สภากาชาดไทย
The Thai Red Cross Society

โรงพยาบาลสมเด็จพระบรมราชเทวี ณ ศรีราชา สภากาชาดไทย

(Queen Savang Vadhana Memorial Hospital)

ประเภท : (Document Type)	Hospital Policy (HP)	วันที่ประกาศใช้เอกสาร : (Issue Date) :	24 ก.พ. 2565
ฝ่าย : (Department)	ฝ่ายเทคโนโลยีสารสนเทศ	วันที่บังคับใช้เอกสาร : (Effective Date) :	- 4 มี.ค. 2565
หมายเลขเอกสาร : (Document No.)	HP-MOI-QSH-006	ครั้งที่แก้ไข : (Revision) :	01
เรื่อง : (Subject)	นโยบายและแนวปฏิบัติความมั่นคงปลอดภัยด้านสารสนเทศ		
ผู้เกี่ยวข้องที่ต้องรับทราบ :	เจ้าหน้าที่ปฏิบัติงานในโรงพยาบาล		

	ชื่อ – สกุล	ลายมือชื่อ	วัน/เดือน/ปี
จัดทำโดย : ตำแหน่ง :	นายธนนัฏฐ์ เกษาประสิทธิ์ หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ		18 ก.พ. 2565
ทบทวนโดย : ตำแหน่ง :	นายแพทย์วิทยา โชคชัยไพศาล ผู้ช่วยผู้อำนวยการ		18 ก.พ. 2565
อนุมัติโดย : ตำแหน่ง :	นายแพทย์ธเนศ จัดวัฒนกุล รองผู้อำนวยการ		21 ก.พ. 2565
อนุมัติโดย : ตำแหน่ง :	รองศาสตราจารย์ นายแพทย์โศภณ นภาธร ผู้อำนวยการ		22 ก.พ. 2565

เอกสารควบคุม

โรงพยาบาลสมเด็จพระบรมราชเทวี ณ ศรีราชา

สภากาชาดไทย

นโยบายและแนวปฏิบัติ

ความมั่นคงปลอดภัยด้านสารสนเทศ

คำนำ

ปัจจุบันมีการนำเทคโนโลยีสารสนเทศและการสื่อสารมาใช้เป็นเครื่องมือสำคัญกันอย่างแพร่หลายมากขึ้นในการให้ได้มาซึ่งข้อมูลสารสนเทศที่เป็นประโยชน์ต่อการดำเนินชีวิตของประชาชน การบริหารและการตัดสินใจในการดำเนินภารกิจภาครัฐและธุรกิจภาคเอกชนรวมถึงการนำสารสนเทศมาใช้ในการกำหนดนโยบาย และการพัฒนาประเทศ ขณะเดียวกันปัญหาความไม่น่าเชื่อถือของสารสนเทศอันเนื่องมาจากความไม่ทันสมัย ความไม่ถูกต้องครบถ้วนเพียงพอที่จะนำไปใช้ก็มักจะเกิดขึ้นตามมาเสมอและปัญหาที่มีความสำคัญอย่างยิ่งซึ่งขณะนี้ได้ทวีความรุนแรงเพิ่มขึ้นทั้งในและต่างประเทศ คือปัญหาด้านการรักษาความมั่นคงปลอดภัยให้กับสารสนเทศ เนื่องจากได้ส่งผลกระทบทำให้ผู้ประกอบการ องค์กรภาครัฐและภาคเอกชนที่มีการดำเนินงานใด ๆ ในรูปแบบของข้อมูลอิเล็กทรอนิกส์ผ่านระบบสารสนเทศขององค์กรขาดความเชื่อมั่นต่อการทำธุรกรรมทางอิเล็กทรอนิกส์ในทุกรูปแบบ ดังนั้น กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารโดยคณะอนุกรรมการความมั่นคงปลอดภัยภายใต้ คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์จึงได้จัดทำประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ ขึ้น เพื่อเป็นแนวทางให้หน่วยงานของภาครัฐได้ใช้จัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคง ปลอดภัยด้านสารสนเทศ เพื่อช่วยให้การดำเนินกิจกรรมหรือการให้บริการต่าง ๆ ของหน่วยงานภาครัฐ มีความมั่นคงปลอดภัยและมีความน่าเชื่อถือมากยิ่งขึ้น

ฝ่ายเทคโนโลยีสารสนเทศ โรงพยาบาลสมเด็จพระบรมราชเทวี ณ ศรีราชา จึงได้จัดทำนโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศขึ้น เพื่อเผยแพร่ให้ทุกหน่วยงานในโรงพยาบาล เสริมสร้างความรู้ ความเข้าใจและสามารถนำไปปฏิบัติตามนโยบายและแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศได้อย่างถูกต้องและมีประสิทธิภาพ

ฝ่ายเทคโนโลยีสารสนเทศ

โรงพยาบาลสมเด็จพระบรมราชเทวี ณ ศรีราชา

สารบัญ

๑. บทนำ

๑.๑ หลักการและเหตุผล

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ ในมาตรา ๕ “หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้” และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ กำหนดให้หน่วยงานของรัฐต้องจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร สารสนเทศถือเป็นสินทรัพย์ที่สำคัญสำหรับการดำเนินงานขององค์กร และเป็นสิ่งที่มีค่ายิ่งสำหรับองค์กรซึ่งจะได้รับการป้องกันรักษาเช่นเดียวกับสินทรัพย์อื่น ทั้งนี้สารสนเทศอาจอยู่ได้ในหลายรูปแบบไม่ว่าจะเป็นเอกสารสิ่งพิมพ์หรือถูกเก็บไว้ในสื่ออิเล็กทรอนิกส์ที่ต้องได้รับการปกป้องจากภัยคุกคามที่อาจก่อให้เกิดความเสียหายต่อองค์กร

นโยบายความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้ จัดทำขึ้นเพื่อเป็นแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยในระบบสารสนเทศ ภายในโรงพยาบาลสมเด็จพระบรมราชเทวี ณ ศรีราชา เพื่อให้มั่นใจได้ว่า การใช้งานระบบสารสนเทศมีความปลอดภัย และเชื่อถือได้ สามารถให้บริการระบบสารสนเทศได้อย่างต่อเนื่อง ลดความเสี่ยงจากการถูกคุกคามจากภัยต่าง ๆ ในระบบสารสนเทศ โดยนโยบายฉบับสอดคล้องกับประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานภาครัฐ พ.ศ. ๒๕๕๓ สอดคล้องกับบริบทองค์กร และผลการประเมินความเสี่ยงในระบบสารสนเทศตามข้อกำหนดมาตรฐาน ISO/IEC 27001 : 2013

๑. ๑.๒ วัตถุประสงค์

๑.๒.๑ เพื่อกำหนดแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศสร้างความน่าเชื่อถือ มั่นคง และปลอดภัย ในระบบสารสนเทศภายในโรงพยาบาลสมเด็จพระบรมราชเทวี ณ ศรีราชา

๑.๒.๒ สร้างความเข้าใจ และความตระหนักในการใช้งานระบบสารสนเทศอย่างปลอดภัยสำหรับผู้ปฏิบัติงานที่เป็นบุคลากรภายในโรงพยาบาล ผู้รับจ้างที่ปฏิบัติหน้าที่ในโรงพยาบาลสมเด็จพระบรมราชเทวี ณ ศรีราชา

๑.๒.๓ กำหนดแนวทางปฏิบัติสำหรับผู้ควบคุมระบบสารสนเทศ (Admin) เพื่อให้มั่นใจได้ว่า ระบบได้รับการเฝ้าระวัง ติดตามความมั่นคงปลอดภัย สอดคล้องตามมาตรฐาน ISO/IEC 27001 : 2013

๑.๓ บทบังคับใช้

นโยบายความมั่นคงปลอดภัยด้านสารสนเทศ ฉบับนี้ให้มีผลบังคับใช้กับ ผู้ใช้งานระบบสารสนเทศ ผู้ทำหน้าที่ดูแลทรัพย์สิน ผู้ใช้ทรัพย์สิน ผู้บริหาร และผู้มีส่วนเกี่ยวข้องในระบบสารสนเทศขององค์กร จะต้องให้ความร่วมมือในการดำเนินการตามนโยบายนี้ ผู้ฝ่าฝืนไม่ปฏิบัติตามนโยบายนี้มีความผิดและจะต้องได้รับการดำเนินการตามระเบียบขององค์กร

๑.๔ การเผยแพร่ และทบทวนนโยบาย

นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของโรงพยาบาลสมเด็จพระบรมราชเทวี ณ ศรีราชาฉบับนี้ จะได้นำออกเผยแพร่โดยการประกาศแจ้งเวียนในระบบสารสนเทศเครือข่ายภายในองค์กร หรือจัดพิมพ์เผยแพร่ อบรมสร้างความตระหนักเพื่อให้บุคลากรโรงพยาบาลสมเด็จพระบรมราชเทวี ณ ศรีราชา และบุคคลภายนอกที่เกี่ยวข้องได้ทราบและถือปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

นโยบายความมั่นคงปลอดภัยสารสนเทศนี้ จะทบทวนปีละ ๑ ครั้ง เพื่อให้สอดคล้องกับบริบทองค์กร และผลการประเมินความเสี่ยงขององค์กร

๒. คำนิยาม

๑. **องค์กร** หมายถึง โรงพยาบาลสมเด็จพระบรมราชเทวี ณ ศรีราชา, ศูนย์ส่งเสริมฟื้นฟูสุขภาพผู้สูงอายุ สภากาชาดไทย และศูนย์บริการสุขภาพ

๒. **แนวปฏิบัติ** หมายถึง แนวทางที่ต้องปฏิบัติตามเพื่อให้สามารถบรรลุวัตถุประสงค์หรือเป้าหมายของนโยบาย

๓. **ผู้ใช้งาน** หมายถึง เจ้าหน้าที่ ลูกจ้าง ผู้ดูแลระบบ ผู้บริหารขององค์กร ผู้รับผิดชอบ ผู้ใช้งานทั่วไป อันได้แก่

- ๓.๑ ผู้บริหารสูงสุด หมายถึง ผู้อำนวยการโรงพยาบาลสมเด็จ ณ ศรีราชา
- ๓.๒ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Office : CIO) หมายถึง รองผู้อำนวยการโรงพยาบาลสมเด็จพระบรมราชเทวี ณ ศรีราชา ที่ดูแลด้านเทคโนโลยีสารสนเทศ
- ๓.๓ ผู้ดูแลระบบ หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายให้มีหน้าที่ดูแลรักษาระบบสารสนเทศ หรือ ระบบเครือข่าย หรืออุปกรณ์ในระบบสารสนเทศ
- ๓.๔ ผู้พัฒนาระบบ หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายให้มีหน้าที่รับผิดชอบพัฒนาระบบแอปพลิเคชัน
- ๓.๕ เจ้าหน้าที่ หมายถึง แพทย์ พยาบาล เจ้าหน้าที่ ลูกจ้างประจำ ลูกจ้างชั่วคราว เจ้าหน้าที่ Out Source และผู้ปฏิบัติงานที่ได้รับมอบหมาย
- ๓.๖ บุคคลภายนอก หมายความว่า บุคคลที่องค์กรอนุญาตให้เข้ามาใช้ระบบเทคโนโลยีสารสนเทศขององค์กรได้ชั่วคราว เพื่อประโยชน์ในการดำเนินงาน รวมถึง พนักงานหรือลูกจ้างบริษัทภายนอกที่เข้ามาติดตั้งหรือดูแลรักษาระบบ หรือ ที่ปรึกษา หรือผู้ปฏิบัติงานตามสัญญาจ้าง นักศึกษาฝึกงาน

๔. **สิทธิของผู้ใช้งาน** หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศขององค์กร

๕. **สินทรัพย์** (Asset) หรือ ทรัพย์สินสารสนเทศ หมายถึง สิ่งใดก็ตามที่มีคุณค่าสำหรับองค์กร อันได้แก่

- ๕.๑ ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ
- ๕.๒ ตัวเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ เครื่องบันทึกข้อมูล และอุปกรณ์อื่นใด
- ๕.๓ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์
- ๕.๔ บุคลากร

๖. **การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ (Access Control)** หมายถึง การอนุญาต การกำหนด

สิทธิ หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก

๗. ความมั่นคงปลอดภัยด้านสารสนเทศ/ระบบสารสนเทศ (Information Security) หมายถึง การดำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) ห้ามปฏิเสธความรับผิด (Non-repudiation) และความน่าเชื่อถือ (Reliability) และหมายความรวมถึง การป้องกันทรัพย์สินสารสนเทศจากการเข้าถึง ใช้ เปิดเผย ขัดขวาง เปลี่ยนแปลงแก้ไข ทำสูญหาย ทำให้เสียหาย ถูกทำลาย หรือล่วงรู้โดยมิชอบ

๘. เหตุการณ์ด้านความมั่นคงปลอดภัย (Information Security event) หมายถึง กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันนำไปสู่ปัญหาด้านความมั่นคงปลอดภัย

