**ประกาศโรงพยาบาลสมเด็จพระสังฆราช องค์ที่ ๑๗**
**เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์**

---

ปัจจุบันโรงพยาบาลสมเด็จพระสังฆราช องค์ที่ ๑๗ ได้นำระบบเทคโนโลยีสารสนเทศและเทคโนโลยีดิจิทัลมาใช้ในการให้บริการทางการแพทย์ การบริหารจัดการ และการดำเนินงานด้านต่าง ๆ อย่างต่อเนื่อง ซึ่งเกี่ยวข้องกับข้อมูลส่วนบุคคล ข้อมูลสุขภาพ ระบบสารสนเทศที่มีความสำคัญ และโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ อันจำเป็นต้องได้รับการดูแลรักษาให้มีความมั่นคงปลอดภัย เพื่อป้องกันการเข้าถึงโดยมิชอบ การรั่วไหลของข้อมูล การหยุดชะงักของระบบ และภัยคุกคามทางไซเบอร์ที่อาจส่งผลกระทบต่อการให้บริการทางการแพทย์และความเชื่อมั่นของประชาชน

อาศัยอำนาจตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ รวมถึงกฎหมาย ระเบียบ และประกาศที่เกี่ยวข้อง โรงพยาบาลสมเด็จพระสังฆราช องค์ที่ ๑๗ จึงออกประกาศฉบับนี้ เพื่อกำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ของโรงพยาบาล ดังต่อไปนี้

ข้อ ๑ ให้มีการตรวจสอบและประเมินความมั่นคงปลอดภัยไซเบอร์ รวมถึงการประเมินความเสี่ยงและการวิเคราะห์ผลกระทบทางธุรกิจ (BIA) อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ

ข้อ ๒ ให้มีการประเมินและทบทวนความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงระบบ เทคโนโลยี หรือสภาพแวดล้อมการดำเนินงานที่มีนัยสำคัญ เพื่อกำหนดมาตรการควบคุมและลดความเสี่ยงอย่างเหมาะสม

ข้อ ๓ ให้มีการจัดทำและทบทวนแผนการรับมือเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Incident Response Plan) อย่างน้อยปีละ ๑ ครั้ง รวมทั้งจัดให้มีการฝึกซ้อมแผนตามความเหมาะสม

ข้อ ๔ ให้กำหนดกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยครอบคลุมมาตรการหลัก ๕ ด้าน ดังนี้

(๑) การระบุและบริหารจัดการความเสี่ยง (Identify)

(๒) การป้องกัน (Protect)

(๓) การตรวจสอบและเฝ้าระวัง (Detect)

(๔) การตอบสนองและการเผชิญเหตุ (Respond)

(๕) การฟื้นฟูระบบและการรักษาความต่อเนื่องทางธุรกิจ (Recover)

ข้อ ๕...

ข้อ ๕ ให้กำหนดมาตรการและกระบวนการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ให้สอดคล้องกับกรอบมาตรฐานตามข้อ ๔ โดยครอบคลุมการเตรียมความพร้อม การตรวจพบและวิเคราะห์เหตุการณ์ การควบคุมและระงับเหตุ การฟื้นฟูระบบ และการทบทวนหลังเกิดเหตุ ทั้งนี้ หากเกิดเหตุการณ์ที่มีนัยสำคัญ ให้รายงานต่อหน่วยงานที่เกี่ยวข้องตามกฎหมายและระเบียบที่กำหนด

ข้อ ๖ ให้ส่งเสริมและสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์แก่บุคลากรทุกระดับรวมถึงผู้ที่เกี่ยวข้องอย่างต่อเนื่อง

ข้อ ๗ ให้หน่วยงานและผู้ที่เกี่ยวข้องนำแนวปฏิบัติและกรอบมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ตามเอกสารแนบท้ายประกาศนี้ไปใช้เป็นแนวทางในการปฏิบัติงาน

ข้อ ๘ ให้กลุ่มงานเทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับมอบหมาย เป็นผู้รับผิดชอบในการกำกับ ดูแลและดำเนินการตามประกาศฉบับนี้ รวมทั้งทบทวนและปรับปรุงให้เป็นปัจจุบันอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ

ข้อ ๙ นโยบายและแนวปฏิบัติตามประกาศฉบับนี้ให้ถือเป็นมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ของโรงพยาบาล และให้มีผลบังคับใช้กับบุคลากร ลูกจ้าง คู่สัญญา และผู้ให้บริการภายนอกที่เกี่ยวข้องกับระบบสารสนเทศของโรงพยาบาล หากฝ่าฝืนหรือไม่ปฏิบัติตามจนก่อให้เกิดความเสียหาย ให้ดำเนินการตามระเบียบทางวินัย กฎหมายที่เกี่ยวข้อง หรือเงื่อนไขในสัญญา แล้วแต่กรณี

ทั้งนี้ ให้มีผลบังคับใช้ตั้งแต่วันประกาศเป็นต้นไป

ประกาศ ณ วันที่ ๒๗ กุมภาพันธ์ พ.ศ. ๒๕๖๙

(นายจิรภัทร กัลยาณพจน์พร)
ผู้อำนวยการโรงพยาบาลสมเด็จพระสังฆราช องค์ที่ ๑๗

**เอกสารแนบท้ายประกาศ**
**แนวปฏิบัติและกรอบมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์**
**โรงพยาบาลสมเด็จพระสังฆราช องค์ที่ ๑๗**

# แนวปฏิบัติและกรอบมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ โรงพยาบาลสมเด็จพระสังฆราช องค์ที่ ๑๗

## ฉบับปี พ.ศ. ๒๕๖๙

**จัดทำโดย**

กลุ่มงานเทคโนโลยีสารสนเทศ

โรงพยาบาลสมเด็จพระสังฆราช องค์ที่ ๑๗

# สารบัญ

หน้า

# แนวปฏิบัติและกรอบมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์
# โรงพยาบาลสมเด็จพระสังฆราช องค์ที่ ๑๗

---

## ๑. บทนำ

โดยที่พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดให้หน่วยงานของรัฐจัดให้มีแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เป็นข้อกำหนดขั้นต่ำ เพื่อใช้เป็นกรอบการดำเนินงานในการบริหารจัดการความเสี่ยง การป้องกัน การตรวจพบ การตอบสนอง และการรับมือกับภัยคุกคามทางไซเบอร์ ตลอดจนเหตุการณ์ที่อาจส่งผลกระทบอย่างมีนัยสำคัญต่อระบบสารสนเทศ ข้อมูล และการดำเนินงานของหน่วยงาน ทั้งนี้ เพื่อให้การดำเนินการดังกล่าวเป็นไปอย่างมีระบบ มีประสิทธิภาพ และสอดคล้องกับกฎหมาย ระเบียบ และมาตรฐานที่เกี่ยวข้อง

โรงพยาบาลสมเด็จพระสังฆราช องค์ที่ ๑๗ ในฐานะหน่วยงานผู้ให้บริการด้านการแพทย์และสาธารณสุข มีการประยุกต์ใช้ระบบสารสนเทศ ระบบเครือข่าย และข้อมูลสุขภาพของผู้รับบริการในการดำเนินภารกิจอย่างต่อเนื่อง ความมั่นคงปลอดภัยของระบบและข้อมูลดังกล่าวจึงมีความสำคัญยิ่งต่อความถูกต้องครบถ้วนของข้อมูล ความต่อเนื่องในการให้บริการ และความเชื่อมั่นของผู้รับบริการ ซึ่งถือเป็นปัจจัยหลักในการสนับสนุนภารกิจของโรงพยาบาลให้ดำเนินไปได้อย่างมั่นคงและมีประสิทธิภาพ

เพื่อให้การดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ของโรงพยาบาลเป็นไปอย่างเหมาะสม โรงพยาบาลสมเด็จพระสังฆราช องค์ที่ ๑๗ จึงจัดทำเอกสารแนวทางปฏิบัติและกรอบมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ฉบับนี้ขึ้น เพื่อใช้เป็นกรอบแนวทางในการกำกับดูแลและดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ให้เป็นไปอย่างมีระบบ สอดคล้องกับกฎหมายและมาตรฐานที่เกี่ยวข้อง ตลอดจนเสริมสร้างขีดความสามารถในการป้องกันและรับมือกับภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ

## ๒. วัตถุประสงค์

๒.๑ เพื่อกำหนดแนวทางและมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ของโรงพยาบาลให้สอดคล้องกับกฎหมายและมาตรฐานที่เกี่ยวข้อง

๒.๒ เพื่อจัดให้มีระบบบริหารจัดการความเสี่ยง การป้องกัน และการตอบสนองต่อภัยคุกคามทางไซเบอร์ที่มีประสิทธิภาพ

๒.๓ เพื่อรักษาความลับ ความถูกต้องครบถ้วน และความพร้อมใช้งานของข้อมูลสุขภาพและระบบสารสนเทศที่สำคัญ

๒.๔ เพื่อลดผลกระทบจากภัยคุกคามและสร้างความต่อเนื่องในการให้บริการทางการแพทย์และสาธารณสุข

๒.๕ เพื่อสร้างความเชื่อมั่นแก่ผู้รับบริการและผู้มีส่วนได้ส่วนเสียต่อมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ของโรงพยาบาล

**๓. ขอบเขตการบังคับใช้**

๓.๑ ด้านบุคลากร

ให้ใช้บังคับแก่ข้าราชการ พนักงานเจ้าหน้าที่ ลูกจ้าง พนักงานจ้างเหมาบริการ นิสิต นักศึกษาฝึกงาน รวมถึงคู่สัญญา ผู้ให้บริการ หรือบุคคลภายนอกที่ได้รับอนุญาตให้เข้าถึงระบบสารสนเทศหรือข้อมูลของโรงพยาบาล ไม่ว่าทางตรงหรือทางอ้อม

๓.๒ ด้านโครงสร้างพื้นฐานสารสนเทศ

ให้ครอบคลุมระบบคอมพิวเตอร์ ระบบเครือข่ายสื่อสาร อุปกรณ์จัดเก็บข้อมูล ระบบสารสนเทศ อุปกรณ์พกพา และโครงสร้างพื้นฐานสารสนเทศทั้งหมดที่เป็นกรรมสิทธิ์ อยู่ในความดูแล หรือได้รับอนุญาตให้ใช้งานภายใต้ความรับผิดชอบของโรงพยาบาล

๓.๓ ด้านข้อมูล

ให้ครอบคลุมข้อมูลสุขภาพ ข้อมูลส่วนบุคคล ข้อมูลชั้นความลับ และข้อมูลสารสนเทศหรือข้อมูลอิเล็กทรอนิกส์ทุกประเภทที่เกี่ยวข้องกับภารกิจ การให้บริการ และการดำเนินงานของโรงพยาบาล

๓.๔ ด้านสถานที่และรูปแบบการเข้าถึงระบบ

ให้ครอบคลุมการปฏิบัติงานและการเข้าถึงระบบสารสนเทศทั้งภายในพื้นที่ของโรงพยาบาลและการเชื่อมต่อจากภายนอกพื้นที่ (Remote Access) ผ่านเครือข่ายหรือช่องทางใด ๆ ตามที่โรงพยาบาลกำหนด

