การจัดการความเสี่ยงในระบบเทคโนโลยีสารสนเทศ

บทที่ 1

1.1 หลักการและเหตุผล

การบริหารจัดการความเสี่ยงเป็นเครื่องมือทางกลยุทธ์ที่สำคัญตามหลักการกำกับดูแลกิจการที่ดี โดยจะช่วยให้การบริหารงานและการตัดสินใจต้านต่างๆ เช่น การวางแผน การกำหนดกลยุทธ์ การติดตามควบคุม และวัดผลการปฏิบัติงานตลอดจนการใช้ทรัพยากรต่างๆ อย่างเหมาะสมและมีประสิทธิภาพมากขึ้น ลดการสูญเสียและโอกาสที่ทำให้เกิดความเสียหายแก่องค์กร โดยเฉพาะอย่างยิ่งในด้านเทคโนโลยีสารสนเทศที่เข้ามา มีบทบาสำคัญในการดำเนินงานขอหน่วยงานภายในองค์กร ทั้งการจัดเก็บข้อมูล การใช้งานอุปกรณ์คอมพิวเตอร์ การติดต่อสื่อสารผ่านระบบเครือข่าย และวิธีการปฏิบัติงานระบบเทคโนโลยีสารสนเทศต่างๆ ภายใต้สภาวะการดำเนินงานของทุกๆ องค์กรล้วนแต่มีความเสี่ยง ซึ่งก็คือความไม่แน่นอนที่จะส่งผลกระทบต่อการดำเนินงานหรือเป้าหมายขององค์กร จึงจำเป็นต้องมีการจัดการความเสี่ยงเหล่านั้นอย่างเป็นระบบ โดยการระบุความเสี่ยงว่ามีปัจจัยเสี่ยงใดบ้างที่กระทบต่อการดำเนินงานหรือเป้าหมายขององค์กรวิเคราะห์ความเสี่ยง จากผลกระทบที่เกิดขึ้นจัดลำดับความสำคัญของปัจจัยเสี่ยง แล้วกำหนดแนวทางในการจัดการความเสี่ยง โดยต้องคำนึงถึงความคุ้มค่าในการจัดการความเสี่ยงอย่างเหมาะสม

1.2 คำจำกัดความและความหมายที่เกี่ยวข้องกับการบริหารความเสี่ยง

ความเสี่ยง (Risk) หมายถึง เหตุการณ์/การกระทำใดๆ ที่มีความไม่แน่นอน ซึ่งหากเกิดขึ้นจะมีผลกระทบในเชิงลบต่อวัตถุประสงค์หรือเป้าหมายขององค์กร หรือลดโอกาสที่จะบรรลุความสำเร็จต่อการบรรลุเป้าหมายและวัตถุประสงค์ของแผนงาน/โครงการที่จะก้าวสู่พันธกิจ และวิสัยทัศน์ ที่กำหนดไว้

ปัจจัยเสี่ยง (Risk Factor) หมายถึง สาเหตุของความเสี่ยงซึ่งจะทำให้ไม่บรรลุวัตถุประสงค์ที่กำหนดไว้ โดยต้องระบุได้ด้วยว่าเหตุการณ์นั้นจะเกิดที่ไหน เมื่อใดและจะเกิดขึ้นได้อย่างไรและทำไม ทั้งนี้สาเหตุของความเสี่ยงที่ระบุควรเป็นสาเหตุที่แท้จริง เพื่อจะได้วิเคราะห์และกำหนดมาตรการความเสี่ยงในภายหลังได้อย่างถูกต้อง

การประเมินความเสี่ยง (Risk Assessment) หมายถึง กระบวนการระบุความเสี่ยงและการวิเคราะห์ความเสี่ยงเพื่อจัดลำดับความเสี่ยง โดยการประเมินจากโอกาสหรือความถี่ที่จะเกิดเหตุการณ์ (Likelihood) และผลกระทบต่อการบรรลุเป้าหมายขององค์กร (Impact)

ระดับของความเสี่ยง (Degree of Risk) หมายถึง สถานะของความเสี่ยงที่ได้จากประเมินโอกาสและผลกระทบของแต่ละปัจจัยเสี่ยงแบ่งเป็น 5 ระดับ คือ ความเสี่ยงสูงมาก ความเสี่ยงสูง ความเสี่ยงป่านกลาง ความเสี่ยงต่ำ และความเสี่ยงต่ำมาก

โอกาส (Opportunity) หมายถึง เหตุการณ์ที่มีความไม่แน่นอน ซึ่งหากเกิดขึ้นจะมีผลกระทบในเชิงบวกต่อวัตถุประสงค์หรือเป้าหมายขององค์กร ซึ่งผู้บริหารและผู้ที่เกี่ยวข้องควรจะได้ทบทวนถึงกลยุทธ์ และแผนงาน ที่เหมาะสมใหม่ เพื่อสร้างคุณค่าเพิ่มให้กับองค์กรนอกเหนือจากแผนงานและโครงการที่ได้กำหนดไว้แล้วการควบคุมภายใน (Internal Control หมายถึง กระบวนการปฏิบัติงานที่บุคลากรในองค์กร โดยคณะกรรมการบริหาร

ผู้บริหารทุกระดับ และพนักงานทุกคนมีบทบาทร่วมกันในการจัดให้มีขึ้น เพื่อสร้าง ความเชื่อมั่นอย่างสมเหตุสมผลว่าการปฏิบัติงานจะบรรลุวัตถุประสงค์ของการควบคุมภายใน

การบริหารจัดการความเสี่ยง (Risk Management) หมายถึง กลวิธีที่เป็นเหตุเป็นผลที่นำมาใช้ใน การบ่งชี้ วิเคราะห์ ประเมิน จัดการ ติดตาม และสื่อสารความเสี่ยงที่เกี่ยวข้องกับกิจกรรมหน่วยงาน/ฝ่ายงาน หรือกระบวนการดำเนินงานขององค์กร เพื่อช่วยลดความสูญเสียในการไม่บรรลุเป้าหมายให้เหลือน้อยที่สุด และเพิ่มโอกาสแก่องค์กรมากที่สุด

การบริหารความเสี่ยงโดยองค์รวม (Enterprise Risk Management : EMR) หมายถึง การบริหารความเสี่ยง โดย มีโครงสร้างองค์กร กระบวนการ และวัฒนธรรมองศ์กรประกอบเข้าด้วยกัน และเป็นกลไกส่วนหนึ่งของการขับเคลื่อนไปสู่ การกำกับดูแลกิจการที่ดี เพื่อบรรลุวัตถุประสงค์และการเติบโตอย่างยั่งยืนขององค์กร และเป็นที่พอใจของผู้มีผลประโยชน์ร่วม โดยครอบคลุมความเสี่ยงทั่วทั้งองค์กร ไม่ว่าจะเป็นความเสี่ยงเกี่ยวกับกลยุทธ์ การดำเนินงาน การปฏิบัติตามกฎระเบียบ และการเงิน ซึ่งความเสี่ยงเหล่านี้อาจทำให้เกิดความเสียหายความไม่แน่นอน และโอกาส รวมถึงการมีผลกระทบต่อวัตถุประสงค์และความต้องการของผู้มีผลประโยชน์ร่วม

1.3 ประโยชน์ของการบริหารความเสี่ยง

การดำเนินการบริหารความเสี่ยงจะช่วยให้ผู้บริหารมีข้อมูลที่ใช้ในการตัดสินใจได้ดียิ่งขึ้น และทำให้องค์กรสามารถจัดการกับปัญหาอุปสรรคและอยู่รอดได้ในสถานการณ์ที่ไม่คาดคิดหรือสถานการณ์ที่อาจทำให้องค์กรเกิดความเสียหาย

ประโยชน์ที่คาดหวังว่าจะได้รับจากการดำเนินการบริหารความเสี่ยง มีดังนี้

1) **เป็นส่วนหนึ่งของหลักการบริหารกิจการบ้านเมืองที่**ดี การบริหารความเสี่ยงจะช่วยคณะทำงานบริหารความเสี่ยงและผู้บริหารทุกระดับตระหนักถึงความเสี่ยงหลักที่สำคัญ และสามารถทำหน้าที่ในการกำกับดูแลองค์กรได้อย่างมีประสิทธิภาพและประสิทธิผลมากยิ่งขึ้น

2) **สร้างฐานข้อมูลที่มีประโยชน์ต่อการบริหารและการปฏิบัติงานในองค์กร** การบริหารความเป็นแหล่งข้อมูลสำหรับผู้บริหารในการตัดสินใจด้านต่างๆ รวมถึงการบริหารความเสี่ยง ซึ่งตั้งอยู่บนสมมุติฐานใน การตอบสนองต่อเป้าหมายและภารกิจหลักขององค์กรรวมถึงระดับความเสี่ยงที่ยอมรับได้

3) **ช่วยสะท้อนให้เห็นภาพรวมของความเสี่ยงต่างๆ ที่สำคัญได้ทั้งหมด** การบริหารความเสี่ยงจะทำให้บุคลากรภายในองค์กรมีความเข้าใจถึงเป้าหมายและภารกิจหลักขององค์กร และตระหนักถึงความเสี่ยงสำคัญที่ส่งผลกระทบในเชิงลบต่อองค์กรได้อย่างครบถ้วน ซึ่งครอบคลุมความเสี่ยงธรรมาภิบาล

4) **เป็นเครื่องมือที่สำคัญในการบริหารงาน** การบริหารความเสี่ยงเป็นเครื่องมือที่ช่วยให้ผู้บริหารสามารถมั่นใจได้ว่าความเสี่ยงได้รับการจัดการอย่างเหมาะสมและทันเวลา รวมทั้งเป็นเครื่องมือที่สำคัญของผู้บริหารในการบริหารงานและ การตัดสินใจในด้านต่างๆ เช่น การวางแผนการกำหนดกลยุทธ์ การติดตามควบคุม และวัดผลการปฏิบัติงาน ซึ่งส่งผลให้ การดำเนินงานของโรงพยาบาลเป็นไปตามเป้าหมายที่กำหนดและสามารถปกป้องผลประโยชน์รวมทั้งเพิ่มมูลค่าแก่องค์กร

5) ช่วยให้การพัฒนาองค์กรเป็นไปในทิศทางเดียวกัน การบริหารความเสี่ยงทำให้รูปแบบการตัดสินใจในระดับการปฏิบัติงานขององค์กรมีการพัฒนาไปในทิศทางเดียวกัน เช่น การตัดสินใจโดยที่ผู้บริหารมีความเข้าใจในกลยุทธ์ วัตถุประสงค์ขององค์กรและระดับความเสี่ยงอย่างชัดเจน

6) ช่วยให้การพัฒนาการบริหารและจัดสรรทรัพยากรเป็นไปอย่างมีประสิทธิภาพและประสิทธิผล การจัดสรรทรัพยากรเป็นไปอย่างเหมาะสม โดยพิจารณาถึงระดับความเสี่ยงในแต่ละกิจกรรม และการเลือกใช้มาตรการในการบริหาร ความเสี่ยง เช่น การใช้ทรัพยากรสำหรับกิจกรรมที่มีความเสี่ยงต่ำและกิจกรรมที่มีความเสี่ยงสูง ย่อมแตกต่างกัน หรือการเลือกใช้มาตรการแต่ละประเภทย่อมใช้ทรัพยากรแตกต่างกัน เป็นต้น

