ประกาศ โรงพยาบาลตำรวจ

เรื่อง นโยบายและแนวปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคล

ของ โรงพยาบาลตำรวจ พ.ศ.๒๕๖๕

****

ตามที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒ มาตรา ๔ พระราชบัญญัตินี้ไม่ใช้บังคับแก่ (๒) การดำเนินการของหน่วยงานของรัฐที่มีหน้าที่ในการรักษาความมั่นคงของรัฐ ซึ่งรวมถึงความมั่นคงทางการคลังของรัฐ หรือการรักษาความปลอดภัยของประชาชน รวมทั้งหน้าที่เกี่ยวกับการป้องกันและปราบปรามการฟอกเงิน นิติวิทยาศาสตร์ หรือการรักษาความมั่นคงปลอดภัยไซเบอร์ และวรรคสาม บัญญัติให้ผู้ควบคุมข้อมูลส่วนบุคคลของหน่วยงานที่ได้รับการยกเว้นตามที่กำหนดในพระราชกฤษฎีกาตามวรรคสอง ต้องจัดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลให้เป็นไปตามมาตรฐานด้วย ประกอบกับพระราชกฤษฎีกากำหนดหน่วยงานและกิจการที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่อยู่ภายใต้บังคับแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒ พ.ศ.๒๕๖๓ มาตรา ๓ วรรคสอง บัญญัติว่าเพื่อประโยชน์ในการคุ้มครองข้อมูลส่วนบุคคล ให้ผู้ควบคุมข้อมูลส่วนบุคคลตามวรรคหนึ่งต้องจัดให้มีมาตรการรักษาความปลอดภัยของข้อมูลส่วนบุคคลให้เป็นไปตามมาตรฐานรักษาความปลอดภัยของข้อมูลส่วนบุคคลให้เป็นไปตามมาตรฐานที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมกำหนด นั้น

เพื่อให้การปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคลของ โรงพยาบาลตำรวจ เป็นไปตามนโยบาย กฎหมาย ระเบียบ และคำสั่งที่เกี่ยวข้อง ให้สามารถนำไปปฏิบัติได้อย่างถูกต้องและมีประสิทธิภาพ โรงพยาบาลตำรวจ จึงออกประกาศนโยบายและแนวปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคลของ โรงพยาบาลตำรวจ พ.ศ.๒๕๖๕ ดังต่อไปนี้

ข้อ ๑ วัตถุประสงค์และขอบเขตของประกาศ

๑.๑ การจัดทำนโยบายและแนวปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคลของโรงพยาบาลตำรวจ พ.ศ.๒๕๖๕ เพื่อให้การคุ้มครองข้อมูลส่วนบุคคลมีประสิทธิภาพ และเพื่อให้มีมาตรการเยียวยา เจ้าของข้อมูลส่วนบุคคลจากการถูกละเมิดสิทธิในข้อมูลส่วนบุคคลที่มีประสิทธิภาพ

๑.๒ กำหนดขอบเขตของการปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคลโดยอ้างอิงประกาศของสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล และให้มีการปรับปรุงอย่างต่อเนื่อง

๑.๓ ประกาศนี้ ต้องเผยแพร่ให้ข้าราชการตำรวจและบุคคลภายนอกที่ปฏิบัติงานให้โรงพยาบาลตำรวจ ได้รับทราบ และต้องถือปฏิบัติตามอย่างเคร่งครัด

๑.๔ เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีปฏิบัติให้ผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคล และเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ทั้งข้าราชการตำรวจและบุคคลภายนอกที่ปฏิบัติงานให้โรงพยาบาลตำรวจ ตระหนักถึงความสำคัญของข้อมูลส่วนบุคคล เกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด

ข้อ ๒...

ข้อ ๒ ประกาศนี้ให้มีผลบังคับใช้ตั้งแต่วันที่ ๑ มิ.ย. พ.ศ.๒๕๖๕ เป็นต้นไป

ข้อ ๓ ในประกาศนี้

"นโยบาย" หมายความว่า หลักการด้านการคุ้มครองข้อมูลส่วนบุคคลซึ่งโรงพยาบาลตำรวจประกาศไว้ เพื่อให้เจ้าหน้าที่และผู้ปฏิบัติงานของ โรงพยาบาลตำรวจ ได้ถือปฏิบัติให้เป็นไปในแนวทางเดียวกัน

"แนวปฏิบัติ" หมายความว่า ขั้นตอนวิธีการที่ โรงพยาบาลตำรวจ ได้กำหนดไว้โดยภาพรวมสำหรับการปฏิบัติงานของเจ้าหน้าที่และผู้ปฏิบัติงานของโรงพยาบาลตำรวจ

"โรงพยาบาล" หมายความว่า โรงพยาบาลตำรวจ โดยรวมถึงหน่วยงานระดับกองบังคับการ และหน่วยงานอื่นที่อยู่ในสังกัดโรงพยาบาลตำรวจ

"ข้อมูลส่วนบุคคล" หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

"ผู้ควบคุมข้อมูลส่วนบุคคล" หมายความว่า บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

"ผู้ประมวลผลข้อมูลส่วนบุคคล" หมายความว่า บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล

"ความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล" หมายความว่า การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของข้อมูลส่วนบุคคล ทั้งนี้เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยมิชอบ

ข้อ ๔ นโยบายด้านการคุ้มครองข้อมูลส่วนบุคคล

๔.๑ การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

โรงพยาบาล เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล รวมถึง การแลกเปลี่ยนข้อมูลส่วนบุคคลเท่าที่จำเป็นและชอบด้วยกฎหมาย มีระยะเวลาในการจัดเก็บที่เหมาะสมตามภารกิจของโรงพยาบาลเพื่อประโยชน์สาธารณะและรักษาความมั่นคงของรัฐ

๔.๒ ข้อจำกัดในการนำข้อมูลส่วนบุคคลไปใช้

โรงพยาบาลจะไม่เปิดเผยข้อมูลส่วนบุคคลที่มีการจัดเก็บและรวบรวมไว้ให้กับผู้ที่ไม่เกี่ยวข้อง เว้นแต่

(๑) การแลกเปลี่ยนข้อมูลของโรงพยาบาล ตั้งแต่เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล รวมถึง การแลกเปลี่ยนข้อมูลส่วนบุคคลต้องมีการได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล และต้องมีการกำหนดกระบวนการความมั่นคงปลอดภัยข้อมูลอย่างเคร่งครัด เพื่อรักษาคุณภาพ ความปลอดภัย และความสมบูรณ์ของข้อมูล

(๒) การเปิดเผยข้อมูลนั้นเป็นไปตามคำพิพากษา คำสั่งศาล หรือที่กฎหมายให้อำนาจหรือกำหนดไว้ ผู้ใช้ข้อมูล หรือทุกคนที่เกี่ยวข้องกับวงจรชีวิตข้อมูลของโรงพยาบาล มีสิทธิในการเข้าถึง

ข้อมูล...

ข้อมูลและระบบสารสนเทศของโรงพยาบาล เพื่อการปฏิบัติงานเฉพาะในส่วนที่ได้รับอนุญาตตามการกำหนดสิทธิในแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลของ โรงพยาบาลตำรวจ เท่านั้น

(๓) เป็นไปเพื่อประโยชน์ของเจ้าของข้อมูลส่วนบุคคลและการขอความยินยอมไม่สามารถดำเนินการได้ในเวลานั้น

(๔) สำหรับการว่าจ้างผู้ให้บริการจากภายนอกเพื่อพัฒนาระบบงานต่างๆ โดยโรงพยาบาลกำหนดให้ผู้ให้บริการจากภายนอกต้องปฏิบัติตามนโยบายและแนวปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคลของ โรงพยาบาลตำรวจ พ.ศ.๒๕๖๕

(๕) การเปิดเผยนั้นเป็นไปเพื่อประโยชน์สาธารณะ หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล

(๖) การปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล

๔.๓ มาตรการรักษาความมั่นคงปลอดภัยของข้อมูล

โรงพยาบาลตำรวจ ดำเนินการตามประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล พ.ศ.๒๕๖๓ ข้อ ๕ ได้กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล โดยครอบคลุมถึงมาตรการด้านการบริหารจัดการ มาตรการทางด้านเทคนิค และมาตรการป้องกันทางกายภาพในเรื่องการเข้าถึงหรือควบคุมการใช้งานข้อมูลส่วนบุคคล เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคล โดยปราศจากอำนาจหรือโดย มิชอบ และให้ทบทวนมาตรการเมื่อมีความจำเป็น หรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม และเพื่อให้สามารถปฏิบัติตามได้อย่างเป็นรูปธรรม โรงพยาบาลตำรวจจึงกำหนดแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลไว้ตามแนวปฏิบัติท้ายประกาศนี้

ข้อ ๕ แนวปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคล

โรงพยาบาลตำรวจ เป็นสถานที่สำหรับให้บริการด้านสุขภาพให้กับผู้ป่วย โดยมุ่งเน้นการรักษา และฟื้นฟูภาวะความเจ็บป่วย โรคต่าง ๆ ทั้งทางร่างกายและทางจิตใจ ซึ่งเกี่ยวข้องกับข้อมูลส่วนบุคคลจำนวนมาก โดยทุกหน่วยจะต้องดำเนินการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเท่าที่จำเป็นภายใต้วัตถุประสงค์อันชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล ดังนี้

๕.๑ ให้ข้าราชการตำรวจในสังกัด ศึกษาทำความเข้าใจและความตระหนักรู้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒

๕.๒ การจัดทำแบบสอบถาม เพื่อสำรวจ การเก็บ ใช้ และเปิดเผยข้อมูลส่วนบุคคล เนื่องจากแต่ละหน่วยงานมีหน้าที่และความรับผิดชอบแตกต่างกัน การจัดทำแบบสอบถามเพื่อการสำรวจอาจจะมีความแตกต่างกัน

๕.๓ ผู้ควบคุม...

๕.๓ ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดทำประกาศความเป็นส่วนตัวหรือคำประกาศเกี่ยวกับความเป็นส่วนตัว (Privacy notice) เพื่อแจ้งให้เจ้าของข้อมูลทราบถึงรายละเอียดก่อนหรือในขณะเก็บรวบรวมข้อมูลส่วนบุคคล ตามมาตรา ๒๓ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒

๕.๔ ผู้บังคับบัญชาจะต้องออกระเบียบ วิธีปฏิบัติ ประกาศ คำสั่ง หรือหนังสือสั่งการเกี่ยวกับมาตราการรักษาความปลอดภัยของข้อมูลส่วนบุคคล เพื่อป้องกันมิให้ข้อมูลส่วนบุคคลรั่วไหล

ข้อ ๖ นโยบายด้านการคุ้มครองข้อมูลส่วนบุคคลนี้ เป็นมาตรการในการคุ้มครองข้อมูลส่วนบุคคลของโรงพยาบาลตำรวจ ซึ่งข้าราชการตำรวจ รวมทั้งลูกจ้างในสังกัด และหน่วยงานภายนอก จะต้องปฏิบัติตามอย่างเคร่งครัด โดยที่ผู้ควบคุมข้อมูลส่วนบุคคลอาจเลือกใช้มาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่แตกต่างไปจากประกาศนี้ได้ หากมาตรฐานดังกล่าวมีมาตราการรักษาความมั่นคงปลอดภัยไม่ต่ำกว่าที่กำหนดในประกาศนี้ และควรให้หน่วยที่มีอำนาจตีความและวินิจฉัยปัญหาอันเกิดจากการปฏิบัติตามประกาศนี้

ข้อ ๗ ให้ผู้ควบคุมข้อมูลส่วนบุคคลแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลโดยไม่ชักช้า ภายใน ๗๒ ชั่วโมง นับแต่ทราบเหตุ

ข้อ ๘ ให้คณะทำงานขับเคลื่อนการดำเนินการตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒ หรือคณะทำงานตามที่โรงพยาบาลตำรวจกำหนด เป็นผู้รับผิดชอบดำเนินการทบทวนนโยบายและแนวปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคลของโรงพยาบาลตำรวจ ให้เป็นปัจจุบัน อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่จำเป็นต้องได้รับการปรับปรุง เพื่อให้นโยบายดังกล่าวมีความเหมาะสมกับสถานการณ์ที่มีการเปลี่ยนแปลง

ประกาศ ณ วันที่ ๒๗ กันยายน พ.ศ. ๒๕๖๕

พลตำรวจโท

(โสภณรัชต์ สิงหจารุ)