๙. สถานการณ์ความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information Security Incident) หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or Unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

๑๐. หน่วยงานภายนอก หมายถึง องค์กรหรือหน่วยงานที่องค์กรอนุญาตให้มีสิทธิในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่าง ๆ ของหน่วยงาน โดยจะได้รับสิทธิในการใช้งานตามอำนาจและต้องรับผิดชอบในการรักษาความลับของข้อมูลขององค์กร

๑๑. ข้อมูลคอมพิวเตอร์ หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง ที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้ความหมายรวมถึงข้อมูลอิเล็กทรอนิกส์ตาม พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ และฉบับแก้ไขเพิ่มเติม (ฉบับที่ 2) พ.ศ. ๒๕๕๑

๑๒. สารสนเทศ (Information) หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่ายและสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ

๑๓. ระบบคอมพิวเตอร์ หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันโดยไม่มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์ หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

๑๔. ระบบเครือข่าย (Network System) หมายถึง ระบบที่สามารถใช้ในงานติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ของโรงพยาบาลสมเด็จพระบรมราชเทวี ณ ศรีราชา ได้ เช่น ระบบแลน (LAN) ระบบอินทราเน็ต (Intranet) ระบบอินเทอร์เน็ต (Internet)

๑๕. ระบบเทคโนโลยีสารสนเทศ (Information Technology System) หมายถึง ระบบงานของ

หน่วยงานที่นำเอาเทคโนโลยีสารสนเทศระบบคอมพิวเตอร์ และระบบเครือข่าย มาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน บริหาร การสนับสนุนการให้บริการ การพัฒนาการควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย แอปพลิเคชันข้อมูล และสารสนเทศ เป็นต้น

๑๖. เจ้าของข้อมูล หมายถึง ผู้ได้รับอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงาน โดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น ๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย

๑๗. รหัสผ่าน (Password) หมายถึง ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

๑๘. ชุดคำสั่งไม่พึงประสงค์ (Malicious software) หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

๑๙. ระยะเวลาเป้าหมายในการเรียกคืนการดำเนินงาน (Recovery Time Objective : RTO) หมายถึง ระยะเวลาที่กำหนดขึ้นเพื่อเป็นเวลาเป้าหมายในการเรียกคืนการดำเนินงาน

๒๐. สถานะเป้าหมายในการเรียกคืนการดำเนินงาน (Recovery Point Objective : RPO) หมายถึง สถานะของการดำเนินงานที่เป็นเป้าหมายในการเรียกคืนการดำเนินงาน หรืออายุของข้อมูลสำรองสำหรับการดำเนินงานที่พร้อมใช้ในการเรียกคืนการดำเนินงาน

๒๑. ระบบและอุปกรณ์เครือข่าย หมายถึง ระบบและอุปกรณ์ที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ขององค์กร

๒๒. โครงสร้างพื้นฐานสารสนเทศ หมายถึง ระบบคอมพิวเตอร์ และระบบเครือข่าย ในการสนับสนุน การให้บริการ ควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย แอปพลิเคชันข้อมูล และสารสนเทศ เป็นต้น

๒๓. ศูนย์ข้อมูลกลาง (Data Center) หมายถึง ห้องระบบคอมพิวเตอร์ และระบบเครือข่าย ในการสนับสนุนการให้บริการด้านเทคโนโลยีสารสนเทศ

๒๔. ทรัพยากรของระบบ หมายถึง แหล่งที่มาของระบบสารสนเทศ เช่น ซีพียู หน่วยความจำ พื้นที่ฮาร์ดดิสก์ และปริมาณการใช้เครือข่าย เป็นต้น

๒๕. ความมั่นคงปลอดภัยด้านการบริหารจัดการ (Administrative Security) หมายถึง การกระทำในระดับบริหารโดยกำหนดนโยบาย มาตรการ หลักเกณฑ์ หรือกระบวนการเพื่อนำมาใช้ในกระบวนการ คัดเลือก การพัฒนา การนำไปใช้ หรือการบำรุงรักษาทรัพย์สินสารสนเทศให้มีความมั่นคงปลอดภัย

๒๖. ความมั่นคงปลอดภัยทางด้านกายภาพ (Physical Security) หมายถึง การจัดให้มีนโยบาย มาตรการ หลักเกณฑ์ หรือกระบวนการใด ๆ เพื่อนำมาใช้ในการป้องกันทรัพย์สินสารสนเทศ สิ่งปลูกสร้าง หรือทรัพย์สินอื่นใดจากการคุกคามของบุคคล ภัยธรรมชาติ อุบัติภัย หรือภัยทางกายภาพอื่น

๓. นโยบายรักษาความมั่นคงปลอดภัยสารสนเทศ

หมวด ๑ นโยบายการเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

มาตรการควบคุมและป้องกันการเข้าใช้งานสารสนเทศ เพื่อการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการควบคุมบุคคลที่ไม่ได้รับอนุญาตเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก จากโปรแกรมชุดคำสั่งไม่พึงประสงค์ที่จะสร้างความเสียหายแก่ข้อมูลหรือการทำงานของระบบเทคโนโลยีสารสนเทศให้หยุดชะงัก และทำให้ตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศได้อย่างถูกต้อง

วัตถุประสงค์

๑) เพื่อให้มีแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัย สำหรับการควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศของโรงพยาบาล

๒) เพื่อให้ผู้รับผิดชอบและผู้มีส่วนเกี่ยวข้อง ได้แก่ผู้บริหาร ผู้ใช้งาน ผู้ดูแลระบบ และบุคคลภายนอกที่ปฏิบัติงานให้กับโรงพยาบาล ได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย

ผู้รับผิดชอบ

๑) ฝ่ายเทคโนโลยีสารสนเทศ

๒) ผู้ดูแลระบบที่ได้รับมอบหมาย

๓) ผู้ใช้งานระบบสารสนเทศ

แนวทางปฏิบัติ

ส่วนที่ ๑ การเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control)

๑.๑ ผู้ดูแลระบบ จะอนุญาตให้ผู้ใช้งานเข้าถึงระบบสารสนเทศที่ต้องการใช้งานได้ ต่อเมื่อได้รับอนุญาตจาก ผู้รับผิดชอบ/เจ้าของข้อมูล/เจ้าของระบบ ตามความจำเป็นต่อการใช้งาน เท่านั้น โดยต้องทำ

เอกสารขอใช้งานระบบสารสนเทศอนุมัติโดยหัวหน้าหน่วยงานต้นสังกัด และอนุมัติให้สิทธิใช้งานโดยหัวหน้าฝ่ายเทคโนโลยีสารสนเทศ หรือหัวหน้าหน่วยงานที่ดูแลรับผิดชอบ

๑.๒ บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบสารสนเทศของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษรต่อหัวหน้าฝ่ายเทคโนโลยีสารสนเทศ หรือหัวหน้าหน่วยงานที่ดูแลรับผิดชอบ

๑.๓ ผู้ดูแลระบบ ต้องกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งาน และหน้าที่ความรับผิดชอบในการปฏิบัติงานของผู้ใช้งานระบบสารสนเทศ โดยกำหนดสิทธิผู้ใช้งานแต่ละกลุ่มงาน ที่ได้รับสิทธิแตกต่างกันดังนี้

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

๑.๔ กำหนดเกณฑ์การระงับสิทธิ์ มอบอำนาจ ให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) ที่ได้กำหนดไว้

ส่วนที่ ๒ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

๒.๑ ผู้ดูแลระบบ ต้องกำหนดการลงทะเบียนผู้ใช้งานใหม่ ดังนี้

๑) จัดทำแบบฟอร์มการลงทะเบียนผู้ใช้งาน ในระบบสารสนเทศ

๒) ผู้ดูแลระบบต้องตรวจสอบบัญชีผู้ใช้งาน เพื่อไม่ให้มีการลงทะเบียนซ้ำซ้อน

๓) ผู้ดูแลระบบต้องตรวจสอบและให้สิทธิ์ในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ

๒.๒ ผู้ดูแลระบบต้องทบทวนบัญชีผู้ใช้งาน สิทธิ์การใช้งานอย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้งเพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต โดยปฏิบัติตามแนวทาง ดังนี้

๑) พิมพ์รายชื่อของผู้ที่ยังมีสิทธิ์ในระบบแยกตามหน่วยงาน

๒) จัดส่งรายชื่อนั้นให้กับผู้บังคับบัญชาของหน่วยงานเพื่อดำเนินการทบทวนรายชื่อและสิทธิ์การเข้าใช้งานว่าถูกต้องหรือไม่

๓) ดำเนินการแก้ไขข้อมูล สิทธิ์ต่าง ๆ ให้ถูกต้องตามที่ได้รับแจ้งกลับจากหน่วยงาน

๔) ขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน เมื่อลาออกต้องดำเนินการภายใน 3 วันหรือเมื่อเปลี่ยนตำแหน่งงานภายในต้องดำเนินการภายใน 7 วัน

๒.๓ การบริหารจัดการรหัสผ่าน

๑) ผู้ดูแลระบบจะกำหนด รหัสเริ่มต้น (Password) ให้ผู้ใช้งาน ซึ่งต้องเปลี่ยนรหัสเริ่มต้นภายใน 7 วันเมื่อเริ่มใช้งาน

๒) การส่งมอบรหัสผ่านเริ่มต้น (Password) ให้ผู้ใช้งานภายในซองปิดสนิท หรือทางจดหมายอิเล็กทรอนิกส์ (e-mail) และทำการยืนยันตัวตนผ่านระบบข้อความโทรศัพท์

๓) กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานลาออก หรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน

๔) กำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่าน (Password) ผิดพลาดได้ไม่เกิน 3 ครั้ง

๕) ผู้ดูแลระบบต้องจัดทำระบบให้ผู้ใช้งานสามารถทำการเปลี่ยนรหัสผ่าน (Password) เองได้ หรือกรณีที่ผู้ใช้งานจำรหัสผ่าน (Password) ไม่ได้ ต้องมีระบบให้ผู้ใช้งานตั้งรหัสผ่าน (Password) ได้ด้วยตนเองผ่านทางจดหมายอิเล็กทรอนิกส์ (e-mail) และทำการยืนยันตัวตนผ่านระบบข้อความโทรศัพท์

๖) ในกรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากหัวหน้าหน่วยงาน โดยมีการกำหนดระยะเวลา การใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนด

๒.๔ ผู้ดูแลระบบ ต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับ ในการควบคุม การเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรง และการเข้าถึงผ่านระบบงานรวมถึง วิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ มีดังต่อไปนี้

๑) ควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรง และการเข้าถึงผ่านระบบงาน

๒) กำหนดรายชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้งานข้อมูลในแต่ละชั้นความลับของข้อมูล

๓) กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

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

๕) กำหนดการเปลี่ยนรหัสผ่าน (Password) ตามระยะเวลาที่กำหนดของระดับ ความสำคัญของระบบสารสนเทศดังนี้

๕.๑ รหัสเข้าใช้งานระบบเครือข่าย

๕.๒ รหัสเข้าใช้ระบบงาน

๖) องค์กรกำหนดให้มาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำสินทรัพย์ออกนอกองค์กร เพื่อบำรุงรักษา ตรวจซ่อม หรือจำหน่าย หากสินทรัพย์ดังกล่าวมีหน่วยความจำ

เก็บข้อมูล ฝ่ายเทคโนโลยีสารสนเทศ จะต้องเก็บหน่วยบันทึกความจำไว้ภายในองค์กร หรือกรณีต้องส่งพร้อมอุปกรณ์ ข้อมูลต่าง ๆ จะต้องสำรอง และลบข้อมูลในสื่อบันทึกก่อนทุกครั้ง

๒.๕ ระบบงานสารสนเทศทางธุรกิจที่เชื่อมโยงกัน (Business Information Systems) เมื่อต้องมีการถ่ายโอนข้อมูล CIO เป็นผู้อนุมัติให้ดำเนินการ ภายใต้การควบคุมให้มีความมั่นคงปลอดภัย และมีการป้องกันจุดอ่อนต่าง ๆ ก่อนตัดสินใจใช้ข้อมูลร่วมกันในระบบงาน หรือระบบเทคโนโลยีสารสนเทศที่จะเชื่อมโยงเข้าด้วยกัน กับหน่วยงานภายนอก ต้องดำเนินการดังนี้

๑) กำหนดนโยบายและมาตรการเพื่อควบคุม ป้องกัน และบริหารจัดการการใช้ข้อมูลร่วมกัน โดยจะต้องมีการทำบันทึกข้อตกลงในการรักษาความลับ (MOU) และการเข้าถึงข้อมูลดังกล่าวมีการเข้ารหัสเพื่อความปลอดภัย

๒) พิจารณาจำกัดหรือไม่อนุญาตการเข้าถึงข้อมูลส่วนบุคคล

๓) กำหนดว่าบุคลากรใดบ้างที่มีสิทธิ์หรือได้รับอนุญาตให้เข้าใช้งาน

๔) กำหนดให้ต้องมีการทะเบียนผู้ใช้งาน

ส่วนที่ ๓ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibility)

