผู้ดูแลระบบเครือข่ายจะต้องจัดให้มีการบันทึกการใช้งาน เพื่อไม่ให้ผู้ใช้งานละเมิดความปลอดภัยและสิทธิการใช้งานของผู้อื่น

(๗) ห้ามมิให้ผู้ใดเข้าใช้งานโดยมิได้รับอนุญาต การบุกรุกหรือพยายามบุกรุกเข้าสู่ระบบถือว่าเป็นการพยายาม รุกล้ำเขตหวงห้ามของทางราชการ

(๘) ผู้ใช้งานต้องไม่ละเมิดต่อผู้อื่น คือ ผู้ใช้งานต้องไม่อ่าน เขียน ลบ เปลี่ยนแปลงหรือแก้ไขใดๆ ในส่วนที่ มิใช่ของตนโดยไม่ได้รับอนุญาต การบุกรุก (Hack) เข้าสู่บัญชีผู้ใช้งาน (User Account) ของผู้อื่น การเผยแพร่ ข้อความใดๆ ที่ก่อให้เกิดความเสียหายเสื่อมเสียแก่ผู้อื่น การใช้ภาษาไม่สุภาพหรือการเขียนข้อความที่ทำให้ผู้อื่น เสียหาย ถือเป็นการละเมิดสิทธิของผู้อื่นทั้งสิ้น ผู้ใช้งานต้องรับผิดชอบแต่เพียงฝ่ายเดียวหน่วยงานไม่มีส่วนร่วมรับผิดชอบความเสียหายดังกล่าว

(๙) หน่วยงานไม่อนุญาตให้ผู้ใช้งานกระทำการใดๆ ที่เข้าข่ายลักษณะเพื่อการค้าหรือการแสวงหาผลกำไร ผ่านเครื่องคอมพิวเตอร์และเครือข่าย เช่น การประกาศแจ้งความ การซื้อหรือการจำหน่ายสินค้า การนำข้อมูลไป ซื้อขาย การรับบริการค้นหาข้อมูลโดยคิดค่าบริการ การให้บริการโฆษณาสินค้า หรือการเปิดบริการอินเทอร์เน็ตแก่บุคคลทั่วไปเพื่อแสวงหากำไร

(๑๐) ห้ามผู้ใช้งานกระทำการใดๆ เกี่ยวกับข้อมูลที่เป็นการขัดต่อกฎหมายหรือศีลธรรมอันดีแห่งสาธารณชน โดยผู้ใช้งานต้องรับรองว่า หากมีการกระทำการใดๆ ดังกล่าว ย่อมถือว่าอยู่นอกเหนือความรับผิดชอบ

๕.๒ การยืนยันตัวบุคคลสำหรับผู้ใช้ที่อยู่ภายนอกองค์กร (User authentication for external connections)

(๑) การเชื่อมต่อจากภายนอกต้องแสดงตัวตนด้วยชื่อผู้ใช้งาน (username) และพิสูจน์ตัวตนด้วยรหัสผ่าน (password) ทุกครั้ง

(๒) การเข้าสู่ระบบสารสนเทศของหน่วยงานจากทางอินเทอร์เน็ตต้องมีการตรวจสอบผู้ใช้งานอีกครั้ง

(๓) การเข้าสู่ระบบจากระยะไกล (Remote Access) ต้องใช้งานผ่าน protocol ที่มีการเข้ารหัสข้อมูลเช่น SSL และต้องมีการพิสูจน์ตัวตน

๕.๓ การระบุอุปกรณ์บนเครือข่าย (Equipment identification in networks)

(๑) ทำการระบุหมายเลขอุปกรณ์บนเครือข่ายประกอบด้วย หมายเลขประจำอุปกรณ์ในระบบเครือข่าย (MAC Address) และหมายเลขประจำเครื่องในระบบเครือข่าย (IP Address)

(๒) ผู้ดูแลระบบมีการเก็บบัญชีการขอเชื่อมต่อเครือข่าย ได้แก่ รายชื่อผู้ขอใช้บริการ รายละเอียดเครื่อง คอมพิวเตอร์ที่ขอใช้บริการรวมถึงหมายเลขประจำเครื่องในระบบเครือข่าย (IP Address) และสถานที่ติดตั้ง

(๓) มีการใช้ไฟร์วอลล์หรืออุปกรณ์เครือข่ายอื่นๆ เพื่อกำหนดว่าหมายเลขประจำเครื่องในระบบเครือข่าย (IP Address) ใดจะสามารถเข้าถึง เครือข่ายส่วนใดของหน่วยงาน

(๔) อุปกรณ์เครือข่ายต้องสามารถตรวจสอบหมายเลขประจำเครื่องในระบบเครือข่าย (IP Address) ของทั้งต้นทางและปลายทางได้

(๕) จัดทำแผนผังระบบเครือข่าย ประกอบด้วย รายละเอียดที่เกี่ยวกับขอบเขตของเครือข่ายภายในและ เครือข่ายภายนอก โดยระบุอุปกรณ์ที่ติดตั้งในระบบเครือข่าย

(๖) ทำการทบทวนแผนผังเครือข่ายพร้อมอุปกรณ์ที่ติดตั้งให้เป็นปัจจุบันอยู่เสมอ อย่างน้อยปีละ ๑ ครั้ง

๕.๔ การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote diagnostic and configuration port protection)

(๑) ทำการควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับการวิเคราะห์ปัญหาและตั้งค่าระบบ ทั้งทางกายภาพและ โดยการระบุตัวตนเข้ามาใช้งาน

(๒) ต้องยกเลิกหรือปิดพอร์ตและบริการบนอุปกรณ์เครือข่ายที่ไม่มีความจำเป็นในการใช้งาน

(๓) ผู้ดูแลระบบต้องกำหนดการเปิด - ปิดพอร์ตของอุปกรณ์เครือข่าย เพื่อควบคุมการเข้าถึงต่อพอร์ตของ อุปกรณ์เครือข่ายต่างๆ โดยจะปิดพอร์ตที่เสี่ยงและก่อให้เกิดความเสียหายต่อระบบเครือข่าย

(๔) ตรวจสอบและปิดพอร์ตของระบบหรืออุปกรณ์ที่ไม่มีความจำเป็นในการใช้งานอย่างสม่ำเสมออย่างน้อย เดือนละ ๑ ครั้ง

(๕) ทำการล็อคอุปกรณ์เครือข่ายที่ใช้สำหรับการปรับแต่งค่าคอนฟิกกูเรชันด้วยกุญแจ เพื่อป้องกันการเข้าถึงทางกายภาพต่ออุปกรณ์และทำการเปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุญาต

๕.๕ การแบ่งแยกเครือข่าย (Segregation in networks)

(๑) ผู้ดูแลระบบมีการแยกกลุ่มเครือข่ายตามกลุ่มของระบบสารสนเทศที่มีการใช้งานโดยแบ่งเป็น ๓ ประเภทใหญ่ๆ คือ

- ระบบเครือข่ายภายใน
- ระบบเครือข่ายภายนอก
- เขตสำหรับการให้บริการ (Demilitarize: DMZ) ที่เชื่อมต่อทั้งเครือข่ายภายในและเครือข่ายภายนอก

เพื่อเป็นการควบคุมและป้องกันการถูกบุกรุกได้อย่างเป็นระบบ

(๒) ผู้ดูแลระบบอาจมีการใช้วิธีการแบ่งแยกเครือข่ายทางกายภาพหรือใช้ Virtual LAN (VLAN)

(๓) ผู้ที่อยู่ในวงเครือข่ายย่อยหนึ่ง จะไม่สามารถเข้าถึงข้อมูลที่อยู่ในอีกวงเครือข่ายหนึ่งได้โดยตรง
(๔) มีการใช้ไฟร์วอลล์กั้นหรือแบ่งเครือข่ายภายในออกเป็นเครือข่ายย่อยๆ
(๕) มีการจัดทำผังเครือข่ายที่แสดงถึงขอบเขตที่ครอบคลุมแต่ละส่วนที่แบ่งแยก โดยมีการปรับปรุงให้เป็น ปัจจุบันหรืออย่างน้อยปีละ ๑ ครั้ง

๕.๖ การควบคุมเส้นทางบนระบบเครือข่าย (Network routing control)
(๑) มีการควบคุมไม่ให้มีการเปิดเผยแผนการใช้หมายเลขเครือข่าย (IP Address)
(๒) จำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องแม่ข่าย เพื่อไม่อนุญาตให้ผู้ใช้บริการสามารถใช้เส้นทางอื่นๆ ได้ นอกจากเส้นทางที่ได้กำหนดไว้ให้เท่านั้น
(๓) ผู้ดูแลระบบเครือข่ายต้องกำหนดการใช้เส้นทางบนระบบเครือข่ายบนอุปกรณ์จัดเส้นทาง (Router) หรือ อุปกรณ์กระจายสัญญาณ (Switch layer ๓) เพื่อควบคุมการใช้งานให้อยู่เฉพาะเส้นทางที่อนุญาตเท่านั้น
(๔) ผู้ดูแลระบบเครือข่ายต้องกำหนดให้มีอุปกรณ์ Firewall เพื่อควบคุมเส้นทางระบบเครือข่าย

๕.๗ การควบคุมการเชื่อมต่อระบบเครือข่าย (Network connection control)
(๑) มีการป้องกันเลขที่อยู่ของหมายเลขประจำเครื่องในระบบเครือข่าย (IP Address) ของระบบเครือข่ายภายในของหน่วยงาน มิให้หน่วยงานภายนอก ที่เชื่อมต่อสามารถมองเห็นได้
(๒) ห้ามเปิดช่องทางการเชื่อมต่อทางเครือข่ายจากภายนอกเข้าสู่เครือข่ายภายในของหน่วยงาน เพื่อให้สามารถ เข้าถึงเครื่องแม่ข่ายสำหรับระบบงานได้จากระยะไกล ยกเว้นในกรณีที่มีความจำเป็น หรือมีความเร่งด่วนสูง ซึ่งจะต้องได้รับอนุมัติจากผู้บังคับบัญชาก่อนดำเนินการทุกกรณี
(๓) มีระบบตรวจจับการบุกรุกทั้งในระดับเครือข่าย และระดับเครื่องแม่ข่าย
(๔) มีการควบคุมไม่ให้มีการเปิดให้บริการบนระบบเครือข่ายโดยไม่ได้รับอนุญาต
(๕) มีการจำกัดสิทธิและความสามารถของผู้ใช้งาน ในการเชื่อมต่อเข้าสู่ระบบเครือข่าย