นายแพทย์ใหญ่ (สบ ๘)

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลของโรงพยาบาลตำรวจ

พ.ศ.๒๕๖๕

เพื่อให้โรงพยาบาลตำรวจ เป็นหน่วยงานที่ปฏิบัติภารกิจหน้าที่ให้บริการด้านสุขภาพให้กับผู้ป่วย โดยมุ่งเน้นการรักษา และฟื้นฟูภาวะความเจ็บป่วยโรคต่าง ๆ ทั้งทางร่างกายและทางจิตใจ เป็นไปอย่างมีมาตรฐานน่าเชื่อถือ สร้างความมั่นคงปลอดภัย และสร้างความเชื่อมั่นต่อการดำเนินกิจกรรมอันครอบคลุมถึงงานสารสนเทศและระบบเทคโนโลยีสารสนเทศที่เกี่ยวข้องกับข้อมูลส่วนบุคคล โรงพยาบาลตำรวจ จึงกำหนดแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลไว้ ดังต่อไปนี้

ข้อ ๑ ในแนวปฏิบัตินี้

“ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง” (Chief Information Officer: CIO) หมายความว่า ผู้บริหารระดับสูงที่นายแพทย์ใหญ่ (สบ๘) แต่งตั้งหรือมอบหมายให้มีหน้าที่รับผิดชอบการบริหารงานสารสนเทศและระบบเทคโนโลยีสารสนเทศของโรงพยาบาลตำรวจ

“หัวหน้าหน่วยงาน” หมายความว่า ผู้บังคับการ รองผู้บังคับการ หัวหน้ากลุ่มงาน ภายในโรงพยาบาลตำรวจ หรือเทียบเท่า

“ผู้ใช้งาน” หมายความว่า ข้าราชการตำรวจ เจ้าหน้าที่ พนักงานของรัฐ ลูกจ้าง ผู้ดูแลระบบของโรงพยาบาล ผู้บริหารโรงพยาบาล ผู้ใช้บริการ รวมทั้งผู้ใช้งานที่ใช้บริการระบบเทคโนโลยีสารสนเทศของโรงพยาบาลตำรวจ

“ผู้ดูแลระบบ” หมายความว่า ผู้ที่ได้รับมอบอำนาจจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูงหรือหัวหน้าหน่วยงานให้รับผิดชอบดูแลรักษาหรือจัดการระบบคอมพิวเตอร์และระบบเครือข่ายไม่ว่าส่วนหนึ่งส่วนใดหรือทั้งระบบ

“สารสนเทศ” หมายความว่า ข้อมูลในรูปแบบต่าง ๆ ที่สามารถนำมาใช้ประกอบการตัดสินใจ หรือใช้ประโยชน์ตามภารกิจของโรงพยาบาล

“เครือข่าย” หมายความว่า ระบบการสื่อสารที่เป็นการเชื่อมต่อคอมพิวเตอร์ ตั้งแต่ ๒ เครื่องขึ้นไปเข้าด้วยกัน เพื่อสะดวกต่อการร่วมใช้ข้อมูล โปรแกรม หรือเครื่องพิมพ์ และอำนวยความสะดวกในการติดต่อแลกเปลี่ยนข้อมูลระหว่างเครื่องได้ตลอดเวลา

“สินทรัพย์” หมายความว่า เครื่องคอมพิวเตอร์ ซอฟต์แวร์ลิขสิทธิ์ อุปกรณ์ประกอบ ข้อมูลสารสนเทศ และอุปกรณ์ที่เกี่ยวข้องด้านเทคโนโลยีสารสนเทศทั้งหมดที่โรงพยาบาลจัดหาไว้ใช้งาน

“สิทธิของผู้ใช้งาน” หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับการเข้าถึงสารสนเทศ เครือข่าย ระบบปฏิบัติการการใช้โปรแกรมระบบงานคอมพิวเตอร์ รวมถึงสิทธิที่เกี่ยวข้องกับระบบสารสนเทศอื่น ๆ ของโรงพยาบาล

"การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ" หมายความว่า การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

"ความมั่นคงปลอดภัยด้านสารสนเทศ" หมายความว่า การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (authenticity) ความรับผิดชอบ (accountability) การห้ามปฏิเสธความรับผิดชอบ (non-repudiation) และความน่าเชื่อถือ (reliability) ของระบบสารสนเทศ

"เหตุการณ์ด้านความมั่นคงปลอดภัย" หมายความว่า กรณีที่เกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัย หรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

"สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด" หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (unwanted or unexpected) ซึ่งอาจทำให้ระบบของโรงพยาบาลถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

"ภัยคุกคามทางไซเบอร์" หมายความว่า การกระทำหรือการดำเนินการใด ๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่มีความเกี่ยวข้องกับข้อมูลสารสนเทศขององค์กร

"การรักษาความมั่นคงทางไซเบอร์" หมายความว่า มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อรักษาไว้ซึ่งความลับ ความถูกต้อง ความพร้อมใช้ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่มีผลกระทบต่อองค์กร

ข้อ ๒ กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใด ๆ แก่โรงพยาบาล หรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ให้ผู้ที่ดำรงตำแหน่งไม่ต่ำกว่ารองนายแพทย์ใหญ่ (สบ ๗) หรือนายแพทย์ (สบ ๗) โรงพยาบาลตำรวจ (ที่ได้รับมอบหมาย) ในฐานะผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer: CIO) ของโรงพยาบาลตำรวจ เป็นผู้รับผิดชอบดำเนินการต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

ข้อ ๓ ผู้ที่เกี่ยวข้องและผู้ใช้งานทั้งหมดจะต้องรับทราบโดยทั่วกัน พร้อมทั้งสร้างความรู้ ความเข้าใจ และฝึกอบรมผู้ใช้งานเพื่อให้เกิดความตระหนักความเข้าใจถึงภัยคุกคามต่าง ๆ และผลกระทบที่เกิดจากการใช้งานสารสนเทศและระบบเทคโนโลยีสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์

หมวด ๑
แนวปฏิบัติของผู้ดูแลระบบ

ข้อ ๔ การรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and Environment Security) ให้ผู้ดูแลระบบปฏิบัติดังต่อไปนี้

๔.๑ กำหนดมาตรการควบคุมการเข้า-ออก ศูนย์คอมพิวเตอร์ของโรงพยาบาล เพื่อดูแลรักษาความปลอดภัย โดยบุคคลที่ต้องการสิทธิในการเข้า-ออก ศูนย์คอมพิวเตอร์ของโรงพยาบาล ต้องขออนุญาตเป็นลายลักษณ์อักษร

๔.๒ พิจารณาอนุมัติและกำหนดสิทธิการเข้า-ออก ศูนย์คอมพิวเตอร์ของโรงพยาบาลให้เป็นไปตามภารกิจของแต่ละหน่วยงานที่ผู้ใช้งานปฏิบัติงาน โดยต้องได้รับอนุมัติจากผู้บังคับบัญชาของโรงพยาบาลเท่านั้น

๔.๓ ต้องทำการยืนยันตัวตนก่อนเข้าศูนย์คอมพิวเตอร์ของโรงพยาบาลทุกครั้งเพื่อป้องกันการเข้า-ออกโดยไม่ได้รับอนุญาต

๔.๔ ควบคุมการลงชื่อ บันทึกวัน เวลา และวัตถุประสงค์การเข้า-ออก ของผู้ใช้งานและบุคคลภายนอก (Visitors) ทุกครั้ง

๔.๕ ควบคุมให้ผู้เข้า-ออกติดบัตรแสดงตัวตนให้เห็นเด่นชัดตลอดระยะเวลาที่อยู่ภายในพื้นที่ศูนย์คอมพิวเตอร์ของโรงพยาบาล

๔.๖ ดูแลและเฝ้าระวังการปฏิบัติงานของบุคคลภายนอก (Visitors) ในขณะที่ปฏิบัติงานในศูนย์คอมพิวเตอร์ของโรงพยาบาลจนกระทั่งเสร็จสิ้นภารกิจและออกจากศูนย์คอมพิวเตอร์ของโรงพยาบาล เพื่อป้องกันการสูญหายของสินทรัพย์หรือป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต

๔.๗ แยกพื้นที่ในการส่งมอบสินทรัพย์ เพื่อตรวจสอบให้เสร็จเรียบร้อยก่อนนำเข้าไปติดตั้งหรือใช้งานภายในศูนย์คอมพิวเตอร์ของโรงพยาบาล

๔.๘ ประชาสัมพันธ์มาตรการควบคุมการเข้า-ออก ศูนย์คอมพิวเตอร์ของโรงพยาบาล แก่ผู้ใช้งานและบุคคลภายนอก (Visitors)

๔.๙ ห้ามนำอาหารและเครื่องดื่มเข้าไปภายในศูนย์คอมพิวเตอร์ของโรงพยาบาล

๔.๑๐ ห้ามสูบบุหรี่ หรือกระทำการใด ๆ อันอาจก่อให้เกิดควันหรือเพลิงในบริเวณภายในศูนย์คอมพิวเตอร์ของโรงพยาบาล

๔.๑๑ ต้องทำการยกเลิก เพิกถอน หรือเปลี่ยนแปลงการอนุญาตการเข้า-ออกศูนย์คอมพิวเตอร์ของโรงพยาบาลของผู้ใช้งานเมื่อมีการออกจากงาน สิ้นสุดการจ้าง เปลี่ยนตำแหน่ง โอน หรือย้ายหน่วยงานสังกัด

๔.๑๒ ทบทวนสิทธิการเข้าถึงพื้นที่ หรือบริเวณที่มีความสำคัญภายในศูนย์คอมพิวเตอร์ของโรงพยาบาลอย่างสม่ำเสมอ หรืออย่างน้อยปีละหนึ่งครั้ง

ข้อ ๕ การกำหนดการจัดวางและป้องกันระบบสารสนเทศ ให้ผู้ดูแลระบบปฏิบัติดังต่อไปนี้

๕.๑ จัดวางระบบสารสนเทศที่มีความสำคัญในพื้นที่ที่มีความมั่นคงและปลอดภัยเพื่อป้องกันการเข้าถึงจากบุคคลที่ไม่ได้รับอนุญาต และเพื่อป้องกันการเข้าถึงพอร์ตของระบบที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ

๕.๒ แยกจัดเก็บระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ที่สำคัญไว้ในพื้นที่ความปลอดภัยสูงแยกต่างหาก

ข้อ ๖ การกำหนดและควบคุมการเดินสายสัญญาณสื่อสารและสายไฟฟ้า ให้ผู้ดูแลระบบปฏิบัติดังต่อไปนี้

๖.๑ ควบคุมการเดินสายสัญญาณสื่อสารและสายไฟฟ้าให้เป็นไปด้วยความเรียบร้อยและปลอดภัย

๖.๒ ควบคุมการเดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกันเพื่อป้องกันการรบกวนของสัญญาณ

๖.๓ ทำแผนผังการเดินสายสัญญาณสื่อสารและสายไฟฟ้าให้ครบถ้วนและถูกต้อง

๖.๔ ปิดประตูตู้สำหรับติดตั้งอุปกรณ์ Server Computer และ อุปกรณ์เครือข่าย ต่างๆ รวมทั้งสายสัญญาณ (Network Cable) (ตู้ Rack) ให้สนิทรวมถึงการล็อคประตูเพื่อป้องกันการเข้าถึงของบุคคลที่ไม่เกี่ยวข้อง

๖.๕ จัดทำป้ายชื่อสำหรับสายสัญญาณสื่อสารและบนอุปกรณ์เพื่อป้องกันการปฏิบัติงานผิดพลาด

๖.๖ ดำเนินการสำรวจระบบสายสัญญาณสื่อสารทั้งหมดเพื่อความถูกต้องและตรวจหาการติดตั้งอุปกรณ์ดักจับสัญญาณโดยผู้ไม่ประสงค์ดี

ข้อ ๗ การกำหนดการบำรุงรักษาระบบสารสนเทศ ให้ผู้ดูแลระบบปฏิบัติดังต่อไปนี้

๗.๑ จัดทำสัญญาการบำรุงรักษาสำหรับระบบและอุปกรณ์คอมพิวเตอร์ที่มีความสำคัญ

๗.๒ กำหนดเงื่อนไขของการให้บริการในสัญญาการบำรุงรักษาให้ชัดเจนเพื่อให้ผู้รับจ้างต้องติดต่อกลับและเข้ามาดำเนินการแก้ไขปัญหาให้แล้วเสร็จภายในระยะเวลาที่เหมาะสม

