ประกาศโรงพยาบาลปราสาท
เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
พ.ศ.๒๕๖๙

เพื่อให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของโรงพยาบาลปราสาท มีความมั่นคงปลอดภัย มีประสิทธิภาพและเชื่อถือได้สอดคล้องกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ตลอดจนเพื่อป้องกันภัยคุกคามที่อาจส่งผลกระทบต่อการให้บริการทางการแพทย์และข้อมูลส่วนบุคคลของผู้ป่วย โรงพยาบาลปราสาทจึงขอกำหนดนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ไว้ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า "ประกาศโรงพยาบาลปราสาท เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๙"

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศ เป็นต้นไป

ข้อ ๓ บรรดาประกาศ ระเบียบ คำสั่ง หรือแนวทางปฏิบัติอื่นใดที่ได้กำหนดไว้แล้ว ซึ่งขัดหรือแย้งกับประกาศนี้ให้ใช้ประกาศนี้แทน

ข้อ ๔ แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ประกอบด้วย

(๑) แนวนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
(๒) แนวปฏิบัติในการรักษาความปลอดภัยด้านสารสนเทศระดับผู้ใช้งาน
(๓) แนวปฏิบัติในการรักษาความปลอดภัยด้านสารสนเทศระดับผู้ดูแลระบบ
(๔) แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของบุคคลภายนอก

ข้อ ๕ ให้ผู้ใช้งาน ผู้ดูแลระบบ และบุคคลภายนอกที่ใช้ระบบเทคโนโลยีสารสนเทศของโรงพยาบาลปราสาท ปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศตามที่กำหนดในเอกสารแนบท้ายประกาศนี้

ผู้ฝ่าฝืนหรือไม่ปฏิบัติตามแนวนโยบายและแนวปฏิบัติตามวรรคหนึ่ง อาจถูกปฏิเสธหรือถูกระงับการใช้งานระบบเทคโนโลยีสารสนเทศของโรงพยาบาลปราสาท และต้องรับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายทั้งปวงที่เกิดขึ้นจากการฝ่าฝืนหรือไม่ปฏิบัตินั้น

ข้อ ๖ กรณีมีปัญหาเกี่ยวกับการปฏิบัติตามประกาศนี้ ให้ผู้อำนวยการเป็นผู้มีอำนาจวินิจฉัยชี้ขาด โดยอาจมอบคณะทำงานด้านการจัดการความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ โรงพยาบาลปราสาท พิจารณาเสนอความเห็นก่อนก็ได้

ประกาศ ณ วันที่ ๒๖ กุมภาพันธ์ ๒๕๖๙

(นางสาวชูหงส์ มหรรทัศนพงศ์)
ผู้อำนวยการโรงพยาบาลปราสาท

เอกสารแนบท้ายประกาศโรงพยาบาลปราสาท
เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
พ.ศ. ๒๕๖๙

หลักการและเหตุผล

พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.๒๕๔๙ มาตรา ๕ กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคง ปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐ หรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ ประกอบกับประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ กำหนดให้หน่วยงานของรัฐต้องจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร โดยข้อ ๑๔ กำหนดให้หน่วยงานของรัฐต้องกำหนดความรับผิดชอบที่ชัดเจน กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติ ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยกำหนดให้ผู้บริหารระดับสูง ซึ่งมีหน้าที่ดูแลรับผิดชอบ ด้านสารสนเทศของหน่วยงานของรัฐเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น และประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคง ปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ (ฉบับที่ ๒) พ.ศ. ๒๕๕๖ ซึ่งมีการปรับปรุงนโยบายและแนวปฏิบัติ ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐให้สอดคล้องกับมาตรฐานสากล โดยให้ยกเลิกความในข้อ ๑๔ ของประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติ ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ และให้ใช้ความต่อไปนี้แทน “ข้อ ๑๔ หน่วยงานของรัฐต้องกำหนดความรับผิดชอบที่ชัดเจน กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศ เกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ทั้งนี้ ให้ผู้บริหารระดับสูงสุดของหน่วยงาน(Chief Executive Officer : CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น” ดังนั้น เพื่อให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของโรงพยาบาลเป็นไปอย่างเหมาะสมมีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินงาน ได้อย่างต่อเนื่องรวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารในลักษณะที่ไม่ถูกต้อง และการถูกคุกคามจากภัยต่างๆ จึงเห็นสมควรให้กำหนดแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร

วัตถุประสงค์

แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของโรงพยาบาลปราสาท มีวัตถุประสงค์ ดังนี้

๑. เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศ หรือเครือข่ายคอมพิวเตอร์ของโรงพยาบาล ให้สามารถดำเนินงานได้อย่างมีประสิทธิภาพและเกิดประสิทธิผล ธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non-repudiation) และความน่าเชื่อถือ (Reliability)

๒. เพื่อกำหนดขอบเขตในการบริหารจัดการความมั่นปลอดภัยระบบเทคโนโลยีสารสนเทศให้สอดคล้องกับมาตรฐาน ISO/IEC ๒๗๐๐๑ หรือมาตรฐานอื่น ๆ ที่เกี่ยวข้องให้เป็นปัจจุบันและมีการปรับปรุงอย่างต่อเนื่อง

๓. เพื่อให้มีการสำรองข้อมูลสารสนเทศอย่างสม่ำเสมอ และมีแผนเตรียมความพร้อมในกรณีฉุกเฉินให้ระบบสารสนเทศใช้งานได้อย่างต่อเนื่องพร้อมใช้งานอยู่เสมอได้ตามปกติ เหมาะสมและสอดคล้องกับการใช้งานตามภารกิจของโรงพยาบาล

๔. เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีปฏิบัติให้แก่ผู้ใช้งาน ผู้ดูแลระบบ และบุคคลภายนอก ที่ปฏิบัติงานให้แก่โรงพยาบาล

๕. เพื่อให้ผู้ใช้งาน ผู้ดูแลระบบ และบุคคลภายนอกที่ปฏิบัติงานให้แก่โรงพยาบาล ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศของโรงพยาบาล รับทราบและถือปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศนี้อย่างเคร่งครัด

องค์ประกอบ

แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ถือเป็นส่วนหนึ่งในการกำหนดและควบคุมให้เป็นไปตามมาตรฐานทางด้านความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศของโรงพยาบาล ทั้งนี้ ผู้ใช้งาน ผู้ดูแลระบบ และบุคคลภายนอกจะต้องคำนึงถึงการควบคุมในส่วนต่าง ๆ ดังนี้

หมวด ๑ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
หมวด ๒ แนวปฏิบัติในการรักษาความปลอดภัยด้านสารสนเทศระดับผู้ใช้งาน
หมวด ๓ แนวปฏิบัติในการรักษาความปลอดภัยด้านสารสนเทศระดับผู้ดูแลระบบ
หมวด ๔ แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของบุคคลภายนอก

คำนิยามศัพท์

เว้นแต่จะกำหนดไว้เป็นอย่างอื่น คำนิยามศัพท์ในแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศนี้ ให้มีความหมาย ดังนี้

“นโยบาย” หมายความว่า หลักการเกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่โรงพยาบาลกำหนดขึ้นและประกาศใช้งาน ทั้งนี้ ตามที่กำหนดไว้ในเอกสารแนบท้ายฉบับนี้

“แนวปฏิบัติ” หมายความว่า ข้อปฏิบัติเกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่โรงพยาบาลกำหนดขึ้นและประกาศใช้งาน เพื่อให้ผู้ใช้งาน ผู้ดูแลระบบ และบุคคลภายนอกปฏิบัติตามโดยเคร่งครัด ทั้งนี้ ตามที่กำหนดไว้ในเอกสารแนบท้ายฉบับนี้

“โรงพยาบาล” หมายความว่า โรงพยาบาลปราสาท

“ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Officer: CEO)” หมายความว่า ผู้อำนวยการโรงพยาบาลปราสาท หรือผู้ที่ได้รับการแต่งตั้งให้ปฏิบัติงานแทน

“คณะกรรมการ” หมายความว่า คณะกรรมการสารสนเทศ ผู้มีอำนาจในการกำกับ ควบคุม ดูแล และบังคับใช้นโยบายด้านเทคโนโลยีสารสนเทศของโรงพยาบาล

"คณะทำงาน" หมายความว่า คณะทำงานพัฒนาระบบบริหารจัดการด้านความปลอดภัยสารสนเทศที่ทำหน้าที่จัดทำ ทบทวน ตรวจสอบ ประเมินผล และปรับปรุงแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้เป็นไปตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ว่าด้วยมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยหรือตามมาตรฐานสากล ในการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ

"ผู้บังคับบัญชา" หมายความว่า ผู้มีอำนาจสั่งการตามโครงสร้างส่วนงานขึ้นตรงผู้อำนวยการโรงพยาบาล

"ผู้ดูแลระบบ (System Administrator)" หมายความว่า เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาหรือจัดการระบบคอมพิวเตอร์และระบบเครือข่ายไม่ว่าส่วนงานใดส่วนงานหนึ่ง

"ผู้พัฒนาระบบ" หมายความว่า เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบพัฒนาโปรแกรมประยุกต์ที่ใช้งานภายในโรงพยาบาล

"ผู้ใช้งาน" หมายความว่า เลขาธิการ ผู้ปฏิบัติงานของโรงพยาบาลหรือ เจ้าหน้าที่ บุคคลภายใต้การควบคุมดูแลของผู้ให้บริการภายนอกที่ปฏิบัติหน้าที่ตามสัญญาจ้าง เจ้าหน้าที่ของรัฐซึ่งมาปฏิบัติงานในโรงพยาบาลตามมติคณะรัฐมนตรี และรวมถึงพนักงานจ้างเหมาบริการ ทั้งที่เป็นบุคคลธรรมดาหรือนิติบุคคล

"หน่วยงานภายนอก" หมายความว่า หน่วยงานของรัฐตามมาตรา ๔ แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ และที่แก้ไขเพิ่มเติม ที่เข้ามาทำการเชื่อมต่อระบบเทคโนโลยีสารสนเทศ หรือนำข้อมูลสารสนเทศของโรงพยาบาลไปใช้ประโยชน์ต่อการบริการต่างๆ

"บุคคลภายนอก" หมายความว่า ผู้ที่เข้ามาติดต่อ ประสานงาน หรือดำเนินงานที่เกี่ยวข้องกับโรงพยาบาลที่อยู่นอกเหนือในส่วนผู้ใช้งาน

"ผู้ตรวจสอบระบบสารสนเทศของโรงพยาบาล (IT Auditor)" หมายความว่า ผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่ตรวจสอบการดำเนินงานที่เกี่ยวกับระบบสารสนเทศ ตรวจสอบข้อมูลจราจรทางคอมพิวเตอร์ (Log) และอื่น ๆ ที่ร้องขอเพื่อใช้ในการตรวจสอบ

"ระบบสารสนเทศ (Information System)" หมายความว่า ระบบงานของโรงพยาบาลที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่โรงพยาบาลสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร

"โปรแกรมประเภทอรรถประโยชน์ (Utility Program/Software)" หมายความว่า โปรแกรมประยุกต์หรือแอปพลิเคชันที่ทำงานบนระบบปฏิบัติการ ที่มีคุณสมบัติการใช้งานนั้นค่อนข้างหลากหลาย ส่วนมากใช้เพื่อบำรุงรักษาและเพิ่มประสิทธิภาพการทำงานของคอมพิวเตอร์ช่วยสนับสนุน เพิ่ม หรือขยายขีดความสามารถของโปรแกรมที่ใช้งานให้มีประสิทธิภาพมากขึ้น

"ระบบซึ่งไวต่อการรบกวน (Sensitive or Critical System)" หมายความว่า ระบบเทคโนโลยีสารสนเทศที่มีความละเอียดอ่อนต่อการเก็บรวบรวม ใช้ หรือรักษาในส่วนของข้อมูลสารสนเทศ ที่เกี่ยวข้องกับประชาชน และเป็นระบบที่มีความสำคัญสูงต่อโรงพยาบาลที่ใช้ในการทำธุรกรรมต่างๆ

"สารสนเทศ (Information)" หมายความว่า ข้อเท็จจริงที่ได้จากการนำเข้าข้อมูลผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความหรือภาพกราฟิกให้เป็นระบบที่ผู้ใช้สามารถเข้าใจง่ายและสามารถนำไปใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ

"ข้อมูลสารสนเทศ" หมายความว่า ข้อมูล ข่าวสาร ความรู้ ข้อเท็จจริง ที่นำมาบันทึกไว้ ในทรัพยากรสารสนเทศของโรงพยาบาล ได้แก่ เอกสาร สื่อบันทึกข้อมูล ซึ่งผู้ใช้งาน ผู้ดูแลระบบ หรือบุคคลภายนอกที่ได้รับอนุญาตให้สามารถรับรู้สารสนเทศจากเอกสารและสื่อบันทึกข้อมูลนั้นได้

"ความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security)" หมายความว่า การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non-repudiation) และความน่าเชื่อถือ (Reliability)

"เหตุการณ์ด้านความมั่นคงปลอดภัย (Information Security Event)" หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

"สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information Security Incident)" หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or Unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม โดยในที่นี้เรียกว่า "อุบัติการณ์"

"เวลาอ้างอิงสากล (Stratum o)" หมายความว่า การเปรียบเทียบเวลาของเครื่องคอมพิวเตอร์แม่ข่ายที่ใช้ในการเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) กับเวลามาตรฐานสากล (ในประเทศไทยนั้นอ้างอิงกับหน่วยงานมาตรฐาน เช่น กรมอุทกศาสตร์กองทัพเรือ หรือศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ เป็นต้น) เพื่อให้สอดคล้องกับกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

"ข้อมูลจราจรทางคอมพิวเตอร์ (Log)" หมายความว่า ข้อมูลที่เกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง วันที่ ปริมาณ ระยะเวลา และชนิดของบริการอื่น ๆ ที่เกี่ยวข้องในการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

"การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ" หมายความว่า การอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศทั้งทางอิเล็กทรอนิกส์และทางกายภาพ โดยโรงพยาบาลจะเป็นผู้พิจารณา

"การถ่ายโอนข้อมูล" หมายความว่า การรับ–ส่งข้อมูลสารสนเทศจากเครื่องคอมพิวเตอร์หนึ่งไปยังเครื่องคอมพิวเตอร์อีกเครื่องหนึ่งที่ผ่านระบบเครือข่ายหรือผ่านสื่อบันทึกข้อมูล

"ระบบคอมพิวเตอร์" หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด เพื่อให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

"ระบบเครือข่าย" หมายความว่า ระบบที่สามารถใช้ในการติดต่อสื่อสาร หรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่างๆ ของโรงพยาบาลได้ เช่น ระบบเครือข่ายแบบมีสาย (LAN) และระบบเครือข่ายแบบไร้สาย (Wireless LAN)

"ระบบอินทราเน็ต (Intranet)" หมายความว่า ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่างๆ ภายในโรงพยาบาลเข้าด้วยกัน เป็นระบบเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลสื่อสารสนเทศภายในโรงพยาบาล

"ระบบเครือข่ายแบบไร้สาย (Wireless LAN)" หมายความว่า เทคโนโลยีในการติดต่อสื่อสารระหว่างเครื่องคอมพิวเตอร์ตั้งแต่ ๒ เครื่อง หรือกลุ่มของเครื่องคอมพิวเตอร์รวมถึงการติดต่อสื่อสารระหว่างเครื่องคอมพิวเตอร์กับอุปกรณ์เครือข่ายคอมพิวเตอร์ซึ่งการสื่อสารจะไม่ใช้สายสัญญาณในการเชื่อมต่อ (LAN) แต่จะใช้คลื่นวิทยุในการรับส่งข้อมูลแทน

"ระบบอินเทอร์เน็ต (Internet)" หมายความว่า ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่าง ๆ ของโรงพยาบาลเข้ากับเครือข่ายอินเทอร์เน็ตสากล

"ทรัพย์สินหรือสินทรัพย์ (Asset)" หมายความว่า สิ่งใดก็ตามที่มีคุณค่าสำหรับโรงพยาบาล เช่น ระบบคอมพิวเตอร์เครือข่าย ระบบคอมพิวเตอร์แม่ข่าย ระบบคอมพิวเตอร์ระบบสารสนเทศ ข้อมูลสารสนเทศ หรือซอฟต์แวร์ที่มีลิขสิทธิ์ เป็นต้น

"พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ" หมายความว่า พื้นที่ที่โรงพยาบาลอนุญาตให้มีการใช้งานระบบเทคโนโลยีสารสนเทศ โดยแบ่งเป็น

(๑) พื้นที่ทำงาน หมายความว่า พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคล และคอมพิวเตอร์แบบพกพาที่ประจำโต๊ะทำงานรวมถึงพื้นที่ทำงานของผู้ดูแลระบบ (System Administrator)

(๒) พื้นที่ควบคุม หมายความว่า พื้นที่ภายในห้องคอมพิวเตอร์ (DC) ห้องคอมพิวเตอร์สำรอง (DR) ที่ใช้สำหรับติดตั้งและจัดเก็บอุปกรณ์ระบบเทคโนโลยีสารสนเทศ ระบบเครือข่ายและข้อมูลคอมพิวเตอร์ของโรงพยาบาล

(๓) พื้นที่ใช้งานระบบเครือข่ายไร้สาย หมายความว่า พื้นที่ในการให้บริการระบบเครือข่ายไร้สายที่อยู่ในพื้นที่ทำงานและพื้นที่ควบคุมของโรงพยาบาล

"เครื่องคอมพิวเตอร์" หมายความว่า เครื่องคอมพิวเตอร์แบบตั้งโต๊ะและเครื่องคอมพิวเตอร์แบบพกพาที่โรงพยาบาลจัดหาให้ หรือเครื่องคอมพิวเตอร์ส่วนบุคคลที่นำเข้ามาเพื่อใช้งานในโรงพยาบาลและต้องได้รับอนุมัติจากส่วนงานที่รับผิดชอบ

"สื่อบันทึกข้อมูล" หมายความว่า อุปกรณ์อิเล็กทรอนิกส์ที่ใช้ในการบันทึกหรือจัดเก็บข้อมูล เช่น Hard Drive หรือ Flash Drive หรือ Handy Drive หรือ Thumb Drive หรือ External Hard Drive

"จดหมายอิเล็กทรอนิกส์ (Electronic mail: e-mail)" หมายความว่า ระบบที่ผู้ใช้งานหรือผู้ดูแลระบบ ใช้ในการรับส่งข้อความระหว่างกันโดยผ่านระบบเครือข่าย ในการรับส่งข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย กราฟิก ภาพเคลื่อนไหว และเสียง โดยที่ผู้ใช้งานหรือผู้ดูแลระบบสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ ตามมาตรฐานที่ใช้ในการรับส่งข้อมูล ได้แก่ SMTP POP๓ และ IMAP

"สิทธิของผู้ใช้งาน" หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศ โดยโรงพยาบาลจะเป็นผู้พิจารณา

"บัญชีผู้ใช้บริการ (Account)" หมายความว่า รายชื่อผู้มีสิทธิใช้งานระบบคอมพิวเตอร์ระบบเครือข่าย ระบบจดหมายอิเล็กทรอนิกส์และระบบเทคโนโลยีสารสนเทศของโรงพยาบาล

"ชื่อผู้ใช้ (Username)" หมายความว่า ชุดของตัวอักษรหรือตัวเลข ที่ถูกกำหนดขึ้นเพื่อใช้ในการลงบันทึกเข้า (Login) ในระบบคอมพิวเตอร์ระบบเครือข่าย และระบบเทคโนโลยีสารสนเทศของโรงพยาบาลที่มีการกำหนดสิทธิการใช้งานไว้

"รหัสผ่าน (Password)" หมายความว่า ตัวอักษรหรืออักขระตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันบัญชีผู้ใช้บริการ เพื่อควบคุมการเข้าถึงระบบคอมพิวเตอร์ระบบเครือข่ายและระบบเทคโนโลยีสารสนเทศของโรงพยาบาล

"เลขที่อยู่ไอพี (IP Address)" หมายความว่า ตัวเลขประจำเครื่องที่ต่ออยู่ในระบบเครือข่าย ซึ่งเลขนี้ของแต่ละเครื่องจะต้องไม่ซ้ำกัน โดยประกอบด้วยชุดของตัวเลข ๔ ส่วน (IPv๔) หรือ ๘ ส่วน (IPv๖) แต่ละกลุ่มตัวเลขคั่นด้วยเครื่องหมายจุด (.) หรือเครื่องหมายทวิภาค (:)

"ลงบันทึกเข้า (Login)" หมายความว่า กระบวนการที่ผู้ใช้งาน ผู้ดูแลระบบ หรือบุคคลภายนอกต้องทำให้เสร็จสิ้นตามเงื่อนไขที่ตั้งไว้ เพื่อการเข้าใช้งานระบบคอมพิวเตอร์ระบบเครือข่าย และระบบเทคโนโลยี สารสนเทศของโรงพยาบาล ซึ่งปกติแล้วจะอยู่ในรูปแบบของการกรอกชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ให้ถูกต้อง

"ลงบันทึกออก (Logout)" หมายความว่า กระบวนการที่ผู้ใช้ทำเพื่อสิ้นสุดการใช้งานระบบคอมพิวเตอร์ระบบเครือข่ายและระบบเทคโนโลยีสารสนเทศของโรงพยาบาล

"โปรแกรมประสงค์ร้าย" หมายความว่า โปรแกรมคอมพิวเตอร์ชุดคำสั่ง และหรือข้อมูลอิเล็กทรอนิกส์ที่ได้รับการออกแบบขึ้นมาโดยมีวัตถุประสงค์เพื่อก่อกวนหรือสร้างความเสียหายไม่ว่าโดยตรงหรือโดยอ้อมแก่ระบบคอมพิวเตอร์หรือระบบเครือข่าย เช่น มัลแวร์ (Malware) เป็นต้น

"Non-Disclosure Agreement (NDA)" หมายความว่า สัญญาที่ทำขึ้นระหว่างโรงพยาบาลกับผู้ใช้งาน ผู้ดูแลระบบ หรือบุคคลภายนอกที่ได้รับอนุญาตให้สามารถรับรู้ข้อมูลสารสนเทศ เพื่อตกลงมิให้เปิดเผยเนื้อหาความรู้หรือข้อมูลใด ๆ ต่อบุคคลที่สาม

"Acceptable Use Policy (AUP)" หมายความว่า ข้อตกลงระหว่างผู้ใช้งาน ผู้ดูแลระบบ หรือบุคคลภายนอก ที่ยอมรับเงื่อนไขในส่วนของนโยบายและแนวปฏิบัติรักษาความปลอดภัยด้านสารสนเทศที่เกี่ยวข้อง

หมวด ๑ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ตามที่พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ มาตรา ๕ กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ กำหนดให้หน่วยงานของรัฐต้องจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร นั้น

เพื่อให้การดำเนินการใด ๆ ด้านเทคโนโลยีสารสนเทศ ของโรงพยาบาลมีความมั่นคงปลอดภัยและเชื่อถือได้ตลอดจนมีมาตรฐานเป็นที่ยอมรับในระดับสากล โรงพยาบาลจึงเห็นควรกำหนดนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศตามพระราชกฤษฎีกาและประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ดังกล่าวจึงกำหนดแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศสำหรับโรงพยาบาล และเพื่อให้ประชาชน หน่วยบริการ หรือผู้ใช้งานภายในระบบสารสนเทศของโรงพยาบาล มีความมั่นใจได้ว่าโรงพยาบาลจะไม่สนับสนุนหรือยินยอมให้มีการกระทำความผิดตามที่พระราชบัญญัติต่าง ๆ ที่เกี่ยวข้องกำหนด โดยกำหนดให้มีสาระสำคัญเพื่อการนำไปดำเนินงานด้านความมั่นคงปลอดภัยในโรงพยาบาล ดังนี้

๑.๑ การเข้าถึงและควบคุมการใช้งานสารสนเทศ

๑.๑.๑ โรงพยาบาลต้องควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล กำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง กำหนดเกี่ยวกับประเภทของข้อมูล ลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล รวมทั้งระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึง

๑.๑.๒ โรงพยาบาลต้องควบคุมให้มีการกำหนดสิทธิการใช้งานของผู้ใช้งานตามหน้าที่รับผิดชอบที่ได้รับมอบหมายรวมถึงการบริหารจัดการการเข้าถึงของผู้ใช้งาน เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผยการล่วงรู้หรือการลักลอบทำสำเนาข้อมูลสารสนเทศ และการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ

๑.๑.๓ โรงพยาบาลต้องทำการคัดเลือกผู้ปฏิบัติงานตามคุณสมบัติของตำแหน่งงานที่กำหนดไว้ในแต่ละตำแหน่ง รวมถึงต้องตรวจสอบเอกสาร ข้อมูล หรือบุคคลอ้างอิง ประวัติการทำงาน การศึกษา คุณสมบัติข้อมูลหลักฐานแสดงตนของผู้ปฏิบัติงาน

๑.๑.๔ โรงพยาบาลต้องดำเนินการฝึกอบรมการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศอย่างสม่ำเสมอ เพื่อสร้างความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศให้แกผู้ใช้งาน

๑.๑.๕ โรงพยาบาลต้องควบคุมการเข้าถึงเครือข่าย เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต

๑.๑.๖ โรงพยาบาลต้องควบคุมการเข้าถึงระบบปฏิบัติการ เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต

๑.๑.๗ โรงพยาบาลต้องควบคุมผู้ที่เกี่ยวข้องในกระบวนการบริหารจัดการการเปลี่ยนแปลงให้มีการแบ่งแยกหน้าที่อย่างเหมาะสม (segregation of duties) เพื่อไม่ให้บุคคลใดบุคคลหนึ่งสามารถปฏิบัติงานได้ตั้งแต่ต้นจนจบกระบวนการ เช่น ผู้มีสิทธิร้องขอ ผู้ที่มีอำนาจในการอนุมัติการเปลี่ยนแปลง ผู้ที่สามารถดำเนินการเปลี่ยนแปลงระบบ เป็นต้น

๑.๑.๘ โรงพยาบาลต้องควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศเพื่อป้องกันการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศโดยไม่ได้รับอนุญาต

๑.๒ การจัดทำระบบสำรองและแผนเตรียมความพร้อมกรณีฉุกเฉิน

โรงพยาบาลต้องจัดทำระบบสำรองและมาตรการควบคุม เพื่อลดความเสี่ยงต่อภัยคุกคามทางกายภาพที่เหมาะสมพร้อมทั้งอยู่ในสภาพพร้อมใช้งาน โดยคัดเลือกระบบสารสนเทศที่สำคัญและจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามการดำเนินงาน พร้อมทั้งต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง การจัดทำแผน เตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ให้มีการทดสอบสภาพ พร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉินอย่างสม่ำเสมอ

๑.๓ การตรวจสอบและประเมินความเสี่ยง

โรงพยาบาลต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยผู้ตรวจสอบภายในโรงพยาบาล (Internal Auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) เพื่อให้โรงพยาบาลได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

๑.๔ การจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

โรงพยาบาลต้องจัดให้มีแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานที่สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่ได้ประกาศใช้งานและดำเนินการประกาศนโยบายและแนวปฏิบัติดังกล่าวให้ผู้เกี่ยวข้องทั้งหมดทราบ เพื่อให้สามารถเข้าถึงเข้าใจและปฏิบัติตามนโยบายและแนวปฏิบัติได้ และต้องกำหนดผู้รับผิดชอบตามนโยบายและแนวปฏิบัติดังกล่าวให้ชัดเจน พร้อมทั้งต้องทบทวนปรับปรุงนโยบายและแนวปฏิบัติให้เป็นปัจจุบันอยู่เสมอ โดยนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่สมบูรณ์จะต้องลงนามโดยผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Officer : CEO) เท่านั้น และต้องจัดเก็บเอกสารภายใต้เอกสารควบคุมคุณภาพในหมวดประกาศแต่งตั้ง เพื่อให้สามารถเข้าถึงนโยบายการรักษาความมั่นคงปลอดภัยด้นสารสนเทศได้ตลอดเวลา โดยมาตรฐานดังกล่าวที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยสารสนเทศของโรงพยาบาล อาจมีการกำหนดหลักเกณฑ์ที่แตกต่างกันตามความจำเป็น แต่อย่างน้อยต้องมีการกำหนดเกี่ยวกับหลักเกณฑ์ ดังต่อไปนี้

๑.๔.๑ การรักษาความมั่นคงปลอดภัยของสารสนเทศ เพื่อให้มีการกำหนดทิศทางการบริหารจัดการและสนับสนุนความปลอดภัยสารสนเทศโดยสอดคล้องกับการดำเนินงานของโรงพยาบาลและกฎหมายระเบียบ หรือข้อบังคับที่เกี่ยวข้อง

๑.๔.๒ โครงสร้างความมั่นคงปลอดภัยสารสนเทศ เพื่อให้มีการกำหนดกรอบการบริหารจัดการโดยต้องมีการเริ่มต้นและควบคุมการปฏิบัติและการดำเนินการด้านความมั่นคงปลอดภัยสารสนเทศภายในโรงพยาบาล

๑.๔.๓ ความมั่นคงปลอดภัยสำหรับทรัพย์ากรบุคคล เพื่อให้ผู้ปฏิบัติงานของโรงพยาบาลปราสาทตั้งแต่เจ้าหน้าที่ ลูกจ้าง เจ้าหน้าที่ของรัฐซึ่งมาปฏิบัติงานในโรงพยาบาล ตามมติคณะรัฐมนตรี และรวมถึงพนักงานจ้างเหมาบริการทั้งที่เป็นบุคคลหรือนิติบุคคล บุคลากรภายใต้การควบคุมดูแล ของผู้ให้บริการภายนอกที่ปฏิบัติหน้าที่ตามสัญญาจ้าง ได้เข้าใจหน้าที่ความรับผิดชอบของตนเองและมีความเหมาะสมตามบทบาทหน้าที่ที่รับผิดชอบ

๑.๔.๔ การบริหารจัดการทรัพย์สิน เพื่อให้มีการระบุทรัพย์สินของโรงพยาบาลและกำหนดหน้าที่ความรับผิดชอบในการบริหารจัดการทรัพย์สินอย่างเหมาะสม

๑.๔.๕ การควบคุมการเข้าถึง เพื่อจำกัดการเข้าถึงระบบสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศของโรงพยาบาล ให้เกิดความปลอดภัยต่อการเข้าถึงระบบสารสนเทศ

๑.๔.๖ การเข้ารหัสข้อมูล เพื่อให้มีการใช้การเข้ารหัสข้อมูลอย่างเหมาะสมและป้องกันข้อมูลไว้ซึ่งความลับ ความถูกต้องของข้อมูล ป้องกันการปลอมแปลงหรือแก้ไขข้อมูลของโรงพยาบาล

๑.๔.๗ ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม เพื่อป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต ทำให้เกิดความเสียหายและแทรกแซงการทำงานที่มีผลต่อระบบสารสนเทศหรืออุปกรณ์ประมวลผลสารสนเทศของโรงพยาบาล และป้องกันการสูญหาย การเสียหายหรือส่งผลกระทบต่อการดำเนินงานของโรงพยาบาล

๑.๔.๘ ความมั่นคงปลอดภัยสำหรับการดำเนินงาน เพื่อให้การปฏิบัติงานกับระบบหรืออุปกรณ์ประมวลผลสารสนเทศเป็นไปอย่างถูกต้องและมั่นคงปลอดภัย ได้รับการป้องกันจากโปรแกรมกำจัดมัลแวร์ รวมถึงการป้องกันการสูญหายของข้อมูล การบันทึกเหตุการณ์และจัดทำหลักฐานต่าง ๆ ในการดำเนินการ

๑.๔.๙ ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล เพื่อให้มีการป้องกันข้อมูลสารสนเทศภายในระบบเครือข่ายในการถ่ายโอนข้อมูลภายในโรงพยาบาล และการถ่ายโอนข้อมูลกับหน่วยงานภายนอก

๑.๔.๑๐ การจัดหา การพัฒนา และการบำรุงรักษาระบบ เพื่อให้ความมั่นคงปลอดภัยสารสนเทศเป็นองค์ประกอบที่สำคัญในการพัฒนาระบบ ตั้งแต่กระบวนการออกแบบ กระบวนการจัดหา การพัฒนาระบบและการบำรุงรักษาระบบให้สามารถดำเนินการได้อย่างต่อเนื่อง

๑.๔.๑๑ ความสัมพันธ์กับผู้ให้บริการภายนอก เพื่อให้มีการรักษาไว้ซึ่งระดับความมั่นคงปลอดภัยและระดับการให้บริการตามที่ตกลงกันไว้ในข้อตกลงการให้บริการของผู้ให้บริการภายนอก และเพื่อป้องกันทรัพย์สินของโรงพยาบาลที่มีการเข้าถึงโดยผู้ให้บริการภายนอก

๑.๔.๑๒ การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ เพื่อให้มีวิธีการที่สอดคล้องกันและได้ผลสำหรับการบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ ซึ่งรวมถึงการแจ้งสถานการณ์ความมั่นคงปลอดภัยสารสนเทศและจุดอ่อนความมั่นคงปลอดภัยสารสนเทศให้ได้รับทราบและตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศที่ได้รับทราบ

๑.๔.๑๓ ประเด็นด้านความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการ เพื่อสร้างความต่อเนื่องของธุรกิจเพื่อวางแผนและจัดเตรียมความพร้อมในส่วนต่าง ๆ รวมถึงทำการตรวจสอบ ทบทวน และประเมินเหตุการณ์ผลกระทบที่จะส่งผลหรืออาจจะส่งผลให้เกิดความไม่ต่อเนื่องในการดำเนินธุรกิจ

๑.๔.๑๔ ความสอดคล้องต่อความต้องการด้านกฎหมาย ระเบียบ ข้อบังคับ เพื่อให้การดำเนินงานภายในโรงพยาบาลมีความสอดคล้องในด้านกฎหมายระเบียบข้อบังคับหรืออื่น ๆ ที่เกี่ยวข้องกับโรงพยาบาลที่ส่งผลต่อความมั่นคงปลอดภัยสารสนเทศ และทั้งที่เป็นความต้องการทางด้านความมั่นคงปลอดภัยสารสนเทศกฎหมาย ระเบียบ ข้อบังคับจากภายนอก โดยให้มีการทบทวนความไม่สอดคล้องอย่างสม่ำเสมอ

๑.๕ การรับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นกับระบบสารสนเทศของโรงพยาบาล

กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใด ๆ แก่โรงพยาบาล หรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Officer : CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหายหรืออันตรายที่เกิดขึ้นนั้น

๑.๖ การทบทวนแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ให้มีการทบทวนแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้นสารสนเทศให้เป็นปัจจุบัน อย่างน้อยปีละ ๑ ครั้ง

๑.๗ การปฏิบัติตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ให้ใช้แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยต้องคำนึงถึงหลักการพื้นฐานของการรักษาความลับ การรักษาความครบถ้วนและการรักษาสภาพความพร้อมใช้งานตามที่โรงพยาบาลประกาศใช้ล่าสุดและให้ผู้ใช้งาน ผู้ดูแลระบบ และบุคคลภายนอกที่ปฏิบัติงานให้แก่โรงพยาบาลลงนามในเอกสาร Non-Disclosure Agreement (NDA) กำหนดเงื่อนไขการจ้างงาน (Terms and Conditions of Employment) และ Acceptable Use Policy (AUP) ที่โรงพยาบาลกำหนดขึ้น เพื่อให้ผู้ใช้งานได้รับทราบและสามารถปฏิบัติตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศได้อย่างถูกต้อง

๑.๘ การรับมือภัยคุกคามทางไซเบอร์

๑.๘.๑ โรงพยาบาลต้องจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของโรงพยาบาล ซึ่งอย่างน้อยต้องประกอบด้วยเรื่อง ดังต่อไปนี้

(๑) แผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยผู้ตรวจประเมิน ผู้ตรวจสอบภายในหรือผู้ตรวจสอบอิสระจากภายนอก อย่างน้อยปีละ ๑ ครั้ง

(๒) แผนการรับมือภัยคุกคามทางไซเบอร์

๑.๘.๒ โรงพยาบาลมีหน้าที่ป้องกันรับมือและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของโรงพยาบาล

๑.๘.๓ โรงพยาบาลต้องกำหนดให้มีกลไกหรือขั้นตอนเพื่อการเฝ้าระวังภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ ที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศของโรงพยาบาล รวมถึงมีมาตรการที่ใช้แก้ปัญหาเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์

๑.๘.๔ เมื่อมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญต่อระบบของโรงพยาบาล ให้รายงานต่อคณะกรรมการที่กำกับดูแล และปฏิบัติการรับมือกับภัยคุกคามทางไซเบอร์ ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของโรงพยาบาล

๑.๘.๕ ในกรณีที่เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ต่อระบบสารสนเทศซึ่งอยู่ในความดูแลรับผิดชอบของโรงพยาบาล ให้ดำเนินการตรวจสอบข้อมูลที่เกี่ยวข้อง ข้อมูลคอมพิวเตอร์และระบบคอมพิวเตอร์รวมถึงพฤติการณ์แวดล้อมของตน เพื่อประเมินว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้นหรือไม่ หากผลการตรวจสอบปรากฏว่าเกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ขึ้น ให้ดำเนินการป้องกัน รับมือและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของโรงพยาบาล

๑.๘.๖ ในกรณีที่เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ซึ่งอยู่ในระดับร้ายแรง ให้ดำเนินการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์หรือระงับการดำเนินการใด ๆ เพื่อป้องกันและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ได้อย่างเหมาะสมและมีประสิทธิภาพ รวมทั้งร่วมกันบูรณาการในการดำเนินการเพื่อควบคุม ระงับ หรือบรรเทาผลที่เกิดจากภัยคุกคามทางไซเบอร์นั้นได้อย่างทันท่วงที และเมื่อภัยคุกคามทางไซเบอร์ดังกล่าวสิ้นสุดลงให้รายงานผลการดำเนินการต่อคณะกรรมการที่กำกับดูแลโดยเร็ว

๑.๘.๗ ในการรับมือและบรรเทาความเสียหายจากภัยคุกคามทางไซเบอร์ในระดับร้ายแรง คณะทำงานด้านความมั่นคงปลอดภัยทางไซเบอร์มีอำนาจออกคำสั่งเฉพาะเท่าที่จำเป็นเพื่อป้องกันภัยคุกคามทางไซเบอร์ให้บุคคลผู้เป็นเจ้าของกรรมสิทธิ์ ผู้ครอบครอง ผู้ใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือผู้ดูแลระบบคอมพิวเตอร์ซึ่งมีเหตุอันเชื่อได้ว่าเป็นผู้เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ หรือได้รับผลกระทบจากภัยคุกคามทางไซเบอร์ดำเนินการ ดังต่อไปนี้

(๑) เฝ้าระวังคอมพิวเตอร์หรือระบบคอมพิวเตอร์ในช่วงระยะเวลาใดระยะเวลาหนึ่ง

(๒) ตรวจสอบคอมพิวเตอร์หรือระบบคอมพิวเตอร์เพื่อหาข้อบกพร่องที่กระทบต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ วิเคราะห์สถานการณ์ และประเมินผลกระทบจากภัยคุกคามทางไซเบอร์

(๓) ดำเนินมาตรการแก้ไขภัยคุกคามทางไซเบอร์เพื่อจัดการข้อบกพร่องหรือกำจัดชุดคำสั่งไม่พึงประสงค์หรือระงับบรรเทาภัยคุกคามทางไซเบอร์ที่ดำเนินการอยู่

(๔) รักษาสถานะของข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ด้วยวิธีการใด ๆ เพื่อดำเนินการทางนิติวิทยาศาสตร์ทางคอมพิวเตอร์

(๕) เข้าถึงข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ที่เกี่ยวข้องเฉพาะเท่าที่จำเป็นเพื่อป้องกันภัยคุกคามทางไซเบอร์

หมวด ๒ แนวปฏิบัติในการรักษาความปลอดภัยด้านสารสนเทศระดับผู้ใช้งาน

๒.๑ การปฏิบัติหน้าที่ทั่วไป

๒.๑.๑ ผู้ใช้งานต้องไม่เปิดเผยข้อมูลอันเป็นความลับของโรงพยาบาล เว้นแต่จะได้รับอนุญาตจากโรงพยาบาล

๒.๑.๒ ผู้ใช้งานต้องให้ความร่วมมือในการเข้าร่วมการฝึกอบรมในลักษณะของการติดตามการเปลี่ยนแปลงของเทคโนโลยีด้านการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ เพื่อให้เกิดความตระหนักและมีความรู้เท่าทันเหตุการณ์ที่จะทำให้ละเมิดต่อนโยบายและแนวปฏิบัติในการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของโรงพยาบาล

๒.๑.๓ ผู้ใช้งานต้องให้ความร่วมมือในการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความปลอดภัยด้านสารสนเทศ หรือข้อกำหนดอื่นใดที่เกี่ยวข้องตามที่โรงพยาบาลได้จัดทำขึ้นตลอดจนให้ข้อเสนอแนะในการปรับปรุงให้มีประสิทธิภาพดีขึ้น

๒.๑.๔ ผู้ใช้งานต้องรักษาความลับและความมั่นคงปลอดภัยด้านสารสนเทศของโรงพยาบาล จากผู้ไม่ได้รับอนุญาตหรือไม่มีหน้าที่รับผิดชอบตามที่โรงพยาบาลกำหนด

๒.๑.๕ ผู้ใช้งานต้องดูแลรักษาป้องกันและใช้งานทรัพย์สินสารสนเทศของโรงพยาบาลอย่างถูกวิธี ทั้งทรัพย์สินในครอบครองและทรัพย์สินส่วนกลางตามมาตรการต่าง ๆ ที่กำหนดไว้ตามแนวปฏิบัติการใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่าย

๒.๑.๖ ผู้ใช้งานต้องปฏิบัติตามนโยบายในการคุ้มครองข้อมูลส่วนบุคคล ในการเข้าถึงข้อมูลการใช้ข้อมูลส่วนบุคคล และเมื่อมีความจำเป็นในการเข้าถึงข้อมูลส่วนบุคคลต้องเป็นไปตามสิทธิที่ได้รับมอบหมายตามหน้าที่รับผิดชอบที่โรงพยาบาลกำหนด

๒.๒ การใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่าย

๒.๒.๑ ผู้ใช้งานต้องใช้ระบบเทคโนโลยีสารสนเทศและอุปกรณ์การประมวลผลข้อมูลที่เกี่ยวข้องทั้งหมดที่โรงพยาบาลเป็นผู้จัดหามานั้นเพื่อประโยชน์ในการปฏิบัติงานตามภารกิจของโรงพยาบาล การใช้งานระบบและอุปกรณ์ต่าง ๆ เพื่อประโยชน์อย่างอื่นให้สามารถใช้ได้เท่าที่จำเป็นในขอบเขตที่จำกัดตามความเหมาะสม ซึ่งจะต้องไม่รบกวนหรือเป็นอุปสรรคต่อการทำงานในระบบสารสนเทศของโรงพยาบาล

๒.๒.๒ ผู้ใช้งานต้องไม่ใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายโดยมีวัตถุประสงค์ดังต่อไปนี้

(๑) โดยทุจริตหรือโดยหลอกลวงนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ที่บิดเบือนหรือปลอมไม่ว่าทั้งหมดหรือบางส่วนหรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ประชาชน

(๒) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายต่อการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคง ในทางเศรษฐกิจของประเทศหรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะของประเทศ หรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน

(๓) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

(๔) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันลามกและข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้

(๕) เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์โดยรู้อยู่แล้วว่าเป็นข้อมูลคอมพิวเตอร์ ตามข้อ ๒.๒.๒ (๑) - (๔)

(๖) นำเข้าสู่ระบบคอมพิวเตอร์ที่ประชาชนทั่วไปอาจเข้าถึงได้ซึ่งข้อมูลคอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติม หรือดัดแปลงด้วยวิธีการ ทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย หรือเป็นการกระทำต่อภาพของผู้ตาย และการกระทำนั้นน่าจะทำให้บิดา มารดา คู่สมรส หรือบุตรของผู้ตายเสียชื่อเสียง ถูกดูหมิ่น หรือถูกเกลียดชัง หรือได้รับความอับอาย ทั้งนี้ เว้นแต่เป็นการนำเข้าสู่ระบบคอมพิวเตอร์โดยสุจริตอันเป็นการติชมด้วยความเป็นธรรมซึ่งบุคคลหรือสิ่งใดอันเป็นวิสัยของประชาชนย่อมกระทำ

(๗) ผู้ใช้งานจะต้องไม่สนับสนุนหรือยินยอมให้มีการกระทำความผิดตามข้อ ๒.๒.๒ ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน

๒.๒.๓ ผู้ใช้งานต้องไม่กระทำการ ดังต่อไปนี้

(๑) เข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน

(๒) ล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะและนำมาตรการดังกล่าวไปเปิดเผยโดยมิชอบในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น

(๓) เข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน

(๔) กระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้ เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้

(๕) ทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วนซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ

(๖) กระทำด้วยประการใดโดยมิชอบ เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้

(๗) ส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์ (e-mail) แก่บุคคลอื่น โดยปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าวอันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข

(๘) จำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตามข้อ ๒.๒.๓ (๑) - (๗)

(๙) กระทำการตามข้อ ๒.๒.๓ (๑) (๒) (๓) (๔) และ (๗) ต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะความมั่นคง ในทางเศรษฐกิจของประเทศหรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ

(๑๐) ติดตั้งฮาร์ดแวร์หรือซอฟต์แวร์ใด ๆ ที่เกี่ยวข้องกับการให้บริการเครือข่าย เช่น Router, Switch, Hub Wireless access point หรืออื่น ๆ ที่ส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศ ของโรงพยาบาลในพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศโดยไม่ได้รับอนุญาต

๒.๒.๔ ผู้ใช้งานต้องปฏิบัติดังต่อไปนี้ สำหรับการใช้งานเครื่องคอมพิวเตอร์ระบบเครือข่ายและอุปกรณ์ต่อพ่วง

(๑) การนำเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ส่วนตัวมาเชื่อมต่อกับเครื่อง

คอมพิวเตอร์และระบบเครือข่ายของโรงพยาบาล ผู้ใช้งานจะต้องได้รับอนุญาตจากผู้บังคับบัญชาที่ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) แต่งตั้งให้มีบทบาทหน้าที่ในการอนุมัติในการร้องขอจากผู้ใช้งานที่จะนำเครื่องคอมพิวเตอร์ และอุปกรณ์คอมพิวเตอร์ส่วนตัวมาเชื่อมต่อกับเครื่องคอมพิวเตอร์และระบบเครือข่ายของโรงพยาบาลและต้องปฏิบัติตามนโยบายนี้โดยเคร่งครัด

(๒) ห้ามแก้ไขหรือซ่อมแซมทรัพย์สินสารสนเทศที่ชำรุดเสียหายด้วยตนเองโดยพลการหรือให้ผู้อื่นที่ไม่มีอำนาจหน้าที่ดำเนินการให้ กรณีที่มีความจำเป็นให้แจ้งส่วนงานขึ้นตรงเลขาธิการด้านดิจิทัลเป็นผู้ดำเนินการ

(๓) ห้ามมิให้นำอุปกรณ์สารสนเทศหรืออุปกรณ์สื่อสารทั้งแบบใช้สายและไม่ใช้สายนอกเหนือจากที่ผู้ดูแลระบบติดตั้งไว้เดิม มาเชื่อมต่อกับระบบสารสนเทศของโรงพยาบาลโดยมิได้รับอนุญาต กรณีที่มีความจำเป็นต้องใช้หรือเชื่อมต่อกับระบบสารสนเทศของโรงพยาบาล ให้แจ้งส่วนงานขึ้นตรงเลขาธิการด้านดิจิทัลเป็นผู้ดำเนินการ

(๔) การปฏิบัติงานกับอุปกรณ์เทคโนโลยีสารสนเทศ ผู้ใช้งานต้องปฏิบัติตามแนวปฏิบัติการป้องกันจากโปรแกรมประสงค์ร้าย (Malware)

(๕) กรณีทำงานที่บ้าน (Work From Home) ผู้ใช้งานต้องดูแลและรับผิดชอบอุปกรณ์คอมพิวเตอร์ของโรงพยาบาลที่ได้รับมอบหมายให้คงอยู่ในสภาพพร้อมใช้งานอยู่เสมอ

(๖) ใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายของโรงพยาบาลอย่างมีประสิทธิภาพและเกิดประโยชน์สูงสุดแก่โรงพยาบาล

(๗) ห้ามดัดแปลงหรือติดตั้งอุปกรณ์เพิ่มเติมใด ๆ ต่ออุปกรณ์คอมพิวเตอร์ของโรงพยาบาล เว้นแต่จะได้รับอนุญาตจากผู้บังคับบัญชาที่ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงแต่งตั้งให้มีบทบาทหน้าที่ในการอนุมัติการดัดแปลงหรือติดตั้งอุปกรณ์เพิ่มเติมนั้น ๆ

(๘) การใช้งานอุปกรณ์เคลื่อนที่แบบพกพา เช่น Notebook หรืออุปกรณ์สื่อสารอื่น ๆ ผู้ใช้งานจะต้องใช้ความระมัดระวังเป็นพิเศษเพื่อให้มั่นใจได้ว่าข้อมูลที่มีความสำคัญของโรงพยาบาลที่บันทึกอยู่ในอุปกรณ์นั้น ๆ จะไม่ถูกเปิดเผย เปลี่ยนแปลง แก้ไข หรือถูกทำลาย

(๙) ไม่ทำการเปลี่ยนแปลงหรือเพิ่มเติมหมายเลขที่อยู่ไอพี (IP Address) ของเครื่องคอมพิวเตอร์แบบตั้งโต๊ะและแบบพกพาภายในโรงพยาบาลโดยไม่ได้รับอนุญาต

(๑๐) ไม่ติดตั้งโปรแกรมคอมพิวเตอร์ที่สามารถใช้ในการตรวจสอบข้อมูลบนระบบเครือข่าย เว้นแต่จะได้รับอนุญาตจากส่วนงานขึ้นตรงเลขาธิการด้านดิจิทัล

(๑๑) ห้ามเคลื่อนย้าย ติดตั้งเพิ่มเติม หรือทำการใด ๆ ต่ออุปกรณ์ส่วนกลาง เช่น อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) หรืออุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลักโดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ (System Administrator)