บทที่ 2
แนวทางการบริหารความเสี่ยง

2.1 หลักการบริหารความเสี่ยง

หลักการบริหารความเสี่ยงโดยใช้กระบวนการบริหารความเสี่ยงตามมาตรฐานของ COSO (The Committee of Sponsoring Organization of the Tread way Commission) ซึ่งกำหนดกรอบการจัดการความเสี่ยงในแนวทาง COSO : ERM (Enterprise Risk Management) ประกอบด้วยหลักการสำคัญ 8 องค์ประกอบ เพื่อให้เกิดการบรรลุวัตถุประสงค์ของการบริหารความเสี่ยง

COSO : ERM (Enterprise Risk Management)

1. สภาพแวดล้อมภายในองค์กรด้านเทคโนโลยีสารสนเทศ (Internal Environment) ได้แก่

- ระบบฐานข้อมูลสารสนเทศและโปรแกรมปฏิบัติการ (Database & Software) เช่น เว็บไซต์ภายใต้อินเทอร์เน็ตโดเมนและฐานข้อมูลเว็บไซต์ดังกล่าว เป็นต้น
- ระบบฐานข้อมูลบริหารงานภายใน ได้แก่ ฐานข้อมูลระบบ Hosxp ฐานข้อมูลระบบ E-IPD Paperless เป็นต้น
- ระบบให้บริการเครือข่าย ได้แก่ โปรแกรมป้องกันไวรัสและการถูกโจมตีจากบุคคลภายนอก(Antivirus) โปรแกรมระบบปฏิบัติการจัดการเครือข่าย (Network Software) เป็นต้น
- อุปกรณ์คอมพิวเตอร์ (Hardware) เช่น เครื่องคอมพิวเตอร์แม่ข่ายระบบฐานข้อมูล (Database Server) เครื่องคอมพิวเตอร์แม่ข่ายที่ใช้จัดเก็บและสำรองข้อมูล (Storage Server) เครื่องแม่ข่ายสำหรับให้บริการเว็บไซต์ (Web Server) เครื่องคอมพิวเตอร์ป้องกันการจู่โจมข้อมูลจากบุคคลภายนอก (Firewall) เครื่องคอมพิวเตอร์ชนิดพกพา (NoteBook) เครื่องสแกนเนอร์ (Scanner) เครื่องพิมพ์คอมพิวเตอร์ (Printer)

อุปกรณ์สำรองไฟฟ้าสำหรับคอมพิวเตอร์ (UPS) อุปกรณ์กระจายสัญญาณเครือข่าย (Switching HUB) อุปกรณ์กระจายสัญญาณเครือข่ายชนิดไร้สาย (Wireless Access point) เป็นต้น

2. วัตถุประสงค์ของการจัดทำแผนบริหารความเสี่ยง (Objective Setting)

1) เพื่อเตรียมความพร้อมรองรับสถานการณ์ฉุกเฉิน ที่อาจจะเกิดขึ้นกับระบบฐานข้อมูลและระบบเทคโนโลยีสารสนเทศของโรงพยาบาลบ่อพลอย

2) เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของระบบฐานข้อมูลและระบบเทคโนโลยีสารสนเทศให้มีเสถียรภาพ และมีความพร้อมสำหรับการใช้งาน

3) เพื่อให้การปฏิบัติงานเป็นไปอย่างมีระบบและต่อเนื่อง สามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที กรณีเกิดสถานการณ์ความไม่แน่นอนและภัยพิบัติ

3. การบ่งชี้หรือการระบุความเสี่ยง (Event Identification)

เป็นกระบวนการที่ผู้บริหารและผู้ปฏิบัติงานร่วมกันระบุความเสี่ยงและปัจจัยเสี่ยงที่เกี่ยวข้องโครงการ/กิจกรรม เพื่อให้ทราบถึงเหตุการณ์ที่เป็นความเสี่ยงที่อาจมีผลกระทบต่อการบรรลุผลสำเร็จตามวัตถุประสงค์ ซึ่งต้องคำนึงถึงสภาพแวดล้อมทั้งภายนอกและภายในองค์กร

วิธีการในการระบุความเสี่ยงมีหลายวิธี เช่น

- การระดมสมอง เพื่อให้ได้ความเสี่ยงที่หลากหลาย
- การใช้ Checklist
- การวิเคราะห์สถานการณ์จากการตั้งคำถาม "What-if"
- การวิเคราะห์ขั้นตอนการปฏิบัติงานในแต่ละขั้นตอน
- การรวบรวมปัญหาที่เกิดขึ้นมาแล้ว

ในขั้นตอนนี้ ควรมีการเก็บข้อมูลความสูญเสียที่เกิดขึ้นในรูปของความถี่ของการเกิดความสูญเสียและความรุนแรงของความสูญเสีย รวมทั้งข้อมูลการดำเนินการใดๆ เพื่อลดความสูญเสียที่เกิดขึ้นในอดีตทั้งที่ประสบผลสำเร็จ และปัญหาอุปสรรคซึ่งจะเป็นประโยชน์ในการดำเนินการต่อไป

4. การประเมินความเสี่ยง (Risk Assessment) ประกอบด้วย 4 ขั้นตอน คือ

1) การกำหนดเกณฑ์การประเมินมาตรฐาน เป็นเกณฑ์ที่จะใช้ประเมินความเสี่ยง ได้แก่ โอกาสที่จะเกิดความเสี่ยง (Likelihood) ระดับความรุนแรงของผลกระทบ (Impact) และระดับของความเสี่ยง (Degree of Risk คณะกรรมการบริหารความเสี่ยงต้องกำหนดเกณฑ์ของหน่วยงานขึ้น ซึ่งอาจกำหนดได้ทั้งเกณฑ์เชิงปริมาณและเชิงคุณภาพ การกำหนดเกณฑ์ของโอกาสที่เกิดความเสี่ยงอาจกำหนดเป็นเกณฑ์ 5 ระดับ (สูงมากรุนแรงมากที่สุด สูง/ค่อนข้างรุนแรง ปานกลาง น้อย และน้อยมาก) ส่วนระดับของความเสี่ยงอาจกำหนดเป็นเกณฑ์ 5 ระดับ (สูงมาก สูง ปานกลาง น้อย และน้อยมาก)

2) การประเมินโอกาสและผลกระทบของความเสี่ยง เป็นการนำความเสี่ยงและปัจจัยเสี่ยงแต่ละปัจจัยที่ระบุไว้มาประเมินโอกาสที่จะเกิดเหตุการณ์ความเสี่ยงเหล่านั้นและประเมินระดับความรุนแรงหรือมูลค่าความเสียหายจากความเสี่ยงตามเกณฑ์มาตรฐานที่กำหนดเพื่อให้เห็นระดับความเสี่ยง ซึ่งแต่ละความเสี่ยงก็จะมีความรุนแรงแตกต่างกัน ทั้งนี้การควบคุมความเสี่ยงหรือหลีกเลี่ยงความเสี่ยงนั้น ก็จะขึ้นอยู่กับมาตรการควบคุมความเสี่ยงของแต่ละหน่วยงาน โดยมีการประเมินใน 2 มิติ ได้แก่ มิติผลกระทบและมิติโอกาสของความเสี่ยง ที่จะเกิดขึ้น

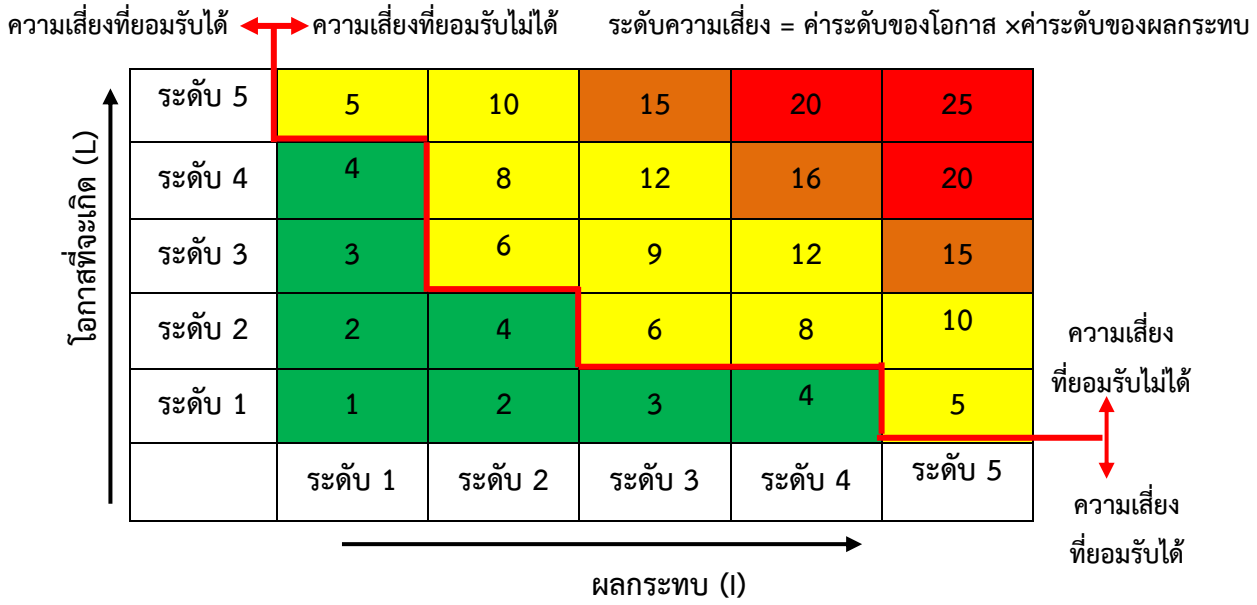
เกณฑ์ประเมินจุดอ่อนหรือโอกาสที่จะเกิดความเสี่ยง มีดังนี้

ระดับ	การประเมิน
1	มีจุดอ่อนน้อยมาก หรือไม่น่าจะเกิดเหตุการณ์นี้ได้ หรือมีโอกาสเกิดได้น้อยมาก
2	มีจุดอ่อนน้อย หรือมีโอกาสเกิดเหตุการณ์ได้น้อย อาจพบได้สักครั้ง ในรอบ 1 ปี
3	มีจุดอ่อนพอควร หรือมีโอกาสเกิดเหตุการณ์ได้บ้าง อย่างน้อย เดือนละ 1 ครั้ง
4	มีจุดอ่อนมาก หรือ มีโอกาสเกิดเหตุการณ์ได้บ่อย เดือนละหลายครั้ง
5	มีจุดอ่อนรอบด้าน หรือ มีโอกาสเกิดเหตุการณ์ได้บ่อยมาก พบทุกๆสัปดาห์

เกณฑ์การประเมินผลกระทบ มีดังนี้

ระดับ	การประเมิน
1	ไม่น่าจะเกิดผลกระทบต่อการให้บริการ หรือมีผลกระทบน้อยมาก
2	มีผลกระทบต่อการให้บริการของโรงพยาบาลในบางจุด
3	มีผลกระทบต่อการให้บริการของโรงพยาบาลใน 1-2 แผนก
4	มีผลกระทบต่อการให้บริการของโรงพยาบาล 3-4 แผนก
5	มีผลกระทบต่อการให้บริการของโรงพยาบาลเป็นวงกว้าง อาจเกิดอันตรายต่อผู้ป่วย

3) การวิเคราะห์ความเสี่ยง เป็นการดูความสัมพันธ์ระหว่างโอกาสที่จะเกิดความเสี่ยงและผลกระทบของความเสี่ยงต่อองค์กรว่าจะก่อให้เกิดระดับความเสี่ยงในระดับใด โดยใช้ตารางระดับความเสี่ยงสูงสุดที่จะต้องบริหารจัดการก่อน