๗.๓ ตรวจสอบและกำหนดให้มีการรับประกันความเสียหายของระบบสารสนเทศ

๗.๔ บำรุงรักษาระบบสารสนเทศตามรอบระยะเวลาที่กำหนดไว้ในสัญญาการบำรุงรักษา

๗.๕ ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามที่ผู้ผลิตแนะนำ

๗.๖ จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้งเพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง

๗.๗ บันทึกปัญหาและข้อบกพร่องที่พบ และรายงานผู้บังคับบัญชาทราบ

๗.๘ ควบคุม และดูแลการปฏิบัติงานของผู้ให้บริการภายนอกให้ปฏิบัติตามสัญญาการจ้างเหมาบำรุงรักษา

๗.๙ กำหนดสิทธิของผู้ให้บริการภายนอกในการเข้าถึงพื้นที่ อุปกรณ์ และข้อมูลที่สำคัญ

ข้อ ๘ การบริหารจัดการสินทรัพย์ ให้ผู้ดูแลระบบปฏิบัติดังต่อไปนี้

๘.๑ บันทึกและตรวจสอบสินทรัพย์ เพื่อเก็บเป็นหลักฐานในการตรวจสอบความถูกต้องและป้องกันการสูญหาย

๘.๒ กำหนดมาตรการหรือเทคนิคในการทำลายข้อมูลสำคัญในสื่อบันทึกข้อมูลก่อนที่จะจำหน่ายหรือนำกลับมาใช้งานใหม่ทุกครั้ง เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้น

๘.๓ กรณีที่สินทรัพย์เกิดความเสียหายและต้องส่งซ่อม ให้ควบคุมการส่งออกไปซ่อมแซมนอกสถานที่เพื่อป้องกันการสูญหายหรือการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต กรณีสินทรัพย์เป็นข้อมูลสำคัญต้องทำการทำลายข้อมูลทิ้งเพื่อไม่ให้ผู้อื่นสามารถเข้าถึงได้

ข้อ ๙ การควบคุมการใช้งานสารสนเทศและบริหารจัดการอุปกรณ์คอมพิวเตอร์แบบพกพาให้ผู้ดูแลระบบปฏิบัติดังต่อไปนี้

๙.๑ ต้องนำอุปกรณ์คอมพิวเตอร์แบบพกพาส่วนตัว หรืออุปกรณ์คอมพิวเตอร์แบบพกพาของโรงพยาบาลที่ได้รับอนุมัติจากผู้บังคับบัญชาให้เชื่อมต่อระบบเครือข่ายภายในและเข้าถึงระบบสารสนเทศของโรงพยาบาล แจ้งขึ้นทะเบียนอุปกรณ์คอมพิวเตอร์แบบพกพา และปฏิบัติตามขั้นตอนปฏิบัติที่โรงพยาบาลกำหนดเพื่อป้องกันการเข้าถึงระบบสารสนเทศด้วยอุปกรณ์คอมพิวเตอร์แบบพกพาโดยไม่ได้รับอนุญาต

๙.๒ ต้องกำหนดมาตรการระบุและพิสูจน์ตัวตนก่อนเข้าถึงอุปกรณ์คอมพิวเตอร์แบบพกพาด้วยบัญชีผู้ใช้งานและรหัสผ่าน เพื่อป้องกันการเข้าถึงจากผู้อื่นและระมัดระวังมิให้ผู้อื่นเข้าถึงอุปกรณ์คอมพิวเตอร์แบบพกพาของตน

๙.๓ ต้องดูแลรักษาข้อมูลองค์กรในอุปกรณ์คอมพิวเตอร์แบบพกพาให้สอดคล้องตามข้อกำหนดการบริหารจัดการข้อมูลองค์กร

๙.๔ ต้องแจ้งผู้บังคับบัญชาของโรงพยาบาลทันทีที่พบว่าอุปกรณ์คอมพิวเตอร์เสียหาย สูญหาย หรือเปลี่ยนเครื่องใหม่ เพื่อจัดการเหตุการณ์ได้อย่างมีประสิทธิภาพ

ข้อ ๑๐ การควบคุมการใช้งานสารสนเทศ ให้ผู้ดูแลระบบปฏิบัติดังต่อไปนี้

๑๐.๑ การอนุมัติและกำหนดสิทธิการเข้าถึงระบบสารสนเทศของผู้ใช้งานให้เป็นไปตามภารกิจหรือแนวปฏิบัติของแต่ละหน่วยงานที่ผู้ใช้งานปฏิบัติงาน โดยต้องได้รับอนุมัติจากผู้บังคับบัญชาแล้วเท่านั้น

๑๐.๒ กำหนดการเข้าถึงด้วยบัญชีผู้ใช้งานแยกเป็นรายบุคคลตามภารกิจหรือแนวปฏิบัติของแต่ละหน่วยงานที่ผู้ใช้งานปฏิบัติงาน

๑๐.๓ จัดเก็บข้อมูลการลงทะเบียนสำหรับสร้างบัญชีผู้ใช้งานไว้เพื่อการตรวจสอบในภายหลัง

๑๐.๔ กำหนดให้ทำการยืนยันตัวตน (Authentication) ของผู้ใช้งานก่อนเข้าถึงระบบสารสนเทศ

๑๐.๕ กำหนดระยะเวลาการออกจากระบบสารสนเทศโดยอัตโนมัติเมื่อไม่มีการใช้งานเกินสามสิบนาที หรือตามความสำคัญของข้อมูลสารสนเทศ

๑๐.๖ กำหนดระยะเวลาการเข้าถึงระบบสารสนเทศที่สำคัญของโรงพยาบาล ตามภารกิจและความจำเป็นของผู้ใช้งาน

๑๐.๗ กำหนดให้เครื่องคอมพิวเตอร์ที่จัดหาโดยโรงพยาบาล พักหน้าจอ (Screen saver) โดยอัตโนมัติ หากไม่มีการใช้งานเครื่องคอมพิวเตอร์ติดต่อกันสิบห้านาที

๑๐.๘ จำกัดระยะเวลาในการเชื่อมต่อ (Limitation of Connection Time) ระบบสารสนเทศเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศหรือโปรแกรมที่มีความเสี่ยงหรือมีความสำคัญสูง

๑๐.๙ จำกัดและควบคุมการเข้าถึงฟังก์ชัน (Functions) ต่าง ๆ ในการใช้งานระบบสารสนเทศของผู้ใช้งานและผู้ดูแลระบบ

๑๐.๑๐ ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อโรงพยาบาล ต้องแยกเครือข่ายออกจากระบบอื่น ๆ ต้องมีการควบคุมสภาพแวดล้อมแยกเป็นสัดส่วน และต้องกำหนดสิทธิการใช้งานเฉพาะผู้ที่มีสิทธิเท่านั้น

๑๐.๑๑ จัดทำระบบบริหารจัดการรหัสผ่านเชิงโต้ตอบสำหรับการระบุและพิสูจน์ตัวตนที่มีความมั่นคงปลอดภัย โดยผู้ใช้งานกำหนดรหัสผ่านที่มีความมั่นคงปลอดภัยตามการบริหารจัดการบัญชีผู้ใช้งาน (User Account) ด้วยตนเอง

๑๐.๑๒ การยกเลิกและเพิกถอนสิทธิการอนุญาตให้เข้าถึงระบบสารสนเทศของผู้ใช้งานต้องทำการยกเลิกและเพิกถอนการอนุญาตเมื่อมีการโอนหรือย้ายหน่วยงาน ออกจากงาน หรือสิ้นสุดการจ้าง

๑๐.๑๓ การเปลี่ยนแปลงสิทธิการอนุญาตให้เข้าถึงระบบสารสนเทศของผู้ใช้งาน กรณีเปลี่ยนตำแหน่ง โอน หรือย้าย ต้องทำการเปลี่ยนแปลงหลังจากได้รับแจ้งจากผู้บังคับบัญชาผู้ใช้งาน

๑๐.๑๔ ดำเนินการทบทวนบัญชีผู้ใช้งานและสิทธิการเข้าถึงระบบสารสนเทศอย่างสม่ำเสมอ หรืออย่างน้อยปีละหนึ่งครั้ง หรือทุกครั้งที่มีการเปลี่ยนแปลงเพื่อป้องกันการเข้าถึงระบบสารสนเทศโดยไม่ได้รับอนุญาต

ข้อ ๑๑ การบริหารจัดการความปลอดภัยเครือข่าย ให้ผู้ดูแลระบบปฏิบัติดังต่อไปนี้

๑๑.๑ กำหนดวิธีปฏิบัติเกี่ยวกับการใช้งานเครือข่ายทั้งภายในและภายนอกโรงพยาบาล

๑๑.๒ กำหนดขั้นตอนการขออนุญาตเพื่อเข้าถึงระบบสารสนเทศที่อยู่ภายในเครือข่ายของโรงพยาบาล

๑๑.๓ กำหนดขั้นตอนการเชื่อมต่อระบบเครือข่ายจากผู้ใช้งานภายนอกโรงพยาบาลอย่างมั่นคงปลอดภัย เช่น การเชื่อมต่อระบบเครือข่ายด้วยเทคโนโลยีเครือข่ายเสมือนส่วนตัว (Virtual Private Network : VPN)

๑๑.๔ ระบุบริการที่โรงพยาบาลอนุญาตให้ใช้งานหรือบริการผ่านระบบเครือข่ายของโรงพยาบาล

๑๑.๕ กำหนดให้มีการระบุและพิสูจน์ตัวตนในการเข้าถึงระบบสารสนเทศของโรงพยาบาล

๑๑.๖ จัดทำทะเบียนอุปกรณ์ที่ใช้งานในระบบเครือข่ายโดยอย่างน้อยประกอบด้วยข้อมูล หมายเลขประจำเครื่อง ตราอักษร แบบรุ่น หมายเลข Mac Address หมายเลข IP Address ที่มา ผู้รับผิดชอบ

วันที่เริ่มติดตั้ง วันที่เลิกใช้งาน และเหตุผลที่เลิกใช้งาน

๑๑.๗ ใช้ข้อมูล MAC Address หรือ IP Address เป็นข้อมูลในการระบุอุปกรณ์บนเครือข่ายเพื่อบ่งชี้อุปกรณ์ที่ได้รับอนุญาตให้เชื่อมต่อเข้าเครือข่ายของโรงพยาบาล และใช้วิธีการทางเทคนิคที่เหมาะสมเพื่อควบคุมการเข้าถึงอุปกรณ์เครือข่ายเหล่านั้น

๑๑.๘ กำหนดให้เฉพาะเครื่องคอมพิวเตอร์ของผู้ดูแลระบบเครือข่ายเท่านั้น ที่สามารถเชื่อมต่อเครือข่ายเพื่อบริหารจัดการระบบและอุปกรณ์เครือข่ายของโรงพยาบาล

๑๑.๙ ตรวจสอบและปิดพอร์ตบนระบบและอุปกรณ์เครือข่ายที่ไม่มีความจำเป็นในการใช้งาน

๑๑.๑๐ ป้องกันและควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับการบริหารจัดการอุปกรณ์ในระบบเครือข่ายทั้งจากภายในและภายนอกโรงพยาบาล

๑๑.๑๑ จัดแบ่งเครือข่ายตามวัตถุประสงค์การใช้งาน บริการ หรือกลุ่มผู้ใช้งาน เช่น เครือข่ายสำหรับผู้ใช้งาน เครือข่ายสำหรับเครื่องแม่ข่าย หรือเครือข่ายสำหรับทดสอบทดลองระบบ เป็นต้น

๑๑.๑๒ ใช้วิธีการทางเทคนิคบนไฟร์วอลล์ (Firewall) หรืออุปกรณ์เครือข่ายอื่น ๆ จำกัดเส้นทางบนเครือข่ายที่โรงพยาบาลไม่อนุญาตให้ใช้งาน เพื่อกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้เฉพาะเส้นทางบนเครือข่ายที่อนุญาตเท่านั้น

๑๑.๑๓ กำหนดมาตรการป้องกันระบบสารสนเทศที่ต้องเชื่อมโยงกับระบบเครือข่ายสาธารณะอย่างมีประสิทธิภาพ

๑๑.๑๔ กำหนดมาตรการป้องกันข้อมูลที่ส่งผ่านทางเครือข่ายสาธารณะเพื่อรักษาความลับและความถูกต้องของข้อมูลที่สำคัญ

๑๑.๑๕ กำหนดเส้นทางบนเครือข่ายที่เหมาะสมเพื่อควบคุมการเชื่อมต่อและการไหลเวียนของสารสนเทศบนเครือข่ายให้มีประสิทธิภาพ

