บทที่ ๑
บทนำ

๑. หลักการและเหตุผล

การนำกระบวนการบริหารความเสี่ยงมาใช้ภายในองค์กร โดยอาศัยหลักการพื้นฐานของการกำกับดูแลกิจการขององค์กรที่ดี (Good Governance) ทั้งนี้ เพื่อให้ผู้มีส่วนได้เสียขององค์กรสามารถเชื่อมั่นอย่างสมเหตุสมผลว่าการดำเนินงานเชิงกลยุทธ์ของงานด้านเทคโนโลยีสารสนเทศ มุ่งไปสู่การบรรลุวัตถุประสงค์และเป้าหมายขององค์กรอย่างมีประสิทธิภาพและประสิทธิผล ดังนั้น การพัฒนากระบวนการบริหารความเสี่ยงด้านสารสนเทศให้ประสบผลสำเร็จได้นั้น จำเป็นจะต้องส่งเสริมและผลักดันให้มีการบริหารความเสี่ยงทั่วทั้งองค์กรทุกระดับ รวมทั้งรณรงค์ให้ผู้บริหารและบุคลากรทุกคนตระหนักและเข้าใจถึงความสำคัญของการบริหารความเสี่ยง

โรงพยาบาลพระอาจารย์มั่น ภูริทัตโต ได้จัดทำแผนบริหารจัดการความเสี่ยงเทคโนโลยีสารสนเทศและการสื่อสาร ประจำปี ๒๕๖๙ ขึ้นเพื่อเป็นกรอบแนวทางในการดำเนินงานการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ ในการระบุความเสี่ยง วิเคราะห์ความเสี่ยง และการกำหนดแนวทางหรือมาตรการควบคุมเพื่อป้องกันหรือลดความเสี่ยง โดยมุ่งหวังให้บรรลุผลตามเป้าประสงค์ของหน่วยงาน เนื่องจากความเสี่ยงอาจนำไปสู่ผลเสียหรือความสูญเสียได้ทั้งทางตรงและทางอ้อม องค์กรจึงต้องเข้าใจประเภทของความเสี่ยงที่เผชิญอยู่เพื่อที่จะได้เลือกวิธีการที่เหมาะสมใน การบริหารความเสี่ยงเหล่านั้นให้อยู่ในระดับที่องค์กรสามารถรองรับได้และทำให้การปฏิบัติงานมีประสิทธิภาพมากยิ่งขึ้น

การบริหารความเสี่ยง คือ กระบวนการที่เป็นระบบในการบริหารปัจจัยและควบคุมกิจกรรม รวมทั้งกระบวนการดำเนินการต่างๆ เพื่อลดมูลเหตุของโอกาส ที่จะทำให้เกิดความเสียหายจากการดำเนินการที่ไม่เป็นไปตามแผน เพื่อให้ระดับของความเสี่ยงและผลกระทบที่จะเกิดขึ้นในอนาคตอยู่ในระดับที่สามารถยอมรับได้ ควบคุมได้และตรวจสอบได้อย่างเป็นระบบ

โรงพยาบาลพระอาจารย์มั่น ภูริทัตโต ได้วิเคราะห์และประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศโดยพิจารณาจากเหตุการณ์ด้านความมั่นคงปลอดภัย (Information Security Event) และภัยพิบัติหรือสถานการณ์อื่น ๆ รวมถึงได้กำหนดแนวทางการบริหารความเสี่ยงด้านสารสนเทศ การเตรียมความพร้อมกรณีฉุกเฉินใน การสำรองและการกู้คืนข้อมูลสารสนเทศ เพื่อจัดทำแผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศของโรงพยาบาลพระอาจารย์มั่น ภูริทัตโต อย่างน้อยปีละ ๑ ครั้ง สำหรับใช้เป็นแนวทางปฏิบัติงานต่อไป

๒. วัตถุประสงค์

๑. เพื่อให้โรงพยาบาลพระอาจารย์มั่น ภูริทัตโต มีแนวทางในการบริหารความเสี่ยงด้านสารสนเทศ รวมถึงการกำหนดแนวทางบริหารความเสี่ยงด้านสารสนเทศ ในการป้องกัน จัดการและลดความเสี่ยงดังกล่าวให้อยู่ในระดับที่ยอมรับได้อย่างต่อเนื่อง

๒. เพื่อให้มีการวางแผน การควบคุม แก้ไขความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารอย่างเหมาะสม

๓. เพื่อให้โรงพยาบาลพระอาจารย์มั่น ภูริทัตโต มีแนวทางในการสำรองข้อมูลระบบคอมพิวเตอร์และระบบสารสนเทศ โดยสามารถกู้คืนระบบและข้อมูลดังกล่าวได้ทันที เพื่อให้ผู้ใช้งาน (User) สามารถปฏิบัติงานได้อย่างต่อเนื่อง

๓. ประโยชน์ของการบริหารความเสี่ยงด้านสารสนเทศ

การดำเนินการบริหารความเสี่ยงจะช่วยให้ผู้บริหารมีข้อมูลที่ใช้ในการตัดสินใจได้ดียิ่งขึ้น และทำให้หน่วยงานสามารถจัดการกับปัญหาอุปสรรคและอยู่รอดได้ในสถานการณ์ที่ไม่คาดคิดหรือสถานการณ์ที่อาจทำให้หน่วยงานเกิดความเสียหาย ประโยชน์ที่คาดหวังว่าจะได้รับจากการดำเนินการบริหารความเสี่ยง มีดังนี้

๑. การบริหารความเสี่ยงจะช่วยคณะกรรมการบริหารความเสี่ยงและควบคุมภายในทุกระดับตระหนักถึงความเสี่ยงหลักที่สำคัญ และสามารถทำหน้าที่ในการกำกับดูแลหน่วยงานได้อย่างมีประสิทธิภาพและประสิทธิผลมากยิ่งขึ้น

๒. สร้างฐานข้อมูลความรู้ที่มีประโยชน์ต่อการบริหารและการปฏิบัติงานในหน่วยงาน การบริหารความเสี่ยงจะเป็นแหล่งข้อมูลสำหรับผู้บริหารในการตัดสินใจด้านต่างๆ ซึ่งรวมถึงการบริหารความเสี่ยงและตั้งอยู่บนสมมติฐานในการตอบสนองต่อเป้าหมายและภารกิจหลักของหน่วยงาน รวมถึงระดับความเสี่ยงที่ยอมรับได้

๓. ช่วยสะท้อนให้เห็นภาพรวมของความเสี่ยงต่างๆ ที่สำคัญได้ทั้งหมด การบริหารความเสี่ยงจะทำให้บุคลากรภายในหน่วยงานมีความเข้าใจถึงเป้าหมายและภารกิจหลักของหน่วยงาน รวมทั้งตระหนักถึงความเสี่ยงสำคัญที่ส่งผลกระทบในเชิงลบต่อหน่วยงานได้อย่างครบถ้วน ซึ่งครอบคลุมความเสี่ยงที่มีเหตุทั้งจากปัจจัยภายในหน่วยงาน (เช่น วัฒนธรรม โครงสร้างองค์กร และบุคลากร เป็นต้น) และจากปัจจัยภายนอกหน่วยงาน (เช่น การเมือง สภาวะเศรษฐกิจ และระบบเทคโนโลยีสารสนเทศ เป็นต้น)

๔. เป็นเครื่องมือที่สำคัญในการบริหารงาน การบริหารความเสี่ยงเป็นเครื่องมือที่ช่วยให้ผู้บริหารสามารถมั่นใจได้ว่าความเสี่ยงได้รับการจัดการอย่างเหมาะสมและทันเวลา รวมทั้งเป็นเครื่องมือที่สำคัญของผู้บริหารในการบริหารงานและการตัดสินใจในด้านต่างๆ เช่น การวางแผน การกำหนดกลยุทธ์ การติดตามควบคุมและวัดผลการปฏิบัติงาน ซึ่งส่งผลให้การดำเนินงานของหน่วยงานเป็นไปตามเป้าหมายที่กำหนด และสามารถปกป้องผลประโยชน์รวมทั้งเพิ่มมูลค่าแก่หน่วยงาน