**๔. คำนิยาม**

เพื่อให้การตีความและการปฏิบัติตามนโยบาย แนวปฏิบัติ และกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของโรงพยาบาลสมเด็จพระสังฆราช องค์ที่ ๑๗ เป็นไปในทิศทางเดียวกัน ให้คำศัพท์และถ้อยคำในเอกสารฉบับนี้มีความหมาย ดังต่อไปนี้

๔.๑ โครงสร้างองค์กรและบทบาทหน้าที่

**"โรงพยาบาล"** หมายถึง โรงพยาบาลสมเด็จพระสังฆราช องค์ที่ ๑๗

**"หน่วยงาน"** หมายถึง กลุ่มงาน ฝ่าย งาน ศูนย์ หรือหน่วยงานภายในโรงพยาบาล รวมถึงหน่วยงานหรือองค์กรภายนอกที่โรงพยาบาลมอบหมายหรือทำสัญญาให้ดำเนินงานด้านระบบสารสนเทศ

**"ผู้บริหาร"** หมายถึง ผู้มีอำนาจในการบังคับบัญชาและกำกับดูแลการปฏิบัติงานในหน่วยงาน เช่น ผู้อำนวยการ รองผู้อำนวยการ หรือหัวหน้ากลุ่มงาน

**"ผู้บริหารระดับสูงสุด"** หมายถึง ผู้อำนวยการโรงพยาบาล ซึ่งเป็นผู้รับผิดชอบสูงสุดด้านการกำกับดูแล กำหนดนโยบาย และตัดสินใจในเรื่องความมั่นคงปลอดภัยไซเบอร์ของโรงพยาบาล

**"ผู้บริหารเทคโนโลยีสารสนเทศ" (Chief Information Officer: CIO)** หมายถึง ผู้ที่ผู้อำนวยการโรงพยาบาลมอบหมายให้รับผิดชอบกำกับ ดูแล วางแผน และบริหารจัดการด้านเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยไซเบอร์ของโรงพยาบาล

**"เจ้าของระบบ" (System Owner)** หมายถึง หน่วยงานหรือกลุ่มงานภายในโรงพยาบาลที่รับผิดชอบหลักในการพัฒนา ใช้งาน และดูแลรักษาระบบคอมพิวเตอร์หรือระบบสารสนเทศ รวมถึงการกำหนดและอนุมัติสิทธิการเข้าถึงระบบของผู้ใช้งาน

**"ผู้ดูแลระบบ" (System Administrator)** หมายถึง บุคลากรที่ได้รับมอบหมายจากผู้บริหารหรือเจ้าของระบบ ให้มีหน้าที่ดูแล บริหารจัดการระบบคอมพิวเตอร์ ระบบสารสนเทศ และระบบเครือข่าย รวมถึงการกำหนด ตรวจสอบ ทบทวน และควบคุมสิทธิการเข้าถึงระบบ

**"ผู้ใช้งาน" (User)** หมายถึง ข้าราชการ พนักงาน ลูกจ้าง พนักงานจ้างเหมาบริการ นักศึกษา ผู้ฝึกงาน รวมถึงบุคคลภายนอกที่ได้รับอนุญาตให้เข้าถึงหรือใช้งานระบบสารสนเทศของโรงพยาบาล

**"สิทธิของผู้ใช้งาน"** หมายถึง สิทธิในการเข้าถึง ใช้งาน หรือจัดการทรัพยากรสารสนเทศตามบทบาทหน้าที่ (Role-based Access Control: RBAC) ที่โรงพยาบาลกำหนด

๔.๒ สินทรัพย์ ระบบ และข้อมูล

**"สินทรัพย์สารสนเทศและเทคโนโลยีสารสนเทศ" (Information and IT Asset)** หมายถึง ฮาร์ดแวร์ ซอฟต์แวร์ ระบบเครือข่าย ระบบคอมพิวเตอร์ ระบบสารสนเทศ และข้อมูลสารสนเทศที่มีคุณค่าและต้องได้รับการคุ้มครองด้านความมั่นคงปลอดภัยไซเบอร์

**"ระบบคอมพิวเตอร์"** หมายถึง ระบบประมวลผลข้อมูลทั้งแบบภายในองค์กร (On-premise) ระบบเสมือน (Virtualization System) ระบบคลาวด์ (Cloud Computing) หรือแบบผสมผสาน (Hybrid) รวมถึงระบบปฏิบัติการและเครื่องคอมพิวเตอร์ที่เชื่อมต่อและใช้งานร่วมกับโปรแกรมประยุกต์

**"ระบบสารสนเทศ"** หมายถึง ระบบงานด้านการแพทย์และการบริหารของโรงพยาบาล เช่น ระบบสารสนเทศโรงพยาบาล (HIS) ระบบห้องปฏิบัติการ (LIS) ระบบรังสีวิทยา (RIS) ระบบเวชระเบียนอิเล็กทรอนิกส์ เว็บไซต์ ระบบอีเมล และระบบอิเล็กทรอนิกส์อื่นที่ใช้ในการดำเนินงาน

**"ข้อมูลสารสนเทศ"** หมายถึง ข้อมูลหรือสารสนเทศในรูปแบบดิจิทัล เช่น ข้อมูลสุขภาพ ข้อมูลส่วนบุคคล ฐานข้อมูล เอกสารอิเล็กทรอนิกส์ และไฟล์ข้อมูลที่จัดเก็บ ประมวลผล หรือถ่ายโอนผ่านระบบสารสนเทศของโรงพยาบาล

**"ระบบหรือบริการที่มีความสำคัญ" (Critical System/Service)** หมายถึง ระบบสารสนเทศหรือบริการที่หากเกิดการหยุดชะงักจะส่งผลกระทบต่อการให้บริการทางการแพทย์ ความปลอดภัยของผู้ป่วย หรือการดำเนินงานหลักของโรงพยาบาล

**"พื้นที่ปฏิบัติงาน"** หมายถึง พื้นที่ภายในโรงพยาบาลหรือสถานที่อื่นที่โรงพยาบาลอนุญาตให้ปฏิบัติงานและเชื่อมต่อเข้าสู่ระบบสารสนเทศของโรงพยาบาล

**"ห้องศูนย์ข้อมูล" (Data Center)** หมายถึง พื้นที่เฉพาะที่ใช้ติดตั้งอุปกรณ์ประมวลผลข้อมูล ระบบเครือข่าย ระบบจัดเก็บข้อมูล และมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งมีการควบคุมและเฝ้าระวังตลอด ๒๔ ชั่วโมง

**"การควบคุมการเข้าถึง" (Access Control)** หมายถึง การกำหนด อนุญาต และควบคุมสิทธิการเข้าถึงระบบสารสนเทศ ข้อมูล และทรัพยากรสารสนเทศของผู้ใช้งาน ตามนโยบายด้านความมั่นคงปลอดภัยไซเบอร์ของโรงพยาบาล

๔.๓ ความมั่นคงปลอดภัยไซเบอร์และเหตุการณ์ที่เกี่ยวข้อง

**"ความมั่นคงปลอดภัยไซเบอร์" (Cybersecurity)** หมายถึง การปกป้องระบบคอมพิวเตอร์ ระบบสารสนเทศ และข้อมูลสารสนเทศจากภัยคุกคามทางไซเบอร์ ครอบคลุมการป้องกัน การตรวจจับ การตอบสนอง และการฟื้นฟู เพื่อรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้งาน (Availability)

**"ภัยคุกคามทางไซเบอร์" (Cyber Threat)** หมายถึง ปัจจัย เหตุการณ์ หรือการกระทำที่มีศักยภาพจะก่อให้เกิดการละเมิดความมั่นคงปลอดภัยไซเบอร์ของระบบคอมพิวเตอร์ ระบบสารสนเทศ หรือข้อมูลสารสนเทศของโรงพยาบาล แต่ยังไม่จำเป็นต้องก่อให้เกิดความเสียหายจริง

**"เหตุการณ์" (Event)** หมายถึง การเกิดขึ้นของเหตุการณ์หรือสภาพการณ์ใด ๆ ที่สามารถสังเกตได้ในระบบคอมพิวเตอร์ ระบบเครือข่าย กระบวนการดำเนินงาน หรือบุคลากร ซึ่งอาจเกี่ยวข้องหรือไม่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ และอาจยังไม่ก่อให้เกิดผลกระทบ

**"เหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์" (Cybersecurity Event)** หมายถึง เหตุการณ์ที่บ่งชี้ถึงความเป็นไปได้ของการละเมิดนโยบาย มาตรการ หรือการควบคุมด้านความมั่นคงปลอดภัยไซเบอร์ แต่ยังไม่ปรากฏผลกระทบหรือความเสียหายอย่างชัดเจน

**"เหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์" (Cybersecurity Incident)** หมายถึง เหตุการณ์ที่เกิดจากภัยคุกคามทางไซเบอร์ หรือการกระทำโดยมิชอบ ซึ่งก่อให้เกิด หรือมีแนวโน้มใกล้จะก่อให้เกิดความเสียหายหรือผลกระทบต่อระบบคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลสารสนเทศ หรือการดำเนินงานของโรงพยาบาล

## ๕. แนวปฏิบัติและกรอบมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์

โรงพยาบาลสมเด็จพระสังฆราช องค์ที่ ๑๗ มี ๒ ส่วน ดังนี้

ส่วนที่ ๑ แนวปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์

ส่วนที่ ๒ กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

## ส่วนที่ ๑ แนวปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์

เอกสารฉบับนี้จัดทำขึ้นเพื่อกำหนดแนวปฏิบัติในการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของโรงพยาบาล ให้เป็นไปตามนโยบายที่โรงพยาบาลประกาศใช้ โดยมุ่งเน้นการนำไปปฏิบัติได้จริง ครอบคลุมการตรวจสอบ การบริหารความเสี่ยง การรับมือเหตุการณ์ และการรายงานผล เพื่อให้การดำเนินงานด้านระบบสารสนเทศและเทคโนโลยีดิจิทัลของโรงพยาบาลมีความมั่นคงปลอดภัยและต่อเนื่อง

### แนวปฏิบัติ

**หัวข้อที่ ๑ แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Audit Plan)**

โรงพยาบาลต้องจัดให้มีการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ ซึ่งอาจเป็นผู้ตรวจสอบภายใน หรือผู้ตรวจสอบอิสระจากภายนอก ตามความเหมาะสม อย่างน้อยปีละ ๑ ครั้ง เพื่อให้การดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์เป็นไปตามนโยบายและกรอบมาตรฐานที่กำหนด โดยมีขอบเขตการตรวจสอบ ดังนี้

**๑.๑ การตรวจสอบนโยบายและเอกสารด้านความมั่นคงปลอดภัยไซเบอร์ (Policy and Documentation Review)**

ตรวจสอบการจัดทำนโยบาย แนวปฏิบัติ แผนงาน และเอกสารที่เกี่ยวข้องด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของโรงพยาบาล เพื่อให้มีความครบถ้วน เหมาะสม ทันสมัย และสอดคล้องกับสภาพแวดล้อมด้านเทคโนโลยี ระบบสารสนเทศ และระดับความเสี่ยงในปัจจุบัน รวมถึงครอบคลุมแผนการรับมือเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์