๑๑.๑๖ ตรวจสอบการใช้งานระบบเครือข่ายด้วยระบบตรวจจับและป้องกันการบุกรุกของบุคคลที่เข้าใช้งานระบบเครือข่ายในลักษณะที่ผิดปกติอย่างสม่ำเสมอ หรืออย่างน้อยเดือนละหนึ่งครั้ง

๑๑.๑๗ ทดสอบความมั่นคงปลอดภัยของระบบเครือข่ายอย่างน้อยปีละหนึ่งครั้งหรือตามสถานการณ์ของภัยคุกคามทางไซเบอร์ในระบบเครือข่าย และนำผลที่ได้ไปปรับปรุงความมั่นคงปลอดภัยระบบเครือข่ายของโรงพยาบาล ให้มีความมั่นคงปลอดภัยมากขึ้นและทันต่อภัยคุกคามทางไซเบอร์ในปัจจุบัน

๑๑.๑๘ ติดตาม ตรวจสอบ ดูแล และปรับปรุงเครือข่ายของโรงพยาบาล ให้มีความมั่นคงปลอดภัยและทันสมัยอยู่เสมอ หากตรวจพบสิ่งผิดปกติเกี่ยวกับการใช้งานระบบเครือข่ายให้รีบดำเนินการแก้ไขและแจ้งผู้บังคับบัญชาทันทีเพื่อป้องกันหรือบรรเทาความเสียหายที่อาจจะเกิดขึ้น

๑๑.๑๙ การยกเลิกและเพิกถอนสิทธิการอนุญาตให้เข้าถึงระบบเครือข่ายของผู้ใช้งาน ต้องทำการยกเลิกและเพิกถอนการอนุญาตเมื่อมีการโอนหรือย้ายหน่วยงาน ออกจากงาน หรือสิ้นสุดการจ้างโดยทันที

๑๑.๒๐ การเปลี่ยนแปลงสิทธิการอนุญาตให้เข้าถึงระบบเครือข่ายของผู้ใช้งานกรณีเปลี่ยนตำแหน่ง โอน หรือย้าย ต้องทำการเปลี่ยนแปลงหลังจากได้รับแจ้งจากผู้บังคับบัญชาผู้ใช้งานโดยทันที

๑๑.๒๑ ดำเนินการทบทวนสิทธิการเข้าถึงเครือข่ายของผู้ใช้งานอย่างสม่ำเสมอหรืออย่างน้อยปีละหนึ่งครั้งเพื่อป้องกันการเข้าถึงระบบเครือข่ายโดยไม่ได้รับอนุญาต

ข้อ ๑๒ การบริหารจัดการในการปฏิบัติงาน ให้ผู้ดูแลระบบปฏิบัติดังต่อไปนี้

๑๒.๑ ไม่นำข้อมูลสารสนเทศของโรงพยาบาลไปเปิดเผยกับบุคคลซึ่งไม่ได้มีความเกี่ยวข้องกับการปฏิบัติหน้าที่ เว้นแต่จะได้รับอนุญาตจากผู้บังคับบัญชา

๑๒.๒ ไม่กระทำการอื่นใดที่มีลักษณะเป็นการละเมิดสิทธิหรือเปิดเผยข้อมูลส่วนบุคคลของผู้ใช้งาน

๑๒.๓ เก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ (Log) เท่าที่จำเป็นตามที่กำหนดไว้ในกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

๑๒.๔ ตั้งเวลาของเครื่องคอมพิวเตอร์และอุปกรณ์เครือข่ายทั้งหมดในโรงพยาบาล ให้ตรงกับเวลาอ้างอิงสากล (Stratum 0)

๑๒.๕ บันทึกข้อมูลกิจกรรมการใช้งานระบบสารสนเทศและระบบเครือข่ายเพื่อใช้ในการตรวจสอบอย่างสม่ำเสมอ

๑๒.๖ ตรวจสอบและดูแลสภาพแวดล้อมของศูนย์คอมพิวเตอร์ รวมทั้งระบบสนับสนุนการทำงานต่าง ๆ เพื่อป้องกันความเสียหายต่อระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์อย่างสม่ำเสมอ

๑๒.๗ จำกัดและควบคุมการใช้งานโปรแกรมอรรถประโยชน์ (Utility program) สำหรับเครื่องคอมพิวเตอร์ที่สำคัญ เนื่องจากการใช้งานโปรแกรมอรรถประโยชน์บางชนิดสามารถทำให้ผู้ใช้งานหลีกเลี่ยงมาตรการป้องกันทางด้านความมั่นคงปลอดภัยด้านสารสนเทศของระบบได้ ดังนั้น เพื่อป้องกันการละเมิด หรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยด้านสารสนเทศที่ได้กำหนดไว้หรือที่มีอยู่แล้วให้ดำเนินการ ดังนี้

(๑) จำกัดสิทธิการเข้าถึงและกำหนดสิทธิอย่างรัดกุมในการอนุญาตให้ใช้โปรแกรมอรรถประโยชน์

(๒) กำหนดการอนุญาตใช้งานโปรแกรมอรรถประโยชน์เป็นรายครั้ง

(๓) จัดเก็บโปรแกรมอรรถประโยชน์ไว้ในสื่อภายนอกถ้าไม่ต้องใช้งานเป็นประจำ

(๔) มีการเก็บบันทึกการเรียกใช้งานโปรแกรมเหล่านี้

(๕) กำหนดให้มีการถอดถอนโปรแกรมอรรถประโยชน์ที่ไม่จำเป็นออกจากเครื่องคอมพิวเตอร์

ข้อ ๑๓ การสำรองและกู้คืนข้อมูลสารสนเทศ ให้ผู้ดูแลระบบปฏิบัติดังต่อไปนี้

๑๓.๑ กำหนดขั้นตอนการสำรองและกู้คืนข้อมูลรวมถึงซอฟต์แวร์หรือฮาร์ดแวร์ที่ใช้โดยมีรายละเอียดอย่างน้อยดังนี้

(๑) กำหนดระบบสารสนเทศสำคัญที่จำเป็นต้องสำรองข้อมูลไว้

(๒) ชื่อระบบสารสนเทศ

(๓) ผู้รับผิดชอบในการสำรองข้อมูล

(๔) ประเภทข้อมูล เช่น ซอฟต์แวร์ระบบปฏิบัติการ และซอฟต์แวร์อื่น ๆ ที่เกี่ยวข้อง ข้อมูลล็อกไฟล์ (Log file) ข้อมูลบัญชีผู้ใช้งานในระบบ เป็นต้น

(๕) ความถี่ในการสำรองข้อมูล

(๖) วิธีการสำรองข้อมูล

(๗) สื่อที่ใช้บันทึก

๑๓.๒ สำรองข้อมูลตามขั้นตอนและความถี่ที่กำหนดไว้ในแต่ละระบบ

๑๓.๓ ตรวจสอบผลสำเร็จของการสำรองข้อมูลทุกครั้ง

๑๓.๔ เลือกใช้สื่อที่เหมาะสม โดยมีอายุจัดเก็บตามระยะเวลาที่กำหนด

๑๓.๕ นำข้อมูลสำรองไปเก็บไว้นอกสถานที่อย่างน้อยหนึ่งชุด

๑๓.๖ สุ่มข้อมูลสำรองมาทดสอบกู้คืนเพื่อตรวจสอบความถูกต้องและความพร้อมใช้งานของข้อมูลในกรณีเกิดเหตุฉุกเฉินอย่างน้อยปีละหนึ่งครั้ง

๑๓.๗ ทบทวนขั้นตอนการสำรองและกู้คืนข้อมูลและประเมินประสิทธิผลการดำเนินการอย่างน้อยปีละหนึ่งครั้ง

ข้อ ๑๔ การบริหารความต่อเนื่อง ให้ผู้ดูแลระบบปฏิบัติดังต่อไปนี้

๑๔.๑ กำหนดระบบสารสนเทศสำคัญที่จำเป็นต้องเตรียมการกู้คืนระบบ

๑๔.๒ ประเมินผลกระทบกรณีระบบสารสนเทศสำคัญของโรงพยาบาลเกิดการหยุดชะงัก หรือไม่สามารถให้บริการได้

๑๔.๓ ประเมินความเสี่ยงระบบสารสนเทศสำคัญ โดยพิจารณาจากกระบวนการดำเนินงาน การวิเคราะห์ผลกระทบเพื่อระบุเหตุการณ์ที่สามารถทำให้บริการระบบสารสนเทศสำคัญหยุดชะงัก หรือไม่สามารถให้บริการได้ กำหนดแผนการลดความเสี่ยงและจัดการกับความเสี่ยงเหล่านั้น ทั้งนี้ กำหนดให้มีการทบทวนความเสี่ยงและผลกระทบอย่างสม่ำเสมอ หรือเมื่อมีการเปลี่ยนแปลงสำคัญ หรืออย่างน้อยปีละหนึ่งครั้ง

๑๔.๔ กำหนดกรอบการดำเนินการในการวางแผนการบริหารความต่อเนื่อง ให้มีองค์ประกอบดังนี้

(๑) ขั้นตอนการเตรียมการ คือ รายละเอียดของขั้นตอนต่าง ๆ ที่ต้องทำก่อนเริ่มดำเนินการตามแผน

(๒) ขั้นตอนกรณีฉุกเฉิน คือ การปฏิบัติในกรณีฉุกเฉินเมื่อเกิดเหตุการณ์คุกคามการให้บริการความมั่นคงปลอดภัย หรือชีวิต

(๓) ขั้นตอนการฟื้นฟู คือ สิ่งที่ต้องดำเนินการเพื่อฟื้นฟูกระบวนการและบริการที่มีความสำคัญ

(๔) ขั้นตอนการดำเนินงานต่อไป คือ รายละเอียดเกี่ยวกับขั้นตอนที่ต้องดำเนินการเพื่อกลับคืนสู่การดำเนินงานตามปกติ

๑๔.๕ จัดทำแผนการบริหารความต่อเนื่อง โดยอ้างอิงจากมาตรฐานการบริหารความต่อเนื่อง ซึ่งมีรายละเอียดอย่างน้อยดังนี้

(๑) ลำดับของผู้มีอำนาจในการสั่งการใช้แผนกู้คืนระบบ

(๒) โครงสร้างของทีมกู้คืนระบบ

(๓) รายชื่อและข้อมูลติดต่อของทีมกู้คืนระบบ

(๔) การสั่งการใช้แผนกู้คืนระบบ

(๕) การสั่งย้ายสถานที่ปฏิบัติงานไปยังศูนย์คอมพิวเตอร์สำรอง

(๖) การเก็บรวบรวมเอกสารและอุปกรณ์ที่จำเป็นเพื่อนำไปใช้งานยังศูนย์คอมพิวเตอร์สำรอง

(๗) การเตรียมความพร้อมของศูนย์คอมพิวเตอร์สำรอง (ก่อนเปิดใช้งานกรณีที่ศูนย์คอมพิวเตอร์หลักไม่สามารถใช้งานได้)

(๘) การแจ้งข้อมูลเกี่ยวกับเหตุการณ์ฉุกเฉินให้ผู้ให้บริการภายนอกได้รับทราบ

(๙) การเริ่มต้นปฏิบัติงาน ณ ศูนย์คอมพิวเตอร์สำรอง

(๑๐) การกลับคืนสู่สภาวะการทำงานตามปกติ (ภายหลังจากที่ได้แก้ไขสถานการณ์ของศูนย์คอมพิวเตอร์หลักแล้ว)

(๑๑) ให้ความรู้แก่ผู้ที่เกี่ยวข้องทั้งหมดทั้งทีมกู้คืนระบบและผู้ให้บริการภายนอกเพื่อให้สามารถปฏิบัติได้อย่างถูกต้องเมื่อมีเหตุฉุกเฉินเกิดขึ้น

๑๔.๖ จัดทำแผนการทดสอบการกู้คืนระบบ และดำเนินการทดสอบตามแผนการทดสอบ บันทึกผล สรุปผลและข้อเสนอแนะ พร้อมทั้งติดตามข้อบกพร่องที่พบในระหว่างการทดสอบเพื่อให้มีการปรับปรุงประสิทธิภาพต่อไปอย่างน้อยปีละหนึ่งครั้ง

๑๔.๗ ทบทวนแผนการบริหารความต่อเนื่อง โดยคำนึงถึงเหตุการณ์ในปัจจุบันและประสิทธิภาพของการปฏิบัติงานเป็นสำคัญอย่างน้อยปีละหนึ่งครั้ง

