กรมการแพทย์

โรงพยาบาลเวชชารักษ์ ลำปาง

แนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

โรงพยาบาลเวชชารักษ์ ลำปาง

กรมการแพทย์

งานเทคโนโลยีสารสนเทศ กลุ่มงานดิจิทัลการแพทย์

ภารกิจด้านการพัฒนาระบบสุขภาพ

จัดทำปีพ.ศ. ๒๕๖๖

สารบัญ

แนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
โรงพยาบาลเวชชารักษ์ ลำปาง
กรมการแพทย์

๑. หลักการและเหตุผล

ตามที่พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ มาตรา ๕ มาตรา ๖ และมาตรา ๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินกิจกรรมหรือการให้บริการต่างๆ ของหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้

โรงพยาบาลเวชชารักษ์ ลำปาง กรมการแพทย์ ได้กำหนดแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขึ้น เพื่อให้ระบบเทคโนโลยีสารสนเทศของโรงพยาบาลเวชชารักษ์ ลำปาง กรมการแพทย์ เป็นไปอย่างเหมาะสม มีประสิทธิภาพ ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยให้สามารถดำเนินงานได้อย่างต่อเนื่องและป้องกันภัยคุกคามต่างๆ ปฏิบัติตามเจตนารมณ์ของพระราชกฤษฎีกาดังกล่าวได้อย่างถูกต้องและเหมาะสม นอกจากนี้ ยังได้เตรียมความพร้อมตามกฎหมายและประกาศด้านเทคโนโลยีสารสนเทศอื่นๆ ที่เกี่ยวข้อง รวมถึงการป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่างๆ ด้วย

๒. วัตถุประสงค์

โรงพยาบาลเวชชารักษ์ ลำปาง กรมการแพทย์ ได้กำหนดแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศมีวัตถุประสงค์ ดังต่อไปนี้

๒.๑ เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารหรือเครือข่ายคอมพิวเตอร์ขององค์กร ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผลและปฏิบัติได้อย่างถูกต้องตามกฎหมายต่างๆ ที่เกี่ยวข้องได้กำหนดไว้

๒.๒ เพื่อเผยแพร่แนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้เจ้าหน้าที่ทุกระดับในองค์กรได้รับทราบและเจ้าหน้าที่ทุกคนจะต้องลงนามยอมรับและปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

๒.๓ เพื่อกำหนดมาตรฐานแนวทางปฏิบัติและวิธีปฏิบัติ ให้ผู้บริหาร เจ้าหน้าที่ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับองค์กร ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร ในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด

๓. องค์ประกอบ

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศโรงพยาบาลเวชชารักษ์ ลำปาง กรมการแพทย์ จัดทำขึ้นเพื่อกำหนดแนวทางและวิธีการปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยแบ่งแนวปฏิบัติออกเป็นส่วนๆ ดังต่อไปนี้

ข้อ ๑ คำนิยาม

“หน่วยงาน” หมายถึง โรงพยาบาลเวชชารักษ์ ลำปาง

“ผู้ใช้งาน” หมายถึง ข้าราชการ ลูกจ้าง และพนักงานราชการ ผู้ดูแลระบบ ผู้บริหารองค์กร ผู้รับบริการ หรือผู้ที่ได้รับอนุญาตให้ใช้เครื่องคอมพิวเตอร์ และระบบเครือข่ายของหน่วยงาน

“ผู้บริหาร” หมายถึง ผู้มีอำนาจในการบังคับบัญชาในหน่วยงาน ได้แก่ รองผู้อำนวยการ หัวหน้ากลุ่มงาน หัวหน้างาน หรือเทียบเท่า เป็นต้น

“ผู้บริหารระดับสูง” หมายถึง ผู้อำนวยการหรือเทียบเท่า

“ผู้ดูแลระบบ” (System Administrator) หมายถึง ผู้ที่ได้รับมอบหมายจากหัวหน้าหน่วยงานให้มีหน้าที่รับผิดชอบดูแลรักษาหรือจัดการระบบคอมพิวเตอร์ และระบบเครือข่ายไม่ว่าส่วนหนึ่งส่วนใด

“เจ้าของข้อมูล” หมายถึง ผู้ได้รับมอบอำนาจจากหัวหน้าหน่วยงานให้รับผิดชอบข้อมูลของระบบงาน โดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น ๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้น เกิดสูญหาย

“สิทธิของผู้ใช้งาน” หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่ เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน โดยหน่วยงานจะเป็นผู้พิจารณาสิทธิในการใช้สินทรัพย์

“สินทรัพย์” หมายถึง ข้อมูล ระบบข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน เช่น เครื่องคอมพิวเตอร์ แบบตั้งโต๊ะและแบบพกพา อุปกรณ์สื่อสารที่สามารถเชื่อมต่อกับ ระบบเครือข่าย อาทิเช่น โทรศัพท์เคลื่อนที่ที่สามารถเชื่อมต่อกับระบบเครือข่ายได้ (Smartphone) อุปกรณ์ระบบเครือข่าย ฮาร์ดแวร์และซอฟต์แวร์ รวมถึงซอฟต์แวร์ที่มีลิขสิทธิ์ เป็นต้น

“ระบบเครือข่าย” หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ของหน่วยงานได้ เช่น ระบบเครือข่ายแบบมีสาย (LAN) และระบบเครือข่ายแบบไร้สาย (Wireless LAN) เป็นต้น

“การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ” หมายถึง การอนุญาต การกำหนดสิทธิ์ หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึง หรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทาง กายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

“ความมั่นคงปลอดภัยด้านสารสนเทศ” หมายถึง การธำรงไว้ซึ่งความลับ ความถูกต้อง ครบถ้วน และสภาพพร้อมใช้งานของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง ความรับผิด การห้ามปฏิเสธความรับผิด และความน่าเชื่อถือ

“เหตุการณ์ด้านความมั่นคงปลอดภัย” หมายถึง การเกิดเหตุการณ์ สภาพของบริการ หรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัย หรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

“สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด” หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ซึ่งอาจทำให้ระบบของหน่วยงานถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

หมวดที่ ๑
การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

วัตถุประสงค์

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

แนวปฏิบัติ

ส่วนที่ ๑ การควบคุมการเข้าถึงสารสนเทศ (Access Control)

ข้อ ๑ ผู้ดูแลระบบ จะอนุญาตให้ผู้ใช้งานเข้าถึงระบบสารสนเทศที่ต้องการใช้งานได้ ต่อเมื่อได้รับอนุญาตจากผู้รับผิดชอบ/เจ้าของข้อมูล/เจ้าของระบบและธุรกรรม ตามความจำเป็นต่อการใช้งาน เท่านั้น

ข้อ ๒ บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบสารสนเทศของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษรต่อหัวหน้าหน่วยงาน

ข้อ ๓ ผู้ดูแลระบบ ต้องกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งานและหน้าที่ความรับผิดชอบในการปฏิบัติงานของผู้ใช้งานระบบสารสนเทศ รวมทั้งมีการทบทวน สิทธิ์การเข้าถึงอย่างสม่ำเสมอ ดังนี้

(๑) กำหนดสิทธิ์ของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง
- อ่านอย่างเดียว
- สร้างข้อมูล
- ป้อนข้อมูล
- แก้ไข
- อนุมัติ
- ไม่มีสิทธิ์

(๒) กำหนดเกณฑ์การระงับสิทธิ์มอบอำนาจให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User access management) ที่ได้กำหนดไว้

(๓) ผู้ดูแลระบบมีหน้าที่ควบคุมดูแลการเข้าถึงระบบสารสนเทศและปฏิบัติงานตามหัวหน้าหน่วยงานมอบหมาย ดังนี้

(๓.๑) อนุญาตให้ผู้ใช้งานเข้าถึงระบบสารสนเทศของหน่วยงานจะกระทำได้ต่อเมื่อได้รับอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบที่ได้รับมอบหมาย

(๓.๒) กำหนดสิทธิ์ของผู้ใช้งานให้เหมาะสมกับการใช้งานและทบทวนสิทธิ์การเข้าถึงนั้นอย่างสม่ำเสมอ

(๓.๓) ติดตั้งระบบการบันทึกและติดตามการใช้งานและตรวจตราการละเมิด ความปลอดภัยที่มีต่อระบบสารสนเทศของหน่วยงานอย่างสม่ำเสมอ

ข้อ ๔. จัดแบ่งประเภทของข้อมูล การจัดลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล ระดับชั้นการเข้าถึง เวลาเข้าถึง และช่องทางการเข้าถึงข้อมูลไว้ให้ชัดเจนโดยใช้แนวทางตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ ซึ่งระเบียบดังกล่าวถือเป็นแนวทางที่เหมาะสมในการจัดการเอกสารอิเล็กทรอนิกส์และในการรักษาความปลอดภัยของเอกสารอิเล็กทรอนิกส์ โดยกำหนดกระบวนการและกรรมวิธีต่อเอกสารที่สำคัญไว้ ดังนี้

(๑) จัดแบ่งระดับชั้นการเข้าถึง
- ระดับชั้นสำหรับผู้บริหาร
- ระดับชั้นสำหรับผู้ใช้งานทั่วไป
- ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมาย

(๒) จัดแบ่งลำดับชั้นความลับของข้อมูล
- ข้อมูลลับที่สุด หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย<u>อย่างร้ายแรงที่สุด</u>
- ข้อมูลลับมาก หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย<u>อย่างร้ายแรงมาก</u>
- ข้อมูลลับ หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย
- ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

(๓) จัดแบ่งประเภทของข้อมูล
- ข้อมูลสารสนเทศด้านการบริหาร เป็นข้อมูลที่เกี่ยวข้องกับข้อมูลนโยบาย ข้อมูลยุทธศาสตร์และคำรับรอง ข้อมูลบุคลากร ข้อมูลงบประมาณการเงินและบัญชี
- ข้อมูลสารสนเทศด้านการแพทย์และการสาธารณสุขเป็นข้อมูลที่เกี่ยวข้องกับการรักษาผู้ป่วย ประวัติผู้ป่วย ข้อมูลทางการแพทย์และข้อมูลสถานพยาบาล

(๔) จัดแบ่งระดับชั้นการเข้าถึง
- ระดับชั้นสำหรับผู้บริหาร เข้าถึงได้ตามอำนาจหน้าที่และลำดับชั้นในบังคับบัญชาในหน่วยงานนั้น
- ระดับชั้นสำหรับผู้ใช้งานทั่วไป เข้าถึงได้เฉพาะข้อมูลที่ได้รับอนุญาตให้เข้าถึงได้ หรือได้ทำการเผยแพร่สำหรับผู้ใช้งานทั่วไป
- ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย เข้าถึงข้อมูลหรือระบบได้โดยสิทธิ์ที่ได้รับมอบหมายตามอำนาจหน้าที่

(๕) รูปแบบของเอกสารอิเล็กทรอนิกส์ให้ถือตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องหลักเกณฑ์และวิธีการในการจัดทำหรือแปลงเอกสาร และข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓

ข้อ ๕. ผู้ดูแลระบบต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังนี้

(๑) ควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบ

(๒) กำหนดบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อใช้ในการพิสูจน์ตัวตนของผู้ใช้งานข้อมูลในแต่ละชั้นความลับ

(๓) กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

(๔) การกำหนดให้เปลี่ยนรหัสผ่าน (Password) ตามระยะเวลาที่กำหนดความสำคัญของข้อมูลแต่ละระดับ

(๕) การรับ-ส่งข้อมูลด้วย SSL, VPN หรือ XML Encryption ผ่านระบบเครือข่าย ต้องเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล

(๖) กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำสินทรัพย์ของหน่วยงานออกนอกหน่วยงาน รวมถึงการบำรุงรักษาตรวจซ่อมให้ดำเนินการสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน

(๗) กำหนดเวลาการเข้าถึงระบบสารสนเทศหากมีการบันทึกแก้ไขข้อมูลสารบบคดีอิเล็กทรอนิกส์ให้เรียกรายงานได้ในเวลาเช้าวันรุ่งขึ้นในอีกวันถัดไปเท่านั่น เนื่องจากระบบจะทำการประมวลผลตอนเที่ยงคืน

(๘) การกำหนดระยะเวลาการเชื่อมต่อ (Limitation of Connection Time) สำหรับการใช้งานระบบสารสนเทศบางระบบให้เป็นไปตามช่วงเวลาการทำงานที่หน่วยงานกำหนด ส่วนระบบสารสนเทศที่มีความสำคัญสูงให้ทำการตัดระบบ และหมดเวลาการใช้งานรวมทั้งปิดการใช้งานด้วยหลังจากที่ไม่มีการใช้งานภายในช่วงระยะเวลา ๑๕ นาที

ข้อ ๖. มีข้อกำหนดการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control) โดยแบ่งการจัดทำข้อปฏิบัติเป็น ๒ ส่วน คือ

(๑) ควบคุมการเข้าถึงสารสนเทศโดยกำหนดแนวทางการควบคุมการเข้าถึงระบบสารสนเทศและสิทธิ์เกี่ยวข้องกับระบบสารสนเทศ

(๒) ปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย

ข้อ ๗. การกำหนดระบบและอุปกรณ์สนับสนุนการปฏิบัติงาน ดังนี้

(๑) มีระบบสนับสนุนการทำงานของระบบสารสนเทศของหน่วยงานที่เพียงพอต่อความต้องการใช้งาน ดังนี้ ระบบรักษาความปลอดภัย (Security) ระบบสำรองกระแสไฟฟ้า (UPS) เครื่องกำเนิดกระแสไฟฟ้าสสำรอง ระบบระบายอากาศ ระบบปรับอากาศและควบคุมความชื้น

(๒) ตรวจสอบหรือทดสอบระบบสนับสนุนเหล่านั้นอย่างสม่ำเสมอ เพื่อให้มั่นใจได้ว่าทำงานได้ปกติและลดความเสี่ยงจากความล้มเหลวในการทำงาน

(๓) ติดตั้งระบบแจ้งเตือนเพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงานภายในห้องศูนย์ข้อมูล (Data Center) เมื่อมีการทำงานเครื่องผิดปกติหรือหยุดการทำงาน