**๑.๒ การตรวจสอบการปฏิบัติตามนโยบายและกรอบมาตรฐาน (Compliance and Implementation Assessment)**

ตรวจสอบการดำเนินงานตามนโยบาย แนวปฏิบัติ และกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่โรงพยาบาลประกาศใช้ รวมถึงการปฏิบัติตามกฎหมาย ระเบียบ และประกาศที่เกี่ยวข้องด้านความมั่นคงปลอดภัยไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคล เพื่อประเมินระดับความสอดคล้องและประสิทธิผลของการควบคุมที่นำไปใช้จริง

**๑.๓ การจัดทำและรายงานผลการตรวจสอบ (Audit Reporting and Follow-up)**

จัดทำรายงานผลการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยสรุปขอบเขตการตรวจสอบ ผลการตรวจสอบ ประเด็นที่ตรวจพบ ความเสี่ยงที่เกี่ยวข้อง และข้อเสนอแนะในการปรับปรุงแก้ไข พร้อมทั้งจัดส่งรายงานผลการตรวจสอบต่อผู้บริหารและหน่วยงานที่เกี่ยวข้อง รวมถึงหน่วยงานกำกับดูแล (หากมี) ภายในระยะเวลาที่กำหนด และติดตามผลการแก้ไขปรับปรุงตามข้อเสนอแนะอย่างเหมาะสม

**หัวข้อที่ ๒ การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Assessment)**

โรงพยาบาลต้องจัดให้มีการประเมินและบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างเป็นระบบ โดยกำหนดนโยบาย ระเบียบวิธีปฏิบัติ และกระบวนการบริหารความเสี่ยงให้ครอบคลุมโครงสร้างองค์กร บทบาทหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้อง

ทั้งนี้ ต้องดำเนินการประเมินความเสี่ยงอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงระบบสารสนเทศ เทคโนโลยี หรือสภาพแวดล้อมที่มีนัยสำคัญ โดยมีแนวทางการดำเนินการ ดังต่อไปนี้

**๒.๑ การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Assessment Process)**

ให้ดำเนินการระบุ วิเคราะห์ และประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่อาจเกิดขึ้นกับระบบสารสนเทศ ข้อมูล และการให้บริการของโรงพยาบาล โดยครอบคลุมขั้นตอน ดังนี้

๒.๑.๑ การระบุความเสี่ยง (Risk Identification)

ดำเนินการระบุความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งรวมถึงความเสี่ยงจากภัยคุกคามทางไซเบอร์ ช่องโหว่ด้านเทคนิค และปัจจัยอื่นที่เกี่ยวข้อง โดยพิจารณาจากกระบวนการปฏิบัติงาน ระบบสารสนเทศ บุคลากร และปัจจัยภายนอก โดยการระบุความเสี่ยงควรครอบคลุมอย่างน้อยประเด็นต่อไปนี้

(ก) ผู้ก่อให้เกิดความเสี่ยงหรือเหตุการณ์ความเสี่ยง

(ข) ประเภทของความเสี่ยง เช่น ความเสี่ยงด้านระบบสารสนเทศ ข้อมูล บุคลากร อุปกรณ์เทคโนโลยีสารสนเทศ หรือการบริหารจัดการ

(ค) สาเหตุของการเกิดเหตุการณ์ความเสี่ยง

(ง) ผลกระทบที่อาจเกิดขึ้นต่อทรัพย์สิน ข้อมูล การดำเนินงาน และการให้บริการของโรงพยาบาล

๒.๑.๒ การวิเคราะห์ความเสี่ยง (Risk Analysis)

ให้ดำเนินการวิเคราะห์ความเสี่ยง โดยมีรายละเอียดอย่างน้อย ดังนี้

(ก) กำหนดเจ้าของความเสี่ยง (Risk Owner)

(ข) ระบุการควบคุมที่มีอยู่ในปัจจุบัน (Existing Controls)

(ค) พิจารณาสาเหตุและสถานการณ์ที่อาจนำไปสู่การเกิดเหตุการณ์ความเสี่ยง

(ง) วิเคราะห์ผลกระทบที่อาจเกิดขึ้นจากเหตุการณ์ความเสี่ยง

๒.๑.๓ การประเมินค่าความเสี่ยง (Risk Evaluation)

ประเมินโอกาสและผลกระทบของความเสี่ยง เพื่อกำหนดระดับความเสี่ยง และพิจารณาระดับความเสี่ยงที่โรงพยาบาลสามารถยอมรับได้ (Risk Appetite) โดยมีรายละเอียดอย่างน้อย ดังนี้

(ก) กำหนดเกณฑ์การประเมินด้านโอกาสและผลกระทบ เช่น ด้านการปฏิบัติการ ด้านกฎหมาย ด้านการเงิน และด้านความปลอดภัยของผู้ป่วย

(ข) ประเมินค่าโอกาสและผลกระทบของแต่ละเหตุการณ์ความเสี่ยง

(ค) จัดลำดับระดับความเสี่ยงเพื่อใช้ในการกำหนดแนวทางจัดการความเสี่ยง

**๒.๒ การจัดการและควบคุมความเสี่ยง (Cybersecurity Risk Treatment and Control)**

โรงพยาบาลต้องจัดทำแผนการบริหารจัดการความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยกำหนดมาตรการจัดการความเสี่ยงที่เหมาะสมตามระดับความเสี่ยง เช่น

- การลดหรือบรรเทาความเสี่ยง (Risk Mitigation)
- การโอนหรือแบ่งปันความเสี่ยง (Risk Transfer or Sharing)
- การยอมรับความเสี่ยง (Risk Acceptance)

ทั้งนี้ ต้องดำเนินการปรับปรุงแก้ไขหรือกำหนดมาตรการเพิ่มเติมตามความจำเป็น เพื่อให้ความเสี่ยงที่เหลืออยู่ในระดับที่โรงพยาบาลสามารถยอมรับได้

**๒.๓ การรายงานและทบทวนความเสี่ยง (Risk Reporting and Review)**

ให้มีการรายงานผลการประเมินและการบริหารจัดการความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ต่อผู้บริหารหรือหน่วยงานที่เกี่ยวข้อง เพื่อใช้ประกอบการกำกับ ดูแล และการตัดสินใจ รวมทั้งให้มีการทบทวนกระบวนการบริหารความเสี่ยงอย่างสม่ำเสมอ หรือเมื่อเกิดเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่มีนัยสำคัญ

**หัวข้อที่ ๓ แผนการรับมือภัยคุกคามทางไซเบอร์ (Cyber Incident Response Plan)**

โรงพยาบาลต้องจัดให้มีแผนการรับมือเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อใช้เป็นกรอบและแนวทางในการปฏิบัติเมื่อเกิดเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ และเพื่อให้สามารถตรวจจับ ควบคุม ระงับ แก้ไข และลดผลกระทบต่อระบบสารสนเทศ ข้อมูล และการให้บริการทางการแพทย์ของโรงพยาบาลได้อย่างเหมาะสมและต่อเนื่อง โดยมีแนวทางการดำเนินการ ดังต่อไปนี้

**๓.๑ โครงสร้างและกระบวนการของแผนการรับมือเหตุการณ์ (Incident Response Structure and Process)**

จัดทำแผนการรับมือเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ ครอบคลุมขั้นตอนสำคัญ ได้แก่

(ก) การแจ้งและรับแจ้งเหตุการณ์ (Incident Reporting)

(ข) การประเมินและวิเคราะห์สถานการณ์ (Incident Assessment and Analysis)

(ค) การควบคุมและระงับเหตุการณ์ (Containment)

(ง) การแก้ไขและฟื้นฟูระบบสารสนเทศและบริการ (Eradication and Recovery)

(จ) การรายงานผล การสรุปบทเรียน และการปรับปรุงมาตรการหลังเกิดเหตุ (Post-Incident Review and Improvement)

**๓.๒ การสื่อสารและการสร้างความเข้าใจเกี่ยวกับแผน (Communication and Awareness)**

จัดให้มีการสื่อสาร เผยแพร่ และสร้างความเข้าใจเกี่ยวกับแผนการรับมือเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์แก่ผู้บริหาร หน่วยงานที่เกี่ยวข้อง และบุคลากรที่มีบทบาทหน้าที่ตามแผน เพื่อให้สามารถปฏิบัติได้อย่างถูกต้อง สอดคล้อง และทันเวลาเมื่อเกิดเหตุการณ์

**๓.๓ การทบทวนและปรับปรุงแผน (Plan Review and Maintenance)**

ตรวจสอบและทบทวนแผนการรับมือเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญต่อระบบสารสนเทศ โครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ หรือบริการที่มีความสำคัญของโรงพยาบาล

**๓.๔ การฝึกซ้อมและการทดสอบแผน (Incident Response Exercise and Testing)**

โรงพยาบาลต้องจัดให้มีการฝึกซ้อมแผนการรับมือเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ ๑ ครั้ง เพื่อทดสอบความพร้อมของบุคลากร กระบวนการทำงาน และการประสานงานระหว่างหน่วยงานที่เกี่ยวข้อง และนำผลการฝึกซ้อมไปใช้ในการปรับปรุงแผนและมาตรการให้มีประสิทธิภาพยิ่งขึ้น

**หัวข้อที่ ๔ การรายงานสถานการณ์ด้านความมั่นคงปลอดภัยไซเบอร์**
**(Cybersecurity Situation Reporting)**

โรงพยาบาลต้องจัดให้มีการรายงานสถานการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ต่อผู้บริหารหรือคณะกรรมการที่เกี่ยวข้อง เพื่อใช้ประกอบการกำกับ ดูแล และการตัดสินใจด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยให้มีการรายงานอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อเกิดเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่มีนัยสำคัญ (Significant Cybersecurity Incident)

รายงานสถานการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ต้องครอบคลุมสาระสำคัญ ดังต่อไปนี้

**๔.๑ สถานะการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Program Status)**
ให้รายงานเกี่ยวกับสถานะการดำเนินงานตามนโยบาย แนวปฏิบัติ และกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของโรงพยาบาล

**๔.๒ เหตุการณ์ภัยคุกคามทางไซเบอร์ (Cybersecurity Incidents and Responses)**
ให้รายงานเกี่ยวกับเหตุการณ์ภัยคุกคามทางไซเบอร์ที่ตรวจพบ รวมถึงผลการดำเนินการในการควบคุม ระงับ แก้ไข และฟื้นฟูผลกระทบจากเหตุการณ์ดังกล่าว

**๔.๓ การดำเนินการด้านกฎหมายและข้อกำหนดที่เกี่ยวข้อง (Legal and Regulatory Actions)**
ให้รายงานเกี่ยวกับการดำเนินการด้านกฎหมาย ระเบียบ หรือข้อกำหนดที่เกี่ยวข้องในการตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ ในกรณีที่มีความจำเป็นหรือมีนัยสำคัญ

**๔.๔ การพัฒนาศักยภาพบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness and Capability Development)**
ให้รายงานเกี่ยวกับการส่งเสริมและพัฒนาความรู้ ความเข้าใจ และทักษะของบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์

