



**กรมอนามัย**  
ศูนย์อนามัยที่ 12 ยะลา

มาตรการกำหนดการเข้าถึง/เข้าใช้งานของศูนย์เทคโนโลยีสารสนเทศ  
ศูนย์อนามัยที่ 12 ยะลา

# การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

## วัตถุประสงค์

- ๑ เพื่อควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย
- ๒ เพื่อกำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึง การกำหนดสิทธิ์ และการมอบอำนาจของหน่วยงานของรัฐ
- ๓ เพื่อให้ผู้ใช้งานได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

## แนวปฏิบัติ

### ส่วนที่ ๑ การควบคุมการเข้าถึงสารสนเทศ (Access Control)

ข้อ ๑. ผู้ดูแลระบบ จะอนุญาตให้ผู้ใช้งานเข้าถึงระบบสารสนเทศที่ต้องการใช้งานได้ ต่อเมื่อได้รับอนุญาตจาก ผู้รับผิดชอบ/เจ้าของข้อมูล/เจ้าของระบบ ตามความจำเป็นต่อการใช้งาน เท่านั้น

ข้อ ๒. บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบสารสนเทศของหน่วยงาน ให้ทำหนังสือขออนุญาตเป็นลายลักษณ์อักษรต่อผู้บริหารระดับสูง หรือหัวหน้าหน่วยงานแล้วแต่กรณีเพื่อให้ความเห็นชอบและอนุญาตก่อน

ข้อ ๓. การกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการใช้งานของผู้ใช้งาน และหน้าที่ความรับผิดชอบในการปฏิบัติงานของผู้ใช้งานระบบสารสนเทศ รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ผู้ดูแลระบบจะเป็นผู้กำหนดสิทธิ์ตามอนุญาตนั้น ดังนี้

- (๑) กำหนดสิทธิ์ของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง
  - อ่านอย่างเดียว
  - สร้างข้อมูล
  - ป้อนข้อมูล
  - แก้ไข
  - อนุมัติ
  - ไม่มีสิทธิ์
- (๒) กำหนดเกณฑ์การระงับสิทธิ์ มอบอำนาจ ให้เป็นไปตามการบริหารจัดการ การเข้าถึงของผู้ใช้งาน (user access management) ที่ได้กำหนดไว้
- (๓) ผู้ดูแลระบบมีหน้าที่ควบคุมดูแลการเข้าถึงระบบสารสนเทศและปฏิบัติงานตามหัวหน้าหน่วยงานมอบหมาย ดังนี้
  - (๓.๑) อนุญาตให้ผู้ใช้งานเข้าถึงระบบสารสนเทศของหน่วยงานจะกระทำต่อเมื่อได้รับอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบที่ได้รับมอบหมาย
  - (๓.๒) กำหนดสิทธิ์ของผู้ใช้งานให้เหมาะสมกับการใช้งานและทบทวนสิทธิ์การเข้าถึงนั้นอย่างสม่ำเสมอ
  - (๓.๓) ติดตั้งระบบการบันทึกและติดตามการใช้งานและตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบสารสนเทศของหน่วยงานอย่างสม่ำเสมอ

ข้อ ๔. การแบ่งประเภทของข้อมูลและการจัดลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล ระดับชั้นการเข้าถึงเวลาเข้าถึงและช่องทางการเข้าถึงไว้ให้ชัดเจน โดยใช้แนวทางตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.๒๕๔๔ ซึ่งระเบียบดังกล่าวเป็นมาตรการที่ละเอียด รอบคอบ ถือว่าเป็นแนวทางที่เหมาะสม ในการจัดการเอกสารอิเล็กทรอนิกส์ และในการรักษาความปลอดภัยของเอกสารอิเล็กทรอนิกส์ โดยได้กำหนดกระบวนการและกรรมวิธีต่อเอกสารที่สำคัญไว้ ดังนี้

(๔.๑) จัดแบ่งระดับชั้นการเข้าถึง

- ระดับชั้นสำหรับผู้บริหาร
- ระดับชั้นสำหรับผู้ใช้งานทั่วไป
- ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย

(๔.๒) จัดแบ่งลำดับชั้นความลับของข้อมูล

- ข้อมูลลับที่สุด หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด
- ข้อมูลลับมาก หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรง
- ข้อมูลลับ หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย
- ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

(๔.๓) จัดแบ่งประเภทของข้อมูล

- ข้อมูลสารสนเทศด้านการบริหาร เป็นข้อมูลที่เกี่ยวข้องกับข้อมูลนโยบาย ข้อมูลยุทธศาสตร์และคำรับรอง ข้อมูลบุคลากร ข้อมูลงบประมาณการเงินและบัญชี
- ข้อมูลสารสนเทศด้านการแพทย์และการสาธารณสุขเป็นข้อมูลที่เกี่ยวข้องกับการรักษา ข้อมูลผู้ป่วย ประวัติผู้ป่วย ข้อมูลทางการแพทย์และข้อมูลสถานพยาบาล

(๔.๔) จัดแบ่งระดับชั้นการเข้าถึง

- ระดับชั้นสำหรับผู้บริหาร เข้าถึงได้ตามอำนาจหน้าที่และลำดับชั้นในบังคับบัญชาในหน่วยงานนั้น
- ระดับชั้นสำหรับผู้ใช้งานทั่วไป เข้าถึงได้เฉพาะข้อมูลที่ได้รับอนุญาตให้เข้าถึงได้หรือได้ทำการเผยแพร่สำหรับผู้ใช้งานทั่วไป
- ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย เข้าถึงข้อมูลหรือระบบได้โดยสิทธิที่ได้รับมอบหมายตามอำนาจหน้าที่

(๔.๕) รูปแบบของเอกสารอิเล็กทรอนิกส์ให้ถือตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องหลักเกณฑ์และวิธีการในการจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์พ.ศ. ๒๕๕๓

ข้อ ๕. ผู้ดูแลระบบ ต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับ ในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธี การทำลายข้อมูลแต่ละประเภทชั้นความลับ มีดังต่อไปนี้

- (๑) ควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน
- (๒) กำหนดรายชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้งานข้อมูลในแต่ละชั้นความลับ

- (๓) กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว
- (๔) กำหนดการเปลี่ยนรหัสผ่าน (Password) ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูลแต่ละระดับ
- (๕) การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL, VPN หรือ XML Encryption เป็นต้น
- (๖) กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่น่าสินทรัพย์ออก นอกหน่วยงาน เช่น บำรุงรักษา ตรวจสอบ ให้ดำเนินการสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน
- (๗) กำหนดเวลาการเข้าถึงระบบสารสนเทศหากมีการบันทึกแก้ไขข้อมูลสารบบคดีอิเล็กทรอนิกส์ให้เรียกรายงานได้ในเวลาเช้าวันรุ่งขึ้นในอีกวันถัดไปเท่านั้น เนื่องจากระบบจะทำการประมวลผลต่อเนื่องกัน
- (๘) การกำหนดระยะเวลาการเชื่อมต่อ (Limitation of connection time) สำหรับการใช้งานระบบสารสนเทศบางระบบให้เป็นไปตามช่วงเวลาการทำงานที่หน่วยงานกำหนด ส่วนระบบสารสนเทศที่มีความสำคัญสูงให้ทำการตัดระบบและหมดเวลาการใช้งานรวมทั้งปิดการใช้งานด้วยหลังจากที่ไม่มีการใช้งานภายในช่วงระยะเวลา ๑๕ นาที

ข้อ ๖. มีข้อกำหนดการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Business requirements for access control) โดยแบ่งการจัดทำข้อปฏิบัติเป็น ๒ ส่วนคือ

- (๑) ควบคุมการเข้าถึงสารสนเทศโดยกำหนดแนวทางการควบคุมเข้าถึงระบบสารสนเทศและสิทธิเกี่ยวข้องกับระบบสารสนเทศ
- (๒) ปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย

ข้อ ๗. การกำหนดระบบและอุปกรณ์สนับสนุนการปฏิบัติงานดังนี้

- (๑) มีระบบสนับสนุนการทำงานของระบบสารสนเทศของหน่วยงานที่เพียงพอต่อความต้องการใช้งานดังนี้ ระบบรักษาความปลอดภัย (Security) ระบบสำรองกระแสไฟฟ้า (UPS)-เครื่องกำเนิดกระแสไฟฟ้าสำรอง ระบบระบายอากาศ ระบบปรับอากาศและควบคุมความชื้น
- (๒) ตรวจสอบหรือทดสอบระบบสนับสนุนเหล่านั้นอย่างสม่ำเสมอเพื่อให้มั่นใจได้ว่าทำงานได้ปกติและลดความเสี่ยงจากความล้มเหลวในการทำงาน
- (๓) (ติดตั้งระบบแจ้งเตือนเพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงานภายในห้องศูนย์ข้อมูล (Data Center) เมื่อมีการทำงานเครื่องผิดปกติหรือหยุดการทำงาน
- (๔) จัดวางอุปกรณ์ในพื้นที่หรือบริเวณที่เหมาะสมเพื่อหลีกเลี่ยงการเข้าถึงจากบุคคลภายนอก และให้แยกอุปกรณ์ที่มีความสำคัญเก็บไว้อีกพื้นที่หนึ่งที่มีความมั่นคงปลอดภัยเพียงพอ
- (๕) ตรวจสอบสื่อดูดซับความชื้นในห้องและตรวจสอบระดับอุณหภูมิความชื้นให้อยู่ระดับปกติเพื่อป้องกันความเสียหายต่ออุปกรณ์ที่อยู่ในห้องศูนย์ข้อมูล (Data Center)
- (๖) การเดินสายไฟสายสัญญาณเครือข่ายของหน่วยงานและสายเคเบิลอื่นที่จำเป็นต้องทำการวางผ่านเข้าไปในบริเวณที่บุคคลภายนอกเข้าถึงได้นั้นให้ร้อยท่อสายสัญญาณต่างๆ

เพื่อป้องกันหุนกระรอกแมลงสาบหรือสัตว์อื่นกัดสายไฟป้องกันการดักจับสัญญาณ การตัดสายสัญญาณอันจะทำให้เกิดความเสียหายต่อระบบเครือข่ายใช้งานไม่ได้

(๗) ต้องจัดทำแผนผังสายสัญญาณสื่อสารต่างๆให้ครบถ้วนถูกต้องโดยสายสัญญาณสื่อสาร และสายไฟฟ้าแยกออกจากกันเพื่อป้องกันการกระแทกแรงบวกรวนของสัญญาณซึ่งกัน และกันแล้วให้จัดเก็บสายสัญญาณต่างๆไว้ในตู้ Rack และปิดใส่สลักกุญแจให้สนิทเพื่อ ป้องกันการเข้าถึงจากบุคคลภายนอกหรือผู้ที่ไม่มีส่วนเกี่ยวข้อง

## ส่วนที่ ๒ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

ข้อ ๘. ผู้ดูแลระบบ ต้องกำหนดการลงทะเบียนผู้ใช้งานใหม่ ดังนี้

- (๑) จัดทำแบบฟอร์มการลงทะเบียนผู้ใช้งาน สำหรับระบบเทคโนโลยีสารสนเทศ
- (๒) ผู้ดูแลระบบต้องตรวจสอบบัญชีผู้ใช้งาน เพื่อไม่ให้เกิดการลงทะเบียนซ้ำซ้อน
- (๓) ผู้ดูแลระบบต้องตรวจสอบและให้สิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบตาม ส่วนที่ ๑ การควบคุมการเข้าถึงสารสนเทศ (Access Control) ข้อ ๓
- (๔) ผู้ดูแลระบบต้องกำหนดให้มีการแจกออกสารหรือสิ่งที่แสดงเป็นลายลักษณ์อักษรให้แก่ผู้ใช้งานเพื่อแสดงถึงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งานในการเข้าถึงระบบเทคโนโลยีสารสนเทศ

ข้อ ๙. ผู้ดูแลระบบ ต้องกำหนดการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-Mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และได้รับความเห็นชอบเป็นลายลักษณ์อักษร

ข้อ ๑๐. ผู้ดูแลระบบต้องทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of user access rights) ต้องจัดให้มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศและปรับปรุงบัญชีผู้ใช้งาน อย่างน้อยปีละ ๑ ครั้ง หรือมีการโยกย้ายเปลี่ยนตำแหน่งลาออกหรือสิ้นสุดการจ้าง โดยปฏิบัติตามแนวทาง ดังนี้