๕.๘ ผู้ติดต่อจากหน่วยงานภายนอก
(๑) ผู้ติดต่อจากหน่วยงานภายนอกทุกคนต้องทำการลงบันทึกข้อมูลในเอกสารแบบฟอร์มการเข้า - ออก ศูนย์คอมพิวเตอร์ของหน่วยงานทุกครั้ง
(๒) ผู้ติดต่อจากหน่วยงานภายนอกที่นำอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการปฏิบัติงาน เข้ามาปฏิบัติงาน ที่ศูนย์คอมพิวเตอร์ของหน่วยงานต้องลงบันทึกรายการอุปกรณ์ไว้ในแบบฟอร์มการเข้า – ออก ศูนย์คอมพิวเตอร์ให้ถูกต้องชัดเจน
(๓) เจ้าหน้าที่ควรตรวจสอบความถูกต้องของข้อมูลที่บันทึกในเอกสารแบบฟอร์มการเข้า - ออกศูนย์คอมพิวเตอร์ เป็นประจำทุกเดือนและจำทำรายงานเสนอผู้บังคับบัญชาทุก ๓ เดือน
(๔) บุคคลภายนอกเข้ามาดำเนินการบำรุงรักษาบริหารจัดการอุปกรณ์เครือข่ายหรือเครื่องแม่ข่ายต้องได้รับการอนุมัติจากเจ้าของระบบสารสนเทศหรือเจ้าของข้อมูลก่อนโดยแสดงเอกสารเป็นหลักฐาน

๕.๙ การใช้งานเครือข่ายไร้สาย (Wireless LAN)
(๑) ผู้ดูแลระบบเครือข่ายต้องกำหนดให้มีการพิสูจน์ตัวตนของผู้ใช้งานก่อนเข้าใช้งานเครือข่าย
(๒) ผู้ดูแลระบบเครือข่ายต้องเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าเริ่มต้น (Default) มาจาก ผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณ (Access Point) มาใช้งาน

(๓) ผู้ดูแลระบบเครือข่ายต้องระบุสิทธิของผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ของผู้ใช้งานนั้นๆ และต้องทบทวนสิทธิอยู่เสมอ

(๔) ชื่อของเครือข่าย (SSID) จะต้องถูกยกเลิกค่าการส่งสัญญาณกระจายไปทั่วเครือข่าย (Broadcast)

๕.๑๐ การบริหารจัดการระบบเครือข่ายสำหรับผู้ดูแลระบบเครือข่าย

(๑) กำหนดค่าเริ่มต้นพื้นฐานของทุกระบบเครือข่ายต้องเป็นการอนุญาตบางส่วนหรือปฏิเสธทั้งหมด (Permit Any & Deny All)

(๒) การเข้าถึงและการปรับแต่งการตั้งค่า (configuration) ของอุปกรณ์ทำได้เฉพาะบุคคลที่ได้รับอนุญาตเท่านั้น และจะต้องทำการสำรองการตั้งค่า (backup configuration) ทุกครั้งที่มีการเปลี่ยนแปลง หรือกระทำการดังกล่าวทุก ๑ เดือน

(๓) การกำหนดหมายเลขประจำเครื่องในระบบเครือข่าย (ip address) ให้กับอุปกรณ์เครือข่าย หรืออุปกรณ์คอมพิวเตอร์ใดๆ ต้องมีการเก็บหลักฐานอย่างชัดเจนเพื่อการตรวจสอบ และจัดทำรายการการเปลี่ยนแปลงทุกๆ ๑ เดือน

(๔) ข้อมูลหมายเลขประจำเครื่องในระบบเครือข่าย (ip address) ต้องไม่เปิดเผยและต้องมีการป้องกันไม่ให้หน่วยงานภายนอกที่เชื่อมตอสามารถมองเห็นได้

(๕) จัดเก็บชื่อผู้ใช้งาน รหัสผ่าน และรายละเอียดอื่นๆ ของผู้ใช้งานและจะต้องไม่เปิดเผยข้อมูลดังกล่าวแก่ผู้ที่ไม่มีสิทธิเพื่อป้องกันการโจรกรรมข้อมูล

(๖) จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ไม่น้อยกว่า ๙๐ วัน

(๗) จัดทำผังเครือข่าย โดยมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายทั้งหมดและปรับปรุงให้เป็นปัจจุบันเสมอ

(๘) ต้องไม่เปิดเผยชื่อผู้ใช้งานและรหัสผ่านในการเข้าใช้งานอุปกรณ์ระบบเครือข่ายอย่างไม่จำเป็น

(๙) หากมีผู้ดูแลระบบเครือข่ายหลายคนจะต้องกำหนดสิทธิตามหน้าที่อย่างชัดเจนและต้องสอดคล้องกับแนวปฏิบัติการเข้าถึงและควบคุมการใช้งานสารสนเทศ

ส่วนที่ ๖
แนวปฏิบัติการควบคุมการเข้าถึงระบบปฏิบัติการ
(Operating system access control)

ขั้นตอนการปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย ผู้ดูแลระบบต้องกำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานระบบปฏิบัติการที่มีความมั่นคงปลอดภัย ซึ่งเริ่ม ตั้งแต่การลงทะเบียน การกำหนดสิทธิ์ การบริหารจัดการรหัสผ่าน และการทบทวนสิทธิต่างๆ รวมถึงข้อกำหนด เกี่ยวกับการอนุญาตให้เข้าใช้ และกำหนดรายละเอียดอื่นๆ เพิ่มเติมโดยมีแนวทางปฏิบัติ ดังนี้

๖.๑ การกำหนดขั้นตอนการปฏิบัติเพื่อเข้าใช้งานระบบปฏิบัติการ

(๑) ซอฟต์แวร์ที่มีลิขสิทธิ์ของหน่วยงานผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็น และห้ามไม่ให้ ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากตรวจพบ ถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานต้องรับผิดชอบแต่เพียงผู้เดียว

(๒) ซอฟต์แวร์ที่หน่วยงานจัดเตรียมไว้ให้ผู้ใช้งานถือเป็นสิ่งจำเป็นห้ามมิให้ผู้ใช้งานทำการติดตั้ง ถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่น

๖.๒ การระบุและยืนยันตัวตนของผู้เข้าใช้งาน (User identification and Authentication)

(๑) ผู้ใช้งานต้องทำการพิสูจน์ตัวตนก่อนการเข้าใช้งาน (login) ระบบสารสนเทศทุกครั้ง โดยการระบุชื่อผู้ใช้งาน (username) และรหัสผ่าน (password) ของตนเองเพื่อป้องกันผู้ไม่มีสิทธิเข้าใจงานระบบสารสนเทศ และต้องทำการออกจากระบบ (logout) ทุกครั้งเมื่อสิ้นสุดการใช้งาน หรือเว้นแต่มีการตั้งค่าระบบไว้เป็นอย่างอื่น

(๒) เจ้าของชื่อบัญชีผู้ใช้ (account) ต้องรับผิดชอบความเสียหายต่างๆ อันจะเกิดขึ้นจากการใช้ชื่อผู้ใช้งานนั้นกระทำการใดๆ อันส่งผลให้อุปกรณ์คอมพิวเตอร์และระบบเครือข่ายเกิดความเสียหายหรือใช้งานไม่ได้ เว้นแต่จะสามารถพิสูจน์ได้ว่าความเสียหายดังกล่าวเกิดจากการกระทำของผู้อื่น

(๓) ผู้ใช้งานสำหรับระบบงานที่มีความสำคัญสูง ต้องทำการพิสูจน์ตัวตนด้วยวิธีการทางเทคนิคที่มีความมั่นคง ปลอดภัยสูง เช่น ใช้วิธีการเข้ารหัสข้อมูล วิธีการทางชีวภาพ (อาทิ การใช้ลายนิ้วมือ)

(๔) ผู้ใช้งานต้องเก็บรักษาบัญชีผู้ใช้ (account) ไว้เป็นความลับ และห้ามเปิดเผยต่อบุคคลอื่น ห้ามโอน จำหน่าย หรือจ่ายแจกให้ผู้อื่น

๖.๓ การบริหารจัดการรหัสผ่าน (Password management system)

(๑) การตั้งรหัสสำหรับชื่อบัญชีผู้ใช้งานใหม่ (account) ผู้ดูแลระบบจะต้องกำหนดรหัสผ่านชั่วคราวด้วยวิธีการสุ่มให้กับผู้ใช้งาน

(๒) ผู้ดูแลระบบสารสนเทศต้องกำหนดให้ผู้ใช้งานเปลี่ยนแปลงรหัสผ่าน (password) ทุกๆ ๙๐ วัน

(๓) ผู้ดูแลระบบสารสนเทศต้องกำหนดจำนวนครั้งที่ยอมให้ใส่รหัสผ่านใหม่เมื่อเกิดการผิดพลาดได้ไม่เกิน ๓ ครั้ง

(๔) เมื่อมีผู้ใช้งานระบบสารสนเทศของหน่วยงาน หมดสถานะภาพการปฏิบัติงาน เช่น ลาออก หรือมิได้เกี่ยวข้องกับระบบงานแล้ว หน่วยงานต้องแจ้งให้เจ้าของระบบสารสนเทศหรือผู้ดูแลระบบทราบทันที เพื่อเปลี่ยนสิทธิหรือระงับสิทธิการใช้งานหรือแล้วแต่กรณี