**๔.๕ ปัญหา อุปสรรค และข้อเสนอแนะ (Issues, Challenges, and Recommendations)**
ให้รายงานเกี่ยวกับปัญหา อุปสรรค และข้อเสนอแนะในการปรับปรุงการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของโรงพยาบาล

**๔.๖ ประเภทเหตุการณ์และระยะเวลาในการรายงานเหตุการณ์**
**(Cybersecurity Incident Classification and Reporting Timeline)**

โรงพยาบาลต้องกำหนดประเภทของเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์และกรอบระยะเวลาในการรายงาน เพื่อให้สามารถควบคุม ระงับ และลดผลกระทบต่อการให้บริการทางการแพทย์ได้อย่างเหมาะสม โดยให้ดำเนินการ ดังนี้

๔.๖.๑ เหตุการณ์ที่มีผลกระทบต่อการให้บริการ หรือมีความรุนแรงสูง (High-Impact or Severe Incidents)
ให้รายงานต่อผู้บริหารหรือผู้รับผิดชอบด้านเทคโนโลยีสารสนเทศของโรงพยาบาลโดยเร็วที่สุดภายหลังตรวจพบเหตุการณ์ และจัดทำรายงานสรุปเหตุการณ์ภายใน ๒๔ ชั่วโมง

๔.๖.๒ เหตุการณ์ที่เกี่ยวข้องกับข้อมูลส่วนบุคคลของผู้ป่วยหรือบุคลากร (Personal Data or Patient Data Incidents)
ให้ดำเนินการประเมินขอบเขตและผลกระทบของเหตุการณ์ รายงานต่อผู้บริหารโรงพยาบาลและดำเนินการตามกฎหมายและระเบียบที่เกี่ยวข้องภายในระยะเวลาที่กฎหมายกำหนด

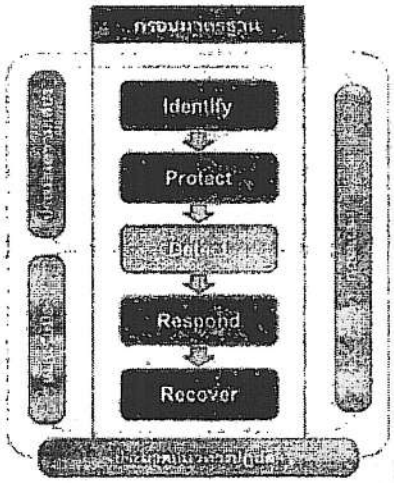
๔.๖.๓ เหตุการณ์ทั่วไปที่ไม่ส่งผลกระทบรุนแรงต่อการให้บริการ (General or Low-Impact Incidents)
ให้บันทึกเหตุการณ์และรายงานสรุปในการประชุมหรือรายงานสถานการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ตามรอบระยะเวลาที่กำหนด

๔.๖.๔ เหตุการณ์ระดับรุนแรงมากหรือระดับวิกฤต (Critical Cybersecurity Incident)
ให้รายงานต่อผู้บริหารด้านเทคโนโลยีสารสนเทศ (Chief Information Officer: CIO) หรือผู้ที่ได้รับมอบหมายโดยทันทีที่ตรวจพบ และรายงานต่อหน่วยงานกำกับดูแลที่เกี่ยวข้องภายใน ๒๔ ชั่วโมง

๔.๖.๕ เหตุการณ์ที่เข้าข่ายการละเมิดข้อมูลส่วนบุคคล (Personal Data Breach)
ในกรณีที่พบว่ามีการรั่วไหลของข้อมูลส่วนบุคคลหรือข้อมูลสุขภาพของผู้ป่วย ให้ดำเนินการประเมินความเสี่ยงและแจ้งเหตุไปยังสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลภายใน ๗๒ ชั่วโมง นับแต่วันที่ทราบเหตุ

## ส่วนที่ ๒ กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน จัดทำขึ้นโดยอ้างอิงแนวคิดตามมาตรฐานสากลด้านความมั่นคงปลอดภัยไซเบอร์ ครอบคลุมกระบวนการ การระบุความเสี่ยง การป้องกัน การตรวจจับ การเผชิญเหตุ และการฟื้นฟู เพื่อให้การดำเนินงานด้านเทคโนโลยีสารสนเทศและสารสนเทศของหน่วยงานมีความมั่นคงปลอดภัย มีความต่อเนื่อง และสอดคล้องกับกฎหมาย ระเบียบ และนโยบายที่เกี่ยวข้อง




รูปภาพที่ ๑ กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ๕ หัวข้อหลัก

### หัวข้อที่ ๑ การระบุความเสี่ยง (Identify)

โรงพยาบาลสมเด็จพระสังฆราช องค์ที่ ๑๗ ดำเนินการระบุและประเมินความเสี่ยงที่อาจเกิดขึ้นต่อคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบสารสนเทศ โครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ รวมถึงผลกระทบต่อการให้บริการทางการแพทย์ ทรัพย์สิน และความปลอดภัยของผู้ป่วยและบุคลากร เพื่อให้การบริหารจัดการความมั่นคงปลอดภัยไซเบอร์เป็นไปอย่างมีประสิทธิภาพและเหมาะสมกับบริบทของโรงพยาบาล

ทั้งนี้ โรงพยาบาลได้กำหนดแผนการรับมือเหตุภัยคุกคามทางไซเบอร์ โดยครอบคลุมโครงสร้างองค์กร บทบาทหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้อง พร้อมจัดให้มีกระบวนการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยดำเนินการประเมินความเสี่ยงอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงระบบที่สำคัญ ซึ่งประกอบด้วยกระบวนการหลัก ดังต่อไปนี้

#### ๑.๑ การจัดการทรัพย์สิน (Asset Management)

๑.๑.๑ หน่วยงานต้องจัดทำและดูแลทะเบียนทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT Asset Inventory) ครอบคลุมฮาร์ดแวร์และซอฟต์แวร์ที่ใช้ในการให้บริการและการบริหารจัดการระบบสารสนเทศ โดยปรับปรุงให้เป็นปัจจุบัน และมีข้อมูลอย่างน้อย ดังนี้

(ก) ชื่อ/คำอธิบายของทรัพย์สิน

(ข) ประเภทของทรัพย์สิน

(ค) หน้าที่หรือฟังก์ชันสำคัญของทรัพย์สิน

(ง) ระบุและการจัดลำดับความสำคัญของทรัพย์สิน

(จ) เจ้าของและ/หรือผู้ดำเนินการของทรัพย์สิน

(ฉ) ตำแหน่งทางกายภาพของทรัพย์สิน

(ช) การขึ้นต่อกันของทรัพย์สิน

๑.๑.๒ หน่วยงานต้องระบุขอบเขตเครือข่ายของบริการที่สำคัญของโรงพยาบาลและระบบที่มีการเชื่อมต่อโดยตรงหรือมีความสำคัญต่อการให้บริการ (Direct and Significant Interface)

๑.๑.๓ หน่วยงานต้องตรวจสอบทะเบียนทรัพย์สินอย่างน้อยปีละ ๑ ครั้ง หากมีการเปลี่ยนแปลงใด ๆ ที่เกี่ยวข้องกับทรัพย์สินให้ปรับปรุงทะเบียนทรัพย์สินดังกล่าวด้วย

๑.๑.๔ หน่วยงานต้องดำเนินการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญรวมถึงรายการทั้งหมดที่ระบุไว้ในทะเบียนทรัพย์ในข้อ ๑.๑.๑ อย่างน้อยปีละ ๑ ครั้ง

๑.๑.๕ หน่วยงานต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ของระบบสารสนเทศที่สำคัญและปรับปรุงให้เป็นปัจจุบันสอดคล้องกับสภาพการใช้งานจริง

**๑.๒ การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง**
**(Risk Assessment and Risk Management Strategy)**

๑.๒.๑ หน่วยงานต้องดำเนินการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงโครงสร้างพื้นฐาน ระบบสารสนเทศ หรือเทคโนโลยีที่มีผลกระทบต่อบริการที่สำคัญ

๑.๒.๒ ภายหลังการประเมินความเสี่ยง หน่วยงานต้องจัดทำและปรับปรุงทะเบียนความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ โดยมีข้อมูลอย่างน้อย ดังนี้

(ก) วันที่ระบุความเสี่ยง (Date the Risk is Identified)

(ข) คำอธิบายของความเสี่ยง (Description of the Risk)

(ค) โอกาสที่จะเกิดขึ้น (Likelihood of Occurrence)

(ง) ความรุนแรงของเหตุการณ์ (Severity of the Occurrence)

(จ) การจัดการความเสี่ยง (Risk Treatment)

(ฉ) เจ้าของความเสี่ยง (Risk Owner)

(ช) สถานะของการจัดการความเสี่ยง (Status of Risk Treatment)

(ซ) ความเสี่ยงที่เหลือ (Residual Risk)

**๑.๓ การประเมินช่องโหว่และการทดสอบเจาะระบบ**
**(Vulnerability Assessment and Penetration Testing)**

๑.๓.๑ หน่วยงานต้องการประเมินช่องโหว่ของอุปกรณ์ของหน่วยงาน ครอบคลุมอุปกรณ์ ระบบ และเครือข่ายที่เกี่ยวข้องกับบริการที่สำคัญของโรงพยาบาล เพื่อระบุจุดอ่อนด้านความมั่นคงปลอดภัย ตามความเหมาะสมของทรัพยากรและความเสี่ยง

๑.๓.๒ ขอบเขตการประเมินอาจประกอบด้วย

(๑) การประเมินความมั่นคงปลอดภัยของโฮสต์ (Host Security Assessment)

(๒) การประเมินความมั่นคงปลอดภัยของเครือข่าย (Network Security Assessment)

(๓) การทบทวนความมั่นคงปลอดภัยของสถาปัตยกรรมระบบ (Architecture Security Review)

๑.๓.๓ หน่วยงานต้องดำเนินการประเมินช่องโหว่ (Vulnerability Assessment) ของระบบและบริการที่มีความสำคัญ เพื่อระบุจุดอ่อนด้านความมั่นคงปลอดภัยไซเบอร์ ก่อนการนำระบบใหม่มาใช้งาน หรือก่อนการเปลี่ยนแปลงระบบสารสนเทศที่มีความสำคัญ ซึ่งรวมถึงการเพิ่มโมดูลแอปพลิเคชัน การปรับปรุงระบบ และการปรับเปลี่ยนเทคโนโลยีที่เกี่ยวข้องกับการดำเนินงานหลักของหน่วยงาน

๑.๓.๔ หน่วยงานควรพิจารณาดำเนินการทดสอบเจาะระบบ (Penetration Testing) สำหรับระบบและบริการที่มีความสำคัญ โดยเฉพาะระบบเทคโนโลยีสารสนเทศ (Information Technology: IT) ที่มีการเชื่อมต่อกับเครือข่ายอินเทอร์เน็ต (Internet Facing) ให้สอดคล้องกับระดับความเสี่ยง และคำนึงถึงผลกระทบต่อการให้บริการหลักของหน่วยงาน

๑.๓.๕ ให้กำหนดขอบเขตของการทดสอบเจาะระบบ (Scope of Penetration Testing) ให้ครอบคลุมโฮสต์ ระบบเครือข่าย และแอปพลิเคชันของระบบและบริการที่มีความสำคัญของหน่วยงาน โดยเฉพาะระบบที่มีการเชื่อมต่ออินเทอร์เน็ตโดยตรง