๒.๒.๕ ผู้ใช้งานต้องให้ความร่วมมือกับโรงพยาบาลในการบำรุงรักษาอุปกรณ์สารสนเทศที่ใช้งานเป็นประจำอย่างน้อย ปีละ ๑ ครั้ง

๒.๓ การควบคุมเข้าถึงระบบปฏิบัติการ

๒.๓.๑ ผู้ใช้งานต้องกำหนดชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ในการใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ของโรงพยาบาล

๒.๓.๒ ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ของโรงพยาบาลร่วมกัน

๒.๓.๓ ผู้ใช้งานควรตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ (Screen Saver) เพื่อทำการล็อค

หน้าจอภาพเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้งานต้องใส่รหัสผ่าน (Password) เพื่อเข้าใช้งาน

๒.๓.๔ ผู้ใช้งานควรทำการลงบันทึกออก (Log out) ทันที เมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

๒.๓.๕ ผู้ใช้งานต้องปิดเครื่องคอมพิวเตอร์ที่ตนเองใช้งานอยู่เมื่อใช้งานประจำวันเสร็จสิ้นหรือเมื่อไม่มีการใช้งาน เว้นแต่เครื่องคอมพิวเตอร์นั้นเป็นเครื่องคอมพิวเตอร์แม่ข่ายให้บริการที่ต้องใช้งานตลอด ๒๔ ชั่วโมง

๒.๓.๖ ผู้ใช้งานต้องให้ความร่วมมือในการปฏิบัติตามข้อกำหนดที่ผู้ดูแลระบบกำหนดขึ้นตามแนวปฏิบัติในการรักษาความปลอดภัยด้านสารสนเทศอย่างเคร่งครัด เพื่อให้ระบบสารสนเทศของโรงพยาบาลมีความมั่นคงปลอดภัย

๒.๔ การใช้งานบัญชีผู้ใช้งาน (Account)

๒.๔.๑ ผู้ใช้งานที่เป็นเจ้าของบัญชีผู้ใช้งานต้องเป็นผู้รับผิดชอบในผลต่าง ๆ อันจะเกิดขึ้นจากการใช้บัญชีผู้ใช้งานของตนเองจากเครื่องคอมพิวเตอร์และระบบเครือข่าย เว้นแต่พิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

๒.๔.๒ ผู้ใช้งานต้องเก็บรักษาบัญชีผู้ใช้งานไว้เป็นความลับและห้ามเปิดเผยต่อผู้บุคคลอื่นห้ามโอนหรือจำหน่ายจ่ายแจกให้กับผู้อื่น

๒.๔.๓ ผู้ใช้งานต้องลงบันทึกการเข้าใช้ (Login) โดยบัญชีผู้ใช้งานของตนเองและทำการลงบันทึกออก (Logout) ทุกครั้ง เมื่อสิ้นสุดการใช้งานหรือหยุดการใช้งานชั่วคราว

๒.๕ การกำหนดรหัสผ่าน(Password) การเปลี่ยนรหัสผ่านและการใช้งานรหัสผ่าน

๒.๕.๑ รหัสผ่านควรมีความยาวไม่น้อยกว่า ๘ ตัวอักษร โดยผสมกันระหว่างตัวเลขและตัวอักษรภาษาอังกฤษที่เป็นตัวพิมพ์เล็กหรือตัวพิมพ์ใหญ่ ตัวอักขระพิเศษ (เช่น @ # $ %) และสัญลักษณ์ต่าง ๆ ด้วย

๒.๕.๒ ไม่ควรกำหนดรหัสผ่านจากข้อมูลส่วนตัว เช่น ชื่อหรือนามสกุลของผู้ใช้งาน ชื่อบุคคลในครอบครัว บุคคลที่มีความสัมพันธ์กับตนหรือคำศัพท์ที่ใช้ในพจนานุกรมหรือจากหมายเลขโทรศัพท์ หรือวันเดือนปีเกิด เป็นต้น

๒.๕.๓ เมื่อผู้ใช้งานได้รับรหัสผ่านจากระบบสารสนเทศหรือได้รับจากผู้ดูแลระบบ ให้ทำการเปลี่ยนรหัสผ่านทันทีเมื่อเข้าใช้งานระบบครั้งแรก และควรทำการเปลี่ยนรหัสผ่านทุก ๆ ๓ เดือน หรือเปลี่ยนรหัสผ่าน (Password) ทุกครั้งที่มีสัญญาณบอกเหตุว่าอาจรั่วไหล

๒.๕.๔ ผู้ใช้งานต้องเก็บรักษารหัสผ่านสำหรับการใช้งานเครื่องคอมพิวเตอร์และระบบสารสนเทศที่ได้มาโดยถือว่าเป็นความลับเฉพาะบุคคลและจะต้องไม่เปิดเผยหรือกระทำใดให้ผู้อื่นทราบ โดยมิได้รับอนุญาตจากผู้บังคับบัญชา

๒.๕.๕ ไม่ทำการบันทึกหรือเก็บรหัสผ่านไว้ในระบบคอมพิวเตอร์ เครื่องคอมพิวเตอร์หรือในรูปแบบอื่น ๆ ที่ไม่ได้ป้องกันการเข้าถึง

๒.๖ การป้องกันจากโปรแกรมประสงค์ร้าย (Malware)

๒.๖.๑ เครื่องคอมพิวเตอร์ที่ใช้งานภายในโรงพยาบาล หรือเครื่องคอมพิวเตอร์ที่ต้องการใช้ระบบเครือข่ายของโรงพยาบาล ต้องติดตั้งโปรแกรมกำจัดมัลแวร์ (Anti Malware) ที่โรงพยาบาลจัดหาหรืออนุญาต รวมทั้งทำการปรับปรุงให้ทันสมัยอยู่เสมอ

๒.๖.๒ ผู้ใช้งานควรทำการอัปเดต (Update) ระบบปฏิบัติการ เว็บเบราว์เซอร์ และโปรแกรมการใช้งานต่าง ๆ อย่างสม่ำเสมอ เพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟต์แวร์ อันเป็นการป้องกันการโจมตีจากภัยคุกคามต่างๆ ตามคำแนะนำที่ผู้ดูแลระบบจะแจ้งให้ทราบเป็นระยะ ๆ

๒.๖.๓ ห้ามมิให้ผู้ใช้งานปิดหรือยกเลิกหรือเปลี่ยนระบบการป้องกันโปรแกรมประสงค์ร้าย (Malware) ที่ติดตั้งอยู่บนเครื่องคอมพิวเตอร์โดยมิได้รับอนุญาตจากส่วนงานขึ้นตรงเฉขาธิการด้านดิจิทัล

๒.๖.๔ หากผู้ใช้งานพบหรือสงสัยว่าเครื่องคอมพิวเตอร์ติดโปรแกรมประสงค์ร้าย (Malware)

ห้ามมิให้ผู้ใช้งานเชื่อมต่อเครื่องคอมพิวเตอร์เข้ากับระบบเครือข่าย เพื่อป้องกันการแพร่กระจายของโปรแกรมประสงค์ร้าย (Malware) ไปยังเครื่องคอมพิวเตอร์เครื่องอื่น ๆ และให้แจ้งส่วนงานขึ้นตรงเลขาธิการด้านดิจิทัลเพื่อทำการแก้ไข

๒.๖.๕ ก่อนการใช้งานสื่อบันทึกพกพา ผู้ใช้งานควรมีการตรวจสอบเพื่อป้องกันและกำจัดโปรแกรมประสงค์ร้าย (Malware)

๒.๖.๖ ในการรับส่งข้อมูลคอมพิวเตอร์หรือสารสนเทศ (Information) ผ่านระบบเครือข่าย ผู้ใช้งานต้องทำการตรวจสอบเพื่อป้องกันและกำจัดโปรแกรมประสงค์ร้าย (Malware) ก่อนการรับส่งทุกครั้ง

๒.๖.๗ ผู้ใช้งานควรทำการตรวจสอบไฟล์ก่อนทำการเปิด โดยโปรแกรมป้องกันโปรแกรมประสงค์ร้าย (Anti Malware) อันเป็นการป้องกันในการเปิดไฟล์ที่สามารถประมวลผลได้ (Executable file) เช่น .inf .exe .com .bat .vbs .scr .pif .hta .txt.exe .doc.exe & .xls.exe เป็นต้น

๒.๗ การใช้ระบบอินเทอร์เน็ต (Internet)

๒.๗.๑ โรงพยาบาลจัดหาบริการอินเทอร์เน็ตไว้เพื่อสนับสนุนการดำเนินงานและอำนวยความสะดวกให้แก่ผู้ใช้งาน ผู้เข้าร่วมประชุม และบุคคลภายนอก เพื่อเพิ่มประสิทธิภาพในการทำงานและการให้บริการของโรงพยาบาล

๒.๗.๒ ผู้ใช้งานต้องใช้งานอินเทอร์เน็ตด้วยความระมัดระวัง และการใช้งานนั้นต้องไม่เป็นสาเหตุให้โรงพยาบาลและบุคคลผู้ที่เกี่ยวข้องกับโรงพยาบาลเสื่อมเสียชื่อเสียง หรือเกี่ยวพันกับการกระทำที่ผิดกฎหมาย ทั้งนี้ การใช้งานอินเทอร์เน็ตในทางที่ผิดถือเป็นความผิดทางวินัยและอาจถูกดำเนินคดีตามกฎหมายได้

๒.๗.๓ การเข้าใช้งานอินเทอร์เน็ตต้องเข้าใช้งานผ่านช่องทาง (Gateway) ที่ได้รับอนุญาต ทั้งนี้ โรงพยาบาลขอสงวนสิทธิ์ในการตรวจสอบการใช้งานอินเทอร์เน็ตของผู้ใช้งาน เพื่อตรวจสอบการใช้งานในลักษณะที่ไม่เหมาะสม

๒.๗.๔ ผู้ใช้งานควรใช้ความระมัดระวังในการคลิกหน้าต่างโฆษณาแบบป๊อปอัพ หรือเข้าสู่ เว็บไซต์ใด ๆ ที่โฆษณาโดยสแปม เนื่องจากเว็บไซต์เหล่านี้อาจมีโปรแกรมประสงค์ร้าย (Malware) แฝงอยู่หรืออาจโจรกรรมข้อมูลในเครื่องคอมพิวเตอร์ของผู้ใช้งาน โดยที่ผู้ใช้งานไม่ได้รับทราบหรือไม่ได้อนุญาต

๒.๗.๕ ผู้ใช้งานควรใช้ความระมัดระวังในการเข้าชม ดาวน์โหลด ทำซ้ำสื่อลามกอนาจารหรือสื่ออื่นใดที่ไม่เหมาะสมหรือขัดต่อกฎหมาย

๒.๗.๖ ผู้ใช้งานต้องใช้ความระมัดระวังในการดาวน์โหลดโปรแกรมใช้งานจากระบบ อินเทอร์เน็ต (Internet) ซึ่งรวมถึงการดาวน์โหลดอัปเดต (Update) โปรแกรมต่างๆ ต้องเป็นไปโดยไม่ละเมิด ลิขสิทธิ์หรือทรัพย์สินทางปัญญาของผู้อื่น

๒.๗.๗ ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ผู้ใช้งานต้องไม่เสนอความคิดเห็นที่ใช้ข้อความยั่วยุหรือให้ร้าย อันจะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของโรงพยาบาล การทำลายความสัมพันธ์กับบุคลากรของโรงพยาบาลทั้งภายในและภายนอก รวมถึงหน่วยงานอื่น ๆ

๒.๗.๘ หลังจากการใช้งานระบบอินเทอร์เน็ต (Internet) เสร็จแล้ว ให้ผู้ใช้งานทำการปิดเว็บเบราว์เซอร์เพื่อป้องกันการใช้งานโดยบุคคลอื่น

๒.๗.๙ โรงพยาบาลไม่สนับสนุนและไม่มีส่วนเกี่ยวข้องกับการแสดงความคิดเห็นส่วนตัวในรูปแบบอิเล็กทรอนิกส์เช่น ผ่านทางเว็บบอร์ดหรือบล็อกของผู้ใช้งาน ผู้เข้าร่วมประชุม หรือบุคคลภายนอก ทั้งนี้ ความเสียหายใด ๆ ที่อาจเกิดขึ้นจากการแสดงความคิดเห็นดังกล่าวถือเป็นความรับผิดชอบส่วนตัวของผู้นั้นเอง

๒.๗.๑๐ โรงพยาบาลไม่สนับสนุนและไม่มีส่วนเกี่ยวข้องกับผู้ใช้งานที่ใช้ระบบอินเทอร์เน็ต (Internet) ของโรงพยาบาลไปกระทำการใด ๆ อันฝ่าฝืนหรือขัดต่อกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์หรือกฎหมายอื่น ๆ

๒.๘ การใช้งานและการควบคุมการใช้งานจดหมายอิเล็กทรอนิกส์ (e-Mail) ของโรงพยาบาล

๒.๘.๑ ผู้ใช้งานอีเมลทั้งหมดของโรงพยาบาลต้องมี e-Mail account เป็นของตนเอง

๒.๘.๒ e-Mail account ต้องได้รับการป้องกันด้วยรหัสผ่านเพื่อป้องกันการถูกล่วงละเมิดและการนำอีเมลไปใช้ในทางที่ผิด

๒.๘.๓ ผู้ใช้งานต้องลบอีเมลที่ไม่จำเป็นออกจาก Mailbox ของตนอยู่เสมอ เพื่อเป็นการรักษาพื้นที่เก็บอีเมล ทั้งนี้ ผู้ใช้งานต้องเก็บรักษาอีเมลที่เกี่ยวข้องกับการทำงานและอีเมลตามที่กฎหมายกำหนดไว้เท่านั้น

๒.๘.๔ ห้ามใช้ e-Mail account ของโรงพยาบาลเพื่อกระทำการใด ๆ ที่เกี่ยวข้องกับสิ่งผิดกฎหมาย เช่น การโฆษณายาสูบ สิ่งมึนเมา สินค้าหนีภาษี หรือการเผยแพร่ซอฟต์แวร์ละเมิดลิขสิทธิ์ เป็นต้น

๒.๘.๕ ห้ามใช้ e-Mail account ของโรงพยาบาลในการประกาศข้อมูลใด ๆ ในชุมชนอิเล็กทรอนิกส์ เช่น เว็บบอร์ด บล็อก กระดานข่าว เว้นแต่การประกาศข้อมูลนั้นเกี่ยวข้องหรือเป็นส่วนหนึ่งของการทำงานให้แก่โรงพยาบาล

๒.๘.๖ ผู้ใช้งานต้องไม่ยินยอมให้บุคคลอื่นทำการส่งอีเมลโดยใช้ e-Mail account ของตนโดยเด็ดขาด ไม่ว่าบุคคลนั้นจะเป็นผู้ใด

๒.๘.๗ ห้ามผู้ใช้งานส่งอีเมลที่ผู้รับไม่ได้ต้องการ เช่น อีเมลขยะ (Junk mail) หรือโฆษณาสินค้าต่าง ๆ (Spam mail)

๒.๘.๘ ห้ามผู้ใช้งานนำ e-Mail account ของโรงพยาบาลไปใช้สร้างหรือมีส่วนร่วมใด ๆ กับการส่งอีเมลหลอกลวงหรือการส่งอีเมลในลักษณะลูกโซ่โดยเด็ดขาด

๒.๘.๙ ห้ามผู้ใช้งานส่งหรือส่งต่ออีเมลที่มีเนื้อหาหรือรูปภาพที่เข้าข่ายการดูหมิ่น หมิ่นประมาท กล่าวร้าย ทำให้บุคคลอื่นเสื่อมเสียชื่อเสียง เหยียดชนชั้น ข่มขู่ ลามก อนาจาร การยั่วยุทางเพศหรืออีเมลที่มีเนื้อหาสุ่มเสี่ยงต่อประเด็นทางวัฒนธรรม ศาสนา กระทบต่อความมั่นคงของชาติหรือสถาบัน พระมหากษัตริย์ โดยเด็ดขาด

๒.๘.๑๐ ห้ามผู้ใช้งานส่งอีเมลที่มีไฟล์แนบเกี่ยวกับการพนัน ภาพลามกอนาจารหรือไฟล์อื่นใดที่ไม่เกี่ยวข้องกับการทำงานและส่งผลเสียต่อโรงพยาบาล

๒.๘.๑๑ ผู้ใช้งานต้องใช้ความระมัดระวังเป็นพิเศษเมื่อจำเป็นต้องเปิดไฟล์แนบที่ได้รับจากผู้ส่งที่ตนเองไม่รู้จัก ซึ่งไฟล์แนบนั้นอาจมีไวรัส อีเมลบอมบ์ หรือโปรแกรมแฝง (ม้าโทรจัน)

๒.๘.๑๒ เมื่อผู้ใช้งานได้รับข้อความเตือนจากซอฟต์แวร์ป้องกันไวรัสว่า เครื่องคอมพิวเตอร์ของตนมีไวรัส ผู้ใช้งานต้องระงับการส่งอีเมลโดยทันทีจนกว่าเครื่องคอมพิวเตอร์จะได้รับการแก้ไขจนกลับเข้าสู่สภาพปกติ

๒.๙ การจัดการเหตุละเมิดการรักษาความมั่นคงปลอดภัย

๒.๙.๑ ให้ผู้ใช้งานตรวจสอบและสังเกตพฤติกรรมของระบบหรือบุคคลที่น่าสงสัย และแจ้งเจ้าหน้าที่ผู้ดูแลระบบที่รับผิดชอบ เมื่อสังเกตเห็นสิ่งผิดปกติหรืออาจเป็นเหตุละเมิดความมั่นคงปลอดภัย เช่น การใช้สิทธิของผู้ดูแลระบบจากระยะไกลเพื่อเข้าถึงระบบสารสนเทศ การแก้ไขข้อมูลบนเว็บไซต์ การพยายามสอบถามหรือหลอกถามรหัสผ่านการเข้ามาใช้อุปกรณ์สารสนเทศโดยไม่ได้รับอนุญาต เป็นต้น

๒.๙.๒ เมื่อเกิดหรือสงสัยว่าจะเกิดเหตุละเมิดความมั่นคงปลอดภัย เช่น ทรัพย์สินสารสนเทศสูญหาย หรือมีความพยายามเข้าถึงระบบสารสนเทศโดยไม่ได้รับอนุญาตเป็นต้น ให้ผู้ใช้งานที่พบเหตุปฏิบัติตามแนวปฏิบัติการจัดการเหตุละเมิดการรักษาความมั่นคงปลอดภัย และห้ามมิให้เจ้าหน้าที่ที่ไม่ได้รับมอบหมายปฏิบัติการอื่นใดที่ไม่ได้กำหนดไว้ในขั้นตอนรับมือเหตุละเมิดโดยพลการ และดำเนินการแจ้งเหตุการณ์ที่กระทบต่อความมั่นคงปลอดภัยด้านสารสนเทศตามช่องทางแจ้งเหตุที่ช่องทางที่กำหนด

๒.๙.๓ ห้ามมิให้ผู้ใช้งานที่ไม่ได้รับอนุญาต ทำการทดสอบระบบรักษาความมั่นคงปลอดภัยโดยเด็ดขาด ถ้าพบว่ามีการกระทำเกิดขึ้นจะถือว่าเป็นการจงใจละเมิดการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๒.๙.๔ ห้ามมิให้ผู้ใช้งานที่ไม่ได้รับอนุญาต ทำการตรวจจับ เฝ้าฟัง ติดตาม ถอดรหัส บันทึกการสื่อสารข้อมูลทั้งในเครือข่ายคอมพิวเตอร์และระบบสื่อสารโดยเด็ดขาด และให้ถือว่าการกระทำดังกล่าวเป็นการจงใจละเมิดการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๒.๙.๕ ผู้ใช้งานที่ละเมิดความมั่นคงปลอดภัยด้านสารสนเทศและบุกรุกทรัพย์สินของโรงพยาบาลหรืออื่น ๆ แล้วแต่กรณี จะมีความผิดทางวินัยและอาจถูกดำเนินคดีตามกฎหมาย

๒.๙.๖ เมื่อส่วนงานขึ้นตรงเลขาธิการด้านดิจิทัลขอความร่วมมือในการปรับปรุงเวอร์ชัน หรือระงับการใช้ทรัพย์สินสารสนเทศเพื่อป้องกันการเกิดเหตุละเมิดการรักษาความมั่นคงปลอดภัย ให้ผู้ใช้งานปฏิบัติตามโดยทันที

๒.๙.๗ ภายหลังการเกิดเหตุละเมิดการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ส่วนงานขึ้นตรงเลขาธิการด้านดิจิทัล ต้องจัดทำรายงานตามที่ผู้ดูแลระบบตรวจพบการละเมิดการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เสนอต่อผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) การละเลยไม่ทำรายงานในเวลาที่กำหนดถือเป็นความบกพร่องในหน้าที่

๒.๑๐ การเคลื่อนย้ายและการทำสำเนาสารสนเทศ

๒.๑๐.๑ ห้ามมิให้คัดลอกหรือทำสำเนาเอกสาร ข้อมูลคอมพิวเตอร์ข้อมูลสารสนเทศที่มีระดับลับขึ้นไป ในระบบสารสนเทศของโรงพยาบาลโดยไม่ได้รับอนุญาต ถ้าพบว่ามีการกระทำเกิดขึ้นจะถือว่าเป็นการจงใจละเมิดการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๒.๑๐.๒ ห้ามมิให้ส่งข้อมูลสารสนเทศของระบบสารสนเทศของโรงพยาบาลออกไปนอกเครือข่ายของโรงพยาบาล หรือนำสำเนาสารสนเทศระดับลับขึ้นไปในระบบสารสนเทศของโรงพยาบาลออกนอกพื้นที่รักษาการณ์โดยไม่ได้รับอนุญาต ถ้าพบว่ามีการกระทำเกิดขึ้นจะถือว่าเป็นการจงใจละเมิดการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๒.๑๐.๓ การทำสำเนาข้อมูลและการส่งข้อมูลของระบบสารสนเทศที่มีระดับความลับตามข้อ ๒.๑๐.๑ ของโรงพยาบาลออกไปนอกเครือข่ายหรือระบบสารสนเทศของโรงพยาบาล ตามที่ผู้ร้องขอหรือผู้ที่ต้องการใช้สำเนาหรือรับข้อมูลดังกล่าวเพื่อใช้ในทางราชการ จะต้องได้รับอนุญาตจากผู้บริหารระดับสูง (CEO) หรือตัวแทนที่ผู้บริหารระดับสูง (CEO) แต่งตั้งและให้ผู้ที่ได้รับอนุญาตจากผู้บังคับบัญชาในการเข้าถึงเอกสารลับเป็นผู้ทำสำเนาออกจากระบบสารสนเทศของโรงพยาบาล โดยส่งสำเนาดังกล่าวให้กับผู้ร้องขอด้วยแผ่น CD/DVD หรือ e-mail หรือสื่อบันทึกข้อมูลอื่น ๆ ที่โรงพยาบาลอนุญาตเท่านั้นและห้ามมิให้คัดลอกหรือทำสำเนาส่งต่อให้ผู้ที่มิได้รับอนุญาต

๒.๑๐.๔ การใช้งานการสื่อสารข้อมูลในระบบอีเมลหรือจดหมายอิเล็กทรอนิกส์ให้ปฏิบัติตามแนวปฏิบัติการใช้งานและการควบคุมการใช้งานจดหมายอิเล็กทรอนิกส์ (e-mail) ของโรงพยาบาล

๒.๑๑ การควบคุมอุปกรณ์คอมพิวเตอร์อุปกรณ์สื่อสารเคลื่อนที่ และสื่อบันทึกข้อมูล

๒.๑๑.๑ ควบคุมอุปกรณ์คอมพิวเตอร์อุปกรณ์สื่อสารเคลื่อนที่และสื่อบันทึกข้อมูลเพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และการสื่อสารเคลื่อนที่

๒.๑๑.๒ ผู้ใช้งานต้องไม่ปล่อยทิ้งอุปกรณ์คอมพิวเตอร์อุปกรณ์สื่อสารเคลื่อนที่และสื่อบันทึกข้อมูลไว้ในที่สาธารณะโดยไม่มีผู้ดูแล และหากปรากฏว่าความเสียหายที่เกิดขึ้นนั้นเกิดจากความประมาทอย่างร้ายแรงของผู้ใช้งาน ผู้ใช้งานจะต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

๒.๑๑.๓ ผู้ใช้งานต้องสำรองข้อมูลสำคัญสูงที่อยู่ภายในอุปกรณ์คอมพิวเตอร์อุปกรณ์สื่อสารเคลื่อนที่และสื่อบันทึกข้อมูลอย่างสม่ำเสมอและมีการเข้ารหัสข้อมูลที่สำรองอย่างเหมาะสม

๒.๑๑.๔ ผู้ใช้งานต้องมีการติดตั้งโปรแกรมป้องกันไวรัสและไฟร์วอลล์สำหรับอุปกรณ์ส่วนตัวที่ใช้เชื่อมต่อเครือข่ายจากภายนอก และต้องเชื่อมต่อผ่านช่องทางที่มีการเข้ารหัสที่เป็นมาตรฐานสากล ได้แก่ VPN

(Virtual Private Network)

๒.๑๑.๕ ผู้ใช้งานต้องแจ้งต่อผู้บังคับบัญชาเพื่อดำเนินการถอดถอนสิทธิ์ในการเข้าถึงจากภายนอกองค์กรเมื่อเสร็จสิ้นการปฏิบัติงานที่ได้รับมอบหมาย