(๕) การส่งมอบรหัสผ่านให้กับผู้ใช้งานต้องเป็นไปอย่างปลอดภัยโดยวิธีการใส่ซองปิดผนึก หรือแจ้งผ่านระบบส่งข้อความ หรือแล้วแต่กรณีและเหตุผลความจำเป็น

๖.๔ การใช้งานโปรแกรมอรรถประโยชน์ (Use of system utilities)

(๑) การใช้งานโปรแกรมยูทิลิตี้ จะต้องได้รับอนุญาตให้ใช้งานตามระดับสิทธิในการใช้งาน หากมีความจำเป็นต้องใช้งานจำเป็นต้องทำการขออนุมัติการใช้งานโปรแกรมยูทิลิตี้ทุกครั้ง

๖.๕ การบริหารจัดการซอฟแวร์และลิขสิทธิ์

(๑) หน่วยงานสนับสนุนและให้ความสำคัญต่อเรื่องทรัพย์สินทางปัญญา ส่งเสริมและอนุญาตให้ผู้ใช้งานใช้ software ที่มีลิขสิทธิ์ตามหน้าที่และความจำเป็นรวมถึงห้ามมิให้ผู้ใช้งานติดตั้ง software ที่ละเมิดลิขสิทธิ์ หากมีการกระทำดังกล่าวจะถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานต้องรับผิดชอบแต่เพียงผู้เดียว

(๒) software ที่หน่วยงานจัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็น ห้ามมิให้ผู้ใด ทำการถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนา เว้นแต่ได้รับอนุญาตจากผู้บังคับบัญชาเรียบร้อยแล้ว

(๓) ผู้ใช้งานต้องพึงระวัง Virus และ Malware ตลอดเวลา และจะต้องทำการแจ้งผู้ดูแลระบบทันที เพื่อป้องกันการแพร่กระจายของ Virus และ Malware

๖.๖ การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of connection time)

(๑) หลักเกณฑ์การยุติการใช้งานระบบสารสนเทศ เมื่อว่างเว้นจากการใช้งานเป็นเวลา ๓๐ นาทีเป็นอย่างน้อย หากเป็นระบบที่มีความเสี่ยงหรือความสำคัญสูง ให้กำหนดระยะเวลายุติการใช้งานระบบเมื่อว่างเว้นจากการใช้งานให้สั้นขึ้นหรือเป็นเวลา ๑๕ นาที ตามความเหมาะสม เพื่อป้องกันการเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต

(๒) ต้องมีการระบุและพิสูจน์ตัวตนเพื่อเข้าใช้งานระบบเทคโนโลยีสารสนเทศอีกครั้ง หลังจากที่ระบบได้หมดเวลาการใช้งานไปแล้ว

(๓) ถ้าไม่มีการใช้งานระบบ ต้องทำการยกเลิกการใช้โปรแกรมประยุกต์และการเชื่อมต่อเข้าสู่ระบบโดยอัตโนมัติ

ส่วนที่ ๗
แนวปฏิบัติการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและข้อมูลสารสนเทศ (Application and Information access control)

เพื่อป้องกันการเข้าถึงสารสนเทศของแอพพลิเคชั่นโดยไม่ได้รับอนุญาตโดยมีแนวปฏิบัติดังนี้

๗.๑ การจำกัดการเข้าถึงสารสนเทศ (Information access restriction) ผู้ดูแลระบบต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งาน ในการเข้าถึงสารสนเทศและฟังก์ชัน (functions) ต่างๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชั่น โดยมีวิธีการปฏิบัติ ดังนี้

(๑) ผู้ดูแลระบบสารสนเทศต้องกำหนดให้ผู้ใช้งานต้องปฏิบัติตามแนวปฏิบัติในส่วนที่ ๓ แนวปฏิบัติการบริหารจัดการการเข้าถึงของผู้ใช้งาน อันได้แก่

- การลงทะเบียนผู้ใช้งาน (User Registration)
- การบริหารจัดการสิทธิ์ของผู้ใช้งาน (User Management)
- การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management)
- การทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน (Review of User Access Rights)

(๒) ผู้ดูแลระบบสารสนเทศต้องกำหนดให้มีการพิสูจน์ตัวตนทุกครั้งของผู้ใช้งาน เมื่อมีการเข้าถึงแอพพลิเคชั่น

(๓) เจ้าของข้อมูลหรือเจ้าของระบบสารสนเทศต้องกำหนดรายการข้อมูลสำหรับการให้บริการ ประกอบด้วยรายละเอียดอย่างน้อย ดังนี้ ประเภทของข้อมูล ลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล ระดับชั้นการเข้าถึง เวลาที่ได้ เข้าถึง และช่องทางการเข้าถึง เป็นต้น ดังนี้

(๓.๑) การจัดประเภทของข้อมูล ประกอบด้วย

- ข้อมูลสารสนเทศด้านการบริหาร เช่น ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์ และ คำรับรอง ข้อมูลบุคลากร ข้อมูลงบประมาณการเงินและบัญชี เป็นต้น
- ข้อมูลสารสนเทศด้านการแพทย์และการสาธารณสุข เช่น ข้อมูลผู้ป่วย ข้อมูลทางการแพทย์ ข้อมูลสถานพยาบาล เป็นต้น

(๓.๒) การจัดแบ่งระดับความสำคัญของข้อมูล ประกอบด้วย

- ข้อมูลที่มีระดับความสำคัญมากที่สุด
- ข้อมูลที่มีระดับความสำคัญปานกลาง
- ข้อมูลที่มีระดับความสำคัญน้อย

(๓.๓) การจัดแบ่งชั้นความลับของข้อมูล ประกอบด้วย

- ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้
- ข้อมูลลับ หมายถึง ข้อมูลที่เมื่อเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย
- ข้อมูลลับมาก หมายถึง ข้อมูลที่เมื่อเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรง
- ข้อมูลลับที่สุด หมายถึง ข้อมูลที่เมื่อเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด

(๓.๔) การจัดแบ่งระดับชั้นการเข้าถึง ประกอบด้วย

- ระดับชั้นสำหรับผู้บริหาร
- ระดับชั้นสำหรับผู้ใช้งานทั่วไป
- ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมาย

(๔) ผู้ดูแลระบบสารสนเทศต้องกำหนดให้ระบบสารสนเทศจำกัดเวลาการเชื่อมต่อ รวมถึงต้องระบุตัวตนก่อนการเข้าใช้งานระบบสารสนเทศใหม่ทุกครั้ง

(๕) ผู้ดูแลระบบสารสนเทศต้องบันทึกข้อมูลพฤติกรรมการใช้งานข้อมูลโดยจัดเก็บ log file ในการเข้าถึงระบบสารสนเทศของผู้ใช้งาน เพื่อให้สามารถตรวจสอบได้ภายหลังและนำมาวิเคราะห์ตรวจสอบเมื่อเกิดการบุกรุกระบบสารสนเทศและระบบเครือข่าย

(๖) การจ้างพนักงาน outsource เพื่อดำเนินการในเรื่องต่างๆ กำหนดให้มีการควบคุมการเข้าถึงแอพพลิเคชั่นและสารสนเทศ ไว้ดังนี้

- กำหนดให้พนักงาน outsource ลงนามในสัญญารักษาความลับ
- แจ้งให้พนักงาน outsource รับทราบและปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน

(๗) มีการแสดงรายละเอียดเท่าที่จำเป็นของระบบงาน หลังจากที่ล็อคอินเสร็จแล้ว

(๘) มีข้อความแสดงเตือน ห้ามผู้ไม่มีสิทธิ์เข้าถึงระบบงาน

๗.๒ ระบบซึ่งไวต่อการรบกวน ผู้ดูแลระบบสารสนเทศต้องกำหนดแนวปฏิบัติในการดูแลและรักษาความมั่นคงปลอดภัยระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อหน่วยงาน โดยจำเป็นต้องได้รับการแยกออกจากระบบอื่นๆ และมีการควบคุมสภาพแวดล้อมโดยเฉพาะ รวมทั้งต้องควบคุมการเข้าถึงโดยการเข้าผ่านอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ และการปฏิบัติงานจากภายนอกหน่วยงานโดยมีวิธีการปฏิบัติ ดังนี้

(๑) ระบบสารสนเทศที่มีความสำคัญมากต่อองค์กรไม่อนุญาตให้สามารถใช้งานจากภายนอกหน่วยงาน หรือใช้งานผ่านอุปกรณ์สื่อสารเคลื่อนที่

(๒) มีการจัดทำระบบสำรองของระบบสารสนเทศที่มีความสำคัญมากต่อองค์กรโดยการสำรองข้อมูล

(๓) ทำการควบคุมการเข้าใช้งานจากเครือข่ายภายในและเครือข่ายภายนอก ตามข้อกำหนดที่ตั้งค่าไว้ใน Firewall

๗.๓ การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องกำหนดข้อปฏิบัติและมาตรการที่เหมาะสมเพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ผู้ดูแลระบบต้องกำหนดแนวปฏิบัติอย่างเป็นทางการ สำหรับการใช้งานอุปกรณ์คอมพิวเตอร์ประเภทพกพา อาทิ เครื่องคอมพิวเตอร์โน้ตบุ๊ก รวมทั้งกำหนดมาตรการการใช้งานอย่างปลอดภัยและเหมาะสม โดยมีแนวทางปฏิบัติ ดังนี้

(๑) มีการวิเคราะห์และประเมินความเสี่ยงจากลักษณะการใช้งานอุปกรณ์คอมพิวเตอร์ประเภทพกพา

(๒) สร้างความตระหนักเพื่อให้ผู้ใช้งานระมัดระวังและป้องกันการใช้อุปกรณ์คอมพิวเตอร์ประเภทพกพา เช่น การใช้งานในที่สาธารณะ ห้องประชุม นอกสถานที่ ซึ่งรวมถึงการเชื่อมต่อผ่านทางเครือข่ายสาธารณะภายนอกหน่วยงานเป็นต้น