ระดับความเสี่ยง (Degree of Risk)	
1 - 4 มีโอกาสที่จะเกิดความเสี่ยง ต่ำ	5 - 12 มีโอกาสที่จะเกิดความเสี่ยง ปานกลาง
13 - 16 มีโอกาสที่จะเกิดความเสี่ยง สูง	17 - 25 มีโอกาสที่จะเกิดความเสี่ยง สูงมาก

4) การจัดลำดับความเสี่ยง เป็นการจัดลำดับความรุนแรงของความเสี่ยงที่มีผลต่อองค์กร เพื่อพิจารณากำหนดกิจกรรมการควบคุมในแต่ละสาเหตุของความเสี่ยงที่สำคัญให้เหมาะสม โดยพิจารณาจากระดับความเสี่ยงที่ประเมินได้ เลือกความเสี่ยงที่มีระดับสูงมากหรือสูงมาจัดทำแผนการบริหารความเสี่ยงเป็นลำดับแรก

5. การตอบสนองความเสี่ยง (Risk Response)

เมื่อความเสี่ยงได้รับการบ่งชี้และประเมินความสำคัญแล้ว ผู้บริหารต้องประเมินวิธีการจัดการความเสี่ยงที่สามารถนำไปปฏิบัติได้และผลของการจัดการเหล่านั้น การพิจารณาทางเลือกในการดำเนินการ จะต้องคำนึงถึงความเสี่ยงที่ยอมรับได้ และต้นทุนที่เกิดขึ้นเปรียบเทียบกับผลประโยชน์ที่จะได้รับเพื่อให้การบริหารความเสี่ยงมีประสิทธิผล ผู้บริหารอาจต้องเลือกวิธีการจัดการความเสี่ยงอย่างใดอย่างหนึ่ง หรือหลายวิธีรวมกัน เพื่อลดระดับโอกาสที่อาจเกิดขึ้นและผลกระทบของเหตุการณ์ให้อยู่ในช่วงที่องค์กรสามารถยอมรับได้ (Risk Tolerance) หลักการตอบสนองความเสี่ยงมี 4 ประการ คือ

- **การหลีกเลี่ยง (Terminate/Avoidance)** เป็นวิธีการที่ง่ายที่สุดในการบริหารความเสี่ยง คือ การเลือกที่จะไม่รับความเสี่ยงไว้เลย อาจหยุดดำเนินการ หรือยกเลิกโครงการ/กิจกรรมที่ก่อให้เกิดความเสียหายได้ การหลีกเลี่ยงความเสี่ยงเมื่อพบว่าผลประโยชน์ที่จะได้รับนั้นไม่คุ้มกับสิ่งที่จะเกิดขึ้นจึงหลีกเลี่ยงที่จะ

เผชิญกับกิจกรรมความเสี่ยงนั้น หรือการหลีกเลี่ยงความเสี่ยงอาจเกิดขึ้นจากหน่วยงานเลือกที่จะหลีกเลี่ยงกิจกรรมความเสี่ยงนั้น โดยมิได้คิดทบทวนถึงผลที่จะได้รับ นำมาซึ่งการเสียโอกาสของหน่วยงานได้

- **การยอมรับ (Take/Acceptance)** เป็นการยอมรับความเสี่ยงหรือความเสียหายที่อาจจะ เกิดขึ้นไว้เองโดยไม่ทำอะไร และยอมรับในผลที่อาจตามมา เนื่องจากเห็นว่าโอกาสหรือความน่าจะเป็นที่จะเกิดความเสียหายอยู่ในวิสัยที่หน่วยงานยอมรับได้ หรือไม่คุ้มค่าสำหรับค่าใช้จ่ายในการสร้างระบบในการจัดการหรือป้องกันความเสี่ยง
- **การควบคุมหรือการลด (Treat/Reduction)** เป็นการปรับปรุงระบบการทำงาน หรือออกแบบ วิธีการทำงานใหม่ เพื่อหาทางป้องกันมิให้มีความเสียหายเกิดขึ้น เป็นการลดโอกาสหรือจำนวนครั้งของความเสียหายที่จะเกิด หากเราไม่สามารถป้องกันไม่ให้ความเสี่ยงเกิดขึ้นได้ ก็ควรขจัดให้หมดไป หรือลดความรุนแรง ของความเสี่ยงลง โดยมีการจัดทำแผนหรือมาตรการควบคุมขึ้น อาจกำหนดเป็นแนวทางปฏิบัติไว้ล่วงหน้า ทั้งนี้วิธี ควบคุมความสูญเสียมีสองวิธีหลัก คือ การป้องกันการเกิดความสูญเสีย และการควบคุมขนาดของความสูญเสีย หลังเกิดความสูญเสียขึ้นการป้องกันการเกิดความสูญเสีย เป็นวิธีการที่พยายามจะลดความถี่ของการเกิดความสูญเสียก็คือการหามาตรการหรือวิธีการใดๆ ในการป้องกันไม่ให้ความสูญเสียเกิดขึ้น
- **การถ่ายโอน (Transfer/Sharing)** การโอนย้ายหรือแบ่งความเสี่ยงไปให้ผู้อื่นช่วยรับผิดชอบ เช่น อุปกรณ์ เครือข่ายเมื่อซื้อมาแล้วมีระยะประกันภัยเพียงหนึ่งปี เพื่อเป็นการรับมือในกรณีที่อุปกรณ์เครือข่ายไม่ ทำงาน องค์กรอาจเลือกซื้อประกัน หรือสัญญาการบำรุงรักษาหลังการขาย

6. กิจกรรมการควบคุมความเสี่ยง (Control Activities)

การวางแผนโดยกำหนดมาตรการเพื่อควบคุมผลกระทบของความเสี่ยงเพื่อให้สามารถบรรลุ เป้าหมายหรือใกล้เคียงกับเป้าหมายที่กำหนดไว้ในการวางแผน จะต้องมีการกำหนดกลยุทธ์ในการควบคุม ผลกระทบของความเสี่ยงที่อาจเกิดขึ้น เพื่อที่จะลดและตรวจหาความเสี่ยงที่ได้ประเมินเอาไว้ โดยให้มีการแต่งตั้งเจ้าหน้าที่ผู้รับผิดชอบเป็นผู้ดูแลรักษาความมั่นคงปลอดภัยของระบบ และป้องกัน/แก้ไข/ควบคุมความเสี่ยงไม่ให้มีผลกระทบต่อระบบที่วางไว้ โดยสามารถดำเนินการตามแผนได้ การควบคุมอาจแบ่งได้เป็น 4 ประเภท คือ

- **ควบคุมเพื่อการป้องกัน (Preventive Control)** เป็นวิธีการควบคุมเพื่อป้องกันไม่ให้ เกิดความเสี่ยงและข้อผิดพลาดตั้งแต่แรก เช่น การอนุมัติ การจัดโครงสร้างองค์กร การควบคุม การเข้าถึง เอกสาร เป็นต้น
- **การควบคุมเพื่อให้ตรวจพบ (Detective Control)** เป็นวิธีการควบคุมเพื่อค้นข้อผิดพลาดที่เกิดขึ้นแล้ว เช่น การวิเคราะห์ การตรวจนับ การรายงานข้อบกพร่อง เป็นต้น
- **การควบคุมโดยการชี้แนะ (Direction Control)** เป็นวิธีควบคุมที่ส่งเสริมหรือกระตุ้น ให้เกิดความสำเร็จตามวัตถุประสงค์

- **การควบคุมเพื่อการแก้ไข (Corrective Control)** เป็นวิธีการควบคุมเพื่อแก้ไข ข้อผิดพลาดที่ เกิดขึ้น ให้ถูกต้อง หรือหาวิธีแก้ไขไม่ให้เกิดข้อผิดพลาดนั้นซ้ำอีกในอนาคตหลังจากประเมินความเสี่ยงแล้ว จะต้องวิเคราะห์การควบคุมที่มีอยู่ว่าได้มีการจัดการควบคุมเพื่อลดความเสี่ยงดังกล่าวหรือไม่ โดยนำผลการจัดระดับ ความเสี่ยงในระดับสูงมากและสูงมาประเมินมาตรการควบคุมเป็นอันดับแรก ใช้ขั้นตอนดังนี้
    - นำปัจจัยเสี่ยงที่อยู่ในระดับสูงมาก หรือสูงมากำหนดวิธีควบคุมที่ควรจะมี เพื่อป้องกันความเสี่ยง หรือปัจจัยเสี่ยงเหล่านั้น
    - พิจารณา หรือประเมินว่าในปัจจุบันความเสี่ยงหรือปัจจัยเสี่ยงนั้นมีการควบคุมอยู่แล้วหรือไม่
    - ถ้ามีการควบคุมแล้ว ให้ประเมินต่อไปว่าการควบคุมนั้นได้ผลตามความต้องการหรือไม่

7. ข้อมูลสารสนเทศและการติดต่อสื่อสาร (Information & Communication)

เป็นสิ่งจำเป็นสำหรับองค์กรในการบ่งชี้ ประเมินและการบริหารจัดการความเสี่ยง ดังนั้น โรงพยาบาลบ่อพลอย ได้รวบรวมและบันทึกข้อมูลสารสนเทศที่เกี่ยวข้องกับองค์กรทั้งจากแหล่งภายนอก และภายในตลอดจนเปิดเผยและสื่อสารอย่างเหมาะสมทั้งในด้านรูปแบบและเวลา เพื่อช่วยให้บุคลากร และผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องสามารถตอบสนองต่อเหตุการณ์ต่างๆ ได้อย่างรวดเร็วและมีประสิทธิภาพ

8. การติดตาม (Monitoring)

การติดตามผลการดำเนินงาน การนำกลยุทธ์ มาตรการหรือแนวทางมาใช้ปฏิบัติ เพื่อลดโอกาสที่เกิดความเสี่ยง หรือลดความเสียหายของผลที่อาจเกิดขึ้นจากความเสี่ยงในโครงการ/กิจกรรมที่ยังไม่มีกิจกรรมควบคุมความเสี่ยง หรือมีแต่ไม่เพียงพอ และนำมาวางแผนจัดการความเสี่ยง ทางเลือกในการบริหารความเสี่ยงมีหลายวิธี ซึ่งสามารถปรับเปลี่ยนหรือนำมาผสมผสานให้เหมาะสมกับสถานการณ์ อาจเป็นการยอมรับความเสี่ยง การลดการควบคุมความเสี่ยง การกระจายความเสี่ยง หรือการหลีกเลี่ยงความเสี่ยง เมื่อองค์กรทราบความเสี่ยงที่ยังเหลืออยู่จากการประเมินความเสี่ยง และการประเมินการควบคุมแล้วให้พิจารณาความเป็นไปได้และค่าใช้จ่ายแต่ละทางเลือก เพื่อตัดสินใจเลือกมาตรการลดความเสี่ยงที่เหมาะสมโดย พิจารณาจาก

1) พิจารณาว่ายอมรับความเสี่ยง หรือจะกำหนดกิจกรรมควบคุมเพื่อลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

2) เปรียบเทียบค่าใช้จ่ายหรือต้นทุนในการจัดการให้มีมาตรการควบคุมกับผลประโยชน์ที่จะได้รับจากมาตรการดังกล่าวว่าคุ้มค่าหรือไม่

3) กรณีเลือกกำหนดกิจกรรมควบคุม เพื่อลดความเสี่ยงให้กำหนดวิธีควบคุมในแผนบริหารความเสี่ยง