๒.๑๒ การทำลายสื่อบันทึกข้อมูลหรือการทำลายไฟล์ข้อมูลที่มีระดับลับขึ้นไป

๒.๑๒.๑ ผู้ใช้งานต้องไม่ทิ้งเอกสารที่เป็นลำดับชั้นความลับ ลับมาก และลับที่สุดไว้ที่เครื่องถ่ายเอกสาร เครื่องปริ้นเตอร์ หรือเครื่องสแกนเนอร์ เมื่อสั่งพิมพ์หรือสำเนาแล้วต้องเก็บเอกสารทันที

๒.๑๒.๒ ผู้ใช้งานต้องไม่ทิ้งเอกสารสำคัญหรือสื่อบันทึกข้อมูลอิเล็กทรอนิกส์ไว้ที่โต๊ะทำงานโดยไม่มีผู้ดูแลหรือไม่ได้ใช้งานและต้องจัดหาสถานที่จัดเก็บอย่างปลอดภัย เช่น เก็บในตู้ที่มีอุปกรณ์ล็อค

๒.๑๒.๓ ห้ามมิให้คัดลอกหรือทำสำเนาเอกสาร ข้อมูลคอมพิวเตอร์ข้อมูลสารสนเทศที่มีระดับลับขึ้นไปในระบบสารสนเทศของโรงพยาบาลโดยไม่ได้รับอนุญาต ถ้าพบว่ามีการกระทำเกิดขึ้นจะถือว่าเป็นการจงใจละเมิดการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๒.๑๒.๔ กรณีผู้ร้องขอสำเนาข้อมูลและได้รับสำเนาข้อมูลตามข้อ ๒.๑๐.๓ ทาง e-mail ของโรงพยาบาลเมื่อใช้งานตามภารกิจแล้วให้ทำการลบ e-mail นั้น ใน Inbox และ Trash ออกจากระบบ

๒.๑๒.๕ หากผู้ที่ร้องขอหรือผู้ที่ต้องการใช้สำเนาหรือรับข้อมูลได้รับสำเนาข้อมูลที่มีระดับลับขึ้นไปจากผู้ที่ได้รับอนุญาตจากผู้บังคับบัญชาลงสื่อบันทึกข้อมูลอื่น ๆ อาทิเช่น Flash Drive, Hard disk ฯลฯ เพื่อใช้ในราชการตามภารกิจเรียบร้อยแล้ว ให้ทำการลบ/ล้างไฟล์ข้อมูลนั้น ๆ ด้วยโปรแกรมเขียนทับ (Wiping) ด้วยบิต ๐ หรือ ๑ ในไฟล์ข้อมูลดังกล่าวทั้งนี้จะต้องแจ้งให้ผู้บังคับบัญชาของผู้ที่ได้รับอนุญาตตามข้อ ๒.๑๐.๓ ทราบว่าได้ทำลายข้อมูลแล้วเป็นลายลักษณ์อักษร

๒.๑๓ การเข้ารหัสข้อมูลที่มีระดับลับขึ้นไป

การนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ ผู้ใช้งานจะต้องปฏิบัติตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ และต้องใช้วิธีการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น การเข้ารหัสข้อมูลแบบสมมาตร (เช่น AES ๒๕๖) การเข้ารหัสข้อมูลแบบอสมมาตร (เช่น public key cryptography) เป็นต้น และมีการทบทวนประสิทธิภาพของวิธีการเข้ารหัสข้อมูลอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าวิธีการเข้ารหัสข้อมูลที่ใช้งานยังคงมีความแข็งแรงเพียงพอ

หมวด ๓ แนวปฏิบัติในการรักษาความปลอดภัยด้านสารสนเทศระดับผู้ดูแลระบบ

๓.๑ การปฏิบัติหน้าที่โดยทั่วไปของผู้ดูแลระบบ

๓.๑.๑ เจ้าหน้าที่ผู้ดูแลระบบมีหน้าที่ปฏิบัติต่อระบบสารสนเทศตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศระดับผู้ใช้งานทั่วไป อีกทั้งยังต้องทำการบริหารและจัดการสารสนเทศหรือระบบสารสนเทศตามบทบาทหน้าที่ทางผู้อำนวยการผู้รับผิดชอบในส่วนงานที่ผู้บังคับบัญชามอบหมาย โดยต้องปฏิบัติเพิ่มเติมในส่วนของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ดังนี้

(๑) ต้องตรวจสอบดูแลรักษาการใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายของโรงพยาบาลให้เป็นไปด้วยความเรียบร้อยและมีประสิทธิภาพ หากตรวจพบสิ่งผิดปกติเกี่ยวกับการใช้งาน เครื่องคอมพิวเตอร์และระบบเครือข่ายให้รีบดำเนินการแก้ไข รวมทั้งป้องกันและบรรเทาความเสียหายที่อาจจะเกิดขึ้นในทันทีในกรณีที่สิ่งผิดปกติดังกล่าวเกิดขึ้นจากการใช้งานของผู้ใช้งานที่ไม่เป็นไปตามนโยบายนี้ ให้รีบแจ้งผู้ใช้งานผู้นั้นให้ยุติการกระทำดังกล่าวในทันที และในกรณีจำเป็นเพื่อป้องกันหรือบรรเทาความเสียหายที่เกิดขึ้นแก่โรงพยาบาล ให้ผู้ดูแลระบบพิจารณาระงับการใช้ระบบเครือข่ายของผู้ใช้บริการดังกล่าวได้ทันที

(๒) ต้องติดตั้งและปรับปรุงโปรแกรมคอมพิวเตอร์สำหรับแก้ไขข้อบกพร่องของเครื่องคอมพิวเตอร์และระบบบนเครือข่าย ให้มีความมั่นคงปลอดภัยในการใช้งานและทันสมัยอยู่เสมอ

(๓) สำหรับระบบงานที่ต้องมีการติดต่อสื่อสารหรือแลกเปลี่ยนข้อมูลผ่านระบบ Internet ควรมีกระบวนการประเมินช่องโหว่ (Vulnerability Assessment) และทดสอบเจาะระบบเครือข่าย (Network Penetration Test) โดยผู้เชี่ยวชาญอย่างน้อยปีรายไตรมาส และ/หรือทุกครั้งที่มีการเปลี่ยนแปลงค่าความปลอดภัย หรือมีการเปลี่ยนแปลงความเสี่ยงทางเทคโนโลยีที่มีนัยสำคัญ รวมทั้งควรจะมีการพิจารณาตามความเหมาะสม

(๔) จัดทำแผนการเปลี่ยนแปลงและแก้ไขซอฟต์แวร์ ระบบสารสนเทศ และระบบปฏิบัติการล่วงหน้าเพื่อใช้ในการดูแลและบำรุงรักษาระบบในอนาคต และให้ผู้เกี่ยวข้องมีเวลาในการทดสอบก่อนการเปลี่ยนแปลงและแก้ไข

(๕) แจ้งผลการตรวจสอบและประเมินแนวโน้มระดับการใช้งานของอุปกรณ์ประมวลผลสารสนเทศ (Capacity) และสรุปประเด็นปัญหารายงานต่อผู้บริหารอย่างสม่ำเสมอทุกเดือนเพื่อที่จะสามารถปรับปรุงประสิทธิภาพและความเพียงพอของอุปกรณ์ประมวลผลสารสนเทศให้ตอบสนองความต้องการของผู้เป็นเจ้าของสารสนเทศทั้งในปัจจุบันและในอนาคต

(๖) ต้องตรวจสอบความมั่นคงปลอดภัยในการใช้งานเครื่องคอมพิวเตอร์แม่ข่าย (Server) และระบบเครือข่าย

(๗) ต้องดูแลรักษาและตรวจสอบช่องทางการสื่อสารของระบบเครือข่ายอยู่เสมอและปิดช่องทางการสื่อสารของระบบเครือข่ายที่ไม่มีความจำเป็นต้องใช้งานในทันที

(๘) ต้องจัดให้มีการลงทะเบียนผู้ใช้งานก่อนอนุญาตให้เข้าใช้ระบบงานต่าง ๆ ของโรงพยาบาล

(๙) ต้องดูแลรักษาและปรับปรุงบัญชีผู้ใช้งาน ระบบยืนยันตัวตน (Authentication) และระบบจดหมายอิเล็กทรอนิกส์ (e-mail) ให้ถูกต้องและเป็นปัจจุบันอยู่เสมอ โดยให้ยกเลิกสิทธิการใช้งานของผู้ใช้บริการที่พ้นสภาพการเป็นผู้ใช้บริการ

(๑๐) ต้องตรวจสอบเครื่องคอมพิวเตอร์ของผู้ใช้งาน หรือเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการไดเรกทอรีสำหรับเครือข่ายโดเมนในส่วนของนโยบายรหัสผ่าน (Password Policy)

ให้มีการกำหนดรหัสผ่าน (Password) รวมทั้งการเก็บรักษารหัสผ่าน (Password) ให้สอดคล้องตามแนวปฏิบัติในการรักษา ความมั่นคงปลอดภัยด้านสารสนเทศระดับผู้ใช้งานทั่วไป ในข้อที่ ๒.๕

(๑๑) ไม่ใช้อำนาจหน้าที่ของตนในการเข้าถึงข้อมูลของผู้ใช้งานที่ใช้งานระบบคอมพิวเตอร์โดยไม่มีเหตุผลอันสมควร

(๑๒) ไม่กระทำการอื่นใดที่มีลักษณะเป็นการละเมิดสิทธิหรือข้อมูลส่วนบุคคลของผู้ใช้งานที่ใช้งานระบบคอมพิวเตอร์หรือมีข้อมูลส่วนบุคคลจัดเก็บไว้ในระบบคอมพิวเตอร์โดยไม่มีเหตุผลอันสมควร

(๑๓) ไม่เปิดเผยข้อมูลที่ได้มาจากการปฏิบัติหน้าที่ ซึ่งข้อมูลดังกล่าวเป็นข้อมูลที่ไม่เปิดเผยให้บุคคลหนึ่งบุคคลใดทราบโดยไม่มีเหตุผลอันสมควร

(๑๔) เมื่อผู้ดูแลระบบพ้นจากหน้าที่ จะต้องคืนทรัพย์สินของโรงพยาบาลที่เกี่ยวข้องกับการปฏิบัติหน้าที่ของตนในทันที และให้หัวหน้ากลุ่มงานที่บังคับบัญชาผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายทำการตรวจสอบการคืนทรัพย์สิน

๓.๑.๒ การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ดูแลระบบ จะต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์(Log) โดยจะต้องเก็บรักษาข้อมูลของผู้ใช้งานที่จำเป็น เพื่อให้สามารถระบุตัวผู้ใช้งานนับตั้งแต่เริ่มใช้งานที่โรงพยาบาลให้บริการและต้องเก็บรักษาไว้เป็นเวลาไม่น้อยกว่า ๙๐ วัน นับตั้งแต่การใช้บริการสิ้นสุดลง การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์(Log) ต้องใช้วิธีการที่มั่นคงปลอดภัย ดังต่อไปนี้

(๑) เก็บในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วนถูกต้องแท้จริงและระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้ โดยสื่อที่ใช้ในการเก็บต้องสามารถใช้ในการยืนยันทางกฎหมายได้และไม่ขัดต่อพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม

(๒) มีระบบการเก็บรักษาความลับของข้อมูลที่จัดเก็บและกำหนดชั้นความลับในการเข้าถึงข้อมูลดังกล่าวเพื่อรักษาความน่าเชื่อถือของข้อมูลและไม่ให้ผู้ดูแลระบบสามารถแก้ไขข้อมูลที่เก็บรักษาไว้ เว้นแต่ผู้ที่กำหนดให้สามารถเข้าถึงข้อมูลดังกล่าวได้ เช่น ผู้ตรวจสอบระบบสารสนเทศของโรงพยาบาลหรือบุคคลที่โรงพยาบาลมอบหมาย

(๓) ในการเก็บข้อมูลจราจรทางคอมพิวเตอร์(Log) นั้น ต้องสามารถระบุรายละเอียดผู้ใช้งานเป็นรายบุคคลได้

(๔) เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์(Log) มีความถูกต้องและนำมาใช้ประโยชนได้จริง ผู้ดูแลระบบต้องตั้งนาฬิกาของอุปกรณ์บริการทุกชนิดให้ตรงกับเวลามาตรฐานประเทศไทย (Stratum ๑) โดยผิดพลาดไม่เกิน ๑๐ มิลลิวินาที

๓.๑.๓ ผู้ดูแลระบบมีหน้าที่ควบคุมและการบริหารจัดการการเปลี่ยนแปลง (ChangeManagement) ดังนี้

(๑) ผู้ที่เกี่ยวข้องในกระบวนการบริหารจัดการการเปลี่ยนแปลง ควรมีการแบ่งแยกหน้าที่อย่างเหมาะสม (segregation of duties) เพื่อไม่ให้บุคคลใดบุคคลหนึ่งสามารถปฏิบัติงานได้ตั้งแต่ต้นจนจบกระบวนการ

(๒) คำขอการเปลี่ยนแปลง (change request) ควรได้รับการอนุมัติจากหน่วยงานเจ้าของระบบ (system owner) เพื่อให้มั่นใจได้ว่าการขอเปลี่ยนแปลงได้รับการพิจารณาความจำเป็นอย่างเหมาะสมจากหน่วยงานเจ้าของระบบ

(๓) มีการประเมินผลกระทบหรือทำการทดสอบก่อนนำไปตั้งค่าบนระบบที่ให้บริการจริง เพื่อลดความเสี่ยงและผลกระทบที่อาจเกิดขึ้น

(๔) จัดทำขั้นตอนในการถอยกลับ (Fallback Procedure) รวมทั้งหน้าที่ความรับผิดชอบของผู้เกี่ยวข้องในการกู้คืนระบบ ในกรณีที่การเปลี่ยนแปลงไม่เป็นไปตามแผน

(๕) ควรมีการติดตามผลหลังการเปลี่ยนแปลงระบบ (post implementation review) เพื่อให้มั่นใจได้ว่าการเปลี่ยนแปลงนั้นเป็นไปตามวัตถุประสงค์ที่กำหนด

๓.๑.๔ ผู้ดูแลระบบต้องควบคุมให้มีการแยกระบบสำหรับการพัฒนาและระบบสำหรับการทดสอบออกจากระบบที่ใช้งานจริง เพื่อป้องกันปัญหาที่อาจมีผลกระทบกับข้อมูลหรือการประมวลผลของระบบที่ใช้งานจริง โดยต้องจัดให้มีการควบคุมดังต่อไปนี้

(๑) ซอร์สโค้ด (Source Code) ของระบบสารสนเทศ ต้องไม่เก็บอยู่ในระบบที่ใช้งานจริง ในกรณีที่มีความจำเป็นต้องเก็บซอร์สโค้ด (Source Code) ในระบบที่ใช้งานจริง เนื่องจากข้อจำกัดของภาษาที่ใช้ในการพัฒนาระบบให้มีการกำหนดสิทธิในการเข้าถึงเฉพาะผู้ที่ได้รับอนุญาตเท่านั้น

(๒) มีการควบคุมเวอร์ชันของคำสั่งในการเขียนโปรแกรม (source code version control) เพื่อป้องกันความเสี่ยงที่อาจเกิดจากการใช้คำสั่งผิดเวอร์ชัน

(๓) มีแนวทางการควบคุมการรักษาความปลอดภัยและความลับของข้อมูลสำคัญที่นำไปใช้ในการทดสอบ เช่น data masking เป็นต้น เพื่อป้องกันความเสี่ยงในการรั่วไหลของข้อมูลสำคัญดังกล่าว

(๔) การนำระบบขึ้นใช้งานจริง ต้องผ่านกระบวนการบริหารจัดการการเปลี่ยนแปลงที่โรงพยาบาลกำหนด เพื่อป้องกันความเสี่ยงหรือข้อผิดพลาดในการปฏิบัติงาน

(๕) กำหนดให้หน่วยงานที่เกี่ยวข้องสอบทานความถูกต้องครบถ้วนตามความต้องการของหน่วยงาน (business requirement) โดยครอบคลุมการรักษาความปลอดภัยตามนโยบายหรือมาตรฐาน ที่โรงพยาบาลกำหนด (security requirement) รวมทั้งพิจารณาจัดทำเอกสารรายละเอียดคุณสมบัติทางเทคนิค (technical specification)

(๖) จัดทำขอบเขตการทดสอบให้ครอบคลุมฟังก์ชันและเงื่อนไขต่าง ๆ ด้านประสิทธิภาพตามความต้องการของหน่วยงาน(business requirement) รวมถึงการควบคุมความมั่นคงปลอดภัยตามนโยบายหรือมาตรฐานที่โรงพยาบาลกำหนด

๓.๒ การกำหนดประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล

๓.๒.๑ กำหนดประเภทข้อมูลหลัก ๆ ดังนี้

(๑) ความลับที่สุด (Top Secret) เป็นข้อมูลสารสนเทศที่มีความสำคัญอย่างสูงต่อการดำเนินธุรกิจและกำหนดให้เฉพาะผู้บริหารระดับสูงหรือบางกลุ่มบุคคลที่ได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงหรือใช้สารสนเทศดังกล่าวได้

(๒) ความลับมาก (Secret) เป็นข้อมูลสารสนเทศที่มีความสำคัญต่อการดำเนินธุรกิจซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วน จะก่อให้เกิดความเสียหายแก่โรงพยาบาลอย่างร้ายแรง เช่น ข้อมูลรหัสผ่านของผู้ดูแลระบบ เป็นต้น

(๓) ความลับ (Confidential) เป็นข้อมูลสารสนเทศที่มีความสำคัญต่อการดำเนินธุรกิจและกำหนดให้บางกลุ่มบุคคลที่ได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงหรือใช้ข้อมูลสารสนเทศดังกล่าวได้ การเปิดเผยหรือการเข้าถึงสารสนเทศในระดับชั้นนี้โดยไม่ได้รับอนุญาต อาจก่อให้เกิดความเสียหายทางด้านการเงินหรือกระทบต่อการดำเนินงานประจำวันหรือความก้าวหน้าทางธุรกิจและอาจก่อให้เกิดความเสียหายต่อชื่อเสียง และ

ภาพลักษณ์ เช่น ข้อมูลส่วนบุคคล ข้อมูลค่า Configuration ของอุปกรณ์ข้อมูลรหัสผ่าน ข้อมูลการประเมิน ความเสี่ยง เป็นต้น

(๔) ใช้ภายใน (Internal Use Only) เป็นข้อมูลสารสนเทศที่อนุญาตให้ใช้ภายในโรงพยาบาลเท่านั้น การเปิดเผยหรือการเข้าถึงข้อมูลสารสนเทศในระดับชั้นนี้โดยไม่ได้รับอนุญาตอาจก่อให้เกิดผลกระทบต่อการปฏิบัติงานประจำวันของโรงพยาบาลได้ แต่ไม่กระทบต่อการดำเนินธุรกิจ เช่น เอกสารนโยบาย มาตรฐานและขั้นตอนการปฏิบัติงาน รายละเอียดเบอร์โทรศัพท์ภายในโรงพยาบาล เอกสารคู่มือการใช้งานระบบต่าง ๆ บันทึกการปฏิบัติงานประจำวัน เป็นต้น

(๕) เปิดเผยต่อบุคคลภายนอก (Public) เป็นข้อมูลสารสนเทศที่ไม่ได้กระทบอย่างมีนัยสำคัญต่อการดำเนินงาน และผู้บริหารระดับสูงอนุมัติให้เปิดเผยต่อสาธารณะได้ อย่างไรก็ดีสารสนเทศในระดับชั้นนี้ต้องได้รับการป้องกันหรือควบคุมอย่างเหมาะสม เพื่อให้มั่นใจว่าสารสนเทศที่ถูกเปิดเผยมีความถูกต้องครบถ้วน (Integrity) เพื่อสร้างความเชื่อมั่นให้กับลูกค้า รวมทั้งรักษาภาพลักษณ์ และชื่อเสียง เช่น รายงานประจำปี หรือข้อมูลบนเว็บไซต์ เป็นต้น

๓.๒.๒ ลำดับความสำคัญของข้อมูล หรือชั้นความลับของข้อมูลผู้ดูแลระบบจะต้องปฏิบัติอย่างเคร่งครัด โดยให้กำหนดประเภทของข้อมูลตามหลักเกณฑ์ข้อ ๓.๒.๑

๓.๒.๓ ระดับชั้นของการเข้าถึงข้อมูลสารสนเทศตามชั้นความลับ ต้องแบ่งสิทธิ์ตามตำแหน่งและตามบทบาทหน้าที่ความรับผิด โดยแบ่งระดับชั้นการเข้าถึงออกเป็น ๓ ลำดับ ดังนี้

(๑) ระดับชั้นสำหรับผู้บริหาร สามารถเข้าถึงข้อมูลสารสนเทศในทุกลำดับชั้นความลับ

(๒) ระดับชั้นสำหรับผู้ใช้งาน หรือผู้ดูแลระบบสามารถเข้าถึงข้อมูลสารสนเทศเฉพาะที่ได้รับมอบหมายตามหน้าที่ความรับผิดชอบ

(๓) ระดับชั้นสำหรับบุคคลภายนอก สามารถเข้าถึงข้อมูลสารสนเทศในลำดับชั้นความลับข้อมูลเปิดเผยได้ (Public)

๓.๒.๔ ระยะเวลาการเข้าถึงข้อมูลสารสนเทศ ได้แก่

(๑) ระบบอินทราเน็ตและระบบภายในของโรงพยาบาล สำหรับผู้ใช้งานหรือผู้ดูแลระบบสามารถเข้าถึงได้ตลอดเวลา

(๒) ระบบเว็บไซต์ (www.nhso.go.th) สำหรับบุคคลภายนอกสามารถเข้าถึงได้ตลอดเวลา

๓.๒.๕ ช่องทางการเข้าถึงข้อมูลสารสนเทศ โดยผู้ต้องการเข้าถึงข้อมูลสารสนเทศจะต้องได้รับอนุญาตจากผู้บังคับบัญชาและทุกครั้งที่มีการเข้าถึงข้อมูลสารสนเทศจะต้องผ่านการยืนยันตัวบุคคล รวมถึงผู้ดูแลระบบต้องกำกับ ติดตาม และทบทวนสิทธิตามที่ผู้ต้องการเข้าถึงข้อมูลร้องขอ โดยช่องทางการเข้าถึงข้อมูลสารสนเทศของโรงพยาบาล มีดังต่อไปนี้

(๑) ช่องทางที่สามารถเข้าถึงข้อมูลสารสนเทศจากภายนอกโรงพยาบาลจะต้องผ่านเครือข่ายทางไกลจากภายนอก (VPN)

(๒) ช่องทางที่สามารถเข้าถึงข้อมูลสารสนเทศจากภายในจะต้องผ่านระบบเครือข่ายภายในโรงพยาบาล

(๓) ช่องทางการรับส่งข้อมูลสารสนเทศสำคัญ โดยผ่านระบบเครือข่ายสาธารณะทั้งจากภายในหรือภายนอกโรงพยาบาลโดยช่องทางและข้อมูลสำคัญดังกล่าวต้องได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล ได้แก่ TLS เวอร์ชัน ๑.๒ เป็นอย่างน้อย หรือ XML Encryption ตามความเหมาะสมของธุรกรรมที่ใช้ในการรับส่งข้อมูลสารสนเทศ

๓.๒.๖ ผู้ดูแลระบบต้องบริหารจัดการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุมการ

เข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้

(๑) ควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

(๒) กำหนดรายชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล

(๓) กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

(๔) กำหนดรหัสยืนยันตัวบุคคลสำหรับผู้ใช้ที่อยู่ภายนอกโรงพยาบาลเพื่อให้สามารถเข้าถึงเครือข่ายและระบบสารสนเทศของโรงพยาบาล โดยการให้ผู้ใช้งานยื่นแบบคำขอรหัสการเข้าใช้งาน VPN ตามแบบคำขอใช้งาน VPN โดยต้องได้รับอนุญาตจากผู้บังคับบัญชา

(๕) กำหนดค่าการเปลี่ยนรหัส (Password) ตามระยะเวลาที่กำหนดของความสำคัญของข้อมูล

(๖) ควรกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของโรงพยาบาล เช่น การส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูล ที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

๓.๒.๗ ผู้ดูแลระบบต้องควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ เพื่อปกป้องข้อมูลสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และการสื่อสารเคลื่อนที่

๓.๒.๘ ผู้ดูแลระบบควรกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของโรงพยาบาล เช่น การส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อมควรสำรองและลบข้อมูลก่อน

๓.๒.๙ ผู้ดูแลระบบต้องปฏิบัติตามนโยบายในการคุ้มครองข้อมูลส่วนบุคคล ในการเข้าถึงข้อมูล การใช้ข้อมูลส่วนบุคคล และเมื่อมีความจำเป็นในการเข้าถึงข้อมูลส่วนบุคคลต้องเป็นไปตามสิทธิที่ได้รับมอบหมายตามหน้าที่รับผิดชอบตามที่โรงพยาบาลกำหนด

๓.๒.๑๐ ผู้ดูแลระบบต้องควบคุม ตรวจสอบ แจ้งเตือนการละเมิดการเข้าใช้งาน การโอนถ่ายข้อมูล หรือการกระทำใด ๆ ของผู้ที่เข้าถึงข้อมูลส่วนบุคคลที่ขัดต่อนโยบายในการคุ้มครองข้อมูลส่วนบุคคลให้ผู้บังคับบัญชารับทราบโดยเร็วที่สุด