ข้อ ๑๕ การรักษาความมั่นคงปลอดภัยทางไซเบอร์ ให้ผู้ดูแลระบบปฏิบัติดังต่อไปนี้

๑๕.๑ เสนอให้โรงพยาบาล แต่งตั้งและแจ้งรายชื่อผู้บังคับบัญชาระดับบริหารและระดับปฏิบัติการเพื่อประสานงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ไปยังสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติกำหนด

๑๕.๒ ต้องปฏิบัติตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยที่สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติกำหนด

๑๕.๓ จัดให้มีกระบวนการในการบ่งชี้ ป้องกัน ตรวจสอบ รับมือ และกู้คืนต่อภัยคุกคามทางไซเบอร์ของโรงพยาบาลอย่างเป็นระบบ รวมทั้งกระบวนการในการแจ้งเหตุและประสานงานกับหน่วยงานต่าง ๆ ตามที่พระราชบัญญัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ.๒๕๖๒ กำหนด

๑๕.๔ จัดให้มีการประเมินความเสี่ยงความมั่นคงปลอดภัยทางไซเบอร์ และจัดทำแผนรับมือหรือตอบสนองต่อภัยคุกคามทางไซเบอร์ พร้อมพิจารณาทบทวนอย่างน้อยปีละหนึ่งครั้ง

๑๕.๕ จัดให้มีการซักซ้อมแผนรับมือหรือตอบสนองต่อภัยคุกคามทางไซเบอร์ตามสถานการณ์ที่สอดคล้องกับบริบทในปัจจุบันหรือตามสถานการณ์ที่ได้ประเมินความเสี่ยงไว้ และนำผลที่ได้จากการซักซ้อมมาแก้ไขปรับปรุงแผนรับมือหรือตอบสนองต่อภัยคุกคามทางไซเบอร์อย่างน้อยปีละหนึ่งครั้ง

๑๕.๖ จัดให้มีการอบรม ประชาสัมพันธ์ หรือสื่อสารเพื่อสร้างความตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์กับผู้ที่เกี่ยวข้องอย่างสม่ำเสมอ

๑๕.๗ ส่งเสริมและสนับสนุนให้ผู้ดูแลระบบได้รับการอบรมเพิ่มพูนความรู้ความเข้าใจและทักษะในการจัดการและรักษาความมั่นคงปลอดภัยทางไซเบอร์

ข้อ ๑๖ การคุ้มครองข้อมูลส่วนบุคคล ให้ผู้ดูแลระบบปฏิบัติดังต่อไปนี้

๑๖.๑ ในกรณีที่หน่วยงานจะต้องมีการร้องขอข้อมูลส่วนบุคคลเพื่อประกอบการดำเนินงาน หน่วยงานนั้นต้องทำการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลในการจัดเก็บและดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลนั้น รวมทั้งจัดเก็บข้อมูลการให้ความยินยอมนั้นไว้เป็นหลักฐาน

๑๖.๒ ข้อมูลส่วนบุคคลที่โรงพยาบาล มีการจัดเก็บต้องจัดให้มีการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคลตามมาตรการหรือประกาศที่โรงพยาบาลกำหนด

๑๖.๓ จัดทำและประกาศใช้นโยบายและแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลและดำเนินการตามนโยบายและแนวปฏิบัติดังกล่าวอย่างเคร่งครัด รวมทั้งจัดให้มีกระบวนการบริหารจัดการเพื่อรองรับสิทธิของผู้เป็นเจ้าของข้อมูลส่วนบุคคลตามที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒ กำหนด

๑๖.๔ จัดให้มีกระบวนการในการจัดการและแจ้งเหตุในกรณีที่ข้อมูลส่วนบุคคลถูกละเมิดความมั่นคงปลอดภัย ภายในระยะเวลาเจ็ดสิบสองชั่วโมงนับแต่เกิดเหตุ

ข้อ ๑๗ การปฏิบัติตามกฎหมาย และมาตรฐานสากล ให้ผู้ดูแลระบบปฏิบัติดังต่อไปนี้

๑๗.๑ ปฏิบัติตามกฎหมาย และมาตรฐานสากลที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๑๗.๒ ตรวจสอบและควบคุมมิให้มีการละเมิดทรัพย์สินทางปัญญาด้านเทคโนโลยีสารสนเทศ

๑๗.๓ ตรวจสอบด้านเทคโนโลยีสารสนเทศของโรงพยาบาล ตามระยะเวลาที่เหมาะสม

๑๗.๔ จัดให้มีการอบรมสร้างความรู้ความเข้าใจเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศสำหรับผู้ใช้งานอย่างน้อยปีละหนึ่งครั้ง

๑๗.๕ ประชาสัมพันธ์ หรือสื่อสารเพื่อสร้างความตระหนักรู้กฎหมาย และมาตรฐานสากลที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศในลักษณะเกร็ดความรู้หรือข้อควรระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่ายผ่านทางระบบอินทราเน็ตของโรงพยาบาล หรือช่องทางที่เหมาะสม

หมวด ๒
แนวปฏิบัติของผู้ใช้งาน

ข้อ ๑๘ การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Security) ให้ผู้ใช้งานปฏิบัติดังต่อไปนี้

๑๘.๑ ปฏิบัติตามมาตรการควบคุมการเข้า-ออก ศูนย์คอมพิวเตอร์โรงพยาบาลอย่างเคร่งครัด

๑๘.๒ ติดบัตรแสดงตัวตนให้เห็นเด่นชัดตลอดระยะเวลาที่อยู่ภายในพื้นที่ศูนย์

๑๘.๓ ทำการยืนยันตัวตนก่อนเข้าศูนย์คอมพิวเตอร์ของโรงพยาบาลทุกครั้ง

๑๘.๔ ลงชื่อ บันทึกวัน เวลา และวัตถุประสงค์การเข้า-ออก ศูนย์คอมพิวเตอร์ของโรงพยาบาล

๑๘.๕ ไม่นำอาหารและเครื่องดื่มเข้าไปภายในศูนย์คอมพิวเตอร์

๑๘.๖ ไม่สูบบุหรี่ หรือกระทำการใด ๆ อันอาจก่อให้เกิดควันหรือเพลิงในบริเวณศูนย์คอมพิวเตอร์

ข้อ ๑๙ การบริหารจัดการสินทรัพย์ ให้ผู้ใช้งานปฏิบัติดังต่อไปนี้

๑๙.๑ ดูแลรักษาสินทรัพย์ที่โรงพยาบาลมอบไว้ให้ใช้งานเสมือนหนึ่งเป็นทรัพย์สินของตนเอง

๑๙.๒ ห้ามทิ้งสินทรัพย์ของโรงพยาบาลไว้โดยไม่มีผู้ดูแล ซึ่งรวมถึงการทิ้งไว้ในรถยนต์ที่สามารถมองเห็นได้จากภายนอก

๑๙.๓ ห้ามให้ผู้อื่นยืมสินทรัพย์ของโรงพยาบาลไปใช้งาน เช่น เพื่อน พี่น้อง หรือญาติ

๑๙.๔ ใช้งานสินทรัพย์และระบบสารสนเทศต่าง ๆ ในการปฏิบัติงานของโรงพยาบาล เท่านั้น

๑๙.๕ แจ้งโรงพยาบาลก่อนดำเนินการเปลี่ยนจุดติดตั้งหรือส่งซ่อมสินทรัพย์คอมพิวเตอร์ในสมุดลงชื่อให้ชัดเจนทุกครั้ง

๑๙.๖ ส่งคืนสินทรัพย์ให้เจ้าหน้าที่ผู้รับผิดชอบของโรงพยาบาล เมื่อผู้ใช้งานต้องการยกเลิกสิทธิการครอบครองสินทรัพย์นั้น ๆ หรือพ้นสภาพการเป็นผู้ปฏิบัติงานของโรงพยาบาล

๑๙.๗ ต้องดำเนินการป้องกันการเข้าถึงเครื่องคอมพิวเตอร์ส่วนตัวเมื่อนำมาใช้งานภายในเครือข่ายของโรงพยาบาล

๑๙.๘ จัดวางสินทรัพย์ต่าง ๆ ในพื้นที่หรือบริเวณที่เหมาะสมเพื่อหลีกเลี่ยงการเข้าถึงโดยไม่ได้รับอนุญาต

๑๙.๙ ปิดเครื่องคอมพิวเตอร์ที่ตนเองใช้งานอยู่เมื่อใช้งานประจำวันเสร็จสิ้น เว้นแต่เครื่องคอมพิวเตอร์นั้นเป็นเครื่องเซิร์ฟเวอร์ให้บริการที่ต้องใช้บริการตลอดยี่สิบสี่ชั่วโมง

๑๙.๑๐ ให้ผู้บังคับบัญชาอนุมัติก่อนทุกครั้งในกรณีที่ต้องการนำอุปกรณ์คอมพิวเตอร์ต่าง ๆ ออกนอกโรงพยาบาล

๑๙.๑๑ ห้ามติดตั้งโปรแกรมคอมพิวเตอร์เพิ่มเติมนอกเหนือจากที่โรงพยาบาลได้ติดตั้งไว้ให้ใช้งาน

๑๙.๑๒ ห้ามติดตั้งโปรแกรมคอมพิวเตอร์ที่สามารถใช้งานการตรวจสอบข้อมูลบนระบบเครือข่าย ยกเว้นการติดตั้งเพื่อการปฏิบัติงานของผู้ดูแลระบบที่เกี่ยวข้อง

๑๙.๑๓ ห้ามติดตั้งโปรแกรมคอมพิวเตอร์ หรืออุปกรณ์คอมพิวเตอร์อื่นใดเพิ่มเติมในเครื่องคอมพิวเตอร์หรือเครือข่ายของหน่วยงาน เพื่อให้บุคคลอื่นสามารถใช้งานเครื่องคอมพิวเตอร์นั้นหรือเครือข่ายของหน่วยงานได้

๑๙.๑๔ ต้องแจ้งผู้บังคับบัญชาทันทีที่พบว่าสินทรัพย์เสียหาย สูญหาย หรือปรากฏว่ามีผู้อื่นเข้าถึงสินทรัพย์ดังกล่าว โดยที่ผู้ใช้งานมิได้อนุญาตเพื่อจัดการเหตุการณ์ได้อย่างมีประสิทธิภาพ

ข้อ ๒๐ การบริหารจัดการบัญชีผู้ใช้งาน (User Account) ให้ผู้ใช้งานปฏิบัติดังต่อไปนี้

๒๐.๑ เปลี่ยนรหัสผ่านทันทีหลังจากได้รับแจ้งจากผู้ดูแลระบบ

๒๐.๒ กำหนดรหัสผ่าน (Password) ตามหลักเกณฑ์ดังนี้

(๑) รหัสผ่านต้องประกอบด้วยตัวอักษรตัวใหญ่ ตัวเล็ก ตัวเลข และตัวอักขระพิเศษผสมกันไม่น้อยกว่า ๘ ตัว เช่น Pol#2022

(๒) ไม่ตั้งรหัสผ่านด้วยข้อมูลที่เกี่ยวข้องกับตนเอง เช่น ชื่อตนเองหรือครอบครัว ชื่อเล่น วันเดือนปีเกิด หรือทะเบียนรถยนต์ รวมทั้งหมายเลขโทรศัพท์

(๓) ไม่ตั้งรหัสผ่านด้วยคำศัพท์ที่มีอยู่ในพจนานุกรม

๒๐.๓ เก็บรักษาชื่อผู้ใช้งาน (Username) และรหัสผ่าน ของตนเองเป็นความลับไม่เผยแพร่ ไม่แจกจ่าย ไม่ใช้ร่วมกับผู้อื่น หรือทำให้ผู้อื่นล่วงรู้ด้วยวิธีการใด ๆ

๒๐.๔ รับผิดชอบต่อการกระทำใด ๆ ที่เกิดจากบัญชีผู้ใช้งานไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม

๒๐.๕ ไม่จดหรือบันทึกบัญชีผู้ใช้งานไว้ในสถานที่ที่ง่ายต่อการคาดเดาหรือสังเกตเห็นของบุคคลอื่น

๒๐.๖ ควรปิดการใช้งาน (Lock) เครื่องคอมพิวเตอร์ทุกครั้งเมื่อผู้ใช้งานไม่อยู่ที่เครื่องคอมพิวเตอร์