(๓) ป้องกันข้อมูลที่จัดเก็บไว้ในอุปกรณ์ฯ จากการถูกเข้าถึงโดยไม่ได้รับอนุญาต ด้วยการเข้ารหัสข้อมูล

(๔) ไม่อนุญาตให้บุคคลภายนอกสามารถเข้าถึงข้อมูลสำคัญหรือลับในอุปกรณ์ฯ

(๕) มีการควบคุมการเข้าถึงระบบงานของหน่วยงานจากระยะไกล โดยการใช้อุปกรณ์คอมพิวเตอร์ประเภท พกพา เชื่อมต่อผ่านทางเครือข่ายสาธารณะ เช่น อินเทอร์เน็ตสาธารณะ

๗.๔ การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking) ต้องกำหนดข้อปฏิบัติ แผนงาน ขั้นตอนปฏิบัติ กำหนดมาตรการควบคุมการปฏิบัติงานของผู้ปฏิบัติงานจากระยะไกล รวมถึงการเตรียมการ ระบบเทคโนโลยีสารสนเทศที่เกี่ยวข้อง เพื่อให้มีความมั่นคงปลอดภัยเพียงพอเพื่อปรับใช้สำหรับการปฏิบัติงานขององค์กรจากภายนอกสำนักงาน โดยมีแนวปฏิบัติดังนี้

(๑) กำหนดให้มีช่องทางการเข้าถึงแอพพลิเคชั่นและสารสนเทศของหน่วยงานได้ ๒ ช่องทาง ดังนี้

- การเข้าถึงแอพพลิเคชั่นและสารสนเทศที่เปิดให้ใช้งานจากภายนอกได้โดยตรง ได้แก่ เว็บไซต์ของหน่วยงาน ระบบจดหมายอิเล็กทรอนิกส์ ระบบหนังสือเวียน
- การเข้าถึงแอพพลิเคชั่นและสารสนเทศผ่าน SSL VPN

(๒) อุปกรณ์คอมพิวเตอร์ที่เชื่อมต่อเข้ากับแอพพลิเคชั่นและสารสนเทศผ่านช่องทางจากภายนอกสำนักงาน ต้องได้รับการติดตั้ง anti-virus ที่ได้มีการ update รวมถึงการ update ระบบปฏิบัติการอย่างสม่ำเสมอ

(๓) ผู้ดูแลระบบต้องมีข้อกำหนดเฉพาะสำหรับการปฏิบัติงานจากระยะไกล ดังนี้

- ชนิดของงานที่อนุญาตและไม่อนุญาตสำหรับการปฏิบัติงานจากระยะไกล
- ระบบงานหรือบริการต่างๆ ที่อนุญาตให้เข้าถึงได้จากระยะไกล
- ชั่วโมงหรือช่วงระยะเวลาการปฏิบัติงาน
- ชั้นความลับของข้อมูลที่อนุญาตให้เข้าถึงได้

(๔) ผู้ดูแลระบบต้องบริหารสิทธิของผู้ใช้งานอย่างสม่ำเสมอตามข้อกำหนด การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management) และการทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน (Review of User Access Rights)

ส่วนที่ ๘
แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม
(Physical and environmental security)

เพื่อป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต ซึ่งก่อให้เกิดความเสียหาย และก่อกวนหรือแทรกแซงต่อทรัพย์สินสารสนเทศของหน่วยงาน โดยมีแนวทางในการปฏิบัติดังนี้

๘.๑ การรักษาความปลอดภัยด้านกายภาพ (Physical security management)

(๑) กำหนดพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงานตามความสำคัญของอุปกรณ์ ระบบเทคโนโลยีสารสนเทศ และระบบข้อมูล เพื่อจุดประสงค์ในการเฝ้าระวัง การควบคุม การรักษา ความมั่นคงปลอดภัย จากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่นๆ ที่อาจจะเกิดขึ้นได้

(๒) การกำหนดและจำแนกบริเวณพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน ประกอบด้วย พื้นที่ส่วนต่างๆ ตามตำแหน่งของพื้นที่ใช้งาน แบ่งออกเป็นพื้นที่ทำงานทั่วไปของเจ้าหน้าที่ด้านเทคโนโลยีสารสนเทศและผู้ดูแลระบบ พื้นที่ติดตั้งเครื่องคอมพิวเตอร์-แม่ข่าย (Server) และจัดเก็บข้อมูลคอมพิวเตอร์ พื้นที่ติดตั้งอุปกรณ์ระบบเครือข่าย (Network Equipment area) พื้นที่ห้องควบคุมระบบไฟฟ้าสำรอง

(๓) ผู้ใช้งานศูนย์คอมพิวเตอร์ของหน่วยงานต้องปิดประตูทุกครั้งที่มีการเข้า – ออกพื้นที่ และการเข้าใช้งานอุปกรณ์ระบบสารสนเทศของตนเองต้องมีการพิสูจน์ตัวตนทุกครั้ง และต้อง logout ทุกครั้งเมื่อสิ้นสุดการใช้งาน หรือว่างเว้นต่อการใช้งานเป็นเวลานาน

(๔) ต้องใส่รหัสผ่านในการเข้าใช้อุปกรณ์คอมพิวเตอร์หรืออุปกรณ์ทุกครั้ง

(๕) ดำเนินการทดสอบระบบป้องกันการบุกรุกทางกายภาพ เพื่อตรวจสอบว่ายังใช้งานได้ปกติ

๘.๒ การควบคุมการเข้า - ออก โดยมีวิธีการควบคุมการเข้า - ออก ดังนี้

(๑) ให้มีการบันทึกเวลาเข้า – ออก ของบุคคลที่เข้าพื้นที่สำคัญทุกครั้ง

(๒) การอนุญาตเข้าพื้นที่ต้องมีการขออนุญาตจากการเข้าพื้นที่ทุกครั้ง

(๓) ไม่อนุญาตให้ผู้ที่ไม่มีกิจเข้าไปในพื้นที่ เว้นแต่ได้รับอนุญาต

(๔) มีการพิสูจน์ตัวตนในการเข้าพื้นที่ ได้แก่ สแกนลายนิ้วมือ เพื่อควบคุมและป้องกันการเข้าศูนย์คอมพิวเตอร์ของหน่วยงานโดยไม่ได้รับอนุญาต

(๕) หากมีบุคคลอื่นใดที่ไม่ใช่ผู้ใช้งาน ขอเข้าใช้ศูนย์คอมพิวเตอร์ของหน่วยงานโดยมิได้ขอสิทธิในการเข้าพื้นที่นั้นไว้เป็นการล่วงหน้า ผู้ดูแลระบบต้องตรวจสอบเหตุผลและความจำเป็นก่อนอนุญาต และ จดบันทึกการเข้า - ออกพื้นที่ไว้เป็นหลักฐาน ทั้งในกรณีที่อนุญาตและไม่อนุญาตให้เข้าพื้นที่

๘.๓ การจำกัดบริเวณสำหรับการเข้าถึงหรือส่งมอบผลิตภัณฑ์โดยบุคคลภายนอก

(๑) จำกัดการเข้าถึงพื้นที่หรือบริเวณที่มีการส่งมอบอุปกรณ์เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

(๒) จำกัดบุคคลซึ่งสามารถเข้าพื้นที่ส่งมอบ

(๓) ต้องตรวจสอบการส่งมอบทุกครั้งเพื่อป้องกันวัสดุที่มีอันตรายก่อนเข้าพื้นที่ใช้งาน

(๔) ต้องตรวจนับและลงทะเบียนอุปกรณ์ให้สอดคล้องกับระเบียบวัสดุ

๘.๔ การจัดวางหรือการป้องกันอุปกรณ์

(๑) ต้องจัดวางอุปกรณ์ในพื้นที่ที่จัดเตรียมไว้อย่างเป็นระเบียบ และมีป้ายกำกับเพื่อบ่งบอกถึงผู้รับผิดชอบอุปกรณ์นั้น

(๒) มีแผนผังแสดงตำแหน่งของอุปกรณ์ที่จัดวางอย่างชัดเจน

(๓) อุปกรณ์ที่มีความสำคัญมากจะต้องแยกการจัดวางออกจากพื้นที่ที่ไม่มีความปลอดภัย หรือมีความเสี่ยงสูงต่อการโจรกรรม

(๔) มิให้นำอาหาร เครื่องดื่ม หรือสูบบุหรี่ในบริเวณหรือพื้นที่ที่มีระบบสารสนเทศ

(๕) มีการตรวจสอบสภาพแวดล้อม เช่น การตรวจสอบอุณหภูมิ ความชื้น เป็นต้น และมีการเก็บหลักฐานการตรวจสอบดังกล่าว เพื่อสำหรับตรวจสอบได้ในภายหลัง

๘.๕ ระบบและอุปกรณ์สนับสนุนการทำงาน

(๑) มีระบบและอุปกรณ์สนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศที่เพียงพอต่อการทำงาน เพื่อป้องกันการล้มเหลวของระบบอุปกรณ์สนับสนุนต่างๆ ดังนี้

- ระบบสำรองไฟฟ้า
- ระบบระบายอากาศ
- ระบบปรับอากาศและควบคุมความชื้น
- ระบบดับเพลิง

(๒) ให้มีการตรวจสอบระบบสนับสนุนอย่างสม่ำเสมอ เพื่อลดความเสี่ยงที่จะเกิดความล้มเหลวในการทำงานของระบบ

(๓) กำหนดให้มีการทำแผนสำรองในกรณีเกิดปัญหาอันทำให้ระบบและอุปกรณ์สนับสนุนการทำงานไม่สามารถให้บริการได้

๘.๖ การเดินสายไฟ สายสื่อสาร และสายเคเบิ้ลอื่นๆ (cabling security)