๕. ช่วยให้การพัฒนาหน่วยงานเป็นไปในทิศทางเดียวกัน การบริหารความเสี่ยงทำให้รูปแบบการตัดสินใจในระดับการปฏิบัติงานของหน่วยงานมีการพัฒนาไปในทิศทางเดียวกัน เช่น การตัดสินใจโดยที่ผู้บริหารมีความเข้าใจในกลยุทธ์ วัตถุประสงค์ของหน่วยงาน และระดับความเสี่ยงอย่างชัดเจน

๖. ช่วยให้การพัฒนาการบริหารและจัดสรรทรัพยากรเป็นไปอย่างมีประสิทธิภาพและประสิทธิผล การจัดสรรทรัพยากรเป็นไปอย่างเหมาะสม โดยพิจารณาถึงระดับความเสี่ยงในแต่ละกิจกรรม และการเลือกใช้มาตรการในการบริหารความเสี่ยง เช่น การใช้ทรัพยากรสำหรับกิจกรรมที่มีความเสี่ยงต่ำและกิจกรรมที่มีความเสี่ยงสูงย่อมแตกต่างกัน หรือการเลือกใช้มาตรการแต่ละประเภทย่อมใช้ทรัพยากรแตกต่างกัน เป็นต้น

๔. กระบวนการบริหารความเสี่ยงด้านสารสนเทศ

๔.๑ ความหมายของการบริหารความเสี่ยง

ความเสี่ยง (Risk) หมายถึง เหตุการณ์ที่มีโอกาสเกิดขึ้นได้และทำให้เกิดความเสียหายต่อสินทรัพย์สารสนเทศของหน่วยงาน เช่น ไวรัสทำให้ข้อมูลเสียหาย ข้อมูลสำคัญถูกเข้าถึงโดยไม่ได้รับอนุญาต

ระดับความเสี่ยงที่ยอมรับได้ (Risk appetite หรือ Acceptable level of risk) หมายถึง ความเสี่ยงที่หากการประเมินเหตุการณ์ความเสี่ยงหนึ่ง และพบว่ามีความเสี่ยงเกินกว่าระดับความเสี่ยงที่ยอมรับได้ผู้ประเมินความเสี่ยงจะต้องนำเสนอแผนการจัดการดังกล่าวต่อหัวหน้างานหรือผู้บังคับบัญชา

แผนการลดความเสี่ยง (Treatment Plan) หมายถึง แผนการจัดการกับเหตุการณ์ความเสี่ยง สำหรับกรณีที่ผู้ประเมินความเสี่ยงได้ประเมินเหตุการณ์ความเสี่ยงหนึ่งและพบว่ามีความเสี่ยงเกินกว่าระดับความเสี่ยงที่ยอมรับได้ ผู้ประเมินความเสี่ยงจะต้องนำเสนอแผนการจัดการดังกล่าวต่อหัวหน้างานหรือ ผู้บังคับบัญชาเพื่อพิจารณาอนุมัติดำเนินการ

ปัจจัยเสี่ยง (Risk Factor) หมายถึง ต้นเหตุหรือสาเหตุที่มาของความเสี่ยงที่จะทำให้วัตถุประสงค์ที่กำหนดไว้ โดยต้องระบุได้ด้วยว่าเหตุการณ์นั้นจะเกิดที่ไหน เมื่อใดและจะเกิดขึ้นได้อย่างไรและทำไม ทั้งนี้สาเหตุของความเสี่ยงที่ระบุควรเป็น สาเหตุที่แท้จริง เพื่อจะได้วิเคราะห์และกำหนดมาตรการความเสี่ยงในภายหลังได้อย่างถูกต้อง

๔.๒ กรอบการบริหารความเสี่ยงตามแนวทาง COSO

การบริหารความเสี่ยงตามแนวทางหรือมาตรฐาน COSO (Committee of Sponsoring Organization of the Tread way Commission) ใช้หลักการบริหารความเสี่ยงทั่วทั้งองค์กร (Enterprise Risk Management : ERM) คือ กระบวนการที่ได้รับอิทธิพลมาจากคณะกรรมการของกระทรวงสาธารณสุข ผู้บริหาร และบุคลากร เป็นกระบวนการที่จะถูกนำมาเพื่อให้สามารถระบุเหตุการณ์อันอาจเกิดขึ้นและส่งผลกระทบต่อองค์กร เพื่อจัดการความเสี่ยงให้อยู่ภายในระดับความเสี่ยงที่องค์กรยอมรับได้ (Risk appetite) การบริหารความเสี่ยงขององค์กรจะทำให้เกิดความเชื่อมั่นได้อย่างสมเหตุสมผลเกี่ยวกับการบรรลุวัตถุประสงค์ขององค์กร

ประโยชน์ของ Enterprise Risk Management : ERM

๑. จัดให้กลยุทธ์ต่างๆ เข้ากันได้กับระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite)

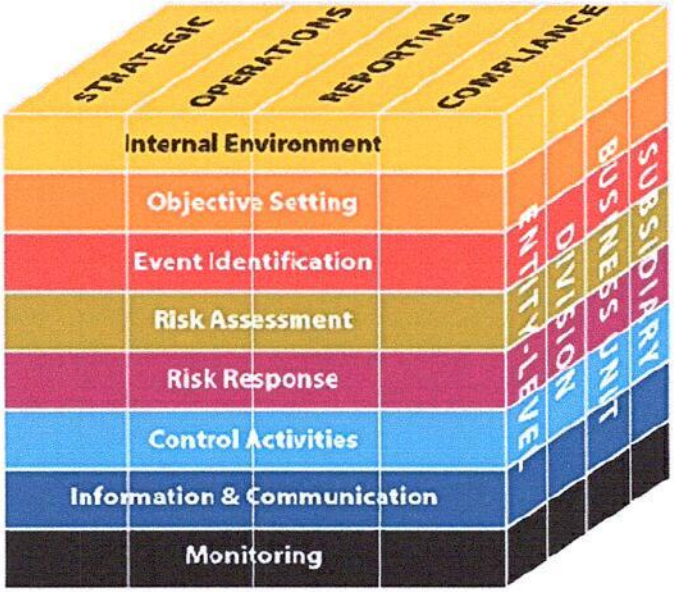
๒. ช่วยให้การตัดสินใจในเรื่องการโต้ตอบกับความเสี่ยงทำได้ดีขึ้น

๓. ลดสิ่งที่ไม่คาดฝันและความสูญเสียที่จะเกิดในการดำเนินงาน

๔. ทำให้การระบุและจัดการความเสี่ยงที่ต่อเนื่อง กันหรือคาบเกี่ยวอย่างทั่วถึงทุกระดับ

๕. การมองถึงเหตุการณ์ในอนาคตที่อาจเกิดขึ้นได้ ทำให้อาจมองเห็นโอกาส และฉวยโอกาส นั้นอย่างเชิงรุกได้

๖. การบริหารและใช้ทรัพยากรได้อย่างเหมาะสม มีประสิทธิภาพและประสิทธิผล



วัตถุประสงค์ของ Enterprise Risk Management : ERM

๑. ด้านกลยุทธ์ (Strategic): เกี่ยวกับการกำหนดเป้าหมายในระดับสูง ซึ่งต้องเป็นแนวทางเดียวกันและต้องสนับสนุนวัตถุประสงค์ขององค์กร

๒. ด้านการปฏิบัติการ (Operations): มีการใช้ทรัพยากรขององค์กรอย่างมีประสิทธิภาพและประสิทธิผล

๓. ด้านการรายงาน (Reporting): การรายงาน (รายงานด้านการเงิน และไม่ใช่ด้านการเงิน) ขององค์กรมีความน่าเชื่อถือ