(๔) จัดวางอุปกรณ์ในพื้นที่หรือบริเวณที่เหมาะสมเพื่อหลีกเลี่ยงการเข้าถึงจากบุคคลภายนอก และให้แยกอุปกรณ์ที่มีความสำคัญเก็บไว้อีกพื้นที่หนึ่งที่มีความมั่นคงปลอดภัยเพียงพอ

(๕) ตรวจสอบสอดส่องดูแลสภาพแวดล้อมภายในห้องและตรวจสอบระดับอุณหภูมิความชื้นให้อยู่ระดับปกติเพื่อป้องกันความเสียหายต่ออุปกรณ์ที่อยู่ภายในห้องศูนย์ข้อมูล (Data Center)

(๖) การเดินสายไฟสายสัญญาณเครือข่ายของหน่วยงานและสายเคเบิลอื่นที่จำเป็นต้องทำการวางผ่านเข้าไปในบริเวณที่บุคคลภายนอกเข้าถึงได้นั้นให้ร้อยท่อสายสัญญาณต่างๆ เพื่อป้องกัน หนู นกกระรอก แมลงสาบ หรือสัตว์อื่นกัดสายไฟ ป้องกันการดักจับ สัญญาณ การตัดสายสัญญาณ อันจะทำให้เกิดความเสียหายต่อระบบเครือข่ายใช้งานไม่ได้

(๗) ต้องจัดทำแผนผังสายสัญญาณสื่อสารต่างๆ ให้ครบถ้วนถูกต้อง โดยสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซงรบกวนของสัญญาณซึ่งกันและกัน แล้วให้จัดเก็บสายสัญญาณต่างๆ ไว้ในตู้ Rack และปิดใส่สลักกุญแจให้สนิท เพื่อป้องกันการเข้าถึงจากบุคคลภายนอกหรือผู้ที่ไม่มีส่วนเกี่ยวข้อง

ส่วนที่ ๒ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

ข้อ ๘ ผู้ดูแลระบบ ต้องกำหนดการลงทะเบียนผู้ใช้งานใหม่ดังนี้

(๑) จัดทำแบบฟอร์มการลงทะเบียนผู้ใช้งาน สำหรับระบบเทคโนโลยีสารสนเทศ

(๒) ผู้ดูแลระบบต้องตรวจสอบบัญชีผู้ใช้งาน เพื่อไม่ให้มีการลงทะเบียนซ้ำซ้อน

(๓) ผู้ดูแลระบบต้องตรวจสอบและให้สิทธิ์ในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ (ตามข้อ ๓)

(๔) ผู้ดูแลระบบต้องกำหนดให้มีการแจกเอกสารหรือสิ่งที่แสดงเป็นลายลักษณ์อักษรให้แก่ผู้ใช้งานเพื่อแสดงถึงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งานในการเข้าถึงระบบเทคโนโลยีสารสนเทศ

ข้อ ๙ ผู้ดูแลระบบ ต้องกำหนดการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์ โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-Mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่และได้รับความเห็นชอบเป็นลายลักษณ์อักษร

ข้อ ๑๐ ผู้ดูแลระบบต้องทบทวนบัญชีผู้ใช้งาน สิทธิ์การใช้งาน อย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง หรือมีการโยกย้าย เปลี่ยนตำแหน่ง ลาออก หรือสิ้นสุดการจ้าง โดยปฏิบัติตามแนวทาง ดังนี้

(๑) พิมพ์รายชื่อของผู้ที่ยังมีสิทธิ์ในระบบแยกตามหน่วยงาน

(๒) จัดส่งรายชื่อนั้นให้กับผู้บังคับบัญชาของหน่วยงานเพื่อดำเนินการทบทวนรายชื่อและสิทธิ์การเข้าใช้งานว่าถูกต้องหรือไม่

(๓) ดำเนินการแก้ไขข้อมูล สิทธิ์ต่างๆ ให้ถูกต้องตามที่ได้รับแจ้งกลับจากหน่วยงาน

(๔) ขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน เมื่อลาออกต้องดำเนินการภายใน ๓ วัน หรือเมื่อเปลี่ยนตำแหน่งงานภายในต้องดำเนินการภายใน ๗ วัน หรือหน่วยงานกำหนด

ข้อ ๑๑ การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน

(๑) กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานลาออก หรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน

(๒) กำหนดชื่อผู้ใช้งานหรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

(๓) ส่งมอบรหัสผ่าน (Password) ชั่วคราวให้กับผู้ใช้งานด้วยวิธการที่ปลอดภัยหลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน (Password)

(๔) กำหนดให้ผู้ใช้งานตอบยืนยันการได้รับรหัสผ่าน (Password)

(๕) กำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่าน (Password) ผิดพลาดได้ไม่เกิน ๓ ครั้ง

(๖) กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

ข้อ ๑๒ ผู้ดูแลระบบ ต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงานรวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ มีดังต่อไปนี้

(๑) ควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

(๒) กำหนดรายชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้งานข้อมูลในแต่ละชั้นความลับของข้อมูล

(๓) กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

(๔) การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ต้องได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL หรือ VPN หรือ XML Encryption เป็นต้น

(๔) กำหนดการเปลี่ยนรหัสผ่าน (Password) ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

(๕) กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำสินทรัพย์ออกนอกหน่วยงาน เช่น บำรุงรักษา ตรวจซ่อม ให้ดำเนินการสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

(๖) เจ้าของข้อมูลต้องมีการตรวจสอบความเหมาะสมของสิทธิ์ในการเข้าถึงข้อมูลของ ผู้ใช้งานอย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิ์ต่างๆ ที่ให้ไว้ยังคงมีความเหมาะสม

(๗) หากมีการกระทำความผิดเกิดขึ้นจากชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของบุคคลใดบุคคลนั้น ต้องเป็นผู้รับผิดชอบต่อการกระทำความผิดนั้นตามกฎหมายระเบียบข้อบังคับที่เกี่ยวข้อง

ข้อ ๑๓ ระบบงานสารสนเทศทางธุรกิจที่เชื่อมโยงกัน (Business Information Systems)

ให้หัวหน้าหน่วยงานพิจารณาประเด็นต่างๆ ทางด้านความมั่นคงปลอดภัย และจุดอ่อนต่างๆ ก่อนตัดสินใจใช้ข้อมูลร่วมกันในระบบงาน หรือระบบเทคโนโลยีสารสนเทศที่จะเชื่อมโยงเข้าด้วยกัน เช่น ระหว่างกรมการแพทย์หรือหน่วยงานที่มาขอเชื่อมโยง

(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 รวมทั้งห้ามทำการเผยแพร่แจกจ่าย ทำให้ผู้อื่นล่วงรู้รหัสผ่าน (Password)

(๒) กำหนดรหัสผ่านประกอบด้วยตัวอักษรไม่น้อยกว่า ๘ ตัวอักษร ซึ่งต้องประกอบด้วย อย่างน้อย ๓ ใน ๕ ประเภท ดังต่อไปนี้

- ตัวอักษรภาษาอังกฤษตัวใหญ่ เช่น A, B, C
- ตัวอักษรภาษาอังกฤษตัวเล็ก เช่น a, b, c
- ตัวอักษรไทย เช่น ก, ข, ค, ง
- ตัวเลข เช่น ๑, ๒, ๓
- อักขระพิเศษต่าง ๆ เช่น ! @ # $ % ^ & *

(๓) หลีกเลี่ยงการตั้งรหัสผ่านที่อยู่บนพื้นฐานที่สามารถเดาได้ง่าย เช่น ชื่อหรือนามสกุลของตนเองหรือตรงกับคำในพจนานุกรม

(๕) ไม่ใช้โปรแกรมคอมพิวเตอร์ ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (save password) สำหรับเครื่องคอมพิวเตอร์ ส่วนบุคคลที่ผู้ใช้งานครอบครองอยู่

(๖) ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

ข้อ ๑๕ การกระทำใด ๆ ที่เกิดจากการใช้บัญชีของผู้ใช้งาน (Username) อันมีกฎหมายกำหนดให้เป็นความผิด ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม ให้ถือว่าเป็นความรับผิดชอบส่วนบุคคล ซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

ข้อ ๑๗. ผู้ใช้งานต้องตระหนักและระมัดระวังต่อการใช้งานข้อมูล ไม่ว่าข้อมูลนั้นจะเป็นของหน่วยงานหรือเป็นข้อมูลของบุคคลภายนอก

ข้อ ๑๘. เอกสารที่เป็นความลับหรือมีระดับความสำคัญด้านความมั่นคงปลอดภัย ซึ่งพิมพ์ออกจากเครื่องพิมพ์ (Printer) ตลอดจนข้อมูลที่เป็นความลับในรูปอิเล็กทรอนิกส์ ผู้ใช้งานต้องปฏิบัติให้เป็นไปตามระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความลับของทางราชการ ดังนี้

(๑) จัดหมวดหมู่เอกสารที่เป็นความลับหรือที่มีระดับความสำคัญสูงไว้ต่างหาก

(๒) จัดเก็บและกำหนดวิธีการป้องกันที่มีความปลอดภัยอย่างเพียงพอ

(๓) การเผยแพร่ เปลี่ยนแปลง ทำซ้ำ หรือทำลาย ต้องได้รับอนุญาตจากหัวหน้าหน่วยงาน หรือผู้ที่เป็นเจ้าของ

(๔) ตรวจสอบความถูกต้องของเอกสารก่อนนำไปใช้งาน

(๕) ทำลายเอกสารที่เป็นความลับ หรือมีระดับความสำคัญสูง เมื่อหมดความจำเป็นในการ ใช้งาน

ข้อ ๑๙ ผู้ใช้งานมีส่วนร่วมในการดูแลรักษาและรับผิดชอบต่อข้อมูลของโรงพยาบาลและข้อมูลของผู้รับบริการ หากเกิดการสูญหาย โดยนำไปใช้ในทางที่ผิด การเผยแพร่โดยไม่ได้รับอนุญาต ผู้ใช้งาน ต้องมีส่วนร่วมในการรับผิดชอบต่อความเสียหายนั้นด้วย

ข้อ ๒๐ ผู้ใช้งานต้องป้องกัน ดูแล รักษาไว้ซึ่งความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูล ตลอดจนเอกสาร สื่อบันทึกข้อมูลคอมพิวเตอร์ หรือสารสนเทศต่าง ๆ ที่เสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ์

ข้อ ๒๑ ผู้ใช้งานมีสิทธิ์โดยชอบธรรมที่จะเก็บรักษา ใช้งาน และป้องกันข้อมูลส่วนบุคคลตาม เห็นสมควร โรงพยาบาลจะให้การสนับสนุนและเคารพต่อสิทธิส่วนบุคคล และไม่อนุญาตให้บุคคล หนึ่งบุคคลใดทำการละเมิดต่อข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตจากผู้ใช้งานที่ครอบครองข้อมูลนั้น ยกเว้น ในกรณีที่หน่วยงานต้องการตรวจสอบข้อมูล หรือคาดว่าข้อมูลนั้นเกี่ยวข้องกับหน่วยงาน ซึ่งหน่วยงานอาจแต่งตั้งให้ผู้ทำหน้าที่ตรวจสอบทำการตรวจสอบข้อมูลเหล่านั้นได้ตลอดเวลา โดย ไม่ต้องแจ้งให้ผู้ใช้งานทราบ

ข้อ ๒๒ ห้ามเปิดหรือใช้งาน (Run) โปรแกรมประเภท Peer-to-Peer (หมายถึง วิธีการจัดเครือข่ายคอมพิวเตอร์แบบหนึ่ง ที่กำหนดให้คอมพิวเตอร์ในเครือข่ายทุกเครื่องเหมือนกันหรือเท่าเทียมกัน หมายความว่าแต่ละเครื่องต่างมีโปรแกรมหรือมีแฟ้มข้อมูลเก็บไว้เอง การจัดแบบนี้ทำให้สามารถใช้โปรแกรมหรือแฟ้มข้อมูลของคอมพิวเตอร์เครื่องใดก็ได้ แทนที่จะต้องใช้จากเครื่องบริการแฟ้ม (File Server) เท่านั้น) หรือโปรแกรมที่มีความเสี่ยงในระดับเดียวกัน เช่น บิททอร์เร้นท์ (Bittorrent), อีมูล (Emule) เป็นต้น เว้นแต่จะได้รับอนุญาตจากหัวหน้าหน่วยงาน

ข้อ ๒๓ ห้ามใช้สินทรัพย์ของหน่วยงาน ที่จัดเตรียมให้เพื่อการเผยแพร่ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใด ที่มีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมาย หรือกระทบต่อภารกิจของหน่วยงาน

ข้อ ๒๔ ห้ามใช้สินทรัพย์ของหน่วยงาน เพื่อการรบกวน ก่อให้เกิดความเสียหาย หรือใช้ในการโจรกรรมข้อมูล หรือสิ่งอื่นใดอันเป็นการขัดต่อกฎหมายและศีลธรรม หรือกระทบต่อภารกิจของหน่วยงาน

ข้อ ๒๕ ห้ามใช้สินทรัพย์ของหน่วยงานเพื่อประโยชน์ทางการค้า

ข้อ ๒๖ ห้ามกระทำการใด ๆ เพื่อการดักข้อมูล ไม่ว่าจะเป็นข้อความ ภาพ เสียง หรือสิ่งอื่นใดในเครือข่ายระบบสารสนเทศของหน่วยงาน โดยเด็ดขาด ไม่ว่าจะด้วยวิธีการใด ๆ ก็ตาม

ข้อ ๒๗ ห้ามกระทำการรบกวน ทำลาย หรือทำให้ระบบสารสนเทศของหน่วยงานต้องหยุดชะงัก

ข้อ ๒๘ ห้ามใช้ระบบสารสนเทศของหน่วยงาน เพื่อการควบคุมคอมพิวเตอร์ หรือระบบสารสนเทศภายนอก โดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบที่ได้รับมอบหมาย

ข้อ ๒๙ ห้ามกระทำการใด ๆ อันมีลักษณะเป็นการลักลอบใช้งานหรือรับรู้รหัสส่วนบุคคลของผู้อื่น ไม่ว่าจะเป็นกรณีใด ๆ เพื่อประโยชน์ในการเข้าถึงข้อมูล หรือเพื่อการใช้ทรัพยากรก็ตาม