๑.๓.๖ หน่วยงานควรดำเนินการทดสอบเจาะระบบอย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง เพื่อประเมินและยืนยันประสิทธิผลของมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ของระบบและบริการที่มีความสำคัญของหน่วยงาน

๑.๓.๗ ผู้ดำเนินการทดสอบเจาะระบบต้องเป็นผู้ที่มีความรู้ ความเชี่ยวชาญ และได้รับการรับรองหรือประกาศนียบัตร (Accreditations and Certifications) ที่เป็นที่ยอมรับตามมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์

๑.๓.๖ หน่วยงานต้องจัดทำรายงานผลการประเมินช่องโหว่หรือการทดสอบเจาะระบบ รวมถึงกำหนดกระบวนการติดตาม แก้ไข และตรวจสอบสถานะของช่องโหว่ที่ตรวจพบ เพื่อให้มั่นใจว่าช่องโหว่ที่มีความเสี่ยงได้รับการแก้ไขอย่างเหมาะสม

๑.๓.๙ กรณีได้รับการร้องขอจากคณะกรรมการหรือหน่วยงานที่มีอำนาจตามกฎหมายด้านความมั่นคงปลอดภัยไซเบอร์ หน่วยงานต้องจัดส่งรายงานสรุปผลการทดสอบเจาะระบบภายในระยะเวลา ๓๐ วัน นับแต่วันที่ได้รับหนังสือร้องขอ

**๑.๔ การจัดการผู้ให้บริการภายนอก (Third Party Management)**

๑.๔.๑ ความรับผิดชอบของโรงพยาบาล

แม้จะมีการจ้างผู้ให้บริการภายนอก โรงพยาบาลยังคงมีความรับผิดชอบ (Responsible) และมีภาระรับผิดชอบ (Accountable) ต่อความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญ โดยต้องดำเนินการอย่างน้อย ดังนี้

- คัดเลือกผู้ให้บริการภายนอกที่มีคุณสมบัติ ความน่าเชื่อถือ และมาตรฐานด้านความมั่นคงปลอดภัยที่เหมาะสม

- กำหนดขอบเขตงาน บทบาท หน้าที่ และความรับผิดชอบของผู้ให้บริการภายนอกให้ชัดเจน
- กำหนดให้ผู้ให้บริการภายนอกต้องปฏิบัติตามนโยบาย แนวปฏิบัติ และมาตรการของโรงพยาบาลด้านความมั่นคงปลอดภัยไซเบอร์ การคุ้มครองข้อมูลส่วนบุคคล และธรรมาภิบาลข้อมูล โดยต้องระบุเป็นเงื่อนไขในขอบเขตงานหรือข้อกำหนดทางเทคนิค (TOR)

๑.๔.๒ ข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ในสัญญา

โรงพยาบาลต้องกำหนดข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ไว้ในข้อตกลงระดับการให้บริการ (Service Level Agreement: SLA) หรือเงื่อนไขของสัญญา เพื่อควบคุมและลดความเสี่ยงที่เกิดจากการเข้าถึง การจัดเก็บ การสื่อสาร หรือการดำเนินการของผู้ให้บริการภายนอก โดยคำนึงถึงอย่างน้อยดังต่อไปนี้

(ก) ประเภทและระดับการเข้าถึงของผู้ให้บริการภายนอกต่อทรัพย์สิน ระบบ หรือข้อมูลของบริการที่สำคัญของโรงพยาบาล ตามความจำเป็นทางธุรกิจและระดับความเสี่ยง

(ข) หน้าที่และความรับผิดชอบของผู้ให้บริการภายนอกในการปกป้องบริการที่สำคัญของโรงพยาบาลจากภัยคุกคามทางไซเบอร์

(ค) ความเสี่ยงที่เกี่ยวข้องกับบริการ ระบบ และห่วงโซ่อุปทานของผู้ให้บริการภายนอก

(ง) สิทธิของโรงพยาบาลในการเข้าตรวจสอบหรือประเมินการปฏิบัติตามข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการภายนอก

๑.๔.๓ การตรวจสอบผู้ให้บริการภายนอก

โรงพยาบาลควรพิจารณาดำเนินการตรวจสอบหรือประเมินความสอดคล้องของผู้ให้บริการภายนอกกับข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ที่ระบุไว้ในสัญญา ตามความเหมาะสมและระดับความเสี่ยงของบริการนั้น

๑.๔.๔ การจัดทำข้อตกลงการประมวลผลข้อมูล (Data Processing Agreement)

ในกรณีที่ผู้ให้บริการภายนอกมีการเข้าถึงหรือประมวลผลข้อมูลสุขภาพหรือข้อมูลส่วนบุคคลของโรงพยาบาล ต้องจัดให้มีการจัดทำและลงนามในข้อตกลงการประมวลผลข้อมูล (Data Processing Agreement: DPA) โดยระบุขอบเขต วัตถุประสงค์ วิธีการประมวลผล และมาตรการด้านความมั่นคงปลอดภัยให้ชัดเจน และต้องสอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้อง

๑.๔.๕ การปรับปรุงสัญญาตามข้อกำหนดใหม่

ในกรณีที่มีการเปลี่ยนแปลงกฎหมาย ระเบียบ หรือข้อบังคับที่เกี่ยวข้องด้านความมั่นคงปลอดภัยไซเบอร์หรือการคุ้มครองข้อมูลส่วนบุคคล โรงพยาบาลควรพิจารณาปรับปรุงเงื่อนไขของสัญญากับผู้ให้บริการภายนอกให้สอดคล้องกับข้อกำหนดดังกล่าว

**หัวข้อที่ ๒ มาตรการป้องกันด้านความมั่นคงปลอดภัยไซเบอร์ (Protect)**

โรงพยาบาลสมเด็จพระสังฆราช องค์ที่ ๑๗ กำหนดมาตรการป้องกันด้านความมั่นคงปลอดภัยไซเบอร์เพื่อป้องกันการเข้าถึง การใช้งาน การเปิดเผย การเปลี่ยนแปลง หรือการทำลายข้อมูลและระบบสารสนเทศโดยไม่ได้รับอนุญาต โดยมุ่งให้การดำเนินงานเป็นไปอย่างเหมาะสมกับภารกิจด้านบริการทางการแพทย์ และสอดคล้องกับกฎหมายและมาตรฐานที่เกี่ยวข้อง ทั้งนี้ ประกอบด้วยมาตรการดังต่อไปนี้

**๒.๑ การควบคุมการเข้าถึง (Access Control)**

โรงพยาบาลต้องควบคุมการอนุญาต การกำหนดสิทธิ์ และการมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานเครือข่าย ระบบสารสนเทศ และอุปกรณ์ทั้งในเชิงอิเล็กทรอนิกส์และทางกายภาพ รวมถึงการเข้าถึงของบุคคลภายนอก โดยคำนึงถึงความจำเป็นตามหน้าที่และความมั่นคงปลอดภัยของระบบเป็นสำคัญ

๒.๑.๑ โรงพยาบาลต้องควบคุมการเข้าถึงข้อมูลและอุปกรณ์ประมวลผลข้อมูล โดยครอบคลุมอย่างน้อย ดังนี้

(ก) การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

(ข) การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

(ค) การควบคุมการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ระบบเครือข่าย

(ง) การควบคุมการเข้าถึงระบบงานและแอปพลิเคชัน

(จ) การบริหารจัดการการเข้าถึงด้านระบบเทคโนโลยีสารสนเทศของผู้ใช้งาน

๒.๑.๒ หน่วยงานต้องกำหนดหลักเกณฑ์การอนุญาตให้เข้าถึงระบบและข้อมูล ให้สอดคล้องกับบทบาท หน้าที่และความรับผิดชอบของเจ้าหน้าที่แต่ละระดับ

๒.๑.๓ หน่วยงานต้องกำหนดประเภทของข้อมูล ลำดับความสำคัญหรือลำดับชั้นความลับ รวมทั้งระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึงและช่องทางการเข้าถึงให้เหมาะสมกับลักษณะข้อมูล

๒.๑.๔ หน่วยงานต้องควบคุมและตรวจสอบการเข้าถึงอินเทอร์เฟซ (Interface) ของบริการที่สำคัญของหน่วยงาน เช่น พอร์ต USB หรือช่องทางเชื่อมต่ออื่น ตามความเหมาะสม

๒.๑.๕ หน่วยงานบันทึกกิจกรรมการโจมตีจากผู้ไม่ประสงค์ดีและความพยายามในการเข้าถึงบริการที่สำคัญของหน่วยงานทั้งหมด

๒.๑.๖ การเข้าถึงระบบสารสนเทศของหน่วยงานต้องมีการเข้ารหัส Transaction ที่มีความปลอดภัย โดยมีใบรับรอง (Certificate) เช่น Secure Socket Layer (SSL) หรือ Transport Layer Security (TLS) เป็นต้น

**๒.๒ การทำให้ระบบมีความแข็งแกร่ง (System Hardening)**

๒.๒.๑ โรงพยาบาลต้องจัดทำแนวทางหรือมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration) สำหรับระบบปฏิบัติการ แอปพลิเคชัน และอุปกรณ์เครือข่ายของระบบที่สำคัญ

๒.๒.๒ มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย ต้องมีหลักการอย่างน้อยดังต่อไปนี้

(ก) การให้สิทธิ์เข้าถึงเท่าที่จำเป็น (Least Access Privilege)

(ข) การแยกหน้าที่ความรับผิดชอบ (Separation of Duties)

(ค) การกำหนดนโยบายรหัสผ่านที่เหมาะสม

(ง) การยกเลิกบัญชีผู้ใช้งานที่ไม่ใช้งานแล้ว

(จ) การปิดหรือยกเลิกบริการและแอปพลิเคชันที่ไม่จำเป็น

(ฉ) การปิดพอร์ตเครือข่ายที่ไม่ได้ใช้งาน

(ช) การป้องกันมัลแวร์ (Malware)

(ซ) การปรับปรุงซอฟต์แวร์และแพตช์ด้านความมั่นคงปลอดภัยอย่างเหมาะสม

๒.๒.๓ หน่วยงานตรวจสอบความสอดคล้องกับมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย ก่อนการเชื่อมต่อทรัพย์สินใหม่ หรือการเปลี่ยนแปลงระบบที่สำคัญ

๒.๒.๔ หน่วยงานต้องตรวจสอบและทบทวนมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัยของระบบที่สำคัญอย่างน้อยปีละ ๑ ครั้ง

๒.๒.๕ หน่วยงานต้องจัดทำกระบวนการเปลี่ยนแปลง (Change Management Process) เพื่อควบคุม ตรวจสอบ และอนุมัติการเปลี่ยนแปลงที่มีผลต่อระบบที่สำคัญ

**๒.๓ การเชื่อมต่อระยะไกล (Remote Control)**

หน่วยงานต้องควบคุมและตรวจสอบการเชื่อมต่อระยะไกลเข้าสู่ระบบที่สำคัญ เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

๒.๓.๑ อนุญาตให้มีการเชื่อมต่อระยะไกลเฉพาะกรณีจำเป็นและได้รับการอนุญาตจากผู้มีอำนาจ