๔. ด้านการปฏิบัติตามข้อกำหนด (Compliance): องค์กรได้ปฏิบัติตามข้อกำหนด หรือกฎหมายระเบียบต่างๆ ที่ใช้องค์กร

องค์ประกอบหลักของ ERM

๑. สภาพแวดล้อมภายในองค์กร (Internal Environment)

๒. การกำหนดวัตถุประสงค์ (Objective Setting)

๓. การระบุเหตุการณ์ (Event Identification)

๔. การประเมินความเสี่ยง (Risk Assessment)

๕. กลยุทธ์ที่ใช้ในการจัดการความเสี่ยง (Risk Response)

๖. กิจกรรมการควบคุม (Control Activities)

เป็นนโยบายและวิธีการต่างๆ ที่กำหนดขึ้นและนำไปปฏิบัติ เพื่อช่วยก่อให้เกิดความเชื่อมั่นได้ว่ามีการดำเนินการกับความเสี่ยงได้อย่างเหมาะสม ซึ่งกิจกรรมการควบคุมสามารถจัดกลุ่มได้ตามลักษณะของวัตถุประสงค์ขององค์กร ทั้งวัตถุประสงค์ด้านกลยุทธ์ ด้านการปฏิบัติงาน ด้านการรายงาน และด้านการปฏิบัติตามกฎระเบียบ

๗. สารสนเทศและการสื่อสาร (information and Communication) ต้องระบุสารสนเทศที่จำเป็น รับทราบได้ และสื่อสารไปยังบุคลากรในองค์กร รูปแบบ และช่วงเวลาที่เหมาะสมเพื่อให้บุคคลกรปฏิบัติหน้าที่ของตนได้

๘. การติดตามประเมินผล (Monitoring) มีการติดตามประเมินผลการบริหารความเสี่ยงแบบครบวงจร และมีการปรับแก้ตามความเหมาะสมซึ่งการประเมินอาจทำได้ทั้งขณะดำเนินงานอยู่ (Ongoing Monitoring Activities) หรือการประเมินแยกต่างหาก (Separate Evaluations) หรือทั้ง ๒ แบบ

๔.๔ กระบวนการในการบริหารความเสี่ยง

ขั้นตอนการดำเนินการ หลักเกณฑ์ในการวิเคราะห์ ประเมิน และการจัดการความเสี่ยงอย่างเหมาะสมตามกระบวนการบริหารความเสี่ยงตามมาตรฐาน COSO (The Committee of Sponsoring Organizations of the Tread way Commission) มี ๗ ขั้นตอน ดังนี้

ขั้นตอนที่ ๑ การกำหนดเป้าหมายการบริหารความเสี่ยง (Objective Setting)

การกำหนดวัตถุประสงค์การดำเนินการบริหารความเสี่ยง เป็นการกำหนดเป้าหมายการบริหารความเสี่ยง โดยมีการกำหนดหลักเกณฑ์การพิจารณาคัดเลือกโครงการ และการวิเคราะห์รายละเอียดโครงการ ทั้งนี้ การกำหนดวัตถุประสงค์ การบริหารความเสี่ยงขึ้นนั้น เพื่อต้องการให้โครงการสำคัญที่มีนัยสำคัญต่อการบรรลุความสำเร็จตามประเด็นยุทธศาสตร์สามารถดำเนินการได้บรรลุเป้าหมายตามที่ตั้งไว้ ซึ่งจะส่งผลให้บรรลุความสำเร็จตามกลยุทธ์ เป้าประสงค์ของประเด็นยุทธศาสตร์ ทั้งนี้ การกำหนดวัตถุประสงค์ของการบริหารความเสี่ยง กำหนดจาก

๑. วิสัยทัศน์และภารกิจขององค์กร

๒. จากเป้าหมายหลักองค์กรให้สอดคล้องกับภารกิจ

๓. เป้าหมายในระดับหน่วยงาน

๔. เป้าหมายของแผนงานโครงการและกิจกรรมที่ทำให้บรรลุเป้าหมายในระดับองค์กรนอกจากนี้วัตถุประสงค์ที่จะ SMART ควรจะ

๑. **Specific** (เฉพาะเจาะจง) มีความชัดเจนและกำหนดผลตอบแทน หรือผลลัพธ์ที่ต้องการที่ทุกคนสามารถเข้าใจได้อย่างชัดเจน

๒. **Measurable** (สามารถวัดได้) สามารถวัดผลการบรรลุวัตถุประสงค์ได้

๓. **Achievable** (สามารถบรรลุผลได้) มีความเป็นไปได้ที่จะบรรลุวัตถุประสงค์ภายใต้เงื่อนไขการใช้ทรัพยากรที่มีอยู่ในปัจจุบัน

๔. **Relevant** (มีความเกี่ยวข้อง) มีความสอดคล้องกับกลยุทธ์และเป้าหมายในการดำเนินงานขององค์กร

๕. **Timeless** (มีกำหนดเวลา) สามารถกำหนดระยะเวลาที่ต้องการบรรลุผล

ขั้นตอนที่ ๒ การระบุความเสี่ยง (Event Identification)

วิธีการระบุความเสี่ยง (Risk Identification) พิจารณาจากข้อมูลภายใน ได้แก่ ความถี่ และความรุนแรงของความสูญเสียในอดีต และการดำเนินงานที่ผ่านมา รวมทั้งการพิจารณาจากข้อมูลภายนอก ได้แก่ ความสูญเสียขององค์การอื่นที่คล้ายคลึงกัน เศรษฐกิจ หรือการเมือง ฯลฯ

ประเภทความเสี่ยง มีดังนี้

ความเสี่ยงด้านกลยุทธ์ (Strategic Risk : S) เกี่ยวข้องกับการบรรลุเป้าหมาย และพันธกิจในภาพรวมโดยความเสี่ยงที่อาจจะเกิดขึ้นเป็นความเสี่ยงเนื่องจาก

๑) การเปลี่ยนแปลงสถานการณ์และเหตุการณ์ภายนอก ส่งผลกลยุทธ์ที่กำหนดไว้ไม่สอดคล้องกับประเด็นยุทธศาสตร์ วิสัยทัศน์

๒) การกำหนดกลยุทธ์ที่ขาดการมีส่วนร่วมจากภาคประชาชน หรือการร่วมมือกับองค์กรอิสระ ทำให้โครงการขาดการยอมรับและโครงการไม่ได้นำไปสู่การแก้ไขปัญหา หรือการตอบสนองต่อความต้องการของผู้รับบริการ หรือผู้มีส่วนได้ส่วนเสียอย่างแท้จริง

๓) เป็นความเสี่ยงที่เกิดขึ้นจากการตัดสินใจผิดพลาด หรือการนำการตัดสินใจมาใช้ไม่ถูกต้อง

ความเสี่ยงด้านการดำเนินการ (Operational Risk : O) เกี่ยวข้องกับประสิทธิภาพ ประสิทธิผล หรือผลการปฏิบัติงานโดยความเสี่ยงที่เกิดขึ้นเป็นความเสี่ยงเนื่องจากระบบงานภายในองค์กร/กระบวนการ/เทคโนโลยี หรือนวัตกรรมที่ใช้/บุคลากร/ความเพียงพอของข้อมูล ส่งผลต่อประสิทธิภาพและประสิทธิผลในการดำเนินโครงการ

ความเสี่ยงด้านการเงิน (Financial Risk : F) เป็นความเสี่ยงเกี่ยวกับการบริหารงบประมาณและการเงินเช่น การบริหารการเงินไม่ถูกต้อง ไม่เหมาะสม ทำให้ขาดประสิทธิภาพและไม่ทันต่อสถานการณ์ หรือเป็นความเสี่ยงที่เกี่ยวข้องกับการเงินขององค์การ เช่น การประมาณการงบประมาณไม่เพียงพอ และไม่สอดคล้องกับขั้นตอนการดำเนินงาน เป็นต้น เนื่องจากขาดการจัดหาข้อมูล การวิเคราะห์ การควบคุม และการจัดทำรายงานเพื่อนำมาใช้ในการบริหารงบประมาณและการเงิน