(๑) หลีกเลี่ยงการเดินสายสัญญาณเครือข่ายของหน่วยงานในลักษณะที่ต้องผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกเข้าถึงได้

(๒) ให้มีการร้อยท่อสายสัญญาณต่าง ๆ เพื่อป้องกันการดักจับสัญญาณ หรือการตัดสายสัญญาณ รวมถึงการป้องกันสัตว์มากัดสาย เพื่อทำให้เกิดความเสียหาย

(๓) ให้เดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซงรบกวนของสัญญาณซึ่งกันและกัน

(๔) ทำป้ายชื่อสำหรับสายสัญญาณและบนอุปกรณ์เพื่อป้องกันการตัดต่อสัญญาณผิดเส้น

(๕) จัดทำผังสายสัญญาณสื่อสารต่างๆ ให้ครบถ้วนและถูกต้อง

(๖) ห้องที่มีสายสัญญาณสื่อสารต่างๆ ปิดใส่สลักให้สนิทเพื่อป้องกันการเข้าถึงของบุคคลภายนอก

(๗) ดำเนินการสำรวจระบบสายสัญญาณสื่อสารทั้งหมดเพื่อตรวจหาการติดตั้งอุปกรณ์ดักจับสัญญาณโดยผู้ไม่ประสงค์ดี

๘.๗ การบำรุงรักษาอุปกรณ์

(๑) กำหนดให้มีการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่กำหนด

(๒) ปฏิบัติตามคำแนะนำในการดำเนินการบำรุงรักษาอุปกรณ์ตามที่ผู้ผลิตแนะนำ

(๓) จัดทำบันทึกในการบำรุงรักษาอุปกรณ์ทุกครั้ง เพื่อสามารถตรวจสอบได้ในภายหลัง

(๔) เจ้าของอุปกรณ์ หรือเจ้าของข้อมูล หรือผู้ดูแลระบบสารสนเทศ หรือผู้ที่ได้รับการแต่งตั้งต้องทำการตรวจสอบและกำกับดูแลการเข้าปฏิบัติงานของบริษัทผู้รับเหมาที่เข้ามาดำเนินการบำรุงรักษาอุปกรณ์ให้อยู่ในความเป็นระเบียบเรียบร้อย

(๕) ในกรณีที่ต้องนำอุปกรณ์ไปซ่อมแซมยังนอกสถานที่ เจ้าของอุปกรณ์ หรือเจ้าของข้อมูล หรือผู้ดูแลระบบสารสนเทศ หรือผู้ที่ได้รับการแต่งตั้งต้องให้จัดทำบันทึกโดยระบุรายละเอียดของอุปกรณ์ดังกล่าวอย่างชัดเจน และลงลายมือชื่อผู้นำออกและผู้อนุญาตกำกับไว้ เพื่อให้สามารถตรวจสอบได้ในภายหลัง

๘.๘ การป้องกันอุปกรณ์ที่ใช้งานอยู่นอกสำนักงาน

(๑) ไม่ทิ้งอุปกรณ์หรือทรัพย์สินของหน่วยงานลำพังในที่สาธารณะ

(๒) ผู้ที่จะนำอุปกรณ์หรือทรัพย์สินของหน่วยงานไปใช้นอกสำนักงานต้องทำการขออนุญาตจากผู้บังคับบัญชา และต้องรับผิดชอบอุปกรณ์หรือทรัพย์สินดังกล่าวเสมือนเป็นของตนเอง

๘.๙ การจำกัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้อีกครั้ง

(๑) ให้ทำลายข้อมูลในอุปกรณ์ก่อนที่จะดำเนินการจำหน่ายอุปกรณ์

(๒) ให้ใช้วิธีการทำลายข้อมูลอิเล็กทรอนิกส์ตามแนวปฏิบัติการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน ข้อที่ ๔.๕ การทำลายสื่อข้อมูลอิเล็กทรอนิกส์ ก่อนนำกลับมาใช้ใหม่ทุกครั้ง

๘.๑๐ การนำทรัพย์สินออกนอกหน่วยงาน

(๑) ให้มีการขออนุญาตก่อนนำทรัพย์สินออกนอกสำนักงานทุกครั้งและมีการเก็บหลักฐานการขออนุญาตดังกล่าว เพื่อให้สามารถตรวจสอบได้ในภายหลัง

(๒) เมื่อมีการนำทรัพย์สินมาคืนที่สำนักงานต้องมีการรับคืนอย่างเป็นระบบ

ส่วนที่ ๙
แนวปฏิบัติการจัดทำระบบสำรองข้อมูลและสารสนเทศ รวมถึงการเตรียมความพร้อมกรณีฉุกเฉิน (Backup and IT Continuity Plan)

๙.๑ เพื่อรักษาความถูกต้องสมบูรณ์และความพร้อมใช้ของสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศ ต้องพิจารณาคัดเลือกระบบสารสนเทศที่สำคัญและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานตามแนวปฏิบัติต่อไปนี้

(๑) มีการจัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของหน่วยงาน พร้อมทั้งกำหนดระบบสารสนเทศที่จะจัดทำระบบสำรอง และจัดทำระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง

(๒) กำหนดให้มีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบ และกำหนดความถี่ในการสำรองข้อมูล หากระบบใดที่มีการเปลี่ยนแปลงบ่อย ควรกำหนดให้มีความถี่ในการสำรองข้อมูลมากขึ้น โดยให้มีวิธีการสำรองข้อมูล ดังนี้

- ผู้ดูแลระบบต้องกำหนดประเภทของข้อมูลที่ต้องทำการสำรองเก็บไว้ และความถี่ในการสำรอง โดยประกอบด้วยข้อมูลคอนฟิกกูเรชัน ข้อมูลในฐานข้อมูล
- ผู้ดูแลระบบต้องกำหนดรูปแบบการสำรองข้อมูลให้เหมาะสมกับข้อมูลที่จะทำการสำรอง เช่น การสำรองข้อมูลแบบเต็ม (full backup) หรือการสำรองข้อมูลแบบส่วนต่าง (incremental backup)
- มีการบันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วัน/เวลาชื่อข้อมูลที่สำรอง สำเร็จ/ไม่สำเร็จ เป็นต้น
- ผู้ดูแลระบบต้องตรวจสอบข้อมูลทั้งหมดของระบบว่ามีการสำรองข้อมูลไว้อย่างครบถ้วน เช่น ซอฟต์แวร์ต่าง ๆ ที่เกี่ยวข้องกับระบบสารสนเทศ ข้อมูลคอนฟิกกูเรชัน ข้อมูลในฐานข้อมูล เป็นต้น
- ผู้ดูแลระบบต้องจัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูล และผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน
- ผู้ดูแลระบบต้องจัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ ระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลสำรองกับหน่วยงานควรห่างกันเพียงพอเพื่อไม่ให้ส่งผลกระทบต่อข้อมูลที่จัดเก็บไว้นอกสถานที่นั้นในกรณีที่เกิดภัยพิบัติกับหน่วยงาน เช่น ไฟไหม้ เป็นต้น
- ผู้ดูแลระบบต้องทดสอบบันทึกข้อมูลสำรองอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ อย่างน้อยไตรมาสละครั้ง
- ผู้ดูแลระบบต้องจัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่ได้สำรองเก็บไว้
- ผู้ดูแลระบบต้องกำหนดให้มีการใช้งานการเข้ารหัสข้อมูลกับข้อมูลลับที่ได้สำรองเก็บไว้

(๓) การปฏิบัติเกี่ยวกับการสำรองข้อมูล ดังนี้

ชนิดอุปกรณ์	รายการ	ความถี่	ผู้รับผิดชอบ
Network Equipment	-ค่า Configuration, policy , rules	- รายเดือน - ก่อนและหลังการเปลี่ยนแปลง	- ผู้ดูแลระบบ - เจ้าของระบบงานหรือเจ้าของอุปกรณ์
Web server	-ค่า Configuration ของระบบปฏิบัติการ -ค่า Configuration Service ต่างๆ -ข้อมูล website ที่เผยแพร่	- ทุกวัน - ก่อนและหลังการเปลี่ยนแปลง	- ผู้ดูแลระบบ - ผู้ดูแลระบบ Web server
Database servers	-ค่า Configuration ของระบบปฏิบัติการ -ค่า Configuration Service ต่างๆ - Log ฐานข้อมูล - ข้อมูลอื่นๆ ที่มีความสำคัญ	- ทุกวัน - ก่อนและหลังการเปลี่ยนแปลง	- ผู้ดูแลระบบ - ผู้ดูแลระบบ Database servers
Server อื่นๆ	-ค่า Configuration ของระบบปฏิบัติการ -ค่า Configuration Service ต่างๆ - ข้อมูลอื่นๆ ที่มีความสำคัญสำหรับระบบนั้นๆ	- รายเดือน - ก่อนและหลังการเปลี่ยนแปลง	- ผู้ดูแลระบบ - ผู้ดูแลระบบ Server - เจ้าของระบบงานหรือเจ้าของอุปกรณ์

(๔) ผู้ดูแลระบบต้องตรวจสอบผลการสำรองข้อมูลด้วยตนเองว่า การสำรองข้อมูลตามรายละเอียดข้างต้นนั้น ถูกต้อง สมบูรณ์หรือไม่ และมีการตรวจสอบเป็นระยะ รวมถึงการประเมินสถานที่ในการจัดเก็บข้อมูลสำรองประจำทุกปีหรือตามความเหมาะสม

(๕) สื่อบันทึกข้อมูลต้องการการเปลี่ยนแปลงตามอายุการใช้งาน

๙.๒ ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสม

(๑) จัดทำแผนเตรียมความพร้อมฉุกเฉินในกรณีไม่สามารถดำเนินวิธีการทางอิเล็กทรอนิกส์ โดยมีรายละเอียดดังนี้