4) ในรอบปีต่อไป ให้พิจารณาผลการติดต่อการบริหารความเสี่ยงในงวดก่อนที่ดำเนินการ มาบริหารความเสี่ยงตามกระบวนการเหล่านั้น หากพบว่ายังมีความเสี่ยงที่มีนัยยะสำคัญซึ่งอาจมีผลต่อการบรรลุวัตถุประสงค์ และเป้าหมายตามแผนปฏิบัติงานขององค์กร ให้นำมาระบุการควบคุมในแผนบริหารความเสี่ยง ด้วยการรายงาน ผลการวิเคราะห์ประเมินและบริหารจัดการความเสี่ยงว่ามีความเสี่ยงที่ยังเหลืออยู่หรือไม่ถ้าไม่มีเหลืออยู่ มีอยู่ในระดับความเสี่ยงสูงมากเพียงใด และมีวิธีการจัดการความเสี่ยงนั้นอย่างไรเสนอต่อผู้บริหาร เพื่อทราบและสั่งการ

2.2 ประเภทความเสี่ยงด้านเทคโนโลยีสารสนเทศ

งานเทคโนโลยีสารสนเทศ ได้กำหนดประเภทความเสี่ยงด้านเทคโนโลยีสารสนเทศ เป็น 8 ประเภท ดังนี้

1) ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk) หมายถึง ความเสี่ยงที่เกิดจากภัยคุกคามทั้งภัยจากธรรมชาติ และภัยที่มนุษย์ทำขึ้น เช่น วาตภัย อุทกภัย อัคคีภัย ฟ้าผ่า กระแสไฟฟ้าขัดข้อง การชุมนุมประท้วง การก่อการร้าย รวมถึงการไม่มีระบบรักษาความ ปลอดภัยห้องปฏิบัติการระบบเครือข่ายและคอมพิวเตอร์ เครื่องคอมพิวเตอร์แม่ข่าย และระบบสื่อสารที่มี ประสิทธิภาพเพียงพอ

2) ความเสี่ยงด้านบุคลากร (Human Risk) หมายถึง ความเสี่ยงที่เกิดจากบุคลากรที่เกี่ยวข้องกับการดำเนินงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร ทั้งในด้านการวางแผน การตรวจสอบการทำงาน การมอบหมายหน้าที่และสิทธิ์ของบุคลากร และ คณะทำงานที่มีส่วนเกี่ยวข้องกับการดำเนินการทุกฝ่ายอย่างละเอียด เพื่อให้บุคลากรมีความรู้ ความเข้าใจ ในการ ใช้งาน การดูแลรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งบุคลากรภายนอกที่ เกี่ยวข้องทั้งทางตรงและทางอ้อม ซึ่งล้วนแต่เป็นความเสี่ยงทั้งสิ้น

3) ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร (Hardware and Data Communication Risk) หมายถึง ความเสี่ยงที่เกิดจากความผิดพลาดของอุปกรณ์ การเคลื่อนย้ายตัวเครื่องอุปกรณ์การ ติดตั้งอุปกรณ์ในพื้นที่ไม่เหมาะสม การถูกภัยคุกคามจากภัยต่างๆ เช่น ไวรัสคอมพิวเตอร์ Malware, Trojan, Adware เป็นต้น ทั้งที่เป็นการโจมตีจากภายใน และมาจากภายนอกโดยผ่านทางเครือข่าย (Networks) หรือ จาก คอมพิวเตอร์โดยตรง เช่น จาก USB Flash Drive หรือ USB External Hard Disk Drive เป็นต้น

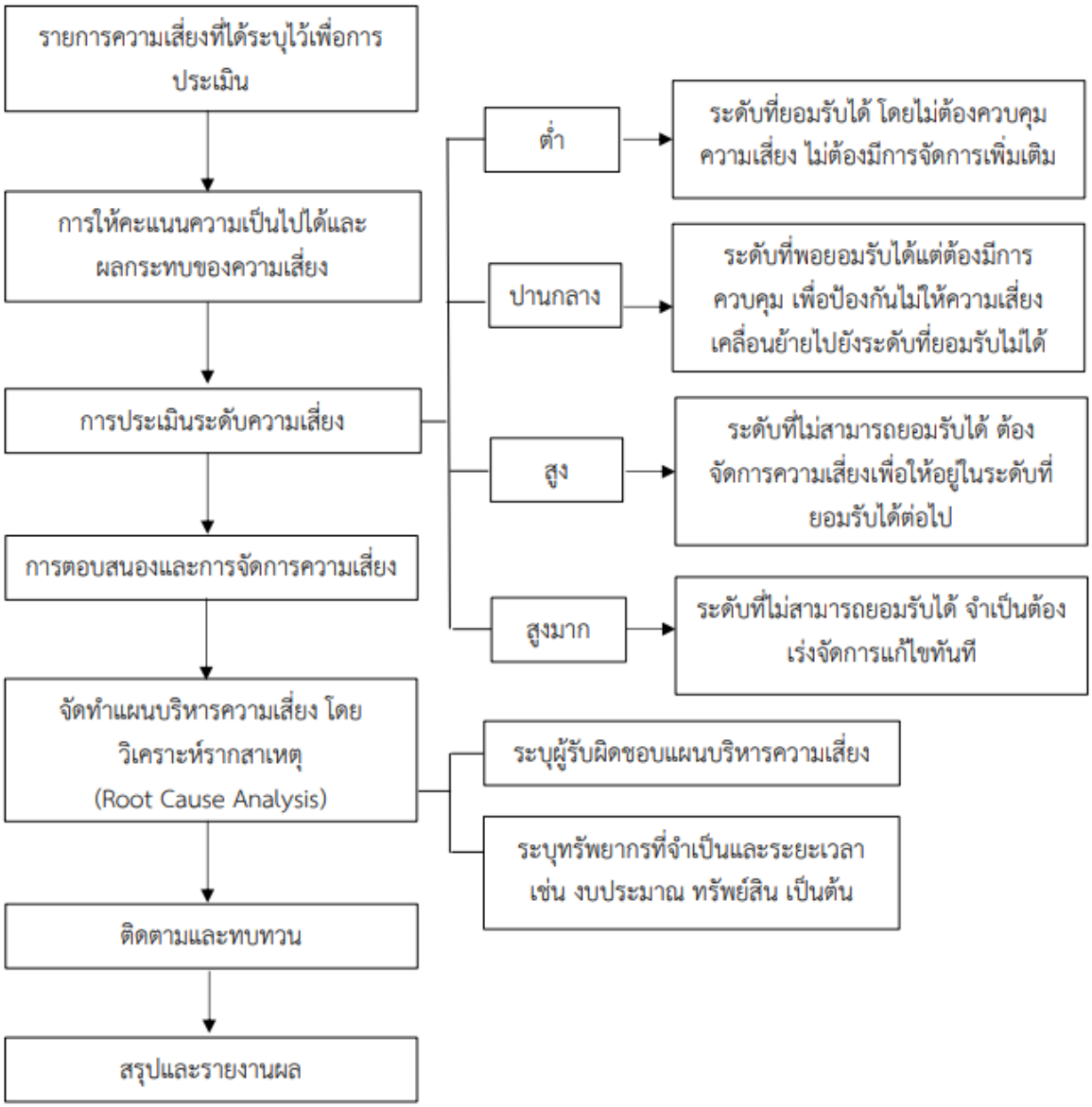
4) ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk) หมายถึง ความเสี่ยงที่เกิดจากระบบการทำงานของโปรแกรมต่างๆ เช่น การใช้โปรแกรมที่ไม่มี การอัพเดทให้ทันสมัยเพื่อลดช่องโหว่ที่อาจเกิดจาก Bug ของซอฟต์แวร์นั้นๆ หรือการถูกผู้ไม่หวังดี (Hacker) เข้ามาทำลายระบบ หรือการใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ ซึ่งคณะฯ อาจถูกฟ้องร้องให้ต้องชำระค่าละเมิดลิขสิทธิ์ เป็นต้น

5) ความเสี่ยงด้านระบบข้อมูล (Database Risk) หมายถึง ความเสี่ยงที่เกิดจากฐานข้อมูลต่างๆ ในระบบสารสนเทศและการสื่อสารอันอาจจะ ก่อให้เกิดความเสียหาย เนื่องจากข้อมูลถูกทำลาย ความเสี่ยงจากผู้บุกรุกข้อมูล เพื่อการโจรกรรมข้อมูลที่สำคัญ การลักลอบเข้ามาแก้ไขเปลี่ยนแปลงข้อมูล ทำให้เกิดความเสียหาย ขาดความน่าเชื่อถือและสร้างความเสื่อมเสีย แก่องค์กรความเสี่ยงเหล่านี้ทำให้มีความจำเป็นที่จะต้องมีการบริหารจัดการความเสี่ยงด้านข้อมูล ดังนั้น การรักษาความปลอดภัยของข้อมูลจึงเป็นเรื่องสำคัญเนื่องจากข้อมูลสารสนเทศและการสื่อสารเป็นปัจจัยสำคัญ สำหรับผู้บริหาร ผู้มีส่วนได้ส่วนเสียโดยตรง รวมถึงประชาชนทั่วไป ดังนั้น การรักษาความปลอดภัยของระบบ ข้อมูลและคอมพิวเตอร์จากภัยต่างๆ ทั้งภัยจากคน ภัยจากธรรมชาติ หรือเหตุการณ์ใดๆ จึงมีความสำคัญและ จำเป็นที่จะต้องมีการป้องกัน เพื่อให้เกิดความมั่นคงต่อระบบข้อมูลสารสนเทศและเทคโนโลยี