ข้อ ๓๐ ห้ามติดตั้งอุปกรณ์หรือกระทำการใด ๆ เพื่อเข้าถึงระบบสารสนเทศของหน่วยงาน โดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบที่ได้รับมอบหมาย

ส่วนที่ ๔ การบริหารจัดการสินทรัพย์(Assets Management)

ข้อ ๓๑ ผู้ใช้งานต้องไม่เข้าไปในห้อง Data Center (Data Center หมายถึง สถานที่ ที่ใช้สำหรับติดตั้งเครื่องคอมพิวเตอร์ แม่ข่ายและ/หรืออุปกรณ์บริหารจัดการเครือข่าย) ที่เป็นเขตหวงห้ามโดย เด็ดขาด เว้นแต่ได้รับอนุญาตจากผู้ดูแล และปฏิบัติตามขั้นตอน/ระเบียบการเข้าห้อง Data Center

ข้อ ๓๒ ผู้ใช้งานต้องไม่นำอุปกรณ์หรือชิ้นส่วนใดออกจากห้อง Data Center เว้นแต่จะได้รับอนุญาตจากผู้ดูแล

ข้อ ๓๓ ผู้ใช้งานต้องไม่นำเครื่องมือหรืออุปกรณ์อื่นใด เชื่อมเข้าเครือข่ายเพื่อการประกอบธุรกิจส่วนบุคคล

ข้อ ๓๔ ผู้ใช้งานต้องไม่คัดลอกหรือทำสำเนาแฟ้มข้อมูลที่มีลิขสิทธิ์กำกับการใช้งาน ก่อนได้รับอนุญาต และผู้ใช้งานต้องไม่ใช้ หรือลบแฟ้มข้อมูลของผู้อื่น ไม่ว่ากรณีใดๆ

ข้อ ๓๗ ผู้ใช้งานต้องทำลายข้อมูลสำคัญในอุปกรณ์สื่อบันทึกข้อมูล แฟ้มข้อมูล ก่อนที่จะกำจัด อุปกรณ์ดังกล่าว และใช้เทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์ สำหรับจัดเก็บ ข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้ และ พิจารณาวิธีการทำลายข้อมูลบนสื่อบันทึกข้อมูลแต่ละประเภท

ข้อ ๓๕ ผู้ใช้งานมีหน้าที่ต้องรับผิดชอบต่อสินทรัพย์ที่หน่วยงานมอบไว้ให้ใช้งานเสมือนหนึ่งเป็นสินทรัพย์ของผู้ใช้งานเอง โดยบรรดารายการสินทรัพย์ (Asset lists) ที่ผู้ใช้งานต้องรับผิดชอบการรับหรือคืนสินทรัพย์ จะถูกบันทึกและตรวจสอบทุกครั้งโดยเจ้าหน้าที่ที่หน่วยงานมอบหมาย

ข้อ ๓๖ ผู้ใช้งานต้องไม่ให้ผู้อื่นยืมสินทรัพย์ ไม่ว่าในกรณีใดๆ เว้นแต่การยืมนั้นได้รับการอนุมัติเป็นลายลักษณ์อักษรจากหัวหน้าหน่วยงาน

ข้อ ๓๗ กรณีทำงานนอกสถานที่ผู้ใช้งานต้องดูแลและรับผิดชอบสินทรัพย์ของหน่วยงานที่ได้รับมอบหมาย

ข้อ ๓๘ ผู้ใช้งานมีหน้าที่ต้องชดใช้ค่าเสียหายไม่ว่าทรัพย์สินนั้นจะชำรุด หรือสูญหายตามมูลค่า ทรัพย์สินหากความเสียหายนั้นเกิดจากความประมาทของผู้ใช้งาน

ข้อ ๓๙ ผู้ใช้งานมีสิทธิ์ใช้สินทรัพย์และระบบสารสนเทศต่างๆ ที่หน่วยงานจัดเตรียมไว้ให้ใช้งานโดยมีวัตถุประสงค์เพื่อการใช้งานของหน่วยงานเท่านั้น ห้ามมิให้ผู้ใช้งานนำสินทรัพย์และระบบสารสนเทศต่างๆ ไปใช้ในกิจกรรมที่หน่วยงานไม่ได้กำหนด หรือทำให้เกิดความเสียหายต่อหน่วยงาน

ข้อ ๔๐ ความเสียหายใดๆ ที่เกิดจากการละเมิดตามข้อ ๔๒ ให้ถือเป็นความผิดส่วนบุคคลโดยผู้ใช้งานต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

ส่วนที่ ๕ การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

ข้อ ๔๑ ผู้ใช้งานจะนำเครื่องคอมพิวเตอร์ อุปกรณ์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์ระบบเครือข่ายของหน่วยงาน ต้องได้รับอนุญาตจากหัวหน้าหน่วยงานและต้องปฏิบัติตามนโยบายนี้โดยเคร่งครัด โดยผู้ใช้งานต้องกรอกแบบฟอร์ม “การขอเชื่อมต่อเครือข่าย” ของหน่วยงาน

ข้อ ๔๒ ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใด ๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลักโดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ ๔๓ ผู้ดูแลระบบ ต้องควบคุมการเข้าถึงระบบเครือข่าย เพื่อบริหารจัดการระบบเครือข่ายได้อย่างมีประสิทธิภาพ ดังต่อไปนี้

(๑) ต้องจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น

(๒) ต้องจำกัดเส้นทางการเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน

(๓) ต้องจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์ แม่ข่าย เพื่อไม่ให้ผู้ใช้งานสามารถใช้เส้นทางอื่นๆ ได้

(๔) ระบบเครือข่ายทั้งหมดของหน่วยงานที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ภายนอกหน่วยงานต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก รวมทั้งต้องมี ความสามารถในการตรวจจับโปรแกรมประสงค์ร้าย (Malware) ด้วย

(๕) ระบบเครือข่ายต้องติดตั้งระบบตรวจจับการบุกรุก (Intrusion Prevention System/Intrusion Detection System) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของหน่วยงานในลักษณะที่ผิดปกติ

(๖) การเข้าสู่ระบบเครือข่ายภายในหน่วยงาน โดยผ่านทางระบบอินเทอร์เน็ตจำเป็นต้องมีการลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่าน เพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนทุกครั้ง

(๗) ต้องป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็น IP Address ภายในของระบบเครือข่ายภายในของหน่วยงาน

(๘) ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

(๙) การระบุอุปกรณ์บนเครือข่าย

- ผู้ดูแลระบบมีการเก็บบัญชีการขอเชื่อมต่อเครือข่าย ได้แก่ รายชื่อผู้ขอใช้บริการ รายละเอียด เครื่องคอมพิวเตอร์ ที่ขอใช้บริการ IP Address และสถานที่ติดตั้ง
- อุปกรณ์ที่นำมาเชื่อมต่อจะได้รับหมายเลข IP Address ตามที่กำหนดโดยผู้ดูแลระบบเครือข่าย
- ผู้ดูแลระบบต้องจำกัดผู้ใช้งานที่สามารถเข้าใช้อุปกรณ์ได้
- กรณีอุปกรณ์ที่มีการเชื่อมต่อจากเครือข่ายภายนอก ต้องมีการระบุหมายเลขอุปกรณ์ว่าสามารถเข้าเชื่อมต่อกับเครือข่ายภายในได้หรือไม่สามารถเชื่อมต่อได้
- อุปกรณ์เครือข่ายต้องสามารถตรวจสอบ IP Address ของทั้งต้นทางและปลายทางได้
- การเข้าใช้งานอุปกรณ์บนเครือข่ายต้องทำการพิสูจน์ตัวตนทุกครั้งที่ใช้อุปกรณ์

ข้อ ๔๔ ผู้ดูแลระบบ ต้องบริหารควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server) และรับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย ในการกำหนดแก้ไข หรือเปลี่ยนแปลงค่าต่างๆ ของซอฟต์แวร์ระบบ (Systems Software)

ข้อ ๔๕ การติดตั้งหรือปรับปรุงซอฟต์แวร์ของระบบงานต้องมีการขออนุมัติจากผู้ดูแลระบบให้ติดตั้งก่อนดำเนินการ

ข้อ ๔๖ ผู้ดูแลระบบ ต้องควบคุมการเข้าถึงระบบเครือข่าย เพื่อบริหารจัดการระบบเครือข่ายได้อย่างมีประสิทธิภาพ ดังต่อไปนี้

(๑) ต้องจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น

(๒) ต้องจำกัดเส้นทางการเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน

(๓) ต้องจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์ แม่ข่าย เพื่อไม่ให้ผู้ใช้งานสามารถใช้เส้นทางอื่นๆ ได้

(๔) ระบบเครือข่ายทั้งหมดของหน่วยงานที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ภายนอกหน่วยงานต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก รวมทั้งต้องมี ความสามารถในการตรวจจับโปรแกรมประสงค์ร้าย (Malware) ด้วย

(๕) ระบบเครือข่ายต้องติดตั้งระบบตรวจจับการบุกรุก (Intrusion Prevention System/Intrusion Detection System) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของหน่วยงานในลักษณะที่ผิดปกติ

(๖) การเข้าสู่ระบบเครือข่ายภายในหน่วยงาน โดยผ่านทางระบบอินเทอร์เน็ตจำเป็นต้องมีการลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่าน เพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนทุกครั้ง

(๗) ต้องป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็น IP Address ภายในของระบบเครือข่ายภายในของหน่วยงาน

(๘) ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

(๙) การระบุอุปกรณ์บนเครือข่าย

- ผู้ดูแลระบบมีการเก็บบัญชีการขอเชื่อมต่อเครือข่าย ได้แก่ รายชื่อผู้ขอใช้บริการ รายละเอียด เครื่องคอมพิวเตอร์ ที่ขอใช้บริการ IP Address และสถานที่ติดตั้ง
- อุปกรณ์ที่นำมาเชื่อมต่อจะได้รับหมายเลข IP Address ตามที่กำหนดโดยผู้ดูแลระบบเครือข่าย
- ผู้ดูแลระบบต้องจำกัดผู้ใช้งานที่สามารถเข้าใช้อุปกรณ์ได้
- กรณีอุปกรณ์ที่มีการเชื่อมต่อจากเครือข่ายภายนอก ต้องมีการระบุหมายเลขอุปกรณ์ว่าสามารถเข้าเชื่อมต่อกับเครือข่ายภายในได้หรือไม่สามารถเชื่อมต่อได้
- อุปกรณ์เครือข่ายต้องสามารถตรวจสอบ IP Address ของทั้งต้นทางและปลายทางได้
- การเข้าใช้งานอุปกรณ์บนเครือข่ายต้องทำการพิสูจน์ตัวตนทุกครั้งที่ใช้อุปกรณ์

ข้อ ๔๗ ผู้ดูแลระบบ ต้องบริหารควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server) และรับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย ในการกำหนดแก้ไข หรือเปลี่ยนแปลงค่าต่างๆ ของซอฟต์แวร์ระบบ (Systems Software)

ข้อ ๔๘ การติดตั้งหรือปรับปรุงซอฟต์แวร์ของระบบงานต้องมีการขออนุมัติจากผู้ดูแลระบบให้ติดตั้งก่อนดำเนินการ

ส่วนที่ ๖ การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

ข้อ ๔๙ ผู้ดูแลระบบ ต้องกำหนดการลงทะเบียนบุคลากรใหม่ของหน่วยงาน (โดยปฏิบัติตามข้อ ๘) ในการใช้งานตามความจำเป็นรวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน (โดยปฏิบัติตามข้อ ๑๐) เช่น การลาออก หรือการเปลี่ยนตำแหน่งงานภายในหน่วยงาน เป็นต้น

ข้อ ๕๐ กำหนดขั้นตอนการปฏิบัติเพื่อเข้าใช้งาน

(๑) ผู้ใช้งานต้องกำหนดรหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ ที่รับผิดชอบ

(๒) หลังจากระบบติดตั้งเสร็จ ควรมีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ หรือมีการทำงานในลักษณะอัตโนมัติซึ่งเอื้อต่อการเปลี่ยนรหัสผ่านของ ผู้ใช้งานที่ได้ถูกกำหนดไว้เริ่มต้นที่มาพร้อมกับการติดตั้งระบบโดยทันที

(๓) ผู้ใช้งานต้องตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ (Screen saver) เพื่อทำการล็อกหน้าจอภาพเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้งานต้องใส่ รหัสผ่าน (Password) เพื่อเข้าใช้งาน

(๔) ก่อนการเข้าใช้ระบบปฏิบัติการต้องทำการลงบันทึกเข้าใช้งาน (Login) ทุกครั้ง

(๕) ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ ของหน่วยงานร่วมกัน

(๖) ผู้ใช้งานต้องทำการลงบันทึกออก (Logout) ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

(๗) ห้ามเปิดหรือใช้งานโปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยง เว้นแต่จะได้รับอนุญาตจากหัวหน้าหน่วยงาน

(๘) ซอฟท์แวร์ที่หน่วยงานจัดเตรียมไว้ให้ผู้ใช้งานถือเป็นสิ่งจำเป็น ห้ามมิให้ผู้ใช้งานทำการติดตั้ง ถอดถอนเปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่น

(๙) ห้ามใช้ทรัพยากรทุกประเภทที่เป็นของหน่วยงาน เพื่อประโยชน์ทางการค้า

(๑๐) ห้ามผู้ใช้งานนำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์ แสดงข้อความรูปภาพไม่เหมาะสม หรือขัดต่อศีลธรรม กรณีผู้ใช้งานสร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์

(๑๑) ห้ามผู้ใช้งานของหน่วยงาน ควบคุมคอมพิวเตอร์ หรือระบบสารสนเทศภายนอกโดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงาน

ส่วนที่ ๗ การควบคุมการเข้าถึงโปรแกรมประยุกต์ หรือแอพพลิเคชั่นและสารสนเทศ (Application and Information Access Control)

ข้อ ๕๑ การใช้งานอุปกรณ์คอมพิวเตอร์ และสื่อสารเคลื่อนที่ ต้องปฏิบัติดังต่อไปนี้

(๑) ระมัดระวังไม่ให้บุคคลภายนอกคัดลอกข้อมูลจากคอมพิวเตอร์ที่นำไปใช้ได้ เว้นแต่ข้อมูลที่ได้มีการเผยแพร่เป็นการทั่วไป