- กำหนดหน้าที่และความรับผิดชอบของเจ้าหน้าที่ ซึ่งดูแลรับผิดชอบการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์
- ผู้ดูแลระบบจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินของระบบเทคโนโลยีสารสนเทศ เพื่อรองรับสถานการณ์ ฉุกเฉินจากภัยพิบัติ

- ผู้ดูแลระบบต้องทดสอบ/ประเมิน และปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินอย่างน้อยปีละ ๑ ครั้ง เพื่อให้แผนมีความทันสมัยและสามารถใช้งานได้ หากเกิดเหตุการณ์ขึ้นจริง
- ผู้ดูแลระบบต้องบันทึกเหตุการณ์เกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่เกิดขึ้น โดยพิจารณาถึงประเภท ปริมาณและหลักฐานสำหรับอ้างอิง เพื่อใช้ในกรณีที่เหตุการณ์มีความเกี่ยวข้องกับการดำเนินการ ทางกฎหมาย
- รายละเอียดที่ปรากฏในแผนเตรียมความพร้อมกรณีฉุกเฉิน ควรมีสาระครอบคลุมภัยพิบัติหรือสถานการณ์ ฉุกเฉินที่มีผลกระทบต่อระบบสารสนเทศของหน่วยงาน โดยมีหัวข้อสำคัญ ดังนี้
    - การเตรียมการเบื้องต้น
    - ผู้รับผิดชอบ
    - มาตรการความปลอดภัยและแผนดำเนินงาน ในการนำระบบคอมพิวเตอร์กลับสู่สภาพปกติ เมื่อเกิด ความเสียหายหรือหยุดทำงาน

(๒) ทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งาน อย่างน้อยปีละ ๑ ครั้ง

ส่วนที่ ๑๐
แนวปฏิบัติการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศและลดความเสี่ยงที่อาจเกิดขึ้นได้ มีวิธีการปฏิบัติต่อไปนี้

๑๐.๑ การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ที่อาจเกิดขึ้นกับระบบสารสนเทศ (Risk assessment) อย่างน้อยปีละ ๑ ครั้ง โดยมีวิธีการปฏิบัติ ดังนี้

(๑) มีการอนุมัติให้ดำเนินการประเมินความเสี่ยงด้านสารสนเทศ

(๒) มีการวางแผนสำหรับการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย

(๓) มีการตรวจสอบและประเมินความเสี่ยงของระบบให้บริการ

หมวดที่ ๒

ส่วนที่ ๑
แนวปฏิบัติในการใช้งานจดหมายอิเล็กทรอนิกส์

การรับ - ส่งจดหมายอิเล็กทรอนิกส์ มีวิธีการปฏิบัติดังนี้

(๑) ผู้ใช้งานต้องลงทะเบียนเพื่อขอใช้งานจดหมายอิเล็กทรอนิกส์ (E-mail) จากผู้ดูแลระบบก่อน

(๒) ผู้ใช้งานที่ได้รับอนุญาตให้ใช้งาน E-mail ได้ จะได้รับ Account ซึ่งประกอบด้วย รหัสผู้ใช้งาน และ รหัสผ่าน (Password) เพื่อเข้าใช้งาน E-mail

(๓) ห้ามผู้ใช้งานใช้ E-mail ที่หน่วยงานจัดสรรให้ ในการรับ - ส่ง หรือใช้งาน E-mail โดยมีวัตถุประสงค์ ดังต่อไปนี้

- เพื่อก่อให้เกิดความเสียหายแก่หน่วยงานและบุคคลอื่น หรือละเมิดสิทธิ์ หรือสร้างความรำคาญต่อผู้อื่น เช่น การจงใจส่งข้อมูลที่มีไวรัสให้กับผู้อื่น การส่งข้อความดูหมิ่นผู้อื่น การส่งจดหมายลูกโซ่ การส่ง Spam mail เป็นต้น
- เพื่อใช้ประโยชน์ในเชิงธุรกิจเป็นการส่วนตัวหรือการพาณิชย์
- เพื่อการกระทำที่ขัดต่อความสงบเรียบร้อย หรือศีลธรรมอันดีของประชาชน เช่น การส่งภาพลามก ให้กับผู้อื่น เป็นต้น
- เพื่อการเปิดเผยข้อมูลที่เป็นความลับหรือข้อมูลที่ไม่ได้รับอนุญาต ซึ่งได้มาจากหน่วยงานหรือผู้ที่มี สิทธิในข้อมูลดังกล่าว

(๔) หากผู้ใช้งานต้องการส่ง E-mail ถึงเจ้าหน้าที่ทุกคนในหน่วยงานหรือกลุ่มของหน่วยงาน ควรแจ้งให้ ผู้ดูแลระบบทราบ

(๕) ผู้ใช้งานไม่ควรนำ E-mail ที่หน่วยงานจัดสรรให้ไปให้ผู้อื่นใช้งาน และหน่วยงานจะไม่รับผิดชอบผลเสียหาย ต่างๆ อันจะเกิดขึ้นจากการยินยอมให้ผู้อื่นใช้ E-mail นั้น ยกเว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้น เกิดจากการกระทำของผู้อื่น

(๖) ห้ามผู้ใช้งานนำ E-mail ไปใช้งานบนเว็บไซต์ซึ่งเสี่ยงต่อการเกิด Spam mail เช่น การนำ E-mail ไปลงทะเบียนเพื่อสมัครงานบนเว็บไซต์สมัครงาน การระบุ E-mail เพื่อแสดงความคิดเห็นบนเว็บไซต์ขายสินค้า เป็นต้น

(๗) ผู้ใช้งานไม่ควรเปิดหรือส่งต่อ E-mail ที่ไม่ทราบแหล่งที่มาหรือไม่น่าเชื่อถือ เช่น E-mail โฆษณาขายสินค้า E-mail ให้สินเชื่อ E-mail เสนอให้รางวัล E-mail หาคู่ เป็นต้น

(๘) ผู้ใช้งานต้องตรวจสอบไวรัสกับไฟล์ที่แนบมาพร้อม E-mail ทุกครั้งเสมอ ถึงแม้ว่าจะมาจากผู้ส่งที่รู้จัก

ส่วนที่ ๒
แนวปฏิบัติในการใช้งานอินเทอร์เน็ต

การใช้งานอินเทอร์เน็ต มีวิธีการปฏิบัติดังนี้

(๑) การเชื่อมต่อเครื่องคอมพิวเตอร์เพื่อเข้าใช้งานอินเทอร์เน็ต ควรเชื่อมต่อผ่านระบบรักษาความมั่นคง ปลอดภัยที่หน่วยงาน จัดสรรไว้เท่านั้น

(๒) ผู้ใช้งานต้องไม่ใช้เครือข่ายอินเทอร์เน็ตของหน่วยงาน ในการเผยแพร่หรือใช้งานโดยมีวัตถุประสงค์ ดังต่อไปนี้

- เพื่อก่อให้เกิดความเสียหายแก่หน่วยงาน และบุคคลอื่น หรือละเมิดสิทธิ์ หรือสร้างความรำคาญต่อผู้อื่น เช่น การตัดต่อภาพของผู้อื่นแล้วนำมาเผยแพร่ทำให้เกิดความอับอาย ลักลอบแก้ไขข้อมูลส่วนบุคคลของผู้อื่น การแสดง ความเห็นดูหมิ่นผู้อื่นบนเว็บไซต์ เป็นต้น
- เพื่อหาประโยชน์ในเชิงธุรกิจเป็นการส่วนตัวหรือการพาณิชย์ เช่น การจำลอง Mail Server โดยมี การใช้อินเทอร์เน็ตของหน่วยงาน ในการส่ง mail จำนวนมาก การจำลอง Web Server เพื่อจัดทำเว็บไซต์สำหรับ ค้าขายโดยมีการใช้อินเทอร์เน็ตของหน่วยงาน เป็นต้น
- เพื่อการกระทำที่ขัดต่อความสงบเรียบร้อย หรือศีลธรรมอันดีของประชาชน เช่น การเข้าสู่เว็บไซต์ ที่ไม่เหมาะสม การใช้ข้อความที่สร้างความตื่นตระหนกกับสังคมโดยรวมบนเว็บบอร์ด เป็นต้น
- เพื่อการเปิดเผยข้อมูลที่เป็นความลับหรือข้อมูลที่ไม่ได้รับอนุญาต ซึ่งได้มาจากหน่วยงาน หรือผู้ที่มี สิทธิ์ในข้อมูลดังกล่าว

(๓) ผู้ใช้งานไม่ควรดาวน์โหลดหรือใช้งานข้อมูลมัลติมีเดีย ที่มีลักษณะการยึดครองช่องสัญญาณการสื่อสาร ข้อมูลตลอดเวลา (Consume Bandwidth) ผ่านอินเทอร์เน็ตในเวลาราชการ เช่น เล่นเกม/ดูหนัง/ฟังเพลงออนไลน์ ดูคลิปวิดีโอผ่านเว็บไซต์ ดาวน์โหลดซอฟต์แวร์ที่มีขนาดใหญ่ผ่านเว็บไซต์ เป็นต้น ในกรณีที่ผู้ใช้งานมีความจำเป็นต้องส่ง ข้อมูลที่มีขนาดใหญ่ ให้ติดต่อผู้ดูแลระบบดำเนินการเท่านั้น

(๔) ผู้ใช้งานที่มีความจำเป็นต้องนำเครื่องคอมพิวเตอร์โน้ตบุ๊กไปเชื่อมต่อเข้ากับอินเทอร์เน็ตนอกเหนือเครือข่าย อินเทอร์เน็ตของหน่วยงานต้องมีการติดตั้งซอฟต์แวร์ป้องกันไวรัสที่มีการ Update ไวรัส ให้มีความทันสมัยตลอดเวลา

(๕) ผู้ใช้งานควรแจ้งข้อเท็จจริงต่อผู้ดูแลระบบ หากพบเห็นการใช้อินเทอร์เน็ตในเครือข่ายของหน่วยงาน ไปในทางที่ไม่เหมาะสม หรือพบเห็นการบุกรุกหรือการละเมิดสิทธิ์ของหน่วยงาน