- (๑) พิมพ์รายชื่อของผู้ที่ยังมีสิทธิในระบบแยกตามหน่วยงาน
- (๒) จัดส่งรายชื่อนั้นให้กับผู้บังคับบัญชาของหน่วยงานเพื่อดำเนินการทบทวนรายชื่อและสิทธิการเข้าใช้งานว่าถูกต้องหรือไม่
- (๓) ดำเนินการแก้ไขข้อมูล สิทธิต่าง ๆ ให้ถูกต้องตามที่ได้รับแจ้งกลับจากหน่วยงาน
- (๔) ทบทวนสิทธิการเข้าถึงผู้ใช้งานอย่างน้อยปีละ ๑ ครั้ง และทบทวนสำหรับผู้ที่มิมีสิทธิในระดับสูงด้วยความถี่มากกว่าผู้ใช้งาน
- (๕) เมื่อเจ้าหน้าที่มีการโยกย้ายเปลี่ยนตำแหน่ง ลาออก สิ้นสุดการจ้างงาน หรือเปลี่ยนหน้าที่ความรับผิดชอบในระบบที่ขอสิทธิการใช้งานให้ถอดถอนสิทธิภายใน ๑-๒ วันทำการ
- (๖) ขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน เมื่อลาออกต้องดำเนินการภายใน ๓ วัน หรือ เมื่อเปลี่ยนตำแหน่งงานภายในต้องดำเนินการภายใน ๗ วัน

ข้อ ๑๑. การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน

- (๑) กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานลาออกหรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน
- (๒) กำหนดชื่อผู้ใช้งานหรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน
- (๓) ส่งมอบรหัสผ่าน (Password) ชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย หลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน (Password)
- (๔) กำหนดให้ผู้ใช้งานตอบยืนยันการได้รับรหัสผ่าน (Password)
- (๕) กำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่าน (Password) ผิดพลาดได้ไม่เกิน ๓ ครั้ง
- (๖) กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

- (๗) ในกรณีที่มีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากหัวหน้าหน่วยงาน โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิ์พิเศษที่ได้รับ ว่าสามารถเข้าถึงได้ถึงระดับใดบ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

ข้อ ๑๒. ผู้ดูแลระบบ ต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับ ในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ มีดังต่อไปนี้

- (๑) ผู้ดูแลระบบต้องกำหนดชั้นความลับของข้อมูลวิธีปฏิบัติในการจัดเก็บข้อมูลและวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่าน
- (๒) เจ้าของข้อมูลจะต้องมีการทบทวนความเหมาะสมของสิทธิ์ในการเข้าถึงข้อมูลของผู้ใช้งานอย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิ์ต่างๆที่ให้ไว้ยังคงมีความเหมาะสม
- (๓) ผู้ดูแลระบบควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน ผู้ดูแลระบบต้องกำหนดรายชื่อผู้ใช้งาน (User Account) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้งานข้อมูลในแต่ละชั้นความลับข้อมูล
- (๔) การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL, VPN หรือ XML Encryption เป็นต้น
- (๕) มีการกำหนดให้เปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูลตามที่ระบุไว้ในเอกสาร “การใช้งานรหัสผ่านผู้ใช้งาน”
- (๖) กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่น่าสินทรัพย์ออกนอกหน่วยงาน เช่น บำรุงรักษา ตรวจสอบ ให้ดำเนินการสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น
- (๗) เจ้าของข้อมูลต้องมีการตรวจสอบความเหมาะสมของสิทธิ์ในการเข้าถึงข้อมูลของผู้ใช้งาน อย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิ์ต่าง ๆ ที่ให้ไว้ยังคงมีความเหมาะสม
- (๘) หากมีการกระทำความผิดเกิดขึ้นจากชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของบุคคลใดบุคคลนั้นต้องเป็นผู้รับผิดชอบต่อการกระทำความผิดนั้นตามกฎหมายระเบียบข้อบังคับที่เกี่ยวข้อง

ข้อ ๑๓. ระบบงานสารสนเทศทางธุรกิจที่เชื่อมโยงกัน (Business Information Systems) ให้หัวหน้าหน่วยงานพิจารณาประเด็นต่าง ๆ ทางด้านความมั่นคงปลอดภัย และจุดอ่อนต่าง ๆ ก่อนตัดสินใจใช้ข้อมูลร่วมกันในระบบงาน หรือระบบเทคโนโลยีสารสนเทศที่จะเชื่อมโยงเข้าด้วยกัน เช่น ระหว่าง กรมอนามัยหรือหน่วยงานที่มาขอเชื่อมโยง

- (๑) กำหนดนโยบายและมาตรการเพื่อควบคุม ป้องกัน และบริหารจัดการการใช้ข้อมูลร่วมกัน
- (๒) พิจารณาจำกัดหรือไม่อนุญาตการเข้าถึงข้อมูลส่วนบุคคล
- (๓) พิจารณาว่ามีบุคลากรใดบ้างที่มีสิทธิ์หรือได้รับอนุญาตให้เข้าใช้งาน

- (๔) พิจารณาเรื่องการลงทะเบียนผู้ใช้งาน
- (๕) ไม่อนุญาตให้มีการใช้งานข้อมูลสำคัญหรือข้อมูลลับร่วมกันในกรณีที่ระบบไม่มีมาตรการป้องกันเพียงพอ



### ส่วนที่ ๓ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

ข้อ ๑๔. การใช้งานรหัสผ่าน ผู้ใช้งานต้องปฏิบัติ ดังนี้

- (๑) ผู้ใช้งานมีหน้าที่ในการป้องกัน ดูแล รักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) โดยผู้ใช้งานแต่ละคนต้องมีบัญชีชื่อผู้ใช้งาน (Username) ของตนเอง ห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามทำการเผยแพร่ แจกจ่าย ทำให้ผู้อื่นล่วงรู้รหัสผ่าน (Password)
- (๒) กำหนดรหัสผ่านประกอบด้วยตัวอักษรไม่น้อยกว่า ๘ ตัวอักษร ซึ่งต้องประกอบด้วยตัวเลข (Numerical character) ตัวอักษร (Alphabet) และตัวอักษรพิเศษ (Special character)
- (๓) หลีกเลี่ยงการตั้งรหัสผ่านที่อยู่บนพื้นฐานที่สามารถเดาได้ง่าย เช่น ชื่อหรือนามสกุลของตนเองหรือตรงกับคำในพจนานุกรม
- (๔) ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์
- (๕) ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (save password) สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่ผู้ใช้งานครอบครองอยู่
- (๖) ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น
- (๗) กำหนดรหัสผ่านเริ่มต้นให้กับผู้ใช้งานให้ยากต่อการเดา และการส่งมอบรหัสผ่านให้กับผู้ใช้งานต้องเป็นไปอย่างปลอดภัย
- (๘) ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (Password) ไม่เกิน ๑๘๐ วันหรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน
- (๙) ผู้ดูแลระบบต้องเปลี่ยนรหัสผ่าน (Password) ไม่เกิน ๙๐ วันหรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน

ข้อ ๑๕. การนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ ผู้ใช้งานจะต้องปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ และต้องใช้วิธีการเข้ารหัส (Encryption) ที่เหมาะสมและเป็นมาตรฐานสากล

ข้อ ๑๖. การกระทำใด ๆ ที่เกิดจากการใช้บัญชีของผู้ใช้งาน (Username) อันมีกฎหมายกำหนดให้เป็นความผิด ไม่ว่าจะการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม ให้ถือว่าเป็นความรับผิดชอบส่วนบุคคล ซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

ข้อ ๑๗. ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนที่จะใช้สิทธิ์หรือระบบสารสนเทศของหน่วยงาน และหากการพิสูจน์ตัวตนนั้นมีปัญหา ไม่ว่าจะเกิดจากรหัสผ่านล้าสมัย หรือเกิดจากความผิดพลาดใด ๆ ก็ดี ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบทันที โดยปฏิบัติตามแนวทาง ดังนี้

- (๑) คอมพิวเตอร์ทุกประเภท การเข้าถึงระบบปฏิบัติการต้องทำการพิสูจน์ตัวตนทุกครั้ง
- (๒) การใช้งานระบบคอมพิวเตอร์อื่นในเครือข่ายจะต้องทำการพิสูจน์ตัวตนทุกครั้ง
- (๓) การใช้งานอินเทอร์เน็ต (Internet) ต้องทำการพิสูจน์ตัวตน และต้องมีการบันทึกข้อมูลซึ่งสามารถบ่งบอกตัวตนบุคคลผู้ใช้งานได้
- (๔) เมื่อผู้ใช้งานไม่อยู่ที่เครื่องคอมพิวเตอร์ ต้องทำการล็อกหน้าจอทุกครั้ง และต้องทำการพิสูจน์ตัวตนก่อนการใช้งานทุกครั้ง

(๕) ผู้ใช้งานต้องตั้งเวลาพักหน้าจอ (screen saver) หลังจากไม่ได้ใช้งานเป็นเวลา ๑๕ นาที และต้องใส่รหัสผ่าน (Password) ให้ถูกต้องจึงจะสามารถเปิดหน้าจอได้

ข้อ ๑๘. ผู้ใช้งานต้องตระหนักและระมัดระวังต่อการใช้งานข้อมูล ไม่ว่าจะข้อมูลนั้นจะเป็นของกรมอนามัย หรือเป็นข้อมูลของบุคคลภายนอก

ข้อ ๑๙. เอกสารที่เป็นความลับหรือมีระดับความสำคัญ ซึ่งพิมพ์ออกจากเครื่องพิมพ์ (Printer) ตลอดจนข้อมูลที่เป็นความลับในรูปอิเล็กทรอนิกส์ ผู้ใช้งานต้องปฏิบัติให้เป็นไปตามกฎระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความลับของทางราชการดังนี้

(๑) จัดหมวดหมู่เอกสารที่เป็นความลับหรือที่มีระดับความสำคัญสูงไว้ต่างหาก

(๒) จัดเก็บและกำหนดวิธีการป้องกันที่มีความปลอดภัยอย่างเพียงพอ

(๓) การเผยแพร่ เปลี่ยนแปลง ทำซ้ำ หรือทำลาย ต้องได้รับอนุญาตจากหัวหน้าหน่วยงาน หรือผู้ที่เป็นเจ้าของ

(๔) ตรวจสอบความถูกต้องของเอกสารก่อนนำไปใช้งาน

(๕) ทำลายเอกสารที่เป็นความลับ หรือมีระดับความสำคัญสูงเมื่อหมดความจำเป็นในการใช้งาน

ข้อ ๒๐. ผู้ใช้งานมีส่วนร่วมในการดูแลรักษาและรับผิดชอบต่อข้อมูลของกรมอนามัย และข้อมูลของผู้รับบริการ หากเกิดการสูญหาย โดยนำไปใช้ในทางที่ผิด การเผยแพร่โดยไม่ได้รับอนุญาต ผู้ใช้งานต้องมีส่วนร่วมในการรับผิดชอบต่อความเสียหายนั้นด้วย

ข้อ ๒๑. ผู้ใช้งานต้องป้องกัน ดูแล รักษาไว้ซึ่งความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูล ตลอดจนเอกสาร สื่อบันทึกข้อมูลคอมพิวเตอร์ หรือสารสนเทศต่าง ๆ ที่เสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ์

ข้อ ๒๒. ผู้ใช้งานมีสิทธิ์โดยชอบธรรมที่จะเก็บรักษา ใช้งาน และป้องกันข้อมูลส่วนบุคคลตามเห็นสมควร กรมอนามัยจะให้การสนับสนุนและเคารพต่อสิทธิส่วนบุคคล และไม่อนุญาตให้บุคคลหนึ่งบุคคลใดทำการละเมิดต่อข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตจากผู้ใช้งานที่ครอบครองข้อมูลนั้น ยกเว้นในกรณีที่กรมอนามัยผู้ทำหน้าที่ตรวจสอบ หรือคาดว่าข้อมูลนั้นเกี่ยวข้องกับกรมอนามัย ซึ่งกรมอนามัยอาจแต่งตั้งให้ผู้ทำหน้าที่ตรวจสอบ ทำการตรวจสอบข้อมูลเหล่านั้นได้ตลอดเวลา โดยไม่ต้องแจ้งให้ผู้ใช้งานทราบ

ข้อ ๒๓. ห้ามเปิดหรือใช้งาน (Run) โปรแกรมประเภท Peer-to-Peer (หมายถึง วิธีการจัดเครือข่ายคอมพิวเตอร์แบบหนึ่ง ที่กำหนดให้คอมพิวเตอร์ในเครือข่ายทุกเครื่องเหมือนกันหรือเท่าเทียมกัน หมายความว่าแต่ละเครื่องต่างมีโปรแกรมหรือมีแฟ้มข้อมูลเก็บไว้เอง การจัดแบบนี้ทำให้สามารถใช้โปรแกรมหรือแฟ้มข้อมูลของคอมพิวเตอร์เครื่องใดก็ได้ แทนที่จะต้องใช้จากเครื่องบริการแฟ้ม (File Server) เท่านั้น) หรือโปรแกรมที่มีความเสี่ยงในระดับเดียวกัน เช่น บิทเทอร์เรนต์ (BitTorrent), อีมูล (Emule) เป็นต้น เว้นแต่จะได้รับการอนุญาตจากหัวหน้าหน่วยงาน