๓.๓ การควบคุมการเข้าถึงระบบสารสนเทศ

๓.๓.๑ ให้ผู้รับผิดชอบในส่วนงานกำหนดมาตรการควบคุมการเข้าใช้งานระบบสารสนเทศของโรงพยาบาลเพื่อดูแลรักษาความปลอดภัย โดยที่ผู้ดูแลระบบจะต้องกำหนดสิทธิในการเข้าใช้งานระบบสารสนเทศของโรงพยาบาลนั้น ผู้เข้าใช้งานในส่วนต่าง ๆ จะต้องขออนุญาตเป็นลายลักษณ์อักษรและให้ผู้บังคับบัญชาที่รับผิดชอบในการกำกับควบคุมผู้ดูแลระบบที่มีหน้าที่ในการให้เข้าถึงระบบสารสนเทศ โดยที่ผู้ดูแลระบบต้องตรวจสอบการดำเนินการและเสนอความผิดปกติต่อผู้บังคับบัญชารับทราบทันที โดยให้โรงพยาบาลจัดทำทะเบียนควบคุมสิทธิที่เหมาะสม รวมถึงรายชื่อหรือกลุ่มผู้มีสิทธิใช้งานทั้งที่ต้องขออนุมัติและไม่ต้องขออนุมัติก่อนเริ่มใช้งานอย่างเป็นลายลักษณ์อักษรในแต่ละระบบสารสนเทศ โดยการเข้าถึงของผู้ใช้งานทั้งหมดต้องสอดคล้องกับการดำเนินงานของโรงพยาบาลและหน้าที่ความรับผิดชอบของผู้ใช้งาน

(๑) ผู้บังคับบัญชา พิจารณาให้สิทธิตามหน้าที่ความรับผิดชอบ และความจำเป็นในการใช้งาน รวมทั้งกำหนดให้มีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ

(๒) ผู้ดูแลระบบกำหนดสิทธิการเข้าถึงข้อมูลและระบบสารสนเทศให้แก่ผู้ใช้งานตามที่ได้รับการอนุมัติจากผู้บังคับบัญชา

๓.๓.๒ ให้ผู้รับผิดชอบในส่วนงานควบคุมให้มีขั้นตอนการลงทะเบียนผู้ใช้งาน เมื่อมีการอนุญาตให้เข้าถึงระบบสารสนเทศ และการตัดออกจากทะเบียนของผู้ใช้งานเมื่อมีการยกเลิกเพิกถอนสิทธิการเข้าใช้งาน ดังนี้

(๑) การลงทะเบียนผู้ใช้งาน

(ก) ผู้ดูแลระบบต้องจัดให้มีการลงทะเบียนผู้ใช้งาน ก่อนอนุญาตให้เข้าใช้ระบบงานต่าง ๆ ของโรงพยาบาล

(ข) การลงทะเบียนผู้ใช้งาน กรณีที่จ้างบุคคลภายนอกพัฒนาระบบ (Outsource) โดยกำหนดให้มีการแสดงหลักฐานที่สามารถระบุตัวบุคคลได้ และการเข้าถึงระบบสารสนเทศต้องได้รับอนุมัติ จากต้นสังกัดของผู้ใช้งานนั้น ๆ ก่อนอนุญาตให้เข้าใช้ระบบงานต่างๆ ของโรงพยาบาล

(ค) ผู้ดูแลระบบต้องสร้างบัญชีผู้ใช้งานแยกเป็นรายบุคคล ในกรณีที่มีความจำเป็น ต้องใช้งานบัญชีผู้ใช้งานร่วมกันให้ขออนุมัติเป็นกรณีไป ผู้ดูแลระบบต้องจัดส่งบัญชีผู้ใช้งานและรหัสผ่านโดยจัดส่งแยกเป็นรายบุคคล

(๒) การยกเลิกหรือเพิกถอนสิทธิการเข้าใช้งาน

(ก) กรณีที่ผู้ใช้งานในส่วนเจ้าหน้าที่ลาออก สิ้นสุดการจ้าง ให้ยกเลิกหรือเพิกถอนสิทธิการเข้าใช้งานตามรอบที่ฝ่ายบริหารและพัฒนาทรัพย์กรบุคคลแจ้งต่อส่วนงานขึ้นตรงเลขาธิการด้านดิจิทัล

(ข) กรณีที่ผู้ใช้งานในส่วนอื่น ๆ ลาออก สิ้นสุดการจ้าง ให้ยกเลิกหรือเพิกถอนสิทธิการเข้าใช้งานตามรอบที่ต้นสังกัดของผู้ใช้งานนั้น ๆ แจ้งต่อส่วนงานขึ้นตรงเลขาธิการด้านดิจิทัล

(ค) กรณีปรับเปลี่ยนตำแหน่งหน้าที่ภายในหน่วยงานโอนย้ายหน่วยงานหรือหมดความจำเป็นในการใช้งาน ให้เปลี่ยนแปลงสิทธิตามรอบที่ฝ่ายบริหารและพัฒนาทรัพย์กรบุคคลหรือต้นสังกัดแจ้งต่อส่วนงานขึ้นตรงเลขาธิการด้านดิจิทัล

(ง) ผู้ดูแลระบบต้องยกเลิกหรือเพิกถอนสิทธิการเข้าใช้งานตามเงื่อนไข (ก)–(ค) ภายใน ๗ วัน ตามการร้องขอจากฝ่ายบริหารและพัฒนาทรัพย์กรบุคคลหรือต้นสังกัดที่แจ้งต่อส่วนงานขึ้นตรงเลขาธิการด้านดิจิทัล

(๓) การทบทวนสิทธิ

(ก) ผู้ดูแลระบบต้องทบทวนสิทธิการเข้าถึงระบบของผู้ใช้งานอย่างน้อยปีละ ๑ ครั้ง และระงับการใช้งานบัญชีผู้ใช้ที่ไม่ได้ใช้งาน

(ข) ให้ส่วนงานขึ้นตรงเลขาธิการด้านดิจิทัลควบคุมและจำกัดสิทธิเพื่อเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิจำเพาะสิทธิพิเศษและสิทธิอื่น ๆ ที่เกี่ยวข้องกับการเข้าถึง ดังนี้

๑) ผู้ดูแลระบบต้องกำหนดสิทธิผู้ใช้งานตามคำร้องขอที่ได้รับอนุมัติการขอเข้าใช้งานระบบจากผู้บังคับบัญชา โดยผู้ใช้งานต้องเข้าใช้งานระบบตามสิทธิที่ตนเองได้รับเท่านั้น

๒) ผู้บังคับบัญชาต้องตรวจสอบและมอบหมายสิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่รับผิดชอบ

๓) หัวหน้าหน่วยงานเจ้าของระบบ หรือเจ้าของข้อมูล หรือผู้รับผิดชอบที่ได้รับมอบหมาย ต้องตรวจสอบและมอบหมายสิทธิเฉพาะตามที่ได้รับการร้องขอ

๔) ในกรณีมีความจำเป็นต้องให้สิทธิจำเพาะหรือสิทธิพิเศษแกผู้ใช้งาน ได้แก่ สิทธิสูงสุดในการเข้าถึงระบบหรือข้อมูล และสิทธิที่เข้าถึงระบบหรือข้อมูลได้มากกว่า

หน้าที่รับผิดชอบ ผู้ใช้งานนั้นต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา และได้รับการตรวจสอบจากหัวหน้าหน่วยงานเจ้าของระบบหรือเจ้าของข้อมูล หรือผู้รับผิดชอบที่ได้รับมอบหมาย โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ถึง ระดับใดบ้างรวมทั้งต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

๕) หัวหน้าหน่วยงานเจ้าของระบบ หรือเจ้าของข้อมูล หรือผู้รับผิดชอบที่ได้รับมอบหมาย ต้องมีการบันทึกจัดเก็บหลักฐานในการขอใช้สิทธิระดับสูงเพื่อการทบทวนและตรวจสอบสิทธิ

(ค) ผู้ดูแลระบบควรจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศของโรงพยาบาล และตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบข้อมูลสารสนเทศ

(ง) ผู้ดูแลระบบต้องจัดบันทึกรายละเอียดการเข้าถึงระบบการแก้ไข เปลี่ยนแปลงสิทธิต่างๆ และการผ่านเข้า-ออกสถานที่ตั้งของระบบ ของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาตเพื่อเป็นหลักฐานในการตรวจสอบ

(จ) ผู้ดูแลระบบต้องบริหารจัดการรหัสผ่านและสิทธิการใช้งานระบบเทคโนโลยีสารสนเทศของผู้ใช้งาน ดังต่อไปนี้

๑) รหัสผู้ใช้งานและรหัสผ่านผู้ดูแลระบบจัดส่งให้กับผู้ใช้งานเริ่มต้นเป็นรหัสชั่วคราว โดยชื่อผู้ใช้งานหรือรหัสผ่านต้องไม่ซ้ำกันและกำหนดให้ระบบจัดการรหัสผ่านตรวจสอบรหัสผ่านว่าต้อง ประกอบด้วยอักขระ ตัวเลข และอักขระพิเศษ ความยาวรวมกันไม่น้อยกว่า ๘ ตัวอักษร กรณีที่ผู้ใช้งานทำการ เปลี่ยนรหัสเอง (สามารถตั้งค่าการจัดการรหัสผ่าน)

๒) ส่งมอบรหัสผ่านชั่วคราว (Temporary Password) ให้กับผู้ใช้บริการด้วยวิธีการที่ปลอดภัย ควรหลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (e-mail) ที่ไม่มีการป้องกัน ในการส่งรหัสผ่าน(Password) และแจ้งผู้ใช้บริการให้ทำการเปลี่ยนรหัสผ่านใหม่

๓) เมื่อมีการส่งมอบรหัสผ่านตามข้อ ๕. (จ) (๒) ให้ผู้ใช้บริการตอบยืนยันการได้รับรหัสผ่านและทำการเปลี่ยนรหัสผ่านใหม่

๔) กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน(Password) เมื่อผู้ใช้งานระบบลาออก หรือพ้นจากตำแหน่งหรือยกเลิกการใช้งาน

๕) แจ้งผู้ใช้งานไม่ให้ทำการบันทึกหรือเก็บรหัสผ่าน(Password) ไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

๖) ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่และมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงระดับใดได้บ้างและต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

๗) กำหนดให้ระบบแจ้งเตือนให้ผู้ใช้งานทำการเปลี่ยนรหัสผ่านทุก ๆ ๓ เดือน

๘) กำหนดระยะเวลาการใช้งานระบบสารสนเทศภายในโรงพยาบาล โดยผู้ใช้งานต้องใช้งานระบบสารสนเทศอย่างต่อเนื่องหากว่างเว้นจากการใช้งานระบบ

สารสนเทศมากกว่า ๓๐ นาที หรือแล้วแต่ความเหมาะสมของระบบสารสนเทศนั้น ๆ โดยต้องกำหนดให้โปรแกรม Browser ปิดการทำงานและกำหนดให้ผู้ใช้งานกรอกรหัสผู้ใช้งานและรหัสผ่านเพื่อเข้าสู่ระบบสารสนเทศใหม่

(ฉ) ผู้ดูแลระบบต้องควบคุมระบบซึ่งไวต่อการรบกวน (Sensitive or Critical system) มีผลกระทบและมีความสำคัญสูงต่อโรงพยาบาล โดยต้องแยกระบบซึ่งไวต่อการรบกวนออกจากระบบอื่น และมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ โดยจัดแบ่งโซนของเครือข่ายและติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ต่าง ๆ ของระบบไว้ในศูนย์คอมพิวเตอร์หรือพื้นที่ปลอดภัยที่ได้มีการจำกัดสิทธิผู้เข้าถึง ทางกายภาพที่เหมาะสม

(ช) ต้องควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานต่อองค์กร ดังนี้

๑) จำกัดการเข้าถึงระบบซึ่งไวต่อการรบกวนจากอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่เฉพาะผู้ได้รับอนุญาตหรือโปรแกรมประยุกต์หรือแอปพลิเคชันอื่นที่ต้องเชื่อมต่อกันเท่านั้น และต้องกำหนดให้มีการระบุและยืนยันตัวตนผ่านระบบที่โรงพยาบาลกำหนด เช่น AD (Active Directory),LDAP (Lightweight Directory Access Protocol), ระบบ SSO (Single Sign On) ของโรงพยาบาลทุกครั้ง

๒) กำหนดให้มีการเข้ารหัสข้อมูลที่เป็นมาตรฐานสากล ได้แก่ TLS เวอร์ชัน ๑.๒ เป็นอย่างน้อย หรือ XML Encryption ในส่วนการรับส่งข้อมูลผ่านเครือข่าย (encryption protocol) เข้าสู่ระบบ ซึ่งไวต่อการรบกวนเพื่อปฏิบัติงานจากภายนอกโรงพยาบาล

๓) กำหนดให้ใช้สายสัญญาณที่มีคุณสมบัติป้องกันสนามแม่เหล็กไฟฟ้า หรือใช้สายใยแก้วนำแสง (Fiber Optic) ติดตั้งท่อหุ้มสายชนิดควบคุมการเข้าถึงแผงพักปลายสาย (Patch Panel) และห้องพักสาย (Cable Room) และมีการตรวจสอบระบบสาย เพื่อตรวจจับอุปกรณ์แปลกปลอม

๔) จัดให้มีการบำรุงรักษาอุปกรณ์และระบบสนับสนุนการทำงานต่าง ๆ เป็นประจำอย่างน้อยปีละ ๑ ครั้ง

๓.๔ การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

๓.๔.๑ ผู้ดูแลระบบต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (Access Point) ให้รั่วไหลออกนอกพื้นที่ใช้ระบบเครือข่ายไร้สายน้อยที่สุด

๓.๔.๒ ผู้ดูแลระบบต้องทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าโดยปริยาย (Default) มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณ (Access Point) มาใช้งาน

๓.๔.๓ ผู้ดูแลระบบต้องกำหนดค่า WPA หรือ WPA-๒ (Wi-Fi Protected Access) เป็นระดับเบื้องต้นในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และอุปกรณ์กระจายสัญญาณ (Access Point) และกำหนดค่าให้ไม่แสดงชื่อระบบเครือข่ายไร้สาย

๓.๔.๔ ผู้ดูแลระบบควรเลือกใช้วิธีการควบคุมการเข้าใช้งานระบบเครือข่ายไร้สาย โดยมีการพิสูจน์ตัวตนด้วยชื่อผู้ใช้ (Username) รหัสผ่าน (Password) ของผู้ใช้บริการที่มีสิทธิในการเข้าใช้งานระบบเครือข่ายไร้สาย หรือการระบุตัวตนด้วยวิธีอื่นใดตามที่กำหนดไว้เท่านั้น เพื่อให้เข้าใช้งานระบบเครือข่ายไร้สายได้อย่างถูกต้อง

๓.๔.๕ ผู้ดูแลระบบควรมีการติดตั้งไฟร์วอลล์ (Firewall) ระหว่างระบบเครือข่ายไร้สายกับระบบ

เครือข่ายในโรงพยาบาล

๓.๔.๖ ผู้ดูแลระบบควรกำหนดให้ผู้ใช้งานเข้าใช้บริการในระบบเครือข่ายไร้สายของโรงพยาบาลด้วยช่องทางที่ปลอดภัยในการติดต่อสื่อสาร เช่น VPN (Virtual Private Network) เพื่อช่วยป้องกันการบุกรุกในระบบเครือข่ายไร้สาย

๓.๔.๗ ผู้ดูแลระบบควรใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สาย เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยที่เกิดขึ้นจากในระบบเครือข่ายไร้สายและจัดส่งรายงานผลการตรวจสอบทุก ๆ ๓ เดือน และในกรณีที่ตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติให้ผู้ดูแลระบบรายงานต่อผู้บังคับบัญชาทราบทันที

๓.๔.๘ ผู้ดูแลระบบต้องควบคุมดูแลไม่ให้บุคคลหรือหน่วยงานภายนอกที่ไม่ได้รับอนุญาตใช้งานระบบเครือข่ายไร้สายในการเข้าสู่ระบบอินทราเน็ต (Intranet) และฐานข้อมูลภายในต่าง ๆ ของโรงพยาบาล

๓.๕ การควบคุมการเข้าถึงระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย

๓.๕.๑ ให้กลุ่มงานที่ได้รับมอบหมายบริหารศูนย์คอมพิวเตอร์ตรวจสอบกำหนดมาตรการควบคุมการเข้า-ออก ศูนย์คอมพิวเตอร์หลักและศูนย์คอมพิวเตอร์สำรอง และให้เจ้าหน้าที่ควบคุมห้องคอมพิวเตอร์ (Server Room) เพื่อควบคุมการเข้าถึงระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่ายของโรงพยาบาล

๓.๕.๒ ผู้ดูแลระบบต้องควบคุมการเข้าถึงระบบเครือข่าย เพื่อบริหารจัดการระบบเครือข่ายได้อย่างมีประสิทธิภาพ ดังต่อไปนี้

(๑) จำกัดสิทธิการใช้งานเพื่อควบคุมผู้ใช้บริการให้สามารถใช้งานเฉพาะระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น

(๒) จำกัดเส้นทางการเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน

(๓) จำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่ายเพื่อไม่ให้ผู้ใช้บริการสามารถใช้เส้นทางอื่น ๆ ได้

(๔) ระบบเครือข่ายทั้งหมดของโรงพยาบาลที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกโรงพยาบาล ควรเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก รวมทั้งต้องมีความสามารถในการตรวจจับ โปรแกรมประสงค์ร้าย (Malware) ด้วย

(๕) ระบบเครือข่ายต้องติดตั้งระบบตรวจจับการบุกรุก (Intrusion Prevention System/Intrusion System) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของโรงพยาบาลในลักษณะที่ผิดปกติ

(๖) ผู้ดูแลระบบต้องดูแลการเข้าสู่ระบบเครือข่ายภายในโรงพยาบาล โดยผ่านทางระบบอินเทอร์เน็ตจำเป็นต้องมีการลงบันทึกเข้า (Login) และต้องมีการพิสูจน์ยืนยันตัวบุคคล (Authentication) เพื่อการตรวจสอบความถูกต้องของผู้ใช้งาน

(๗) เลขที่อยู่ไอพี (IP Address) ภายในของระบบเครือข่ายภายในของโรงพยาบาลจำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้

(๘) การใช้เครื่องมือต่างๆ เพื่อการตรวจสอบระบบเครือข่าย ควรได้รับการอนุมัติจากผู้ดูแลระบบและจำกัดการใช้งานเฉพาะที่จำเป็น

๓.๕.๓ ผู้ดูแลระบบต้องควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server) และรับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่าต่าง ๆ ของซอฟต์แวร์ระบบ (System Software)

๓.๕.๔ ให้ผู้ดูแลระบบที่ดูแลความมั่นคงปลอดภัยสารสนเทศที่โรงพยาบาลแต่งตั้ง กำหนดมาตรการควบคุมการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์ (Log) มี

ความถูกต้องและสามารถระบุถึงตัวบุคคลได้ตามแนวทาง ดังต่อไปนี้

(๑) ควรจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วน ถูกต้อง แท้จริง และระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้ และข้อมูลที่ใช้ในการจัดเก็บต้องกำหนดชั้นความลับในการเข้าถึงข้อมูลและผู้ดูแลระบบไม่ได้รับอนุญาตในการแก้ไขข้อมูลที่เก็บรักษาไว้ ยกเว้นผู้ตรวจสอบระบบสารสนเทศของโรงพยาบาล (IT Auditor) หรือบุคคลที่โรงพยาบาลมอบหมาย ทั้งนี้การจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ต้องเป็นไปตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์พ.ศ. ๒๕๕๐

(๒) ควรกำหนดให้มีการบันทึกการทำงานของระบบบันทึกการปฏิบัติงานของผู้ใช้งาน (Application Log) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้าออกระบบ บันทึกการพยายาม เข้าสู่ระบบ บันทึกการใช้งาน Command Line และ Firewall Log เป็นต้น เพื่อประโยชน์ในการตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย ๙๐ วัน นับตั้งแต่การใช้บริการสิ้นสุดลง

(๓) ควรตรวจสอบบันทึกการปฏิบัติงานหรือรายงานการเข้าถึงของผู้ใช้งานระบบสารสนเทศของโรงพยาบาลอย่างสม่ำเสมอ

(๔) ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่าง ๆ และจำกัดสิทธิการเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

(๕) ให้ผู้รับผิดชอบในส่วนงานกำหนดมาตรการควบคุมบุคคลจากหน่วยงานภายนอก ที่ต้องการสิทธิในการเข้าใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) ของโรงพยาบาล โดยจะต้องขออนุญาตเป็นลายลักษณ์อักษรต่อผู้บังคับบัญชา

(๖) มีการควบคุมช่องทาง (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุมและมีการป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ ดังนี้

(ก) กำหนดให้มีการเข้ารหัสในลักษณะของ TLS เวอร์ชัน ๑.๒ เป็นอย่างน้อยสำหรับการเข้าถึงพอร์ตที่ใช้ปรับแต่งระบบ

(ข) กำหนดรหัสผู้ใช้และรหัสผ่านสำหรับผู้ที่มีสิทธิ

(ค) ติดตั้งอุปกรณ์สำหรับการป้องกันตรวจสอบระบบเครือข่ายจากภายนอก

(ง) กำหนดให้มีการระบุอุปกรณ์บนเครือข่าย โดยต้องมีวิธีการที่สามารถระบุอุปกรณ์บนเครือข่ายได้และใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยัน ดังนี้

๑) มีการจัดทำทะเบียนรายการเครื่องคอมพิวเตอร์และอุปกรณ์ที่สามารถเชื่อมต่อกับเครื่องคอมพิวเตอร์และระบบเครือข่ายของโรงพยาบาล ได้แก่ รายชื่อผู้ขอใช้บริการรายละเอียดเครื่องคอมพิวเตอร์หรืออุปกรณ์ที่ขอใช้บริการ IP Address และสถานที่ติดตั้ง

๒) ทบทวนทะเบียนรายการเครื่องคอมพิวเตอร์และอุปกรณ์บนเครือข่ายอย่างสม่ำเสมออย่างน้อยปีละ ๑ ครั้ง

(๗) ทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งานและกลุ่มของระบบสารสนเทศ รวมถึงระบบสารสนเทศที่ไวต่อการรบกวนที่มีผลกระทบและมีความสำคัญสูงต่อองค์กรต้องได้รับการแยกออกจากระบบอื่น ๆ ดังนี้

(ก) แบ่งแยกเครือข่ายด้วยอุปกรณ์ป้องกันการบุกรุก (Firewall) โดยเฉพาะในส่วนของระบบฐานข้อมูลและระบบโปรแกรมประยุกต์ (Application) ด้วยพอร์ตการใช้งานเฉพาะ

(ข) กำหนดกลุ่มของเครือข่ายเสมือน (VLAN) เพื่อแบ่งแยก

๑) ผู้ใช้งานระหว่างกลุ่มหรือโรงพยาบาลหรือพื้นที่การใช้งาน

๒) กลุ่มผู้ใช้งานกับระบบสารสนเทศหลัก

๓) ระบบสารสนเทศหลักกับเครือข่ายภายนอก

(๘) การควบคุมการเชื่อมต่อทางเครือข่ายที่มีการใช้งานร่วมกันหรือเชื่อมต่อระหว่างโรงพยาบาล ดังนี้

(ก) กำหนดให้แต่ละกลุ่มหรือโรงพยาบาลภายในมีเครือข่ายเสมือนของตนเอง

(ข) การเชื่อมต่อระหว่างเครือข่ายกำหนดโดยอุปกรณ์สลับเส้นทางหลัก(Core Switch)

(ค) เครือข่ายเสมือนที่ต่างกันไม่สามารถติดต่อกันได้ ยกเว้นการเชื่อมต่อมายังระบบสารสนเทศของโรงพยาบาล

(๙) การควบคุมการจัดเส้นทางบนเครือข่าย มีดังนี้

(ก) กำหนดการควบคุมการจัดการเส้นทางบนเครือข่ายผ่านอุปกรณ์สลับเส้นทางหลัก (Core Switch)

(ข) เครือข่ายเสมือนที่ต่างกันไม่สามารถติดต่อกันได้ ยกเว้นการเชื่อมต่อมายังระบบสารสนเทศส่วนกลาง

(๑๐) วิธีการใด ๆ ที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้จากระยะทางไกลต้องได้รับการอนุญาตจากส่วนงานขึ้นตรงเลขาธิการด้านดิจิทัล

(๑๑) การเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับหน่วยงานอย่างเพียงพอ

(ก) การใช้งานระบบต้องผ่านการพิสูจน์ตัวตนจากระบบของโรงพยาบาล

(ข) ควบคุมและป้องกันการใช้งานพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย ดังนี้

๑) ผู้ใช้งานต้องมีการขออนุญาตเข้าถึงพอร์ตดังกล่าวอย่างเป็นลายลักษณ์อักษร

๒) ผู้ดูแลระบบต้องควบคุมให้มีการบันทึกการเข้าใช้งานทุกครั้ง รวมถึงตรวจสอบบันทึกการเข้าใช้งานอย่างสม่ำเสมอ