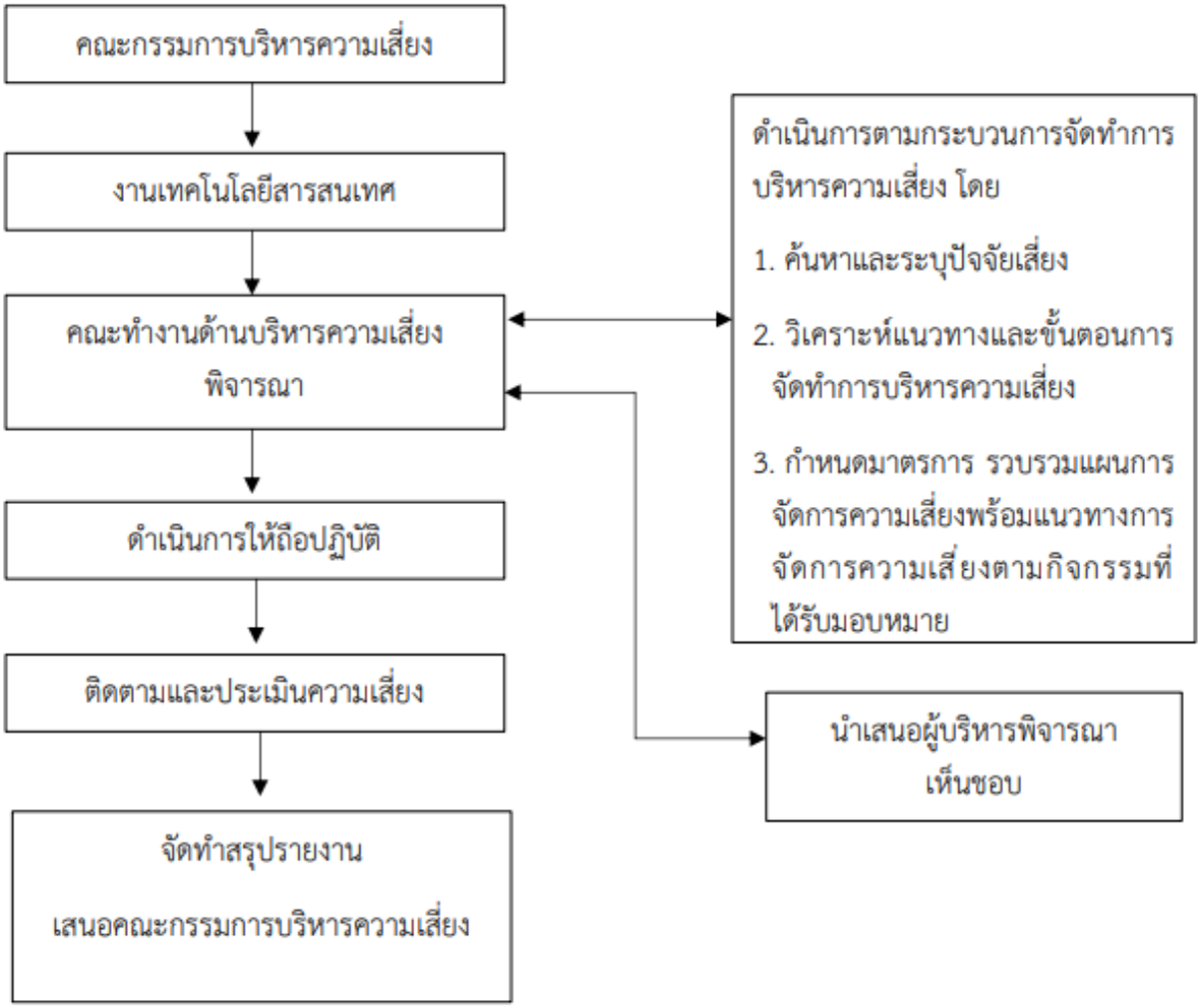
บทที่ 3 กระบวนการบริหารความเสี่ยง

โรงพยาบาลบ่อพลอย ได้ตระหนักถึงความสำคัญของข้อมูลที่อาจประสบกับความเสียหายจากปัจจัยเสี่ยงต่างๆ งานเทคโนโลยีสารสนเทศ จึงจัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศกระบวนการบริหารจัดการความเสี่ยงของหน่วยงานเริ่มต้นจากการรวบรวมข้อมูลที่เกี่ยวข้องกับกิจกรรม/ปัจจัยเสี่ยง หรือกระบวนงานที่มีผลต่อการดำเนินงานด้านเทคโนโลยีสารสนเทศ และทำการศึกษาข้อมูล ระดมความคิดเห็นร่วมกับผู้ปฏิบัติงานด้านกิจกรรมนั้นๆ ดังตารางการบริหารจัดการความเสี่ยงที่ได้จัดทำการวิเคราะห์โดยแยกการวิเคราะห์ ออกเป็นกิจกรรมต่างๆ ดังต่อไปนี้

3.1 แผนภูมิแนวทางและขั้นตอนการบริหารความเสี่ยง



3.2 กระบวนการจัดทำการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ



3.3 การวิเคราะห์ปัจจัยเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ

การระบุความเสี่ยง (Risk identification) เป็นการชี้ให้เห็นถึงความเสี่ยงด้านต่างๆ ที่องค์กรเผชิญอยู่ ผลสรุปการกำหนดประเด็นความเสี่ยงด้านเทคโนโลยีสารสนเทศ รวมทั้งการประเมินระดับความเป็นไปได้ และผลกระทบมีดังนี้

ตารางที่ 1 แบบประเมินจุดอ่อนในระบบเทคโนโลยีสารสนเทศของโรงพยาบาลบ่อพลอย

IT Components	Vulnerability	Score
1. IT - Hardware		
1.1 Server and Main Switches Crash or Failure	อาจแยกประเมิน server แต่ละเครื่องหรือประเมินทั้งห้องร่วมกัน (เลือก 0 หรือ 1 แต่ละข้อ) 1. กายภาพของห้อง server ระบบล็อคประตู [O, 1] =1 ระบบสลับการทำงานเครื่องปรับอากาศ [O , 1] =1 ระบบวัดอุณหภูมิ [0 , 1] =1 ระบบตรวจจับควัน [0 , 1) =1 ระบบแจ้งเตือนอัคคีภัย [0 , 1) =1 ถังดับเพลิงที่เหมาะสม [0, 1) =1 ความสะอาด [0 , 1) 1 การกำจัดสิ่งของไม่จำเป็นและเชื้อไฟออกจากห้อง [O , 1] 0 2. การจัดระเบียบสายสัญญาณและป้ายกำกับ สายสัญญาณด้านหน้า [0 , 1] 1 สายสัญญาณด้านหลัง [0, 1] 0 ป้ายกำกับสายสัญญาณ [0 , 1) 0 ป้ายกำกับ server [0 , 1) 0 แผนผังตำแหน่งสายและช่องสัญญาณ [0 , 1) 0 3. การป้องกันการโจมตีพื้นฐาน มี firewall [0 , 1) 1 เก็บ log [0 , 1) 1 ตรวจสอบ log เป็นระยะ [0, 1] 1 **คะแนน รวม = 11/16**	**3** เกณฑ์ Score 0 ถึง 4 = 5 5 ถึง 7 = 4 8 ถึง 11 = 3 12 ถึง 14 = 2 15 ถึง 16 = 1
1.2 Network Switches Crash or Failure	ประเมิน switches ที่อยู่ในจุดต่างๆ นอกห้อง (เลือก 0 หรือ 1 แต่ละข้อ) 1. กายภาพของตู้ switches มีตู้ [0 , 1] 1 ระบบล็อคประตู [0, 1] 1 ความสะอาด [0, 1] 0	**3** เกณฑ์ Score 0 ถึง 2 = 5 3 ถึง 4 = 4 5 ถึง 6 = 3 7 = 2

IT Components	Vulnerability	Score
	การกำจัดสิ่งของไม่จำเป็นและเชื้อไฟออกจากตู้ [0, 1] 1 2. การจัดระเบียบสายสัญญาณและการป้องกันสัตว์กัดแทะ สายสัญญาณด้านหน้า [O , 1] 1 สายสัญญาณด้านหลัง [O , 1] 0 การป้องกันสัตว์กัดแทะ [O , 1] 0 3. ระบบบำรุงรักษา ตรวจสอบและบำรุงรักษาเป็นประจำ [0, 1] 1 **คะแนน รวม = 5/8**	
1.3 Workstation and Printers Failure	ประเมินภาพรวม PC ที่อยู่ในจุดต่าง ๆ ของโรงพยาบาล (เลือก 0 หรือ 1 แต่ละข้อ) 1.กายภาพของเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง ระบบป้องกันสายไฟสายสัญญาณ [0, 1) 1 ระบบป้องกันไฟตกไฟกระชาก [O, 1) 0 ความสะอาด [O , 1] 0 การป้องกันน้ำและอาหารหกใส่ [0 , 1) 0 ระบบป้องกันคนนอกเข้าถึง [0 , 1] 1 2. ระบบปฏิบัติการและระบบขับเคลื่อน (driver) ถูกลิขสิทธิ์ทั้งหมด [0 , 1) 0 เป็น version ที่ทันสมัยหรือเหมาะสมที่สุด [0, 1) 1 3. ระบบบำรุงรักษา ตรวจสอบและบำรุงรักษาเป็นประจำ [0, 1] 1 **คะแนน รวม = 4/8**	**4** เกณฑ์ Score 0 ถึง 2 = 5 3 ถึง 4 = 4 5 ถึง 6 = 3 7 = 2
2. IT – System Software		
2.1 Operating System Failure	ประเมินภาพรวม OS ที่อยู่ใน server ทั้งหมด ของโรงพยาบาล (เลือก 0 หรือ 1 แต่ละข้อ) 1. ระบบปฏิบัติการและระบบขับเคลื่อน (driver) ถูกลิขสิทธิ์ทั้งหมด [0 , 1] 0 เป็น version ที่ทันสมัยหรือเหมาะสมที่สุด [0 , 1] 1 2. แผ่นติดตั้งระบบปฏิบัติการ ในกรณี ต้องกู้คืนระบบ มีแผ่นติดตั้งครบทั้งหมด [O, 1] 1 **คะแนน รวม = 2/3**	**3** เกณฑ์ Score 0 = 5 1 = 4 2 = 3 3= 1

IT Components	Vulnerability	Score
3. IT- Applications		
3.1 Front Offices	ประเมินระบบ HIS ที่ใช้บริการส่วนหน้าทั้งหมดของโรงพยาบาล (เลือก 0 หรือ 1 แต่ละข้อ) 1. การใช้ทรัพยากรของ server CPU ไม่ overload [0 , 1] 1 หน่วยความจำยังไม่หมด [0 , 1] 1 พื้นที่ hard disk ยังเพียงพอ [0, 1] 1 2. แผ่นติดตั้งระบบ HIS ในกรณี ต้องกู้คืนระบบ มีแผ่นติดตั้งครบทั้งหมด [0 , 1] 1 3. ระบบบำรุงรักษา ตรวจสอบและบำรุงรักษาเป็นประจำ [0, 1] 1 **คะแนนรวม = 5/5**	**1** เกณฑ์ Score 0 ถึง 1 = 5 2 = 4 3 = 3 4 = 2
3.2 Back Offices	ประเมินระบบที่ใช้บริการส่วนหลังทั้งหมดของโรงพยาบาล (เลือก 0 หรือ 1 แต่ละข้อ) 1.การใช้ทรัพยากรของ server CPU ไม่ overload [0 , 1] 1 หน่วยความจำยังไม่หมด [0, 1) 1 พื้นที่ hard disk ยังเพียงพอ [O, 1] 1 2. แผ่นติดตั้งระบบ HIS ในกรณี ต้องกู้คืนระบบ มีแผ่นติดตั้งครบทั้งหมด [0, 1) 1 3. ระบบบำรุงรักษา ตรวจสอบและบำรุงรักษาเป็นประจำ [0, 1] 1 **คะแนนรวม = 5/5**	**1** เกณฑ์ Score 0 ถึง 1 = 5 2 = 4 3 = 3 4 = 2
4. IT- Communication, Connectivity		
4.1 Intranet	ประเมินระบบเครือข่ายภายในของโรงพยาบาล (เลือก 0 หรือ 1 แต่ละข้อ) 1. การใช้ทรัพยากรของระบบเครือข่าย traffic ไม่เกินร้อยละ 80 [0 , 1] 1 bandwidth ไม่เกินร้อยละ 80 [0 , 1] 1 2. การแยกวง เช่น vlan มีการแยกวงที่เหมาะสม [0, 1) 0 แยกระบบ HIS ออกจากระบบอินเทอร์เน็ต [0, 1] 0	**3** เกณฑ์ Score 0 ถึง 1 = 5 2 = 4 3 = 3 4 = 2