ความเสี่ยงด้านการปฏิบัติตามกฎหมาย/กฎระเบียบ (Compliance Risk : C) เกี่ยวข้องกับการปฏิบัติตามกฎระเบียบต่าง ๆ โดยความเสี่ยงที่อาจเกิดขึ้นเป็นความเสี่ยง เนื่องจากความไม่ชัดเจน ความไม่ทันสมัย หรือความไม่ครอบคลุมของกฎหมาย กฎระเบียบ ข้อบังคับต่างๆ รวมทั้งนิติกรรมต่างๆ รวมทั้งการทำนิติกรรมสัญญา การร่างสัญญาไม่ครอบคลุมการดำเนินงาน

ขั้นตอนที่ ๓ การประเมินความเสี่ยง (Risk Assessment)

โอกาสที่จะเกิดความเสียหายต่อองค์กร คือ การพิจารณาปัจจัยเสี่ยงแต่ละปัจจัยว่ามีโอกาสที่จะเกิดขึ้นในระดับมากน้อยเพียงใด

ความเสียหายที่จะกระทบต่อองค์กร คือ การพิจารณาปัจจัยเสี่ยงแต่ละปัจจัยว่าหากเกิดขึ้นแล้วมีผลกระทบต่อหน่วยงานมากน้อยแค่ไหน

ความสำคัญของความเสี่ยงที่องค์กรเผชิญอยู่ คือ การลำดับความสำคัญของแต่ละปัจจัยเสี่ยง เพื่อพิจารณาว่าความเสี่ยงใดควรพิจารณาจัดการก่อนหลัง

การประเมินความเสี่ยงประกอบด้วย

๑) มีการกำหนดหลักเกณฑ์การประเมินความเสี่ยง (ความรุนแรง x โอกาส)

๒) ประเมินความเสี่ยงตามหลักเกณฑ์ความรุนแรงและโอกาส

๓) กำหนดกลยุทธ์ที่ใช้ในการจัดการความเสี่ยงและแนวทางการจัดการความเสี่ยง

๔) การจัดทำแผนภูมิความเสี่ยง เพื่อช่วยให้สามารถตัดสินใจในการวางแผนบริหารความเสี่ยงได้อย่างเหมาะสม และสามารถเห็นภาพว่าเมื่อรวมทุกปัจจัยเสี่ยงแล้ว ปัจจัยเสี่ยงใดควรได้รับการจัดการก่อนหลัง โอกาสที่จะเกิดความเสียหายต่อองค์กร และความเสียหายที่จะกระทบต่อองค์กรพิจารณาได้ ๒ ลักษณะ คือ

๑. วิธีการประเมินความเสี่ยงเชิงคุณภาพ (Qualitative Approach) ซึ่งจะไม่มีการระบุค่าของความเสียหายออกมาเป็นตัวเลข แต่ระบุออกเป็นระดับความรุนแรงของความเสียหาย และระดับของความเป็นไปได้ที่เหตุการณ์จะเกิดขึ้น

๒. วิธีการประเมินความเสี่ยงเชิงปริมาณ (Quantitative Approach) ซึ่งจะต้องระบุค่าของความเสียหายออกมาเป็นตัวเลข (โดยเฉพาะเป็นตัวเงิน) และโอกาสที่เหตุการณ์นั้นจะเกิดออกมาในรูปของความน่าจะเป็น (Probability)

การประเมินความเสี่ยงด้านสารสนเทศ

การประเมินความเสี่ยงด้านสารสนเทศทางการแพทย์ โรงพยาบาลพระอาจารย์มั่น ภูริทัตโต ได้ประเมินความเสี่ยงที่เกิดจากบุคคล จากทางด้านเทคนิค และจากภัยพิบัติหรือสถานการณ์อื่นๆ เป็นแนวทางในการดำเนินงาน โดย โรงพยาบาลพระอาจารย์มั่น ภูริทัตโต ได้ประเมินสถานการณ์ความเสี่ยงด้านสารสนเทศของงานสารสนเทศทางการแพทย์ ปรากฏ ดังนี้

ความเสี่ยง	ความสูญเสียที่คาดว่าจะเกิดขึ้น	โอกาส	ผลกระทบ	ระดับความเสี่ยง	ผลประเมินระดับความเสี่ยง	แนวทางการแก้ไข
ความเสี่ยงที่เกิดจากบุคคล (People)						
เหตุการณ์หรือภัยที่เกิดจากบุคลากร ภายในโรงพยาบาลพระอาจารย์มั่น ภูริทัตโต	- ระบบคอมพิวเตอร์ติดไวรัส หรือหนอนอินเตอร์เน็ตจากอินเตอร์เน็ต หรือไฟล์ที่คัดลอกจากอุปกรณ์ บันทึกข้อมูลแบบพกพา เช่น Flash Driver และ External Harddisk,Storage ส่งผลให้ระบบคอมพิวเตอร์และระบบสารสนเทศประมวลผล ข้อมูลได้ช้าลงหรืออาจทำงานผิดพลาดได้	๓	๓	๙	ค่อนข้างสูง	-ผู้ดูแลระบบ(System Administrator) ตัดการเชื่อมต่อเครื่องที่ติดไวรัสดังกล่าว ออกจากระบบเครือข่าย ภายใน และดำเนินการสแกนไวรัสเพื่อกำจัดไวรัสเครื่องดังกล่าว -หากไวรัสดังกล่าวไม่หายไป ให้ดำเนินการสแกนไวรัสที่เครื่องคอมพิวเตอร์แม่ข่าย (Server)
เหตุการณ์หรือภัย ที่เกิดจากผู้ไม่ประสงค์ดี	-ระบบคอมพิวเตอร์และระบบสารสนเทศอาจถูกบุกรุกโจมตี หรือถูกขโมยข้อมูลสารสนเทศ หรือปรับแต่งแก้ไขระบบหน้าเว็บไซต์ ซึ่งอาจส่งผลให้ระบบคอมพิวเตอร์ และระบบสารสนเทศล่มได้	๑	๓	๓	ต่ำ	ตรวจสอบพอร์ตทั้งหมดที่ใช้เชื่อมต่อแล้วให้ปิดพอร์ตที่ไม่ใช้งาน โดยทันที
ความเสี่ยงที่เกิดจากกระบวนการ (Process)						
เหตุการณ์หรือภัย ที่เกิดจากการโจรกรรมอุปกรณ์ประมวลผล (Process Device)	-อุปกรณ์ประมวลผลข้อมูล (Process Device) สูญหาย และอาจเสี่ยงต่อการถูกโจรกรรมข้อมูลบนอุปกรณ์ประมวลผลข้อมูล (Process Device) ซึ่งส่งผลกระทบต่อ โรงพยาบาล ระบบปรับอากาศชำรุดส่งผลให้อุณหภูมิ ในห้องServer และสารสนเทศสูงขึ้นทำให้อุปกรณ์ประมวลผลข้อมูล	๑	๓	๓	ต่ำ	-ผู้พบเหตุแจ้งให้หัวหน้ากลุ่มงานสุขภาพดิจิทัล ทราบเพื่อรายงานตามลำดับขั้นและสั่งการต่อไป -ผู้ดูแลระบบ(System Administrator) ตรวจสอบความครบถ้วนและความเสียหายและระบบ ปรับอากาศ พร้อมทั้งรายงานให้ หัวหน้างาน ทราบ เพื่อสั่งการต่อไป