(๒) เมื่อหมดความจำเป็นต้องใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ แล้วให้รีบนำส่งคืนเจ้าหน้าที่ที่รับผิดชอบทันที

(๓) หากปรากฏว่าความเสียหายที่เกิดขึ้นนั้นเกิดจากความประมาทอย่างร้ายแรงของผู้นำไปใช้ ผู้นำไปใช้ต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

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

ข้อ ๕๒ ซอฟต์แวร์ (Software) ที่หน่วยงานได้จัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็นต่อการทำงาน ห้ามมิให้ผู้ใช้งานทำการถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่นๆ ยกเว้นได้รับการอนุญาตจากหัวหน้าหน่วยงานหรือผู้ที่ได้รับมอบหมายที่มีสิทธิ์ในลิขสิทธิ์

ข้อ ๕๓ คอมพิวเตอร์ของผู้ใช้งานติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ (Anti virus) ตามที่หน่วยงานได้ประกาศให้ใช้ เว้นแต่คอมพิวเตอร์นั้นเป็นเครื่องเพื่อการศึกษา โดยต้องได้รับอนุญาตจากหัวหน้าหน่วยงาน

ข้อ ๕๔ บรรดาข้อมูล ไฟล์ ซอฟต์แวร์ หรือสิ่งอื่นใด ที่ได้รับจากผู้ใช้งานอื่นต้องได้รับการตรวจสอบไวรัสคอมพิวเตอร์และโปรแกรมไม่ประสงค์ดีก่อนนำมาใช้งานหรือเก็บบันทึกทุกครั้ง

ข้อ ๕๕ ผู้ใช้งานต้องทำการปรับปรุงข้อมูลสำหรับตรวจสอบและปรับปรุงระบบปฏิบัติการ (Update patch) ให้ใหม่เสมอ เพื่อเป็นการป้องกันความเสียหายที่อาจเกิดขึ้น

ข้อ ๕๖ ผู้ใช้งานต้องพึงระวังไวรัสและโปรแกรมไม่ประสงค์ดีตลอดเวลา รวมทั้งเมื่อพบสิ่งผิดปกติ ผู้ใช้งานต้องแจ้งเหตุแก่ผู้ดูแลระบบ

ข้อ ๕๗ เมื่อผู้ใช้งานพบว่าเครื่องคอมพิวเตอร์ติดไวรัส ผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์เข้าสู่เครือข่าย และต้องแจ้งแก่ผู้ดูแลระบบ

ข้อ ๕๘ ห้ามลักลอบทำสำเนา เปลี่ยนแปลง ลบทิ้ง ซึ่งข้อมูล ข้อความ เอกสาร หรือสิ่งใดๆ ที่เป็นสินทรัพย์ของหน่วยงาน หรือของผู้อื่น โดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงาน

ข้อ ๕๙ ห้ามทำการเผยแพร่ไวรัสคอมพิวเตอร์ มัลแวร์ หรือโปรแกรมอันตรายใดๆ ที่อาจก่อให้เกิดความเสียหายมาสู่สินทรัพย์ของหน่วยงาน สิทธิ์ที่จะพัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ สามารถดำเนินการได้ แต่ต้องไม่ดำเนินการดังนี้

(๑) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ ที่จะทำลายกลไกรักษาความปลอดภัยระบบ รวมทั้งการกระทำในลักษณะเป็นการแอบใช้รหัสผ่าน การลักลอบทำสำเนาข้อมูล บุคคลอื่นหรือแกะรหัสผ่านของบุคคลอื่น

(๒) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ ซึ่งทำให้ผู้ใช้งานมีสิทธิ์และลำดับความสำคัญในการครอบครองทรัพยากรระบบมากกว่าผู้ใช้งานอื่น

(๓) พัฒนาโปรแกรมใดที่จะทำซ้ำตัวโปรแกรมหรือแฝงตัวโปรแกรมไปกับโปรแกรมอื่นในลักษณะเช่นเดียวกับหนอนหรือไวรัสคอมพิวเตอร์

(๔) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ ที่จะทำลายระบบจำกัดสิทธิการใช้ (License) ซอฟต์แวร์

(๕) นำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์แสดงข้อความรูปภาพไม่เหมาะสม หรือขัดต่อศีลธรรมประเพณีอันดีงามของประเทศไทย กรณีที่ผู้ใช้งานสร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์

ข้อ ๖๐ การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก (Outsourced software development)

(๑) จัดให้มีการควบคุมโครงการพัฒนาซอฟต์แวร์โดยผู้รับจ้างให้บริการจากภายนอก

(๒) พิจารณาระบุว่าใครจะเป็นผู้มีสิทธิ์ในทรัพย์สินทางปัญญาสำหรับซอร์สโค้ดในการพัฒนาซอฟต์แวร์โดยผู้รับจ้างให้บริการจากภายนอก

(๓) พิจารณากำหนดเรื่องการสงวนสิทธิ์ที่จะตรวจสอบด้านคุณภาพและความถูกต้องของซอฟต์แวร์ที่จะมีการพัฒนาโดยผู้ให้บริการภายนอก โดยระบุไว้ในสัญญาจ้างที่ทำกับผู้ให้บริการภายนอกนั้น

(๔) ให้มีการตรวจสอบโปรแกรมไม่ประสงค์ดี ในซอฟต์แวร์ต่างๆ ที่จะทำการติดตั้งก่อนดำเนินการติดตั้ง

(๕) หลังจากการส่งมอบการพัฒนาซอฟแวร์จากหน่วยงานภายนอก หน่วยงานต้องดำเนินการเปลี่ยนรหัสผ่านต่างๆ

(๖) ผู้พัฒนาระบบจากภายนอก (Outsource) ต้องลงนามในสัญญาไม่เปิดเผยข้อมูล (Non-Disclosure Agreement) ก่อนดำเนินการ

(๗) ผู้พัฒนาระบบจากภายนอก (Outsource) ต้องถือปฏิบัติตามแนวนโยบาย และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของหน่วยงาน

ส่วนที่ ๙ การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)

ข้อ ๖๑ ต้องมีการตรวจสอบว่าอุปกรณ์ที่เป็นของส่วนตัวซึ่งใช้ในการเข้าถึงระบบเทคโนโลยีสารสนเทศของหน่วยงานจากระยะไกลมีการป้องกันไวรัสและการใช้งานไฟร์วอลล์ ตามที่หน่วยงานกำหนด

ข้อ ๖๒ ผู้ใช้งานจากระยะไกลทุกคน ต้องผ่านการพิสูจน์ตัวตนก่อนการใช้งาน เพื่อเพิ่มความปลอดภัย เช่น รหัสผ่าน หรือวิธีการเข้ารหัส เป็นต้น

ข้อ ๖๓ ไม่อนุญาตให้ใช้งานอุปกรณ์ที่เป็นของส่วนตัวเพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศของหน่วยงานจากระยะไกล หากอุปกรณ์ดังกล่าวไม่อยู่ภายใต้การควบคุมตามนโยบายความมั่นคงปลอดภัยของหน่วยงาน

ส่วนที่ ๑๐ การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

ข้อ ๖๔ ผู้ดูแลระบบ ต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point) ให้รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายน้อยที่สุด

ข้อ ๖๕ ผู้ดูแลระบบ ต้องใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายเพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย และในกรณีที่ตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติ ให้ผู้ดูแลระบบ รายงานต่อหัวหน้าหน่วยงานทราบทันที

ข้อ ๖๖ ผู้ดูแลระบบ ต้องควบคุมดูแลไม่ให้บุคคลหรือหน่วยงานภายนอกที่ไม่ได้รับอนุญาตใช้งานระบบเครือข่ายไร้สายในการเข้าสู่ ระบบเครือข่ายและระบบสารสนเทศภายในหน่วยงาน

ข้อ ๖๗ ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของหน่วยงาน จะต้องทำการลงทะเบียนกับผู้ดูแลระบบและต้องได้รับพิจารณาอนุญาตจากหัวหน้าหน่วยงานอย่างเป็นลายลักษณ์อักษร

ข้อ ๖๘ ผู้ดูแลระบบ ต้องทำการลงทะเบียนกำหนดสิทธิ์ผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สาย ให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงาน ก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้ง มีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ จะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

ส่วนที่ ๑๑ การควบคุมการใช้งานอุปกรณ์ป้องกันเครือข่าย (Firewall Control)

ข้อ ๖๙ หน่วยงานมีหน้าที่ในการบริหารจัดการ การติดตั้งและกำหนดค่าของ Firewall ทั้งหมด

ข้อ ๗๐ ผู้ใช้งานอินเทอร์เน็ตจะต้องทำการลงบันทึกเข้าใช้งาน (Login) ก่อนการใช้ทุกครั้ง

ข้อ ๗๑ การเข้าถึงตัวอุปกรณ์ Firewall จะต้องสามารถเข้าถึงได้เฉพาะผู้ที่ได้รับมอบหมายให้ดูแลจัดการเท่านั้น

ข้อ ๗๒ จะต้องมีการสำรองข้อมูลการกำหนดค่าต่างๆ ของอุปกรณ์ป้องกันเครือข่าย (Firewall) เป็นประจำทุกเดือนและทุกครั้งก่อนที่จะมีการเปลี่ยนแปลงค่า

ข้อ ๗๓ เครื่องคอมพิวเตอร์ แม่ข่ายที่ให้บริการระบบงานสารสนเทศต่างๆ ภายในหน่วยงานที่มีลักษณะที่เป็นอินทราเน็ตจะต้องไม่อนุญาตให้มีการเชื่อมต่อเพื่อใช้งานอินเทอร์เน็ตเว้นแต่มีความจำเป็นโดยจะต้องกำหนดเป็นกรณีไป

ข้อ ๗๔ หน่วยงานมีสิทธิ์ที่จะระงับหรือบล็อกการใช้งานของเครื่องคอมพิวเตอร์ ลูกข่ายที่มีพฤติกรรมการใช้งานที่ผิดหรือเสี่ยงต่อความปลอดภัยของระบบเครือข่ายส่วนรวม หรือเกิดจากการทำงานของ โปรแกรมที่มีความเสี่ยงต่อความปลอดภัยจนกว่าจะได้รับการแก้ไข

ข้อ ๗๕ ผู้ละเมิดนโยบายด้านความปลอดภัยของ Firewall จะถูกระงับการใช้งานอินเทอร์เน็ตทันที

ส่วนที่ ๑๒ การควบคุมการใช้จดหมายอิเล็กทรอนิกส์ (E-Mail)

ข้อ ๗๖ ในการลงทะเบียนบัญชีผู้ใช้งานจดหมายอิเล็กทรอนิกส์ (E-Mail) ต้องทำการกรอกข้อมูลขอเข้าใช้บริการจดหมายอิเล็กทรอนิกส์ (E-Mail) โดยยื่นคำขอกับเจ้าหน้าที่หน่วยงาน

ข้อ ๗๗ เมื่อได้รับรหัสผ่าน (Password) ครั้งแรกในการเข้าระบบจดหมายอิเล็กทรอนิกส์ (E-Mail) และเมื่อมีการเข้าสู่ ระบบในครั้งแรกนั้น ให้เปลี่ยนรหัสผ่าน (Password) โดยทันที

ข้อ ๗๘ ไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-Mail Address) ของผู้อื่นเพื่ออ่านหรือรับหรือส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้งานและให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์ (E-Mail) เป็นผู้รับผิดชอบต่อการใช้งานในจดหมายอิเล็กทรอนิกส์ (E-Mail) ของตน

ข้อ ๗๙ หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (E-Mail) เสร็จสิ้นต้องลงบันทึกออก (Logout) ทุกครั้ง

ข้อ ๘๐ การส่งข้อมูลที่เป็นความลับ ไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์ (E-Mail) เว้นเสียแต่ว่าจะใช้วิธีการเข้ารหัสข้อมูล E-Mail ที่หน่วยงานกำหนดไว้และให้ใช้ความระมัดระวังในการระบุชื่อที่อยู่ E-Mail ของผู้รับให้ถูกต้องเพื่อป้องกันการส่งผิดตัวผู้รับ

ข้อ ๘๑ ห้ามส่ง E-Mail ที่มีลักษณะเป็นจดหมายขยะ (Spam Mail)

ข้อ ๘๒ ห้ามส่งจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่มีลักษณะเป็นจดหมายลูกโซ่ (Chain Letter)

ข้อ ๘๓ ห้ามส่งจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่มีลักษณะเป็นการละเมิดต่อกฎหมาย หรือสิทธิของบุคคลอื่น

ข้อ ๘๔ ห้ามส่งจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่มีไวรัสไปให้กับบุคคลอื่นโดยเจตนา

ข้อ ๘๕ ให้ระบุชื่อของผู้ส่งในจดหมายอิเล็กทรอนิกส์ (E-Mail) ทุกฉบับที่ส่งไป

ข้อ ๘๖ ผู้ใช้งานต้องทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนการเปิดเพื่อตรวจสอบไฟล์โดยใช้โปรแกรมป้องกันไวรัส เป็นการป้องกันในการเปิดไฟล์ที่เป็น Executable file เช่น .exe .com เป็นต้น

ข้อ ๘๗ ผู้ใช้งานต้องไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

ข้อ ๘๘ ผู้ใช้งานต้องไม่ใช้ข้อความที่ไม่สุภาพหรือรับส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสม หรือข้อมูลอันอาจทำให้เสียชื่อเสียงของหน่วยงาน ทำให้เกิดความแตกแยกระหว่างหน่วยงาน ผ่านทางจดหมายอิเล็กทรอนิกส์

ส่วนที่ ๑๓ การควบคุมการใช้อินเทอร์เน็ต (Internet)

ข้อ ๘๙ เครื่องคอมพิวเตอร์ส่วนบุคคล และเครื่องคอมพิวเตอร์แบบพกพา ก่อนทำการเชื่อมต่ออินเทอร์เน็ตผ่านเว็บเบราเซอร์ (Web browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัส และควรทำการอุดช่องโหว่ ของระบบปฏิบัติการ

ข้อ ๙๐ ในการรับส่งข้อมูลคอมพิวเตอร์ ผ่านทางอินเตอร์ เน็ตจะต้องมีการตรวจจับไวรัส (Virus scanning) โดยโปรแกรมป้องกันไวรัสก่อนการรับส่งข้อมูลทุกครั้ง