๓.๑ การใช้งานรหัสผ่าน ผู้ใช้งานต้องปฏิบัติ ดังนี้

๑) ผู้ใช้งานมีหน้าที่ในการป้องกัน ดูแล รักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) โดยผู้ใช้งานแต่ละคนต้องมีบัญชีชื่อผู้ใช้งาน (Username) ของตนเอง ห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามทำการเผยแพร่ แจกจ่าย ทำให้ผู้อื่นล่วงรู้รหัสผ่าน (Password)

๒) การกำหนดรหัสผ่าน (Password) ที่ปลอดภัย และเดาสุ่มได้ยาก ซึ่งประกอบด้วย

- กำหนดให้ความยาวไม่น้อยกว่า 8 ตัวอักษร(รหัส เข้าระบบงาน / รหัสเข้าใช้งานเครือข่าย / รหัสเครื่อง
- ใช้อักขระพิเศษประกอบ เช่น :;<> เป็นต้น
- ไม่กำหนดรหัสผ่านอย่างเป็นแบบแผน เช่น “abcdef”, “aaaaa” เป็นต้น
- การกำหนดรหัสผ่านใหม่ต้องไม่ซ้ำกับของเดิมครั้งสุดท้าย
- ไม่กำหนดรหัสผ่านที่เกี่ยวข้องผู้ใช้งาน เช่น ชื่อ, นามสกุล หรือวันเกิด เป็นต้น
- ไม่กำหนดรหัสผ่านที่เป็นคำศัพท์ในพจนานุกรม
- ไม่กำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเอง หรือบุคคลในครอบครัว

๓) ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

๔) ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่ผู้ใช้งานครอบครองอยู่

๕) ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

๖) ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (Password) ไม่เกิน 180 วันหรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน

๓.๒ ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนที่จะใช้สินทรัพย์หรือระบบสารสนเทศของหน่วยงาน และหากการพิสูจน์ตัวตนนั้นมีปัญหา ไม่ว่าจะเกิดจากรหัสผ่านล็อกก็ดี หรือเกิดจากความผิดพลาดใด ๆ ก็ดี ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบทันที โดยปฏิบัติตามแนวทาง ดังนี้

๑) คอมพิวเตอร์ทุกประเภท ก่อนการเข้าถึงระบบปฏิบัติการต้องทำการพิสูจน์ตัวตนทุกครั้ง

๒) การใช้งานระบบคอมพิวเตอร์อื่นในเครือข่ายจะต้องทำการพิสูจน์ตัวตนทุกครั้ง

๓) การใช้งานโปรแกรมประยุกต์ (Application) ระบบสารสนเทศที่ให้บริการแก่ผู้รับบริการจะต้องทำการพิสูจน์ตัวตนทุกครั้ง

๔) การใช้งานระบบการจัดเก็บข้อมูลภายใน (Own Cloud) จะต้องทำการพิสูจน์ตัวตนทุกครั้ง

๕) การใช้งานอินเทอร์เน็ต (Internet) ต้องทำการพิสูจน์ตัวตน และต้องมีการบันทึกข้อมูลซึ่งสามารถบ่งบอกตัวตนบุคคลผู้ใช้งานได้

๖) เมื่อผู้ใช้งานไม่อยู่ที่เครื่องคอมพิวเตอร์ ต้องทำการล็อกหน้าจอทุกครั้ง และต้องทำการพิสูจน์ตัวตนก่อนการใช้งานทุกครั้ง

๗) เครื่องคอมพิวเตอร์ทุกเครื่องต้องทำการตั้งเวลาพักหน้าจอ (Screen Saver) โดยตั้งเวลาอย่างน้อย ๓๕ นาที

๓.๓ ผู้ใช้งานต้องตระหนักและระมัดระวังต่อการใช้งานข้อมูล ไม่ว่าข้อมูลนั้นจะเป็นขององค์กร หรือเป็นข้อมูลของบุคคลภายนอก

๓.๔ ข้อมูลที่เป็นความลับหรือมีระดับความสำคัญ ที่อยู่ในการครอบครอง/ดูแลของหน่วยงาน ห้ามไม่ให้ทำการเผยแพร่ เปลี่ยนแปลง ทำซ้ำ หรือทำลาย โดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงาน

๓.๕ ผู้ใช้งานมีส่วนร่วมในการดูแลรักษาและรับผิดชอบต่อข้อมูลขององค์กร และข้อมูลของผู้รับบริการ และมีความตระหนักในการเก็บรักษาข้อมูลอย่างปลอดภัย ป้องกันการสูญหาย การนำไปใช้ในทางที่ผิด การเผยแพร่โดยไม่ได้รับอนุญาต ผู้ใช้งานต้องมีส่วนร่วมในการรับผิดชอบต่อความเสียหายนั้นด้วย

๓.๖ ผู้ใช้งานต้องป้องกัน ดูแล รักษาไว้ซึ่งความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูล ตลอดจนเอกสาร สื่อบันทึกข้อมูลคอมพิวเตอร์ หรือสารสนเทศต่าง ๆ ที่เสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ์

๓.๗ ผู้ใช้งานมีสิทธิ์เข้าถึงข้อมูล ต้องเก็บรักษา ใช้งาน และป้องกันข้อมูลส่วนบุคคลอย่างปลอดภัย และไม่อนุญาตให้บุคคลหนึ่งบุคคลใดทำการละเมิดต่อข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตจากผู้ใช้งานที่ครอบครองข้อมูลนั้น ยกเว้นในกรณีที่องค์กรต้องการตรวจสอบข้อมูล หรือคาดว่าข้อมูลนั้นเกี่ยวข้องกับองค์กร ซึ่งองค์กรจะแต่งตั้งให้ผู้ทำหน้าที่ตรวจสอบข้อมูลเหล่านั้นได้ตลอดเวลา โดยไม่ต้องแจ้งให้ผู้ใช้งานทราบ

๓.๘ ห้ามเปิดหรือใช้งาน (Run) โปรแกรมประเภท Peer-to-Peer (หมายถึง วิธีการจัดเครือข่าย

คอมพิวเตอร์แบบหนึ่ง ที่กำหนดให้คอมพิวเตอร์ในเครือข่ายทุกเครื่องเหมือนกันหรือเท่าเทียมกัน หมายความว่า แต่ละเครื่องต่างมีโปรแกรมหรือมีแฟ้มข้อมูลเก็บไว้เอง การจัดแบบนี้ทำให้สามารถใช้โปรแกรมหรือแฟ้มข้อมูลของคอมพิวเตอร์เครื่องใดก็ได้ แทนที่จะต้องใช้จากเครื่องบริการแฟ้ม (File Server) เท่านั้น) หรือโปรแกรมที่มีความเสี่ยงในระดับเดียวกัน เช่น บิทเทอร์เรนท์ (Bittorrent), อีมูล (Emule) เป็นต้น เว้นแต่จะได้รับอนุญาตจากหัวหน้าหน่วยงาน

๓.๙ ห้ามเปิดหรือใช้งาน (Run) โปรแกรมออนไลน์ทุกประเภท เพื่อความบันเทิง เช่น การดูหนัง ฟังเพลง เกมส์ เป็นต้น ในระหว่างเวลาปฏิบัติงาน

๓.๑๐ ห้ามใช้สินทรัพย์ของหน่วยงาน ที่จัดเตรียมให้ เพื่อการเผยแพร่ ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใด ที่มีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมาย หรือกระทบต่อภารกิจขององค์กร

๓.๑๑ ห้ามใช้สินทรัพย์ของหน่วยงาน เพื่อการรบกวน ก่อให้เกิดความเสียหาย หรือใช้ในการโจรกรรมข้อมูล หรือสิ่งอื่นใดอันเป็นการขัดต่อกฎหมายและศีลธรรม หรือกระทบต่อภารกิจ ขององค์กร

๓.๑๒ ห้ามใช้สินทรัพย์ และระบบสารสนเทศขององค์กรเพื่อประโยชน์ทางการค้า

๓.๑๓ ห้ามกระทำการใด ๆ เพื่อการดักข้อมูล ไม่ว่าจะเป็นข้อความ ภาพ เสียง หรือสิ่งอื่นใด ในเครือข่ายระบบสารสนเทศขององค์กรโดยเด็ดขาด ไม่ว่าจะด้วยวิธีการใด ๆ ก็ตาม

๓.๑๔ ห้ามกระทำการรบกวน ทำลาย หรือทำให้ระบบสารสนเทศของหน่วยงานต้องหยุดชะงัก

๓.๑๕ ห้ามใช้ระบบสารสนเทศขององค์กร เพื่อการควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอกโดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบที่ได้รับมอบหมาย

๓.๑๖ ห้ามกระทำการใด ๆ อันมีลักษณะเป็นการลักลอบใช้งานหรือรับรู้รหัสส่วนบุคคลของผู้อื่น ไม่ว่าจะเป็นกรณีใด ๆ เพื่อประโยชน์ในการเข้าถึงข้อมูล หรือเพื่อการใช้ทรัพยากรก็ตาม

๓.๑๗ ห้ามติดตั้งอุปกรณ์หรือกระทำการใด ๆ เพื่อเข้าถึงระบบสารสนเทศขององค์กรโดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบที่ได้รับมอบหมาย

๓.๑๘ ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของหน่วยงานที่ยังไม่ได้ประกาศ อย่างเป็นทางการผ่านระบบอินเตอร์เน็ต (Internet)

๓.๑๙ ระมัดระวังการดาวน์โหลด โปรแกรมใช้งานจากระบบอินเทอร์เน็ต (Internet) การอัปเดต (Update) โปรแกรมต่างๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์

๓.๒๐ ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของหน่วยงาน

๓.๒๑ ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ไม่เสนอความคิดเห็น หรือใช้ข้อความที่ ยั่วยุให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของหน่วยงาน การทำลายความสัมพันธ์กับบุคลากรของหน่วยงานอื่นๆ

๓.๒๒ ผู้ใช้งานไม่นำเข้าข้อมูลคอมพิวเตอร์ใดๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิด เกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามก และไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเทอร์เน็ต

๓.๒๓ ห้ามใช้งานอุปกรณ์จัดเก็บข้อมูลพกพา Flash Drive, Handy Drive หรือ Thumb Drive กับเครื่องคอมพิวเตอร์ที่ใช้ในการปฏิบัติงานของโรงพยาบาล การส่งข้อมูลให้ใช้วิธีการส่งผ่านทาง e-Mail เพื่อป้องกันไวรัสคอมพิวเตอร์ที่จะติดมากับอุปกรณ์พกพา

๓.๒๔ การสำรองข้อมูลให้ทำการสำรองข้อมูลในระบบ Own Cloud ที่โรงพยาบาลจัดไว้ให้

๓.๒๕ หลังจากใช้งานระบบอินเทอร์เน็ต (Internet) เสร็จแล้ว ให้ปิดเว็บเบราว์เซอร์ (Web Browser) เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่นๆ

๓.๒๖ หลังจากใช้งานอินเทอร์เน็ตเสร็จแล้ว ให้ทำการออกจากระบบเพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น ๆ

๓.๒๗ ผู้ใช้งานต้องปฏิบัติตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ อย่างเคร่งครัด

ส่วนที่ ๔ การใช้สื่อสังคมออนไลน์ (Social Network)

๔.๑ "สื่อสังคมออนไลน์" หมายความว่า สื่อ ช่องทางในการติดต่อสื่อสาร การแลกเปลี่ยนข้อมูลระหว่างกัน โดยใช้เทคโนโลยีสารสนเทศ ที่เน้นการสร้างและเผยแพร่เนื้อหาระหว่างผู้ใช้งานด้วยกัน (creation and exchange of user-generated content) หรือสนับสนุนการสื่อสารสองทาง หรือการนำเสนอและเผยแพร่ภาพ เนื้อหาและข้อมูลต่าง ๆ ในวงกว้างได้ด้วยตนเอง ซึ่งนิยมเรียกกันเป็นภาษาอังกฤษว่า Social media หรือ Social network ซึ่งรวมถึงสื่อดังต่อไปนี้

๑. กระดานข่าว (web board หรือ online forums)

๒. เครือข่ายสังคมออนไลน์ (social networking services) เช่น Facebook, WhatsApp, Instagram, LinkedIn เป็นต้น

๓. ระบบส่งข้อความทันที (instant messaging) เช่น LINE, Facebook Messanger, WhatsApp เป็นต้น

๔. สื่อสำหรับการเผยแพร่และแลกเปลี่ยนเนื้อหาที่เป็นภาพนิ่ง เสียง วีดิทัศน์ หรือ แฟ้มข้อมูล หรือให้บริการเนื้อที่เก็บข้อมูลบนอินเทอร์เน็ต (Photo-sharing, Audio-sharing, Video-sharing, File-sharing,และ Online storage services) เช่น Flickr, Podcast, YouTube, Instagram, Dropbox, Google Drive,Microsoft OneDrive