ความเสี่ยง	ความสูญเสียที่คาดว่าจะเกิดขึ้น	โอกาส	ผลกระทบ	ระดับความเสี่ยง	ผลประเมินระดับความเสี่ยง	แนวทางการแก้ไข
	(Process Device) ได้รับความเสียหาย					- หัวหน้างาน ประชาสัมพันธ์ให้กับ บุคลากรได้รับทราบถึงการหยุดให้บริการชั่วคราว - หัวหน้างาน ประสานงานกับกลุ่มงานสุขภาพดิจิทัล เพื่อสอบถามปัญหา และระยะเวลา การแก้ไขที่จะสามารถกลับมาให้บริการ -ผู้ดูแลระบบ(System Administrator) เปิดการใช้งานระบบคอมพิวเตอร์ และระบบสารสนเทศ รวมทั้งรายงานให้ หัวหน้างาน และผู้บริหารทราบตามลำดับ -หัวหน้างานประชาสัมพันธ์ให้กับบุคลากรได้รับทราบว่าระบบคอมพิวเตอร์และระบบสารสนเทศ สามารถกลับมาใช้งานได้ปกติ
	เหตุการณ์อัคคีภัย - สินทรัพย์ (Asset) ที่ย้ายไม่ทันอาจถูกไฟไหม้ - อุปกรณ์ประมวลผลข้อมูล (Process Device) ภายในห้องเซิร์ฟเวอร์ ไม่สามารถให้บริการได้	๑	๓	๓	ต่ำ	แนวทางการปฏิบัติตามแผนป้องกันและระงับอัคคีภัยในการรักษาความมั่นคงปลอดภัยสารสนเทศ <u>กรณีที่ ๑</u> ไฟเริ่มไหม้หรือสามารถดับไฟได้ -ให้ผู้พบเหตุนำถังดับเพลิงฉีดบริเวณที่เป็นต้นเพลิงของไฟไหม้จนไฟดับ - ผู้พบเหตุรายงานให้ผู้อำนวยการทราบโดยเร็ว -ผู้ดูแลระบบ (System Administrator) ประเมินสถานการณ์ในเบื้องต้นว่า ควรหยุดให้บริการระบบคอมพิวเตอร์ และระบบสารสนเทศหรือไม่ - ถ้าหยุดให้บริการ หัวหน้างาน สั่งการให้กับบุคลากรได้รับทราบถึงการหยุดให้บริการ ชั่วคราวเนื่องจากเหตุไฟไหม้ -ผู้ดูแลระบบ (System Administrator) ตรวจสอบความเสียหาย ผลกระทบและความพร้อมใช้งานของอุปกรณ์ประมวลผลข้อมูล (Process Device)

ความเสี่ยง	ความสูญเสียที่คาดว่าจะเกิดขึ้น	โอกาส	ผลกระทบ	ระดับความเสี่ยง	ผลประเมินระดับความเสี่ยง	แนวทางการแก้ไข
						ระบบปรับอากาศ และสภาพภายในห้องเซิร์ฟเวอร์ พร้อมทั้งรายงานให้ผู้อำนวยการ หัวหน้างาน ทราบตามลำดับชั้นและสั่งการต่อไป -หากเสียหายเล็กน้อยให้ผู้ดูแลระบบ(System Administrator) ดำเนินการแก้ไข และเปิดการใช้งานระบบคอมพิวเตอร์ และระบบสารสนเทศ -หัวหน้า ประชาสัมพันธ์ให้กับบุคลากรได้รับทราบว่า ระบบคอมพิวเตอร์และระบบสารสนเทศ สามารถกลับมาใช้งานได้แล้ว -หากเสียหายมากให้ผู้ดูแลระบบ(System Administrator) รายงานให้หัวหน้ากลุ่มงานสุขภาพดิจิทัลทราบ ตามลำดับชั้นและสั่งการต่อไป <u>กรณีที่ ๒</u> ไฟไหม้เริ่มลุกลามถึงขั้นรุนแรง - ให้ผู้พบเหตุโทรแจ้งหน่วยดับเพลิง เป็นลำดับแรก และแจ้งให้ หัวหน้ากลุ่มงานสุขภาพดิจิทัลทราบโดยเร็ว - ผู้พบเหตุนำถังดับเพลิงฉีดบริเวณไฟที่เริ่มลุกลาม และบริเวณโดยรอบ หากไม่สามารถระงับเหตุได้ ให้ออกจากพื้นที่โดยเร็ว -หัวหน้างาน ประชาสัมพันธ์ให้กับบุคลากรได้รับทราบถึงการหยุด ให้บริการเนื่องจากเหตุไฟไหม้
	เหตุการณ์ที่เกิดจาก ภัยพิบัติหรือสถานการณ์อื่นๆ เช่น อุทกภัย วาตภัย และการชุมนุมประท้วง หรือความไม่สงบเรียบร้อยทางการเมือง - เช่น กรณีการชุมนุมประท้วง หรือความไม่สงบเรียบร้อยทางการเมืองอาจถูกปิดกั้นการเข้า	๑	๒	๒	ต่ำ	- หากสามารถระงับเหตุได้ ให้ผู้ดูแลระบบ (System Administrator)ตรวจสอบความเสียหาย ผลกระทบ และความพร้อมใช้งานของอุปกรณ์ประมวลผลข้อมูล (Process Device)ระบบปรับอากาศ และสภาพภายในห้องเซิร์ฟเวอร์ รายงานให้หัวหน้ากลุ่มงาน

ความเสี่ยง	ความสูญเสียที่คาดว่าจะเกิดขึ้น	โอกาส	ผลกระทบ	ระดับความเสี่ยง	ผลประเมินระดับความเสี่ยง	แนวทางการแก้ไข
	ออกและอาจเสี่ยงต่อการถูกตัดไฟฟ้า/น้ำบริเวณโรงพยาบาล					สุขภาพดิจิทัลทราบ ตามลำดับชั้นและสั่งการต่อไป - หากไม่สามารถระงับเหตุได้ ให้ผู้ดูแลระบบ (System Administrator)รายงานให้หัวหน้ากลุ่มงานสุขภาพดิจิทัลทราบ ตามลำดับชั้นและสั่งการต่อไป - ถ้าเกิดเหตุการณ์ไฟฟ้าดับ ให้ดำเนินการตามแนวทางแก้ไข - กำหนดให้ผู้ใช้งาน (User) ปฏิบัติงานจากสถานที่ปฏิบัติงานสำรองหรือที่พักอาศัย
ทรัพย์สินครุภัณฑ์ระบบปฏิบัติการด้านเทคโนโลยี (Hardware, Software)	-ไม่เพียงพอต่อการใช้งาน -ไม่พร้อมใช้งาน	๓	๓	๙	**ค่อนข้างสูง**	-จัดทำแผนคุมทะเบียนทรัพย์สินตามระเบียบพัสดุ สำรวจ จัดซื้อ/จัดหา ให้พร้อมใช้งานตามแผนที่กำหนด - กำหนดแนวทางการควบคุม กำกับ ติดตาม ประเมินการใช้งาน การเข้ารหัส ในระบบเครื่องคอมพิวเตอร์ให้ครบทุกเครื่อง - ปรับปรุงระบบการยืม-คืน เมื่อนำอุปกรณ์ระบบคอมพิวเตอร์ไปใช้นอกสำนักงาน - ประกาศใช้นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
โครงข่ายการสื่อสาร (Communication Network)	-ไม่เพียงพอต่อการใช้งาน -ไม่พร้อมใช้งาน	๓	๓	๙	**ค่อนข้างสูง**	- กำหนดแนวทางการควบคุม กำกับ ติดตาม ประเมินการใช้งาน การเข้ารหัส ในระบบเครื่องคอมพิวเตอร์ให้ครบทุกเครื่อง - ประกาศใช้นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ความเสี่ยง	ความสูญเสียที่คาดว่าจะเกิดขึ้น	โอกาส	ผลกระทบ	ระดับความเสี่ยง	ผลประเมินระดับความเสี่ยง	แนวทางการแก้ไข
ข้อมูลและสารสนเทศ (Information)		๒	๒	๔	**ค่อนข้างต่ำ**	- กำหนดแนวทางการควบคุม กำกับ ติดตาม ประเมินการใช้งาน การเข้ารหัส - ประกาศใช้นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