๒๐.๗ เปลี่ยนรหัสผ่านทันทีเมื่อคาดว่ามีการล่วงรู้รหัสผ่านจากบุคคลอื่น

๒๐.๘ ไม่ใช้รหัสผ่านซึ่งเคยใช้มาแล้ว (Password History) อย่างน้อยสามรหัสผ่าน

๒๐.๙ ไม่ควรใช้โปรแกรมคอมพิวเตอร์ช่วยจำรหัสผ่านโดยอัตโนมัติ

๒๐.๑๐ แจ้งผู้ดูแลระบบทันทีหากไม่สามารถใช้งานบัญชีผู้ใช้งานได้

๒๐.๑๑ กำหนดให้เครื่องคอมพิวเตอร์พักหน้าจออัตโนมัติหากไม่มีการใช้งานเครื่องคอมพิวเตอร์ติดต่อกันสิบห้านาที โดยให้ป้อนชื่อผู้ใช้งาน และรหัสผ่านอีกครั้งก่อนใช้งาน

ข้อ ๒๑ การบริหารจัดการความปลอดภัยเครือข่ายของโรงพยาบาล ให้ผู้ใช้งานปฏิบัติดังต่อไปนี้

๒๑.๑ ต้องใช้บริการสารสนเทศผ่านระบบเครือข่ายตามที่โรงพยาบาลกำหนดไว้เท่านั้น

๒๑.๒ ลงทะเบียนคำขอใช้งานและต้องได้รับอนุญาตจากผู้บังคับบัญชาก่อนการเข้าถึงเครือข่ายภายในโรงพยาบาลด้วยเครื่องคอมพิวเตอร์ส่วนตัว

๒๑.๓ การใช้งานเครือข่ายอินทราเน็ตผ่านเครือข่ายอินเทอร์เน็ตจากภายนอกของโรงพยาบาล ผู้ใช้งานต้องเชื่อมต่อด้วยเทคโนโลยีเครือข่ายเสมือนส่วนตัว (Virtual Private Network: VPN) ตามที่โรงพยาบาลกำหนด

๒๑.๔ ห้ามกระทำการใด ๆ ที่ส่งผลกระทบ ชะลอ ขัดขวาง หรือรบกวน การส่งผ่านข้อมูลในการดำเนินงานของโรงพยาบาล ในระบบเครือข่ายของโรงพยาบาล จนไม่สามารถทำงานตามปกติได้

ข้อ ๒๒ การใช้งานอุปกรณ์คอมพิวเตอร์ ให้ผู้ใช้งานปฏิบัติดังต่อไปนี้

๒๒.๑ อุปกรณ์คอมพิวเตอร์ที่โรงพยาบาล จัดไว้ให้ใช้งานถือเป็นทรัพย์สินของโรงพยาบาล และมีวัตถุประสงค์เพื่อใช้ในการดำเนินงานของโรงพยาบาล เท่านั้น

๒๒.๒ ดูแลรักษาอุปกรณ์คอมพิวเตอร์โดยจัดเก็บไว้ในที่ปลอดภัย ไม่วางทิ้งไว้ในสถานที่เสี่ยงต่อการสูญหาย และหลีกเลี่ยงการใช้งานอุปกรณ์คอมพิวเตอร์แบบพกพาในสภาพแวดล้อมที่อาจมีผลกระทบต่อความเสียหายของอุปกรณ์

๒๒.๓ รับผิดชอบในการป้องกันการสูญหายของข้อมูล ในกรณีที่อุปกรณ์คอมพิวเตอร์สูญหายหรือเสียหาย ผู้ใช้งานต้องแจ้งต่อผู้บังคับบัญชาโดยเร็ว

๒๒.๔ ดูแลรักษาข้อมูลของโรงพยาบาลที่จัดเก็บในอุปกรณ์คอมพิวเตอร์ให้สอดคล้องตามการบริหารจัดการข้อมูลองค์กร

๒๒.๕ เมื่อผู้ใช้งานพ้นสภาพการเป็นข้าราชการตำรวจในสังกัดโรงพยาบาล ต้องส่งอุปกรณ์คอมพิวเตอร์และอุปกรณ์เสริมทั้งหมดที่โรงพยาบาล จัดไว้ให้ใช้งาน คืนต่อโรงพยาบาล

๒๒.๖ การยืม การคืน หรือส่งซ่อมอุปกรณ์คอมพิวเตอร์แบบพกพาที่โรงพยาบาลจัดไว้ให้ใช้งานให้เป็นไปตามขั้นตอนปฏิบัติที่โรงพยาบาลกำหนด

๒๒.๗ ห้ามผู้ใช้งานทำการเปลี่ยนแปลงแก้ไข Configuration หรือส่วนประกอบของอุปกรณ์คอมพิวเตอร์ของโรงพยาบาล โดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

๒๒.๘ การใช้อุปกรณ์คอมพิวเตอร์ที่โรงพยาบาลจัดไว้ให้ใช้งานในการเข้าถึงระบบสารสนเทศของโรงพยาบาล ผู้ใช้งานต้องทำการเชื่อมต่อ VPN และยืนยันตัวตน (Authentication) ของผู้ใช้งานก่อนเข้าถึงระบบสารสนเทศของโรงพยาบาล ที่เคยใช้งานล่าสุด

๒๒.๙ เพื่อป้องกันการเข้าถึงอุปกรณ์คอมพิวเตอร์โดยไม่ได้รับอนุญาต ผู้ใช้งานจะต้องกำหนดมาตรการป้องกันการเข้าถึงอุปกรณ์คอมพิวเตอร์ ได้แก่ การใช้บัญชีผู้ใช้งานและรหัสผ่าน

๒๒.๑๐ ก่อนการใช้งานกับสื่อบันทึกข้อมูลต่าง ๆ ต้องมีการตรวจสอบเพื่อหาไวรัสคอมพิวเตอร์โดยโปรแกรมป้องกันไวรัสคอมพิวเตอร์

๒๒.๑๑ ไม่นำอาหาร เครื่องดื่ม หรือสิ่งที่เป็นของเหลว มาวางใกล้บริเวณเครื่องคอมพิวเตอร์

๒๒.๑๒ ไม่วางของทับบนเครื่องคอมพิวเตอร์ หรือแป้นพิมพ์

๒๒.๑๓ กรณีต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพา ควรใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพาเพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน เช่น การตกจากที่สูง เป็นต้น

ข้อ ๒๓ การบริหารจัดการซอฟต์แวร์และทรัพย์สินทางปัญญา ให้ผู้ใช้งานปฏิบัติดังต่อไปนี้

๒๓.๑ ไม่คัดลอก แก้ไข ถอดถอนโปรแกรมมาตรฐานต่าง ๆ ที่ถูกติดตั้งบนเครื่องคอมพิวเตอร์ของโรงพยาบาลหรือนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือนำไปให้ผู้อื่นใช้งาน

๒๓.๒ ไม่ติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ละเมิดทรัพย์สินทางปัญญา หากมีการตรวจสอบพบความผิดฐานละเมิดทรัพย์สินทางปัญญา โรงพยาบาลจะถือว่าเป็นความผิดส่วนบุคคล

๒๓.๓ ไม่ติดตั้งโปรแกรมคอมพิวเตอร์บนเครื่องคอมพิวเตอร์ของโรงพยาบาลเพิ่มเติมก่อนได้รับอนุญาตจากผู้ดูแลระบบ

๒๓.๔ ปฏิบัติตามเงื่อนไขการใช้งานหรือที่กำหนดไว้ของทรัพย์สินทางปัญญาต่าง ๆ ที่โรงพยาบาลหรือผู้ใช้งานมีใช้งานหรือครอบครอง

๒๓.๕ ห้ามเปลี่ยนแปลงหรือแก้ไขซอฟต์แวร์สำเร็จรูปที่โรงพยาบาลจัดหามาใช้งาน เว้นแต่โรงพยาบาลได้รับอนุญาตให้เปลี่ยนแปลงแก้ไขได้จากเจ้าของลิขสิทธิ์

๒๓.๖ ไม่นำผลงานของผู้อื่นหรือผลงานใด ๆ ที่มีลิขสิทธิ์มาทำการ “คัดลอก” หรือ “ดัดแปลง” ก่อนได้รับอนุญาตจากเจ้าของลิขสิทธิ์

ข้อ ๒๔ การป้องกันโปรแกรมไม่พึงประสงค์ ให้ผู้ใช้งานปฏิบัติดังต่อไปนี้

๒๔.๑ ไม่เปิดไฟล์ที่ไม่ทราบแหล่งที่มา หรือมาจากแหล่งที่มาที่ไม่น่าเชื่อถือ

๒๔.๒ การนำอุปกรณ์จัดเก็บข้อมูลต่าง ๆ เช่น Thumb Drive และ Data Storage มาใช้งานร่วมกับเครื่องคอมพิวเตอร์ของโรงพยาบาล ให้ตรวจสอบหาโปรแกรมไม่พึงประสงค์ก่อนทุกครั้ง

๒๔.๓ ตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรืออีเมล (E-mail) หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัสก่อนเปิดใช้งาน

๒๔.๔ ตรวจสอบฐานข้อมูลไวรัสของโปรแกรมป้องกันไวรัส กรณีไม่ปรับปรุงให้เป็นปัจจุบันผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบโดยทันที

๒๔.๕ ห้ามถอดถอนโปรแกรมป้องกันไวรัสที่โรงพยาบาลได้ติดตั้งไว้ให้

๒๔.๖ ระมัดระวังการเข้าเว็บไซต์ที่มีความเสี่ยงเนื่องจากการเปิดไฟล์หรือเข้าเว็บไซต์อาจได้รับไวรัสจากไฟล์หรือเข้าเว็บไซต์เหล่านั้น

ข้อ ๒๕ การใช้งานอินเทอร์เน็ต ให้ผู้ใช้งานปฏิบัติดังต่อไปนี้

๒๕.๑ ปฏิบัติตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์อย่างเคร่งครัด

๒๕.๒ ไม่ใช้งานอินเทอร์เน็ตของโรงพยาบาล เพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัวและการเข้าสู่เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาที่ขัดต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม

๒๕.๓ ไม่เปิดเผยข้อมูลสำคัญที่เป็นความลับของโรงพยาบาล โดยไม่ได้รับอนุญาต

๒๕.๔ ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของโรงพยาบาล ที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต

๒๕.๕ ไม่เสนอความคิดเห็นหรือใช้ข้อความยั่วยุ ให้ร้ายบุคคลอื่น หรือข้อมูลที่ผิดกฎหมายในการใช้งานกระดานสนทนา (Web Board) สาธารณะ

๒๕.๖ ไม่ใช้งานโปรแกรมแบบเพียร์ทูเพียร์ (Peer to Peer : P2P) ผ่านเครือข่ายโรงพยาบาล

๒๕.๗ ไม่เข้าเว็บไซต์เครือข่ายสังคม (Social Network) เช่น Facebook Twitter หรือ Game online เป็นต้น นอกเหนือจากการปฏิบัติงานผ่านเครือข่ายโรงพยาบาล

๒๕.๘ ไม่ใช้งานสตรีมมิ่งมีเดีย (Streaming Media) นอกเหนือจากการปฏิบัติงานผ่านเครือข่ายโรงพยาบาล

๒๕.๙ ต้องปิดเว็บบราวเซอร์เมื่อสิ้นสุดการใช้งานเพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น

ข้อ ๒๖ การใช้งานจดหมายอิเล็กทรอนิกส์หรืออีเมล ให้ผู้ใช้งานปฏิบัติดังต่อไปนี้

๒๖.๑ การปฏิบัติงานที่เกี่ยวข้องกับโรงพยาบาล ให้ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์หรืออีเมล (E-mail address) ของโรงพยาบาล (ชื่อบัญชีผู้ใช้งาน @policehospital.org) ที่ผู้ดูแลระบบกำหนดให้เท่านั้น

๒๖.๒ ระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์หรืออีเมลเพื่อไม่ให้เกิดความเสียหายต่อโรงพยาบาล ในการละเมิดทรัพย์สินทางปัญญา ละเมิดศีลธรรม สร้างความรำคาญต่อผู้อื่นหรือผิดกฎหมาย รวมทั้งไม่แสวงหาผลประโยชน์ หรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจ

๒๖.๓ ห้ามเข้าถึงข้อมูลจดหมายอิเล็กทรอนิกส์หรืออีเมลของผู้อื่นโดยไม่ได้รับอนุญาต

๒๖.๔ ห้ามปลอมแปลงจดหมายอิเล็กทรอนิกส์หรืออีเมล

๒๖.๕ ใช้คำพูดที่สุภาพในการส่งจดหมายอิเล็กทรอนิกส์หรืออีเมล

๒๖.๖ สำรองข้อมูลจดหมายอิเล็กทรอนิกส์หรืออีเมลอย่างสม่ำเสมอ

๒๖.๗ ออกจากระบบ (Log out) ทุกครั้งเมื่อไม่ใช้งานระบบจดหมายอิเล็กทรอนิกส์หรืออีเมล เพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์