๕. บล็อก (blogs) เช่น WordPress, Blogger และไมโครบล็อก (microblogs) เช่น Twitter

๖. เว็บไซต์สำหรับการสร้างและแก้ไขเนื้อหาร่วมกัน (wikis) เช่น Wikipedia

๗. เกมออนไลน์หรือโลกเสมือนที่มีผู้ใช้งานหลายคน (multi-user virtual environments)

๘. สื่ออิเล็กทรอนิกส์หรือสื่อออนไลน์อื่นในลักษณะเดียวกันหรือคล้ายคลึงกันที่เปิดให้ใช้งานเพื่อเป็นช่องทางสื่อสารระหว่างบุคคล ระหว่างกลุ่มบุคคล หรือกับสาธารณะ

๔.๒ การใช้งานสื่อสังคมออนไลน์ของผู้ใช้งาน

๑. การใช้สื่อสังคมออนไลน์ ต้องตระหนักถึงหน้าที่ตามกฎหมายในการคุ้มครองความลับ (Confidentiality) และความเป็นส่วนตัว (Privacy) ของข้อมูลผู้ป่วย หลีกเลี่ยงการเปิดเผยข้อมูลส่วนบุคคลของผู้ป่วยหรือผู้แทนโดยชอบธรรม หรือตามที่กฎหมายกำหนดไว้ และแม้แต่จะได้รับความยินยอมแล้วก็ตาม ต้องพิจารณาข้อดีข้อเสียของการเปิดเผยข้อมูลส่วนบุคคล ที่อาจจะส่งผลต่อผู้ป่วย ตนเอง โรงพยาบาล และสาธารณประโยชน์ อย่างรอบคอบ

๒. การใช้สื่อสังคมออนไลน์ต้องเคารพศักดิ์ศรีความเป็นมนุษย์ หลีกเลี่ยงการกระทำหรือการเผยแพร่เนื้อหาที่ละเมิดศักดิ์ศรีความเป็นมนุษย์หรืออาจทำให้บุคคลอื่นเสียหาย เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง ถูกคุกคาม หรือถูกกลั่นแกล้ง

๓. การใช้สื่อสังคมออนไลน์ต้องทำการศึกษาเงื่อนไขการให้บริการของผู้ให้บริการสื่อสังคมออนไลน์อย่างละเอียดรอบคอบ

๔. การใช้สื่อสังคมออนไลน์ต้องทำการกำหนดค่าความเป็นส่วนตัว เพื่อจำกัดการเข้าถึงข้อมูลส่วนตัวจากบุคคลอื่น ทำการแยกบัญชีสื่อสังคมออนไลน์ออกจากกันระหว่างเรื่องส่วนตัวและเรื่องการให้บริการ ทั้งนี้จะต้องคอยตรวจสอบเนื้อหาข้อมูลในสื่อสังคมออนไลน์ เพื่อให้แน่ใจว่ามีข้อมูลที่ถูกต้อง ไม่มีเนื้อหาที่ไม่เหมาะสมที่อาจส่งผลกระทบต่อตนเอง ผู้ป่วย และโรงพยาบาล

๕. ในการขอรับความยินยอมในการเปิดเผยข้อมูลจากผู้ป่วย บุคคลใดบุคคลหนึ่ง หรือผู้แทนโดยชอบตามกฎหมาย ต้องแจ้งวัตถุประสงค์ รูปแบบ ช่องทาง ผลดีผลเสีย ในการเปิดเผยข้อมูลให้ทราบอย่างเข้าใจถ่องแท้ พร้อมทั้งให้มีการซักถามก่อนให้ความยินยอม และต้องเป็นการยินยอมโดยสมัครใจอย่างแท้จริง

๖. การเปิดเผยข้อมูลจะต้องทำการปกปิดข้อมูลที่สามารถระบุถึง อ้างถึงตัวผู้ป่วยหรือบุคคลใดบุคคลหนึ่งได้ เช่น ชื่อ นามสกุล หมายเลขประจำตัวใดๆ เช่น เลขที่ผู้ป่วย เลขที่บัตรประชาชน เลขที่เตียงผู้ป่วย ที่อยู่ผู้ป่วย เป็นต้น

๗. ห้ามถ่ายภาพแฟ้มประวัติผู้ป่วย เอกสารการรักษาพยาบาล เอกสารผลการตรวจวิเคราะห์ต่างๆ รวมถึงภาพจากหน้าจอคอมพิวเตอร์ ข้อมูลระบบสารสนเทศของระบบที่เกี่ยวข้องกับการรักษาพยาบาล และระบบผลการตรวจวิเคราะห์ต่าง ๆ

๘. ห้ามเผยแพร่ภาพถ่าย วีดิทัศน์ ที่ไม่เหมาะสม เช่น ภาพถ่ายในหอผู้ป่วย ภาพถ่ายในห้องตรวจการรักษา ห้องคลอด ห้องผ่าตัด ภาพถ่ายขณะให้การรักษาพยาบาล การทำหัตถการ ภาพถ่ายในการดูแลรักษาผู้บาดเจ็บหรือเสียชีวิต ภาพที่ทำให้เข้าใจผิด ภาพแสดงการดูหมิ่นเหยียดหยาม ภาพลามกอนาจาร ภาพ

เหตุการณ์หวาดเสียวรุนแรง ภาพที่แสดงการระบายอารมณ์และการนินทา หรือภาพใด ๆ ที่อาจทำให้ผู้ป่วย หรือผู้ใดผู้หนึ่งได้รับความเสียหายในสื่อสังคมออนไลน์ ไม่ว่าภาพนั้นจะสามารถระบุตัวตนของผู้ป่วย บุคคลใดบุคคลหนึ่งได้หรือไม่ก็ตาม

๙. ห้ามใช้สื่อสังคมออนไลน์ในการประกาศ โฆษณา การใช้เครื่องหมายของโรงพยาบาลและสภากาชาดไทย ใช้ จ้าง หรือยินยอมให้ผู้อื่นประกาศ โฆษณาผลิตภัณฑ์ การประกอบวิชาชีพ ความรู้ความชำนาญทั้งของตนเองและของผู้อื่นในลักษณะที่ขัดต่อข้อบังคับทางวิชาชีพ จริยธรรม และกฎหมายต่างๆ

๑๐. ห้ามใช้สื่อสังคมออนไลน์ในการแสดงความคิดเห็นที่เป็นข้อถกเถียงหรือสุ่มเสี่ยงอย่างมากต่อสังคม เช่น ชาติ ศาสนา พระมหากษัตริย์ การเมืองการปกครอง เป็นต้น

๑๑. ในการใช้สื่อสังคมออนไลน์ไม่ว่าจะอยู่ในสถานการณ์ใดๆ จะต้องไม่กระทบกระเทือนหรือเป็นอุปสรรคต่อการให้บริการผู้ป่วย หรือทำให้ผู้ป่วยไม่ได้รับการบริการด้วยมาตรฐานที่ดีที่สุดตามสถานการณ์นั้นๆ

๑๒. ในการให้คำปรึกษาออนไลน์ ต้องชี้แจงให้ผู้ป่วยเข้าใจ และตระหนักถึงความเสี่ยงและข้อจำกัดของการให้คำปรึกษาออนไลน์ก่อนให้คำปรึกษา พร้อมทั้งให้ข้อมูลเพื่อให้เข้ามารับการตรวจรักษาอย่างถูกต้องตามช่องทางปกติ หากไม่ต้องการให้คำปรึกษาออนไลน์ ต้องชี้แจงเหตุผล และแนะนำให้เข้ารับการรักษาตามช่องทางปกติ

๑๓. ในการลงข้อความใด ๆ ในสื่อสังคมออนไลน์อาจถูกนำไปใช้โดยผู้อื่น ต้องคำนึงถึงความถูกต้องเหมาะสม และผลกระทบที่ตามมา เนื่องจากเมื่อมีการลงข้อความไปแล้ว ข้อความต่างๆ จะมีการเผยแพร่ไปอย่างรวดเร็ว และไม่สามารถทำการลบได้

๑๔. การใช้สื่อสังคมออนไลน์ต้องหลีกเลี่ยงการใช้ถ้อยคำที่ไม่เหมาะสม ไม่สุภาพ โดยเด็ดขาด

๑๕. เมื่อไม่ใช้งานสื่อสังคมออนไลน์ ต้องทำการออกจากระบบทันที เพื่อป้องกันการเข้าถึงสื่อสังคมออนไลน์จากผู้อื่น

ส่วนที่ ๕ การบริหารจัดการสินทรัพย์ (Assets Management)

๕.๑ ศูนย์ข้อมูลกลาง (Data Center) เป็นสถานที่ที่ใช้สำหรับติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายและ/หรืออุปกรณ์บริหารจัดการเครือข่าย) ที่เป็นเขตหวงห้ามโดยเด็ดขาด เว้นแต่ได้รับอนุญาตจากผู้ดูแลระบบ

๕.๒ ผู้ดูแลระบบมีหน้าที่ควบคุมการปฏิบัติงานในห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ การนำอุปกรณ์หรือชิ้นส่วนใดออกจากห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ จะต้องได้รับอนุญาตจากผู้ดูแลระบบ

๕.๓ ผู้ใช้งานต้องไม่นำเครื่องมือ หรืออุปกรณ์อื่นใดเชื่อมต่อเข้าระบบเครือข่าย เพื่อการประกอบธุรกิจส่วนบุคคล หรือกระทำการใด ๆ ที่ผิดกฎหมาย

๕.๔ ผู้ใช้งานต้องไม่คัดลอกหรือทำสำเนาแฟ้มข้อมูลที่มีลิขสิทธิ์กำกับการใช้งาน ก่อนได้รับอนุญาตและผู้ใช้งานต้องไม่ใช้ หรือลบแฟ้มข้อมูลของผู้อื่น ไม่ว่ากรณีใด ๆ

๕.๕ ผู้ใช้งานต้องทำลายข้อมูลสำคัญในอุปกรณ์สื่อบันทึกข้อมูล แฟ้มข้อมูล ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว และใช้เทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์ สำหรับจัดเก็บ ข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้ และพิจารณาวิธีการทำลายข้อมูลบนสื่อบันทึกข้อมูลแต่ละประเภท ตามข้อกำหนด การทำลายและเคลื่อนย้ายสื่อบันทึกข้อมูล (Disposal and Removal of Media Procedure) SP-COM-11 ดังนี้

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

๕.๖ ผู้ใช้งานมีหน้าที่ต้องรับผิดชอบต่อสินทรัพย์ที่หน่วยงานมอบไว้ให้ใช้งานเสมือนหนึ่งเป็นสินทรัพย์ของผู้ใช้งานเอง โดยบรรดารายการสินทรัพย์ (Asset Lists) ที่ผู้ใช้งานต้องรับผิดชอบการรับหรือคืนสินทรัพย์ จะถูกบันทึกและตรวจสอบทุกครั้งโดยผู้ดูแลระบบ

๕.๗ กรณีนำทรัพย์สินไปทำงานนอกสถานที่ ต้องได้รับการอนุมัติเป็นลายลักษณ์อักษรจากหัวหน้าหน่วยงาน โดยผู้ใช้งานต้องดูแลและรับผิดชอบสินทรัพย์ของหน่วยงานที่ได้รับมอบหมายให้มีความปลอดภัยจากการโจรกรรมทรัพย์สิน และข้อมูลภายใน

๕.๘ ผู้ใช้งานมีหน้าที่ต้องชดใช้ค่าเสียหายไม่ว่าทรัพย์สินนั้นจะชำรุด หรือสูญหายตามมูลค่าทรัพย์สินหากความเสียหายนั้นเกิดจากความประมาทของผู้ใช้งาน

๕.๙ ผู้ใช้งานต้องไม่ให้ผู้อื่นยืมคอมพิวเตอร์ หรือโน้ตบุ๊ก ไม่ว่าในกรณีใด ๆ เว้นแต่การยืมนั้นได้รับการอนุมัติเป็นลายลักษณ์อักษรจากหัวหน้าหน่วยงานต้นสังกัด และเมื่อการใช้งานจบลง ผู้ครอบครองเครื่องต้องเปลี่ยนรหัสเข้าเครื่องทันที

๕.๑๐ ผู้ใช้งานมีสิทธิ์ใช้สินทรัพย์และระบบสารสนเทศต่าง ๆ ที่หน่วยงานจัดเตรียมไว้ให้ใช้งานโดยมีวัตถุประสงค์เพื่อการใช้งานของหน่วยงานเท่านั้น ห้ามมิให้ผู้ใช้งานนำสินทรัพย์และระบบสารสนเทศต่าง ๆ ไปใช้ในกิจกรรมที่หน่วยงานไม่ได้กำหนด หรือทำให้เกิดความเสียหายต่อองค์กร

๕.๑๑ ความเสียหายใด ๆ ที่เกิดจากการละเมิดตามข้อ ๔.๑๐ ให้ถือเป็นความผิดส่วนบุคคลโดยผู้ใช้งานต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

ส่วนที่ ๖ การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

มีวัตถุประสงค์เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต โดยฝ่ายเทคโนโลยีสารสนเทศ ผู้ให้บริการเครือข่าย ควบคุมการให้บริการเครือข่ายอย่างปลอดภัยดังนี้