หมายเหตุ เกณฑ์การประเมินการให้คะแนนโอกาสที่จะเกิดและผลกระทบ

ระดับ ๑ = รุนแรงน้อยที่สุด / โอกาสเกิดน้อยที่สุด
ระดับ ๒ = รุนแรงน้อย / โอกาสเกิดน้อย
ระดับ ๓ = รุนแรงปานกลาง / โอกาสเกิดปานกลาง
ระดับ ๔ = รุนแรงมาก / โอกาสเกิดมาก
ระดับ ๕ = รุนแรงมากที่สุด / โอกาสเกิดมากที่สุด

แผนผังประเมินความเสี่ยง

ผลกระทบของความเสี่ยง

๕	๑๐	๑๕	๒๐	๒๕
๔	๘	๑๒	๑๖	๒๐
๓	๖	๙	๑๒	๑๕
๒	๔	๖	๘	๑๐
๑	๒	๓	๔	๕

สีแดง ระดับความเสี่ยงสูง ค่าระหว่าง ๑๕ - ๒๕

สีเหลือง ระดับความเสี่ยงค่อนข้างสูง ค่าระหว่าง ๘ - ๑๔

สีเขียว ระดับความเสี่ยงค่อนข้างต่ำ ค่าระหว่าง ๔ - ๗

สีฟ้า ระดับความเสี่ยงต่ำ ค่าระหว่าง ๑ - ๓

๖. การเตรียมความพร้อมกรณีฉุกเฉินในสภาวะวิกฤต

เนื่องจากเหตุการณ์ที่เป็นความเสี่ยงด้านสารสนเทศทางการแพทย์ข้างต้น โรงพยาบาลพระอาจารย์มั่น ภูริทัตโต จึงได้ดำเนินการจัดทำแนวทางการเตรียมความพร้อมกรณีฉุกเฉินในสภาวะวิกฤต เพื่อป้องกันภัยจากเหตุการณ์หรือภัยที่จะเกิดขึ้น ดังนี้

๖.๑ เหตุการณ์หรือภัยที่เกิดจากบุคลากร (People)

๖.๑.๑ เหตุการณ์หรือภัยที่เกิดจากบุคลากรของโรงพยาบาลพระอาจารย์มั่น ภูริทัตโต มีแนวปฏิบัติเพื่อเตรียมรับสถานการณ์ ดังนี้

(๑) กำหนดให้ปฏิบัติตามประกาศกระทรวงสาธารณสุข เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ.๒๕๖๗

(๒) การสร้างความรู้ความเข้าใจในการใช้ระบบคอมพิวเตอร์และระบบสารสนเทศเบื้องต้นเพื่อลดความเสี่ยงด้านสารสนเทศ

(๓) มีการประชาสัมพันธ์ให้ความรู้แก่บุคลากรผ่านช่องทางสื่อสารต่าง ๆ ตามความเหมาะสม เช่น ผ่านระบบ Website ติดบอร์ดประชาสัมพันธ์ Line, Chat, Facebook หรือสื่อ Social Media อื่น ๆ เป็นต้น

๖.๑.๒ เหตุการณ์หรือภัยที่เกิดจากบุคคลภายนอกผู้ไม่ประสงค์ดี มีแนวปฏิบัติเพื่อเตรียมรับสถานการณ์ ดังนี้

(๑) ติดตั้งและใช้งาน Firewall เพื่อป้องกันการบุกรุกจากผู้ไม่ประสงค์ดีต่อระบบคอมพิวเตอร์ และระบบสารสนเทศ ข้อมูลสารสนเทศ และอุปกรณ์ประมวลผลข้อมูล (Process Device)

(๒) ติดตั้งซอฟต์แวร์ป้องกันไวรัส (Anti-Virus) / หนอนคอมพิวเตอร์ (Worm) หรือโปรแกรมไม่ประสงค์ดี (Anti-Malware) ที่เครื่องคอมพิวเตอร์แม่ข่าย (Server) และเครื่องคอมพิวเตอร์ลูกข่าย (Client)

๖.๒ เหตุการณ์หรือภัยที่เกิดจากกระบวนการ (Process)

๖.๒.๑ การโจรกรรมอุปกรณ์ประมวลผลข้อมูล (Process Device มีแนวปฏิบัติเพื่อเตรียมรับสถานการณ์ ดังนี้

(๑) มีมาตรการควบคุมการเข้า – ออกห้องเซิร์ฟเวอร์ ดังนี้

(๑.๑) ปฏิบัติตามหลักเกณฑ์สำหรับการปฏิบัติงานภายในห้องเซิร์ฟเวอร์ ตามที่โรงพยาบาลได้กำหนด

(๑.๒) การติดตั้ง ซ่อมแซม และนำอุปกรณ์ใดๆ ออกจากห้องเซิร์ฟเวอร์ ต้องได้รับอนุมัติจากหัวหน้ากลุ่มงานสุขภาพดิจิทัล ก่อนเริ่มดำเนินการทุกครั้ง

(๑.๓) ห้ามผู้ที่ไม่มีส่วนเกี่ยวข้องเข้าไปในห้องเซิร์ฟเวอร์ เว้นแต่ได้รับอนุญาตจากหัวหน้ากลุ่มงานสุขภาพดิจิทัล

(๑.๔) ผู้ใช้งาน (User) หรือบุคคลภายนอก

(๑.๔.๑) ต้องติดบัตรแสดงตนตลอดระยะเวลา ที่ปฏิบัติงาน โดยมีผู้ดูแลระบบ

(๑.๔.๒) ต้องไม่นำอาหารหรือเครื่องดื่มเข้าไปในห้องเซิร์ฟเวอร์

(๑.๔.๓) ห้ามสูบบุหรี่ ในห้องเซิร์ฟเวอร์

(๑.๕) มีการติดตั้งกล้องวงจรปิดบันทึกเหตุการณ์บริเวณทางเข้าและภายในห้องเซิร์ฟเวอร์ เพื่อเฝ้าระวังเหตุการณ์หรือภัยที่จะเกิดขึ้น

๖.๒.๒ เหตุการณ์หรือภัยที่เกิดจากด้านเทคนิค มีแนวปฏิบัติเพื่อเตรียมรับสถานการณ์ ดังนี้

(๑) มีการตรวจความพร้อมอุปกรณ์ประมวลผลข้อมูล (Process Device) ทั้งทางกายภาพและด้านเทคนิคให้พร้อมใช้งานอยู่เสมออย่างน้อยเดือนละ ๑ ครั้ง หากพบอุปกรณ์ประมวลผลข้อมูล (Process Device) หรืออุปกรณ์ภายในห้องเซิร์ฟเวอร์ชำรุดเสียหาย หรือใกล้เสื่อมสภาพการใช้งานให้รายงานหัวหน้ากลุ่มงานสุขภาพดิจิทัลทราบ เพื่อรายงานตามลำดับชั้นและสั่งการแก้ไข ด้วยการซ่อมแซมหรือจัดซื้อ ทดแทนต่อไป

(๒) มีการตรวจสอบปริมาณการเข้าถึงเครือข่ายภายนอก (Internet) เพื่อสังเกตปริมาณการใช้งานอัตราความเร็วของข้อมูล เพื่อเฉลี่ยแบนด์วิดท์ (Bandwidth) ให้ทั่วถึงทั้งองค์กร และป้องกัน ไม่ให้ผู้ใช้งาน (User) มีการใช้แบนด์วิดท์ (Bandwidth) มากเกินไป

๖.๒.๓ เหตุการณ์ไฟฟ้าดับ มีแนวปฏิบัติเพื่อเตรียมรับสถานการณ์ ดังนี้

มีการติดตั้งเครื่องสำรองไฟฟ้า (APC) จำนวน ๒ เครื่องขนาด ๑,๐๐๐ VA ๖๐๐ W เพื่อควบคุมการจ่ายกระแสไฟฟ้าและป้องกันความเสียหายที่อาจเกิดขึ้นกับระบบคอมพิวเตอร์และระบบสารสนเทศ รวมถึงอุปกรณ์ประมวลผลข้อมูล (Process Device) โดยทั้ง ๒ เครื่อง สามารถสำรองไฟฟ้า ได้เป็นเวลาประมาณ ๒๐ นาที ซึ่งเพียงพอต่อการจัดเก็บและสำรองข้อมูลสารสนเทศในกรณีที่เกิดไฟฟ้าดับ