๒.๓.๒ ใช้โปรโตคอลหรือช่องทางการเชื่อมต่อที่มีความปลอดภัย เช่น Internet Protocol Security (IPSEC)

๒.๓.๓ การเชื่อมต่อระยะไกลต้องดำเนินการผ่านระบบเครือข่ายเสมือน (Virtual Private Network: VPN)

๒.๓.๔ ควรใช้วิธีการพิสูจน์ตัวตน (Authentication Techniques) ที่มีความมั่นคงปลอดภัย เช่น การยืนยันตัวตนหลายปัจจัย (Two Factor Authentication) กำหนดระยะเวลาในการเปลี่ยนรหัสผ่าน

๒.๓.๕ ใช้การเข้ารหัสสำหรับการเชื่อมต่อเครือข่ายทั้งหมด เช่น HTTPS, SSH, SCP เป็นต้น

๒.๓.๖ ไม่อนุญาตให้เชื่อมต่อระยะไกลจากการใช้คำสั่งระบบ (Issuing System Commands) ที่จะส่งผลกระทบต่อการดำเนินการบริการที่สำคัญของหน่วยงานเว้นแต่จะได้รับอนุญาต

๒.๓.๗ จำกัดการรับส่งข้อมูลเฉพาะเท่าที่จำเป็นต่อการปฏิบัติงาน

**๒.๔ สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media)**

๒.๔.๑ หน่วยงานต้องควบคุมการใช้งานสื่อบันทึกข้อมูลแบบถอดได้และอุปกรณ์คอมพิวเตอร์พกพาที่เชื่อมต่อกับระบบที่สำคัญ โดยใช้มาตรการอย่างน้อย ดังนี้

(ก) เปิดใช้งานพอร์ตเชื่อมต่อเฉพาะเมื่อจำเป็นเท่านั้น

(ข) ใช้สื่อบันทึกข้อมูลที่ได้รับอนุญาตเท่านั้น

(ค) ตรวจสอบความปลอดภัยและมัลแวร์ (Malware) ก่อนเชื่อมต่อ

๒.๔.๒ หน่วยงานต้องเข้ารหัสข้อมูลที่ละเอียดอ่อนทั้งหมดของบริการที่สำคัญของหน่วยงาน สำหรับสื่อบันทึกข้อมูลแบบถอดได้

๒.๔.๓ หน่วยงานต้องมีการกำหนดวิธีการที่ปลอดภัยในการทำลายสื่อบันทึกข้อมูลแบบถอดได้ เพื่อป้องกันการรั่วไหลของข้อมูล

**๒.๕ การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)**

๒.๕.๑ หน่วยงานต้องเผยแพร่ประชาสัมพันธ์ เกี่ยวกับแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์และสร้างความตระหนักถึงความสำคัญของการปฏิบัติหรือข้อระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่ายเพื่อให้บุคลากรรับทราบและนำไปปฏิบัติ

๒.๕.๒ หน่วยงานต้องจัดทำและปรับปรุง คู่มือการใช้งานระบบสารสนเทศให้เป็นปัจจุบัน และมีการเผยแพร่ผ่านช่องทางที่เหมาะสมของหน่วยงาน

๒.๕.๓ หน่วยงานต้องจัดฝึกอบรมการใช้งานระบบสารสนเทศของหน่วยงานอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการปรับปรุง และเปลี่ยนแปลงการใช้งานของระบบสารสนเทศที่สำคัญ

๒.๕.๔ หน่วยงานต้องสร้างความตระหนัก (Awareness Program) เรื่องการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ความเสี่ยงด้านเทคโนโลยีสารสนเทศ การใช้งานระบบอย่างปลอดภัยให้แก่บุคลากรทุกระดับ

๒.๕.๕ หน่วยงานควรจัดให้มีการฝึกอบรม และพัฒนาความรู้ความเชี่ยวชาญให้ครอบคลุม และเพียงพอต่อการปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ กับเจ้าหน้าที่ที่ดูแล ระบบสารสนเทศ

**๒.๖ การแบ่งปันข้อมูล (Information Sharing)**

โรงพยาบาลต้องกำหนดแนวปฏิบัติในการแบ่งปันข้อมูลที่เกี่ยวข้องกับเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์และภัยคุกคามทางไซเบอร์ เพื่อสนับสนุนการป้องกัน การเฝ้าระวัง และการรับมือเหตุการณ์อย่างเหมาะสม โดยคำนึงถึงความมั่นคงปลอดภัยของข้อมูล การคุ้มครองข้อมูลส่วนบุคคล และกฎหมายที่เกี่ยวข้อง ทั้งนี้ ให้มีแนวทางการดำเนินการ ดังต่อไปนี้

๒.๖.๑ กำหนดขั้นตอนและผู้รับผิดชอบในการแจ้งและแบ่งปันข้อมูลเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ภายในโรงพยาบาลให้ชัดเจน

๒.๖.๒ กำหนดหลักเกณฑ์ของเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ต้องมีการแจ้งหรือแบ่งปันข้อมูล เช่น เหตุการณ์ที่กระทบต่อระบบสารสนเทศ ข้อมูลผู้ป่วย หรือการให้บริการที่มีความสำคัญ

๒.๖.๓ แบ่งปันข้อมูลเฉพาะเท่าที่จำเป็นกับหน่วยงานหรือบุคคลที่เกี่ยวข้อง เช่น ผู้บริหาร เจ้าของระบบ ผู้ดูแลระบบ หรือหน่วยงานที่ได้รับผลกระทบ เพื่อให้สามารถดำเนินมาตรการป้องกันหรือแก้ไขได้อย่างเหมาะสม

๒.๖.๔ จัดให้มีการจำแนกระดับความลับของข้อมูล และเลือกวิธีการแบ่งปันข้อมูลให้เหมาะสมกับระดับความอ่อนไหวของข้อมูลนั้น

๒.๖.๕ ใช้ช่องทางในการแบ่งปันข้อมูลที่มีความเหมาะสมและปลอดภัย เช่น ระบบภายใน อีเมลทางราชการ หรือช่องทางที่โรงพยาบาลกำหนด พร้อมควบคุมสิทธิการเข้าถึงข้อมูล

๒.๖.๖ พิจารณาการคุ้มครองข้อมูลส่วนบุคคลก่อนการแบ่งปันข้อมูล โดยหลีกเลี่ยงการเปิดเผยข้อมูลส่วนบุคคลที่ไม่จำเป็น หรือดำเนินการปกปิดข้อมูลส่วนบุคคลเท่าที่สามารถทำได้

๒.๖.๗ ในกรณีจำเป็นต้องแบ่งปันข้อมูลกับหน่วยงานภายนอก ให้ดำเนินการภายใต้ข้อตกลงหรือคำสั่งที่โรงพยาบาลกำหนด และต้องไม่ขัดต่อกฎหมาย ระเบียบ หรือประกาศที่เกี่ยวข้อง

๒.๖.๘ ทบทวนแนวปฏิบัติในการแบ่งปันข้อมูลด้านความมั่นคงปลอดภัยไซเบอร์เป็นระยะให้เหมาะสมกับบริบทของโรงพยาบาล

**หัวข้อที่ ๓ มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)**

โรงพยาบาลดำเนินการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Treat Detection and Monitoring) เพื่อให้สามารถตรวจพบเหตุการณ์ผิดปกติ การกระทำโดยมิชอบ หรือการใช้โปรแกรมที่ไม่พึงประสงค์ที่อาจส่งผลกระทบต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ และการให้บริการที่สำคัญของ

โรงพยาบาลได้อย่างทันท่วงที ทำให้สามารถรับมือกับภัยคุกคามได้ทันท่วงที ป้องกันความเสียหายที่ร้ายแรง ลดอัตราความสำเร็จของการโจมตี และทำให้การกู้คืนระบบรวดเร็วขึ้น

**๓.๑ การสร้างกลไกและกระบวนการตรวจจับภัยคุกคามทางไซเบอร์**

๓.๑.๑ การตรวจจับเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์

โรงพยาบาลต้องตรวจจับเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับบริการที่สำคัญของโรงพยาบาล ดังนี้

(ก) ใช้เครื่องมือหรือระบบในการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ที่เหมาะสมกับบริบทและทรัพยากรของโรงพยาบาล เช่น ระบบตรวจสอบ Log ระบบป้องกันมัลแวร์ ระบบรักษาความปลอดภัยเครือข่าย หรือเครื่องมือที่มากับระบบสารสนเทศที่ใช้งานอยู่

(ข) มีการตรวจสอบบันทึกเหตุการณ์ (Log) และกิจกรรมเครือข่ายของระบบที่สำคัญอย่างสม่ำเสมอ และสามารถตอบสนองต่อเหตุการณ์ที่ผิดปกติได้ตามความเหมาะสม ทั้งนี้ อาจพิจารณาใช้เครื่องมือสนับสนุน เช่น ระบบรวบรวมและวิเคราะห์ Log หรือบริการจากผู้ให้บริการภายนอกตามศักยภาพของโรงพยาบาล

(ค) มีแนวทางหรือระบบแจ้งเตือนเหตุการณ์ผิดปกติหรือเหตุการณ์ที่น่าสงสัย เพื่อให้ผู้ดูแลระบบสามารถรับทราบและดำเนินการต่อได้อย่างเหมาะสม

(ง) พิจารณาการจัดตั้งหรือใช้บริการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศจากภายนอก (เช่น บริการ SOC) ตามความจำเป็นและความเหมาะสมของทรัพยากร

๓.๑.๒ การจัดประเภทและวิเคราะห์เหตุการณ์

โรงพยาบาลต้องมีแนวทางในการจัดประเภทและวิเคราะห์เหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ตรวจพบ ดังนี้

(ก) มีการวิเคราะห์ข้อมูลการแจ้งเตือน และ Log เพื่อพิจารณาว่าเป็นเหตุการณ์ผิดปกติหรือภัยคุกคามประเภทใด

(ข) เชื่อมโยงเหตุการณ์ที่เกี่ยวข้อง เพื่อระบุขอบเขตและความร้ายแรงของภัยคุกคาม

(ค) จัดประเภทเหตุการณ์ที่ผิดปกติที่วิเคราะห์ได้จากพฤติกรรมของผู้ใช้งานในหน่วยงาน (Behavior Analytics) เพื่อใช้ประกอบการประเมินเหตุการณ์ตามความเหมาะสม

๓.๑.๓ การระบุภัยคุกคามและการเตรียมความพร้อมเบื้องต้น

โรงพยาบาลต้องมีการระบุภัยคุกคามหรือเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับบริการที่สำคัญ และประเมินผลกระทบในระดับที่เหมาะสม

(ก) วิเคราะห์ความเสี่ยงและผลกระทบที่เกิดขึ้นจากภัยคุกคามหรือเหตุการณ์ดังกล่าวว่าส่งผลต่อบริการหรือหน่วยงาน

(ข) เตรียมความพร้อมในการตอบสนองต่อภัยคุกคามหรือเหตุการณ์ดังกล่าว อย่างน้อย ดังนี้