๓) ผู้ดูแลระบบต้องเปิดพอร์ตสื่อสาร (Port) เท่าที่จำเป็นต้องใช้งานเท่านั้น โดยผู้ดูแลระบบต้องดำเนินการตรวจสอบพอร์ตสื่อสาร (Port) และปิดพอร์ตสื่อสาร (Port) ที่ไม่มีความจำเป็นในการใช้งานของระบบหรืออุปกรณ์และกรณีที่จำเป็นต้องใช้งานพอร์ตสื่อสาร (Port) จะต้องมีการยืนยันตัวตนทุกครั้งก่อนอนุญาติให้ใช้งาน

๓.๖ การควบคุมการเข้าถึงระบบปฏิบัติการ

๓.๖.๑ ให้กลุ่มงานที่ได้รับมอบหมายบริหารศูนย์คอมพิวเตอร์ควบคุมการเข้าถึงระบบปฏิบัติการโดยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย ดังต่อไปนี้

(๑) ควบคุมการเข้าถึงระบบปฏิบัติการ เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต และอนุญาตให้มีการใช้งานได้เฉพาะผู้ใช้งานที่ได้รับการอนุมัติอย่างเป็นลายลักษณ์อักษร

(๒) ควบคุมให้ไม่มีการเปิดเผยข้อมูลที่เกี่ยวข้องกับระบบหรือแอปพลิเคชันจนกว่าผู้ใช้งานจะผ่านขั้นตอนการยืนยันตัวตนเพื่อเข้าใช้งานระบบอย่างสมบูรณ์

(๓) ควบคุมให้มีการแจ้งเตือนโดยระบุว่าอนุญาตเฉพาะบุคคลที่เกี่ยวข้องเท่านั้น ที่มีสิทธิเข้าใช้งานและให้มีการบันทึกล็อก (Log) การเข้าใช้งานทุกครั้งที่ผู้ใช้งานทำการเข้าถึงระบบทั้งที่ดำเนินการสำเร็จและดำเนินการไม่สำเร็จ

(๔) ระงับการล็อกอินเป็นระยะเวลาตามที่กำหนดหากตรวจสอบพบว่ามีการยืนยันตัวตน

ไม่ถูกต้องติดต่อกัน

(๕) ควบคุมไม่ให้มีการส่งรหัสผ่านโดยไม่มีการเข้ารหัสระหว่างการยืนยันการเข้าถึงระบบหรือแอปพลิเคชันผ่านระบบเครือข่าย

(๖) ควบคุมให้มีการตัดการใช้งาน หลังจากที่ไม่มีกิจกรรมการใช้งานเป็นเวลาอย่างน้อย ๓๐ นาที หรือตามความจำเป็นของระบบสารสนเทศที่กำหนด

๓.๖.๒ ผู้ดูแลระบบต้องควบคุมให้มีการระบุและยืนยันตัวตนด้วยชื่อผู้ใช้งาน ดังต่อไปนี้

(๑) ต้องกำหนดให้ผู้ใช้งานมีบัญชีผู้ใช้งานของแต่ละบุคคล เพื่อใช้ในการยืนยันตัวตนในการเข้าถึงระบบสารสนเทศ

(๒) ต้องควบคุมให้มีการยืนยันตัวตนของผู้ใช้งานผ่านระบบที่โรงพยาบาลกำหนด เช่น AD (Active Directory), LDAP (Lightweight Directory Access Protocol), ระบบ SSO (Single Sign On) ของโรงพยาบาลทุกครั้งพร้อมบันทึกข้อมูลการเข้าถึง

(๓) ในกรณีที่มีความจำเป็นต้องมีการใช้บัญชีผู้ใช้ร่วมกัน (Shared User ID) ผู้ใช้งานต้องได้รับอนุมัติจากผู้บังคับบัญชาและต้องมีตรวจสอบการใช้งานของบัญชีผู้ใช้งานดังกล่าวอย่างสม่ำเสมอ

๓.๖.๓ ผู้ดูแลระบบต้องจัดทำหรือจัดให้มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (Interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งรองรับการบริหารจัดการรหัสผ่านอย่างน้อย ดังนี้

(๑) การตั้งบัญชีผู้ใช้งานของแต่ละบุคคล

(๒) การกำหนดรหัสผ่านที่มีความซับซ้อน

(๓) การเปลี่ยนรหัสผ่านตามรอบที่กำหนด

(๔) ไม่อนุญาตให้ใช้รหัสผ่านซ้ำตามจำนวนครั้งที่กำหนด

(๕) ตัดการเชื่อมต่อหากตรวจสอบพบว่ามีการยืนยันตัวตนไม่ถูกต้องติดต่อกัน

(๖) ไม่แสดงรหัสผ่านจริงบนหน้าจอในขณะที่มีการเข้าสู่ระบบรับส่ง และเก็บรหัสผ่านแยกจากข้อมูลอื่นในรูปแบบที่ปลอดภัย โดยการเข้ารหัส

๓.๖.๔ ผู้ดูแลระบบต้องจำกัดและควบคุมการใช้งานโปรแกรมประเภทอรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว ดังนี้

(๑) ไม่อนุญาตให้ผู้ใช้งานติดตั้งโปรแกรมอรรถประโยชน์ใด ๆ ลงในเครื่องคอมพิวเตอร์ของโรงพยาบาล เว้นแต่จะได้รับอนุญาตจากผู้บังคับบัญชา โดยต้องพิจารณาให้สิทธิตามหน้าที่ความรับผิดชอบและความจำเป็นที่ต้องใช้งานเท่านั้น และโปรแกรมอรรถประโยชน์ที่นำมาใช้จะต้องถูกต้องตามลิขสิทธิ์การใช้งาน

(๒) หากโปรแกรมอรรถประโยชน์ใด ๆ จำเป็นต้องใช้สิทธิสูงในการดำเนินงานจะต้องมีการบันทึก จัดเก็บหลักฐานในการขอใช้สิทธิระดับสูงเพื่อการทบทวนและตรวจสอบสิทธิตามรอบการทบทวน สิทธิที่โรงพยาบาลได้กำหนด

(๓) ต้องมีการบันทึกเหตุการณ์ (Log) การใช้งานโปรแกรมอรรถประโยชน์และตรวจสอบอย่างสม่ำเสมอ

(๔) ต้องทำการเพิกถอนหรือระงับโปรแกรมอรรถประโยชน์เมื่อไม่จำเป็นต้องใช้งาน

๓.๖.๕ ผู้ดูแลระบบต้องให้ยุติการใช้งานระบบสารสนเทศนั้น เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่ง (Session Time-Out) ดังนี้

(๑) กำหนดให้มีการตัดการใช้งาน หลังจากที่ไม่มีกิจกรรมการใช้งานอุปกรณ์ที่เชื่อมต่อเข้าระบบสารสนเทศเป็นเวลา ๓๐ นาทีโดยอัตโนมัติหรือแล้วแต่ความเหมาะสมของระบบสารสนเทศ

(๒) หากระบบไม่สามารถตัดการเชื่อมต่อแบบอัตโนมัติต้องกำหนดให้ใช้โปรแกรมพักหน้าจอที่ต้องใส่รหัสผ่านหรือกำหนดให้มีการล็อคหน้าจอหลังจากไม่มีการใช้งานเป็นเวลา ๑๐ นาที

๓.๖.๖ ต้องจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ หรือโปรแกรมประเภทอรรถประโยชน์ที่มีความเสี่ยงสูงหรือมีความสำคัญสูง ดังนี้

(๑) การเข้าถึงระบบสารสนเทศหรือโปรแกรมประเภทอรรถประโยชน์ที่มีความเสี่ยงสูงหรือมีความสำคัญสูงทั้งจากภายในโรงพยาบาลและการใช้งานในสถานที่สาธารณะหรือพื้นที่นอกโรงพยาบาลต้องกำหนดให้มีการยืนยันตัวตนซ้ำหลังจากเข้าใช้งานต่อเนื่องอย่างน้อยทุก ๘ ชั่วโมง

(๒) กำหนดให้มีการตัดการใช้งานหรือการเชื่อมต่อผ่านระบบอินเทอร์เน็ตหรือเครือข่ายเสมือน (VPN) หลังจากที่ไม่มีกิจกรรมการใช้งานเป็นเวลา ๑๕ นาที

๓.๗ การควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่

๓.๗.๑ ผู้ดูแลระบบต้องควบคุมให้มีการติดตั้งโปรแกรมป้องกันไวรัสในอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และต้องปรับปรุงให้โปรแกรมดังกล่าวทันสมัยอยู่เสมอ

๓.๗.๒ ผู้ดูแลระบบต้องมีการเข้ารหัสไฟล์ข้อมูลที่มีการเข้ารหัสอัลกอริทึม (Algorithm) ที่เป็นมาตรฐานสากล ได้แก่ Triple DES หรือ RSA ในส่วนการจัดเก็บข้อมูล (file encryption) ที่มีความสำคัญต่อโรงพยาบาล

๓.๗.๓ ผู้ดูแลระบบต้องควบคุมให้มีการระบุและยืนยันตัวตนที่มีความมั่นคงปลอดภัยสำหรับการเข้าถึงระบบงานของหน่วยงานจากภายนอกโรงพยาบาล ผ่านระบบ Active Directory หรือ Lightweight Directory Access Control ของโรงพยาบาลทุกครั้ง

๓.๗.๔ ผู้ดูแลระบบต้องดำเนินการทบทวนสิทธิในการเข้าถึงของผู้ใช้งานจากภายนอกองค์กรอย่างสม่ำเสมอ

๓.๘ การปฏิบัติเมื่อเกิดเหตุละเมิดการรักษาความมั่นคงปลอดภัย (กรณีการเข้าถึงระบบ โดยไม่ได้รับอนุญาต)

๓.๘.๑ เมื่อผู้ดูแลระบบได้รับแจ้งเหตุให้วิเคราะห์ว่าเป็นเหตุละเมิดประเภทใด เกิดผลกระทบอย่างไรและมีวิธีการรับมืออย่างไรบ้าง

๓.๘.๒ ผู้ดูแลระบบต้องรายงานให้โรงพยาบาลและบุคคลที่เกี่ยวข้องรับทราบทันทีตามขั้นตอนการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล (Personal data breach management procedure)

๓.๘.๓ ผู้ดูแลระบบปฏิบัติการตามวิธีรับมือกับเหตุละเมิดตามความเหมาะสม ในกรณีนี้อาจได้แก่ การเปลี่ยนแปลงรหัสผ่านการแยกระบบที่มีปัญหาออก การปิดบริการที่สงสัย การปิดเส้นทาง การเข้าสู่ระบบสารสนเทศ การยกเลิกบัญชีผู้ใช้งานที่ถูกใช้ในการเข้าถึงระบบโดยมิได้รับอนุญาต ในบางกรณีเจ้าหน้าที่ที่เกี่ยวข้องจะต้องค้นหาและจับกุมผู้ก่อเหตุละเมิด

๓.๘.๔ ผู้ดูแลระบบและเจ้าหน้าที่ที่เกี่ยวข้องรวบรวมข้อมูลและหลักฐานของเหตุการณ์

๓.๘.๕ ผู้ดูแลระบบตรวจสอบว่าวิธีการรับมือที่ใช้ได้ผลหรือมีประสิทธิภาพหรือไม่ แล้วเพิ่มเติมมาตรการเพื่อลดช่องโหว่หรือถอดแยกส่วนของระบบสารสนเทศที่มีปัญหาออก

๓.๘.๖ ผู้ดูแลระบบกู้คืนระบบสารสนเทศสู่สภาพเดิมและทำรายงานแจ้งผู้ที่เกี่ยวข้อง

๓.๙ การปฏิบัติภายหลังการเกิดเหตุละเมิดการรักษาความมั่นคงปลอดภัย

หลังจากเกิดเหตุละเมิดความมั่นคงปลอดภัย ผู้รับผิดชอบในส่วนงานจะต้องปฏิบัติตามกระบวนการดังต่อไปนี้

๓.๙.๑ รวบรวมการเรียนรู้รูปแบบของสถานการณ์ วิเคราะห์รายงานเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ

๓.๙.๒ สำรวจความเสียหายที่เกิดจากเหตุละเมิดการรักษาความมั่นคงปลอดภัย ตรวจสอบสาเหตุและจุดอ่อนหรือข้อบกพร่องที่ก่อให้เกิดการละเมิด ทำรายงานและทบทวนมาตรการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่เกี่ยวข้อง เสนอคณะกรรมการเพื่อพิจารณา

๓.๑๐ การสำรองข้อมูล

การพิจารณาคัดเลือกและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานที่เหมาะสม เจ้าหน้าที่ผู้ดูแลระบบจะต้องปฏิบัติ ดังต่อไปนี้

๓.๑๐.๑ พิจารณาและจัดหมวดหมู่ของข้อมูล โดยกำหนดระดับความสำคัญของข้อมูลที่จำเป็นต้องทำสำรอง

๓.๑๐.๒ สำหรับข้อมูลที่มีความลับสูงให้ทำการเข้ารหัสก่อนทำการสำรอง

๓.๑๐.๓ พิจารณากำหนดวิธีการสำรองในประเด็น ดังนี้

(๑) ขนาด (สำรองทั้งหมดหรือสำรองเฉพาะส่วนที่แตกต่าง)

(๒) ความถี่ของการสำรอง ควรกำหนดโดยคำนึงถึงความต้องการใช้หากข้อมูลสูญหายหรือเรียกใช้งานไม่ได้และความจำเป็นของข้อมูลเพื่อให้ธุรกิจขององค์กรดำเนินต่อไปได้อย่างไม่ติดขัดหรือเพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้

(๓) วางขั้นตอนการเรียกกลับมาใช้อย่างเป็นลายลักษณ์อักษร

๓.๑๐.๔ ระหว่างทำการสำรอง เจ้าหน้าที่จะต้องปฏิบัติ ดังต่อไปนี้

(๑) ตรวจสอบผลการสำรองข้อมูล ว่าได้ข้อมูลที่ถูกต้องและครบถ้วนสมบูรณ์หรือไม่

(๒) จัดทำบันทึกการสำรองข้อมูลให้ชัดเจน ครบถ้วนสมบูรณ์และง่ายต่อการสืบค้น

๓.๑๐.๕ หลังทำการสำรอง เจ้าหน้าที่จะต้องปฏิบัติ ดังต่อไปนี้

(๑) เก็บข้อมูลที่สำรองเอาไว้ในพื้นที่ที่ห่างออกไปไกลพอที่จะไม่ได้รับความเสียหายอันเกิดจากภัยพิบัติในพื้นที่หลัก

(๒) ข้อมูลที่สำรองจะต้องได้รับการป้องกันทั้งทางกายภาพและสภาพแวดล้อมที่เหมาะสมตามมาตรฐานเดียวกับที่ใช้ในข้อมูลหลัก มาตรการที่ใช้ป้องกันสื่อบันทึกข้อมูลในพื้นที่หลักก็ควรนำมาใช้กับพื้นที่สำรองด้วย

(๓) ทำการทดสอบสื่อบันทึกข้อมูลสำรองและขั้นตอนในการนำข้อมูลสำรองกลับมาใช้ควรได้รับการตรวจสอบและทดสอบอย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจว่ามีประสิทธิภาพเพียงพอ และสามารถทำได้เสร็จสิ้นภายในระยะเวลาที่ถูกจัดสรรไว้ตามกระบวนการกู้คืน เพื่อให้มั่นใจว่าสามารถนำข้อมูลกลับมาใช้อีกได้เมื่อเกิดเหตุการณ์ฉุกเฉินจริง

(๔) จัดหาตู้เก็บหรือที่จัดเก็บสื่อบันทึกข้อมูลสำรอง เพื่อให้เป็นหมวดหมู่และเป็นระเบียบเรียบร้อย ง่ายต่อการค้นหาหรือนำกลับมาใช้และจัดให้มีการควบคุมการนำสื่อบันทึกไปใช้ที่สามารถตรวจสอบได้

๓.๑๑ การสำรองและกู้คืนข้อมูล

๓.๑๑.๑ รับผิดชอบในการสำรองและกู้คืนข้อมูลต้องมีขั้นตอนปฏิบัติ ดังนี้

(๑) ผู้อำนวยการที่รับผิดชอบในส่วนงานเป็นผู้กำกับดูแลการปฏิบัติงานในการสำรอง และกู้คืนข้อมูล และกำหนดแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

(๒) ผู้ดูแลระบบที่ได้รับมอบหมายจากส่วนงานขึ้นตรงเลขาธิการด้านดิจิทัล เป็นเจ้าหน้าที่

ผู้ปฏิบัติงานในการสำรองและกู้คืนข้อมูลและเป็นผู้จัดทำวิธีปฏิบัติการสำรองและกู้คืนข้อมูลของโรงพยาบาล

๓.๑๑.๒ ผู้ดูแลระบบร่วมกับผู้บังคับบัญชาต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง ดังนี้

(๑) ดำเนินการวิเคราะห์และคัดเลือกระบบที่มีความสำคัญสูง

(๒) ดำเนินการวิเคราะห์เหตุการณ์ที่มีผลทำให้ระบบที่มีความสำคัญสูงติดขัดหรือไม่สามารถทำงานได้อันเป็นผลมาจากภัยพิบัติ

(๓) ดำเนินการวิเคราะห์ผลกระทบอันเป็นผลมาจากภัยพิบัติต่อระบบที่มีความสำคัญสูง

(๔) ผู้ดูแลระบบ ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติ

(๕) ผู้ดูแลระบบ ต้องดำเนินการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉินอย่างสม่ำเสมออย่างน้อยปีละ ๑ ครั้ง และดำเนินการปรับปรุงแผนให้เป็นปัจจุบัน โดยในการทดสอบผู้ดูแลระบบต้องสื่อสารแผนเตรียมความพร้อมกรณีฉุกเฉินให้ผู้ใช้งานที่เกี่ยวข้องได้รับทราบ และผู้ใช้งานที่เกี่ยวข้องกับแผนเตรียมความพร้อมกรณีฉุกเฉิน ต้องเข้าร่วมการทดสอบแผนและดำเนินงานตามแผนที่กำหนดไว้เมื่อเกิดเหตุการณ์ฉุกเฉิน

๓.๑๒ การสร้างความตระหนัก

ผู้รับผิดชอบต้องอบรมเรียนรู้เพื่อสร้างความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศ ดังนี้

๓.๑๒.๑ ผู้ดูแลระบบต้องฝึกอบรม เรียนรู้ในส่วนงานที่รับผิดชอบในด้านความมั่นคงปลอดภัยสารสนเทศอย่างต่อเนื่องและนำมาประยุกต์ใช้อย่างเคร่งครัด สม่ำเสมอ

๓.๑๒.๒ ส่วนงานขึ้นตรงเลขาธิการด้านดิจิทัลเป็นผู้ให้การสนับสนุนในการอบรมสร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนักความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศอย่างน้อย ๑ ครั้งต่อปี

๓.๑๒.๓ ผู้รับผิดชอบการอบรมต้องมีการจัดเก็บบันทึกเอกสารในการจัดฝึกอบรมไว้เป็นหลักฐานด้วย เช่น บันทึกการฝึกอบรม เอกสารฝึกอบรม เป็นต้น

๓.๑๒.๔ ผู้รับผิดชอบการอบรม ต้องดำเนินการประเมินผลการอบรมเพื่อวัดระดับความเข้าใจของผู้เข้ารับการอบรมและรับฟังข้อเสนอแนะเพื่อนำไปปรับปรุงการอบรมครั้งต่อไป โดยอาจใช้แบบประเมินความเข้าใจ แบบสอบถาม ความคิดเห็นหรือวิธีการอื่นที่เหมาะสม

๓.๑๓ การตรวจสอบและการประเมินผล

๓.๑๓.๑ โรงพยาบาลต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (information security audit and assessment) อย่างน้อยปีละ ๑ ครั้ง โดยผู้ตรวจสอบภายใน (internal auditor) เพื่อให้โรงพยาบาลได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศและเพื่อลดความเสี่ยงในการเกิดการหยุดชะงักของการให้บริการ รวมถึงจัดให้มีการทำแผนเพื่อปรับปรุงหรือแก้ไขปัญหาที่พบ โดยต้องมีการวางแผนการตรวจสอบ และกำหนดกิจกรรมที่เกี่ยวข้องกับการตรวจสอบระบบสารสนเทศ

๓.๑๓.๒ โรงพยาบาลต้องควบคุมการเข้าถึงและใช้งานเครื่องมือที่ใช้ในการตรวจสอบและประเมินความเสี่ยงเพื่อมิให้เกิดการใช้งานผิดประเภทหรือถูกละเมิดการใช้งาน (Compromise) เพื่อลดความเสี่ยงที่อาจ

เกิดขึ้นกับระบบ เช่น การหยุดชะงักของการให้บริการ การใช้งานผิดประเภท หรือถูกละเมิดการใช้งานเป็นต้น

๓.๑๓.๓ โรงพยาบาลต้องจัดทำรายงานผลการตรวจสอบและประเมินความเสี่ยงสารสนเทศ พร้อมข้อเสนอแนะเพื่อการปรับปรุง และนำเสนอให้ผู้บังคับบัญชารับทราบและพิจารณาดำเนินการตามความเหมาะสม ทั้งนี้ต้องมีการติดตามผลการดำเนินการแก้ไขปรับปรุงตามข้อเสนอแนะเป็นระยะ

๓.๑๔ ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๓.๑๔.๑ การจัดทำประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ มีดังนี้

(๑) แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

(๒) ต้องจัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ ทั้งโดยผู้ตรวจสอบภายในหรือโดยผู้ตรวจสอบอิสระภายนอกอย่างน้อย ปีละ ๑ ครั้ง โดยมีขอบเขตของการตรวจสอบ ดังนี้

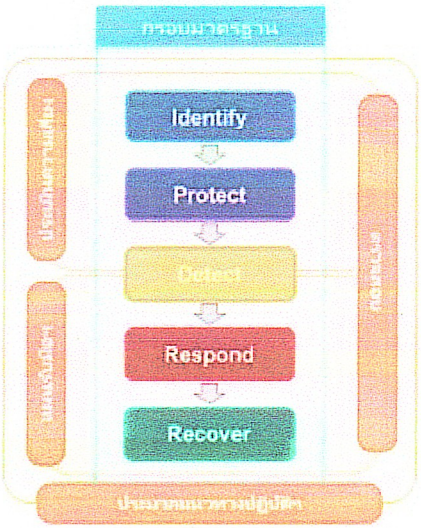
(ก) กระบวนการจัดทำและผลการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA)

(ข) บริการที่สำคัญที่โรงพยาบาลเป็นเจ้าของและใช้หรือให้บริการตามผลการวิเคราะห์ในข้อ ๓.๑๔.๑ (๒) (ก)

(๓) จัดส่งผลสรุปรายงานการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์เสนอโรงพยาบาลหรือคณะกรรมการที่กำกับดูแล

(๔) ต้องมีการจัดทำเอกสารประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างชัดเจนครอบคลุมนโยบาย มาตรการควบคุมและขั้นตอนปฏิบัติงาน โดยต้องมีการทบทวน และปรับปรุงเอกสารอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงสำคัญ

(๕) หน่วยงานที่รับผิดชอบต้องจัดทำแผนปรับปรุงหรือแก้ไขตามข้อค้นพบจากการตรวจสอบและรายงานความก้าวหน้าในการดำเนินการต่อโรงพยาบาลหรือคณะกรรมการที่เกี่ยวข้อง



รูปที่ ๑ ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๓.๑๔.๒ การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แนวปฏิบัติ เพื่อให้โรงพยาบาลสามารถประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ได้อย่างมีประสิทธิภาพ และต่อเนื่องโรงพยาบาลต้องกำหนดนโยบายการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามที่ระบุไว้ในนโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับโรงพยาบาลให้ครอบคลุมเรื่องโครงสร้างองค์กรและบทบาทหน้าที่ของผู้ที่เกี่ยวข้องในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และต้องนำนโยบายดังกล่าวมาจัดทำระเบียบวิธีปฏิบัติและกระบวนการในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของโรงพยาบาล โดยต้องจัดให้มีการประเมินความเสี่ยงด้านการรักษาความมนคงปลอดภัยไซเบอร์ อย่างน้อยปีละ ๑ ครั้ง ต้องประกอบด้วยรายละเอียดอย่างน้อยดังต่อไปนี้

(๑) การประเมินความเสี่ยง (Risk Assessment)

(ก) การระบุความเสี่ยง (Risk Identification) ต้องระบุถึงความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งรวมถึงความเสี่ยงจากภัยคุกคามทางไซเบอร์และช่องโหว่ต่าง ๆ โดยความเสี่ยงดังกล่าวอาจมีสาเหตุมาจากกระบวนการปฏิบัติงาน ระบบงานบุคลากรหรือปัจจัยภายนอก

(ข) การวิเคราะห์ความเสี่ยง (Risk Analysis) ต้องเข้าใจและวิเคราะห์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อหาแนวทางในการจัดการความเสี่ยงที่เหมาะสม

(ค) การประเมินค่าความเสี่ยง (Risk Evaluation) ต้องประเมินถึงโอกาส ที่ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์จะเกิดขึ้นและผลกระทบต่อการปฏิบัติงานและการดำเนินธุรกิจรวมถึงกำหนดระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ (Risk Appetite)