ข้อ ๒๔. ห้ามเปิดหรือใช้งาน (Run) โปรแกรมออนไลน์ทุกประเภท เพื่อความบันเทิง เช่น การดูหนัง ฟังเพลง เกมส์ เป็นต้น ในระหว่างเวลาปฏิบัติราชการ

ข้อ ๒๕. ห้ามใช้สินทรัพย์ของหน่วยงาน ที่จัดเตรียมให้ เพื่อการเผยแพร่ ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใด ที่มีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมาย หรือกระทบต่อภารกิจของกรมอนามัย

ข้อ ๒๖. ห้ามใช้สินทรัพย์ของหน่วยงาน เพื่อการรบกวน ก่อให้เกิดความเสียหาย หรือใช้ในการโจรกรรมข้อมูล หรือสิ่งอื่นใดอันเป็นการขัดต่อกฎหมายและศีลธรรม หรือกระทบต่อภารกิจของกรมอนามัย

ข้อ ๒๗. ห้ามใช้สินทรัพย์ของกรมอนามัยเพื่อประโยชน์ทางการค้า

ข้อ ๒๘. ห้ามกระทำการใด ๆ เพื่อการดักข้อมูล ไม่ว่าจะ เป็นข้อความ ภาพ เสียง หรือสิ่งอื่นใด ในเครือข่ายระบบสารสนเทศของกรมอนามัย โดยเด็ดขาด ไม่ว่าจะด้วยวิธีการใด ๆ ก็ตาม

- ข้อ ๒๙. ห้ามกระทำการรบกวน ทำลาย หรือทำให้ระบบสารสนเทศของหน่วยงานต้องหยุดชะงัก
- ข้อ ๓๐. ห้ามใช้ระบบสารสนเทศของกรมอนามัย เพื่อการควบคุมคอมพิวเตอร์หรือระบบสารสนเทศ ภายนอก โดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบที่ได้รับมอบหมาย
- ข้อ ๓๑. ห้ามกระทำการใด ๆ อันมีลักษณะเป็นการลักลอบใช้งานหรือรับรู้รหัสส่วนบุคคลของผู้อื่น ไม่ว่าจะป็นกรณีใด ๆ เพื่อประโยชน์ในการเข้าถึงข้อมูล หรือเพื่อการใช้ทรัพยากรก็ตาม
- ข้อ ๓๒. ห้ามติดตั้งอุปกรณ์หรือกระทำการใด ๆ เพื่อเข้าถึงระบบสารสนเทศของกรมอนามัย โดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบที่ได้รับมอบหมาย

## ส่วนที่ ๔ การบริหารจัดการสินทรัพย์ (Assets Management)

ข้อ ๓๓. ผู้ใช้งานต้องไม่เข้าไปในห้องควบคุมระบบคอมพิวเตอร์และเครือข่าย ที่เป็นเขตหวงห้ามโดยเด็ดขาด เว้นแต่ได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ ๓๔. ผู้ใช้งานต้องไม่นำอุปกรณ์หรือชิ้นส่วนใดออกจากห้องควบคุมระบบคอมพิวเตอร์และเครือข่าย เว้นแต่จะได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ ๓๕. ผู้ใช้งานต้องไม่นำเครื่องมือ หรืออุปกรณ์อื่นใด เชื่อมเข้าเครือข่ายเพื่อการประกอบธุรกิจส่วนบุคคล

ข้อ ๓๖. ผู้ใช้งานต้องไม่คัดลอกหรือทำสำเนาเพิ่มข้อมูลที่มีลิขสิทธิ์กำกับการใช้งาน ก่อนได้รับอนุญาต และผู้ใช้งานต้องไม่ใช้ หรือลบเพิ่มข้อมูลของผู้อื่น ไม่ว่ากรณีใด ๆ

ข้อ ๓๗. ผู้ใช้งานต้องทำลายข้อมูลสำคัญในอุปกรณ์สื่อบันทึกข้อมูล เพิ่มข้อมูล ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว และใช้เทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้เกิดการเข้าถึงข้อมูลสำคัญและข้อมูลอยู่ในภาวะซึ่งเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ์นั้นได้ และพิจารณาวิธีการทำลายข้อมูลบนสื่อบันทึกข้อมูลแต่ละประเภท ดังนี้

ประเภทสื่อบันทึกข้อมูล	วิธีทำลาย
กระดาษ	ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร
Flash Drive	- ให้การทำลายข้อมูลบน Flash Drive ตามมาตรฐาน DOD 5220.22 M ของกระทรวงกลาโหมสหรัฐอเมริกา ซึ่งเป็นมาตรฐานการทำลายข้อมูลโดยการเขียนทับข้อมูลเดิมหลายรอบ - ใช้วิธีการทุบหรือบดให้เสียหาย
แผ่น CD/DVD	ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร
เทป	ใช้วิธีการทุบหรือบดให้เสียหาย หรือเผาทำลาย
ฮาร์ดดิสก์	- ใช้การทำลายข้อมูลบนฮาร์ดดิสก์ตามมาตรฐาน DOD 5220.22 M ของกระทรวงกลาโหมสหรัฐอเมริกา ซึ่งเป็นมาตรฐานการทำลายข้อมูลโดยการเขียนทับข้อมูลเดิมหลายรอบ - ใช้วิธีการทุบหรือบดให้เสียหาย

ข้อ ๓๘. ผู้ใช้งานมีหน้าที่ต้องรับผิดชอบต่อสินทรัพย์ที่หน่วยงานมอบไว้ให้ใช้งานเสมือนหนึ่งเป็นสินทรัพย์ของผู้ใช้งานเอง โดยบรรดารายการสินทรัพย์ (Asset lists) ที่ผู้ใช้งานต้องรับผิดชอบ การรับหรือคืนสินทรัพย์ จะถูกบันทึกและตรวจสอบทุกครั้งโดยเจ้าหน้าที่ที่หน่วยงานมอบหมาย

ข้อ ๓๙. กรณีทำงานนอกสถานที่ผู้ใช้งานต้องดูแลและรับผิดชอบสินทรัพย์ของหน่วยงานที่ได้รับมอบหมาย

ข้อ ๔๐. ผู้ใช้งานมีหน้าที่ต้องชดเชยค่าเสียหายไม่ว่าทรัพย์สินนั้นจะชำรุด หรือสูญหายตามมูลค่าทรัพย์สิน หากความเสียหายนั้นเกิดจากความประมาทของผู้ใช้งาน

ข้อ ๔๑. ผู้ใช้งานต้องไม่ให้อื่นยืมคอมพิวเตอร์ หรือโน้ตบุ๊ก ไม่ว่าในกรณีใด ๆ เว้นแต่การยืมนั้นได้รับการอนุมัติเป็นลายลักษณ์อักษรจากหัวหน้าหน่วยงาน

ข้อ ๔๒. ผู้ใช้งานมีสิทธิ์ใช้สินทรัพย์และระบบสารสนเทศต่าง ๆ ที่หน่วยงานจัดเตรียมไว้ให้ใช้งาน โดยมีวัตถุประสงค์เพื่อการใช้งานของหน่วยงานเท่านั้น ห้ามมิให้ผู้ใช้งานนำสินทรัพย์และระบบสารสนเทศต่าง ๆ ไปใช้ในกิจกรรมที่หน่วยงานไม่ได้กำหนด หรือทำให้เกิดความเสียหายต่อกรมอนามัย

ข้อ ๔๓. ความเสียหายใด ๆ ที่เกิดจากการละเมิดตามข้อ ๔๒ ให้ถือเป็นความผิดส่วนบุคคล โดยผู้ใช้งานต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

## ส่วนที่ ๕ การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

ข้อ ๔๔. มาตรการควบคุมการเข้า-ออกห้องควบคุมระบบคอมพิวเตอร์และเครือข่าย

- (๑) ผู้ติดต่อจากหน่วยงานภายนอกทุกคน ต้องทำการแลกบัตรที่ใช้ระบุตัวตน เช่น บัตรประชาชน หรือใบอนุญาตขับขี่ กับเจ้าหน้าที่รักษาความปลอดภัย เพื่อรับบัตร ผู้ติดต่อ (Visitor) แล้วทำการลงบันทึกข้อมูลลงในสมุดบันทึก ตามที่ระบุไว้ในเอกสาร “บันทึกการเข้าออกพื้นที่”
- (๒) ผู้ติดต่อจากหน่วยงานภายนอก ที่นำอุปกรณ์คอมพิวเตอร์ หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานมาปฏิบัติงานที่ห้องควบคุมระบบคอมพิวเตอร์และเครือข่าย ต้องลงบันทึก รายการอุปกรณ์ ในแบบฟอร์มการขออนุญาตเข้าออกตามที่ระบุไว้ในเอกสาร “บันทึกการเข้าออกพื้นที่” ให้ถูกต้องชัดเจน
- (๓) ผู้ดูแลระบบ ต้องตรวจสอบความถูกต้องของข้อมูลในสมุดบันทึก แบบฟอร์มการ ขออนุญาตเข้าออกกับเจ้าหน้าที่รักษาความปลอดภัยเป็นประจำทุกเดือน

ข้อ ๔๕. ผู้ใช้งานจะนำเครื่องคอมพิวเตอร์ อุปกรณ์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์ ระบบเครือข่าย ของหน่วยงาน ต้องได้รับอนุญาตจากหัวหน้าหน่วยงานและต้องปฏิบัติตามนโยบายนี้โดยเคร่งครัด

ข้อ ๔๖. การขออนุญาตใช้งาน พื้นที่ Web Server ชื่อโดเมนย่อย (Sub Domain Name) ที่หน่วยงานรับผิดชอบอยู่ จะต้องทำหนังสือขออนุญาตต่อหัวหน้าหน่วยงาน และจะต้องไม่ติดตั้งโปรแกรม ใด ๆ ที่ส่งผลกระทบต่อการทำงานของระบบและผู้ใช้คนอื่น ๆ

ข้อ ๔๗. ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใด ๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลัก โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ ๔๘. ผู้ดูแลระบบ ต้องควบคุมการเข้าถึงระบบเครือข่าย เพื่อบริหารจัดการระบบเครือข่ายได้ อย่างมีประสิทธิภาพ ดังต่อไปนี้

- (๑) ต้องจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะระบบเครือข่ายที่ ได้รับอนุญาตเท่านั้น
- (๒) ต้องจำกัดเส้นทางการเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน
- (๓) ต้องจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์ แม่ข่าย เพื่อไม่ให้ผู้ใช้งานสามารถใช้เส้นทางอื่น ๆ ได้
- (๔) ระบบเครือข่ายทั้งหมดของหน่วยงานที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกหน่วยงานต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก รวมทั้งต้องมีความสามารถในการตรวจจับโปรแกรมประสงค์ร้าย (Malware) ด้วย
- (๕) ระบบเครือข่ายต้องติดตั้งระบบตรวจจับการบุกรุก (Intrusion Prevention System/Intrusion Detection System) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้า ใช้งานระบบเครือข่ายของหน่วยงานในลักษณะที่ผิดปกติ
- (๖) การเข้าสู่ระบบเครือข่ายภายในหน่วยงาน โดยผ่านทางระบบอินเทอร์เน็ตจำเป็นต้องมี การลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่าน เพื่อตรวจสอบความถูกต้องของ ผู้ใช้งานก่อนทุกครั้ง

- (๗) ต้องป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็น IP Address ภายในของระบบเครือข่ายภายในของหน่วยงาน
- (๘) ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ
- (๙) การระบุอุปกรณ์บนเครือข่าย
  - ผู้ดูแลระบบมีการเก็บบัญชีการขอเชื่อมต่อเครือข่าย ได้แก่ รายชื่อผู้ขอใช้บริการ รายละเอียด เครื่องคอมพิวเตอร์ที่ขอใช้บริการ IP Address และสถานที่ติดตั้ง
  - อุปกรณ์ที่นำมาเชื่อมต่อจะได้รับมอบหมายเลข IP Address ตามที่กำหนดโดยผู้ดูแลระบบเครือข่าย
  - ผู้ดูแลระบบต้องจำกัดผู้ใช้งานที่สามารถเข้าใช้อุปกรณ์ได้
  - กรณีอุปกรณ์ที่มีการเชื่อมต่อจากเครือข่ายภายนอก ต้องมีการระบุหมายเลขอุปกรณ์ว่าสามารถเข้าเชื่อมต่อกับเครือข่ายภายในได้หรือไม่สามารถเชื่อมต่อได้
  - อุปกรณ์เครือข่ายต้องสามารถตรวจสอบ IP Address ของทั้งต้นทางและปลายทางได้
  - การเข้าใช้งานอุปกรณ์บนเครือข่ายต้องทำการพิสูจน์ตัวตนทุกครั้งที่ใช้อุปกรณ์
- (๑๐) กำหนดระยะเวลาผู้ใช้งานที่อยู่ในระบบเครือข่ายให้ออกจากระบบเครือข่ายเมื่อ
  - เว้นว่างจากการใช้งานเป็นเวลานาน