- การกำหนดแนวทางการแจ้งเหตุและการประสานงานกับผู้รับผิดชอบ
- การจำกัดผลกระทบเบื้องต้น เช่น การแยกระบบหรือเครือข่ายที่ได้รับผลกระทบตามความเหมาะสม

- การรวบรวมข้อมูลหรือหลักฐานที่จำเป็นเพื่อใช้ในการวิเคราะห์เหตุการณ์
- การบันทึกเหตุการณ์และข้อสังเกต เพื่อใช้เป็นข้อมูลสำหรับการปรับปรุงมาตรการในอนาคต
- การแจ้งผู้เกี่ยวข้องหรือผู้มีส่วนได้เสียตามความเหมาะสม และเป็นไปตามกฎหมายหรือระเบียบที่เกี่ยวข้อง

หมายเหตุ : รายละเอียดเชิงลึกด้านการตอบสนองเหตุการณ์ ให้เป็นไปตามแผนการรับมือเหตุภัยคุกคามทางไซเบอร์ของโรงพยาบาล

**๓.๔ การทบทวนและปรับปรุงกระบวนการเฝ้าระวัง**

โรงพยาบาลต้องทบทวนและประเมินความเหมาะสมของกระบวนการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงระบบ เทคโนโลยี หรือรูปแบบการให้บริการที่มีผลกระทบต่อความมั่นคงปลอดภัยไซเบอร์ เพื่อให้กระบวนการดังกล่าวมีความสอดคล้องกับสถานการณ์ปัจจุบันและสามารถรองรับความเสี่ยงได้อย่างเหมาะสม

## หัวข้อที่ ๔ มาตรการเผชิญเหตุด้านความมั่นคงปลอดภัยไซเบอร์ (Respond)

โรงพยาบาลสมเด็จพระสังฆราช องค์ที่ ๑๗ กำหนดมาตรการเผชิญเหตุด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อให้สามารถตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ตรวจพบได้อย่างเป็นระบบ ลดผลกระทบต่อการให้บริการทางการแพทย์ ระบบสารสนเทศ และข้อมูลสำคัญของโรงพยาบาล โดยมีแผนและแนวปฏิบัติที่ชัดเจน ดังต่อไปนี้

**๔.๑ แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)**

๔.๑.๑ การจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์

โรงพยาบาลต้องจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ เพื่อกำหนดแนวทาง ขั้นตอน และความรับผิดชอบในการตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ โดยแผนดังกล่าวควรครอบคลุมรายละเอียดอย่างน้อย ดังนี้

๔.๑.๑.๑ โครงสร้างทีมรับมือเหตุการณ์ (Cyber Incident Response Team: CIRT)

โรงพยาบาลต้องกำหนดโครงสร้างทีมรับมือเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ หรือแต่งตั้งบุคลากรที่รับผิดชอบทำหน้าที่ดังกล่าวตามความเหมาะสมของขนาดและทรัพยากรของโรงพยาบาล โดยต้องระบุบทบาท หน้าที่ และช่องทางการติดต่ออย่างชัดเจน เช่น

(ก) ผู้ประสานงานหลักและผู้ประสานงานสำรอง
(ข) ผู้รับผิดชอบด้านเทคนิคระบบสารสนเทศ
(ค) ผู้รับผิดชอบด้านกฎหมายหรือระเบียบที่เกี่ยวข้อง
(ง) ผู้รับผิดชอบด้านการสื่อสารภายในและภายนอก

หมายเหตุ : อาจไม่จำเป็นต้องจัดตั้งทีม CIRT ขนาดใหญ่ แต่สามารถมอบหมายหน้าที่ให้บุคลากรที่เกี่ยวข้องและควรได้รับการฝึกอบรมหรือพัฒนาความรู้ด้านการรับมือเหตุการณ์อย่างสม่ำเสมอ

๔.๑.๑.๒ โครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure)

โรงพยาบาลต้องกำหนดแนวทางการรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ให้เป็นไปตามกฎหมาย ระเบียบ และข้อกำหนดที่เกี่ยวข้อง ดังนี้

(ก) ศึกษาและพิจารณากฎหมายที่เกี่ยวข้อง เช่น กฎหมายด้านความมั่นคงปลอดภัยไซเบอร์ กฎหมายคุ้มครองข้อมูลส่วนบุคคล และกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

(ข) กำหนดระยะเวลาและช่องทางการรายงานเหตุให้ชัดเจน

(ค) จัดทำแบบฟอร์มหรือเอกสารรายงานเหตุการณ์ เพื่อใช้เป็นหลักฐานในการตรวจสอบหรือสืบสวนในภายหลัง

๔.๑.๑.๓ เกณฑ์และขั้นตอนการเรียกใช้งานแผนและทีมรับมือเหตุการณ์

โรงพยาบาลต้องกำหนดเกณฑ์ที่ชัดเจนในการพิจารณาเริ่มใช้งานแผนการรับมือภัยคุกคามทางไซเบอร์ ดังนี้

(ก) ระดับความรุนแรงหรือผลกระทบต่อการให้บริการ

(ข) ความผิดปกติของระบบสารสนเทศ

(ค) ลักษณะหรือรูปแบบของการโจมตีทางไซเบอร์

รวมถึงกำหนดแนวทางการประสานงานในกรณีเกิดเหตุในช่วงเวลานอกเวลาราชการ วันหยุด หรือเหตุฉุกเฉินที่ส่งผลกระทบในวงกว้าง

๔.๑.๑.๔ ขั้นตอนการจำกัดขอบเขตและควบคุมเหตุการณ์ (Containment)

เมื่อเกิดเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ โรงพยาบาลต้องดำเนินการควบคุมและจำกัดผลกระทบของเหตุการณ์โดยเร็ว ดังนี้

(ก) การแยกหรือจำกัดการเชื่อมต่อของระบบหรือเครือข่ายที่ได้รับผลกระทบ

(ข) การควบคุมสิทธิ์การเข้าถึงระบบในช่วงที่เกิดเหตุ

(ค) การปรับปรุงหรือทบทวนมาตรการด้านความมั่นคงปลอดภัยที่เกี่ยวข้อง เช่น การตั้งค่าระบบ การควบคุมการเข้าถึง หรือการปรับปรุงแพตช์

(ง) การตรวจสอบและกำจัดซอฟต์แวร์ที่ไม่พึงประสงค์ออกจากระบบที่ได้รับผลกระทบ

๔.๑.๑.๕ การเรียกใช้งานกระบวนการกู้คืน (Recovery Process)

โรงพยาบาลต้องเตรียมความพร้อมในการกู้คืนระบบและข้อมูลหลังจากสามารถควบคุมเหตุการณ์ได้แล้ว ดังนี้

(ก) กำหนดลำดับความสำคัญของระบบและข้อมูลที่ต้องกู้คืน

(ข) ตรวจสอบความปลอดภัยของระบบก่อนนำกลับมาใช้งาน

(ค) สื่อสารกับผู้มีส่วนได้เสียเกี่ยวกับสถานะและผลกระทบจากการกู้คืน

(ง) บันทึกขั้นตอนการกู้คืนไว้เป็นเอกสารเพื่อใช้เป็นข้อมูลอ้างอิงในอนาคต

๔.๑.๑.๖ ขั้นตอนการสอบสวนและวิเคราะห์สาเหตุของเหตุการณ์

โรงพยาบาลต้องมีแนวทางในการรวบรวมข้อมูลและวิเคราะห์เหตุการณ์ เพื่อระบุสาเหตุและผลกระทบที่เกิดขึ้น โดยอาจรวมถึงรายละเอียดต่าง ๆ ดังนี้

(ก) การรวบรวมข้อมูลจากบันทึกเหตุการณ์หรือหลักฐานที่เกี่ยวข้อง

(ข) การประเมินผลกระทบต่อระบบและการให้บริการ

(ค) การประสานงานกับหน่วยงานภายนอกที่เกี่ยวข้องตามความจำเป็น

(ง) การพิจารณาว่าจำเป็นต้องดำเนินการตามกฎหมายหรือข้อกำหนดใดหรือไม่

๔.๑.๑.๗ การเก็บรักษาพยานหลักฐาน (Preservation of Evidence)

ในกรณีที่จำเป็น โรงพยาบาลต้องมีแนวทางในการเก็บรักษาพยานหลักฐานอย่างเหมาะสม เพื่อสนับสนุนการสอบสวนหรือการดำเนินการทางกฎหมาย ดังนี้

(ก) บันทึกรายละเอียดการจัดการพยานหลักฐานอย่างเป็นระบบ

(ข) ควบคุมการเข้าถึงและการจัดเก็บพยานหลักฐานให้ปลอดภัย

(ค) ป้องกันการแก้ไขหรือเปลี่ยนแปลงพยานหลักฐาน

๔.๑.๑.๘ แนวปฏิบัติในการประสานงานกับบุคคลภายนอก

โรงพยาบาลต้องกำหนดแนวทางในการประสานงานกับผู้ให้บริการหรือหน่วยงานภายนอกที่เกี่ยวข้องกับการรับมือเหตุการณ์ ดังนี้

(ก) การกำหนดขอบเขต บทบาท และความรับผิดชอบของบุคคลภายนอก

(ข) การรักษาความลับของข้อมูล

(ค) การใช้ช่องทางการสื่อสารที่เหมาะสมและปลอดภัย

๔.๑.๑.๙ การทบทวนหลังการดำเนินการ (After-Action Review)

หลังจากเหตุการณ์สิ้นสุด โรงพยาบาลต้องดำเนินการทบทวนผลการดำเนินงาน ดังนี้

(ก) ประเมินประสิทธิภาพของการตอบสนองต่อเหตุการณ์

(ข) วิเคราะห์จุดแข็ง จุดอ่อน และข้อจำกัดของกระบวนการ

(ค) ถอดบทเรียนและจัดทำข้อเสนอแนะเพื่อปรับปรุงแผนและแนวปฏิบัติ

(ง) ปรับปรุงนโยบาย แนวปฏิบัติ หรือการฝึกอบรมให้เหมาะสมยิ่งขึ้น

**๔.๒ แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)**

โรงพยาบาลสมเด็จพระสังฆราช องค์ที่ ๑๗ ต้องจัดทำแผนการสื่อสารในภาวะวิกฤต เพื่อรองรับสถานการณ์ที่เกิดจากเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ และเพื่อให้การสื่อสารทั้งภายในและภายนอกหน่วยงานเป็นไปอย่างถูกต้อง เหมาะสม ทันเวลา และลดผลกระทบต่อการให้บริการและความเชื่อมั่นของผู้มีส่วนได้เสีย

แผนการสื่อสารในภาวะวิกฤตครอบคลุมทั้ง การสื่อสารเมื่อเกิดเหตุการณ์จริง และ การสื่อสารแผนการรับมือภัยคุกคามทางไซเบอร์ให้บุคลากรที่เกี่ยวข้องรับทราบล่วงหน้า โดยมีแนวทางการดำเนินการดังต่อไปนี้

๔.๒.๑ การจัดทำแผนการสื่อสารในภาวะวิกฤต

โรงพยาบาลต้องจัดทำแผนการสื่อสารในภาวะวิกฤต เพื่อใช้เป็นแนวทางในการสื่อสารเมื่อเกิดเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ส่งผลกระทบต่อระบบสารสนเทศ การให้บริการ หรือภาพลักษณ์ขององค์กร