๖.๒.๔ เหตุการณ์อัคคีภัย มีแนวปฏิบัติเพื่อเตรียมรับสถานการณ์ ดังนี้

(๑) มีการติดตั้งอุปกรณ์ตรวจจับควัน กรณีเกิดเหตุการณ์กระแสไฟฟ้าขัดข้องหรือมีควันไฟเกิดขึ้น ภายในห้องเซิร์ฟเวอร์ อุปกรณ์ดังกล่าวจะส่งสัญญาณแจ้งเตือนเพื่อให้เจ้าหน้าที่หรือผู้พบเหตุทราบและเข้ามาระงับเหตุฉุกเฉินก่อนเกิดอัคคีภัยได้อย่างทันท่วงทีเพราะเป็นภัยที่มีผลกระทบรุนแรงที่สุด

(๒) มีการติดตั้งถังดับเพลิงชนิดที่ใช้สารเคมีไม่ทำอันตรายต่ออุปกรณ์ประมวลผลข้อมูล (Process Deice) ห้องเซิร์ฟเวอร์ จำนวน ๑ ถัง เพื่อให้เจ้าหน้าที่รักษาความปลอดภัยหรือผู้พบเหตุใช้ระงับเหตุก่อนไฟเริ่มลุกลามถึงขั้นรุนแรง

๖.๒.๕ เหตุการณ์ที่เกิดจากภัยพิบัติหรือสถานการณ์อื่นๆ เช่น อุทกภัย วาตภัย และการชุมนุมประท้วง หรือความไม่สงบเรียบร้อยทางการเมือง มีแนวปฏิบัติเพื่อเตรียมรับสถานการณ์ ดังนี้

(๑) ให้ผู้ใช้งาน (User) สำรองข้อมูลสารสนเทศส่วนตัวลงในอุปกรณ์บันทึกข้อมูลแบบพกพา เช่น Flash Drive และ External Hard disk

(๒) มีการล็อคประตูทางเข้าด้วยระบบรหัสผ่านเพื่อป้องกันไม่ให้บุคคลภายนอกเข้าไปภายในห้องเซิร์ฟเวอร์โดยไม่ได้รับอนุญาต

(๓) ตรวจสอบการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ เพื่อให้ผู้ใช้งาน (User) ปฏิบัติงานจากภายนอกโรงพยาบาล (Teleworking) โดยผ่านเครือข่ายภายนอก (Internet) ได้

(๔) ตรวจสอบความพร้อมของข้อมูลสารสนเทศที่ได้สำรองระบบคอมพิวเตอร์และระบบสารสนเทศ รวมถึงข้อมูลสารสนเทศที่ได้บันทึกลงในตลับเทปแม่เหล็ก (Magnetic Tape Drive) หรืออุปกรณ์สำรองข้อมูลอื่นใด สำหรับเตรียมนำไปกู้คืน

(๕) เมื่อกลุ่มงานสุขภาพดิจิทัล ได้รับแจ้งว่าจะเกิดเหตุชุมนุมประท้วงหรือความไม่สงบเรียบร้อยทางการเมืองบริเวณโรงพยาบาล ซึ่งอาจถูกปิดกั้นการเข้าออก และอาจเสี่ยงต่อการถูกตัดไฟฟ้า/น้ำให้ผู้ดูแลระบบ (System Administrator) นำตลับเทปแม่เหล็ก (Magnetic Tape Dive) หรืออุปกรณ์สำรองข้อมูลอื่นใด ที่สำรองข้อมูลไว้ไปเก็บในสถานที่ปลอดภัย

๖.๓ เหตุการณ์ที่เกิดจากเทคโนโลยี (Technology)

๖.๓.๑ ทรัพย์สิน ครุภัณฑ์ ระบบปฏิบัติการด้านเทคโนโลยี

๖.๓.๒ การสื่อสารและเครือข่ายสารสนเทศ

๖.๓.๓ โครงข่ายสารสนเทศ

๖.๓.๔ ข้อมูลสารสนเทศ

มีแนวปฏิบัติเพื่อเตรียมรับสถานการณ์ ตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศทางการแพทย์ โรงพยาบาลพระอาจารย์มั่น ภูริทัตโต

๗. ระยะเวลาเป้าหมายในการฟื้นคืนสภาพเมื่อเกิดสภาวะวิกฤต

กระบวนงาน	ระดับผลกระทบ	ระยะเวลาเป้าหมายในการฟื้นคืนสภาพเมื่อเกิดสภาวะวิกฤต		
		ภายใน ๑ วัน	ภายใน ๗ วัน	มากกว่า ๗ วัน
๘.๑ เหตุการณ์หรือภัยที่เกิดจากบุคลากร (People)				
๘.๑.๑ เหตุการณ์หรือภัยที่เกิดจากบุคลากรภายในโรงพยาบาลพระอาจารย์มั่น ภูริทัตโต	ค่อนข้างสูง	✓		
๘.๑.๒ เหตุการณ์หรือภัยที่เกิดจากบุคคลภายนอกหรือผู้ไม่ประสงค์ดี	ต่ำ	✓		
๘.๒ เหตุการณ์หรือภัยที่เกิดจากกระบวนการ (Process)				
๘.๒.๑ เหตุการณ์หรือภัยที่เกิดจากการโจรกรรมอุปกรณ์ประมวลข้อมูล (Process Device)	ต่ำ	✓		
๘.๒.๒ เหตุการณ์หรือภัยที่เกิดจากด้านเทคนิค	ต่ำ	✓		
๘.๒.๓ เหตุการณ์ไฟฟ้าดับ	ต่ำ	✓		

กระบวนงาน	ระดับผลกระทบ	ระยะเวลาเป้าหมาย ในการฟื้นคืนสภาพเมื่อเกิดสภาวะวิกฤต		
		ภายใน ๑ วัน	ภายใน ๗ วัน	มากกว่า ๗ วัน
๘.๒.๔ เหตุการณ์อัคคีภัย	ต่ำ		✓	
๘.๒.๕ เหตุการณ์ที่เกิดจากภัยพิบัติหรือสถานการณ์อื่น ๆ เช่น อุทกภัย วาตภัยและการชุมนุมประท้วง หรือความไม่สงบเรียบร้อยทางการเมือง	ต่ำ	✓		
๘.๓ เหตุการณ์ที่เกิดจากเทคโนโลยี (Technology)				
๘.๓.๑ ทรัพย์สิน ครุภัณฑ์ ระบบปฏิบัติการด้านเทคโนโลยี	ค่อนข้างสูง		✓	
๘.๓.๒ การสื่อสารและเครือข่าย	ค่อนข้างสูง	✓		
๘.๓.๓ โครงข่ายสารสนเทศ	ค่อนข้างสูง	✓		
๘.๓.๔ ข้อมูลสารสนเทศ	ค่อนข้างต่ำ	✓		

๘. โครงสร้างและทีมบริหารความต่อเนื่อง

เพื่อให้แผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านกลุ่มงานสุขภาพดิจิทัล โรงพยาบาลพระอาจารย์มั่น ภูริทัตโตสามารถนำไปปฏิบัติได้อย่างมีประสิทธิภาพ จึงต้องมีการจัดตั้งทีมบริหารความต่อเนื่อง ซึ่งประกอบด้วยผู้อำนวยการโรงพยาบาล หัวหน้างาน และบุคลากรกลุ่มงานสุขภาพดิจิทัล เนื่องจากมีความรู้ความสามารถด้านระบบคอมพิวเตอร์และระบบสารสนเทศ ประกอบกับปฏิบัติหน้าที่ (System Administrator) ของโรงพยาบาลพระอาจารย์มั่น ภูริทัตโต