ข้อ ๔๙. ผู้ดูแลระบบ ต้องบริหารควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server) และรับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนดแก้ไข หรือเปลี่ยนแปลงค่าต่าง ๆ ของซอฟต์แวร์ระบบ (Systems Software)

ข้อ ๕๐. การติดตั้งหรือปรับปรุงซอฟต์แวร์ของระบบงานต้องมีการขออนุมัติจากผู้ดูแลระบบให้ติดตั้งก่อนดำเนินการ

ข้อ ๕๑. กำหนดให้มีการจัดเก็บซอร์สโค้ด ไบรารี และเอกสารสำหรับซอฟต์แวร์ของระบบงานไว้ในสถานที่ที่มีความมั่นคงปลอดภัย

ข้อ ๕๒. การจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้ตามแนวทาง พ.ร.บ. คอมพิวเตอร์ ๒๕๕๐

ข้อ ๕๓. กำหนดมาตรการควบคุมการใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) จากผู้ใช้งานภายนอกหน่วยงาน เพื่อดูแลรักษาความปลอดภัยของระบบ ตามแนวทางปฏิบัติ ดังต่อไปนี้

- (๑) บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) ของหน่วยงานจะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุญาตจากหัวหน้าหน่วยงาน
- (๒) มีการควบคุมช่องทาง (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม
- (๓) วิธีการใด ๆ ที่สามารถเข้าสู่ข้อมูล หรือระบบข้อมูลได้จากระยะไกลต้องได้รับการอนุญาตจากหัวหน้าหน่วยงาน
- (๔) การเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องแสดงหลักฐาน ระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับหน่วยงานอย่างเพียงพอ
- (๕) การเข้าสู่ระบบเครือข่ายภายในและระบบสารสนเทศในหน่วยงานจากระยะไกลต้องมีการลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์

ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่าน เพื่อตรวจสอบความถูกต้องของ  
ผู้ใช้งานก่อนทุกครั้ง

ข้อ ๕๔. กำหนดให้มีการแบ่งแยกเครือข่าย ดังต่อไปนี้

(๑) Internet แบ่งแยกเครือข่ายเป็นเครือข่ายย่อย ๆ ตามอาคารต่าง ๆ เพื่อควบคุมการเข้าถึง  
เครือข่ายโดยไม่ได้รับอนุญาต

(๒) Intranet แบ่งเครือข่ายภายในและเครือข่ายภายนอก เพื่อความปลอดภัยในการใช้งาน  
ระบบสารสนเทศภายใน

ข้อ ๕๕. กำหนดการป้องกันเครือข่ายและอุปกรณ์ต่าง ๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจน  
และต้องทบทวนการกำหนดค่า Parameter ต่าง ๆ เช่น IP Address อย่างน้อยปีละ ๑ ครั้ง นอกจากนี้  
การกำหนดแก้ไขหรือเปลี่ยนแปลงค่า Parameter ต้องแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

ข้อ ๕๖. ระบบเครือข่ายทั้งหมดที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกหน่วยงาน  
ต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือโปรแกรมในการทำ Packet Filtering เช่น การใช้ไฟร์วอลล์  
(Firewall) หรือฮาร์ดแวร์อื่น ๆ รวมทั้งต้องมีความสามารถในการตรวจจับมัลแวร์ (Malware) ด้วย

ข้อ ๕๗. ต้องมีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคล ที่  
เข้าใช้งานระบบเครือข่ายของหน่วยงาน ในลักษณะที่ผิดปกติ โดยมีการตรวจสอบการบุกรุกผ่านระบบเครือข่าย  
การใช้งานในลักษณะที่ผิดปกติ และการแก้ไขเปลี่ยนแปลงระบบเครือข่าย โดยบุคคลที่ไม่มีอำนาจหน้าที่  
เกี่ยวข้อง

ข้อ ๕๘. IP address ของระบบงานเครือข่ายภายในจำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอก  
ที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันมิให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของ  
ระบบเครือข่ายได้โดยง่าย

ข้อ ๕๙. การใช้เครื่องมือต่าง ๆ (Tools) เพื่อการตรวจสอบระบบเครือข่ายต้องได้รับการอนุมัติจาก  
ผู้ดูแลระบบและจำกัดการใช้งานเฉพาะเท่าที่จำเป็น



## ส่วนที่ ๖ การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

ข้อ ๖๐. ผู้ดูแลระบบ ต้องกำหนดการลงทะเบียนบุคลากรใหม่ของหน่วยงาน (โดยปฏิบัติตามข้อ ๘) ในการใช้งานตามความจำเป็นรวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน (โดยปฏิบัติตามข้อ ๑๐) เช่น การลาออก หรือการเปลี่ยนตำแหน่งงานภายในหน่วยงาน เป็นต้น

ข้อ ๖๑. กำหนดขั้นตอนการปฏิบัติเพื่อเข้าใช้งาน

- (๑) ผู้ใช้งานต้องกำหนดรหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ที่รับผิดชอบ
- (๒) หลังจากระบบติดตั้งเสร็จ ต้องมีระบบบริหารจัดการรหัสผ่าน ที่สามารถทำงานเชิงโต้ตอบหรือมีการทำงานในลักษณะอัตโนมัติซึ่งเอื้อต่อการเปลี่ยนรหัสผ่านของผู้ใช้งานที่ได้ถูกกำหนดไว้เริ่มต้นที่มาพร้อมกับการติดตั้งระบบโดยทันที ต้องยกเลิกบัญชีผู้ใช้งานหรือเปลี่ยนรหัสผ่านของทุกรหัสผู้ใช้งานที่ได้ถูกกำหนดไว้เริ่มต้นที่มาพร้อมกับการติดตั้งระบบทันที
- (๓) ผู้ใช้งานต้องตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ (Screen Saver) เพื่อทำการล็อกหน้าจอภาพเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้งานต้องใส่รหัสผ่าน (Password) เพื่อเข้าใช้งาน
- (๔) ก่อนการเข้าใช้ระบบปฏิบัติการต้องทำการลงบันทึกเข้าใช้งาน (Login) ทุกครั้ง
- (๕) ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ของหน่วยงานร่วมกัน
- (๖) ผู้ใช้งานต้องทำการลงบันทึกออก (Logout) ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน
- (๗) ห้ามเปิดหรือใช้งานโปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยง เว้นแต่จะได้รับอนุญาตจากหัวหน้าหน่วยงานกรมอนามัย
- (๘) ซอฟต์แวร์ที่กรมอนามัย ใช้นี้มีลิขสิทธิ์ ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็น และห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใด ที่ไม่มีลิขสิทธิ์ หากตรวจพบ ถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานรับผิดชอบแต่เพียงผู้เดียว
- (๙) ซอฟต์แวร์ที่กรมอนามัยจัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็น ห้ามมิให้ผู้ใช้งานทำการติดตั้ง ถอดถอนเปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไปใช้งาน ที่อื่น
- (๑๐) ห้ามใช้ทรัพยากรทุกประเภทที่เป็นของกรมอนามัย เพื่อประโยชน์ทางการค้า
- (๑๑) ห้ามผู้ใช้งานนำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์ แสดงข้อความรูปภาพ ไม่เหมาะสม หรือขัดต่อศีลธรรม กรณีผู้ใช้งานสร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์
- (๑๒) ห้ามผู้ใช้งานของหน่วยงาน ควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอก โดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงาน

ข้อ ๖๒. การระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication) กำหนดให้ผู้ใช้งานแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตนด้วยการใช้รหัสผ่าน เพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนทุกครั้ง โดยปฏิบัติตามแนวทางที่กำหนดไว้ในข้อ ๑๑.

ข้อ ๖๓. การใช้งานโปรแกรมประเภทยูทิลิตี้ (Use of System Utilities) ต้องจำกัดและควบคุมการใช้งาน โปรแกรมยูทิลิตี้สำหรับโปรแกรมคอมพิวเตอร์ที่สำคัญ เนื่องจากการใช้งานโปรแกรมยูทิลิตี้บางชนิดสามารถทำให้ผู้ใช้หลักเสี่ยงมาตรการป้องกันทางด้านความมั่นคงปลอดภัยของระบบได้ เพื่อป้องกันการละเมิดหรือหลักเสี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว ให้ดำเนินการ ดังนี้

- (๑) การใช้งานโปรแกรมยูทิลิตี้ ต้องได้รับการอนุมัติจากผู้ดูแลระบบ และต้องมีการพิสูจน์ยืนยันตัวตนสำหรับการเข้าไปใช้งานโปรแกรมยูทิลิตี้ เพื่อจำกัดและควบคุมการใช้งาน
- (๒) โปรแกรมยูทิลิตี้ที่นำมาใช้งานต้องไม่ละเมิดลิขสิทธิ์
- (๓) ต้องจัดเก็บโปรแกรมยูทิลิตี้ออกจากซอฟต์แวร์สำหรับระบบงาน
- (๔) มีการจำกัดสิทธิ์ผู้ที่ได้รับอนุญาตให้ใช้งานโปรแกรมยูทิลิตี้
- (๕) ต้องยกเลิกหรือลบทั้งโปรแกรมยูทิลิตี้และซอฟต์แวร์ที่เกี่ยวข้องกับระบบงานที่ไม่มีความจำเป็นในการใช้งาน รวมทั้งต้องป้องกันไม่ให้ผู้ใช้งานสามารถเข้าถึงหรือใช้งานโปรแกรมยูทิลิตี้ได้

ข้อ ๖๔. การกำหนดเวลาใช้งานระบบสารสนเทศ (Session Time-Out)

- (๑) กำหนดให้ระบบสารสนเทศมีการตัดและหมดเวลาการใช้งาน เมื่อมีการว่างเว้นจากการใช้งาน เป็นเวลา ๓๐ นาที เป็นอย่างน้อย ต้องยุติการใช้งานระบบสารสนเทศ (Session Time-Out)
- (๒) ระบบสารสนเทศที่มีความเสี่ยงหรือความสำคัญสูงให้กำหนดระยะเวลายุติการใช้งานระบบเมื่อว่างเว้นจากการใช้งานให้สั้นขึ้นตามความเหมาะสม หรือเป็นเวลา ๑๕ นาที

ข้อ ๖๕. การจำกัดระยะเวลาการเชื่อมต่อระบบเทคโนโลยีสารสนเทศ (Limitation of connection time)

- (๑) ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศหรือแอปพลิเคชันที่มีความเสี่ยงหรือมีความสำคัญสูง เพื่อให้มีความมั่นคงปลอดภัย ดังนี้
  - กำหนดระยะเวลาการเชื่อมต่อระบบเทคโนโลยีสารสนเทศและการสื่อสารสำหรับระบบสารสนเทศ หรือแอปพลิเคชันที่มีความเสี่ยง หรือมีความสำคัญสูงเพื่อให้ผู้ใช้งาน สามารถใช้งานได้นานที่สุด ภายในระยะเวลาที่กำหนดเท่านั้น โดยกำหนดให้ใช้ได้ ๓ ชั่วโมงต่อการเชื่อมต่อ ๑ ครั้ง
- (๒) กำหนดให้ระบบเทคโนโลยีสารสนเทศ ที่มีความสำคัญสูง ระบบงานที่มีการใช้งานในสถานที่ที่มีความเสี่ยง (ในที่สาธารณะหรือพื้นที่ภายนอกหน่วยงาน) มีการจำกัดช่วงระยะเวลาการเชื่อมต่อ ภายใน ๓๐ นาที

## ส่วนที่ ๗ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and Information Access Control)

ข้อ ๖๖. ผู้ดูแลระบบ ต้องกำหนดการลงทะเบียนผู้ใช้งานใหม่ (โดยปฏิบัติตามข้อ ๘) ในการใช้งานตามความจำเป็นรวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน (โดยปฏิบัติตามข้อ ๑๐) เช่น การลาออกหรือการเปลี่ยนตำแหน่งงานภายในหน่วยงาน เป็นต้น

ข้อ ๖๗. ผู้ดูแลระบบ ต้องกำหนดสิทธิ์การใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-Mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่ และต้องได้รับความเห็นชอบจากหัวหน้าหน่วยงานเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

ข้อ ๖๘. ผู้ดูแลระบบ ต้องกำหนดระยะเวลาในการเชื่อมต่อระบบสารสนเทศ ที่ใช้ในการปฏิบัติงานระบบสารสนเทศต่าง ๆ เมื่อผู้ใช้งานไม่มีการใช้งานระบบสารสนเทศ เกิน ๑๕ นาที ระบบจะยุติการใช้งาน ผู้ใช้งานต้องทำการการลงบันทึกเข้าใช้งาน (Login) ก่อนเข้าระบบสารสนเทศอีกครั้ง

ข้อ ๖๙. ผู้ดูแลระบบ ต้องบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่านของบุคลากร ดังต่อไปนี้