IT Components	Vulnerability	Score
	3. ระบบบำรุงรักษา ตรวจสอบและบำรุงรักษาเป็นประจำ [0, 1] 1 **คะแนนรวม = 3/5**	
4.2 Internet	ประเมินระบบเครือข่ายที่เชื่อมต่ออินเทอร์เน็ตของโรงพยาบาล (เลือก 0 หรือ 1 แต่ละข้อ) 1. การใช้ทรัพยากรของระบบเครือข่าย Traffic ไม่เกินร้อยละ 80 [0 , 1] 1 bandwidth ไม่เกินร้อยละ 80 [0 , 1] 1 2. การเพิ่มสายสำรอง กรณีผู้ให้บริการหยุดชะงัก มีสายสำรองที่ 2 [0, 1)1 มีสายสำรองที่ 3 [0, 1)1 3. ระบบบำรุงรักษา 1 **คะแนนรวม = 5/5**	**1** เกณฑ์ Score 0 ถึง 1 = 5 2 = 4 3 = 3 4 = 2
5. IT – Operational (Human) Error		
5.1 Backup Error	ประเมินระบบงานที่ทำให้การสำรองข้อมูลเกิดความผิดพลาด (เลือก 0 หรือ 1 แต่ละข้อ) 1. ขั้นตอนการปฏิบัติงานที่เหมาะสม มีขั้นตอนการปฏิบัติงานชัดเจน [O, 1) 1 ผู้สำรองข้อมูลเข้าใจและปฏิบัติได้ถูกต้อง [0 , 1] 1 2. ระบบตรวจสอบข้อมูลสำรอง มีระบบตรวจสอบความครบถ้วนสมบูรณ์ [O, 1] 1 มีการทดลอง restore กลับ [0 , 1] 1 3. ระบบกำกับดูแลโดยผู้บังคับบัญชา กำกับดูแลเป็นประจำ [0, 1) 1 **คะแนนรวม = 5/5**	**1** เกณฑ์ Score 0 ถึง 1 = 5 2 = 4 3 = 3 4 = 2
5.2 Data Loss Error	ประเมินระบบงานที่ทำให้ข้อมูลที่ผู้ใช้บันทึกไม่เกิดความผิดพลาด (เลือก 0 หรือ 1 แต่ละข้อ) 1. ขั้นตอนการปฏิบัติงานที่เหมาะสม มีขั้นตอนการปฏิบัติงานชัดเจน [0, 1] 1 ผู้บันทึกข้อมูลเข้าใจและปฏิบัติได้ถูกต้อง [0, 1] 1 2. ระบบป้องกันข้อมูลสูญหายหรือผิดพลาด ปิดช่องว่างจากขันตอนการทำงาน [0, 1] 0 ปิดช่องว่างจากโปรแกรม [O, 1) 0	**3** เกณฑ์ Score 0 ถึง 1 = 5 2 = 4 3 = 3 4 = 2

IT Components	Vulnerability	Score
	3. ระบบกำกับดูแลโดยผู้บังคับบัญชา กำกับดูแลเป็นประจำ [0, 1) 1 **คะแนนรวม = 3/5**	
6. Data Loss and Privacy Breach		
6.1 Data Backup	ประเมินระบบงานที่ทำให้ข้อมูลสำรองสูญหาย (เลือก 0 หรือ 1 แต่ละข้อ) 1. ระบบ offline backup มีระบบ offline backup [0 , 1] 1 อุปกรณ์เก็บข้อมูลสำรองมีจำนวนเพียงพอ [0, 1] 1 อุปกรณ์เก็บข้อมูลสำรองมีที่เก็บปลอดภัย [0, 1] 0 2. ระบบป้องกันข้อมูลสำรองถูกจารกรรม มีระบบห้ามบุคลากรนำข้อมูลสำรองออกสู่ภายนอก [0, 1) 1 3. ระบบกำกับดูแลโดยผู้บังคับบัญชา กำกับดูแลเป็นประจำ [O , 1] 1 **คะแนนรวม=4/5**	**2** เกณฑ์ Score 0 ถึง 1 = 5 2 = 4 3 = 3 4 = 2
6.2 Data Protection Policy and Regulations	ประเมินการป้องกันความลับและความเป็นส่วนตัวของข้อมูล (เลือก 0 หรือ 1 แต่ละข้อ) 1.ระบบห้ามการเข้าถึงข้อมูลที่บุคลากรไม่มีส่วนเกี่ยวข้อง มีระบบล็อคหรือมีระเบียบห้ามการเข้าถึงข้อมูลที่ตนเองไม่มีส่วนเกี่ยวข้อง [0 , 1] 1 2. ระบบอภิบาลข้อมูล มีการสำรวจและจัดทำทะเบียนข้อมูลสำคัญ [0, 1) 1 มีการจัดประเภทข้อมูลที่ต้องปกปิด [0 , 1] 1 มีขั้นตอนการจัดการข้อมูลสำคัญตั้งแต่ต้นทางจนถึงปลายทาง [0 , 1] 1 3. ระบบกำกับดูแลโดยผู้บังคับบัญชา กำกับดูแลเป็นประจำ [0 , 1] 0 **คะแนนรวม=4/5**	**2** เกณฑ์ Score 0 ถึง 1 = 5 2 = 4 3 = 3 4 = 2
6.3 PDPA Implementation	ประเมินการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล ให้คะแนน 0 ถึง 5	**1**

IT Components	Vulnerability	Score
7. IT – Future Development		
7.1 No Data Dictionary	ประเมินเอกสารที่ใช้พัฒนาระบบต่อเนื่องในอนาคต (เลือก 0 หรือ 1) มีเอกสาร Data Dictionary ครบทุกตารางในฐานข้อมูล [0, 1) 0	**5**
7.2 No System Blueprint	ประเมินเอกสารที่ใช้พัฒนาระบบต่อเนื่องในอนาคต (เลือก 0 หรือ 1) 0 มีเอกสาร วิเคราะห์และออกแบบระบบ ที่พัฒนาเอง [0 , 1] 0	**5**
7.3 No System Document or Comments	ประเมินการบันทึก comment และ version ของ ผู้พัฒนาโปรแกรม (เลือก 0 หรือ 1) 0 มีเอกสาร version control และ source code comment [0, 1) 0	**5**
8. IT – Vendor and Outsource Failure		
8.1 Vendor stop Support	ประเมินสัญญาที่ทำกับบริษัทภายนอก (เลือก 0 หรือ 1) มีสัญญาที่บริษัทจะต้องส่งมอบเอกสารสำคัญและข้อมูลทั้งหมด เมื่อหมดสัญญา [0 , 1] 1	**1**
9. IT – Hacking Unauthorized Intrusions		
	ประเมินภาพรวมจุดต่าง ๆ ของโรงพยาบาล (เลือก 0 หรือ 1 แต่ละข้อ) 1. เครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง มีระบบหรือระเบียบล็อคหน้าจอเมื่อไม่มีผู้ใช้งาน [O, 1] 1 เข้ารหัสข้อมูลส่วนตัวผู้ป่วย [0 , 1] 1 มีการป้องกันการถ่ายภาพหน้าจอในจุดที่คนนอกเข้าถึง [0, 1] 0 2. ระบบเครือข่าย ปิดสัญญาณช่องเชื่อมต่อเครือข่ายที่ไม่มีการใช้งาน [0, 1] 1 มีการเข้ารหัสและตั้งรหัสผ่านการใช้ wifi access [0, 11 1 เปลี่ยนรหัส wifi บ่อย ๆ [O, 1] 0 3. ระเบียบปฏิบัติด้านความมั่นคงปลอดภัย ห้ามใช้ username ร่วมกัน [O , 1] 1 ตั้ง username และ password ซับซ้อน [O, 1] 1	**2** เกณฑ์ Score 0 ถึง 2 = 5 3 ถึง 4 = 4 5 ถึง 6 = 3 7 = 2

IT Components	Vulnerability	Score
	ห้ามติด password ไว้ในที่เปิดเผย [0 , 1] 1 **คะแนนรวม=7/8**	
10. Environment Factors		
10.1 Flooding – Internal	10.1 Flooding – Internal ประเมินจุดอ่อนที่ทรัพย์สิน IT อาจเสียหายจากน้ำรั่วในสำนักงาน (เลือก 0 หรือ 1) มีระบบป้องกันไม่ให้น้ำรั่วไหลลงสู่ทรัพย์สิน IT 0 1 1	**1**
	10.2 Flooding – External ประเมินจุดอ่อนที่ทรัพย์สิน IT อาจเสียหายจากอุทกภัยในพื้นที่ (เลือก 0 หรือ 1) มีระบบป้องกันไม่ให้อุทกภัยสร้างความเสียหายต่อทรัพย์สิน IT [0 , 1] 1	**1**
	10.3 Fire – Internal ประเมินจุดอ่อนที่ทรัพย์สิน IT อาจเสียหายจากไฟไหม้ในโรงพยาบาล (เลือก 0 หรือ 1) มีระบบป้องกันไม่ให้ไฟไหม้ทรัพย์สิน IT [0 , 1] 1	**1**
	10.4 Fire – External ประเมินจุดอ่อนที่ทรัพย์สิน IT อาจเสียหายจากอัคคีภัยในพื้นที่ (เลือก 0 หรือ 1) มีระบบป้องกันไม่ให้ไฟไหม้ทรัพย์สิน IT [0 , 1] 0	**5**
	10.5 Utilities – Electricity ประเมินจุดอ่อนที่ทรัพย์สิน IT อาจเสียหายจากไฟฟ้าตกหรือกระชาก (เลือก 0 หรือ 1) มีระบบป้องกันไม่ให้ไฟฟ้าสร้างความเสียหายต่อทรัพย์สิน IT [0 , 1] 0	**5**
	10.6 Criminal – Theft ประเมินจุดอ่อนที่ทรัพย์สิน IT อาจเสียหายจากโจรกรรม (เลือก 0 หรือ 1) มีระบบป้องกันไม่ให้มีโจรหรือขโมยสร้างความเสียหายต่อทรัพย์สิน IT [0 , 1] 0	**5**
	10.7 Criminal – Break-ins ประเมินจุดอ่อนที่ทรัพย์สิน IT อาจเสียหายจากการงัดแงะหรือย่อง	**1**

IT Components	Vulnerability	Score
	เบา (เลือก 0 หรือ 1) มีระบบป้องกันไม่ให้มีโจรหรือขโมยสร้างความเสียหายต่อทรัพย์สิน IT [0 , 1] 1	
	10.8 Civil Unrest – Protest, Mob ประเมินจุดอ่อนที่ทรัพย์สิน IT อาจเสียหายจากเหตุจลาจล วัยรุ่นทะเลาะกัน (เลือก 0 หรือ 1) มีระบบป้องกันไม่ให้มีผู้สร้างความเสียหายต่อทรัพย์สิน IT [0, 1] 0	**5**
11. Patient Risks due to IT Errors/Misuse		
	ประเมินจุดอ่อนการใช้ IT ที่อาจทำให้เกินอันตรายต่อผู้ป่วย (เลือก 0 หรือ 1 แต่ละข้อ) 1. ระบบแจ้งเตือนเมื่อพบค่าวิกฤต มีระบบแจ้งเตือนเมื่อพบค่าวิกฤตของผู้ป่วย [0, 1] 1 มีการแจ้งเตือนผู้เกี่ยวข้องทันที [0, 1] 1 มีการตรวจสอบว่าระบบแจ้งเตือนทำงานได้ตามปกติ [0, 1] 0 2. ระบบตรวจสอบการสั่งการรักษาหรือไม่สั่งการรักษาที่เหมาะสม มีระบบตรวจสอบการสั่งการรักษาที่เหมาะสม [0, 1] 1 มีระบบตรวจสอบการไม่สั่งการรักษาที่เหมาะสมและแจ้งเตือน [0, 1] 0 3. ระบบป้องกันความผิดพลาดในการบันทึกข้อมูล ตรวจสอบบุคคลหัวหน้าตรวจสอบ มีระบบป้องกันความผิดพลาดในการบันทึกข้อมูล [0, 1] 1 มีระบบตรวจสอบบุคคลแบบ double check [0, 1] 1 มีระบบหัวหน้ายืนยันการดำเนินการกรณีสำคัญยิ่งยวด [0, 1] 1 **คะแนนรวม=6/8**	**3** เกณฑ์ Score 0 ถึง 2 = 5 3 ถึง 4 = 4 5 ถึง 6 = 3 7 = 2