๒๖.๘ ตรวจสอบเอกสารที่แนบมาจากจดหมายอิเล็กทรอนิกส์หรืออีเมลก่อนทำการเปิดโดยใช้โปรแกรมป้องกันไวรัส

๒๖.๙ ไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์หรืออีเมลที่ได้รับจากผู้ส่งที่ไม่รู้จักหรือมีลักษณะสแปมเมล (Spam Mail) เช่น การหลอกลวง การขายสินค้า หรือการสมัครสมาชิก เป็นต้น

๒๖.๑๐ ไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์ที่มีลักษณะเป็นอีเมลลูกโซ่ (Chain E-mail/Letter)

๒๖.๑๑ ตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์หรืออีเมล (Inbox) ของตนเองทุกวันและควรลบจดหมายอิเล็กทรอนิกส์หรืออีเมลที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้พื้นที่ระบบจดหมายอิเล็กทรอนิกส์หรืออีเมล

ข้อ ๒๗ การใช้งานเครือข่ายสังคมออนไลน์ (Social Network) ให้ผู้ใช้งานปฏิบัติดังต่อไปนี้

๒๗.๑ กรณีจำเป็นต้องใช้การประชาสัมพันธ์ผ่านเครือข่ายสังคมออนไลน์ (Social Network) ในนามของโรงพยาบาลผู้รับผิดชอบต้องแสดงตำแหน่ง หน้าที่ และสังกัดให้ชัดเจนเพื่อความน่าเชื่อถือ โดยอาจใช้รูปสัญลักษณ์หรือเครื่องหมายแสดงสังกัดได้

๒๗.๒ การนำเสนอเนื้อหาข้อมูลผ่านเครือข่ายสังคมออนไลน์ (Social Network) ควรนำเสนอเกี่ยวกับภารกิจของโรงพยาบาลได้แก่ วิสัยทัศน์ พันธกิจ ผลการดำเนินงาน และข่าวสารที่เป็นประโยชน์ มีความถูกต้อง ใช้ภาษาที่สุภาพ และมีรูปแบบที่น่าสนใจ โดยเนื้อหาต้องผ่านความเห็นชอบจากผู้บังคับบัญชาก่อนทุกครั้ง

๒๗.๓ ห้ามเปิดเผยข้อมูลสำคัญหรือข้อมูลที่เป็นความลับของโรงพยาบาลผ่านเครือข่ายสังคมออนไลน์ (Social Network) เว้นแต่ได้รับอนุญาตจากเจ้าของข้อมูล

๒๗.๔ กรณีประชาชนหรือหน่วยงานอื่นมีความคิดเห็นแตกต่างต้องชี้แจงด้วยเหตุผล งดเว้นการโต้ตอบด้วยความรุนแรง และควรพิจารณานำความคิดเห็นดังกล่าวมาใช้ในการพัฒนาปรับปรุงในเรื่องที่เกี่ยวข้องต่อไป

๒๗.๕ ห้ามแสดงความคิดเห็นที่อาจทำให้เข้าใจว่าเป็นความคิดเห็นจากโรงพยาบาล และต้องแสดงข้อความจำกัดความรับผิดชอบ (Disclaimer) ว่าเป็นความคิดเห็นส่วนตัว

๒๗.๖ หากเกิดความผิดพลาดจากการใช้งานเครือข่ายสังคมออนไลน์ (Social Network) ผู้ใช้งาน (User) ต้องรับผิดชอบความเสียหายที่เกิดขึ้น และแจ้งต่อผู้บังคับบัญชาโดยเร็วที่สุดเพื่อดำเนินการตามความเหมาะสม

๒๗.๗ ต้องมีความตระหนักเรื่องความมั่นคงปลอดภัยด้านสารสนเทศอยู่เสมอและต้องรับผิดชอบหากเกิดความเสียหายใด ๆ ที่มีผลกระทบกับโรงพยาบาลจากการใช้งานเครือข่ายสังคมออนไลน์

๒๗.๘ อนุญาตให้ใช้งานเครือข่ายสังคมออนไลน์ในรูปแบบและลักษณะตามที่โรงพยาบาลได้กำหนดไว้เท่านั้น

ข้อ ๒๘ การบริหารจัดการข้อมูลองค์กร ให้ผู้ใช้งานปฏิบัติดังต่อไปนี้

๒๘.๑ ระมัดระวังในการนำสื่อบันทึกข้อมูลให้ผู้อื่นใช้งาน

๒๘.๒ ดูแลรักษาความลับของข้อมูลลับ โดยหากข้อมูลอยู่ในรูปแบบอิเล็กทรอนิกส์จะต้องมีการป้องกันการเข้าถึงจากผู้ไม่มีสิทธิ หรือพิจารณาใช้มาตรการการเข้ารหัสโดยจะต้องใช้เทคโนโลยีที่ทางโรงพยาบาลกำหนดให้ หรืออย่างน้อยจะต้องเป็นเทคโนโลยีที่ได้รับการยอมรับและเป็นที่รู้จักดี

๒๘.๓ ไม่นำข้อมูลไปเปิดเผยกับบุคคลซึ่งไม่มีความเกี่ยวข้องกับการปฏิบัติหน้าที่เว้นแต่ได้รับอนุญาตจากผู้บังคับบัญชา

๒๘.๔ กำหนดประเภท ลำดับชั้นความลับ รวมถึงระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึงสำหรับข้อมูลสารสนเทศแต่ละชนิดอย่างเหมาะสม

๒๘.๕ การจัดลำดับชั้นความลับของข้อมูล แบ่งออกเป็น ๕ ระดับ ดังนี้

(๑) ระดับเปิดเผยได้ (Public) หมายถึง สารสนเทศที่เปิดเผยสู่สาธารณชนโดยบุคคลที่มีหน้าที่หรือได้รับมอบอำนาจให้ดำเนินการเผยแพร่ได้ โดยสารสนเทศที่เปิดเผยดังกล่าวได้ถูกพิจารณาแล้วว่าเมื่อมอบให้บุคคลอื่นแล้วจะไม่ก่อให้เกิดความเสียหายต่อองค์กร

(๒) ระดับส่วนบุคคลของผู้ปฏิบัติงาน (Personal) หมายถึง สารสนเทศที่เป็นข้อมูลของแต่ละบุคคลที่ใช้ในการปฏิบัติงาน

(๓) ระดับส่วนบุคคลของผู้ใช้บริการ (Data Privacy) หมายถึง สารสนเทศที่เป็นข้อมูลของผู้ใช้บริการจัดเก็บไว้ในระบบหรือระบบงานเพื่อดำเนินการต่าง ๆ

(๔) ระดับใช้ภายในเท่านั้น (Internal Use Only หรือ Internal Use) หมายถึง สารสนเทศทั่วไปที่ใช้สื่อสารกันภายในเท่านั้น

(๕) ระดับลับ (Confidential) หมายถึง สารสนเทศที่ถูกพิจารณาแล้วว่า มีความสำคัญ

๒๘.๖ ระดับการเข้าถึง คือ

(๑) การเข้าถึงเพื่อการอ่าน (Read)

(๒) การเข้าถึงเพื่อการเขียน (Write)

(๓) การเข้าถึงเพื่อการแก้ไข (Edit)

(๔) การเข้าถึงเพื่อการลบ (Delete)

๒๘.๗ เวลาที่ได้เข้าถึง สามารถเข้าถึงข้อมูลได้ตลอดเวลายี่สิบสี่ชั่วโมง เจ็ดวันหรือตามภารกิจและความจำเป็นของผู้ใช้งานที่ได้รับมอบหมาย

๒๘.๘ ช่องทางการเข้าถึง ต้องจำกัดช่องทางการใช้งานหรือการเข้าถึงข้อมูลเท่าที่มีความจำเป็นต่อการใช้งานเท่านั้น

ข้อ ๒๙ การบริหารจัดการการเข้ารหัสข้อมูล ให้ผู้ใช้งานปฏิบัติดังต่อไปนี้

๒๙.๑ กำหนดมาตรฐานและระเบียบวิธีปฏิบัติการบริหารจัดการการเข้ารหัสข้อมูลครอบคลุมขอบเขตหน้าที่ ความรับผิดชอบของหน่วยงานที่เกี่ยวข้อง วิธีการเข้ารหัสข้อมูล (cryptographic algorithm) ที่สอดคล้องตามระดับความสำคัญของข้อมูล และการบริหารจัดการกุญแจเข้ารหัสข้อมูล (key management) ข้อมูลสำคัญกับภายนอก

๒๙.๒ กำหนดให้มีการเข้ารหัสข้อมูลสำคัญและช่องทางการสื่อสารที่ใช้รับส่ง

๒๙.๓ วิธีการเข้ารหัสข้อมูล ควรใช้มาตรฐานการเข้ารหัสข้อมูลที่เชื่อถือได้และเป็นมาตรฐานสากล เช่น การเข้ารหัสข้อมูลแบบสมมาตร (เช่น AES) หรือการเข้ารหัสข้อมูลแบบอสมมาตร (เช่น public key cryptography) เป็นต้น โดยมีการทบทวนประสิทธิภาพของวิธีการเข้ารหัสข้อมูลอย่างสม่ำเสมอเพื่อให้มั่นใจว่าวิธีการเข้ารหัสข้อมูลที่ใช้งานยังคงมีความแข็งแรงเพียงพอ

๒๙.๔ การบริหารจัดการกุญแจเข้ารหัสข้อมูล (key management) ควรกำหนดกระบวนการที่มีความรัดกุม ปลอดภัยครอบคลุมตั้งแต่การสร้างและติดตั้ง การจัดเก็บ และการยกเลิกกุญแจเข้ารหัสข้อมูล ดังนี้

๒๙.๔.๑ การสร้างและติดตั้งกุญแจเข้ารหัสข้อมูล ให้ปฏิบัติดังนี้

(๑) มีการควบคุมสภาพแวดล้อมในการสร้างรหัสที่มีความรัดกุมปลอดภัยเช่น เลือกใช้ผู้ให้บริการออกใบรับรอง (Certification Authority) ที่น่าเชื่อถือ มีขั้นตอนการทำลายหลักฐานที่ใช้หลังจากสร้างกุญแจแล้วเสร็จ

(๒) กุญแจเข้ารหัสข้อมูลจะต้องไม่มีบุคคลใดบุคคลหนึ่งรู้รหัสทั้งหมด

(๓) กำหนดขนาดของกุญแจเข้ารหัสข้อมูลที่มีความยาวเพียงพอในการป้องกันการถูกถอดรหัส เช่น การถูกโจมตีแบบ brute force เป็นต้น การแลกเปลี่ยนกุญแจต้องผ่านกระบวนการและช่องทางที่ปลอดภัยกำหนดไม่ให้ใช้กุญแจเข้ารหัสข้อมูลเดียวกันกับหลายระบบสารสนเทศ

๒๙.๔.๒ การจัดเก็บกุญแจเข้ารหัสข้อมูล ให้ปฏิบัติดังนี้

(๑) มีการรักษาความปลอดภัยของกุญแจเข้ารหัสข้อมูลทั้งด้าน physicalและ logical โดยใช้อุปกรณ์รักษาความปลอดภัย HSM หรืออุปกรณ์ที่ทำหน้าที่ในลักษณะเดียวกัน

(๒) มีการสำรองข้อมูลกุญแจเข้ารหัสข้อมูล โดยวิธีการเก็บรักษากุญแจเข้ารหัสข้อมูลชุดสำรองต้องมีการรักษาความปลอดภัยในระดับเดียวกับกุญแจเข้ารหัสข้อมูลชุดหลัก

๒๙.๔.๓ การเปลี่ยนและเพิกถอนกุญแจเข้ารหัสข้อมูล ให้ปฏิบัติดังนี้

(๑) กำหนดเกณฑ์และแนวทางในการเปลี่ยนและเพิกถอนกุญแจเข้ารหัสข้อมูล เช่น กรณีกุญแจหมดอายุ ล้าสมัย หรือไม่ปลอดภัย เป็นต้น

(๒) กำหนดกระบวนการทำลายกุญแจโดยต้องมั่นใจว่าไม่สามารถนำกุญแจนั้นมาใช้งานได้อีก

ข้อ ๓๐ การใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities) ให้ผู้ใช้งานปฏิบัติดังต่อไปนี้