- (๑) กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบลาออก หรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน
- (๒) กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง
- (๓) กำหนดชื่อผู้ใช้งานหรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน
- (๔) ในกรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากหัวหน้าหน่วยงาน โดยมีการกำหนดระยะเวลา การใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิ์พิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

ข้อ ๗๐. ผู้ดูแลระบบ ต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้

- (๑) ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน
- (๒) ต้องกำหนดรายชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้งานข้อมูล ในแต่ละชั้นความลับของข้อมูล
- (๓) กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว
- (๔) การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL, VPN หรือ XML Encryption เป็นต้น
- (๕) กำหนดการเปลี่ยนรหัสผ่าน (Password) ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

- (๖) กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่น่าสินทรัพย์ออกนอกหน่วยงาน เช่น บำรุงรักษา ตรวจสอบ ให้ดำเนินการสำรองและลบข้อมูล ที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น
  - (๗) ต้องสำรองข้อมูลและระบบ และทดสอบการกู้คืนข้อมูลและระบบอย่างสม่ำเสมอ โดยกำหนดความถี่ในการดำเนินงานอย่างชัดเจนในแต่ละระบบ
  - (๘) ไม่เก็บข้อมูลสำคัญขององค์กรไว้บนอุปกรณ์แบบพกพา เว้นแต่มีความจำเป็น และข้อมูลดังกล่าวจะต้องมีการเข้ารหัสข้อมูลที่เป็นมาตรฐาน
  - (๙) ข้อมูลที่มีชั้นความลับที่ต้องส่งออกไปนอกองค์กร โดยถูกจัดเก็บไว้บนอุปกรณ์แบบพกพาหรือถูกส่งผ่านระบบเครือข่ายไร้สาย ต้องผ่านการอนุมัติจากเจ้าของระบบงาน และธุรกรรม และทำการเข้ารหัสข้อมูลและระบบเครือข่ายไร้สายก่อนเท่านั้น
  - (๑๐) การเคลื่อนย้ายข้อมูลที่มีชั้นความลับ ต้องกระทำโดยบุคคลที่เจ้าของระบบงานและธุรกรรมกำหนด และจะต้องทำลายข้อมูลดังกล่าวทันทีเมื่อไม่มีการใช้งานแล้ว
- ข้อ ๗๑. ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูง ให้ปฏิบัติดังนี้
- (๑) ระบบที่ไวต่อการรบกวน โดยมีผลกระทบและมีความสำคัญสูงได้แก่ระบบข้อมูลผู้ป่วยที่เป็นข้อมูลที่เกี่ยวข้องกับการรักษาพยาบาลและข้อมูลทางการแพทย์ ระบบบุคลากรที่เป็นข้อมูลส่วนบุคคลของเจ้าหน้าที่ภายในกรมอนามัย
  - (๒) ต้องมีการควบคุมสภาพแวดล้อมของระบบที่ไวต่อการรบกวนโดยเฉพาะ
    - ๒.๑) มีห้องปฏิบัติงานแยกเป็นสัดส่วน และต้องกำหนดสิทธิ์ให้เฉพาะผู้ที่ได้รับมอบหมายเท่านั้น เข้าไปปฏิบัติงานในห้องควบคุมดังกล่าว
    - ๒.๒) ติดตั้งระบบแยกต่างหากจากระบบสารสนเทศอื่นและกำหนดสิทธิ์ในการเข้าถึงข้อมูล
  - (๓) ต้องควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกองค์กร
- ข้อ ๗๒. การใช้งานอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องปฏิบัติดังต่อไปนี้
- (๑) ตรวจสอบความพร้อมของคอมพิวเตอร์ และอุปกรณ์ที่จะนำไปใช้งานว่าอยู่ในสภาพพร้อมใช้งานหรือไม่ และตรวจสอบโปรแกรมมาตรฐานว่าถูกต้องตามลิขสิทธิ์
  - (๒) รมัควางไม่ให้บุคคลภายนอกคัดลอกข้อมูลจากคอมพิวเตอร์ที่นำไปใช้ได้ เว้นแต่ข้อมูลที่ได้มีการเผยแพร่เป็นการทั่วไป
  - (๓) เมื่อหมดความจำเป็นต้องใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่แล้ว ให้รับนำส่งคืนเจ้าหน้าที่ที่รับผิดชอบทันที
  - (๔) เจ้าหน้าที่ที่รับผิดชอบในการรับคืนต้องตรวจสอบสภาพความพร้อมใช้งานของอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ที่รับคืนด้วย
  - (๕) หากปรากฏว่าความเสียหายที่เกิดขึ้นนั้นเกิดจากความประมาทอย่างร้ายแรงของผู้นำไปใช้ ผู้นำไปใช้ต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

## ส่วนที่ ๘ การบริหารจัดการซอฟต์แวร์และลิขสิทธิ์ และการป้องกันโปรแกรมไม่ประสงค์ดี (Software Licensing and intellectual property and Preventing MalWare)

ข้อ ๗๓. กรมอนามัย ได้ให้ความสำคัญต่อเรื่องทรัพย์สินทางปัญญา ดังนั้นซอฟต์แวร์ที่หน่วยงานอนุญาตให้ใช้งานหรือที่หน่วยงานมีลิขสิทธิ์ ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็น และห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากมีการตรวจสอบพบความผิดฐานละเมิดลิขสิทธิ์ ถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงผู้เดียว

ข้อ ๗๔. ซอฟต์แวร์ (Software) ที่หน่วยงานได้จัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็นต่อการทำงาน ห้ามมิให้ผู้ใช้งานทำการ ถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่น ๆ ยกเว้นได้รับการอนุญาตจากหัวหน้าหน่วยงานหรือผู้ที่ได้รับมอบหมายที่มีสิทธิ์ในลิขสิทธิ์

ข้อ ๗๕. คอมพิวเตอร์ของผู้ใช้งานติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ (Anti virus) ตามที่หน่วยงานได้ประกาศให้ใช้ เว้นแต่คอมพิวเตอร์นั้นเป็นเครื่องเพื่อการศึกษา โดยต้องได้รับอนุญาตจากหัวหน้าหน่วยงาน

ข้อ ๗๖. บรรดาข้อมูล ไฟล์ ซอฟต์แวร์ หรือสิ่งอื่นใด ที่ได้รับจากผู้ใช้งานอื่นต้องได้รับการตรวจสอบไวรัสคอมพิวเตอร์และโปรแกรมไม่ประสงค์ดีก่อนนำมาใช้งานหรือเก็บบันทึกทุกครั้ง

ข้อ ๗๗. ผู้ใช้งานต้องทำการปรับปรุงข้อมูล สำหรับตรวจสอบและปรับปรุงระบบปฏิบัติการ (Update patch) ให้ใหม่เสมอ เพื่อเป็นการป้องกันความเสียหายที่อาจเกิดขึ้น

ข้อ ๗๘. ผู้ใช้งานต้องพึงระวังไวรัสและโปรแกรมไม่ประสงค์ดีตลอดเวลา รวมทั้งเมื่อพบสิ่งผิดปกติ ผู้ใช้งานต้องแจ้งเหตุแก่ผู้ดูแลระบบ

ข้อ ๗๙. เมื่อผู้ใช้งานพบว่าเครื่องคอมพิวเตอร์ติดไวรัส ผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์เข้าสู่เครือข่าย และต้องแจ้งแก่ผู้ดูแลระบบ

ข้อ ๘๐. ห้ามลักลอบทำสำเนา เปลี่ยนแปลง ลบทิ้ง ซึ่งข้อมูล ข้อความ เอกสาร หรือสิ่งใด ๆ ที่เป็นทรัพย์สินของหน่วยงาน หรือของผู้อื่น โดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงาน

ข้อ ๘๑. ห้ามทำการเผยแพร่ไวรัสคอมพิวเตอร์ มัลแวร์ หรือโปรแกรมอันตรายใด ๆ ที่อาจก่อให้เกิดความเสียหายมาสู่ทรัพย์สินของหน่วยงาน สิทธิ์ที่จะพัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ สามารถดำเนินการได้ แต่ต้องไม่ดำเนินการดังนี้

- (๑) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ที่จะทำลายกลไกรักษาความปลอดภัยระบบ รวมทั้งการกระทำในลักษณะเป็นการแอบใช้รหัสผ่าน การลักลอบทำสำเนาข้อมูลบุคคลอื่นหรือแกระหัสผ่านของบุคคลอื่น
- (๒) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ซึ่งทำให้ผู้ใช้งานมีสิทธิ์และลำดับความสำคัญในการครอบครองทรัพยากรระบบมากกว่าผู้ใช้งานอื่น
- (๓) พัฒนาโปรแกรมใดที่จะทำซ้ำตัวโปรแกรมหรือแฝงตัวโปรแกรมไปกับโปรแกรมอื่นในลักษณะเช่นเดียวกับหนอนหรือไวรัสคอมพิวเตอร์
- (๔) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ที่จะทำลายระบบจำกัดสิทธิการใช้ (License) ซอฟต์แวร์
- (๕) นำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์แสดงข้อความรูปภาพไม่เหมาะสม หรือขัดต่อศีลธรรมประเพณีอันดีงามของประเทศไทย กรณีที่ผู้ใช้งานสร้างเว็บเพจ บนเครือข่ายคอมพิวเตอร์

ข้อ ๘๒. การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก (Outsourced software development)

- (๑) จัดให้มีการควบคุมโครงการพัฒนาซอฟต์แวร์โดยผู้รับจ้างให้บริการจากภายนอก
- (๒) พิจารณาระบุว่าใครจะเป็นผู้มีสิทธิในทรัพย์สินทางปัญญาสำหรับซอร์สโค้ด ในการพัฒนาซอฟต์แวร์โดยผู้รับจ้างให้บริการจากภายนอก
- (๓) พิจารณากำหนดเรื่องการสงวนสิทธิ์ที่จะตรวจสอบด้านคุณภาพและความถูกต้องของซอฟต์แวร์ที่จะมีการพัฒนาโดยผู้ให้บริการภายนอก โดยระบุไว้ในสัญญาจ้างที่ทำกับผู้ให้บริการภายนอกนั้น
- (๔) ให้มีการตรวจสอบโปรแกรมไม่ประสงค์ดี ในซอฟต์แวร์ต่าง ๆ ที่จะทำการติดตั้งก่อนดำเนินการติดตั้ง
- (๕) หลังจากการส่งมอบการพัฒนาซอฟต์แวร์จากหน่วยงานภายนอก หน่วยงานต้องดำเนินการเปลี่ยนรหัสผ่านต่าง ๆ
- (๖) ผู้พัฒนาระบบจากภายนอก (outsourcer) ต้องลงนามในสัญญาไม่เปิดเผยข้อมูล (Non-Disclosure Agreement) ก่อนดำเนินการ
- (๗) ผู้พัฒนาระบบจากภายนอก (outsourcer) ต้องถือปฏิบัติตามแนวนโยบาย และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของกรมอนามัย

## ส่วนที่ ๙ การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)

ข้อ ๘๓. ต้องมีการตรวจสอบว่าอุปกรณ์ที่เป็นของส่วนตัวซึ่งใช้ในการเข้าถึงระบบเทคโนโลยีสารสนเทศของหน่วยงานจากระยะไกลมีการป้องกันไวรัสและการใช้งานไฟร์วอลล์ตามที่หน่วยงานกำหนด

ข้อ ๘๔. ต้องมีการจัดเตรียมอุปกรณ์สำหรับการปฏิบัติงานจากระยะไกล การจัดเก็บข้อมูล และอุปกรณ์สื่อสารไว้ให้กับผู้ใช้งานจากระยะไกล

ข้อ ๘๕. ผู้ใช้งานจากระยะไกลทุกคน ต้องผ่านการพิสูจน์ตัวตนก่อนการใช้งาน เพื่อเพิ่มความปลอดภัยจะต้องมีการตรวจสอบ เช่น รหัสผ่าน หรือวิธีการเข้ารหัส เป็นต้น

ข้อ ๘๖. ไม่อนุญาตให้ใช้งานอุปกรณ์ที่เป็นของส่วนตัวเพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศของหน่วยงานจากระยะไกล หากอุปกรณ์ดังกล่าวไม่อยู่ภายใต้การควบคุมตามนโยบายความมั่นคงปลอดภัยของหน่วยงาน

ข้อ ๘๗. ต้องกำหนดชนิดของงาน ชั่วโมงการทำงาน ชั้นความลับของข้อมูล ระบบงานและบริการต่างๆ ของหน่วยงานที่อนุญาตและไม่อนุญาตให้ปฏิบัติงานจากระยะไกล

ข้อ ๘๘. ต้องกำหนดขั้นตอนปฏิบัติสำหรับการขออนุมัติ การขอยกเลิก การกำหนดหรือปรับปรุงสิทธิ์การเข้าถึงระบบงาน และการคืนอุปกรณ์ที่ใช้ปฏิบัติงานจากระยะไกล

## ส่วนที่ ๑๐ การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

ข้อ ๘๙. ผู้ดูแลระบบ ต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point) ให้รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายน้อยที่สุด