ข้อ ๙๑ ห้ามใช้เครือข่ายอินเทอร์เน็ตขององค์การ เพื่อกระทำการต่อไปนี้

(๑) หาประโยชน์ในเชิงธุรกิจส่วนตัว

(๒) กระทำการที่ก่อให้เกิดความเสียหายต่อภาพลักษณ์ และชื่อเสียงขององค์การ เช่น การเผยแพร่ข้อมูลที่อาจก่อความเสียหายต่อองค์การ หรือข้อมูลสำคัญที่เป็น ความลับขององค์การ

(๓) กระทำผิดกฎหมาย เช่น

- แพร่กระจายโปรแกรมไม่ประสงค์ดี (Malware) เช่น ไวรัสคอมพิวเตอร์
- กระทำการที่ไม่เหมาะสมขัดต่อศีลธรรม เช่น การเล่นพนันออนไลน์ การนำเข้าหรือเผยแพร่สื่อลามกอนาจาร
- กระทำการที่ส่งผลร้าย กระทบกับความมั่นคงของชาติ ศาสนา พระมหากษัตริย์ เช่น การก่อการร้าย
- กระทำการข่มขู่คุกคาม หรือละเมิดสิทธิของผู้อื่นให้ได้รับความเสียหาย เช่น การนำเข้าหรือเผยแพร่ภาพ เสียง สื่อผสมภาพและเสียง (Multimedia) ของ ผู้อื่น ทั้งที่เป็นข้อมูลจริง หรือข้อมูลเท็จอันเกิดจากการสร้าง ตัดต่อ แต่งเติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ที่ทำให้ผู้อื่นนั้นเสีย ชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย
- กระทำการเป็นภัยต่อสังคม เช่น การนำเข้าหรือเผยแพร่ ข้อมูลที่มีลักษณะอันเป็นเท็จเพื่อสร้างความสับสนวุ่นวาย หรือเพื่อการหลอกลวงให้เกิดความเสียหายต่างๆ

ข้อ ๙๒ ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของหน่วยงานที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต (Internet)

ข้อ ๙๓ ในการใช้งานระบบเครือข่ายอินเทอร์เน็ตไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของหน่วยงาน

ข้อ ๙๔ ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ไม่เสนอความคิดเห็น หรือใช้ข้อความที่ยั่วยุให้ร้ายที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของหน่วยงาน การทำลายความสัมพันธ์กับบุคลากรของหน่วยงานอื่นๆ

ข้อ ๙๕ ผู้ใช้งานไม่นำเข้าข้อมูลคอมพิวเตอร์ใดๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิด เกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามก และไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเทอร์เน็ต

ข้อ ๙๖ หลังจากใช้งานระบบอินเทอร์เน็ต (Internet) เสร็จแล้วให้ปิดเว็บเบราเซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่นๆ

ข้อ ๙๗ หลังจากใช้งานอินเทอร์เน็ตเสร็จแล้วให้ทำการออกจากระบบเพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่นๆ

ข้อ ๙๘ ผู้ใช้งานต้องปฏิบัติตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และ/หรือ กฎหมาย ระเบียบ วิธีปฏิบัติทางคอมพิวเตอร์อื่นๆ ที่เกี่ยวข้องอย่างเคร่งครัด

ส่วนที่ ๑๔ การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล

ข้อ ๙๙ แนวทางปฏิบัติการใช้งานทั่วไป

(๑) เครื่องคอมพิวเตอร์ที่หน่วยงานอนุญาตให้ใช้งาน เป็นสินทรัพย์ของหน่วยงานเพื่อใช้ในงานราชการ

(๒) ไม่อนุญาตให้ผู้ใช้งานทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ส่วนบุคคลของหน่วยงาน

(๓) การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ส่วนบุคคลตรวจซ่อมจะต้องดำเนินการ โดยเจ้าหน้าที่ของหน่วยงานหรือผู้รับจ้างเหมาบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้ทำสัญญากับหน่วยงานเท่านั้น

(๔) ก่อนการใช้งานสื่อบันทึกพกพาต่างๆ ต้องมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัส

(๕) ผู้ใช้งาน มีหน้าที่และรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์

ข้อ ๑๐๐ การใช้รหัสผ่าน ให้ผู้ใช้งานปฏิบัติตามแนวทาง “การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน” ที่ระบุไว้ในเอกสารส่วนที่ ๓

ข้อ ๑๐๑ การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)

(๑) ผู้ใช้งานต้องตรวจสอบหาไวรัสจากสื่อต่างๆ เช่น Floppy Disk, Flash Drive และ Data Storage อื่นๆ ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์

(๒) ผู้ใช้งานต้องตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัสก่อนใช้งาน

(๓) ผู้ใช้งานต้องตรวจสอบข้อมูลคอมพิวเตอร์ใดที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ซึ่งมีผลทำให้ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

(๔) อุปกรณ์สื่อบันทึกข้อมูลที่ไม่ใช้งานแล้วต้องทำลายตามวิธีการที่กำหนดไว้ในส่วนที่ ๔ ข้อ ๓๗

ข้อ ๑๐๒ การสำรองข้อมูลและการกู้คืน

(๑) ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ ไว้บนสื่อบันทึกอื่นๆ เช่น CD, DVD, External Hard Disk เป็นต้น

(๒) ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

(๓) ผู้ใช้งานต้องประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้บน Hard Disk ไม่ควรจะเป็นข้อมูลสำคัญเกี่ยวข้องกับการทำงาน เพราะหาก Hard Disk เสียไป ก็ไม่กระทบต่อการดำเนินการของหน่วยงาน

ส่วนที่ ๑๕ การใช้งานเครื่องคอมพิวเตอร์แบบพกพา

ข้อ ๑๐๓ แนวทางปฏิบัติการใช้งานทั่วไป

(๑) เครื่องคอมพิวเตอร์แบบพกพาที่หน่วยงานอนุญาตให้ใช้งาน เป็นสินทรัพย์ของหน่วยงาน เพื่อใช้ในงานราชการ

(๒) ผู้ใช้งานต้องศึกษาและปฏิบัติตามคู่มือการใช้งานอย่างละเอียด เพื่อการใช้งานอย่างปลอดภัยและมีประสิทธิภาพ

(๓) ไม่ดัดแปลงแก้ไขส่วนประกอบต่างๆ ของคอมพิวเตอร์ และรักษาสภาพของคอมพิวเตอร์ ให้มีสภาพเดิม

(๔) ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพา ควรใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์ แบบพกพา เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน เช่น การตกจากโต๊ะทำงาน หรือหลุดมือ เป็นต้น

(๕) หลีกเลี่ยงการใช้นิ้วหรือของแข็ง เช่น ปลายปากกา กดสัมผัสหน้าจอ LCD ให้เป็นรอยขีดข่วนหรือทำให้จอ LCD ของเครื่องคอมพิวเตอร์แบบพกพาแตกเสียหายได้

(๖) ไม่วางของทับบนหน้าจอและแป้นพิมพ์

(๗) การเช็ดทำความสะอาดหน้าจอภาพต้องเช็ดอย่างเบามือที่สุด และต้องเช็ดไปในแนวทางเดียวกันห้ามเช็ดแบบหมุนวน เพราะจะทำให้หน้าจอมีรอยขีดข่วนได้

(๘) การใช้เครื่องคอมพิวเตอร์แบบพกพาเป็นระยะเวลานานเกินไป ในสภาพที่มีอากาศร้อนจัด ต้องปิดเครื่องคอมพิวเตอร์ เพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง

(๙) การเคลื่อนย้ายเครื่องขณะที่เครื่องเปิดใช้งานอยู่ ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น

ข้อ ๑๐๔ ความปลอดภัยทางด้านกายภาพ

(๑) ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย เช่น ควรล็อคเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

(๒) ผู้ใช้งานไม่เก็บหรือใช้งานคอมพิวเตอร์ แบบพกพาในสถานที่ที่มีความร้อน/ความชื้น/ฝุ่นละอองสูงและต้องระวังป้องกันการตกกระทบ

ส่วนที่ ๑๖ การตรวจจับการบุกรุก (Intrusion Detection System/Intrusion Prevention System Policy : IDS/IPS)

ข้อ ๑๐๕ IDS/IPS Policy ครอบคลุมทุกโฮสต์ (Host) ในเครือข่ายของหน่วยงานและเครือข่ายข้อมูลทั้งหมด รวมถึงเส้นทางที่ข้อมูลอาจเดินทาง ซึ่งไม่อยู่ในเครือข่ายอินเทอร์เน็ตทุกเส้นทาง

ข้อ ๑๐๖ ระบบทั้งหมดที่สามารถเข้าถึงได้จากอินเทอร์เน็ตหรือที่สาธารณะจะต้องผ่านการตรวจสอบจากระบบ IDS/IPS

ข้อ ๑๐๗ โฮสต์ (Host) และเครือข่ายทั้งหมดที่มีการส่งผ่านข้อมูลผ่าน IDS/IPS จะต้องมีการบันทึกผลการตรวจสอบ

ข้อ ๑๐๘ ต้องมีการตรวจสอบเหตุการณ์ข้อมูลจราจร พฤติกรรมการใช้งาน กิจกรรม และบันทึก ปริมาณข้อมูลเข้าใช้งานเครือข่ายเป็นประจำทุกวันโดยผู้ดูแลระบบ

ข้อ ๑๐๙ IDS/IPS จะทำงานภายใต้กฎควบคุมพื้นฐานของ Firewall ที่ใช้ในการเข้าถึงเครือข่ายของระบบสารสนเทศตามปกติ

ข้อ ๑๑๐ จะต้องรายงานพฤติกรรมการใช้งานกิจกรรม หรือเหตุการณ์ทั้งหมดที่มีความเสี่ยงต่อการบุกรุก การโจมตีระบบ พฤติกรรมที่น่าสงสัย หรือการพยายามเข้าระบบ ทั้งที่ประสบความสำเร็จและไม่ประสบความสำเร็จให้ผู้บริหารระดับสูงหรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่ทราบทันทีที่ตรวจพบ

ข้อ ๑๑๑ หน่วยงานมีสิทธิ์ในการยุติการเชื่อมต่อเครือข่ายของเครื่องคอมพิวเตอร์ที่มีพฤติกรรมเสี่ยงต่อการบุกรุกระบบ โดยไม่ต้องมีการแจ้งแก่ผู้ใช้งานล่วงหน้า

ข้อ ๑๑๒ ผู้ที่ถูกตรวจสอบว่าพยายามกระทำการอันใดที่เป็นการละเมิดนโยบายของกระทรวงสาธารณสุข การพยายามเข้าถึงระบบโดยมิชอบ การโจมตีระบบหรือมีพฤติกรรมเสี่ยงต่อการทำงานของระบบสารสนเทศ จะถูกระงับการใช้เครือข่ายทันที หากการกระทำดังกล่าวเป็นการกระทำความผิดที่สอดคล้องกับกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ หรือเป็นการกระทำที่ส่งผลให้เกิดความเสียหายต่อข้อมูลและทรัพยากรระบบของหน่วยงานจะต้องถูกดำเนินคดีตามขั้นตอนของกฎหมาย

ส่วนที่ ๑๗ การติดตั้งและกำหนดค่าของระบบ (System Installation and Configuration)

ข้อ ๑๑๓ การปรับปรุงระบบปฏิบัติการ (Operating System Update)

(๑) ตรวจสอบเครื่องแม่ข่ายและอุปกรณ์ระบบ

(๒) ติดตั้งระบบปฏิบัติการตรงตามความต้องการการใช้งาน

(๓) กำหนดชื่อและรหัสผ่าน ผู้ดูแลระบบ และชื่อผู้ใช้งาน (User)

(๔) กำหนดค่าติดตั้งชื่อเครื่อง (Computer Name) / IP Address

(๕) ปรับปรุง/กำหนดค่าระดับความปลอดภัยของระบบปฏิบัติการ (กรณีที่ระบบปฏิบัติการที่มี Service Patch Update)

(๖) ติดตั้งโปรแกรม Antivirus/ปรับปรุง Virus Definition และกำหนดค่าการตรวจสอบระบบการสแกนและปรับปรุงโปรแกรม

ข้อ ๑๑๔ การบริหารบัญชีผู้ใช้งาน/สิทธิ์การเข้าถึงและการใช้งานระบบ (User Account Management)

(๑) กำหนดชื่อและรหัสผ่านของผู้ดูแลระบบ (System Adminstrator)

(๒) กำหนดชื่อผู้ใช้งาน (User Name) และรหัสผ่าน (Password)

(๓) บันทึกบัญชีผู้ใช้งานและสิทธิการเข้าใช้ระบบ

ข้อ ๑๑๕ การปรับปรุงการรักษาความปลอดภัย/Anti Virus (System Security & Antivirus update)

(๑) ติดตาม เฝ้าระวัง ระบบการทำงานของคอมพิวเตอร์ การเข้าใช้ระบบ

(๒) Performance ของระบบ หรือตรวจสอบจากระบบรักษาความปลอดภัยที่ติดตั้ง

(๓) ปรับปรุง/กำหนดค่าระบบความปลอดภัยให้เหมาะสมกับปัญหา

(๔) ปรับปรุงโปรแกรม Antivirus และ Definition ให้ทันสมัยเป็นประจำทุกสัปดาห์

(๕) ดำเนินการ Scan ตรวจหาไวรัสคอมพิวเตอร์ เป็นประจำ

ข้อ ๑๑๖ ติดตั้ง/ปรับปรุงระบบจัดการฐานข้อมูล (Database Management Operation)

(๑) ติดตั้งระบบจัดการฐานข้อมูลตามความต้องการของระบบสารสนเทศ

(๒) กำหนดค่าระบบหรือโปรแกรมฐานข้อมูล ให้ทำงานร่วมกับระบบปฏิบัติการได้อย่างถูกต้องและมีประสิทธิภาพตามข้อกำหนดของระบบฐานข้อมูล

(๓) สร้าง และกำหนดรายชื่อผู้บริหารระบบฐานข้อมูล (Database Admin) ชื่อผู้ใช้งานอื่นและสิทธิ์การใช้