๓๐.๑ ห้ามติดตั้งซอฟต์แวร์อื่น ๆ หรือซอฟต์แวร์ที่ได้มาจากแหล่งภายนอก รวมทั้งการใช้ไฟล์อื่นที่โรงพยาบาล ไม่อนุญาตให้ใช้งาน

๓๐.๒ ซอฟต์แวร์ที่ใช้ต้องมีลิขสิทธิ์การใช้งานที่ถูกต้อง ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็น และห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากตรวจพบถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานต้องรับผิดชอบแต่เพียงผู้เดียว

๓๐.๓ หากต้องการใช้งานโปรแกรมอรรถประโยชน์ที่ไม่อนุญาต เนื่องจากการใช้งานโปรแกรมอรรถประโยชน์บางชนิดสามารถทำให้ผู้ใช้ไม่ปลอดภัย ต้องได้รับความเห็นชอบที่เป็นลายลักษณ์อักษรจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง หรือผู้ที่ได้รับมอบหมายให้เป็นผู้พิจารณาอนุญาต

๓๐.๔ กำหนดให้มีการถอดถอนการติดตั้งโปรแกรมอรรถประโยชน์รวมทั้งซอฟต์แวร์ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศและการสื่อสารของโรงพยาบาลที่ไม่จำเป็นออกจากระบบ เมื่อไม่จำเป็นต้องใช้งาน

หมวด ๓
การจัดหา พัฒนาและดูแลรักษาระบบสารสนเทศ

ข้อ ๓๑ การจัดหา พัฒนา และดูแลรักษาระบบสารสนเทศของโรงพยาบาล ให้ปฏิบัติดังต่อไปนี้

๓๑.๑ การจัดหาและพัฒนาที่เกี่ยวข้องกับด้านเทคโนโลยีสารสนเทศ ให้หน่วยงานประสานงานกับโรงพยาบาลหรือหน่วยงานที่เกี่ยวข้อง เพื่อพิจารณาให้ความเห็นด้านความมั่นคงปลอดภัย และความสอดคล้องกับโครงสร้างพื้นฐานและเครือข่ายของโรงพยาบาล ก่อนนำเสนอพิจารณาอนุมัติจัดหาและพัฒนาทุกครั้ง

๓๑.๒ การจัดหาและพัฒนาที่เกี่ยวข้องกับโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศที่มีความสำคัญยิ่งและมีลักษณะสุ่มเสี่ยงต่อความล้มเหลวในการให้บริการ หากมีเพียงชุดเดียวให้ผู้รับผิดชอบพิจารณาจัดหาอุปกรณ์สำรองไว้ ทั้งนี้ ต้องได้รับความเห็นชอบจากผู้บังคับบัญชา

๓๑.๓ การพิจารณาให้ความเห็นด้านความมั่นคงปลอดภัย ให้คำนึงถึงเรื่องดังต่อไปนี้

(๑) สิทธิในทรัพย์สินทางปัญญาสำหรับชุดคำสั่ง (Source Code) ในการพัฒนา

(๒) การตรวจสอบด้านคุณภาพและความถูกต้องของระบบสารสนเทศ

(๓) การตรวจสอบชุดคำสั่งที่ไม่พึงประสงค์

(๔) ข้อจำกัดในการเปิดเผยข้อมูลของโรงพยาบาล

(๕) มาตรฐานและคุณภาพการให้บริการด้านความมั่นคง

(๖) การทดสอบระบบสารสนเทศ

๓๑.๔ ไม่อนุญาตให้นำข้อมูลสำคัญของโรงพยาบาล เช่น ข้อมูลลับ ข้อมูลส่วนบุคคล ข้อมูลผู้ป่วยนอก / ผู้ป่วยใน หรือข้อมูลใช้ภายในเท่านั้น ไปใช้ในการทดสอบกับระบบงานเพื่อป้องกันการรั่วไหลของข้อมูล เว้นแต่ได้รับการอนุมัติจากผู้บังคับบัญชาก่อน

๓๑.๕ ดูแล ติดตาม และควบคุมการปฏิบัติงานของผู้ให้บริการพัฒนาระบบสารสนเทศจากภายนอก (outsourced system development) ให้เป็นไปตามนโยบายของโรงพยาบาลกำหนด

๓๑.๖ ต้องทดสอบการทำงานของระบบที่ได้รับการพัฒนาโดยผู้ใช้งานหรือผู้ทดสอบอื่นที่เป็นอิสระจากผู้พัฒนาระบบสารสนเทศดังกล่าว เพื่อให้มั่นใจได้ว่าระบบที่ได้รับการพัฒนาดังกล่าวสามารถทำงาน

ได้ถูกต้องตรงความต้องการของผู้ใช้งาน และเป็นไปตามนโยบายของโรงพยาบาลกำหนด ทั้งนี้ควรระมัดระวังโดยจัดให้มีแนวทางควบคุมและป้องกันการรั่วไหลของข้อมูลที่ใช้ในการทดสอบหากข้อมูลดังกล่าวเป็นความลับหรือมีความสำคัญ

๓๑.๗ ต้องทดสอบระบบสารสนเทศที่ได้รับการพัฒนาหรือแก้ไขเปลี่ยนแปลงเพื่อให้มั่นใจว่าการทำงานมีประสิทธิภาพ การประมวลผลถูกต้องครบถ้วน และเป็นไปตามความต้องการของผู้ใช้งาน พร้อมทั้งปรับปรุงแผนบริหารความต่อเนื่องให้สอดคล้องกับการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบสารสนเทศดังกล่าว

๓๑.๘ ต้องควบคุมสภาพแวดล้อมของการพัฒนาระบบสารสนเทศ (development environment) ซึ่งได้แก่ บุคลากรผู้พัฒนาระบบ ขั้นตอนการพัฒนาระบบ และเทคโนโลยีสำหรับการพัฒนาระบบให้มีความมั่นคงปลอดภัยตลอดขั้นตอนการพัฒนาระบบโดยคำนึงถึงเรื่องดังนี้

(๑) การรักษาความลับของข้อมูลที่นำมาประมวลผล จัดเก็บ ส่งผ่านระบบการควบคุม การนำข้อมูลเข้าและออกจากระบบที่อยู่ระหว่างการพัฒนา

(๒) การควบคุมการเข้าถึงสภาพแวดล้อมของการพัฒนาระบบสารสนเทศอย่างรัดกุมเหมาะสม

(๓) การติดตามหากมีการเปลี่ยนแปลงสภาพแวดล้อมของการพัฒนาระบบสารสนเทศ

(๔) มีการจัดเก็บข้อมูลสำรองในพื้นที่นอกโรงพยาบาล ที่มีความมั่นคงปลอดภัย

๓๑.๙ ควบคุมการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบสารสนเทศตลอดทุกขั้นตอนตามการควบคุมที่ได้กำหนดไว้ โดยอย่างน้อยต้องมีในเรื่องดังต่อไปนี้

(๑) มีการประเมินผลกระทบที่อาจเกิดขึ้นจากการเปลี่ยนแปลง

(๒) กำหนดวิธีปฏิบัติให้คำขอที่จะให้มีการแก้ไขหรือพัฒนาต้องมาจากผู้ที่มีสิทธิและอนุมัติคำขอโดยผู้มีอำนาจ ต้องควบคุมผลข้างเคียงที่อาจเกิดขึ้นเนื่องจากมีการแก้ไข มีการตรวจรับจากผู้มีอำนาจภายหลังการแก้ไขหรือพัฒนาแล้วเสร็จก่อนโอนย้ายระบบงาน รวมทั้งมีการจัดเก็บรายละเอียดของคำขอไว้เป็นต้น

(๓) กำหนดวิธีปฏิบัติในกรณีที่มีการแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ในกรณีฉุกเฉิน และบันทึกเหตุผลความจำเป็นและขออนุมัติจากผู้มีอำนาจทุกครั้ง

(๔) ปรับปรุงเอกสารประกอบระบบงานทั้งหมดหลังจากที่ได้มีการแก้ไขเปลี่ยนแปลง เพื่อให้ทันสมัยอยู่เสมอ เช่น เอกสารประกอบรายละเอียดโครงสร้างข้อมูล คู่มือระบบงานทะเบียนรายชื่อผู้มีสิทธิใช้งาน ขั้นตอนการทำงานของโปรแกรม และต้องจัดเก็บเอกสารดังกล่าวในที่ปลอดภัยและสะดวกต่อการใช้งาน

(๕) จัดเก็บโปรแกรม version ก่อนการเปลี่ยนแปลงไว้ใช้งาน หรือมีกระบวนการถอยกลับ สู่สภาพเดิม (fail-back) ของระบบงานในกรณีระบบงานผิดพลาดหรือไม่สามารถใช้งานได้

(๖) มีการสื่อสารให้กับบุคคลที่เกี่ยวข้องได้รับทราบและสามารถปฏิบัติงานได้อย่างถูกต้อง

(๗) บันทึกและจัดเก็บหลักฐานทั้งหมด (audit tail) ที่เกี่ยวข้องกับการเปลี่ยนแปลงเพื่อใช้ประกอบในกรณีที่มีการตรวจสอบ

หมวด ๔
การบริหารจัดการความเสี่ยงและการตรวจสอบด้านเทคโนโลยีสารสนเทศ

ข้อ ๓๒ การบริหารจัดการความเสี่ยง ให้โรงพยาบาลปฏิบัติดังต่อไปนี้

๓๒.๑ กำหนดปัจจัยต่าง ๆ ที่เกี่ยวข้องกับการประเมินความเสี่ยง โดยอย่างน้อยต้องกำหนดในเรื่องดังต่อไปนี้

(๑) เป้าหมายการประเมินความเสี่ยง

(๒) กระบวนการ วัตถุประสงค์ และข้อกำหนดทางธุรกิจ

(๓) กฎ ระเบียบ ข้อกำหนดในสัญญา และข้อบังคับที่โรงพยาบาลต้องปฏิบัติ

(๔) ข้อกำหนดด้านความมั่นคงปลอดภัย

(๕) เทคโนโลยีสารสนเทศที่โรงพยาบาลใช้งาน

(๖) ผลกระทบที่เกิดขึ้นหากระบบสารสนเทศไม่สามารถใช้งานได้

(๗) โอกาสการเกิดขึ้นของเหตุการณ์ความเสี่ยง

๓๒.๒ กำหนดเกณฑ์การประเมินความเสี่ยง ได้แก่ วิธีการคิดโอกาสการเกิดขึ้นของเหตุการณ์ความเสี่ยง และวิธีการคิดผลกระทบของเหตุการณ์ความเสี่ยง

๓๒.๓ กำหนดระดับความเสี่ยงที่ยอมรับได้

๓๒.๔ วิเคราะห์และประเมินความเสี่ยงต่อสินทรัพย์สารสนเทศอย่างน้อยปีละหนึ่งครั้ง หรือทุกครั้งที่มีการเปลี่ยนแปลงสินทรัพย์ของระบบสารสนเทศสำคัญแล้วส่งผลกระทบสูงต่อผลการประเมินความเสี่ยงล่าสุด และบริหารจัดการความเสี่ยงเหล่านั้น ดังนี้

(๑) จัดทำแผนการลดความเสี่ยงโดยพิจารณาถึงลำดับความสำคัญในการดำเนินการ ค่าใช้จ่าย ความคุ้มค่า หรือประโยชน์ที่ได้รับ และผู้รับผิดชอบในการดำเนินการ

(๒) นำเสนอแผนการลดความเสี่ยงต่อผู้บังคับบัญชาเพื่อพิจารณาและให้ข้อคิดเห็นตามความจำเป็น

(๓) ผู้บังคับบัญชาสั่งการให้ดำเนินการตามแผนและรายงานผลการดำเนินการให้ได้รับทราบเป็นระยะ ๆ จนกระทั่งเสร็จสิ้น

ข้อ ๓๓ การตรวจสอบด้านเทคโนโลยีสารสนเทศ ให้โรงพยาบาลปฏิบัติดังต่อไปนี้

๓๓.๑ จัดให้มีการตรวจสอบด้านเทคโนโลยีสารสนเทศตามมาตรฐานสากลจากผู้ตรวจสอบภายใน หรือผู้ตรวจสอบอิสระภายนอกอย่างน้อยปีละหนึ่งครั้ง

๓๓.๒ จัดให้มีการตรวจสอบด้านเทคโนโลยีสารสนเทศด้วยวิธีทางเทคนิคอย่างน้อยปีละหนึ่งครั้ง