ความเสี่ยงมาพิจารณา ตามแผนผังประเมินความเสี่ยง ดังนี้

Risk Value			Probability				
			Very Low	Low	Medium	High	Very High
			1	2	3	4	5
Impact	Very High	5	5	10	15	20	25
	High	4	4	8	12	16	20
	Medium	3	3	6	9	12	15
	Low	2	2	4	6	8	10
	Very Low	1	1	2	3	4	5

จากแผนผังประเมินความเสี่ยง จะเห็นว่า เหตุการณ์ที่มีค่าคะแนนความเสี่ยงตั้งแต่ 17 ถึง 25 จะเป็นเหตุการณ์ที่เร่งต้องจัดการความเสี่ยงโดยเร่งด่วน (แสดงในตารางเป็นสีแดง) ส่วนเหตุการณ์ที่มีค่าคะแนนความเสี่ยง ตั้งแต่ 1-3 จะเป็นเหตุการณ์ที่ยังไม่ต้องเร่งรีบจัดการ (แสดงในตารางเป็นสีเหลือง)

ตารางที่ 2 ตารางเกณฑ์ความสามารถในการยอมรับความเสี่ยง

ความเสี่ยง	คะแนน	แถบสี	ความหมาย
ต่ำ	**1-3**		Acceptable or Limited Focus ระดับที่ยอมรับได้ โดยไม่ต้องควบคุมความเสี่ยง ไม่ต้องมีการจัดการ เพิ่มเติม
ปานกลาง	**4-9**		Tolerable but caution or Management Discretion/Medium Risk ระดับที่พอยอมรับได้ แต่ต้องมีการควบคุม เพื่อป้องกันไม่ให้ความเสี่ยง เคลื่อนย้ายไปยังระดับที่ยอมรับไม่ได้
สูง	**10-16**		Intolerable or Attention Required/High Risk ระดับที่ไม่สามารถยอมรับได้โดยต้องจัดการความเสี่ยง เพื่อให้อยู่ใน ระดับที่ยอมรับได้ต่อไป
สูงมาก	**17-25**		Intolerable or Immediate Attention Require/High Risk ระดับที่ไม่สามารถยอมรับได้จำเป็นต้องเร่งจัดการควบคุมให้อยู่ใน ระดับที่ยอมรับได้ทันที

ตารางที่ 3 การประเมินจุดอ่อนในระบบเทคโนโลยีสารสนเทศ ปี พ.ศ. 2567

IT Components	Probability(P)	Impact (I)	Risk = P x I
1. IT - Hardware			
1.1 Server and Main Switches Crash or Failure	3	5	15
1.2 Network Switches Crash or Failure	3	2	6
1.3 Workstation and Printers Failure	4	3	12
2. IT – System Software			
2.1 Operating System Failure	3	3	9
3. IT- Applications			
3.1 Front Offices	1	5	5
3.2 Back Offices	1	5	5
4. IT- Communication, Connectivity			
4.1 Intranet	3	3	9
4.2 Internet	1	3	3
5. IT – Operational (Human) Error			
5.1 Backup Error	1	5	5
5.2 Data Loss Error	3	5	15
6. Data Loss and Privacy Breach			
6.1 Data Backup	2	5	10
6.2 Data Protection Policy and Regulations	2	4	8
6.3 PDPA Implementation	1	4	4
7. IT – Future Development			
7.1 No Data Dictionary	5	1	5
7.2 No System Blueprint	5	1	5
7.3 No System Document or Comments	5	1	5
8. IT – Vendor and Outsource Failure			
8.1 Vendor stop Support	1	5	5
9. IT – Hacking Unauthorized Intrusions	2	5	10
10. Environment Factors			
10.1 Flooding – Internal	1	5	5
10.2 Flooding – External	1	2	2
10.3 Fire – Internal	1	5	5

IT Components	Probability(P)	Impact (I)	Risk = P x I
10.4 Fire – External	5	5	25
10.5 Utilities – Electricity	5	3	15
10.6 Criminal – Theft	5	5	25
10.7 Criminal – Break-ins	1	5	5
10.8 Civil Unrest – Protest, Mob	5	2	10
11. Patient Risks due to IT Errors/Misuse	3	4	12

กลยุทธ์ในการแก้ไขความเสี่ยง

กลยุทธ์ที่ 1 การลดความเสี่ยง

กลยุทธ์ที่ 2 การย้าย/**การถ่ายโอน** ความเสี่ยง

กลยุทธ์ที่ 3 การหลีกเลี่ยงความเสี่ยง

กลยุทธ์ที่ 4 การยอมรับความเสี่ยง

ตารางที่ 4 กลยุทธ์ในการแก้ไขความเสี่ยง จุดอ่อนในระบบเทคโนโลยีสารสนเทศ ปี พ.ศ. 2567

เหตุการณ์ที่ทำให้เกิดความเสี่ยง	ค่าระดับความเสี่ยง	เป้าหมายในการควบคุม	มาตรการควบคุม
1. Fire – External ประเมินจุดอ่อนที่ทรัพย์สิน IT อาจเสียหายจากไฟไหม้ในโรงพยาบาล	สูงมาก	ลดโอกาสที่จะเกิดเหตุการณ์	1. จัดทำแผนอบรมให้ความรู้และทักษะที่จำเป็น ให้ความรู้เกี่ยวกับอัคคีภัย 2. จัดทำนโยบาย ระเบียบปฏิบัติเพื่อรักษาความมั่นคงปลอดภัย ระบบอัคคีภัย เผยแพร่พร้อมประเมินการรับรู้ความเข้าใจของบุคลากร 3. ซ้อมแผนอัคคีภัยในทุกๆปีเพื่อความพร้อม อุปกรณ์เครื่องมือดับเพลิงครอบคลุมทุกจุดในโรงพยาบาล 4. ใช้ 5 ส และ Lean มาดำเนินการ
		ลดผลเสียหายที่จะเกิดเหตุการณ์	1. ปรับปรุงพัฒนาระบบอัคคีภัยแบบอัตโนมัติให้ครอบคลุมทุกจุด 2. จัดทำแผนรับสถานการณ์เพื่อให้สามารถดำเนินการได้อย่างต่อเนื่อง (Business Continuity Plan : BCP)

เหตุการณ์ที่ทำให้เกิดความเสี่ยง	ค่าระดับความเสี่ยง	เป้าหมายในการควบคุม	มาตรการควบคุม
2. Criminal – Theft ประเมินจุดอ่อนที่ทรัพย์สิน IT อาจเสียหายจากโจรกรรม	สูงมาก	ลดโอกาสที่จะเกิดเหตุการณ์	1. ทำงานร่วมกับทีม ENV ของโรงพยาบาล ประเมินอาคาร สถานที่ เพื่อจัดทำแผน 2. จัดทำแบบการประเมินความเสี่ยงทุกจุดในโรงพยาบาลบ่อพลอย พร้อมวิเคราะห์ เพื่อหาความเสี่ยง 3. จัดทำนโยบาย ระเบียบปฏิบัติเพื่อรักษาความมั่นคงปลอดภัย ความเสียหายอันเกิดจากการโจรกรรม พร้อมประเมินความพร้อมของบุคลากรโรงพยาบาลบ่อพลอย
		ลดผลเสียหายที่จะเกิดเหตุการณ์	1. ติดตั้งระบบกล้องวงจรปิดเพิ่มเติม พร้อมตรวจสอบการทำงานในทุกๆวันให้สามารถตอบสนองได้ทันที เมื่อเกิดอุบัติการณ์ 2. จัดทำแผนรับสถานการณ์เพื่อให้สามารถดำเนินการได้อย่างต่อเนื่อง (Business Continuity Plan : BCP)
		ย้ายกระบวนการป้องกันโอกาสที่จะเกิดเหตุการณ์	1. ปรับปรุงพัฒนาระบบกล้องวงจรปิดให้ครอบคลุมทุกจุดภายในโรงพยาบาลบ่อพลอย 2. จัดจ้าง เจ้าหน้าที่ในการเฝ้าระวังต่อการโจรกรรม ให้ครอบคลุม
3. IT Hacking Unauthorized Intrusions	สูง	ลดโอกาสที่จะเกิดเหตุการณ์	1. จัดทำแผนอบรมให้ความรู้และทักษะที่จำเป็น ให้ความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ วิธีป้องกันตนเองจากโจมตีทางไซเบอร์ 2. จัดทำนโยบาย ระเบียบปฏิบัติเพื่อรักษาความมั่นคงปลอดภัย ในระบบเทคโนโลยีสารสนเทศ เผยแพร่ พร้อมประเมินการรับผู้ของบุคคลกรโรงพยาบาลบ่อพลอย 3. จัดทำระบบ Domain Controller เพื่อนำมาบริหาร จัดการในระบบเครือข่าย 4. จัดหา ติดตั้งโปรแกรม ชุดโปรแกรมป้องกันไวรัส (Anti Virus) และปรับปรุงโปรแกรมให้ทันสมัยอยู่เสมอ 5. จัดหาซอฟแวร์ลิขสิทธิ์ เช่น windows,

เหตุการณ์ที่ทำให้เกิดความเสี่ยง	ค่าระดับความเสี่ยง	เป้าหมายในการควบคุม	มาตรการควบคุม
			office ฯลฯ เพื่อลดช่องโวในการโจมตีจากภายนอก 6. ตรวจสอบการทำงานของ Firewall ที่ระบบคอมพิวเตอร์ส่วนกลางที่เป็นทางผ่านเข้าออกไปยังระบบเครือข่ายภายนอก และ Update Patch
		ลดผลเสียหายที่จะเกิดเหตุการณ์	1. ปรับปรุงพัฒนาระบบเครือข่าย ออกแบบระบบ VLAN และ IP Network ให้สอดรับกับความจำเป็นในการใช้งาน 2. จัดทำแผนรับสถานการณ์เพื่อให้สามารถดำเนินการได้อย่างต่อเนื่อง (Business Continuity Plan : BCP)
4. Server and Main Switches Crash or Failure	สูง	ลดโอกาสที่จะเกิดเหตุการณ์	1. จัดทำแบบการประเมินการทำงานของอุปกรณ์ Computer Server ,UPS, Main Switches ทำการตรวจสอบ ควบคุม กำกับดูแล โดยผู้ได้รับมอบหมายจาก คณะกรรมการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศโรงพยาบาลบ่อพลอย 2. ปรับปรุง ห้อง Server ดังนี้ 2.1 ปรับปรุงระบบล็อคประตู จากกุญแจเป็น ระบบแสกนลายนิ้วมือเพื่อเข้าห้อง พร้อมจัดเก็บประวัติการเข้าห้อง 2.2 จัดหาอุปกรณ์วัดอุณหภูมิ ความชื้น ตรวจจับควัน พร้อมบันทึกผล 2.3 ติดตั้งระบบดับเพลิงอัตโนมัติ ภายในห้อง Server
		ลดผลเสียหายที่จะเกิดเหตุการณ์	1. ติดตั้งระบบเครือข่ายสำรองที่สามารถใช้งานจริงได้ในทันทีเมื่อเครือข่ายหยุดทำงาน โดยติดตั้งไว้อิสระจากระบบจริง 2. จัดทำแผนรับสถานการณ์เพื่อให้สามารถ