(๒) การจัดการความเสี่ยง (Risk Treatment) ต้องมีแนวทางจัดการควบคุมและป้องกันความเสี่ยงที่เหมาะสมสอดคล้องกับผลการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้ความเสี่ยงที่เหลืออยู่ (Residual Risk) อยู่ในระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ โดยต้องคำนึงถึงความสมดุลระหว่างต้นทุนในการป้องกันความเสี่ยงและผลประโยชน์ที่คาดว่าจะได้รับนอกจากนี้ต้องกำหนดดัชนีชี้วัดความเสี่ยงที่สำคัญ (Key Risk Indicator: KRI) ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับการดำเนินธุรกิจ ให้สอดคล้องกับความสำคัญของความมั่นคงปลอดภัยไซเบอร์แต่ละงานเพื่อใช้ติดตามและทบทวนความเสี่ยง

(๓) การติดตามและทบทวนความเสี่ยง (Risk Monitoring and Review) ต้องมีกระบวนการที่มีประสิทธิภาพในการติดตาม และทบทวนความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้อยู่ภายใต้ระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ตามที่กำหนดไว้

(๔) การรายงานความเสี่ยง (Risk Reporting) ต้องรายงานระดับความเสี่ยง และผลการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ต่อคณะกรรมการของหน่วยงานที่ได้รับมอบหมายเป็นประจำ เช่น ตามรอบการประชุมของคณะกรรมการของหน่วยงานที่ได้รับมอบหมาย ทั้งนี้ ต้องทบทวนระเบียบวิธีปฏิบัติและกระบวนการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ ๑ ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เช่น กรณีที่มีการเปลี่ยนแปลงของระบบความมั่นคงปลอดภัยไซเบอร์ ความเสี่ยง มาตรฐานสากล อย่างมีนัยสำคัญ เป็นต้น

(๕) บทบาทผู้รับผิดชอบ ต้องกำหนดบทบาทหน้าที่ของผู้ที่เกี่ยวข้องกับการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างชัดเจน ดังนี้

(ก) ผู้อำนวยการโรงพยาบาลหรือผู้บริหารระดับสูง เป็นผู้กำหนดนโยบายและกำกับภาพรวมของการบริหารความเสี่ยง

(ข) หัวหน้าหน่วยงานด้านความมั่นคงปลอดภัยไซเบอร์ (เช่น CISO) รับผิดชอบการกำหนดแนวทางและติดตามผลการประเมิน

(ค) เจ้าหน้าที่ความมั่นคงปลอดภัยสารสนเทศ รับผิดชอบดำเนินการประเมินความเสี่ยง จัดทำรายงานและควบคุมมาตรการ

(ง) เจ้าหน้าที่ของหน่วยงานต่างๆ มีหน้าที่ให้ข้อมูลที่เกี่ยวข้องเพื่อประเมินความเสี่ยงอย่างถูกต้อง

(๖) วิธีการและเครื่องมือที่ใช้ในการประเมิน โรงพยาบาลควรกำหนดเครื่องมือที่มีประสิทธิภาพเพื่อใช้ในการประเมินความเสี่ยง ดังนี้

(ก) แบบฟอร์มประเมินความเสี่ยง ที่ครอบคลุมความน่าจะเป็นผลกระทบและมาตรการควบคุม

(ข) การใช้ Risk Matrix หรือ Heatmap เพื่อจัดลำดับความสำคัญของความเสี่ยง

(ค) เครื่องมือซอฟต์แวร์สำหรับบริหารความเสี่ยง (เช่น GRC Tools) หากมีความพร้อมด้านงบประมาณ

(ง) การอ้างอิงข้อมูลจาก Threat Intelligence ภายนอก เช่น CERT หรือฐานข้อมูลช่องโหว่ (CVE)

(๗) การให้ความรู้และสร้างความเข้าใจในองค์กร โรงพยาบาลต้องดำเนินการอบรม และเสริมสร้างความเข้าใจเรื่องการประเมินความเสี่ยงด้านไซเบอร์แก่ผู้เกี่ยวข้อง ดังนี้

(ก) จัดอบรมและเวิร์กช็อปให้เจ้าหน้าที่เข้าใจแนวทางการประเมินความเสี่ยงอย่างน้อยปีละ ๑ ครั้ง

(ข) ส่งเสริมการเรียนรู้แบบ On-the-job Training โดยเจ้าหน้าที่ความมั่นคง

(ค) จัดทำเอกสารคู่มือแนวทางขั้นตอน เช่น แบบฟอร์มและกรณีศึกษา

๓.๑๔.๓ แผนการรับมือภัยคุกคามทางไซเบอร์ แนวปฏิบัติ

(๑) ต้องจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan) ที่กำหนดว่าควรตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์อย่างไร โดยแผนการรับมือภัยคุกคามทาง ไซเบอร์ ต้องมีรายละเอียดอย่างน้อยดังต่อไปนี้

(ก) โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT) รวมถึงบทบาทและความรับผิดชอบที่กำหนดไว้อย่างชัดเจนของสมาชิก ในทีมแต่ละคนและรายละเอียดการติดต่อ

(ข) โครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure) ซึ่งกำหนดว่าโรงพยาบาลจะปฏิบัติตามภาระหน้าที่ในการรายงานภายใต้พระราชบัญญัติและกฎหมายย่อยใด ๆ ที่ทำขึ้นภายใต้กฎหมายดังกล่าวตลอดจนภาระหน้าที่ในการรายงานภายใต้กฎหมายและข้อกำหนดด้านกฎระเบียบ ที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(ค) เกณฑ์และขั้นตอนในการเรียกใช้งาน (Activate) การตอบสนองต่อเหตุการณ์และ CIRT

(ง) ขั้นตอนจำกัดขอบเขต (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

(จ) การเรียกใช้งานกระบวนการกู้คืน (Recovery Process)

(ฉ) ขั้นตอนในการสอบสวน (Investigate) สาเหตุและผลกระทบของเหตุการณ์

(ช) ขั้นตอนการเก็บรักษาหลักฐาน (Preservation of Evidence) ก่อนเริ่มกระบวนการกู้คืน ซึ่งรวมถึงการได้มาของบันทึกการยึดหลักฐานคอมพิวเตอร์ที่ได้มาหรืออุปกรณ์อื่น ๆ เพื่อสนับสนุนการสอบสวน

(ซ) ระเบียบวิธีการมีส่วนร่วม (Engagement Protocols) กับบุคคลภายนอกหรือแนวปฏิบัติการบริหารจัดการบุคคลภายนอก ซึ่งรวมถึงรายละเอียดการติดต่อ เช่น ผู้ขาย สำหรับบริการด้านนิติวิทยาศาสตร์/การกู้คืนและการบังคับใช้กฎหมายเพื่อดำเนินคดี

(ฌ) กระบวนการทบทวนหลังการดำเนินการ (After-Action Review Process) เพื่อระบุและแนะนำให้ปรับปรุงการดำเนินการเพื่อป้องกันการเกิดซ้ำ

(๒) ต้องตรวจสอบให้แน่ใจว่าแผนการรับมือภัยคุกคามทางไซเบอร์ได้รับการสื่อสารอย่างมีประสิทธิผลไปยังบุคลากรที่เกี่ยวข้องทั้งหมดที่สนับสนุนบริการสำคัญของโรงพยาบาล

(๓) ต้องทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ อย่างน้อยปีละ ๑ ครั้ง โดยนับแต่วันที่แผนได้รับการอนุมัติ

(๔) ต้องทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ เมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญในสภาพแวดล้อมการปฏิบัติการทางไซเบอร์ของบริการที่สำคัญของโรงพยาบาล

(๕) ต้องมีการทดสอบหรือซ้อมแผนตอบสนองต่อเหตุการณ์อย่างน้อยปีละ ๑ ครั้ง เช่น การจำลองเหตุการณ์ (Simulation) หรือการฝึกซ้อมแบบโต๊ะ (Tabletop Exercise) เพื่อประเมินความพร้อม ของทีมและปรับปรุงแผนให้ทันสมัย

(๖) ต้องมีการจัดทำบันทึกเหตุการณ์ (Incident Log) ทุกครั้งที่เกิดภัยคุกคามหรือเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ พร้อมรายละเอียดการดำเนินการตอบสนองและกู้คืนเพื่อใช้ในการทบทวนและรายงานต่อผู้มีอำนาจ

(๗) เจ้าของบริการที่สำคัญหรือผู้บริหารระดับสูงต้องให้การสนับสนุนทรัพย์กร และมีส่วนร่วมในการอนุมัติแผนรับมือภัยคุกคาม เพื่อให้แผนสามารถนำไปปฏิบัติได้จริงอย่างมีประสิทธิภาพ

๓.๑๔:๔ กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

(๑) กรอบมาตรฐาน ประกอบไปด้วย ๕ หัวข้อหลัก (ดังรูปที่ ๑) ดังนี้

(ก) การระบุความเสี่ยงที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ข้อมูลคอมพิวเตอร์ระบบคอมพิวเตอร์ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ทรัพย์สินและชีวิตร่างกายของบุคคล (Identify)

(ข) การจัดการทรัพย์สิน (Asset Management)

(ค) การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy)

(ง) การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing)

(จ) การจัดการผู้ให้บริการภายนอก (Third Party Management)

(๒) มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect)

(ก) การควบคุมการเข้าถึง (Access Control)

(ข) การทำให้ระบบมีความแข็งแกร่ง (System Hardening)

(ค) การเชื่อมต่อระยะไกล (Remote Connection)

(ง) สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media)

(จ) การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)

(ฉ) การแบ่งปันข้อมูลและข่าวกรองด้านความมั่นคงปลอดภัย (Information Sharing)

(ช) การดูแลรักษาและอัปเดตระบบ (System Maintenance and Patch Management)

(ซ) การรักษาความปลอดภัยของข้อมูล (Data Security)

(ฌ) เทคโนโลยีป้องกัน (Protective Technologies) เช่น Firewall, DLP, EDR

(๓) มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)

(ก) การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring)

(ข) การตรวจจับเหตุการณ์ผิดปกติและเหตุการณ์ต้องสงสัย (Anomalies and Events)

(ค) การตรวจสอบอย่างต่อเนื่อง(Security Continuous Monitoring)

(ง) กระบวนการตรวจจับที่กำหนดไว้ (Detection Processes)

(๔) มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)

(ก) แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)

(ข) แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)

(ค) การฝึกซ้อมรับมือเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise)

(ง) การวิเคราะห์เหตุการณ์และผลกระทบ (Incident Analysis)

(จ) มาตรการลดผลกระทบและจำกัดความเสียหาย (Mitigation)

(ฉ) การพัฒนาแนวปฏิบัติจากบทเรียนที่ผ่านมา (Improvements and Lessons Learned)

(๕) มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์

(ก) การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery)

(ข) การสื่อสารและประสานงานระหว่างกระบวนการฟื้นฟู (Recovery Communications)

(ค) การทบทวนและปรับปรุงแผนฟื้นฟู (Recovery Improve)

๓.๑๔.๕ หัวข้อหลักที่ ๑ การระบุความเสี่ยงที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ทรัพย์สินและชีวิตร่างกายของบุคคล (Identify)

<u>กรอบมาตรฐาน</u>

(๑) การจัดการทรัพย์สิน (Asset Management)

(ก) ต้องมีทะเบียนทรัพย์สิน (Inventory) ที่ระบุทรัพย์สินของบริการที่สำคัญของหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและดูแลรักษาทะเบียนทรัพย์สินให้เป็นปัจจุบัน โดยทะเบียนทรัพย์สินต้องมีข้อมูลอย่างน้อย ดังนี้

๑) ชื่อ/คำอธิบายของทรัพย์สิน บริการที่สำคัญของโรงพยาบาล

๒) ฟังก์ชันที่สำคัญของทรัพย์สิน บริการที่สำคัญของโรงพยาบาล

๓) การระบุและการจัดลำดับความสำคัญของทรัพย์สินบริการที่สำคัญของโรงพยาบาล

๔) เจ้าของและหรือผู้ดำเนินการของทรัพย์สิน บริการที่สำคัญของโรงพยาบาล

๕) ตำแหน่งทางกายภาพของทรัพย์สิน บริการที่สำคัญของโรงพยาบาล

๖) การขึ้นต่อกันของทรัพย์สิน บริการที่สำคัญของโรงพยาบาลบนระบบ/เครือข่ายภายในและ/หรือภายนอก

(ข) ต้องระบุขอบเขตเครือข่ายของบริการที่สำคัญของโรงพยาบาลและระบบคอมพิวเตอร์ที่เชื่อมต่อโดยตรงและมีนัยสำคัญ (Direct and Significant Interface)

(ค) ต้องมีการตรวจสอบทะเบียนทรัพย์สินอย่างน้อยปีละ ๑ ครั้ง หากมีการเปลี่ยนแปลงใด ๆ กับทรัพย์สินของบริการที่สำคัญของโรงพยาบาลให้ปรับปรุงทะเบียนทรัพย์สินดังกล่าวด้วย

(ง) ต้องดำเนินการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญของโรงพยาบาล ซึ่งรวมถึงรายการทั้งหมดที่ระบุไว้ในทะเบียนทรัพย์ในข้อ ๓.๑๔.๕ (๑) (ก) อย่างน้อยปีละ ๑ ครั้ง

(๒) การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy)

(ก) ต้องประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์อย่างน้อย ปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญที่กระทบต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศของโรงพยาบาล ทางสารสนเทศตามเกณฑ์ประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่กำหนดไว้ในการบริหารความเสี่ยง (Risk Management) ตามนโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ที่คณะกรรมการประกาศกำหนด

(ข) ต้องปรับปรุงทะเบียนความเสี่ยงทุกครั้งหลังการประเมินความเสี่ยง ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ทะเบียนความเสี่ยงต้องจัดทำเอกสารโดยมีรายละเอียดอย่างน้อย ดังต่อไปนี้

๑) วันที่ระบุความเสี่ยง (Date the Risk is Identified)

๒) คำอธิบายของความเสี่ยง (Description of the Risk)

๓) โอกาสที่จะเกิดขึ้น (Likelihood of Occurrence)

๔) ความรุนแรงของเหตุการณ์ (Severity of the Occurrence)

๕) การจัดการความเสี่ยง (Risk Treatment)

๖) เจ้าของความเสี่ยง (Risk Owner)

๗) สถานะของการจัดการความเสี่ยง (Status of Risk Treatment)

๘) ความเสี่ยงที่เหลือ (Residual Risk)

(๓) การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing)

(ก) ต้องดำเนินการประเมินช่องโหว่ของบริการที่สำคัญของโรงพยาบาล อ้างอิงตามหลักการบริหารความเสี่ยงของหน่วยงานเพื่อระบุจุดอ่อนด้านความมั่นคงปลอดภัยและการควบคุม โดยครอบคลุมบริการที่สำคัญของโรงพยาบาล ซึ่งเป็น

๑) ระบบเทคโนโลยีสารสนเทศ (Information Technology (IT) system)

๒) ระบบที่ใช้ควบคุมเครื่องจักรในอุตสาหกรรม (Industrial Control System: ICS)

(ข) ต้องตรวจสอบให้แน่ใจว่าขอบเขตของการประเมินช่องโหว่แต่ละรายการประกอบด้วย

๑) การประเมินความมั่นคงปลอดภัยของโฮสต์ (Host Security Assessment)

๒) การประเมินความมั่นคงปลอดภัยของเครือข่าย (Network Security Assessment)

๓) การตรวจสอบความมั่นคงปลอดภัยของสถาปัตยกรรม (Architecture Security Review)

(ก) ต้องทำการประเมินช่องโหว่ของบริการที่สำคัญของโรงพยาบาล เพื่อระบุจุดอ่อนด้านความมั่นคงปลอดภัยและควบคุมก่อนที่จะทำการทดสอบระบบใหม่ใด ๆ ที่เชื่อมต่อ

หรือดำเนินการเปลี่ยนแปลงระบบที่สำคัญใด ๆ กับบริการที่สำคัญของโรงพยาบาล การเปลี่ยนแปลงระบบที่สำคัญ ได้แก่ การเพิ่มโมดูลแอปพลิเคชัน (Adding New Application Module) การปรับปรุงระบบและการปรับเปลี่ยนเทคโนโลยี

(ง) ควรพิจารณาดำเนินการทดสอบเจาะระบบ (Penetration Testing) บริการที่สำคัญของโรงพยาบาล โดยเฉพาะอย่างยิ่งระบบเทคโนโลยีสารสนเทศ (Information Technology: IT) ที่เชื่อมต่อกับอินเทอร์เน็ต (Internet Facing) ให้สอดคล้องกับระดับของความเสี่ยง และพิจารณาผลกระทบหรือความเสี่ยงจากการทดสอบเจาะระบบด้วย

(จ) ต้องตรวจสอบให้แน่ใจว่าขอบเขตของการทดสอบเจาะระบบ (Scope of a Penetration Test) รวมถึงการทดสอบเจาะระบบของโฮสต์ เครือข่าย และแอปพลิเคชันบริการที่สำคัญของโรงพยาบาล โดยเฉพาะอย่างยิ่งทุกระบบที่เป็นมีการเชื่อมต่ออินเทอร์เน็ตโดยตรง (Internet Facing)

(ฉ) ควรพิจารณาดำเนินการทดสอบเจาะระบบอย่างน้อยปีละ ๑ ครั้ง ตามความจำเป็น เพื่อตรวจสอบความถูกต้องของระบบรักษาความมั่นคงปลอดภัยไซเบอร์ บริการที่สำคัญของโรงพยาบาล ก่อนที่จะทำการทดสอบระบบใหม่ หรือการเปลี่ยนแปลงระบบที่สำคัญ เช่น โมดูลเสริมการปรับปรุงระบบ และการปรับเปลี่ยนเทคโนโลยี เป็นต้น

(ช) ต้องตรวจสอบให้แน่ใจว่าการทดสอบเจาะระบบและผู้ทดสอบเจาะระบบ (Penetration Testers) ที่ทำการทดสอบเจาะระบบบนโครงสร้างพื้นฐานสำคัญสารสนเทศมีการรับรองและได้รับ ประกาศนียบัตร (Accreditations and Certifications) ที่เป็นที่ยอมรับในอุตสาหกรรมและเป็นอิสระจากระบบที่ทำการทดสอบเจาะระบบ ทั้งนี้ คุณสมบัติของผู้ทดสอบเจาะระบบให้เป็นไปตามหลักเกณฑ์และวิธีการที่หน่วยงานควบคุมหรือกำกับดูแลกำหนด

(ซ) ต้องตรวจสอบให้แน่ใจว่าการทดสอบเจาะระบบทั้งหมดโดยผู้ให้บริการทดสอบเจาะระบบดำเนินการภายใต้การดูแลของหน่วยงาน

(ฌ) ต้องสร้างกระบวนการเพื่อติดตามและจัดการกับช่องโหว่ที่ระบุไว้ในผลการประเมินช่องโหว่และในผลการทดสอบเจาะระบบและตรวจสอบว่าช่องโหว่ที่ระบุทั้งหมดได้รับการแก้ไขอย่างเพียงพอ

(๔) การจัดการผู้ให้บริการภายนอก (Third Party Management)

(ก) ต้องรับผิดชอบ (Responsible) และมีภาระรับผิดชอบ (Accountable) ต่อการดูแลรักษาความมั่นคงปลอดภัยไซเบอร์ของโครงสร้างพื้นฐานสำคัญทางสารสนเทศ แม้ว่าผู้ให้บริการภายนอกจะดำเนินงานใด ๆ ก็ตามในส่วนของบริการที่สำคัญของโรงพยาบาล

(ข) ต้องกำหนดข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์เพื่อลดความเสี่ยง ที่เกี่ยวข้องกับการเข้าถึงกระบวนการจัดเก็บ การสื่อสารและการดำเนินการของโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ของผู้ให้บริการภายนอกในข้อตกลงระดับการให้บริการ (Service Level Agreement) หรือเงื่อนไขของสัญญากับผู้ให้บริการภายนอก โดยข้อกำหนดดังกล่าวต้องคำนึงถึงรายละเอียดอย่างน้อย ดังต่อไปนี้

๑) ประเภทของผู้ให้บริการภายนอกที่เข้าถึงทรัพย์สินของบริการที่สำคัญของโรงพยาบาลตามความต้องการทางธุรกิจของโรงพยาบาล และโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคง ปลอดภัยไซเบอร์

๒) ภาระหน้าที่ของผู้ให้บริการภายนอกในการปกป้องบริการที่สำคัญของ

โรงพยาบาลจากภัยคุกคามทางไซเบอร์

๓) ความเสี่ยงที่เกี่ยวข้องกับบริการและห่วงโซ่อุปทานผลิตภัณฑ์

๔) สิทธิของโรงพยาบาลในการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการภายนอก

(ค) ควรพิจารณาสร้างกระบวนการตรวจสอบความถูกต้องของผู้ให้บริการ ภายนอกว่าสอดคล้องกับข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ในเงื่อนไขของสัญญา เช่น การตรวจสอบ โดยบุคคลที่สามและการตรวจสอบผลิตภัณฑ์

(ง) ควรพิจารณาดำเนินการเจรจาต่อรองเงื่อนไขของสัญญาจ้างให้สอดคล้องกรณีที่มีข้อกำหนดทางกฎหมายหรือข้อบังคับใหม่

๓.๑๔.๖ หัวข้อหลักที่ ๒ มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect)

<u>กรอบมาตรฐาน</u>

(๑) การควบคุมการเข้าถึง (Access Control)

(ก) ต้องตรวจสอบให้แน่ใจว่าการเข้าถึงบริการที่สำคัญของโรงพยาบาลถูกจำกัดไว้ดังนี้

๑) บุคลากรและกิจกรรมที่ได้รับอนุญาต

๒) อุปกรณ์และอินเทอร์เฟซ (Interface) ที่ได้รับอนุญาต

(ข) ในส่วนที่เกี่ยวกับภาระหน้าที่ภายใต้ข้อ ๓.๑๔.๖ (๑) (ก) โรงพยาบาลต้องกำหนดให้แต่ละบุคลากร กิจกรรมและกระบวนการที่ได้รับอนุญาต มีการใช้เทคนิคการตรวจสอบสิทธิที่สอดคล้องกับโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Profile) สำหรับแต่ละโหมดการเข้าถึงบริการที่สำคัญของโรงพยาบาล

(ค) ต้องเก็บรักษาบันทึกของการเข้าถึงทั้งหมด (Logs of All Access) และความพยายามทั้งหมดในการเข้าถึงบริการที่สำคัญของโรงพยาบาล และตรวจสอบบันทึกเหล่านี้เพื่อหากิจกรรมที่ผิดปกติเป็นประจำ ความสม่ำเสมอในการตรวจสอบบันทึกเหล่านี้ควรสอดคล้องกับความถี่หรือความสม่ำเสมอ ของกิจกรรมการเข้าถึงดังกล่าว

(ง) ต้องตรวจสอบให้แน่ใจว่าการเข้าถึงอินเทอร์เฟซ (Interface) ของบริการที่สำคัญของโรงพยาบาล (เช่น USB, พอร์ตอนุกรม) และการเข้าถึงทางลอจิคอล (Logical) มีการกำกับดูแล ดังนี้

๑) ดำเนินการภายใต้การกำกับดูแลของส่วนงานขึ้นตรงเลขาธิการด้านดิจิทัล

๒) ดำเนินการในสถานที่ หากเป็นไปได้

(๒) การทำให้ระบบมีความแข็งแกร่ง (System Hardening)

(ก) ต้องสร้างมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) สำหรับระบบปฏิบัติการ แอปพลิเคชัน และอุปกรณ์เครือข่าย ทั้งหมดของบริการที่สำคัญของโรงพยาบาลที่สอดคล้องกับโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัย ไซเบอร์ (Cybersecurity Risk Profile) ของบริการที่สำคัญของโรงพยาบาล

(ข) มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ต้องมีหลักการรักษาความมั่นคงปลอดภัยอย่างน้อยดังต่อไปนี้

๑) สิทธิพิเศษในการเข้าถึงน้อยที่สุด (Least Access Privilege)

๒) การแบ่งแยกหน้าที่ (Separation of Duties)

๓) การบังคับใช้นโยบายความซับซ้อนของรหัสผ่าน

๔) การลบบัญชีที่ไม่ได้ใช้

๕) การลบบริการและแอปพลิเคชันที่ไม่จำเป็น เช่น การลบคอมไพเลอร์(Removal of Compiler) และแอปพลิเคชันสนับสนุนผู้ให้บริการภายนอก (Vendor Support Application)

๖) การปิดพอร์ตเครือข่ายที่ไม่ได้ใช้งาน

๗) การป้องกันมัลแวร์(Malware)

๘) การปรับปรุงซอฟต์แวร์และแพตช์ (Patch) ความมั่นคงปลอดภัยของระบบอย่างทันการณ์และเหมาะสม

(ค) ต้องตรวจสอบให้แน่ใจว่ามีการใช้มาตรฐานการกำหนดค่าขั้นต่ำ ด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ตามที่ระบุไว้ก่อนที่จะมีทรัพย์สินใด ๆ เชื่อมต่อหรือเมื่อมีการเปลี่ยนแปลงหรือปรับปรุงบริการที่สำคัญของโรงพยาบาล

(ง) ต้องตรวจสอบมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standard) ของบริการที่สำคัญของโรงพยาบาลอย่างน้อยปีละ ๑ ครั้ง เพื่อให้แน่ใจว่ามาตรฐานเหล่านี้ยังคงมีประสิทธิภาพต่อภัยคุกคามทางไซเบอร์