(๔) ปรับปรุง/กำหนดค่าระบบให้เหมาะสม ทันสมัย หรือป้องกันการเกิดปัญหาเป็นประจำ

ข้อ ๑๑๗ ติดตั้งฐานข้อมูลโปรแกรมระบบงานต่างๆ/กำหนดค่าระบบของโปรแกรมและกำหนดผู้ใช้และสิทธิ์การเข้าใช้บริการ หรือเข้าถึงฐานข้อมูล

(๑) ติดตั้งโปรแกรมระบบงานตามความต้องการหรือการพัฒนา

(๒) กำหนดค่า หรือโปรแกรม หรือบริการให้ทำงานร่วมกับระบบปฏิบัติการ เป็นไปตามโปรแกรมหรือระบบงานนั้นอย่างถูกต้องและมีประสิทธิภาพ

(๓) ติดตั้งฐานข้อมูลและเชื่อมต่อระบบงาน และทำการทดสอบการให้บริการตามระบบงานนั้นกำหนด

(๔) แจ้งผู้ใช้งาน หรือเจ้าของระบบงาน โดยแจ้งรายชื่อ รหัสผ่าน และสิทธิ์การเข้าใช้ระบบและฐานข้อมูลตามที่กำหนดไว้

(๕) กำหนดเกณฑ์การสำรอง/สำเนา/ทดสอบกู้คืน (Restore Test)

(๖) บันทึกข้อกำหนด ค่าติดตั้ง และบัญชีชื่อผู้ใช้งานแต่ละระดับของระบบทุกครั้งที่มีการสร้าง/ปรับปรุง

ส่วนที่ ๑๘ การจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log)

ข้อ ๑๑๘ จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วนถูกต้อง แท้จริง ระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้ และข้อมูลที่ใช้ในการจัดเก็บ ต้องกำหนดชั้นความลับในการเข้าถึง

ข้อ ๑๑๙ ห้ามแก้ไขข้อมูลจราจรคอมพิวเตอร์ (Log) ที่เก็บรักษาไว้

ข้อ ๑๒๐ กำหนดให้มีการบันทึกการทำงานของระบบบันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้า–ออกระบบ บันทึกการพยายามเข้าสู่ระบบ เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกไว้อย่างน้อย ๙๐ วัน นับตั้งแต่การใช้งานสิ้นสุดลง โดยปฏิบัติตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

ข้อ ๑๒๑ ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่างๆ และจำกัดสิทธิ์การเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

หมวดที่ ๒
การรักษาความปลอดภัยด้านข้อมูลและสำรองข้อมูล

วัตถุประสงค์

๑. เพื่อให้ระบบสารสนเทศของหน่วยงานสามารถให้บริการได้อย่างต่อเนื่อง

๒. เพื่อให้เป็นมาตรฐานแนวทางปฏิบัติและความรับผิดชอบของผู้ดูแลระบบในการปฏิบัติงานให้กับหน่วยงานอย่างเคร่งครัดและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย

๓. เพื่อให้ผู้ใช้งานได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

แนวปฏิบัติ

ส่วนที่ ๑ การรักษาความปลอดภัยฐานข้อมูล

ข้อ ๑ กำหนดสิทธิ์และความสำคัญของข้อมูลและฐานข้อมูล

(๑) จัดทำบัญชีฐานข้อมูล การจำแนกกลุ่มทรัพยากรของระบบหรือการทำงาน โดยให้กำหนดกลุ่มผู้ใช้งานและสิทธิของกลุ่มผู้ใช้งาน

(๒) กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ์ หรือการมอบอำนาจ ดังนี้

(๒.๑) กำหนดสิทธิ์ของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง

- อ่านอย่างเดียว
- สร้างข้อมูล
- ป้อนข้อมูล
- แก้ไข
- อนุมัติ
- ไม่มีสิทธิ์

(๒.๒) กำหนดเกณฑ์การระงับสิทธิ์มีการมอบอำนาจ ให้เป็นไปตามการบริหารจัดการการเข้าของผู้ใช้งาน (User Access Management) ที่ได้กำหนดไว้

(๒.๓) ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของหน่วยงานจะต้องขออนุญาต เป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาตจากหัวหน้าหน่วยงานหรือ ผู้ดูแลระบบที่ได้รับมอบหมาย

(๓) ขั้นตอนปฏิบัติเพื่อการจัดเก็บข้อมูล

(๓.๑) จัดแบ่งประเภทของข้อมูล ออกเป็น

- ข้อมูลสารสนเทศด้านการบริหาร เช่น ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์และคำรับรอง ข้อมูลบุคลากร ข้อมูลงบประมาณการเงินและบัญชี เป็นต้น
- ข้อมูลสารสนเทศด้านการแพทย์ที่ให้บริการ เช่น ข้อมูลผู้ป่วย ข้อมูลยาและ เวชภัณฑ์ ข้อมูลสถานพยาบาล เป็นต้น

(๓.๒) จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น ๓ ระดับ คือ

- ข้อมูลที่มีระดับความสำคัญมากที่สุด
- ข้อมูลที่มีระดับความสำคัญปานกลาง
- ข้อมูลที่มีระดับความสำคัญน้อย

(๓.๓) จัดแบ่งลำดับชั้นความลับของข้อมูล

- ข้อมูลลับที่สุด หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด
- ข้อมูลลับมาก หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้ เกิดความเสียหายอย่างร้ายแรง
- ข้อมูลลับ หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย
- ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร ทั่วไปได้

(๓.๔) จัดแบ่งระดับชั้นการเข้าถึง

- ระดับชั้นสำหรับผู้บริหาร
- ระดับชั้นสำหรับผู้ใช้งานทั่วไป
- ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย

(๓.๕) การกำหนดเวลาที่ได้เข้าถึง

(๓.๖) การกำหนดจำนวนช่องทางที่สามารถเข้าถึง

ข้อ ๒ ข้อมูลข่าวสาร สารสนเทศทุกประเภทในฐานข้อมูลต้องได้รับการจัดระดับการป้องกันผู้มีสิทธิ์เข้าใช้หรือดำเนินการ รวมทั้งรายละเอียดอื่นๆ ที่จำเป็นต่อมาตรการรักษาความปลอดภัย

ข้อ ๓ การปฏิบัติเกี่ยวกับข้อมูลที่เป็นความลับให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ และแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ หมวดที่ ๑ ข้อ ๑๒

ข้อ ๔ หน่วยงานเจ้าของฐานข้อมูล ผู้มีสิทธิ์และอำนาจในสายงาน เป็นผู้พิจารณาคุณสมบัติของผู้ใช้งานและโปรแกรมที่ได้รับอนุญาตให้กระทำการใดๆ กับข้อมูลนั้นได้ตามสิทธิและจัดให้มีแฟ้มลงบันทึกเข้าออก (Log File) การใช้งานสำหรับฐานข้อมูลตามความจำเป็น เพื่อประโยชน์ ในการตรวจสอบความถูกต้องของการใช้งานฐานข้อมูล

ส่วนที่ ๒ การสำรองข้อมูล

ข้อ ๕ พิจารณาคัดเลือกระบบสารสนเทศที่สำคัญและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน โดยเรียงลำดับความจำเป็นมากไปน้อย

ข้อ ๖ กำหนดหน้าที่และความรับผิดชอบของเจ้าหน้าที่ในการสำรองข้อมูล

ข้อ ๗ มีการจัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของหน่วยงาน พร้อมทั้งกำหนดระบบสารสนเทศที่จะจัดทำระบบสำรอง และจัดทำระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๘ มีการทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๙ ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

ข้อ ๑๐ ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง หรือตามความเหมาะสมโดยคำนึงถึงความเสี่ยงต่างๆ ที่จะเกิดขึ้น เพื่อให้ระบบมีสภาพพร้อมใช้งานอยู่เสมอ

ข้อ ๑๑ มีการทบทวนระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉิน ที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน อย่างน้อยปีละ ๑ ครั้ง

หมวดที่ ๓
การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

วัตถุประสงค์

๑. เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศหรือสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดได้

๒. เพื่อเป็นการป้องกันและลดระดับความเสี่ยงที่อาจจะเกิดขึ้นได้กับระบบสารสนเทศ

๓. เพื่อเป็นแนวทางในการปฏิบัติหากเกิดความเสี่ยงที่เป็นอันตรายต่อระบบสารสนเทศ

แนวปฏิบัติ

ส่วนที่ ๑ การตรวจสอบและประเมินความเสี่ยง

ข้อ ๑ จัดลำดับความสำคัญของความเสี่ยง

ข้อ ๒ ค้นหาวิธีการดำเนินการเพื่อลดความเสี่ยง

ข้อ ๓ ศึกษาข้อดีข้อเสียของวิธีการดำเนินการเพื่อลดความเสี่ยง

ข้อ ๔ สรุปผลข้อเสนอแนะและแนวทางแก้ไขเพื่อลดความเสี่ยงที่ตรวจสอบได้

ข้อ ๕ มีการตรวจสอบและประเมินความเสี่ยงและให้จัดทำรายงานพร้อมข้อเสนอแนะ

ข้อ ๖ มีมาตรการในการตรวจประเมินระบบสารสนเทศ อย่างน้อย ดังนี้

(๑) กำหนดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้แบบอ่านได้อย่างเดียว

(๒) ในกรณีที่จำเป็นต้องเข้าถึงข้อมูลในแบบอื่นๆ ให้สร้างสำเนาสำหรับข้อมูลนั้น เพื่อให้ผู้ตรวจสอบใช้งาน รวมทั้งต้องทำลายหรือลบโดยทันทีที่ตรวจสอบเสร็จ หรือต้องจัดเก็บไว้โดยมีการป้องกันเป็นอย่างดี

(๓) กำหนดให้มีการระบุและจัดสรรทรัพยากรที่จำเป็นต้องใช้ในการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย

(๔) กำหนดให้มีการเฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้งบันทึกข้อมูลล็อก แสดงการเข้าถึงนั้น ซึ่งรวมถึงวันและเวลาที่เข้าถึงระบบงานที่สำคัญๆ

(๕) ในกรณีที่มีเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ กำหนดให้แยกการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบ ออกจากระบบให้บริการจริงหรือระบบที่ใช้ในการพัฒนาและมีการจัดเก็บป้องกันเครื่องมือนั้นจากการเข้าถึงโดยไม่ได้รับอนุญาต

ส่วนที่ ๒ ความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศ

จากการติดตามตรวจสอบความเสี่ยงต่างๆ รวมถึงเหตุการณ์ด้านความมั่นคงปลอดภัยในระบบ เทคโนโลยีสารสนเทศ สามารถแยกเป็นภัยต่างๆ ได้ ๔ ประเภท ดังนี้

ประเภทที่ ๑ ภัยที่เกิดจากเจ้าหน้าที่หรือบุคลากรของหน่วยงาน (Human Error) เช่น เจ้าหน้าที่หรือบุคลากรของหน่วยงานขาดความรู้ความเข้าใจในเครื่องมืออุปกรณ์คอมพิวเตอร์ทั้งด้าน Hardware และ Software ซึ่งอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหาย ใช้งานไม่ได้ เกิดการชะงักงัน หรือหยุดทำงาน และส่งผลให้ไม่สามารถใช้งานระบบเทคโนโลยีสารสนเทศได้อย่างเต็มประสิทธิภาพ ได้กำหนดแนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ ไว้ดังนี้

(๑) จัดหลักสูตรอบรมเจ้าหน้าที่ของหน่วยงาน ให้มีความรู้ความเข้าใจในด้าน Hardware และ Software เบื้องต้น เพื่อลดความเสี่ยงด้าน Human error ให้น้อยที่สุด ทำให้เจ้าหน้าที่มีความรู้ความเข้าใจการใช้และบริหารจัดการเครื่องมืออุปกรณ์ทางด้านสารสนเทศ ทั้งทางด้าน Hardware และ Software ได้มีประสิทธิภาพยิ่งขึ้น ทำให้ความเสี่ยงที่เกิดจาก Human error ลดน้อยลง

ประเภทที่ ๒ ภัยที่เกิดจาก Software ที่สร้างความเสียหายให้แก่เครื่องคอมพิวเตอร์หรือ ระบบเครือข่ายคอมพิวเตอร์ประกอบด้วย ไวรัสคอมพิวเตอร์ (Computer Virus) หนอนอินเทอร์เน็ต (Internet Worm) ม้าโทรจัน (Trojan Horse) และข่าวไวรัสหลอกลวง (Hoax) พวก Software เหล่านี้อาจรบกวนการทำงาน และก่อให้เกิดความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศ ถึงขั้นทำให้ระบบเครือข่าย คอมพิวเตอร์ใช้งานไม่ได้ ได้กำหนดแนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ภัยจาก Software ดังนี้

(๑) ติดตั้ง Firewall ที่เครื่องคอมพิวเตอร์แม่ข่าย ทำหน้าที่ในการกำหนดสิทธิ์การเข้าใช้งานเครื่องคอมพิวเตอร์แม่ข่าย และป้องกันการบุกรุกจากภายนอก

(๒) ติดตั้งซอฟต์แวร์ Anti virus ดักจับไวรัสที่เข้ามาในระบบเครือข่าย และสามารถตรวจสอบได้ว่ามีไวรัสชนิดใดเข้ามาทำความเสียหายกับระบบเครือข่ายคอมพิวเตอร์

ประเภทที่ ๓ ภัยจากไฟไหม้หรือระบบไฟฟ้า จัดเป็นภัยร้ายแรงที่ทำความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศ ได้กำหนดแนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ ดังนี้

(๑) ติดตั้งอุปกรณ์สำรองไฟฟ้า (UPS) เพื่อควบคุมการจ่ายกระแสไฟฟ้าให้กับระบบเครื่องแม่ข่าย (Server) ในกรณีเกิดกระแสไฟฟ้าขัดข้อง ระบบเครือข่ายคอมพิวเตอร์จะสามารถให้บริการได้ในระยะเวลาที่สามารถจัดเก็บและสำรองข้อมูลไว้อย่างปลอดภัย

(๒) ติดตั้งอุปกรณ์ตรวจจับควัน กรณีที่เกิดเหตุการณ์กระแสไฟฟ้าขัดข้องหรือมีควันไฟ เกิดขึ้นภายในห้องควบคุมระบบเครือข่าย อุปกรณ์ดังกล่าวจะส่งสัญญาณแจ้งเตือนที่ หน่วยรักษาความปลอดภัยเพื่อทราบ และรีบเข้ามาระงับเหตุฉุกเฉินอย่างทันท่วงที ซึ่งมีการตรวจสอบความพร้อมของอุปกรณ์อย่างสม่ำเสมอ