๔.๒.๒ องค์ประกอบของแผนการสื่อสารในภาวะวิกฤต อย่างน้อยต้องประกอบด้วย

(ก) การจัดตั้งทีมสื่อสารในภาวะวิกฤต และโครงสร้างการเรียกใช้งาน (Call Tree)

(ข) การกำหนดสถานการณ์จำลองเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่อาจเกิดขึ้นพร้อมแนวทางการสื่อสารในแต่ละกรณี

(ค) การระบุกลุ่มเป้าหมายและผู้มีส่วนได้เสียที่เกี่ยวข้อง

(ง) การระบุโฆษกหลัก และผู้เชี่ยวชาญด้านเทคนิคที่ได้รับมอบหมายให้ให้ข้อมูลต่อสาธารณะ

(จ) การกำหนดช่องทางหรือแพลตฟอร์มในการสื่อสารที่เหมาะสม

๔.๒.๓ การสื่อสารแผนการรับมือภัยคุกคามทางไซเบอร์ภายในหน่วยงาน

หน่วยงานต้องดำเนินการสื่อสารแผนการรับมือภัยคุกคามทางไซเบอร์ให้แก่บุคลากรที่เกี่ยวข้องกับการสนับสนุนบริการที่สำคัญ เพื่อให้สามารถเข้าใจบทบาท หน้าที่ และขั้นตอนการปฏิบัติได้อย่างถูกต้อง ดังนี้

(ก) วางแผนการสื่อสารให้เหมาะสมกับบริบทของโรงพยาบาล รวมถึงช่องทางการสื่อสาร เนื้อหาที่สื่อสาร และผู้รับผิดชอบ

(ข) ตรวจสอบให้มั่นใจว่าบุคลากรที่เกี่ยวข้องได้รับการสื่อสารและสามารถเข้าใจแผนการรับมือภัยคุกคามทางไซเบอร์ได้อย่างเหมาะสม

๔.๒.๔ การทบทวนและการฝึกซ้อมแผนการสื่อสารในภาวะวิกฤต

หน่วยงานต้องทบทวนแผนการสื่อสารในภาวะวิกฤต รวมถึงการประสานงานระหว่างหน่วยงานที่เกี่ยวข้อง และควรดำเนินการฝึกซ้อมแผนอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการปรับปรุงแผนหรือโครงสร้างการรับมือเหตุการณ์

๔.๒.๕ การรายงานและการสื่อสารความคืบหน้าเมื่อเกิดเหตุการณ์

ในกรณีเกิดเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ หน่วยงานต้องจัดทำรายงานเหตุการณ์ (Incident Report) และรายงานความคืบหน้าการดำเนินการให้ผู้บริหารหรือคณะกรรมการที่เกี่ยวข้องทราบอย่างต่อเนื่อง ตามระดับความรุนแรงและผลกระทบของเหตุการณ์

**หัวข้อที่ ๕ มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)**

มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคมทางไซเบอร์ (Cybersecurity Recovery) มุ่งเน้นการฟื้นฟูระบบสารสนเทศ ข้อมูล และการดำเนินงานของโรงพยาบาล หลังจากเกิดเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Incident) เพื่อให้สามารถกลับมาดำเนินงานได้อย่างต่อเนื่อง รวดเร็ว และลดผลกระทบต่อการให้บริการทางการแพทย์

ทั้งนี้ มาตรการดังกล่าวไม่จำกัดเฉพาะการกู้คืนระบบ (Recovery) เท่านั้น แต่ยังครอบคลุมการเสริมสร้างความสามารถในการฟื้นตัว (Cyber Resilience) การสื่อสารเพื่อสร้างความเชื่อมั่นแก่ผู้มีส่วนได้เสีย (Stakeholders Communication) และการถอดบทเรียนเพื่อนำไปปรับปรุงมาตรการด้านความมั่นคงปลอดภัยไซเบอร์ในระยะยาว

**๕.๑ จัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP)**

โรงพยาบาลควรจัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP) เพื่อให้มั่นใจว่าบริการที่สำคัญ (Critical Services) และทรัพย์สินสารสนเทศที่สำคัญ (Critical Information Assets) สามารถกลับมาให้บริการได้ตามปกติภายหลังเกิดเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์

แผนความต่อเนื่องทางธุรกิจต้องกำหนดมาตรการในการควบคุมเหตุการณ์ การขจัดภัยคุกคาม และการฟื้นฟูระบบงาน (Containment, Eradication and Recovery) ให้สอดคล้องกับระดับความรุนแรงของภัยคุกคาม (Severity Level) ควรประกอบด้วยสาระสำคัญอย่างน้อย ดังนี้

(ก) การกำหนดบทบาท หน้าที่ และความรับผิดชอบของผู้เกี่ยวข้อง (Roles and Responsibilities) รวมถึงกลยุทธ์การสื่อสารในภาวะวิกฤต (Crisis Communication Strategy)

(ข) การวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA) เพื่อระบุระบบ กระบวนการหรือบริการที่มีความสำคัญ และจัดลำดับความสำคัญในการฟื้นฟู (Recovery Priority)

(ค) การกำหนดระยะเวลาสูงสุดที่ระบบสามารถหยุดชะงักได้ (Maximum Tolerable Period of Disruption: MTPD)

(ง) การกำหนดระยะเวลาเป้าหมายในการฟื้นคืนสภาพของระบบ (Recovery Time Objective: RTO)

(จ) การกำหนดจุดเป้าหมายในการกู้คืนข้อมูล (Recovery Point Objective : RPO)

(ฉ) การวิเคราะห์ความเสี่ยงและกำหนดกลยุทธ์เพื่อลดผลกระทบ (Risk Mitigation Strategy)

(ช) การจัดให้มีระบบสำรองข้อมูลและระบบทดแทน (Backup and Redundancy) เพื่อรองรับการกู้คืนระบบ

(ซ) การจัดเตรียมสถานที่สำรองหรือแนวทางการปฏิบัติงานทดแทน (Alternate Site / Alternate Work Arrangement)

(ฌ) การควบคุมและตรวจสอบสิทธิการเข้าถึงระบบทั้งในระบบหลักและระบบสำรอง (Access Control for Primary and Backup Systems)

ทั้งนี้ การจัดทำแผนความต่อเนื่องทางธุรกิจต้องเป็นไปตามหลักเกณฑ์และแนวทางที่หน่วยงานกำกับกำหนด และสอดคล้องกับกรอบมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์

**๕.๒ การฝึกซ้อมและทบทวนแผนความต่อเนื่องทางธุรกิจ (BCP Testing and Review)**

โรงพยาบาลต้องจัดให้มีการฝึกซ้อมและทบทวนแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP) อย่างน้อยปีละ ๑ ครั้ง เพื่อประเมินความพร้อมและประสิทธิภาพของแผนในการรองรับเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ และเหตุขัดข้องของระบบสารสนเทศที่อาจส่งผลกระทบต่อการให้บริการทางการแพทย์และการดำเนินงานของโรงพยาบาล

การฝึกซ้อมและทบทวนแผนความต่อเนื่องทางธุรกิจควรครอบคลุมแนวทางดังต่อไปนี้

๕.๒.๑ การเตรียมความพร้อมและสร้างความเข้าใจ (Training and Awareness)

จัดให้มีการฝึกอบรมหรือสื่อสารสร้างความเข้าใจแก่บุคลากรที่เกี่ยวข้อง เกี่ยวกับบทบาทหน้าที่ ขั้นตอนการปฏิบัติ และช่องทางการประสานงานตามแผนความต่อเนื่องทางธุรกิจ เพื่อให้สามารถปฏิบัติได้อย่างถูกต้องเมื่อเกิดเหตุการณ์จริง

๕.๒.๒ การซ้อมสถานการณ์จำลอง (Scenario-based Exercise)

จัดให้มีการซ้อมตามสถานการณ์จำลองที่เหมาะสมกับบริบทของโรงพยาบาล และระดับความรุนแรงของเหตุการณ์ เพื่อทดสอบการตัดสินใจ การสื่อสาร และการประสานงานระหว่างหน่วยงาน

ตัวอย่างสถานะการณ์จำลอง

- ระบบเวชระเบียนล่มชั่วคราว
- ระบบเครือข่ายไม่สามารถใช้งานได้บางส่วน
- เหตุการณ์โจมตีทางไซเบอร์ที่กระทบต่อการให้บริการผู้ป่วย

๕.๒.๓ รูปแบบการฝึกซ้อม

โรงพยาบาลควรพิจารณาจัดให้มีการฝึกซ้อมในรูปแบบที่เหมาะสมกับศักยภาพและทรัพยากรของหน่วยงาน โดยอาจประกอบด้วย

(ก) การซ้อมบนโต๊ะจำลองสถานการณ์ (Tabletop Exercise)
เพื่อทดสอบความเข้าใจในบทบาทหน้าที่ การตัดสินใจ และการสื่อสารระหว่างหน่วยงานหรือทีมที่เกี่ยวข้อง

(ข) การซ้อมเชิงเทคนิค (Technical Drill)
เช่น การทดสอบการกู้คืนข้อมูลจากระบบสำรอง (Backup) หรือระบบทดแทน เพื่อประเมินความสามารถในการกู้คืนระบบตามค่าระยะเวลาเป้าหมายในการกู้คืนระบบ (Recovery Time Objective: RTO) และระยะเวลาข้อมูลสูญหายที่ยอมรับได้ (Recovery Point Objective: RPO) ที่กำหนดไว้

๕.๒.๔ การประเมินผลและปรับปรุงแผน (Lessons Learned and Improvement)

(ก) บันทึกผลการฝึกซ้อม ปัญหา อุปสรรค และข้อจำกัดที่พบจากการฝึกซ้อม

(ข) นำผลการประเมินและบทเรียนที่ได้รับ (Lessons Learned) มาปรับปรุงแผนความต่อเนื่องทางธุรกิจ และมาตรการด้านความมั่นคงปลอดภัยไซเบอร์ให้เหมาะสมและทันสมัยอย่างต่อเนื่อง

## เอกสารอ้างอิง

- พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒
- ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง การกำหนดหลักเกณฑ์ ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทาง สารสนเทศ และ การมอบหมายการควบคุมและกำกับดูแล พ.ศ. ๒๕๖๔
- ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง แนว ปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔
- ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง หน้าที่ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและหน่วยงานควบคุมหรือกำกับดูแล พ.ศ. ๒๕๖๗
- (ร่าง) นโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
- (ร่าง) ประกาศสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เรื่อง การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง สำหรับหน่วยงานของรัฐและ หน่วยงาน โครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ.๒๕๖๔ (NIST ๘๐๐-๓๙)
- (ร่าง) ประกาศสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เรื่อง การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ.๒๕๖๔ (NIST ๘๐๐-๓๐)
- (ร่าง) ประกาศสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เรื่อง กรอบการบริหารความเสี่ยงด้านไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้าง พื้นฐานสำคัญทางสารสนเทศ พ.ศ.๒๕๖๔ (NIST ๘๐๐-๓๓)
- นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โรงพยาบาลสมเด็จพระสังฆราช องค์ที่ ๑๗ ปี ๒๕๖๘