(จ) ต้องจัดทำกระบวนการจัดการเปลี่ยนแปลง (Change Management Process) เพื่ออนุญาตและตรวจสอบความถูกต้องของการเปลี่ยนแปลงระบบทั้งหมดที่มีต่อบริการที่สำคัญของโรงพยาบาล

(๓) การเชื่อมต่อระยะไกล (Remote Connection)

(ก) ต้องตรวจสอบให้แน่ใจว่าการเชื่อมต่อระยะไกลทั้งหมดมายังบริการที่สำคัญของโรงพยาบาล มีมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีประสิทธิภาพเพื่อป้องกันและตรวจจับการเข้าถึงโดยไม่ได้รับอนุญาต

(ข) สำหรับการเชื่อมต่อระยะไกลกับบริการที่สำคัญของโรงพยาบาล ต้องปฏิบัติตามแนวทางปฏิบัติ ดังต่อไปนี้

๑) ในกรณีที่เป็นไปได้ ให้เปิดใช้งานการเชื่อมต่อไปยังหรือจากไซต์ระยะไกล เมื่อจำเป็นเท่านั้น

๒) ในกรณีที่เป็นไปได้ ให้ใช้เทคนิคการพิสูจน์ตัวตน (Authentication Techniques) ที่มีความมั่นคงปลอดภัยในการส่ง (Transmission Security) และความสมบูรณ์ของข้อความ (Message Integrity) ที่แข็งแกร่ง

๓) ใช้การเข้ารหัสสำหรับการเชื่อมต่อเครือข่ายทั้งหมด เช่น https, ssh, scp เป็นต้น

๔) ไม่อนุญาตให้เชื่อมต่อระยะไกลจากการใช้คำสั่งระบบ (Issuing System Commands) ที่ส่งผลกระทบต่อการดำเนินบริการที่สำคัญของโรงพยาบาล เว้นแต่จะได้รับอนุญาตอย่างชัดเจนเนื่องจากความต้องการทางธุรกิจ

๕) จำกัดการไหลของข้อมูลเฉพาะฟังก์ชันขั้นต่ำที่จำเป็นสำหรับการเชื่อมต่อ

๖) บันทึกและตรวจสอบการเชื่อมต่อระยะไกลทั้งหมด (Logging and Monitoring)

๗) ตรวจสอบและประเมินความปลอดภัยของเครื่องมือที่ใช้ในการเชื่อมต่อระยะไกลเป็นประจำ (Remote Access Tool Review)

๘) มาตรการควบคุมการเข้าถึงแบบเงื่อนไขตามบริบท (Context-Aware Access Control) มาใช้งานที่เป็นลายลักษณ์อักษร

๙) พิจารณานำระบบควบคุมการเข้าถึงเครือข่าย (Network Access Control: NAC)

๑๐) จัดทำแนวปฏิบัติการเชื่อมต่อระยะไกล (Remote Access Procedure) ที่

เป็นลายลักษณ์อักษร

(๔) สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media)

(ก) ต้องตรวจสอบให้แน่ใจว่ามีการใช้การควบคุมอย่างเข้มงวดในการเชื่อมต่อสื่อบันทึกข้อมูลแบบถอดได้และอุปกรณ์คอมพิวเตอร์แบบพกพา (เช่น แล็ปท็อป) กับบริการที่สำคัญของโรงพยาบาล โดยใช้มาตรการอย่างน้อย ดังนี้

๑) ในกรณีที่มีฟังก์ชันให้ปิดใช้งานพอร์ตการเชื่อมต่อภายนอกทั้งหมด (เช่น พอร์ต USB ที่รองรับสื่อบันทึกข้อมูลแบบถอดได้ และอุปกรณ์คอมพิวเตอร์แบบพกพาและเปิดใช้งานเมื่อจำเป็นเท่านั้น

๒) ใช้สื่อบันทึกข้อมูลที่ได้รับอนุญาตตามข้อ ๓.๑๔.๖ (๔) (ก) ๑. เท่านั้น

๓) ตรวจสอบว่าสื่อบันทึกข้อมูลแบบถอดได้และอุปกรณ์คอมพิวเตอร์พกพาทั้งหมดไม่มีมัลแวร์ก่อนที่จะเชื่อมต่อกับบริการที่สำคัญของโรงพยาบาล

(ข) ต้องเข้ารหัสข้อมูลที่ละเอียดอ่อนทั้งหมดของบริการที่สำคัญของโรงพยาบาลบนสื่อบันทึกข้อมูลแบบถอดได้

(๕) การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)

(ก) ต้องให้ความสำคัญกับแผนงานในการสร้างตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness) สำหรับพนักงาน ผู้รับเหมา ผู้ให้บริการภายนอกและบุคคลที่สามที่สามารถเข้าถึงโครงสร้างพื้นฐานสำคัญทางสารสนเทศได้ โดยต้องมีรายละเอียดอย่างน้อย ดังต่อไปนี้

๑) กิจกรรมให้ความรู้แก่บุคลากรทุกประเภท ได้แก่

๑.๑) พนักงานใหม่ (New Employees)

๑.๒) ผู้ใช้และระดับบริหาร (Users and Management)

๑.๓) เจ้าหน้าที่สนับสนุนโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เช่น ผู้ให้บริการ IT และ ICS and Service Providers)

๑.๔) ผู้ขาย ผู้รับเหมา และผู้ให้บริการ (Vendors, Contractors and Service Providers)

๒) การเผยแพร่ความรับผิดชอบของกลุ่มบุคคลตามลำดับสำหรับการรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญของโรงพยาบาล

๓) การตระหนักรู้กฎหมายความมั่นคงปลอดภัยไซเบอร์ กฎ ระเบียน นโยบาย แนวปฏิบัติ มาตรฐานและขั้นตอนที่เกี่ยวข้องกับการใช้งาน และการเข้าถึงโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(๔) การสื่อสารอย่างสม่ำเสมอและทันท่วงทีครอบคลุมเนื้อหาสำหรับการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์และภัยคุกคามทางไซเบอร์ ผลกระทบและการบรรเทาผลกระทบ

(ข) ต้องทบทวนแผนงานในการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ ๑ ครั้ง เพื่อให้แน่ใจว่าเนื้อหาของแผนงานยังคงเป็นปัจจุบันและมีรายละเอียดที่เกี่ยวข้องและเหมาะสม

(ค) จัดให้มีการวัดผลความเข้าใจของผู้เข้าร่วมแผนงานการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์อย่างสม่ำเสมอ เช่น การจัดทำแบบทดสอบหรือการจำลองสถานการณ์ภัยคุกคาม(Phishing Simulation) เพื่อประเมินความเข้าใจและการตอบสนองของผู้ใช้

(ง) ควรดำเนินกิจกรรมเสริมสร้างจิตสำนึกด้านความมั่นคงปลอดภัยไซเบอร์อย่าง

ต่อเนื่อง เช่น การจัดกิจกรรมในเดือนแห่งความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness Month) หรือการส่งข่าวสารและคำแนะนำด้านภัยคุกคามเป็นประจำทุกเดือน

(๖) การแบ่งปันข้อมูล (Information Sharing)

ต้องกำหนดขั้นตอนเพื่อแบ่งปันข้อมูลเกี่ยวกับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์และภัยคุกคามทางไซเบอร์ในส่วนที่เกี่ยวกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และมาตรการบรรเทาผลกระทบใด ๆ ที่ดำเนินการเพื่อตอบสนองต่อเหตุการณ์หรือภัยคุกคามดังกล่าวกับบุคคลที่ได้รับผลกระทบหรืออาจได้รับผลกระทบจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์หรือภัยคุกคามด้านความมั่นคงปลอดภัยไซเบอร์ (เช่น ผู้ใช้ ผู้รับเหมาที่ให้บริการแก่บริการที่สำคัญของโรงพยาบาล และเจ้าของคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่จำเป็นต้องเชื่อมต่อกับบริการที่สำคัญของโรงพยาบาล) เพื่อให้สามารถใช้มาตรการป้องกั ที่จำเป็นได้ ทั้งนี้ รายละเอียดแนวทาง และรูปแบบในการแบ่งปันข้อมูลเพื่อความเป็นมาตรฐานในการปฏิบัติงาน และสามารถใช้ข้อมูลได้อย่างมีประสิทธิภาพ ให้เป็นไปตามหลักเกณฑ์และวิธีการที่โรงพยาบาลประกาศกำหนด

๓.๑๔.๗ หัวข้อหลักที่ ๓ มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)

<u>กรอบมาตรฐาน</u>

(๑) การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring)

(ก) ต้องสร้างกลไกและกระบวนการเพื่อ

๑) ตรวจจับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ทั้งหมดที่เกี่ยวข้องกับบริการที่สำคัญของโรงพยาบาล

๒) การจัดประเภทและวิเคราะห์เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่ตรวจพบ

๓) การระบุว่ามีภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศหรือไม่

(ข) ต้องดำเนินการทบทวนกลไกและกระบวนการภายในข้อ ๓.๑๔.๗ (๑) (ก) อย่างน้อยปีละ ๑ ครั้ง เพื่อให้แน่ใจว่ากลไกและกระบวนการต่าง ๆ ยังคงมีประสิทธิภาพ

(ค) เพื่อเพิ่มประสิทธิภาพในการตรวจจับภัยคุกคามทางไซเบอร์ ให้พิจารณาดำเนินการดังต่อไปนี้

๑) จัดให้มีการใช้เทคโนโลยีหรือตัวช่วยในการตรวจสอบภัยคุกคามทางไซเบอร์ เช่น ระบบตรวจจับการบุกรุก (Intrusion Detection System: IDS), ระบบป้องกันการบุกรุก (Intrusion Prevention System: IPS), ระบบบริหารจัดการเหตุการณ์และข้อมูลความปลอดภัย (Security Information and Event Management: SIEM) หรือศูนย์ปฏิบัติการด้านความมั่นคงปลอดภัยไซเบอร์ (Security Operations Center: SOC)

๒) กำหนดขอบเขตระยะเวลาในการตรวจจับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ โดยเฉพาะสำหรับเหตุการณ์ที่มีระดับความรุนแรงสูง เพื่อให้สามารถแจ้งเตือนและตอบสนองได้อย่างทันท่วงที

๓) จัดให้มีการตรวจสอบและวิเคราะห์บันทึกข้อมูล (Log) และกิจกรรมที่เกี่ยวข้อง

กับบริการที่สำคัญของโรงพยาบาลอย่างต่อเนื่องตามระดับความเสี่ยงหรืออย่างน้อยในรอบเวลาที่เหมาะสม เพื่อให้สามารถตรวจพบความผิดปกติได้อย่างรวดเร็ว

๓.๑๔.๘ หัวข้อหลักที่ ๔ มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)

<u>กรอบมาตรฐาน</u>

(๑) แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident ResponsePlan)

(ก) ต้องมการจัดทำสื่อสาร ฝึกซ้อม ทบทวน และปรับปรุงแผนการรับมือภัยคุกคามทางไซเบอร์ ตามที่ระบุไว้ในประมวลแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ ๑ ครั้ง เพื่อให้แน่ใจว่าแผนการรับมือภัยคุกคามทางไซเบอร์สามารถดำเนินการได้อย่างมีประสิทธิภาพและประสิทธิผล

(ข) แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)

๑) ต้องจัดทำแผนการสื่อสารในภาวะวิกฤตเพื่อตอบสนองต่อวิกฤตที่เกิดจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

๒) ต้องตรวจสอบให้แน่ใจว่าแผนการสื่อสารในภาวะวิกฤต

๒.๑) จัดตั้งทีมสื่อสารในภาวะวิกฤตเพื่อเปิดใช้งานในช่วงวิกฤต

๒.๒) ระบุสถานการณ์จำลองเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เป็นไปได้และแผนการดำเนินการที่เกี่ยวข้อง

๒.๓) ระบุกลุ่มเป้าหมายและผู้มีส่วนได้ส่วนเสียสำหรับสถานการณ์จำลองเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์แต่ละประเภท

๒.๔) ระบุโฆษกหลักและผู้เชี่ยวชาญด้านเทคนิคที่จะเป็นตัวแทนขององค์กรเมื่อกล่าวแถลงกับสื่อมวลชน

๒.๕) ระบุแพลตฟอร์ม/ช่องทางการเผยแพร่ที่เหมาะสม (เช่น สื่อดั้งเดิมและโซเชียลมีเดีย) สำหรับการเผยแพร่ข้อมูล

๓) ต้องตรวจสอบให้แน่ใจว่ามีแผนการสื่อสารในภาวะวิกฤตรวมถึง การประสานงานระหว่างทุกฝ่ายที่ได้รับผลกระทบ เพื่อให้แน่ใจว่ามีการตอบสนองที่ประสานกันและสอดคล้องกันในช่วงวิกฤต

๔) ต้องดำเนินการฝึกซ้อมแผนการสื่อสารในภาวะวิกฤตอย่างน้อยปีละ ๑ ครั้ง เพื่อให้แน่ใจว่าสามารถสื่อสารและเผยแพร่ข้อมูลได้อย่างทันท่วงทีและมีประสิทธิผลในช่วงวิกฤตอันเนื่องมาจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

(ค) ให้กำหนดระยะเวลาการตอบสนองต่อเหตุการณ์ที่ตรวจพบตามระดับความรุนแรงของภัยคุกคาม และจัดให้มีขั้นตอนการรายงานเหตุการณ์ตามลำดับความเร่งด่วนและผู้รับผิดชอบ

(ง) แผนการรับมือภัยคุกคามทางไซเบอร์ต้องครอบคลุมถึงภัยคุกคามที่เกิดจากบุคคลภายใน (Insider Threat) และภัยคุกคามจากห่วงโซ่อุปทาน (Supply Chain Threat)

(จ) ให้ระบุขั้นตอนและช่องทางการประสานงานกับหน่วยงานที่เกี่ยวข้อง เช่น หน่วยตอบสนองเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศ (CSIRT หรือ CERT) อย่างชัดเจนในแผนการสื่อสารในภาวะวิกฤต

๓.๑๔.๙ หัวข้อหลักที่ ๕ มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)

<u>กรอบมาตรฐาน</u>

(๑) การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity

Resilience and Recovery)

(ก) ต้องจัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan : BCP) เพื่อให้แน่ใจว่าบริการที่สำคัญของโรงพยาบาล สามารถให้บริการที่จำเป็นต่อไปได้ในกรณีที่เกิดการหยุดชะงัก เนื่องจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ เพื่อให้สามารถใช้ปฏิบัติงานได้จริง รวมถึงสอบทานแผนของผู้ให้บริการภายนอก เพื่อพิจารณาความสอดคล้องกับแผนของโรงพยาบาล เช่น ความสอดคล้องกันของขอบเขต คำนิยามและการกำหนดระยะเวลาที่สำคัญ : Maximum Tolerable Period of Disruption (MTPD), Recovery Time Objective (RTO) และ Recovery Point Objective (RPO) เป็นต้น และให้เป็นไปตามหลักเกณฑ์และวิธีการที่โรงพยาบาลประกาศกำหนด

(ข) ต้องตรวจสอบให้แน่ใจว่ามีการฝึกซ้อม BCP อย่างน้อยปีละ ๑ ครั้ง เพื่อประเมินประสิทธิภาพของ BCP ต่อภัยคุกคามทางไซเบอร์และเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

(ค) ให้โรงพยาบาลจัดทำแผนการกู้คืนระบบเทคโนโลยีสารสนเทศ (Disaster Recovery Plan: DRP) แยกต่างหากจากแผนความต่อเนื่องทางธุรกิจ เพื่อรองรับสถานการณ์ที่ระบบเทคโนโลยีสารสนเทศได้รับผลกระทบโดยตรง

(ง) ให้มีการทดสอบและฝึกซ้อมแผนความต่อเนื่องทางธุรกิจและแผนการกู้คืนระบบ (BCP และ DRP) โดยใช้สถานการณ์จำลองจริง (Realistic Scenario) เพื่อประเมินความพร้อมของบุคลากร ระบบ และกระบวนการ

(จ) ให้กำหนดค่าเป้าหมายระยะเวลาการกู้คืนระบบ (Recovery Time Objective: RTO) และเป้าหมายการสูญเสียข้อมูลสูงสุดที่ยอมรับได้ (Recovery Point Objective: RPO) สำหรับแต่ละระบบหรือบริการที่สำคัญอย่างชัดเจนและให้เป็นไปตามขอบเขตที่โรงพยาบาลกำหนด

หมวด ๔ แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของบุคคลภายนอก

๔.๑ การปฏิบัติการเข้าออกพื้นที่ภายในโรงพยาบาล

๔.๑.๑ บุคคลภายนอกที่มีความจำเป็นจะต้องติดต่อโรงพยาบาล จะต้องติดบัตรผู้มาติดต่อจากเจ้าหน้าที่รักษาความปลอดภัยของอาคารและต้องติดบัตรผ่านตรงจุดที่สามารถมองเห็นได้ชัดเจน

๔.๑.๒ บุคคลภายนอกที่มีความจำเป็นจะต้องนำเครื่องคอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานเชื่อมต่อระบบเครือข่ายอินเทอร์เน็ตที่โรงพยาบาลให้บริการ จะต้องขออนุญาตใช้งานเครื่องคอมพิวเตอร์หรืออุปกรณ์เชื่อมต่อและต้องมีเจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาลงนามในการอนุญาตหรือพิสูจน์ ตัวตนของบุคคลภายนอกก่อนทำการเชื่อมต่ออินเทอร์เน็ตโดยต้องไม่กระทำ ดังต่อไปนี้

(๑) เข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน

(๒) ล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะและนำมาตรการดังกล่าวไปเปิดเผยโดยมิชอบในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น

(๓) เข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน

(๔) กระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้ เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้

(๕) ทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลงหรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วนซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ

(๖) กระทำด้วยประการใดโดยมิชอบ เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้

(๗) ส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์(e-mail) แก่บุคคลอื่น โดยปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าวอันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข

(๘) กระทำโดยประการที่น่าจะเกิดความเสียหายต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทาง เศรษฐกิจของประเทศ หรือการบริการสาธารณะ หรือเป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีไว้เพื่อประโยชน์สาธารณะ

๔.๑.๓ บุคคลภายนอกที่มีความจำเป็นจะต้องเข้าออกศูนย์คอมพิวเตอร์หลัก ศูนย์คอมพิวเตอร์สำรองและห้องคอมพิวเตอร์(Server Room) ต้องนำบัตรผู้ติดต่อที่ได้จากเจ้าหน้าที่รักษาความปลอดภัยของอาคารหรือผู้ดูแลพื้นที่ภายในโรงพยาบาล โดยสิทธิจะขึ้นอยู่กับเหตุผลความจำเป็นในการขอเข้าไปยังพื้นที่ปฏิบัติงานภายในศูนย์คอมพิวเตอร์หลัก ศูนย์คอมพิวเตอร์สำรอง และห้องคอมพิวเตอร์(Server Room) นั้น ๆ

๔.๑.๔ บุคคลภายนอกจะต้องมีเจ้าหน้าที่ติดตาม (Escort) ตลอดระยะเวลาที่เข้ามาปฏิบัติงานภายในพื้นที่ของโรงพยาบาล และโรงพยาบาลจะต้องจัดทำทะเบียนคุมสำหรับลงบันทึกวันและเวลาการเข้า-ออกพื้นที่สำคัญและวัตถุประสงค์ของบุคคลภายนอก

๔.๑.๕ บุคคลภายนอกที่มีความจำเป็นจะต้องเข้ามาปฏิบัติงานภายในโรงพยาบาล ต้องมีการลงทะเบียนแจ้งล่วงหน้าอย่างน้อย ๑ วันทำการ โดยระบุชื่อ หน่วยงานต้นสังกัด วัตถุประสงค์ และระยะเวลาการเข้าปฏิบัติงาน เพื่อให้หน่วยงานสามารถตรวจสอบและพิจารณาอนุมัติตามความเหมาะสม

๔.๑.๖ สิทธิในการเข้าใช้งานพื้นที่สำคัญของบุคคลภายนอก ให้มีผลใช้บังคับเฉพาะในช่วงเวลาที่ได้รับอนุมัติและต้องสิ้นสุดลงโดยอัตโนมัติเมื่อพ้นกำหนดเวลาที่ได้รับอนุญาต ทั้งนี้ หากมีความจำเป็นต้องขยายเวลาต้องดำเนินการขออนุมัติใหม่ตามขั้นตอนที่กำหนด

๔.๑.๗ ให้โรงพยาบาลจัดให้มีระบบควบคุมการเข้า-ออก พร้อมทั้งจัดเก็บข้อมูลการเข้าใช้พื้นที่สำคัญของบุคคลภายนอกไว้เป็นหลักฐานประกอบการตรวจสอบย้อนหลังอย่างน้อย ๑ ปี

๔.๒ การกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้ที่อยู่ภายนอกโรงพยาบาลสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของโรงพยาบาล

๔.๒.๑ ให้ทำการเชื่อมต่อระบบเครือข่ายภายในกับระบบเครือข่ายภายนอกโรงพยาบาล ด้วยการใช้เทคโนโลยีที่เรียกว่า Secure Socket Layer VPN หรือ SSL-VPN โดยการนำโครงข่ายสาธารณะมาใช้เป็นสื่อในการส่งข้อมูลระหว่างบุคคลภายนอกและระบบงานภายในโรงพยาบาล โดยใช้การเข้ารหัสข้อมูลสร้างเป็นระบบเครือข่ายเสมือนขึ้น ซึ่งเป็นการทำ VPN ในระดับ Application Layer ผ่านพอร์ต ๔๔๓ โดยจะใช้กลไกในการแลกเปลี่ยน Key สำหรับการเข้ารหัสข้อมูล โดยจะรับ Public Key ที่ถูกแจกจ่ายมาผ่านทาง Certificate Authority (CA) เพื่อใช้ในการถอดรหัสจาก Private Key ที่อุปกรณ์ที่เปิดใช้งาน SSL VPN ทำให้สามารถควบคุมและกำหนดสิทธิการเข้าใช้งานระบบงานภายในของโรงพยาบาลในแต่ละบุคคลได้โดยสามารถระบุชนิดของ Application ที่ผู้ใช้งานแต่ละคนสามารถใช้ได้

๔.๒.๒ บุคคลภายนอกที่ต้องการขอใช้บริการการตรวจสอบข้อมูลหรือใช้ระบบสารสนเทศของโรงพยาบาลผ่านระบบเครือข่ายเสมือน (VPN) ต้องผ่านการตรวจสอบตามขั้นตอนที่ทางโรงพยาบาลกำหนดเพื่อระบุตัวตนของผู้ใช้งาน โดยส่วนงานขึ้นตรงเลขาธิการด้านดิจิทัลจะเป็นผู้ตรวจสอบและเก็บหลักฐานการระบุตัวตนของบุคคลภายนอกที่ใช้งาน

๔.๒.๓ บุคคลภายนอกที่ได้รับชื่อผู้ใช้ รหัสผ่านในการเข้าใช้บริการ VPN ต้องรักษาไว้ ซึ่งความลับของชื่อผู้ใช้รหัสผ่านและไม่เผยแพร่ให้ผู้อื่นรับทราบ หากเกิดความเสียหายต่อโรงพยาบาลบุคคลภายนอกที่ใช้งานต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

๔.๒.๔ บุคคลภายนอกที่ได้รับสิทธิการใช้งาน VPN จะต้องรักษาชื่อผู้ใช้และรหัสผ่านไว้เป็นความลับ ห้ามเผยแพร่หรือแบ่งปันสิทธิการใช้งานให้ผู้อื่นโดยเด็ดขาด ทั้งนี้ หากพบว่ามีการละเมิดหรือใช้งานผิดวัตถุประสงค์ โรงพยาบาลมีสิทธิในการระงับการใช้งานทันที และอาจดำเนินการตามกฎหมาย ที่เกี่ยวข้องได้

๔.๒.๕ ให้มีการบันทึกและจัดเก็บข้อมูลการใช้งานระบบ VPN ของบุคคลภายนอก (Log File) อย่างเป็นระบบ และตรวจสอบเป็นระยะเพื่อป้องกันการเข้าถึงหรือใช้งานระบบโดยมิชอบ ทั้งนี้ Log File ดังกล่าวต้องเก็บรักษาไว้อย่างน้อย ๙๐ วัน หรือเป็นระยะเวลาตามที่กฎหมายหรือข้อกำหนดกลางที่เกี่ยวข้องระบุไว้

๔.๒.๖ โรงพยาบาลจะดำเนินการทบทวนสิทธิการใช้งาน VPN ของบุคคลภายนอกเป็นระยะ ๆ อย่างน้อยปีละ ๑ ครั้ง และจะยกเลิกบัญชีผู้ใช้งานที่ไม่มีการใช้งานต่อเนื่องเกินกว่า ๓ เดือน หรือเมื่อพ้นระยะเวลาของโครงการ/ภารกิจที่ได้รับอนุญาต

๔.๒.๗ บุคคลภายนอกผู้ใช้งาน VPN ต้องแจ้งเจ้าหน้าที่ผู้รับผิดชอบทันที เมื่อพบเหตุการณ์ผิดปกติหรือสงสัยว่าบัญชีผู้ใช้งานอาจถูกเข้าถึงโดยมิชอบ เพื่อให้สามารถดำเนินมาตรการตอบสนองและป้องกันความเสียหายได้อย่างทันท่วงที