๖.๑ กำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้เฉพาะบริการที่อนุญาตเท่านั้น การเข้าสู่ระบบเครือข่ายภายในหน่วยงาน โดยผ่านทางระบบอินเทอร์เน็ตต้องลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่าน เพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนทุกครั้ง

๖.๒ การยืนยันบุคคลที่ผู้ใช้อยู่นอกองค์กร จะต้องเป็นผู้ที่ได้รับอนุญาตเท่านั้นที่สามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศขององค์กรจากการเชื่อมต่อจากภายนอก (user authentication for external connections)

๖.๓ ผู้ดูแลระบบจัดเก็บบัญชีการขอเชื่อมต่อเครือข่าย ได้แก่ รายชื่อผู้ขอใช้บริการรายละเอียดดังนี้

- เครื่องคอมพิวเตอร์ที่ขอใช้บริการ IP Address และสถานที่ติดตั้ง
- ผู้ดูแลระบบต้องจำกัดผู้ใช้งานที่สามารถเข้าใช้อุปกรณ์ได้
- กรณีอุปกรณ์ที่มีการเชื่อมต่อจากเครือข่ายภายนอก ต้องมีการระบุหมายเลขอุปกรณ์ว่าสามารถเข้าเชื่อมต่อกับเครือข่ายภายในได้หรือไม่สามารถเชื่อมต่อได้
- อุปกรณ์เครือข่ายต้องสามารถตรวจสอบ IP Address ของทั้งต้นทางและปลายทางได้
- ต้องป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็น IP Address ภายในของระบบเครือข่ายภายในของหน่วยงาน

๖.๔ ผู้ดูแลระบบ ควบคุมและป้องกันไม่ให้มีการเข้าถึงพอร์ต และปรับแต่งระบบจากผู้ที่ไม่ได้รับอนุญาต โดยกำหนดสิทธิการเข้าถึงจากไฟร์วอลล์ Firewall

๖.๕ เพื่อความปลอดภัยองค์กรได้มีการแบ่งแยกเครือข่าย (Segregation in networks) ตามกลุ่มการให้บริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มระบบสารสนเทศ ดังนี้

๑) เครือข่ายจากหอพัก แพทย์ พยาบาล เจ้าหน้าที่ สามารถใช้งานทั่วไป เช่น Social Media หรือ YouTube ได้

๒) เครือข่ายจากงานบริการ สามารถเข้าถึงได้เฉพาะระบบสารสนเทศการบริการ เพื่อความปลอดภัยของระบบสารสนเทศในองค์กร

๖.๖ ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใด ๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลัก โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ

๖.๗ ระบบเครือข่ายทั้งหมดขององค์กร ที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกหน่วยงานต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก โดยเชื่อมต่อผ่าน Firewall รวมทั้งต้องมีความสามารถในการตรวจจับโปรแกรมประสงค์ร้าย (Malware)

๖.๘ กำหนดการป้องกันเครือข่ายและอุปกรณ์ต่าง ๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจนและต้องทบทวนการกำหนดค่า Parameter ต่าง ๆ เช่น IP Address Configuration อย่างน้อยปีละ ๒ ครั้ง นอกจากนี้การกำหนดแก้ไขหรือเปลี่ยนแปลงค่า Parameter ได้ จะเป็นผู้ดูแลระบบที่ได้รับอนุญาตเท่านั้น และการเปลี่ยนแปลงแต่ละครั้งต้องขออนุมัติจากหัวหน้าฝ่ายเทคโนโลยีสารสนเทศ หรือหัวหน้าหน่วยงานที่ดูแลรับผิดชอบ

๖.๙ ระบบเครือข่ายทั้งหมดที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกหน่วยงานต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือโปรแกรมในการทำ Packet Filtering เช่น การใช้ไฟร์วอลล์ (Firewall) ที่มีความสามารถในการตรวจจับมัลแวร์ (Malware)

๖.๑๐ มีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) โดยใช้ Firewall เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของหน่วยงาน ในลักษณะที่ผิดปกติ โดยมีการตรวจสอบการบุกรุกผ่านระบบเครือข่าย การใช้งานในลักษณะที่ผิดปกติ และการแก้ไขเปลี่ยนแปลงระบบเครือข่ายโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

ส่วนที่ ๗ การควบคุมการใช้งานอุปกรณ์ป้องกันเครือข่าย (Firewall Control)

๗.๑ ผู้ดูแลระบบมีหน้าที่ในการบริหารจัดการ การติดตั้งและกำหนดค่าของ Firewall ทั้งหมด

๗.๒ กำหนดค่าเริ่มต้น Firewall โดยตั้งเป็นปฏิเสธทั้งหมด (Deny) และอนุมัติเปิดให้บริการเป็นครั้ง ๆ กรณีที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ ต้องผ่านการเห็นชอบจากคณะกรรมการสารสนเทศของโรงพยาบาล

๗.๓ บริการ (Services) และเส้นทางเชื่อมต่ออินเทอร์เน็ตที่ไม่อนุญาตตาม Policy จะต้องถูกบล็อก (Block) โดย Firewall โดยความเห็นชอบจากคณะกรรมการสารสนเทศของโรงพยาบาล

๗.๔ ผู้ดูแลระบบกำหนดค่า Parameter การบริการและการเชื่อมต่อที่อนุญาต จะต้องมีการบันทึกการเปลี่ยนแปลงทุกครั้งหากมีการเปลี่ยนแปลงค่าต่าง ๆ ของ Firewall โดยบันทึกในเอกสาร แบบฟอร์มบันทึกการร้องขอการเปลี่ยนแปลงหรือแก้ไขระบบ FM-COM-018

๗.๕ มีการกำหนดมาตรการป้องกันการเข้าถึงตัวอุปกรณ์ Firewall จากผู้ที่ไม่ได้รับมอบหมาย

โดยการกำหนด IP Address ของผู้ดูแลระบบที่ได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงอุปกรณ์ Firewall ได้

ส่วนที่ ๘ การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต กำหนดให้มีการควบคุมการเข้าถึงระบบปฏิบัติการ โดยมีรายละเอียดดังนี้

๘.๑ กำหนดการเข้าใช้งานระบบอย่างปลอดภัย โดยระบุยืนยันตัวตนของผู้ใช้งาน (User identification and authentication) ตามสิทธิการเข้าถึงระบบปฏิบัติการที่ผู้ดูแลระบบจัดไว้ให้

๘.๒ ผู้ดูแลระบบบริหารจัดการรหัสผ่าน (password management system) เพื่อให้มีการใช้งานอย่างปลอดภัย และมีการทำงานเชิงโต้ตอบ (interactive) กับผู้ใช้งาน ดังนี้

- แจ้งเตือนเมื่อใส่รหัสผิด และ Lock การใช้งานเมื่อใส่รหัสผิดเกิน ๓ ครั้ง
- แจ้งเตือนให้มีการเปลี่ยนรหัสก่อนถึงกำหนดการให้เปลี่ยนรหัสผ่าน

๘.๓ ควบคุมการใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities) โดย

- ผู้ใช้งานไม่สามารถติดตั้งโปรแกรมได้ด้วยตนเอง ต้องแจ้งผู้ดูแลระบบเพื่อดำเนินการเท่านั้น
- ห้ามไม่ให้ผู้ใช้งาน ปรับแต่งโปรแกรมอรรถประโยชน์

๘.๔ การกำหนดเวลาใช้งานระบบสารสนเทศ (Session Time - Out)

๑) กำหนดให้ระบบสารสนเทศมีการตัดและหมดเวลาการใช้งาน รวมทั้งปิดการใช้งานด้วย หลังจากที่ไม่มีกิจกรรมการใช้งานช่วงระยะเวลาอย่างน้อย ๓๕ นาที

๒) กำหนดให้ระบบสารสนเทศมีการตัดและหมดเวลาการใช้งานที่สั้นขึ้นสำหรับระบบสารสนเทศที่มีความเสี่ยงสูง

๘.๕ การจำกัดระยะเวลาการเชื่อมต่อระบบเทคโนโลยีสารสนเทศ (Limitation of Connection Time) กำหนดไว้ดังนี้

๑) กำหนดให้ระบบเทคโนโลยีสารสนเทศมีการจำกัดระยะเวลาการเชื่อมต่อสำหรับการใช้งาน เพื่อให้ผู้ใช้งานสามารถใช้งานได้นานที่สุดภายในระยะเวลาที่กำหนด และกำหนดให้ใช้งานได้ตามช่วงเวลาการทำงานที่หน่วยงานกำหนดเท่านั้น

๒) กำหนดให้ระบบเทคโนโลยีสารสนเทศที่มีความสำคัญสูง ระบบงานที่มีการใช้งานในสถานที่ที่มีความเสี่ยง (ในที่สาธารณะหรือพื้นที่ภายนอกหน่วยงาน) มีการจำกัดช่วงระยะเวลาการเชื่อมต่อ

ส่วนที่ ๙ การควบคุมการเข้าโปรแกรมประยุกต์ หรือ แอปพลิเคชัน และระบบสารสนเทศ (Application and Information access control)

๙.๑ การติดตั้งหรือปรับปรุงซอฟต์แวร์ของระบบงานอยู่ในความรับผิดชอบของผู้ดูแลระบบ และจะต้องขออนุมัติจากหัวหน้าฝ่ายเทคโนโลยีสารสนเทศ หรือหัวหน้าหน่วยงานที่ดูแลรับผิดชอบ ก่อนดำเนินการปรับปรุงตามกระบวนการบริหารการเปลี่ยนแปลง (Change Management)

๙.๒ กำหนดให้ผู้ดูแลระบบมีการจัดเก็บซอร์สโค้ด (Source Code), ไลบรารี (Library) และเอกสารสำหรับซอฟต์แวร์ของระบบงานไว้ใน Server และมีการสำรองข้อมูลจัดเก็บไว้เพื่อป้องกันการสูญหาย เสียหาย หรือ ถูกทำลาย

๙.๓ องค์กรให้ความสำคัญต่อเรื่องทรัพย์สินทางปัญญา ซอฟต์แวร์ที่ใช้ภายในองค์กร เป็นซอฟต์แวร์ที่มีลิขสิทธิ์ และห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากมีการตรวจสอบพบความผิดฐานละเมิดลิขสิทธิ์ ถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงผู้เดียว

๙.๔ คอมพิวเตอร์ของผู้ใช้งานติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ (Antivirus) และอัปเดตอย่างสม่ำเสมอตามที่ฝ่ายเทคโนโลยีสารสนเทศจัดไว้ให้ และต้องเปิดใช้งานโปรแกรมดังกล่าวตามปกติ

๙.๕ ผู้ดูแลระบบ รับผิดชอบในการปรับปรุงข้อมูล สำหรับตรวจสอบและปรับปรุงระบบปฏิบัติการ (Update patch) ให้ทันสมัยเสมอ เพื่อเป็นการป้องกันความเสียหายที่อาจเกิดขึ้น

๙.๖ เมื่อผู้ใช้งานพบว่าเครื่องคอมพิวเตอร์มีการทำงานผิดปกติ หรือมีแนวโน้มติดไวรัส ผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์เข้าสู่ระบบเครือข่าย และต้องแจ้งแก่ผู้ดูแลระบบทันที

๙.๗ ห้ามทำการเผยแพร่ไวรัสคอมพิวเตอร์ มัลแวร์ หรือโปรแกรมอันตรายใด ๆ ที่อาจก่อให้เกิดความเสียหายมาสู่สินทรัพย์ขององค์กร

๙.๘ กรณีพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก (Outsourced Software Development) ต้องมีการควบคุมดังนี้

๑) จัดให้มีการควบคุมโครงการพัฒนาซอฟต์แวร์โดยผู้รับจ้างให้บริการจากภายนอก ตามกระบวนการจัดซื้อ จัดจ้างภาครัฐ

๒) ซอฟต์แวร์ที่จ้างหน่วยงานภายนอกพัฒนา ถือว่าองค์กรเป็นผู้มีสิทธิ์ในทรัพย์สินทางปัญญาสำหรับซอฟต์แวร์ที่พัฒนานั้น

๓) พิจารณากำหนดเรื่องการสงวนสิทธิ์ที่จะตรวจสอบด้านคุณภาพและความถูกต้องของซอฟต์แวร์ที่จะมีการพัฒนาโดยผู้ให้บริการภายนอก โดยระบุไว้ในสัญญาจ้างที่ทำกับผู้ให้บริการภายนอก

๔) ให้มีการตรวจสอบโปรแกรมไม่ประสงค์ดี ในซอฟต์แวร์ต่าง ๆ ที่จะทำการติดตั้งก่อนดำเนินการติดตั้งเพื่อใช้งาน

๕) หลังจากการส่งมอบการพัฒนาซอฟต์แวร์จากหน่วยงานภายนอก หน่วยงานต้องดำเนินการเปลี่ยนรหัสผ่านต่าง ๆ โดยทันที