(๖) ผู้ใช้งานไม่ควรดาวน์โหลดไฟล์ข้อมูลหรือโปรแกรมจากเว็บไซต์ที่ไม่น่าเชื่อถือหรือไม่มั่นใจว่าปลอดภัย เช่น Freeware โปรแกรมรักษาจอภาพ เกมส์ และโปรแกรมที่ลงท้ายด้วย exe หรือ com หากมีความจำเป็นต้องดาวน์โหลดต้องมีการตรวจสอบด้วยโปรแกรมป้องกันไวรัสก่อนการนำไปใช้ทุกครั้ง

ส่วนที่ ๓
แนวปฏิบัติการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย
(Wireless LAN access control)

การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย มีวิธีการปฏิบัติดังนี้

(๑) Wireless Policy ครอบคลุมทุกโฮสต์ในเครือข่ายของหน่วยงานและเครือข่ายข้อมูลทั้งหมด รวมถึงเส้นทางที่ข้อมูลอาจเดินทาง ซึ่งไม่อยู่ในเครือข่ายอินเทอร์เน็ตทุกเส้นทาง Wireless Policy อาจมีการเปลี่ยนแปลงตามเทคโนโลยีใหม่ และกระบวนการที่สอดคล้องและเหมาะสมในอนาคต

(๒) ผู้ดูแลระบบ มีหน้าที่ในการบริหารจัดการ การติดตั้ง กำหนดค่าการให้บริการและการเชื่อมต่อเครื่องไร้สายทั้งหมด

(๓) การจัดการจุดเชื่อมต่อไร้สายในพื้นที่ของหน่วยงานจะต้องถูกตรวจสอบอุปกรณ์ติดตั้ง และกำหนดค่าโดยผู้ดูแลระบบเท่านั้น

(๔) ทุกจุดเชื่อมต่อเครือข่ายไร้สายและอุปกรณ์ที่เกี่ยวข้อง เช่น Access Point จุดเชื่อมต่อสายสัญญาณ Switch จะต้องมีความปลอดภัยมีรูปแบบในการจัดเก็บและเข้าถึงอุปกรณ์

(๕) ฟังก์ชันที่ใช้ในการตั้งค่าของจุดเชื่อมต่อจะต้องสามารถเข้าถึงได้เฉพาะผู้ที่มีหน้าที่ในการดูแลระบบ

(๖) จุดเชื่อมต่อจะต้องมีการกำหนดค่า Gateway ที่เป็นค่าที่กำหนดไว้ของเครือข่ายส่วนนั้นเท่านั้น

(๗) ผู้ดูแลระบบ ต้องเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าเริ่มต้น (Default) มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณ (Access Point) มาใช้งาน

(๘) SSID จะต้องถูกยกเลิกค่าการ Broadcast

(๙) เลือกใช้เทคโนโลยี Authentication และมีการกำหนดค่าการเข้ารหัสในการเชื่อมต่อ

(๑๐) อุปกรณ์ที่ใช้ในการเข้าถึงเครือข่ายของหน่วยงานจะต้องรองรับมาตรฐาน IEEE ๘๐๒.๑๑g การเชื่อมต่อ จะต้องมีซอฟต์แวร์ป้องกันไวรัส

(๑๑) ทุกจุดเชื่อมจะต้องกำหนดรหัสผ่านเพื่อเข้าใช้งาน คุณลักษณะการจัดการรหัสผ่านนี้ จะถูกเก็บไว้และส่ง ในรูปแบบที่เข้ารหัส

(๑๒) ห้ามไม่ให้เจ้าหน้าที่ หรือทีมงานเครือข่ายบอกค่าติดตั้งของเครือข่ายไร้สายกับผู้ใช้งานหรือบุคคลภายนอก

(๑๓) ผู้ละเมิดนโยบายการรักษาความมั่นคงปลอดภัยของเครือข่ายไร้สาย จะถูกระงับการใช้งานอินเทอร์เน็ตทันที

เอกสาร ๑
แผนเตรียมความพร้อมกรณีฉุกเฉิน

๑. บทนำ

๑.๑ หลักการและเหตุผล

การนำระบบเทคโนโลยีสารสนเทศมาใช้ในการบริหารจัดการภายในองค์กร และสนับสนุน ส่งเสริมให้เจ้าหน้าที่มีการใช้งานระบบเทคโนโลยีสารสนเทศมากขึ้น เพื่ออำนวยความสะดวก รวดเร็ว ในการให้บริการต่อประชาชน อนึ่ง การใช้งานระบบสารสนเทศทุกระบบต้องรักษาความถูกต้องของข้อมูลเป็นสิ่งสำคัญ เพื่อไม่ให้เกิดความผิดพลาด ซึ่งอาจมีผลกระทบต่อวงกว้าง ดังนั้นหน่วยงานจำเป็นจะต้องมีการจัดการฐานข้อมูล การเฝ้าระวัง การจัดเก็บและการดูแลรักษาข้อมูลสารสนเทศเพื่อให้ เกิดความมั่นคงปลอดภัย และมีความพร้อมในการที่จะนำข้อมูลสารสนเทศดังกล่าวไปใช้งานได้ อย่างเต็มประสิทธิภาพตลอดเวลา

ในขณะเดียวกันระบบเทคโนโลยีสารสนเทศอาจได้รับความเสียหายจากการถูกโจมตี จากไวรัสคอมพิวเตอร์ จากบุคลากร จากปัญหาไฟฟ้า จากอัคคีภัย หรือจากปัจจัยทั้งภายในและภายนอกต่างๆ ที่อาจก่อให้เกิดความเสียหายต่อระบบเทคโนโลยีสารสนเทศ และส่งผลกระทบต่อการดำเนินงานของหน่วยงาน ดังนั้นเพื่อป้องกันและแก้ไขปัญหา จึงมีความจำเป็นที่จะต้องมีแผนรองรับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ

๑.๒ วัตถุประสงค์

(๑) เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของฐานข้อมูลและเทคโนโลยีสารสนเทศให้มีเสถียรภาพและมีความพร้อมสำหรับการใช้งาน

(๒) เพื่อลดความเสียหายที่จะอาจเกิดแก่ระบบเทคโนโลยีสารสนเทศ

(๓) เพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่อง และมีประสิทธิภาพ สามารถ

แก้ไขสถานการณ์ได้อย่างทันท่วงที

(๔) เพื่อเตรียมความพร้อมรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศของหน่วยงาน

(๕) เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและผู้ปฏิบัติ ในการดูแลรักษาระบบ

๒. การวิเคราะห์ความเสี่ยง

จากการวิเคราะห์และตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศของหน่วยงานพบประเภทความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศดังนี้

๒.๑ ความเสี่ยงด้านเทคนิค

เป็นความเสี่ยงที่อาจเกิดขึ้นจากระบบคอมพิวเตอร์ เครื่องมือและอุปกรณ์เอง อาจเกิดถูกโจมตีจากไวรัสหรือโปแกรมไม่ประสงค์ดี ถูกก่อกวนจาก Hacker ถูกเจาะทำลายระบบจาก Cracker เป็นต้น

๒.๒ ความเสี่ยงด้านผู้ปฏิบัติงาน

เป็นความเสี่ยงที่อาจเกิดขึ้นจากการดำเนินการ การจัดความสำคัญในการเข้าถึงข้อมูลไม่เหมาะสมกับการใช้งานหรือการให้บริการ โดยผู้ใช้อาจเข้าสู่ระบบสารสนเทศ หรือใช้ข้อมูลต่างๆ ของกรมเกินกว่าอำนาจหน้าที่ของตนเองที่มีอยู่ และอาจทำให้เกิดความเสียหายต่อข้อมูลสารสนเทศได้

๒.๓ ความเสี่ยงด้านภัยหรือสถานการณ์ฉุกเฉิน

เป็นความเสี่ยงที่อาจเกิดจากภัยพิบัติตามธรรมชาติหรือสถานการณ์ร้ายแรงที่ก่อให้เกิดความเสียหายร้ายแรงกับข้อมูลสารสนเทศ เช่น ไฟฟ้าขัดข้อง น้ำท่วม ไฟไหม้ อาคารถล่ม การชุมนุมประท้วง หรือความไม่สงบเรียบร้อยในบ้านเมือง เป็นต้น

๒.๔ ความเสี่ยงด้านการบริหารจัดการ

เป็นความเสี่ยงจากการแนวนโยบายในการบริหารจัดการที่อาจส่งผลกระทบต่อการดำเนินการด้านสารสนเทศ

เพื่อให้ระบบเทคโนโลยีสารสนเทศของหน่วยงานมีความมั่นคงปลอดภัย และสามารถนำเทคโนโลยีสารสนเทศมาสนับสนุนการปฏิบัติงานให้เกิดประโยชน์สูงสุด จึงจำเป็นจะต้องจัดทำแผนรองรับสถานการณ์ฉุกเฉิน เพื่อเป็นกรอบแนวทางในการดูแลรักษาระบบเทคโนโลยีสารสนเทศ และแก้ไขปัญหาที่อาจจะส่งผลกระทบต่อฐานข้อมูลและระบบเทคโนโลยีสารสนเทศของหน่วยงาน

๓. แผนรองรับสถานการณ์ฉุกเฉิน

๓.๑ สถานการณ์ฉุกเฉินที่เกิดจากความขัดข้องด้านเทคนิค

๓.๑.๑ กรณีการป้องกันไวรัสล้มเหลว

(๑) กรณีถูกไวรัสหรือผู้บุกรุก เพื่อจำกัดความเสียหายที่อาจแพร่กระจายไปยังเครื่องอื่นในระบบเครือข่ายให้ทำการจำกัดการเชื่อมต่อเข้าระบบเครือข่าย