(๓) ติดตั้งอุปกรณ์ดับเพลิงชนิดก๊าซ ที่ห้องควบคุมระบบคอมพิวเตอร์เพื่อไว้ใช้ในกรณีเหตุฉุกเฉิน (ไฟไหม้) โดยมีการตรวจสอบความพร้อมของอุปกรณ์และทดลองใช้งานโดยสม่ำเสมอ

ประเภทที่ ๔ ภัยจากน้ำท่วม (อุทกภัย) ความเสี่ยงต่อความเสียหายจากน้ำท่วม จัดเป็นภัยร้ายแรงที่ทำความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศ ได้กำหนดแนวทางปฏิบัติเพื่อเตรียมรับ สถานการณ์ ดังนี้

(๑) เฝ้าระวังภัยอันเกิดจากน้ำท่วมโดยติดตามจากพยากรณ์อากาศของกรมอุตุนิยมวิทยาตลอดเวลา

(๒) ถอดเทป Back up ข้อมูลทั้งหมด ไปเก็บไว้ในที่ปลอดภัย

(๓) ดำเนินการตัดระบบไฟฟ้าในห้องควบคุม โดยปิดเบรคเกอร์เครื่องปรับอากาศ เพื่อป้องกันเครื่องควบคุมเสียหาย และป้องกันภัยจากไฟฟ้า

(๔) เจ้าหน้าที่ช่วยกันเคลื่อนย้ายเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่ายไว้ในที่สูง

(๕) กรณีน้ำลดลงเรียบร้อยแล้วให้ช่างไฟฟ้าตรวจสอบระบบไฟฟ้าในห้องควบคุมเครือข่ายว่าสามารถใช้งานได้ปกติหรือไม่ และเตรียมความพร้อมห้องควบคุมระบบเครือข่าย สำหรับติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย

(๖) ทำการติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย พร้อมทั้งทดสอบการใช้งานของเครื่องคอมพิวเตอร์แม่ข่ายแต่ละเครื่องว่าสามารถให้บริการได้ตามปกติหรือไม่ ตรวจสอบระบบ Network ว่าสามารถเชื่อมต่อและให้บริการกับเครื่องคอมพิวเตอร์ลูกข่ายได้หรือไม่

(๗) เมื่อตรวจสอบแล้วว่าเครื่องคอมพิวเตอร์แม่ข่ายและระบบเครือข่ายสามารถให้บริการข้อมูลได้เรียบร้อยแล้ว แจ้งให้หน่วยงานที่เกี่ยวข้องทราบ เพื่อเข้ามาใช้บริการได้ตามปกติ

หมวดที่ ๔
การรักษาความปลอดภัยด้านกายภาพ สถานที่ และสภาพแวดล้อม

วัตถุประสงค์

เพื่อกำหนดมาตรการในการควบคุมและป้องกันการรักษาความมั่นคงปลอดภัยในการเข้าใช้งานหรือเข้าถึงพื้นที่ใช้งานในระบบสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ ระบบเทคโนโลยีสารสนเทศ ข้อมูลซึ่งมีผลบังคับใช้กับผู้ใช้งานและรวมถึงบุคคล และหน่วยงานภายนอกที่มีส่วนเกี่ยวข้องกับการใช้งาน ระบบเทคโนโลยีสารสนเทศของหน่วยงาน

แนวปฏิบัติ

ข้อ ๑ อาคาร สถานที่ และพื้นที่ใช้งานระบบสารสนเทศ หมายถึง ที่ซึ่งเป็นที่ตั้งของระบบคอมพิวเตอร์ ระบบเครือข่าย หรือระบบสารสนเทศอื่นๆ พื้นที่เตรียมข้อมูลจัดเก็บคอมพิวเตอร์ และอุปกรณ์พื้นที่ปฏิบัติงานของบุคลากรทางคอมพิวเตอร์ รวมทั้งเครื่องคอมพิวเตอร์ ส่วนบุคคลและอุปกรณ์ประกอบที่ ติดตั้งประจำโต๊ะทำงาน

ข้อ ๒ ห้องควบคุมระบบเครือข่ายคอมพิวเตอร์ ต้องมีลักษณะ ดังนี้

(๑) กำหนดเป็นเขตหวงห้ามเด็ดขาด หรือเขตหวงห้ามเฉพาะโดยพิจารณาตาม ความสำคัญแล้วแต่กรณี

(๒) ต้องเป็นพื้นที่ที่ไม่ตั้งอยู่ในบริเวณที่มีการผ่านเข้า–ออก ของบุคคลเป็นจำนวนมาก

(๓) จะต้องไม่มีป้ายหรือสัญลักษณ์ ที่บ่งบอกถึงการมีระบบสำคัญอยู่ภายในสถานที่ดังกล่าว

(๔) จะต้องปิดล็อก หรือใส่กุญแจประตูหน้าต่างหรือห้องเสมอเมื่อไม่มีเจ้าหน้าที่ประจำอยู่

(๕) หากจำเป็นต้องใช้เครื่องโทรสารหรือเครื่องถ่ายเอกสาร ให้ติดตั้งแยกออกมาจากบริเวณดังกล่าว

(๖) ไม่อนุญาตให้ถ่ายรูปหรือบันทึกภาพเคลื่อนไหวในบริเวณดังกล่าว เป็นอันขาด

(๗) จัดพื้นที่สำหรับการส่งมอบผลิตภัณฑ์ โดยแยกจากบริเวณที่มีทรัพยากรสารสนเทศจัดตั้งไว้เพื่อป้องกันการเข้าถึงระบบจากผู้ไม่ได้รับอนุญาต

ข้อ ๓ การกำหนดบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย

(๑) มีการจำแนกและกำหนดพื้นที่ของระบบเทคโนโลยีสารสนเทศต่างๆ อย่างเหมาะสม เพื่อจุดประสงค์ในการเฝ้าระวัง ควบคุม การรักษาความมั่นคงปลอดภัย จากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่นๆ ที่อาจเกิดขึ้นได้

(๒) กำหนดและแบ่งแยกบริเวณพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศให้ชัดเจน รวมทั้ง จัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้รับทราบทั่วกัน โดยการ กำหนดพื้นที่ดังกล่าวอาจแบ่งออกได้เป็นพื้นที่ทำงานทั่วไป (General Working Area) พื้นที่ทำงานของผู้ดูแลระบบ (System Administrator Area) พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศ (IT Equipment Area) พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data Storage Area) และพื้นที่ใช้งานเครือข่ายไร้สาย (Wireless LAN Coverage Area) เป็นต้น

ข้อ ๔ การควบคุมการเข้าออกอาคารสถานที่

(๑) กำหนดสิทธิ์ผู้ใช้งาน ที่มีสิทธิ์ผ่านเข้า-ออก และช่วงเวลาที่มีสิทธิ์ในการผ่านเข้าออกในแต่ละ “พื้นที่ใช้งานระบบ” อย่างชัดเจน

(๒) การเข้าถึงอาคารของหน่วยงาน ของบุคคลภายนอก หรือผู้มาติดต่อ เจ้าหน้าที่รักษาความปลอดภัย จะต้องให้มีการแลกบัตรที่ใช้ระบุตัวตนของบุคคลนั้นๆ เช่น บัตรประชาชน ใบอนุญาตขับขี่ เป็นต้น แล้วทำการลงบันทึกข้อมูลบัตรในสมุดบันทึก และรับแบบฟอร์มการเข้าออกพร้อมกับบัตรผู้ติดต่อ (Visitor) ของหน่วยงาน

(๓) ให้มีการบันทึกวันและเวลาการเข้า-ออกพื้นที่สำคัญของผู้ที่มาติดต่อ (Visitors)

(๔) ผู้มาติดต่อต้องติดบัตรให้เห็นเด่นชัดตลอดระยะเวลาที่อยู่ภายในหน่วยงาน

(๕) บริษัทผู้ได้รับการว่าจ้างต้องติดบัตรให้เห็นเด่นชัดตลอดระยะเวลาการทำงาน

(๖) จัดเก็บบันทึกการเข้า-ออกสำหรับพื้นที่หรือบริเวณที่มีความสำคัญ เช่น (Data Center) เป็นต้น เพื่อใช้ในการตรวจสอบในภายหลังเมื่อมีความจำเป็น

(๗) ดูแลผู้ที่มาติดต่อในพื้นที่หรือบริเวณที่มีความสำคัญจนกระทั่งเสร็จสิ้นภารกิจและจากไป เพื่อป้องกันการสูญหายของทรัพย์สินหรือป้องกันการเข้าถึงทางกายภาพโดย ไม่ได้รับอนุญาต

(๘) มีกลไกการอนุญาตการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญของบุคคลภายนอก และต้องมีเหตุผลที่เพียงพอในการเข้าถึงบริเวณดังกล่าว

(๙) สร้างความตระหนักให้ผู้ที่มาติดต่อจากภายนอกเข้าใจในกฎเกณฑ์หรือข้อกำหนดต่างๆ ที่ต้องปฏิบัติระหว่างที่อยู่ในพื้นที่หรือบริเวณที่มีความสำคัญ

(๑๐) มีการควบคุมการเข้าถึงพื้นที่ที่มีข้อมูลสำคัญจัดเก็บหรือประมวลผลอยู่

(๑๑) ไม่อนุญาตให้ผู้ไม่มีกิจเข้าไปในพื้นที่หรือบริเวณที่มีความสำคัญเว้นแต่ได้รับการอนุญาต

(๑๒) มีการพิสูจน์ตัวตน เช่น การใช้บัตรรูด การใช้รหัสผ่าน เป็นต้น เพื่อควบคุมการเข้า-ออกในพื้นที่หรือบริเวณที่มีความสำคัญ (Data Center)

(๑๓) จัดให้มีการดูแลและเฝ้าระวังการปฏิบัติงานของบุคคลภายนอกในขณะที่ปฏิบัติงานในพื้นที่หรือบริเวณที่มีความสำคัญ

(๑๔) จัดให้มีการทบทวน หรือยกเลิกสิทธิ์การเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญอย่างน้อยปีละ ๑ ครั้ง

ข้อ ๕ ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting Utilities)

(๑) มีระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศของหน่วยงานที่เพียงพอต่อความต้องการใช้งานโดยให้มีระบบดังต่อไปนี้

- ระบบสำรองกระแสไฟฟ้า (UPS)
- เครื่องกำเนิดกระแสไฟฟ้าสำรอง (Generator) (หากมี)
- ระบบระบายอากาศ
- ระบบปรับอากาศ และควบคุมความชื้น

(๒) ให้มีการตรวจสอบหรือทดสอบระบบสนับสนุนเหล่านั้นอย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าระบบทำงานตามปกติ และลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ

(๓) ติดตั้งระบบแจ้งเตือน เพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงานภายในห้องเครื่องทำงานผิดปกติหรือหยุดการทำงาน

ข้อ ๖ การเดินสายไฟ สายสื่อสาร และสายเคเบิ้ลอื่นๆ (Cabling Security)

(๑) หลีกเลี่ยงการเดินสายสัญญาณเครือข่ายของหน่วยงานในลักษณะที่ต้องผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกเข้าถึงได้

(๒) ให้มีการร้อยท่อสายสัญญาณต่างๆ เพื่อป้องกันการดักจับสัญญาณ หรือการตัดสายสัญญาณเพื่อทำให้เกิดความเสียหาย

(๓) ให้เดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซง รบกวนของสัญญาณซึ่งกันและกัน

(๔) ทำป้ายชื่อสำหรับสายสัญญาณและบนอุปกรณ์เพื่อป้องกันการตัดต่อสัญญาณผิดเส้น

(๕) จัดทำผังสายสัญญาณสื่อสารต่างๆ ให้ครบถ้วนและถูกต้อง

(๖) พิจารณาใช้งานสายไฟเบอร์ออฟติก แทนสายสัญญาณสื่อสารแบบเดิม (เช่น สายสัญญาณแบบ Coaxial cable) สำหรับระบบสารสนเทศที่สำคัญ

(๗) ดำเนินการสำรวจระบบสายสัญญาณสื่อสารทั้งหมดเพื่อตรวจหาการติดตั้งอุปกรณ์ดักจับสัญญาณโดยผู้ไม่ประสงค์ดี

ข้อ ๗ การบำรุงรักษาอุปกรณ์ (Equipment Maintenance)

(๑) ให้มีกำหนดการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่แนะนำโดยผู้ผลิต

(๒) ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามที่ผู้ผลิตแนะนำ

(๓) จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้ง เพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง

(๔) จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว

(๕) ควบคุมและสอดส่องดูแลการปฏิบัติงานของผู้ให้บริการภายนอกที่มาทำการบำรุงรักษาอุปกรณ์ภายในหน่วยงาน

(๖) จัดให้มีการอนุมัติสิทธิ์การเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญโดยผู้รับจ้างให้บริการจากภายนอก (ที่มาทำการบำรุงรักษาอุปกรณ์) เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

ข้อ ๘ การนำทรัพย์สินของหน่วยงานออกนอกหน่วยงาน (Removal of Property)

(๑) ให้มีการขออนุญาตก่อนนำอุปกรณ์หรือทรัพย์สินนั้นออกไปใช้งานนอกหน่วยงาน

(๒) กำหนดผู้รับผิดชอบในการเคลื่อนย้ายหรือนำอุปกรณ์ออกนอกหน่วยงาน

(๓) กำหนดระยะเวลาของการนำอุปกรณ์ออกไปใช้งานนอกหน่วยงาน

(๔) เมื่อมีการนำอุปกรณ์ส่งคืนให้ตรวจสอบว่าสอดคล้องกับระยะเวลาที่อนุญาตและตรวจสอบการชำรุดเสียหายของอุปกรณ์ด้วย

(๕) บันทึกข้อมูลการนำอุปกรณ์ของหน่วยงานออกไปใช้งานนอกหน่วยงาน เพื่อเอาไว้เป็นหลักฐานป้องกันการสูญหาย รวมทั้งบันทึกข้อมูลเพิ่มเติมเมื่อนำอุปกรณ์ส่งคืน