๙.๙ องค์กรให้ความสำคัญต่อเรื่องทรัพย์สินทางปัญญา ดังนั้นซอฟต์แวร์ที่หน่วยงานอนุญาตให้ใช้งานหรือที่หน่วยงานมีลิขสิทธิ์ ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็น และห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากมีการตรวจสอบพบความผิดฐานละเมิดลิขสิทธิ์ ถือว่าเป็นความผิดส่วนบุคคลผู้ใช้งานจะต้องรับผิดชอบแต่เพียงผู้เดียว

๙.๑๐ ซอฟต์แวร์ (Software) ที่ได้จัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็นต่อการทำงานห้ามมิให้ผู้ใช้งานทำการ ถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่น ๆ

๙.๑๑ การใช้งานโปรแกรมอรรถประโยชน์ (Use of system Utilities) ต้องจำกัดและควบคุมการใช้งานโปรแกรมอรรถประโยชน์สำหรับโปรแกรมคอมพิวเตอร์ที่สำคัญ เนื่องจากการใช้งานโปรแกรมอรรถประโยชน์บางชนิด สามารถทำให้ผู้ใช้หลีกเลี่ยงมาตรการป้องกันทางด้านความมั่นคงปลอดภัยของระบบได้ เพื่อป้องกันการละเมิด หรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว ให้ดำเนินการ ดังนี้

๑) การใช้งานโปรแกรมอรรถประโยชน์ต้องได้รับการอนุมัติจากผู้ดูแลระบบ และต้องมีการพิสูจน์ ยืนยันตัวตนสำหรับการเข้าไปใช้งานโปรแกรมอรรถประโยชน์ เพื่อจำกัดและควบคุมการใช้งาน

๒) โปรแกรมอรรถประโยชน์ที่นำมาใช้งานต้องไม่ละเมิดลิขสิทธิ์

๓) ต้องจัดเก็บโปรแกรมอรรถประโยชน์ออกจากซอฟต์แวร์สำหรับระบบงาน

๔) มีการจำกัดสิทธิ์ผู้ที่ได้รับอนุญาตให้ใช้งานโปรแกรมอรรถประโยชน์

๕) ต้องยกเลิกหรือลบทิ้งโปรแกรมอรรถประโยชน์และซอฟต์แวร์ที่เกี่ยวข้องกับระบบงานที่ไม่มีความจำเป็นในการใช้งาน รวมทั้งต้องป้องกันไม่ให้ผู้ใช้งานสามารถเข้าถึงหรือใช้งานโปรแกรมอรรถประโยชน์ได้

ส่วนที่ ๑๐ การควบคุมการใช้จดหมายอิเล็กทรอนิกส์ (e-Mail)

๑๐.๑ แจ้งความประสงค์ขอใช้งานจดหมายอิเล็กทรอนิกส์ (e-Mail) ผ่านฝ่ายเทคโนโลยีสารสนเทศเพื่อส่งต่อไปยังสำนักเทคโนโลยีสารสนเทศและดิจิตอล สภากาชาดไทย เพื่อลงทะเบียนบัญชีผู้ใช้งานจดหมายอิเล็กทรอนิกส์ (e-Mail)

๑๐.๒ ฝ่ายเทคโนโลยีสารสนเทศ รับรหัสจดหมายอิเล็กทรอนิกส์ผู้ใช้งานจากสภากาชาดไทย ผ่าน e-mail เวลาใส่รหัสผ่านต้องไม่ปรากฏหรือแสดงรหัสผ่านออกมา แต่ต้องแสดงออกมาในรูปของสัญลักษณ์แทนตัวอักษรนั้น เช่น “x” หรือ “*” ในการพิมพ์แต่ละตัวอักษร

๑๐.๓ เมื่อได้รับรหัสผ่าน (Password) ครั้งแรกในการเข้าระบบจดหมายอิเล็กทรอนิกส์ (e-Mail) และเมื่อมีการเข้าสู่ระบบในครั้งแรกนั้น ให้เปลี่ยนรหัสผ่าน (Password) โดยทันที

๑๐.๔ ผู้ดูแลระบบ ต้องกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิดได้ เช่น ไม่เกิน 3 ครั้ง

๑๐.๕ ไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์

๑๐.๖ เปลี่ยนรหัสผ่าน (Password) ทุก 180 วัน

๑๐.๗ หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (e-Mail) เสร็จสิ้นต้องลงบันทึกออก (Logout) ทุกครั้ง

๑๐.๘ การส่งข้อมูลที่เป็นความลับ ไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์ (e-Mail) เว้นเสียแต่ว่าจะใช้วิธีการเข้ารหัสข้อมูล e-Mail ที่หน่วยงานกำหนดไว้ให้ใช้ความระมัดระวังในการระบุชื่อที่อยู่ e-Mail ของผู้รับให้ถูกต้อง เพื่อป้องกันการส่งผิดตัวผู้รับ

๑๐.๙ ห้ามส่ง e-Mail ที่มีลักษณะเป็นจดหมายขยะ (Spam Mail)

๑๐.๑๐ ห้ามส่ง e-Mail ที่มีลักษณะเป็นจดหมายลูกโซ่ (Chain Letter)

๑๐.๑๑ ห้ามส่ง e-Mail ที่มีลักษณะเป็นการละเมิดต่อกฎหมาย หรือสิทธิของบุคคลอื่น

๑๐.๑๒ ห้ามส่ง e-Mail ที่มีไวรัสไปให้กับบุคคลอื่นโดยเจตนา

๑๐.๑๓ ให้ระบุชื่อของผู้ส่งใน e-Mail ทุกฉบับที่ส่งไป

๑๐.๑๔ ให้ทำการสำรองข้อมูล e-Mail ตามความจำเป็นอย่างสม่ำเสมอ (แม้ว่าหน่วยงานจะทำการสำรองข้อมูล e-Mail ไว้ให้แต่ก็เพียงช่วงระยะเวลาหนึ่งเท่านั้น ดังนั้น e-Mail ที่เก่ามาก ๆ และจำเป็นต้องใช้งานจึงมีความจำเป็นต้องสำรองเก็บไว้ด้วยตนเอง)

๑๐.๑๕ ผู้ใช้งานต้องทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนการเปิดเพื่อตรวจสอบไฟล์โดยใช้โปรแกรมป้องกันไวรัส เป็นการป้องกันในการเปิดไฟล์ที่เป็น Executable file เช่น .exe .com เป็นต้น

๑๐.๑๖ ผู้ใช้งานต้องไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

๑๐.๑๗ ผู้ใช้งานต้องใช้ข้อความที่ไม่สุภาพหรือรับส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสม ข้อมูล อันอาจทำให้เสียชื่อเสียงของหน่วยงาน ทำให้เกิดความแตกแยกระหว่างหน่วยงาน ผ่านทางจดหมายอิเล็กทรอนิกส์

๑๐.๑๘ ผู้ใช้งานต้องตรวจสอบกล่องจดหมายอิเล็กทรอนิกส์ (Inbox) ของตนเองทุกวัน และควรจัดเก็บ แฟ้มข้อมูลและจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจำนวนน้อยที่สุด และควรลบ จดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบ เพื่อลดปริมาณการใช้เนื้อที่ระบบจดหมายอิเล็กทรอนิกส์

๑๐.๑๙ ข้อควรระวัง ผู้ใช้งานควรโอนย้ายจดหมายอิเล็กทรอนิกส์ที่จะใช้อ้างอิงภายหลังมายังเครื่องคอมพิวเตอร์ของตน เพื่อเป็นการป้องกันผู้อื่นแอบอ่านจดหมายได้ ดังนั้นไม่ควรจัดเก็บข้อมูล หรือจดหมายอิเล็กทรอนิกส์ที่ไม่ได้ใช้แล้วไว้ในกล่องจดหมายอิเล็กทรอนิกส์ (Inbox)

๑๐.๒๐ ผู้ใช้งานต้องใช้จดหมายอิเล็กทรอนิกส์ภาครัฐ สำหรับใช้รับ-ส่งข้อมูลในระบบราชการตามมติคณะรัฐมนตรีเมื่อวันที่ ๑๙ ธันวาคม ๒๕๕๐ เรื่อง การพัฒนาระบบจดหมายอิเล็กทรอนิกส์ กลางเพื่อการสื่อสารในภาครัฐ

ส่วนที่ ๑๑ การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

๑๑.๑ ผู้ดูแลระบบ ต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point) ให้รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายน้อยที่สุด

๑๑.๒ ผู้ดูแลระบบ ต้องทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่า โดยปริยาย (Default) มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณแบบไร้สาย (AccessPoint) มาใช้งานและกำหนดให้ซ่อน SSID (Service Set Identifier)

๑๑.๓ ผู้ดูแลระบบ ต้องกำหนดค่า Wireless Security เป็นแบบ WEP (Wired EquivalentPrivacy) หรือ WPA (Wi-Fi Protected Access) ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และอุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point) และกำหนดค่าให้ไม่แสดงชื่อระบบเครือข่ายไร้สาย

๑๑.๔ ผู้ดูแลระบบ เลือกใช้วิธีการควบคุม MAC Address (Media Access Control Address) และชื่อผู้ใช้งาน (Username) รหัสผ่าน (Password) ของผู้ใช้งานที่มีสิทธิ์ในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะอุปกรณ์ที่มี MAC address (Media Access Control Address) และชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ตามที่กำหนดไว้เท่านั้นให้เข้าใช้ระบบเครือข่ายไร้สายได้อย่างถูกต้อง

๑๑.๕ ผู้ดูแลระบบ ต้องมีการติดตั้งไฟร์วอลล์ (Firewall) ระหว่างระบบเครือข่ายไร้สายกับระบบเครือข่ายภายในหน่วยงาน

๑๑.๖ ผู้ใช้งานที่ประสงค์ ใช้งานในระบบเครือข่ายไร้สายติดต่อสื่อสารกับเครือข่ายภายในหน่วยงานผ่านทาง VPN (Virtual Private Network) ต้องขออนุมัติใช้งานเป็นลายลักษณ์อักษรต่อ หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ หรือหัวหน้าหน่วยงานที่มีหน้าที่ดูแลรับผิดชอบ เพื่อเปิดการให้บริการและควบคุมการให้บริการในช่วงเวลาที่กำหนด เพื่อช่วยป้องกันการบุกรุกในระบบเครือข่าย

๑๑.๗ ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์ Firewall จะต้องส่งค่าไปจัดเก็บที่อุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ โดยจะต้องจัดเก็บข้อมูลจราจรไม่น้อยกว่า 90 วัน

๑๑.๘ การกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละส่วนของเครือข่ายจะต้องกำหนดค่าอนุญาตเฉพาะพอร์ตการเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น

๑๑.๙ ผู้ดูแลระบบสามารถระงับหรือบล็อกการใช้งานของเครื่องคอมพิวเตอร์ลูกข่ายที่มีพฤติกรรมการใช้งานที่ผิดนโยบาย หรือเกิดจากการทำงานของโปรแกรมที่มีความเสี่ยงต่อความปลอดภัยจนกว่าจะได้รับการแก้ไข

๑๑.๑๑ การเชื่อมต่อในลักษณะของการ Remote Login จากภายนอกมายังเครื่องแม่ข่ายหรืออุปกรณ์เครือข่ายภายใน จะต้องบันทึกรายการของการดำเนินการตามแบบการขออนุญาตดำเนินการ เกี่ยวกับเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย และจะต้องได้รับความเห็นชอบจากหัวหน้าฝ่ายเทคโนโลยีสารสนเทศ หรือหัวหน้าหน่วยงานที่ดูแลรับผิดชอบ

ส่วนที่ ๑๒ การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล (Personal Computer)

๑๒.๑ แนวทางปฏิบัติการใช้งานทั่วไป

๑) เครื่องคอมพิวเตอร์ที่หน่วยงานอนุญาตให้ใช้งาน เป็นสินทรัพย์ของหน่วยงานในองค์กร

๒) โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของหน่วยงานต้องเป็นโปรแกรมที่ถูกลิขสิทธิ์ ห้ามผู้ใช้งานคัดลอกโปรแกรมต่างๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัวหรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๓) ไม่อนุญาตให้ผู้ใช้งานทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์

๔) การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ส่วนบุคคลตรวจซ่อมจะต้องดำเนินการโดยเจ้าหน้าที่ของฝ่ายเทคโนโลยีสารสนเทศ หรือผู้รับจ้างเหมาบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้ทำสัญญากับองค์กรเท่านั้น

๕) ก่อนการใช้งานสื่อบันทึกพกพาต่างๆ ต้องมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัส

๖) ผู้ใช้งาน มีหน้าที่และรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์

๗) ปิดเครื่องคอมพิวเตอร์ส่วนบุคคลที่ตนเองครอบครองใช้งานอยู่เมื่อใช้งานประจำวันเสร็จสิ้นหรือเมื่อมีการยุติการใช้งานเกินกว่า ๑ ชั่วโมง