ข้อ ๙๐. ผู้ดูแลระบบ ต้องทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่า โดยปริยาย (Default) มาจากผู้ผลิตพื้นที่ที่นำอุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point) มาใช้งาน และกำหนดให้ชื่อ SSID (Service Set Identifier) โดยเฉพาะระบบงานที่เป็นชั้นความลับ ดังกล่าวด้วย

ข้อ ๙๑. ผู้ดูแลระบบ ต้องกำหนดค่า Wireless Security เป็นแบบ WEP (Wired Equivalent Privacy) หรือ WPA (Wi-Fi Protected Access) หรือ ที่ดีกว่า ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และ อุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point) และกำหนดค่าให้ไม่แสดงชื่อระบบเครือข่ายไร้สาย

ข้อ ๙๒. ผู้ดูแลระบบ เลือกใช้วิธีการควบคุม MAC Address (Media Access Control Address) และชื่อผู้ใช้งาน (Username) รหัสผ่าน (Password) ของผู้ใช้งานที่มีสิทธิ์ในการใช้งานระบบเครือข่าย ไร้สาย โดยจะอนุญาตเฉพาะอุปกรณ์ที่มี MAC address (Media Access Control Address) และชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ตามที่กำหนดไว้เท่านั้นให้เข้าใช้ระบบเครือข่ายไร้สายได้อย่างถูกต้อง

ข้อ ๙๓. ผู้ดูแลระบบ ต้องมีการติดตั้งไฟร์วอลล์ (Firewall) ระหว่างระบบเครือข่ายไร้สายกับระบบเครือข่ายภายในหน่วยงาน

ข้อ ๙๔. ผู้ดูแลระบบ ควรกำหนดให้ผู้ใช้งานในระบบเครือข่ายไร้สายติดต่อสื่อสารกับเครือข่ายภายในหน่วยงานผ่านทาง VPN (Virtual Private Network) เพื่อช่วยป้องกันการบุกรุกในระบบเครือข่ายไร้สาย

ข้อ ๙๕. ผู้ดูแลระบบ ต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อบนระบบเครือข่ายไร้สาย

ข้อ ๙๖. ผู้ดูแลระบบ ต้องใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายเพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย และจัดส่งรายงานผลการตรวจสอบทุก ๓ เดือน และในกรณีที่ตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติ ให้ผู้ดูแลระบบ รายงานต่อหัวหน้าหน่วยงานทราบทันที

ข้อ ๙๗. ผู้ดูแลระบบ ต้องควบคุมดูแลไม่ให้บุคคลหรือหน่วยงานภายนอกที่ไม่ได้รับอนุญาต ใช้งานระบบเครือข่ายไร้สายในการเข้าสู่ระบบอินทราเน็ต (Intranet) และฐานข้อมูลภายในต่าง ๆ ของหน่วยงาน

ข้อ ๙๘. ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของกรมอนามัย จะต้องทำการลงทะเบียนกับผู้ดูแลระบบและต้องได้รับพิจารณาอนุญาตจากหัวหน้าหน่วยงานอย่างเป็นทางการ

ข้อ ๙๙. ผู้ดูแลระบบ ต้องทำการลงทะเบียนกำหนดสิทธิ์ผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงาน ก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้ง มีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ จะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน



## ส่วนที่ ๑๑ การควบคุมการใช้งานอุปกรณ์ป้องกันเครือข่าย (Firewall Control)

ข้อ ๑๐๐. หน่วยงานมีหน้าที่ในการบริหารจัดการ การติดตั้งและกำหนดค่าของ Firewall ทั้งหมด

ข้อ ๑๐๑. การกำหนดค่าเริ่มต้นของ Firewall ต้องกำหนดเป็นปฏิเสธทั้งหมด (Deny)

ข้อ ๑๐๒. ทุกบริการ (Services) และเส้นทางเชื่อมต่ออินเทอร์เน็ตที่ไม่อนุญาตตาม Policy จะต้องถูกบล็อก (Block) โดย Firewall

ข้อ ๑๐๓. ผู้ใช้งานอินเทอร์เน็ตจะต้องทำการลงบันทึกการใช้งาน (Login) ก่อนการใช้งานทุกครั้ง

ข้อ ๑๐๔. การกำหนดค่าบริการและการเชื่อมต่อที่อนุญาต จะต้องมีการบันทึกการเปลี่ยนแปลงทุกครั้ง หากมีการเปลี่ยนแปลงค่าต่าง ๆ ของ Firewall

ข้อ ๑๐๕. การเข้าถึงตัวอุปกรณ์ Firewall จะต้องสามารถเข้าถึงได้เฉพาะผู้ที่ได้รับมอบหมายให้ดูแลจัดการเท่านั้น

ข้อ ๑๐๖. ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์ Firewall จะต้องส่งค่าไปจัดเก็บที่อุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ โดยจะต้องจัดเก็บข้อมูลจราจรไม่น้อยกว่า ๙๐ วัน

ข้อ ๑๐๗. การกำหนดนโยบายในการให้บริการอินเทอร์เน็ตกับเครื่องคอมพิวเตอร์ลูกข่ายจะเปิดพอร์ตการเชื่อมต่อพื้นฐานของโปรแกรมทั่วไป ที่อนุญาตให้ใช้งาน ซึ่งหากมีความจำเป็นที่จะใช้งานพอร์ตการเชื่อมต่อนอกเหนือที่กำหนด จะต้องได้รับความยินยอมจากหน่วยงานก่อน

ข้อ ๑๐๘. การกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละส่วนของเครือข่าย จะต้องกำหนดค่าอนุญาตเฉพาะพอร์ตการเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น โดยระบุให้กับเครื่องคอมพิวเตอร์แม่ข่ายเป็นรายเครื่องที่ให้บริการจริง และการกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายหรืออุปกรณ์ในเครือข่าย ต้องขออนุญาตเป็นลายลักษณ์อักษรต่อหัวหน้าหน่วยงานโดยต้องระบุข้อมูลดังนี้

(๑) หมายเลข Port ที่ต้องการขอให้เปิด

(๒) หมายเลข IP Address ของปลายทางที่ต้องการติดต่อสื่อสาร

(๓) วัตถุประสงค์ หรือชื่อแอปพลิเคชันที่ต้องการใช้งานผ่าน Port นั้นๆ

ข้อ ๑๐๙. จะต้องมีการสำรองข้อมูลการกำหนดค่าต่าง ๆ ของอุปกรณ์ Firewall เป็นประจำ ทุกเดือน ทุกสัปดาห์ หรือทุกครั้งก่อนที่จะมีการเปลี่ยนแปลงค่า

ข้อ ๑๑๐. เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบงานสารสนเทศต่าง ๆ ภายในหน่วยงาน ที่มีลักษณะที่เป็นอินเทอร์เน็ตจะต้องไม่อนุญาตให้มีการเชื่อมต่อเพื่อใช้งานอินเทอร์เน็ต เว้นแต่มีความจำเป็น โดยจะต้องกำหนดเป็นกรณีไป

ข้อ ๑๑๑. หน่วยงานมีสิทธิ์ที่จะระงับหรือบล็อกการใช้งานของเครื่องคอมพิวเตอร์ลูกข่ายที่มีพฤติกรรมการใช้งานที่ผิดนโยบายหรือเสี่ยงต่อความปลอดภัยของระบบเครือข่ายส่วนรวม หรือเกิดจากการทำงานของโปรแกรมที่มีความเสี่ยงต่อความปลอดภัยจนกว่าจะได้รับการแก้ไข

ข้อ ๑๑๒. การเชื่อมต่อในลักษณะของการควบคุมระยะไกล Remote Login จากภายนอกมายังเครื่องแม่ข่าย หรืออุปกรณ์เครือข่ายภายใน

(๑) ขออนุญาตการใช้งานเป็นลายลักษณ์อักษร

(๒) เก็บข้อมูล Logfile ที่ Firewall

(๓) เก็บ Logfile จากตัว Applications

ข้อ ๑๑๓. ผู้ละเมิดนโยบายด้านความปลอดภัยของ Firewall จะถูกระงับการใช้งานอินเทอร์เน็ตทันทีจนกว่าจะได้รับการแก้ไข

ข้อ ๑๑๔. ต้องตรวจสอบและปิดพอร์ตของระบบหรืออุปกรณ์ที่ไม่มีความจำเป็นในการใช้งานอย่างสม่ำเสมออย่างน้อยสัปดาห์ละ ๑ ครั้ง

## ส่วนที่ ๑๒ การควบคุมการใช้จดหมายอิเล็กทรอนิกส์ (E-Mail)

ข้อ ๑๑๕. ในการลงทะเบียนบัญชีผู้ใช้งานจดหมายอิเล็กทรอนิกส์ (E-Mail) ต้องทำการกรอกข้อมูลขอเข้าใช้บริการจดหมายอิเล็กทรอนิกส์ (E-Mail) โดยยื่นคำขอกับเจ้าหน้าที่หน่วยงาน

ข้อ ๑๑๖. รหัสจดหมายอิเล็กทรอนิกส์ เวลาใส่รหัสผ่านต้องไม่ปรากฏหรือแสดงรหัสผ่านออกมา แต่ต้องแสดงออกมาในรูปของสัญลักษณ์แทนตัวอักษรนั้น เช่น “x” หรือ “O” ในการพิมพ์แต่ละตัวอักษร

ข้อ ๑๑๗. เมื่อได้รับรหัสผ่าน (Password) ครั้งแรกในการเข้าระบบจดหมายอิเล็กทรอนิกส์ (E-Mail) และเมื่อมีการเข้าสู่ระบบในครั้งแรกนั้น ให้เปลี่ยนรหัสผ่าน (Password) โดยทันที

ข้อ ๑๑๘. ผู้ดูแลระบบ ต้องกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิดได้ เช่น ไม่เกิน ๓ ครั้ง

ข้อ ๑๑๙. ไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์

ข้อ ๑๒๐. เปลี่ยนรหัสผ่าน (Password) ทุก ๓ - ๖ เดือน

ข้อ ๑๒๑. ไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-Mail Address) ของผู้อื่นเพื่ออ่านหรือรับหรือส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้งานและให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์ (E-Mail) เป็นผู้รับผิดชอบต่อการใช้งานในจดหมายอิเล็กทรอนิกส์ (E-Mail) ของตน

ข้อ ๑๒๒. หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (E-Mail) เสร็จสิ้นต้องลงบันทึกออก (Logout) ทุกครั้ง

ข้อ ๑๒๓. การส่งข้อมูลที่เป็นความลับ ไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์ (E-Mail) เว้นเสียแต่ว่าจะใช้วิธีการเข้ารหัสข้อมูล E-Mail ที่หน่วยงานกำหนดไว้ ให้ใช้ความระมัดระวังในการระบุชื่อที่อยู่ E-Mail ของผู้รับให้ถูกต้องเพื่อป้องกันการส่งผิดตัวผู้รับ

ข้อ ๑๒๔. ห้ามส่งจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่มีลักษณะเป็นจดหมายขยะ (Spam Mail)

ข้อ ๑๒๕. ห้ามส่งจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่มีลักษณะเป็นจดหมายลูกโซ่ (Chain Letter)

ข้อ ๑๒๖. ห้ามส่งจดหมายอิเล็กทรอนิกส์ (E-Mail) E-Mail ที่มีลักษณะเป็นการละเมิดต่อกฎหมายหรือสิทธิของบุคคลอื่น

ข้อ ๑๒๗. ห้ามส่งจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่มีไวรัสไปให้กับบุคคลอื่นโดยเจตนา

ข้อ ๑๒๘. ให้ระบุชื่อของผู้ส่งใน จดหมายอิเล็กทรอนิกส์ (E-Mail) ทุกฉบับที่ส่งไป

ข้อ ๑๒๙. ให้ทำการสำรองข้อมูล จดหมายอิเล็กทรอนิกส์ (E-Mail) ตามความจำเป็นอย่างสม่ำเสมอ (แม้ว่าหน่วยงานจะทำการสำรองข้อมูล จดหมายอิเล็กทรอนิกส์ (E-Mail) ไว้ให้แต่ก็เพียงช่วงระยะเวลาหนึ่งเท่านั้น ดังนั้น จดหมายอิเล็กทรอนิกส์ (E-Mail) ที่เก่ามาก ๆ และจำเป็นต้องใช้งานจึงมีความจำเป็นต้องสำรองเก็บไว้ด้วยตนเอง)

ข้อ ๑๓๐. ผู้ใช้งานต้องทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนการเปิดเพื่อตรวจสอบไฟล์โดยใช้โปรแกรมป้องกันไวรัส เป็นการป้องกันในการเปิดไฟล์ที่เป็น Executable file เช่น .exe .com เป็นต้น