ข้อ ๙ การป้องกันอุปกรณ์ที่ใช้งานอยู่นอกหน่วยงาน (Security of Equipment off-premises)

(๑) กำหนดมาตรการความปลอดภัยเพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์หรือทรัพย์สินของหน่วยงานออกไปใช้งาน เช่น การขนส่ง การเกิดอุบัติเหตุกับอุปกรณ์

(๒) ไม่ทิ้งอุปกรณ์หรือทรัพย์สินของหน่วยงานไว้โดยลำพังในที่สาธารณะ

(๓) เจ้าหน้าที่มีความรับผิดชอบดูแลอุปกรณ์หรือทรัพย์สินเสมือนเป็นทรัพย์สินของตนเอง

ข้อ ๑๐ การกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง (Secure Disposal or re-use of Equipment)

(๑) ให้ทำลายข้อมูลสำคัญในอุปกรณ์ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว

(๒) มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้การเข้าถึงข้อมูลสำคัญนั้นได้

หมวดที่ ๕
การดำเนินการตอบสนองเหตุการณ์ ความมั่นคงปลอดภัย ทางระบบสารสนเทศ

วัตถุประสงค์

เพื่อกำหนดมาตรการในการป้องกันการบุกรุกและการโจมตี หรือเหตุการณ์ละเมิดความปลอดภัยระบบสารสนเทศให้มีความมั่นคงปลอดภัย

แนวปฏิบัติ

ข้อ ๑ ระบบป้องกันผู้บุกรุก

(๑) ดำเนินการตรวจสอบ Log File หรือรายงานของระบบป้องกันการบุกรุก สิ่งที่ทำการตรวจสอบ มีดังนี้

- มีการโจมตีมากน้อยเพียงใด และเป็นการโจมตีประเภทใดมากที่สุด
- ลักษณะของการโจมตีที่เกิดขึ้นมีรูปแบบที่สามารถคาดเดาได้หรือไม่
- ระดับความรุนแรงมากน้อยเพียงใด
- หมายเลขไอพีของเครือข่ายที่เป็นผู้โจมตี

ข้อ ๒ ระบบไฟร์วอลล์

(๑) ดำเนินการตรวจระบบป้องกันการบุกรุกอย่างน้อยเดือนละ ๑ ครั้ง

(๒) ดำเนินการตรวจสอบบันทึกของ Log File และรายงานของไฟร์วอลล์ สิ่งที่ต้อง ตรวจสอบ มีดังต่อไปนี้

- Packet ที่ไฟร์วอลล์ได้ทำการ Block
- ลักษณะของ Packet ที่ถูก Block
- Packet ของหมายเลขไอพี ของเครือข่ายใดถูก Block เป็นจำนวนมาก

(๓) กรณีตรวจพบการโจมตีระบบหรือเหตุการณ์ละเมิดความปลอดภัยระบบสารสนเทศให้แจ้งหัวหน้าหน่วยงาน เพื่อตัดสินใจดำเนินการแก้ไขปัญหา

ข้อ ๓ ระบบป้องกันภัยคุกคามทางอินเทอร์เน็ต ภัยคุกคามทางอินเทอร์เน็ตหรือมัลแวร์ (Malware) ประกอบด้วย ไวรัส หนอนอินเทอร์เน็ต โทรจัน รวมถึงสปายแวร์

(๑) ดำเนินการตรวจสอบ Log File และรายงานของอุปกรณ์ที่เกี่ยวข้องกับระบบป้องกันภัยคุกคามทางอินเทอร์เน็ตสิ่งที่ต้องตรวจสอบมีดังนี้

- มัลแวร์ประเภทใดถูกพบเป็นจำนวนมาก
- มัลแวร์ถูกส่งมาจากเครือข่ายใด และถูกส่งไปยังที่ใด
- มีการส่งมัลแวร์ จากเครือข่ายภายในหน่วยงานไปยังภายนอกหรือไม่

(๒) ศึกษาหาวิธีแก้ไขเครื่องคอมพิวเตอร์ ที่ติดมัลแวร์ โดยเฉพาะมัลแวร์ประเภทที่ตรวจพบว่ากระจายอยู่ในเครือข่ายของหน่วยงาน

(๓) ตรวจสอบพบว่าเครื่องคอมพิวเตอร์ ภายในเครือข่ายติดมัลแวร์หรือส่งมัลแวร์ออกไปข้างนอก ต้องระงับการเชื่อมต่อของเครื่องที่ติดมัลแวร์กับระบบเครือข่าย แล้วทำการ แก้ไขเครื่องนั้นทันที

หมวดที่ ๖
การสร้างความตระหนักในเรื่องการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ

วัตถุประสงค์

๑. เพื่อสร้างความรู้ความเข้าใจ ในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์ ให้แก่ผู้ใช้งานของโรงพยาบาล

๒. เพื่อให้การใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์ เกิดความมั่นคงปลอดภัย

๓. เพื่อป้องกันและลดการกระทำความผิดที่เกิดขึ้นจากการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์โดยไม่คาดคิด

แนวปฏิบัติ

ข้อ ๑ จัดให้มีการทบทวน ปรับปรุงนโยบายและแนวปฏิบัติให้เป็นปัจจุบันอยู่เสมอ อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๒ จัดฝึกอบรมแนวปฏิบัติตามแนวนโยบายโดยการจัดฝึกอบรมโดยใช้วิธีการเสริมเนื้อหาแนวปฏิบัติตามแนวนโยบายเข้ากับหลักสูตรอบรมต่างๆ ตามแผนการฝึกอบรมของหน่วยงาน

ข้อ ๓ เผยแพร่ นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และสร้างความตระหนักถึงความสำคัญของการปฏิบัติให้กับบุคลากร โดยการจัดอบรมปีละไม่น้อยกว่า ๑ ครั้ง

ข้อ ๔ ติดประกาศประชาสัมพันธ์ให้ความรู้เกี่ยวกับแนวปฏิบัติในลักษณะเกร็ดความรู้ หรือข้อระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย โดยมีการปรับเปลี่ยนเกร็ดความรู้อยู่เสมอ

ข้อ ๕ ระดมการมีส่วนร่วมและลงสู่ภาคปฏิบัติด้วยการกำกับ ติดตาม ประเมินผล และสำรวจความต้องการของผู้ใช้งาน

ข้อ ๖ ให้มีการสร้างความตระหนักเกี่ยวกับโปรแกรมไม่ประสงค์ดี เพื่อให้เจ้าหน้าที่มีความรู้ความเข้าใจและสามารถป้องกันตนเองได้และให้รับทราบขั้นตอนปฏิบัติเมื่อพบเหตุโปรแกรมไม่ประสงค์ดีว่าต้อง ดำเนินการอย่างไร

ข้อ ๗ สร้างความรู้ความเข้าใจให้แก่ผู้ใช้งานให้ตระหนักถึงเหตุการณ์ด้านความมั่นคงปลอดภัยที่เกิดขึ้นและสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด เพื่อให้ผู้ใช้งานปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของหน่วยงาน

ข้อ ๘ ผู้ใช้งานต้องตระหนักและปฏิบัติตามกฎหมายใดๆ ที่ได้ประกาศใช้ในประเทศไทย รวมทั้ง กฎระเบียบของกระทรวงสาธารณสุข และข้อตกลงระหว่างประเทศอย่างเคร่งครัด ทั้งนี้หากผู้ใช้งานไม่ปฏิบัติตามกฎหมายดังกล่าว ถือว่าความผิดนั้นเป็นความผิดส่วนบุคคลซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

หมวดที่ ๗
หน้าที่และความรับผิดชอบ

วัตถุประสงค์

เพื่อกำหนดหน้าที่ความรับผิดชอบของผู้บริหารระดับสูง ผู้อำนวยการ หัวหน้า เจ้าหน้าที่ ตลอดจนผู้ที่ได้รับมอบหมายให้ดูแลรับผิดชอบด้านสารสนเทศ

แนวปฏิบัติ

ข้อ ๑ ระดับนโยบาย ผู้รับผิดชอบ ได้แก่

- ผู้บริหารระดับสูง (Chief Executive Office: CEO) ของหน่วยงาน
- ผู้อำนวยการหรือเทียบเท่าระดับผู้อำนวยการ

(๑) รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตาม กำกับดูแล ควบคุมตรวจสอบเจ้าหน้าที่ในระดับปฏิบัติ

(๒) รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นกรณีระบบ คอมพิวเตอร์ หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใดๆ แก่หน่วยงานหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ข้อ ๒ ระดับบริหารผู้รับผิดชอบ ได้แก่ หัวหน้าศูนย์คอมพิวเตอร์ หรือเทียบเท่าหัวหน้ากลุ่มงานด้านเทคโนโลยีสารสนเทศ

(๑) รับผิดชอบ กำกับ ดูแลการปฏิบัติงานของผู้ปฏิบัติ ตลอดจนศึกษา ทบทวน วางแผน ติดตามการบริหารความเสี่ยง และระบบรักษาความปลอดภัยฐานข้อมูลและเทคโนโลยีสารสนเทศ

(๒) รับผิดชอบในการควบคุม ดูแล รักษาความปลอดภัยระบบสารสนเทศและระบบฐานข้อมูล

ข้อ ๓ ระดับปฏิบัติ หรือผู้รับผิดชอบ ได้แก่

- ผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่จากหัวหน้าส่วนราชการระดับกรมและระดับหน่วยงานสังกัดกรม เช่น นักวิชาการคอมพิวเตอร์ เจ้าหน้าที่ด้านเทคโนโลยีสารสนเทศ ผู้ปฏิบัติงานด้านสารสนเทศ เป็นต้น

(๑) ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

(๒) ประสานการปฏิบัติงานตามแผนป้องกันและแก้ไขปัญหาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศจากสถานการณ์ ความไม่แน่นอนและภัยพิบัติ

(๓) รับผิดชอบควบคุม ดูแล รักษาความปลอดภัย และบำรุงรักษา ระบบเครื่องคอมพิวเตอร์ ระบบเครือข่าย ห้องควบคุมระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย

(๔) ทำการสำรองข้อมูลและเรียกคืนข้อมูล (Backup and Recovery) ตามรอบระยะเวลาที่กำหนด

(๕) ป้องกันการถูกเจาะระบบ และแก้ไขปัญหาการถูกเจาะเข้าระบบฐานข้อมูลจากบุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาต

(๖) รับผิดชอบในการรักษาความปลอดภัย ระบบอินเทอร์เน็ต

(๗) ปฏิบัติงานอื่นๆ ตามที่ได้รับมอบหมายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของโรงพยาบาล

หมวดที่ ๘
การบริหารจัดการการใช้บริการจากหน่วยงานภายนอก

วัตถุประสงค์

เพื่อให้หน่วยงานภายนอก ได้ปฏิบัติตามนโยบายรักษาความมั่นคงปลอดภัยด้านสารสนเทศของโรงพยาบาล ทำให้ระบบสารสนเทศดำเนินไปได้อย่างต่อเนื่องและมีประสิทธิภาพ

แนวปฏิบัติ

ข้อ ๑ มีการประเมินความเสี่ยงจากการเข้าถึง ข้อมูล และระบบสารสนเทศ หรืออุปกรณ์ที่ใช้ในการประมวลผลโดยหน่วยงานภายนอก และกำหนดมาตรการควบคุมที่เหมาะสมก่อนที่จะอนุญาตให้เข้าถึงข้อมูล และระบบสารสนเทศ หรืออุปกรณ์ดังกล่าวได้

ข้อ ๒ การเข้าใช้งานระบบสารสนเทศ หรือเข้าถึงข้อมูลของหน่วยงานจากหน่วยงานภายนอกต้องมีการขออนุญาตอย่างเป็นทางการ และได้รับอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบที่ได้รับมอบหมายก่อนเสมอ

ข้อ ๓ การบริการ และการดำเนินงานจากหน่วยงานภายนอก จะต้องปฏิบัติตามนโยบายการรักษา ความมั่นคงปลอดภัยด้านสารสนเทศ แนวทางการปฏิบัติงาน มาตรฐาน และกฎข้อบังคับต่างๆ ของหน่วยงาน

ข้อ ๔ ผู้ดูแลระบบต้องให้สิทธิ์การเข้าถึงข้อมูลต่อหน่วยงานภายนอกเท่าที่จำเป็นเท่านั้น

ข้อ ๕ ต้องมีการทำสัญญาการรักษาความลับขององค์กร ระหว่างหน่วยงานและหน่วยงานภายนอกที่เข้ามาปฏิบัติงานก่อนเปิดให้ใช้บริการระบบเสมอ

ข้อ ๖ ผู้ให้บริการหน่วยงานภายนอก ต้องจัดทำแผนการดำเนินงาน และวิธีการดำเนินงาน เป็นอย่างน้อย เพื่อควบคุมหรือตรวจสอบการให้บริการของผู้ให้บริการให้เป็นไปอย่างถูกต้อง มั่นคงปลอดภัย และเป็นไปตามขอบเขต ที่ได้กำหนดไว้

ข้อ ๗ สัญญาระหว่างหน่วยงาน และหน่วยงานภายนอก ในการให้บริการต้องระบุถึงหัวข้อต่างๆ ดังต่อไปนี้ เป็นอย่างน้อย

- รายละเอียดการให้บริการ แผนการดำเนินงาน วิธีการดำเนินงาน และสิ่งที่ต้องส่งมอบ
- ระดับการให้บริการ (Service Level)
- หน้าที่และความรับผิดชอบขององค์การและหน่วยงานภายนอก ในการให้บริการในครั้งนี้
- ระยะเวลาในการให้บริการ และการตรวจรับงานบริการในครั้งนี้
- ราคา และเงื่อนไขการชำระเงิน
- ความเป็นเจ้าของและลิขสิทธิ์ของอุปกรณ์ ฮาร์ดแวร์ หรือซอฟต์แวร์ ที่ทำการจัดซื้อหรือพัฒนาขึ้น (ถ้ามี)
- การรักษาความลับของข้อมูลที่ได้รับจากการให้บริการแก่องค์การ

เอกสารอ้างอิง

๑. แนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศกรมการแพทย์ ปี ๒๕๖๖ สำนักดิจิทัลการแพทย์ กรมการแพทย์