๘) ทำการตั้งค่า Screen Saver ของเครื่องคอมพิวเตอร์ที่ตนเองรับผิดชอบให้มีการล็อกหน้าจอหลังจากที่ไม่ได้ใช้งานเกินกว่าอย่างน้อย ๓๕ นาที เพื่อป้องกันบุคคลอื่นมาใช้งานที่เครื่องคอมพิวเตอร์

๙) ห้ามนำเครื่องคอมพิวเตอร์ส่วนตัวมาใช้กับระบบเครือข่ายขององค์กร ยกเว้นจะได้รับการตรวจสอบจากผู้ดูแลระบบ และขึ้นทะเบียนก่อนการใช้งาน

๑๒.๒ การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)

๑) ผู้ใช้งานต้องตรวจสอบหาไวรัสจากสื่อต่าง ๆ เช่น Flash Drive และ Data Storage อื่น ๆ ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์

๒) ผู้ใช้งานต้องตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัสก่อนใช้งาน

๓) ผู้ใช้งานต้องตรวจสอบข้อมูลคอมพิวเตอร์ใดที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ซึ่งมีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความ เสียหายถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่ กำหนดไว้

ส่วนที่ ๑๓ การใช้งานเครื่องคอมพิวเตอร์แบบพกพา (Notebook)

๑๓.๑ แนวทางปฏิบัติของการใช้งานทั่วไป

๑) เครื่องคอมพิวเตอร์แบบพกพาที่หน่วยงานอนุญาตให้ใช้งาน เป็นสินทรัพย์ของ หน่วยงาน เพื่อใช้ในงานราชการ

๒) โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์แบบพกพาของหน่วยงาน ต้องเป็นโปรแกรมที่ถูกลิขสิทธิ์ห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัวหรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๓) ผู้ใช้งานต้องศึกษาและปฏิบัติตามคู่มือการใช้งานอย่างละเอียด เพื่อการใช้งานอย่างปลอดภัยและมีประสิทธิภาพ และไม่ดัดแปลงแก้ไขส่วนประกอบต่าง ๆ ของคอมพิวเตอร์ และรักษาสภาพของคอมพิวเตอร์ให้มีสภาพเดิม

๔) การเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพา ต้องดำเนินการด้วยความระมัดระวัง และมีการป้องกันอันตรายที่เกิดจากการกระทบกระเทือน หลีกเลี่ยงการจับหน้าจอขณะขนย้าย ควรยกฐานเครื่องเมื่อต้องการเคลื่อนย้าย

๕) ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย เช่น ควรล็อกเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

๖) ผู้ใช้งานไม่เก็บหรือใช้งานคอมพิวเตอร์แบบพกพาในสถานที่ที่มีความร้อน/ความชื้น/ฝุ่นละอองสูง และต้องระวังป้องกันการตกกระทบ

๑๓.๒ การควบคุมการเข้าถึงระบบปฏิบัติการ ผู้ใช้งานต้องกำหนดชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์แบบพกพา และจัดเก็บไว้เป็นความลับ และ ล๊อกเอาท์ทันทีที่เลิกใช้งาน

ส่วนที่ ๑๔ การตรวจจับการบุกรุก (Intrusion Detection System/Intrusion Prevention System Policy:IDS/IPS)

๑๔.๑ IDS/IPS Policy เป็นนโยบายการติดตั้งระบบตรวจสอบการบุกรุก และตรวจสอบความปลอดภัยของเครือข่าย เพื่อป้องกันทรัพยากร ระบบสารสนเทศ และข้อมูลบนเครือข่ายภายในองค์กร ให้มีความมั่นคงปลอดภัย เป็นแนวทางการปฏิบัติเกี่ยวกับการตรวจสอบการบุกรุกเครือข่าย พร้อมกับบทบาทและความรับผิดชอบที่เกี่ยวข้อง

๑๔.๒ IDS/IPS Policy ครอบคลุมทุกโฮสต์ (Host) ในเครือข่ายของหน่วยงานและเครือข่ายข้อมูลทั้งหมด รวมถึงเส้นทางที่ข้อมูลอาจเดินทาง ซึ่งไม่อยู่ในเครือข่ายอินเทอร์เน็ตทุกเส้นทาง โฮสต์ (Host) และเครือข่ายทั้งหมดที่มีการส่งผ่านข้อมูลผ่าน IDS/IPS จะต้องมีการตรวจสอบและ Update Patch/Signature สม่ำเสมอ

๑๔.๓ ระบบทั้งหมดที่สามารถเข้าถึงได้จากอินเทอร์เน็ตหรือที่สาธารณะจะต้องผ่านการตรวจสอบจากระบบ IDS/IPS

๑๔.๔ พฤติกรรมการใช้งาน กิจกรรม หรือเหตุการณ์ทั้งหมด ที่มีความเสี่ยงต่อการบุกรุกการโจมตีระบบ พฤติกรรมที่น่าสงสัย หรือการพยายามเข้าระบบ ทั้งที่ประสบความสำเร็จและไม่ประสบ ความสำเร็จจะต้องมีการรายงานให้ผู้ดูแลระบบทราบทันทีที่ตรวจพบ

๑๔.๕ องค์กรสามารถยุติการเชื่อมต่อเครือข่ายของเครื่องคอมพิวเตอร์ที่มีพฤติกรรมเสี่ยงต่อการบุกรุกระบบ โดยไม่ต้องมีการแจ้งแก่ผู้ใช้งานล่วงหน้า

ส่วนที่ ๑๕ การจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log)

๑๕.๑ จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วน ถูกต้อง แท้จริง ระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้ และข้อมูลที่ใช้ในการจัดเก็บ ต้องกำหนดชั้นความลับในการเข้าถึง

๑๕.๒ ห้ามแก้ไขข้อมูลจราจรคอมพิวเตอร์ (Log) ที่เก็บรักษาไว้

๑๕.๓ กำหนดให้มีการบันทึกการทำงานของระบบบันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้า – ออกระบบบันทึกการพยายามเข้าสู่ระบบ เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกไว้อย่างน้อย ๙๐ วัน นับตั้งแต่การใช้งานสิ้นสุดลง โดยปฏิบัติตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

๑๕.๔ ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่าง ๆ และจำกัดสิทธิ์การเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

ส่วนที่ ๑๖ การเข้าถึงด้านกายภาพ สถานที่ และสภาพแวดล้อม (Physical Environment)

๑๖.๑ อาคาร สถานที่ และพื้นที่ใช้งานระบบสารสนเทศ หมายถึง ที่ซึ่งเป็นที่ตั้งของระบบคอมพิวเตอร์ระบบเครือข่าย หรือระบบสารสนเทศอื่น ๆ พื้นที่เตรียมข้อมูลจัดเก็บคอมพิวเตอร์และอุปกรณ์พื้นที่ปฏิบัติงานของบุคลากรทางคอมพิวเตอร์ รวมทั้งเครื่องคอมพิวเตอร์ส่วนบุคคลและอุปกรณ์ประกอบที่ติดตั้งประจำโต๊ะทำงาน

๑๖.๒ กำหนดให้ศูนย์ข้อมูลกลาง (Data Center) ต้องมีลักษณะดังนี้

๑) กำหนดเป็นเขตหวงห้ามเด็ดขาด หรือเขตหวงห้ามเฉพาะผู้ดูแลระบบที่ได้รับมอบหมาย ควบคุมการเข้าพื้นที่โดย finger scan และปิดล๊อกตลอดเวลา

๒) พื้นที่ที่ไม่ตั้งอยู่ในบริเวณที่มีการผ่านเข้า–ออก ของบุคคลเป็นจำนวนมาก และไม่มีป้ายหรือสัญลักษณ์ที่บ่งบอกถึงการมีระบบสำคัญอยู่ภายในสถานที่ดังกล่าว

๓) ไม่อนุญาตให้ถ่ายรูป หรือบันทึกภาพเคลื่อนไหวในบริเวณดังกล่าว

๔) ไม่ติดตั้ง หรือใช้เครื่องโทรสารหรือเครื่องถ่ายเอกสาร ให้ติดตั้งแยก ออกมาด้านนอก

๕) จัดพื้นที่สำหรับการส่งมอบผลิตภัณฑ์ โดยแยกจากบริเวณที่มีทรัพยากรสารสนเทศจัดตั้ง

ไว้ เพื่อป้องกันการเข้าถึงระบบจากผู้ไม่ได้รับอนุญาต

๖) กรณีที่ไม่ใช่ผู้ดูแลระบบ ต้องการเข้าพื้นที่ควบคุม จะต้องขออนุมัติเป็นลายลักษณ์อักษร ลงบันทึกการเข้า-ออกพื้นที่ทุกครั้ง และการปฏิบัติงานต้องอยู่ภายใต้การดูแลของผู้ดูแลระบบตลอดเวลาที่ปฏิบัติงาน

๑๖.๓ ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting Utilities)

๑) มีระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศของหน่วยงานที่เพียงพอต่อความต้องการใช้งานโดยให้มีระบบดังต่อไปนี้

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

๓) ให้มีการตรวจสอบหรือทดสอบระบบสนับสนุนตามแผนที่กำหนด

๔) ติดตั้งระบบแจ้งเตือน เพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงานภายในศูนย์ข้อมูลกลาง (Data Center) ทำงานผิดปกติหรือหยุดการทำงาน

๕) การเดินสายไฟ สายสื่อสาร และสายเคเบิลอื่น ๆ (Cabling Security)

- จัดทำผังสายสัญญาณ เพื่อให้สามารถวางแผนการตรวจสอบได้
- ให้มีการร้อยท่อสายสัญญาณ เพื่อป้องกันการดักจับสัญญาณ หรือสายสัญญาณได้รับความเสียหาย
- ให้เดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซงรบกวนของสัญญาณซึ่งกันและกัน
- สำรวจระบบสายสัญญาณสื่อสารสม่ำเสมอเพื่อตรวจหาการติดตั้งอุปกรณ์ดักจับสัญญาณโดยผู้ไม่ประสงค์ดี

๑๖.๔ การบำรุงรักษาอุปกรณ์ (Equipment Maintenance)

๑) ให้มีกำหนดการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่กำหนด

๒) จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้ง เพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง

๓) จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว

๔) จัดให้มีการอนุมัติสิทธิ์การเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญโดยผู้รับจ้างให้บริการจากภายนอก (ที่มาทำการบำรุงรักษาอุปกรณ์) เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๑๖.๕ การป้องกันอุปกรณ์ที่ใช้งานอยู่นอกหน่วยงาน (Security of Equipment Off-Premises)

๑) กำหนดมาตรการความปลอดภัยเพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์หรือทรัพย์สินของหน่วยงานออกไปใช้งาน เช่น การขนส่ง การเกิดอุบัติเหตุกับอุปกรณ์

๒) ไม่ทิ้งอุปกรณ์หรือทรัพย์สินของหน่วยงานไว้โดยลำพังในที่สาธารณะ

๓) เจ้าหน้าที่มีความรับผิดชอบดูแลอุปกรณ์หรือทรัพย์สินเสมือนเป็นทรัพย์สินของตนเอง

ส่วนที่ ๑๗ การบริหารจัดการการเปลี่ยนแปลง (Change Management)

๑๗.๑ การขอเปลี่ยนแปลง การตั้งค่าระบุรายละเอียดเหตุผลและความจำเป็นที่จะดำเนินกเปลี่ยนแปลงเป็นลายลักษณ์อักษร

๑๗.๒ จัดทำแผนดำเนินการเปลี่ยนแปลงการตั้งค่าที่จะเปลี่ยนแปลง

๑๗.๓ ทำการประเมินผลกระทบของการเปลี่ยนแปลงที่สำคัญเป็นลายลักษณ์อักษร ทั้งใน ด้านการปฏิบัติงาน (operation) ระบบรักษาความปลอดภัย (security) และการทำงาน (functionality) ของระบบงานที่เกี่ยวข้อง

๑๗.๔ จัดทำรายงานเมื่อดำเนินการเปลี่ยนแปลงการตั้งค่าเสร็จสิ้น

๑๗.๕ บันทึกการเปลี่ยนแปลงการตั้งค่าและจัดเก็บข้อมูลการตั้งค่าไว้

๑๗.๖ การแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ในกรณีฉุกเฉิน (emergency change) ต้องการบันทึกเหตุผลความจำเป็นและขออนุมัติจากผู้มีอำนาจหน้าที่ทุกครั้ง

๑๗.๗ การร้องขอให้มีการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ ต้องจัดทำให้เป็นลายลักษณ์อักษร (อาจเป็น electronic transaction เช่น email เป็นต้น) และได้รับอนุมัติจากผู้มีอำนาจหน้าที่ เช่น หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ, หัวหน้าหน่วยงานที่ดูแลรับผิดชอบ เป็นต้น

ส่วนที่ ๑๘ การทำสอบเจาะระบบเพื่อหาช่องโหว่ (Penetration Test)

๑๘.๑ ติดตั้งเครื่องมือที่ใช้ในการทดสอบและประเมินความเสี่ยงกับช่องโหว่ที่อาจเกิดขึ้นในระบบและหาวิธีการแก้ไขได้ล่วงหน้าก่อนจะเกิดเหตุการณ์ไม่พึงประสงค์