๘.๑ หน้าที่ความรับผิดชอบทีมบริหารความต่อเนื่อง ดังนี้

๘.๑.๑ หัวหน้าทีมและรองหัวหน้าทีม มีหน้าที่ในการพิจารณาแนวทางการแก้ไขปัญหา กำหนดขอบเขต และสั่งการให้ผู้รับผิดชอบดำเนินการแก้ไข พร้อมทั้งรายงานให้คณะผู้บริหารระดับสูงโรงพยาบาลพระอาจารย์มั่น ภูริทัตโต ทราบ

๘.๑.๒ ผู้ประสานงาน มีหน้าที่ในการติดต่อประสานงานภายในและหน่วยงานภายนอกโรงพยาบาลพระอาจารย์มั่น ภูริทัตโต และจัดเตรียมเอกสารที่เกี่ยวข้อง รวมถึงจัดทำรายงานในแต่ละสถานการณ์

๘.๑.๓ ผู้ดูแลระบบ (System Administrator) มีหน้าที่การพัฒนาและบริหารจัดการระบบคอมพิวเตอร์และระบบสารสนเทศ รวมถึงข้อมูลสารสนเทศ ตลอดจนการรักษาความมั่นคงปลอดภัย ดูแลสิทธิของผู้ใช้งาน (User) แก้ไขปัญหาการใช้งาน และดูแลห้องเซิร์ฟเวอร์

๘.๒ รายชื่อทีมบริหารความต่อเนื่องและหน้าที่รับผิดชอบ

ชื่อ – นามสกุล	หน้าที่รับผิดชอบ	เบอร์โทรศัพท์
นางศิริกัญญา ถาบุตร	- ผู้ดูแลระบบ	๐๙๕-๒๒๓๙๒๖๙
นายวชิรวิทย์ อุดมฉวี	- ผู้ดูแลระบบ	๐๘๕-๗๖๐๔๘๒๐
นางสาวขวัญฤดี นามนนท์	- ผู้ดูแลระบบ	๐๖๓-๑๖๒๖๓๖๘
นางสาวพัชราภรณ์ แสงหาญ	- ผู้ดูแลระบบ	๐๘๒-๐๓๗๒๙๒๕
นายพงษ์ดนัย วรสาร	- ผู้ดูแลระบบ	๐๘๐-๙๘๙๖๙๒๒
นางสาววรรณนิดา นามแสง	- ผู้ดูแลระบบ	๐๙๕-๓๖๕๐๓๘๐
นายอภิวัฒน์ อินธิกาย	- ผู้ดูแลระบบ	๐๙๘-๑๘๕๒๔๒๑
นายชนุดม อาษา	- ผู้ดูแลระบบ	๐๙๒-๘๘๒-๓๗๕๐

๙. การสำรองข้อมูลและกู้คืนข้อมูลสารสนเทศ

เนื่องจากระบบคอมพิวเตอร์และระบบสารสนเทศ รวมถึงข้อมูลสารสนเทศส่วนใหญ่ ถูกติดตั้งและจัดเก็บบนระบบประมวลผลกลาง ณ ห้องเซิร์ฟเวอร์ ซึ่งเป็นการอำนวยความสะดวกแก่ผู้ใช้งาน (User) เป็นอย่างมาก แต่ก็มีความเสี่ยงสูงมากเช่นกัน ซึ่งเป็นผู้ดูแลรับผิดชอบหลัก จึงได้จัดทำแนวปฏิบัติการสำรองข้อมูลและกู้คืนข้อมูลสารสนเทศ เพื่อให้ระบบคอมพิวเตอร์และระบบสารสนเทศ รวมถึงข้อมูลสารสนเทศอยู่ในสภาพพร้อมใช้งานสามารถให้บริการได้อย่างต่อเนื่อง และสามารถกู้คืนกลับมาใช้งานได้โดยเร็วหากเกิดปัญหา

๙.๑ แนวปฏิบัติในการดูแลระบบคอมพิวเตอร์และระบบสารสนเทศ รวมถึงข้อมูลสารสนเทศตลอดจนอุปกรณ์ประมวลผลข้อมูล (Process Device) ได้มอบหมายให้ผู้ดูแลระบบ (System Administrator) ดูแลระบบคอมพิวเตอร์และระบบสารสนเทศ รวมถึงข้อมูลสารสนเทศ ตลอดจนให้ตรวจสอบอุปกรณ์ประมวลผลข้อมูล (Process Device) ณ ห้องเซิร์ฟเวอร์ อย่างสม่ำเสมออย่างน้อยสัปดาห์ละ ๑ ครั้ง หากพบข้อผิดพลาดให้รายงานหัวหน้ากลุ่มงานสุขภาพดิจิทัล ทราบโดยทันที

๙.๒ แนวปฏิบัติในการสำรองข้อมูลสารสนเทศ กำหนดดังนี้

๙.๒.๑ ผู้ดูแลระบบ (System Administrator) ต้องดำเนินการสำรองข้อมูลสารสนเทศไว้ในอุปกรณ์สำรอง ตามขั้นตอนของโปรแกรมสำรองข้อมูล

๙.๒.๒ ผู้ดูแลระบบ (System Administrator) ต้องพิมพ์รายละเอียดไว้ในอุปกรณ์สำรองอื่นที่ใช้สำหรับการสำรองข้อมูล ได้แก่ รูปแบบการสำรองข้อมูลแบบรายวันหรือรายสัปดาห์ หรือรายเดือน วันและเวลา และผู้รับผิดชอบ พร้อมทั้งตรวจสอบความถูกต้องสมบูรณ์ของการ

๙.๓ แนวปฏิบัติการกู้คืนระบบ

หากระบบคอมพิวเตอร์และระบบสารสนเทศเกิดปัญหาไม่สามารถใช้งานได้ หรือข้อมูลสารสนเทศสูญหาย ให้ผู้ดูแลระบบ (System Administrator) ดำเนินการกู้คืนข้อมูลสารสนเทศที่สำรองไว้ในอุปกรณ์สำรองเพื่อนำข้อมูลสารสนเทศกลับมาใช้งาน

๙.๔ กลุ่มงานสุขภาพดิจิทัล ต้องดำเนินการทดสอบสภาพความพร้อมใช้งานของระบบคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลสารสนเทศและระบบสำรองข้อมูล ตามระดับความเสี่ยงที่ยอมรับได้ อย่างน้อยปีละ ๑ ครั้ง ดังนี้

๙.๔.๑ พิจารณาคัดเลือกระบบคอมพิวเตอร์และระบบสารสนเทศที่สำคัญเพื่อดำเนินการทดสอบ พร้อมทั้งเตรียมความพร้อมก่อนการทดสอบ เพื่อมิให้เกิดความเสี่ยงและความเสียหายแก่ทางราชการ

๙.๔.๒ จัดทำรายงานเสนอหัวหน้ากลุ่มงานสุขภาพดิจิทัล (DCIO : Department Chief Information Officer) ก่อนดำเนินการทดสอบ

๙.๔.๓ ดำเนินการทดสอบระบบคอมพิวเตอร์และระบบสารสนเทศตามที่กำหนดไว้

๙.๔.๔ รายงานผลการทดสอบเสนอหัวหน้ากลุ่มงานสุขภาพดิจิทัล

(ลงชื่อ).....ผู้เสนอ
(นางสาวพัชราภรณ์ แสงหาญ)
ตำแหน่ง นักวิชาการคอมพิวเตอร์ปฏิบัติการ

(ลงชื่อ).....ผู้เห็นชอบ
(นางศิริกัญญา ถาบุตร)
ตำแหน่ง นักวิชาการคอมพิวเตอร์ปฏิบัติการ
หัวหน้ากลุ่มงานสุขภาพดิจิทัล

(ลงชื่อ).....ผู้อนุมัติ
(นายพันธวี คำสาว)
ตำแหน่ง ผู้อำนวยการโรงพยาบาลพระอาจารย์มั่น ภูริทัตโต