ข้อ ๑๓๑. ผู้ใช้งานต้องไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

ข้อ ๑๓๒. ผู้ใช้งานต้องไม่ใช้ข้อความที่ไม่สุภาพหรือรับส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสม ข้อมูลอันอาจทำให้เสียชื่อเสียงของหน่วยงาน ทำให้เกิดความแตกแยกระหว่างหน่วยงาน ผ่านทางจดหมายอิเล็กทรอนิกส์

ข้อ ๑๓๓. ผู้ใช้งานต้องตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ของตนเองทุกวัน และควรจัดเก็บแฟ้มข้อมูลและจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจำนวนน้อยที่สุด และควรลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้เนื้อที่ระบบจดหมายอิเล็กทรอนิกส์

ข้อ ๑๓๔. ผู้ใช้งานควรโอนย้ายจดหมายอิเล็กทรอนิกส์ที่จะใช้อ้างอิงภายหลังกายเครื่องคอมพิวเตอร์ของตน เพื่อเป็นการป้องกันผู้อื่นแอบอ่านจดหมายได้ ดังนั้นไม่ควรจัดเก็บข้อมูล หรือจดหมายอิเล็กทรอนิกส์ที่ไม่ได้ใช้แล้วไว้ในตู้จดหมายอิเล็กทรอนิกส์

ข้อ ๑๓๕. ผู้ใช้งานต้องใช้จดหมายอิเล็กทรอนิกส์ภาครัฐ สำหรับใช้รับ-ส่งข้อมูลในระบบราชการ ตามมติคณะรัฐมนตรีเมื่อวันที่ ๑๘ ธันวาคม ๒๕๕๐ เรื่อง การพัฒนาระบบจดหมายอิเล็กทรอนิกส์กลางเพื่อการสื่อสารในภาครัฐ

## ส่วนที่ ๑๓ การควบคุมการใช้อินเทอร์เน็ต (Internet)

ข้อ ๑๓๖. ผู้ดูแลระบบ ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ต ที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่หน่วยงานจัดสรรไว้เท่านั้น เช่น Proxy, Firewall, IPS-IDS เป็นต้น ห้ามผู้ใช้งานทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น เช่น Dial-up Modem ยกเว้นแต่ว่ามีเหตุผลความจำเป็นและต้องทำการขออนุญาตจากหัวหน้าหน่วยงานเป็นลายลักษณ์อักษร

ข้อ ๑๓๗. เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา ก่อนทำการเชื่อมต่ออินเทอร์เน็ต ผ่านเว็บเบราว์เซอร์ (Web browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัส และทำการอุดช่องโหว่ของระบบปฏิบัติการ

ข้อ ๑๓๘. ในการรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเทอร์เน็ตจะต้องมีการตรวจจับไวรัส (Virus scanning) โดยโปรแกรมป้องกันไวรัสก่อนการรับส่งข้อมูลทุกครั้ง

ข้อ ๑๓๙. ห้ามใช้เครือข่ายอินเทอร์เน็ตขององค์การ เพื่อกระทำการต่อไปนี้

(๑) หาประโยชน์ในเชิงธุรกิจส่วนตัว

(๒) เพื่อความบันเทิง ได้แก่ การเล่นเกมส์ ดูภาพยนตร์ ฟังเพลง

(๓) กระทำการที่ก่อให้เกิดความเสียหายต่อภาพลักษณ์ และชื่อเสียงขององค์การ เช่นการเผยแพร่ข้อมูลที่อาจก่อความเสียหายต่อองค์การ หรือข้อมูลสำคัญที่เป็นความลับขององค์การ

(๔) กระทำผิดกฎหมาย เช่น

- นำเข้าหรือเผยแพร่ ข้อมูลหรือชุดโปรแกรมที่ละเมิดลิขสิทธิ์
- แพร่กระจายโปรแกรมไม่ประสงค์ดี (Malware) เช่น ไวรัสคอมพิวเตอร์
- กระทำการที่ไม่เหมาะสมขัดต่อศีลธรรม เช่น การเล่นเกมออนไลน์ การนำเข้าหรือเผยแพร่สื่อลามก อนาจาร
- กระทำการที่ส่งผลร้าย กระทบกับความมั่นคงของชาติ ศาสนา พระมหากษัตริย์ เช่น การก่อการร้าย
- กระทำการข่มขู่ คุกคาม หรือละเมิดสิทธิของผู้อื่นให้ได้รับความเสียหาย เช่น การนำเข้าหรือเผยแพร่ภาพ เสียง สื่อผสมภาพและเสียง (Multimedia) ของผู้อื่น ทั้งที่เป็นข้อมูลจริงหรือข้อมูลเท็จอันเกิดจากการสร้าง ตัดต่อ แต่งเติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ที่ทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชังหรือได้รับความอับอาย
- กระทำการเป็นภัยต่อสังคม เช่น การนำเข้าหรือเผยแพร่ ข้อมูลที่มีลักษณะอันเป็นเท็จ เพื่อสร้างความสับสนวุ่นวาย หรือเพื่อการหลอกลวงให้เกิดความเสียหายต่างๆ

ข้อ ๑๔๐. ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของหน่วยงานที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต (Internet)

ข้อ ๑๔๑. รมัตระวังการดาวน์โหลด โปรแกรมใช้งานจากระบบอินเทอร์เน็ต (Internet) การอัปเดต (Update) โปรแกรมต่าง ๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์

ข้อ ๑๔๒. ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของหน่วยงาน

ข้อ ๑๔๓. ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ไม่เสนอความคิดเห็น หรือใช้ข้อความที่ยั่ว ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของหน่วยงาน การทำลายความสัมพันธ์กับบุคลากรของหน่วยงานอื่น ๆ

ข้อ ๑๔๔. ผู้ใช้งานไม่นำเข้าข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามก และไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเทอร์เน็ต

ข้อ ๑๔๕. หลังจากใช้งานระบบอินเทอร์เน็ตแล้ว ให้ปิดเว็บเบราว์เซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น ๆ

ข้อ ๑๔๖. หลังจากใช้งานอินเทอร์เน็ตเสร็จแล้ว ให้ทำการออกจากระบบเพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น ๆ

ข้อ ๑๔๗. ผู้ใช้งานต้องปฏิบัติตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และ/หรือกฎหมาย ระเบียบ วิธีปฏิบัติทางคอมพิวเตอร์ อื่นๆ ที่เกี่ยวข้อง อย่างเคร่งครัด

## ส่วนที่ ๑๔ การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล

### ข้อ ๑๔๘. แนวทางปฏิบัติการใช้งานทั่วไป

- (๑) เครื่องคอมพิวเตอร์ที่หน่วยงานอนุญาตให้ใช้งาน เป็นสินทรัพย์ของหน่วยงานเพื่อใช้ในงานราชการ
- (๒) โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของหน่วยงานต้องเป็นโปรแกรมที่หน่วยงานได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย
- (๓) ไม่อนุญาตให้ผู้ใช้งานทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ส่วนบุคคลของหน่วยงาน
- (๔) การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ส่วนบุคคลตรวจสอบจะต้องดำเนินการโดยเจ้าหน้าที่ของหน่วยงานหรือผู้รับจ้างเหมาบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้ทำสัญญากับกรมอนามัย เท่านั้น
- (๕) ก่อนการใช้งานสื่อบันทึกพกพาต่าง ๆ ต้องมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัส
- (๖) ผู้ใช้งาน มีหน้าที่และรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์
- (๗) ปิดเครื่องคอมพิวเตอร์ส่วนบุคคลที่ตนเองครอบครองใช้งานอยู่เมื่อใช้งานประจำวันเสร็จสิ้น หรือเมื่อมีการยุติการใช้งานเกินกว่า ๑ ชั่วโมง
- (๘) ทำการตั้งค่า Screen Saver ของเครื่องคอมพิวเตอร์ที่ตนเองรับผิดชอบให้มีการล็อกหน้าจอหลังจากที่ไม่ได้ใช้งานเกินกว่า ๑๕ นาที เพื่อป้องกันบุคคลอื่นมาใช้งานที่เครื่องคอมพิวเตอร์
- (๙) ห้ามนำเครื่องคอมพิวเตอร์ส่วนตัวที่เจ้าหน้าที่เป็นเจ้าของมาใช้กับระบบเครือข่ายของหน่วยงาน โดยไม่มีการติดตั้งโปรแกรมป้องกันไวรัสอย่างเหมาะสม และต้องปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานอย่างเคร่งครัด ยกเว้นจะได้รับการตรวจสอบจากผู้ดูแลระบบของหน่วยงานก่อนการใช้งาน

ข้อ ๑๔๙. การใช้รหัสผ่าน ให้ผู้ใช้งานปฏิบัติตามแนวทาง “การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน” ที่ระบุไว้ในเอกสารส่วนที่ ๓

### ข้อ ๑๕๐. การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)

- (๑) ผู้ใช้งานต้องตรวจสอบหาไวรัสจากสื่อต่าง ๆ เช่น Floppy Disk, Flash Drive และ Data Storage อื่น ๆ ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์
- (๒) ผู้ใช้งานต้องตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัส ก่อนใช้งาน
- (๓) ผู้ใช้งานต้องตรวจสอบข้อมูลคอมพิวเตอร์ใดที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ซึ่งมีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

- (๔) อุปกรณ์สื่อบันทึกข้อมูลที่ไม่ใช้งานแล้ว ต้องทำลายตามวิธีการที่กำหนดไว้ใน ส่วนที่ ๔ ข้อ ๓๗
- ข้อ ๑๕๑. การสำรองข้อมูลและการกู้คืน
- (๑) ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่น ๆ เช่น CD, DVD, External Hard Disk เป็นต้น
  - (๒) ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลสำรองไว้ อย่างสม่ำเสมอ
  - (๓) ผู้ใช้งานต้องประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้บน Hard Disk ไม่ควรจะเป็นข้อมูลสำคัญเกี่ยวข้องกับการทำงาน เพราะหาก Hard Disk เสียไป ก็ไม่กระทบ ต่อการดำเนินงานของหน่วยงาน



## ส่วนที่ ๑๕ การใช้งานเครื่องคอมพิวเตอร์แบบพกพา

### ข้อ ๑๕๒. แนวทางปฏิบัติการใช้งานทั่วไป

- (๑) เครื่องคอมพิวเตอร์แบบพกพาที่หน่วยงานอนุญาตให้ใช้งาน เป็นสินทรัพย์ของหน่วยงานเพื่อใช้ในงานราชการ
- (๒) โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์แบบพกพาของหน่วยงานต้องเป็นโปรแกรมที่หน่วยงาน ได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย
- (๓) ผู้ใช้งานต้องศึกษาและปฏิบัติตามคู่มือการใช้งานอย่างละเอียด เพื่อการใช้งานอย่างปลอดภัยและมีประสิทธิภาพ
- (๔) ไม่ดัดแปลงแก้ไขส่วนประกอบต่าง ๆ ของคอมพิวเตอร์และรักษาสภาพของคอมพิวเตอร์ให้มีสภาพเดิม
- (๕) ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพา ควรใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพา เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน เช่น การตกจากโต๊ะทำงาน หรือหลุดมือ เป็นต้น
- (๖) หลีกเลี่ยงการใช้นิ้วหรือของแข็ง เช่น ปลายปากกา กดสัมผัสหน้าจอ LCD ให้เป็นรอยขีดข่วนหรือทำให้จอ LCD ของเครื่องคอมพิวเตอร์แบบพกพาแตกเสียหายได้
- (๗) ไม่วางของทับบนหน้าจอและแป้นพิมพ์
- (๘) การเช็ดทำความสะอาดหน้าจอภาพต้องเช็ดอย่างเบามือที่สุด และต้องเช็ดไปในแนวทางเดียวกันห้ามเช็ดแบบหมุนวน เพราะจะทำให้หน้าจอมีรอยขีดข่วนได้
- (๙) การใช้เครื่องคอมพิวเตอร์แบบพกพาเป็นระยะเวลานานเกินไป ในสภาพที่มีอากาศร้อนจัด ต้องปิดเครื่องคอมพิวเตอร์เพื่อเป็นการพักเครื่องสักกระยะหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง
- (๑๐) การเคลื่อนย้ายเครื่อง ขณะที่เครื่องเปิดใช้งานอยู่ ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น

### ข้อ ๑๕๓. ความปลอดภัยทางด้านกายภาพ

- (๑) ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย เช่น ควรล็อกเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย
- (๒) ผู้ใช้งานไม่เก็บหรือใช้งานคอมพิวเตอร์แบบพกพาในสถานที่ที่มีความร้อน/ความชื้น/ฝุ่นละอองสูงและต้องระวังป้องกันการตกกระทบ

### ข้อ ๑๕๔. การควบคุมการเข้าถึงระบบปฏิบัติการ

- (๑) ผู้ใช้งานต้องกำหนดชื่อผู้ใช้งาน (User name) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์แบบพกพา
- (๒) ผู้ใช้งานต้องกำหนดรหัสผ่านให้มีคุณภาพดีอย่างน้อยตาม ที่ระบุไว้ในเอกสาร “การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน” ส่วนที่ ๗ การควบคุม

การเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and Information Access Control) ข้อ ๖๙

- (๓) ผู้ใช้งานต้องตั้งการใช้งานโปรแกรมรักษาจอภาพ (Screen Saver) โดยตั้งเวลาประมาณ ๑๕ นาที ให้ทำการล็อกหน้าจอเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานต้องใส่รหัสผ่าน
- (๔) ผู้ใช้งานต้องทำการ Logout ออกจากระบบทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

ข้อ ๑๕๕. การใช้รหัสผ่านให้ผู้ใช้งานปฏิบัติตามแนวทางการบริหารจัดการรหัสผ่านที่ระบุไว้ในเอกสาร “การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน” ส่วนที่ ๓ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

ข้อ ๑๕๖. การสำรองข้อมูลและการกู้คืน

- (๑) ผู้ใช้งานต้องทำการสำรองข้อมูลจากเครื่องคอมพิวเตอร์แบบพกพา โดยวิธีการและสื่อต่าง ๆ เพื่อป้องกันการสูญหายของข้อมูล
- (๒) ผู้ใช้งานต้องจะเก็บรักษาสื่อสำรองข้อมูล (Backup media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล
- (๓) แผ่นสื่อสำรองข้อมูลต่าง ๆ ที่เก็บข้อมูลไว้จะต้องทำการทดสอบการกู้คืนอย่างสม่ำเสมอ
- (๔) แผ่นสื่อสำรองข้อมูลที่ไม่ใช้งานแล้ว ต้องทำลายไม่ให้นำไปใช้งานได้อีก
- (๕) ผู้ใช้งานต้องประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้บน Hard Disk ไม่ควรจะเป็นข้อมูลสำคัญเกี่ยวข้องกับการทำงาน เพราะหาก Hard Disk เสียไป ก็ไม่กระทบ ต่อการดำเนินงานของหน่วยงาน

## ส่วนที่ ๑๖ การตรวจจับการบุกรุก

### (Intrusion Detection System / Intrusion Prevention System Policy : IDS/IPS )

ข้อ ๑๕๗. IDS/IPS Policy เป็นนโยบายการติดตั้งระบบตรวจสอบการบุกรุก และตรวจสอบความปลอดภัยของเครือข่าย เพื่อป้องกันทรัพยากร ระบบสารสนเทศ และข้อมูลบนเครือข่ายภายในหน่วยงาน ให้มีความมั่นคงปลอดภัย เป็นแนวทางการปฏิบัติเกี่ยวกับการตรวจสอบการบุกรุกเครือข่าย พร้อมกับบทบาทและความรับผิดชอบที่เกี่ยวข้อง

ข้อ ๑๕๘. IDS/IPS Policy ครอบคลุมทุกโฮสต์ (Host) ในเครือข่ายของหน่วยงานและเครือข่าย ข้อมูลทั้งหมด รวมถึงเส้นทางที่ข้อมูลอาจเดินทาง ซึ่งไม่อยู่ในเครือข่ายอินเทอร์เน็ตทุกเส้นทาง

ข้อ ๑๕๙. ระบบทั้งหมดที่สามารถเข้าถึงได้จากอินเทอร์เน็ตหรือที่สาธารณะจะต้องผ่านการตรวจสอบจากระบบ IDS/IPS

ข้อ ๑๖๐. ระบบทั้งหมดใน DMZ (Demilitarized zone) จะต้องได้รับการตรวจสอบรูปแบบการให้บริการก่อนการติดตั้งและเปิดให้บริการ

ข้อ ๑๖๑. โฮสต์ (Host) และเครือข่ายทั้งหมดที่มีการส่งผ่านข้อมูลผ่าน IDS/IPS จะต้องมีการบันทึกผลการตรวจสอบ

ข้อ ๑๖๒. ระบบ IDS/IPS จะต้องมีการตรวจสอบและ Update Patch/Signature เป็นประจำ

ข้อ ๑๖๓. ต้องมีการตรวจสอบเหตุการณ์ ข้อมูลจราจร พฤติกรรมการใช้งาน กิจกรรม และบันทึกปริมาณข้อมูลเข้าใช้งานเครือข่ายเป็นประจำทุกวันโดยผู้ดูแลระบบ

ข้อ ๑๖๔. IDS/IPS จะทำงานภายใต้กฎควบคุมพื้นฐานของ Firewall ที่ใช้ในการเข้าถึงเครือข่ายของระบบสารสนเทศตามปกติ

ข้อ ๑๖๕. เครื่องแม่ข่ายที่มีการติดตั้ง host-based IDS จะต้องมีการตรวจสอบข้อมูลประจำวัน

ข้อ ๑๖๖. ต้องรายงานพฤติกรรมการใช้งาน กิจกรรม หรือเหตุการณ์ทั้งหมด ที่มีความเสี่ยงต่อการบุกรุก การโจมตีระบบ พฤติกรรมที่น่าสงสัย หรือการพยายามเข้าระบบ ทั้งที่ประสบความสำเร็จและไม่ประสบความสำเร็จ ให้ผู้บริหารระดับสูงหรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่ ทราบทันทีที่ตรวจพบ

ข้อ ๑๖๗. ต้องรายงานพฤติกรรม กิจกรรมที่น่าสงสัย หรือระบบการทำงานที่ผิดปกติ ที่ถูกค้นพบ ให้หัวหน้าหน่วยงานหรือผู้ที่ได้รับมอบหมายทราบ ภายใน ๑ ชั่วโมงหลังจากที่ตรวจพบ

ข้อ ๑๖๘. การตรวจสอบการบุกรุกทั้งหมดจะต้องเก็บบันทึกข้อมูลไว้ไม่น้อยกว่า ๙๐ วัน

ข้อ ๑๖๙. ระบบ IDS/IPS มีรูปแบบการตอบสนองต่อเหตุการณ์ที่เกิดขึ้น ได้แก่ รายงานผลการตรวจพบของเหตุการณ์ต่าง ๆ ดำเนินการตามขั้นตอนเพื่อลดความเสียหาย ลบซอฟต์แวร์มัลแวร์ที่ตรวจพบ ป้องกันเหตุการณ์ที่อาจเกิดอีกในอนาคต และดำเนินการตามแผน

ข้อ ๑๗๐. หน่วยงานมีสิทธิ์ในการยุติการเชื่อมต่อเครือข่ายของเครื่องคอมพิวเตอร์ที่มีพฤติกรรมเสี่ยงต่อการบุกรุกระบบ โดยไม่ต้องมีการแจ้งแก่ผู้ใช้งานล่วงหน้า

ข้อ ๑๗๑. ผู้ที่ถูกตรวจสอบว่าพยายามกระทำการอันใดที่เป็นการละเมิดนโยบายของกรมอนามัย การพยายามเข้าถึงระบบโดยมิชอบ การโจมตีระบบ หรือมีพฤติกรรมเสี่ยงต่อการทำงานของระบบสารสนเทศ จะถูกระงับการใช้เครือข่ายทันที หากการกระทำดังกล่าวเป็นการกระทำความผิดที่สอดคล้องกับ กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ หรือเป็นการกระทำที่ส่งผลให้เกิดความเสียหายต่อข้อมูล และทรัพยากรระบบของหน่วยงาน จะต้องถูกดำเนินคดีตามขั้นตอนของกฎหมาย

## ส่วนที่ ๑๗ การติดตั้งและกำหนดค่าของระบบ (System Installation and Configuration)

- ข้อ ๑๗๒. การปรับปรุงระบบปฏิบัติการ (Operating System Update)
- (๑) ตรวจสอบเครื่องแม่ข่าย และอุปกรณ์ระบบ
  - (๒) ติดตั้งระบบปฏิบัติการตรงตามความต้องการการใช้งาน
  - (๓) กำหนดชื่อและรหัสผ่าน ผู้ดูแลระบบ และชื่อผู้ใช้งาน (User)
  - (๔) กำหนดค่าติดตั้ง ชื่อเครื่อง (Computer Name) / IP Address
  - (๕) ปรับปรุง / กำหนดค่าระดับความปลอดภัยของระบบปฏิบัติการ (กรณีที่มีระบบปฏิบัติการที่มี Service Patch Update)
  - (๖) ติดตั้งโปรแกรม Antivirus / ปรับปรุง Virus Definition และกำหนดค่าการตรวจสอบระบบการสแกนและปรับปรุงโปรแกรม
- ข้อ ๑๗๓. การบริหารบัญชีผู้ใช้งาน/สิทธิ์การเข้าถึงและการใช้งานระบบ (User Account Management)
- (๑) กำหนดชื่อและรหัสผ่าน ผู้ดูแลระบบ (System Administrator)
  - (๒) กำหนดชื่อผู้ใช้งาน (User Name) และรหัสผ่าน (Password)
  - (๓) บันทึกบัญชีผู้ใช้งานและสิทธิ์การเข้าใช้ระบบ
- ข้อ ๑๗๔. การปรับปรุงการรักษาความปลอดภัย / Anti-Virus (System Security & Antivirus Update)
- (๑) ติดตาม เฝ้าระวัง ระบบการทำงานของคอมพิวเตอร์ การเข้าใช้ระบบ
  - (๒) Performance ของระบบ หรือตรวจสอบจากระบบรักษาความปลอดภัยที่ติดตั้ง
  - (๓) ปรับปรุง / กำหนดค่าระบบความปลอดภัย ให้เหมาะสมกับปัญหา
  - (๔) ปรับปรุงโปรแกรม Antivirus และ Definition ให้ทันสมัยเป็นประจำทุกสัปดาห์
  - (๕) ดำเนินการ Scan ตรวจสอบไวรัสคอมพิวเตอร์ เป็นประจำ
- ข้อ ๑๗๕. การติดตั้ง / ปรับปรุงระบบจัดการฐานข้อมูล (Database Management Operation)
- (๑) ติดตั้งระบบจัดการฐานข้อมูล ตามความต้องการของระบบงานที่หน่วยงานใช้
  - (๒) กำหนดค่าระบบหรือโปรแกรมฐานข้อมูล ให้ทำงานร่วมกับระบบปฏิบัติการได้อย่างถูกต้อง และมีประสิทธิภาพ ตามระบบฐานข้อมูลนั้นกำหนด
  - (๓) สร้าง และกำหนดรายชื่อผู้บริหารระบบฐานข้อมูล (Database Admin) ชื่อผู้ใช้งานอื่นและสิทธิ์การใช้
  - (๔) ปรับปรุง / กำหนดค่าระบบให้เหมาะสม ทันสมัย หรือป้องกันการเกิดปัญหาอยู่เสมอ
- ข้อ ๑๗๖. การติดตั้งฐานข้อมูลโปรแกรมระบบงานต่าง ๆ / กำหนดค่าระบบของโปรแกรมและกำหนดผู้ใช้และสิทธิ์การเข้าใช้บริการ หรือเข้าถึงฐานข้อมูล
- (๑) ติดตั้งโปรแกรมระบบงานตามความต้องการ หรือการพัฒนา
  - (๒) กำหนดค่า หรือโปรแกรม หรือบริการ ให้ทำงานร่วมกับระบบปฏิบัติการ เป็นไปตามโปรแกรมหรือระบบงานนั้นอย่างถูกต้องและมีประสิทธิภาพ
  - (๓) ติดตั้งฐานข้อมูลและเชื่อมต่อระบบงาน และทำการทดสอบการให้บริการตามระบบงานนั้นกำหนด
  - (๔) แจ้งผู้ใช้งาน หรือเจ้าของระบบงาน ให้สามารถเริ่มใช้งานได้ โดยแจ้งรายชื่อ รหัสผ่าน และสิทธิ์การเข้าใช้ระบบและฐานข้อมูลตามที่กำหนดไว้
  - (๕) กำหนดเกณฑ์การสำรอง / สำเนา / ทดสอบกู้คืน (Restore Test)
  - (๖) บันทึกข้อกำหนด ค่าติดตั้ง และบัญชีชื่อผู้ใช้งานแต่ละระดับของระบบทุกครั้งที่มีการสร้าง / ปรับปรุง

## ส่วนที่ ๑๘ การจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log)

ข้อ ๑๗๗. จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วน ถูกต้อง แท้จริง ระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้ และข้อมูลที่ใช้ในการจัดเก็บ ต้องกำหนดชั้นความลับในการเข้าถึง

ข้อ ๑๗๘. ห้ามแก้ไขข้อมูลจราจรคอมพิวเตอร์ (Log) ที่เก็บรักษาไว้

ข้อ ๑๗๙. กำหนดให้มีการบันทึกการทำงานของระบบบันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้า - ออกระบบ บันทึกการพยายามเข้าสู่ระบบ เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกไว้อย่างน้อย ๙๐ วัน นับตั้งแต่การใช้งานสิ้นสุดลง โดยปฏิบัติตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

ข้อ ๑๘๐. ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่าง ๆ และจำกัดสิทธิ์การเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น