๑๘.๒ เมื่อเครื่องมือตรวจสอบพบช่องโหว่ในระบบสารสนเทศผู้ดูแลระบบต้องรายงานให้กับผู้รับผิดชอบและผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศทราบ โดยกำหนดลำดับความรุนแรงของความเสี่ยงที่อาจเกิดขึ้น

๑๘.๓ ผู้ดูและระบบกำหนดความเร่งด่วนในการแก้ไขปัญหาและจัดทำแผนดำเนินการให้ผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศและการสื่อทราบและอนุมัติการดำเนินการ

๑๘.๔ หากไม่มีการแก้ไขจากผู้รับผิดชอบตามกำหนดผู้ดูแลระบบสามารถระงับการให้บริการระบบสารสนเทศดังกล่าวได้ทันทีจนกว่าจะได้รับการแก้ไข

หมวด ๒ นโยบายการรักษาความปลอดภัยและระบบสำรองข้อมูล

วัตถุประสงค์

๑) เพื่อให้ระบบสารสนเทศของหน่วยงานสามารถให้บริการได้อย่างต่อเนื่อง

๒) เพื่อให้เป็นมาตรฐาน แนวทางปฏิบัติและความรับผิดชอบของผู้ดูแลระบบในการปฏิบัติงาน

๓) เพื่อให้ผู้ใช้งานได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ผู้รับผิดชอบ

๑) ผู้ดูแลระบบที่ได้รับมอบหมาย

๒) เจ้าหน้าที่ที่ได้รับมอบหมาย

๓) ผู้ใช้งาน

<u>แนวทางปฏิบัติ</u>

ส่วนที่ ๑ การรักษาความปลอดภัยฐานข้อมูล (Database Security)

๑.๑ กำหนดสิทธิ์และความสำคัญของข้อมูลและฐานข้อมูล

๑) จัดทำบัญชีฐานข้อมูล การจำแนกกลุ่มทรัพยากรของระบบหรือการทำงาน โดยให้กำหนดกลุ่มผู้ใช้งานและสิทธิของกลุ่มผู้ใช้งาน

๒) กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศที่เกี่ยวข้องกับการอนุญาตการกำหนดสิทธิ์ หรือการมอบอำนาจ ดังนี้

๒.๑ กำหนดสิทธิ์ของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง

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

๒.๒ กำหนดเกณฑ์การระงับสิทธิ์ การมอบอำนาจ ให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) ที่ได้กำหนดไว้

๒.๓ ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบที่ได้รับมอบหมาย

๓) ขั้นตอนปฏิบัติเพื่อการจัดเก็บข้อมูล

๓.๑ จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น ๓ ระดับ คือ

- ข้อมูลที่มีระดับความสำคัญมากที่สุด
- ข้อมูลที่มีระดับความสำคัญปานกลาง
- ข้อมูลที่มีระดับความสำคัญน้อย

๓.๒ จัดแบ่งลำดับชั้นความลับของข้อมูล

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

๓.๓ จัดแบ่งระดับชั้นการเข้าถึง

- ระดับชั้นสำหรับผู้บริหาร
- ระดับชั้นสำหรับผู้ใช้งานทั่วไป
- ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย

๑.๒ การปฏิบัติเกี่ยวกับข้อมูลที่เป็นความลับให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความลับทางราชการ พ.ศ. ๒๕๕๔ และแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศส่วนที่ ๒

๑.๓ หน่วยงานเจ้าของฐานข้อมูล ผู้มีสิทธิ์และอำนาจในสายงาน เป็นผู้พิจารณาคุณสมบัติของผู้ใช้งานและโปรแกรมที่ได้รับอนุญาตให้กระทำการใด ๆ กับข้อมูลนั้นได้ตามสิทธิและจัดให้มีแฟ้มลงบันทึกเข้า-ออก (Log File) การใช้งานสำหรับฐานข้อมูลตามความจำเป็น เพื่อประโยชน์ในการตรวจสอบความถูกต้องของการใช้งานฐานข้อมูล

๑.๔ ในกรณีฐานข้อมูลที่มีการใช้ร่วมกันระหว่างส่วนราชการ หรือแลกเปลี่ยน หรือขอใช้ข้อมูลจากส่วนราชการให้จัดทำข้อตกลงการใช้ข้อมูล หรือสำหรับการแลกเปลี่ยนสารสนเทศระหว่างหน่วยงานกับหน่วยงานภายนอก ดังต่อไปนี้

๑) กำหนดนโยบาย ขั้นตอนปฏิบัติ และมาตรฐานเพื่อป้องกันข้อมูลและสื่อบันทึกข้อมูลที่จะมีการขนย้ายหรือส่งไปยังอีกสถานที่หนึ่ง

๒) กำหนดหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องและขั้นตอนปฏิบัติในการใช้ข้อมูลร่วมกันหรือแลกเปลี่ยนข้อมูล เช่น วิธีการส่ง การรับ เป็นต้น

๓) กำหนดหน้าที่ความรับผิดชอบในการป้องกันข้อมูล

๔) กำหนดขั้นตอนปฏิบัติสำหรับตรวจสอบว่าใครเป็นผู้ส่งข้อมูลและใครเป็นผู้รับข้อมูล เพื่อเป็นการป้องกันการปฏิเสธ

๕) กำหนดความรับผิดชอบสำหรับกรณีที่ข้อมูลที่แลกเปลี่ยนกันเกิดการสูญหายหรือเกิดเหตุการณ์ความเสียหายอื่น ๆ กับข้อมูลนั้น

๖) กำหนดสิทธิ์การเข้าถึงข้อมูล

๗) กำหนดมาตรฐานทางเทคนิคที่ใช้ในการเข้าถึงข้อมูลหรือซอฟต์แวร์

๘) กำหนดมาตรการพิเศษสำหรับป้องกันเอกสาร ข้อมูล ซอฟต์แวร์ หรืออื่น ๆ ที่มีความสำคัญ เช่น กุญแจที่ใช้ในการเข้ารหัส เป็นต้น

ส่วนที่ ๒ การสำรองข้อมูล (Backup)

๒.๑ พิจารณาคัดเลือกระบบสารสนเทศที่สำคัญและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน โดยเรียงลำดับความจำเป็นมากไปน้อย

๒.๒ กำหนดหน้าที่และความรับผิดชอบของเจ้าหน้าที่ในการสำรองข้อมูล

๒.๓ มีการจัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของหน่วยงาน พร้อมทั้งกำหนดระบบสารสนเทศที่จะจัดทำระบบสำรอง และจัดทำระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ 1 ครั้ง

๒.๔ กำหนดให้มีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบ และกำหนดความถี่ในการสำรองข้อมูล หากระบบใดที่มีการเปลี่ยนแปลงบ่อยกำหนดให้มีความถี่ในการสำรองข้อมูลมากขึ้น โดยให้มีวิธีการสำรองข้อมูล ดังนี้

๑) กำหนดประเภทของข้อมูลที่ต้องทำการสำรองเก็บไว้ และความถี่ในการสำรอง

๒) กำหนดรูปแบบการสำรองข้อมูลให้เหมาะสมกับข้อมูลที่จะทำการสำรองข้อมูล

๓) บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการส ารองข้อมูล ได้แก่ ผู้ดำนินการ วัน/เวลาชื่อข้อมูลที่สำรอง สำเร็จ/ไม่สำเร็จ เป็นต้น

๔) ตรวจสอบการกำหนดค่า (Configuration) ต่าง ๆ ของระบบการสำรองข้อมูล

๕) จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูล และผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน

๖) จัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ ระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลสำรองกับหน่วยงานต้องห่างกันเพียงพอ เพื่อไม่ให้ส่งผลกระทบต่อข้อมูลที่จัดเก็บไว้นอก สถานที่นั้นในกรณีที่เกิดภัยพิบัติกับหน่วยงาน

๗) ดำเนินการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรองที่ใช้จัดเก็บข้อมูลนอกสถานที่

๘) ทดสอบบันทึกข้อมูลสำรองอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ

๙) ตรวจสอบและทดสอบประสิทธิภาพและประสิทธิผลของขั้นตอนปฏิบัติในการกู้คืนข้อมูลอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง หรือตามความเหมาะสมโดยคำนึงถึง ความเสี่ยงต่าง ๆ ที่จะเกิดขึ้น

๒.๕ ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดย

๑) ประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญเหล่านั้น และกำหนดมาตรการเพื่อลดความเสี่ยงเหล่านั้น เช่น ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว การชุมนุมประท้วงทำให้ไม่สามารถเข้ามาใช้ระบบงานได้ เป็นต้น

๒) กำหนดขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ ระยะเวลาเป้าหมายในการกู้คืนระบบทรัพยากรที่จำเป็น

๓) มีการกำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอก เช่น ผู้ให้บริการเครือข่าย ฮาร์ดแวร์ ซอฟต์แวร์ เป็นต้น เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อ

๔) การสร้างความตระหนัก หรือให้ความรู้แก่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติหรือสิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน เป็นต้น

๕) มีการทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ 1 ครั้ง

๖) ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง หรือตามความเหมาะสมโดยคำนึงถึงความเสี่ยงต่าง ๆ ที่จะเกิดขึ้น เพื่อให้ระบบมีสภาพพร้อมใช้งานอยู่เสมอ

หมวด ๓ นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

วัตถุประสงค์

๑) เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศหรือสถานการณ์ด้านความ มั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดได้

๒) เพื่อเป็นการป้องกันและลดระดับความเสี่ยงที่อาจจะเกิดขึ้นได้กับระบบสารสนเทศ

๓) เพื่อเป็นแนวทางในการปฏิบัติหากเกิดความเสี่ยงที่เป็นอันตรายต่อระบบสารสนเทศแนวปฏิบัติ

ผู้รับผิดชอบ

๑) ผู้ดูแลระบบที่ได้รับมอบหมาย

๒) เจ้าหน้าที่ที่ได้รับมอบหมาย

๓) ผู้ใช้งาน

แนวทางปฏิบัติ

ส่วนที่ ๑ การตรวจสอบและประเมินความเสี่ยง (Risk Assessment)

ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศหรือสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดได้ ที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ โดยผู้ตรวจสอบภายในของหน่วยงาน (Internal Auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) อย่างน้อยปีละ ๑ ครั้ง เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ โดยมีแนวทางในตรวจสอบและประเมินความเสี่ยง ดังนี้

๑) กำหนดเกณฑ์การประเมินความเสี่ยง (Risk Criteria)

๒) การประเมินความเสี่ยง (Risk Assessment)

๓) การจัดลำดับความสำคัญของความเสี่ยง (Risk Level)

๔) ค้นหาวิธีเพื่อลดความเสี่ยง และจัดทำแผนลดความเสี่ยง (Risk Treatment Plan)

๕) ติดตามความเสี่ยงที่ยังคงเหลือในระบบสารสนเทศ

๖) รายงานผลการประเมินความเสี่ยง ต่อที่ประชุมทบทวนฝ่ายบริหาร

หมวด ๔ นโยบายการสร้างความตระหนักด้านความปลอดภัยสารสนเทศ

วัตถุประสงค์

๑) เพื่อสร้างความรู้และเข้าใจในการใช้ระบบสารสนเทศแก่ผู้ใช้งาน และตระหนักถึงการใช้งานระบบสารสนเทศให้ปลอดภัย และเป็นไปตามที่กฎหมายกำหนด

๒) เพื่อป้องกัน และลดการกระทำความผิดที่เกิดขึ้นจากการใช้ระบบสารสนเทศด้วยความไม่ระวังหรือผิดวัตถุประสงค์

ผู้รับผิดชอบ

๑) ผู้ดูแลระบบที่ได้รับมอบหมาย

๒) เจ้าหน้าที่ที่ได้รับมอบหมาย

๓) ผู้ใช้งาน

แนวทางปฏิบัติ

๑) จัดกิจกรรมการอบรมสร้างความตระหนักแก่บุคลากรในโรงพยาบาลอย่างน้อยปีละ ๑ ครั้ง โดยมีรายละเอียดการอบรมสร้างความตระหนักในนโยบายความมั่นคงปลอดภัยด้านขององค์กร และมีการประเมินผลจากกิจกรรมดังกล่าว

๒) จัดกิจกรรมเสริมสร้างความรู้ ความเข้าใจ สม่ำเสมอ เช่น การเผยแพร่ข้อมูล ข่าวสารด้านความปลอดภัย ผ่านเว็บไซต์ หรือ Intranet ภายในองค์กร และมีการประเมินผลจากกิจกรรมดังกล่าว

๓) ติดตามประสิทธิภาพการนำนโยบายความมั่นคงปลอดภัยด้านสารสนเทศขององค์กร ผ่านกระบวนการตรวจติดตามภายใน (Internal Audit) และการติดตามอุบัติการณ์ (Incident) ที่เกิดขึ้นในระบบสารสนเทศ