(๒) วิเคราะห์หาสาเหตุและผลกระทบที่เกิดจากไวรัสที่ระบาด

(๓) ดำเนินการป้องกันระบบเครือข่ายเพื่อหยุดยั้งการระบาดของไวรัส

(๔) ตรวจสอบและติดตามเครื่องที่ติดไวรัสและดำเนินการแก้ไข

(๕) กรณีที่ทำให้เครื่องคอมพิวเตอร์ไม่สามารถดำเนินการใช้ได้ตามปกติ ให้แจ้งเหตุ ให้เจ้าหน้าที่ศูนย์คอมพิวเตอร์ทราบ หรือกรณีมีเหตุอันทำให้ศูนย์สารสนเทศไม่สามารถดำเนินการให้บริการด้านเครือข่ายได้ ศูนย์คอมพิวเตอร์จะต้องประกาศให้ทุกหน่วยงานในสังกัดทราบ

๓.๑.๒ กรณีการป้องกันผู้บุกรุกล้มเหลว

(๑) กรณีที่มีผู้บุกรุก ผู้ดูแลระบบต้องวิเคราะห์หาสาเหตุของการเข้ามาในระบบและผลของความเสียหายที่เกิดขึ้น โดยตรวจสอบจาก log และตรวจสอบการตั้งค่าของ Firewall

(๒) ผู้ดูแลระบบแจ้งผู้อำนวยการศูนย์สารสนเทศให้ทราบโดยด่วน

(๓) ดำเนินการหยุดยั้งการบุกรุก ปิดช่องโหว่ต่างๆ ที่ทำให้ผู้บุกรุกเข้ามาได้

๓.๑.๓ กรณีอุปกรณ์จัดเก็บข้อมูลเสียหาย

(๑) แจ้งให้ผู้ปฏิบัติงานที่เกี่ยวข้องทราบ

(๒) รีบดำเนินการจัดหาอุปกรณ์จัดเก็บข้อมูลมาเปลี่ยนใหม่ และนำข้อมูลที่ได้สำรองไว้ มากู้คืนข้อมูลโดยเร็ว

(๓) ทดสอบความสมบูรณ์ของข้อมูล และแจ้งให้ผู้ปฏิบัติงานที่เกี่ยวข้องทราบ

๓.๑.๕ กรณีไฟฟ้าขัดข้อง

(๑) ระบบสารสนเทศมี UPS ซึ่งสามารถสำรองกระแสไฟฟ้าได้ ๑ ชั่วโมง เพื่อรอให้เครื่องกำเนิดกระแสไฟฟ้า (Electric generator) ทำงาน

(๒) มีการสำรองพร้อมเชื้อเพลิงสำหรับเครื่องกำเนิดกระแสไฟฟ้าสามารถใช้งานต่อเนื่องได้ ๒ วัน

(๓) แจ้งเตือนไปยังผู้บังคับบัญชาทราบ

(๔) หากเครื่องสำรองไฟฟ้าและเครื่องกำเนิดกระแสไฟฟ้ามีปัญหา แจ้งผู้บังคับบัญชา เพื่อดำเนินการแก้ไขปัญหาที่เกิดขึ้น หรือจัดหาเครื่องสำรองไฟฟ้าทดแทน

๓.๒ สถานการณ์ฉุกเฉินที่เกิดจากภัยต่างๆ

๓.๒.๑ กรณีไฟไหม้

(๑) หากเกิดไฟไหม้ขณะปฏิบัติงานอยู่ ให้ผู้ปฏิบัติงานรีบเคลื่อนย้ายออกภายนอกตัวอาคาร ให้ผู้ที่สามารถการใช้เครื่องดับเพลิงได้ ใช้เครื่องดับเพลิงที่ติดตั้งอยู่ทำการดับไฟ

(๒) หากไม่สามารถควบคุมไฟได้ ผู้ดูแลระบบต้องรีบเคลื่อนย้ายอุปกรณ์จัดเก็บข้อมูลสำรองออกภายนอกตัวอาคาร โทรแจ้งดับเพลิง ที่เบอร์ ๑๙๙

(๓) หากเกิดไฟไหม้ขณะที่ไม่มีผู้ปฏิบัติงาน แล้วปรากฏว่าอุปกรณ์ต่างๆ ชำรุดเสียหาย ให้รีบดำเนินการจัดซ่อมหรือจัดหาอุปกรณ์ต่างๆ มาเพื่อให้การปฏิบัติงานดำเนินต่อไปได้ และออกแบบติดตั้งระบบตรวจจับไฟ และดับไฟอัตโนมัติ

(๔) อบรมวิธีการใช้งานเครื่องดับเพลิงและการหนีไฟให้กับผู้ปฏิบัติงานอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง

๓.๒.๒ กรณีน้ำท่วม

(๑) ผู้ดูแลระบบปิดระบบและทำการเคลื่อนย้ายอุปกรณ์ต่างๆ ที่ยังสามารถใช้งานได้ไปไว้ที่สถานที่ห่างไกลจากจุดน้ำท่วม

(๒) ผู้ดูแลระบบนำข้อมูลสำรองที่ได้จัดเก็บไว้มากู้คืน ในส่วนที่เกิดความเสียหาย

(๓) ผู้ตรวจสอบรายการทรัพย์สิน สำรวจความชำรุด เสียหาย จัดส่งซ่อมหรือจัดหาเพื่อให้สามารถดำเนินการได้ และรายงานต่อผู้บังคับบัญชาทราบ

๓.๒.๓ กรณีแผ่นดินไหว

(๑) ให้ผู้ปฏิบัติงานรีบเคลื่อนย้ายออกภายนอกตัวอาคาร

(๒) ผู้ดูแลระบบนำข้อมูลสำรอง เคลื่อนย้ายไปด้วยหากสามารถทำได้

(๓) เมื่อเหตุการณ์สงบ ตรวจสอบความชำรุด เสียหาย และดำเนินการแก้ไขเพื่อให้ระบบสามารถดำเนินการต่อไปได้ และรายงานต่อผู้บังคับบัญชาทราบ

๓.๓ สถานการณ์ฉุกเฉินที่เกิดจากความไม่สงบเรียบร้อยในบ้านเมืองเช่น การก่อการร้าย การชุมนุมประท้วง

(๑) กรณีที่ไม่สามารถเข้ามาปฏิบัติงานได้ ผู้ดูแลระบบ Remote เข้ามาเพื่อตรวจสอบการทำงานของระบบ หากพบว่าระบบไม่สามารถดำเนินการได้ตามปกติ แจ้งผู้บังคับบัญชาทราบ

(๒) หลังเหตุการณ์ความไม่สงบ ให้ผู้ดูแลระบบและผู้ตรวจสอบรายการทรัพย์สินตรวจสอบความชำรุด เสียหายซึ่งอาจได้รับจากเหตุการณ์ดังกล่าว หากพบความชำรุดเสียหาย ให้ดำเนินการติดต่อบริษัทที่รับผิดชอบดูแลบำรุงรักษา

๓.๔ สถานการณ์ฉุกเฉินที่เกิดจากการบุคคล เช่น กรณีโจรกรรม

๓.๔.๑ กรณีโจรกรรม

(๑) ผู้ปฏิบัติงานแจ้งผู้บังคับบัญชาให้ทราบโดยด่วน

(๒) สำรวจตรวจสอบรายการทรัพย์สินที่สูญหาย

(๓) ผู้ดูแลระบบรีบดำเนินการจัดหาอุปกรณ์เพื่อติดตั้งทดแทนอุปกรณ์เดิม และนำข้อมูลที่ได้สำรองไว้กู้คืน ให้ผู้ปฏิบัติงานสามารถใช้ระบบงานต่างๆ ได้โดยเร็วที่สุด

๓.๔.๒ กรณีผู้ปฏิบัติงานไม่สามารถมาปฏิบัติงานได้

(๑) แจ้งผู้บังคับบัญชาทราบ

(๒) ปฏิบัติตามคู่มือการดำเนินการหากมีการจัดทำไว้ หรือติดต่อประสานงานกับบุคคลอื่นเพื่อให้สามารถปฏิบัติงานแทนได้

๔. การกำหนดผู้รับผิดชอบ

หน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศของหน่วยงานในกรณีที่เกิดเหตุฉุกเฉิน ดังนี้

๑. รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษาตลอดจน ติดตาม กำกับ ดูแล ควบคุม ตรวจสอบ เจ้าหน้าที่ผู้ดูแลรับผิดชอบการปฏิบัติงาน ได้แก่

๑.๑. หัวหน้าส่วนราชการ

๑.๒. หัวหน้าฝ่ายวิชาการและแผนงาน /หัวหน้ากลุ่มงานสารสนเทศและสถิติ

๒. รับผิดชอบการปฏิบัติงาน ดูแลระบบ ดูแลห้องแม่ข่าย ได้แก่

๒.๑. นักวิชาการคอมพิวเตอร์ของส่วนราชการ

๒.๒. เจ้าหน้าระบบงานคอมพิวเตอร์ของส่วนราชการ

๒.๓. เจ้าหน้าที่ของส่วนราชการที่ได้รับมอบหมายงาน

๓. รับผิดชอบการประสานงานหน่วยงานที่เกี่ยวข้อง ได้แก่

๓.๑ นักวิชาการคอมพิวเตอร์ของส่วนราชการ

๓.๒ เจ้าหน้าระบบงานคอมพิวเตอร์ของส่วนราชการ

๓.๓ เจ้าหน้าที่ของส่วนราชการที่ได้รับมอบหมายงาน

๔. รับผิดชอบการสำรวจ ตรวจสอบรายการทรัพย์สิน ได้แก่

๔.๑ นักวิชาการคอมพิวเตอร์ของส่วนราชการ

๔.๒ เจ้าหน้าระบบงานคอมพิวเตอร์ของส่วนราชการ

๔.๓ เจ้าหน้าที่ของส่วนราชการที่ได้รับมอบหมายงาน