เหตุการณ์ที่ทำให้เกิดความเสี่ยง	ค่าระดับความเสี่ยง	เป้าหมายในการควบคุม	มาตรการควบคุม
			ดำเนินการได้อย่างต่อเนื่อง (Business Continuity Plan : BCP)
5. Data Loss Error ประเมินระบบงานที่ทำให้ข้อมูลที่ผู้ใช้บันทึกไม่เกิดความผิดพลาด	สูง	ลดโอกาสที่จะเกิดเหตุการณ์	1. อบรมพัฒนาศักยภาพของเจ้าหน้าที่ ให้มีความรู้ความเข้าใจในการบันทึกข้อมูลให้ถูกต้องครบถ้วน สมบูรณ์ 2. ปรับปรุงพัฒนาระบ HIS ให้เป็นปัจจุบันและสามารถนำข้อมูลไปใช้งานได้อย่างถูกต้อง มีการตรวจสอบข้อมูลอยู่สม่ำเสมอ เพื่อป้องกันความผิดพลาด
6. Utilities – Electricity	สูง	ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)	1. ป้องกันความเสี่ยงเสียหายจากไฟฟ้าตกหรือกระชาก รวมถึงทบทวนมาตรการ และแนวปฏิบัติ ปีละ 1 ครั้ง 2. ปรับปรุงระบบไฟฟ้าเป็น 3 เฟส และแยกระบบไฟฟ้าออกจากระบบภายในโรงพยาบาล 3. จัดทำโครงการจัดซื้อเครื่องสำรองไฟให้กับจุดบริการให้ครอบคลุมการใช้งาน ที่จำเป็นและเหมาะสม

แผนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

งานเทคโนโลยีสารสนเทศ โรงพยาบาลบ่อพลอย

ระดับความเสี่ยงที่จัดทำแผนการบริหารความเสี่ยง : ปานกลาง - สูง

วัตถุประสงค์ : เพื่อให้การดำเนินงานด้านการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศของโรงพยาบาลบ่อพลอย บรรลุเป้าประสงค์ของการบริหารความเสี่ยง

ผู้รับผิดชอบ : งานเทคโนโลยีสารสนเทศ

ประเภทความเสี่ยง/กิจกรรม	แผนปฏิบัติ	ระยะเวลา	ปีงบ 2567				ปีงบ 2568				ปีงบ 2569				งบประมาณ	ผลลัพธ์ความก้าวหน้า
			ไตรมาส				ไตรมาส				ไตรมาส					
			1	2	3	4	1	2	3	4	1	2	3	4		
1.Fire -External	1.อบรมให้ความรู้และทักษะที่จำเป็นให้ความรู้เกี่ยวกับอัคคีภัย	ปีละ1 ครั้ง			↔				↔				↔			ระดับความเสี่ยงลดลง จาก 25 (สูงมาก) เหลือ 15 (สูง)
	2.จัดทำแผนอัคคีภัย เพื่อรักษาความมั่นคงปลอดภัยระบบอัคคีภัยร่วมกับทีม ENV				↔				↔				↔			
	3.ซ้อมแผนอัคคีภัย เพิ่มความพร้อมของบุคลากร อุปกรณ์ดับเพลิง				↔				↔				↔		30,000 บาท/ปี	
	4. จัดหาระบบอัคคีภัยภายในอาคารแบบระบบอัตโนมัติ									↔					1,000,000 บาท	

ประเภทความเสี่ยง/กิจกรรม	แผนปฏิบัติ	ระยะเวลา	ปีงบ 2567				ปีงบ 2568				ปีงบ 2569				งบประมาณ	ผลลัพธ์ความก้าวหน้า
			ไตรมาส				ไตรมาส				ไตรมาส					
			1	2	3	4	1	2	3	4	1	2	3	4		
2. Criminal – Theft	1. ทำงานร่วมกับทีม ENV ประเมินความเสี่ยงให้ครอบคลุม พร้อมประชุมร่วมกันวิเคราะห์หาจุดเสี่ยงภายใน รพ.	2 ครั้ง/ปี	↔		↔		↔		↔		↔		↔			ระดับความเสี่ยงลดลง จาก 25 (สูงมาก) เหลือ 15 (สูง)
	2. ปรับปรุงและติดตั้งระบบกล้องวงจรปิดให้ครอบคลุมทุกจุดเสี่ยง	ปีเว้นปี			↔								↔		800,000 บาท	
	3. จัดทำแผนรับสถานการณ์เพื่อให้สามารถดำเนินการได้อย่างต่อเนื่อง (Business Continuity Plan : BCP)	1 ครั้ง/ปี	↔				↔				↔					
	4.จัดเวรยามรักษาความปลอดภัย/เฝ้าระวังต่อการโจรกรรม ให้ครอบคลุมทุกพื้นที่ ตลอด 24 ชม.		←	—	—	—	—	—	—	—	—	—	—	→		

ประเภทความเสี่ยง/กิจกรรม	แผนปฏิบัติ	ระยะเวลา	ปีงบ 2567				ปีงบ 2568				ปีงบ 2569				งบประมาณ	ผลลัพธ์ความก้าวหน้า
			ไตรมาส				ไตรมาส				ไตรมาส					
			1	2	3	4	1	2	3	4	1	2	3	4		
IT Hacking Unauthorized Intrusions	1. อบรมให้ความรู้และทักษะที่จำเป็นให้ความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์	ปีละ1 ครั้ง			↔				↔				↔			ระดับความเสี่ยงลดลง จาก 20 (สูงมาก) เหลือ 15 (สูง)
	2. จัดทำนโยบาย ระเบียบปฏิบัติเพื่อรักษาความมั่นคงปลอดภัย ในระบบเทคโนโลยี		↔				↔				↔					
	3. จัดทำระบบ Domain Controller เพื่อนำมาบริหารจัดการในระบบเครือข่าย			↔	↔										30,000 บาท	
	4. จัดหา ติดตั้งโปรแกรม ชุดโปรแกรมป้องกันไวรัส และปรับปรุงโปรแกรมให้ทันสมัย		↔	↔	↔	↔	↔	↔	↔	↔	↔	↔	↔	→	140,000 บาท	
	5. จัดทำโครงการจัดซื้อคอมพิวเตอร์ หรือ จัดหาซอฟแวร์ลิขสิทธิ์	ปีละ1 ครั้ง	↔				↔				↔				1,600,000 บาท	ระดับความเสี่ยงลดลง จาก 25 (สูงมาก) เหลือ 15 (สูง)
	6. ตรวจสอบการทำงานของ Firewall ที่ระบบคอมพิวเตอร์ส่วนกลางที่เป็นทางผ่านเข้าออกไปยังระบบเครือข่ายภายนอก และ Update Patch	ทุกวัน	↔	↔	↔	↔	↔	↔	↔	↔	↔	↔	↔	→		

ประเภทความเสี่ยง/กิจกรรม	แผนปฏิบัติ	ระยะเวลา	ปีงบ 2567				ปีงบ 2568				ปีงบ 2569				งบประมาณ	ผลลัพธ์ความก้าวหน้า
			ไตรมาส				ไตรมาส				ไตรมาส					
			1	2	3	4	1	2	3	4	1	2	3	4		
	7. ปรับปรุงพัฒนาระบบเครือข่าย ออกแบบระบบ VLAN และ IP Network ให้สอดรับกับความจำเป็นในการใช้งาน							←	—	→					1,000,000 บาท	
4. Server and Main Switches Crash or Failure	1. จัดทำแบบการประเมินการทำงานของอุปกรณ์ Computer Server ,UPS, Main Switches ทำการตรวจสอบ ควบคุม กำกับ ดูแล โดยทีมเทคโนโลยีสารสนเทศ				←	—	—	—	—	—	—	—	—	→		ระดับความเสี่ยงลดลง จาก 15 (สูง) เหลือ 9 (ปานกลาง)
	2. ปรับปรุงระบบล็อคประตู จากกุญแจ เป็น ระบบแสกนลายนิ้วมือ		←	→											12,000 บาท	
	3. จัดหาอุปกรณ์วัดอุณหภูมิและความชื้น พร้อมบันทึกผล		←	→											2,000 บาท	

ประเภทความเสี่ยง/กิจกรรม	แผนปฏิบัติ	ระยะเวลา	ปีงบ 2567				ปีงบ 2568				ปีงบ 2569				งบประมาณ	ผลลัพธ์ความก้าวหน้า
			ไตรมาส				ไตรมาส				ไตรมาส					
			1	2	3	4	1	2	3	4	1	2	3	4		
	4.ติดตั้งระบบเครือข่ายสำรองที่สามารถใช้งานจริงได้ในทันทีเมื่อเครือข่ายหยุดทำงาน โดยติดตั้งไว้อิสระจากระบบจริง (DR Siite)		↔	↔											60,000 บาท	
	5.จัดทำแผนรับสถานการณ์เพื่อให้สามารถดำเนินการได้อย่างต่อเนื่อง (Business Continuity Plan)	ปีละ1 ครั้ง			↔				↔				↔			
5. Data Protection Policy and Regulations การป้องกันความลับและความเป็นส่วนตัวของข้อมูล	1. อบรมพัฒนาศักยภาพของเจ้าหน้าที่ ให้มีความรู้ความเข้าใจในการบันทึกข้อมูลให้ถูกต้อง ครบถ้วน สมบูรณ์ ป้องกัน ปกปิดความลับของผู้มารับบริการ	ปีละ1ครั้ง		↔				↔					↔			5,000 บาท	ระดับความเสี่ยงลดลง จาก 15 (สูง) เหลือ 10 (ปานกลาง)
	2. ปรับปรุงพัฒนาระบ HIS ให้เป็นปัจจุบันและสามารถนำข้อมูลไปใช้งานได้อย่างถูกต้อง มีการตรวจสอบข้อมูลอยู่สม่ำเสมอเพื่อป้องกันความผิดพลาด	ทุกเดือน	↔	↔	↔	↔	↔	↔	↔	↔	↔	↔	↔	↔		

ประเภทความเสี่ยง/กิจกรรม	แผนปฏิบัติ	ระยะเวลา	ปีงบ 2567				ปีงบ 2568				ปีงบ 2569				งบประมาณ	ผลลัพธ์ความก้าวหน้า
			ไตรมาส				ไตรมาส				ไตรมาส					
			1	2	3	4	1	2	3	4	1	2	3	4		
6. Utilities – Electricity	1. จัดทำนโยบาย ระเบียบและแนวปฏิบัติ ในการจัดการการป้องกันความเสี่ยงเสียหายจากไฟฟ้าตกหรือกระชาก รวมถึงทบทวนมาตรการ และแนวปฏิบัติ	ปีละ1 ครั้ง	↔				↔				↔					ระดับความเสี่ยงลดลง จาก 15 (สูง) เหลือ 10(ปานกลาง)
	2.ปรับปรุงระบบไฟฟ้าเป็น 3 เฟส และแยกระบบไฟฟ้าออกจากระบบภายในโรงพยาบาล			↔												
	3.จัดทำโครงการจัดซื้อเครื่องสำรองไฟให้กับจุดบริการให้ครอบคลุมการใช้งาน ที่จำเป็น และเหมาะสม	ปีละ1 ครั้ง	↔				↔				↔					

บทที่ 4 สรุปและข้อเสนอแนะ

การจัดการความเสี่ยง (Risk Management) คือ กระบวนการในการระบุ วิเคราะห์ ประเมิน ดูแล ตรวจสอบ และควบคุมความเสี่ยงที่สัมพันธ์กับกิจกรรม หน้าที่ และกระบวนการทำงานเพื่อให้องค์กร ลดความเสียหายจากความเสี่ยงมากที่สุด อันเนื่องมาจากภัยที่องค์กรต้องเผชิญในช่วงเวลาใดเวลาหนึ่ง เมื่อเทคโนโลยีสารสนเทศก้าวเข้ามามีบทบาทสำคัญในฐานะกลไกอันทรงพลังในการขับเคลื่อนการดำเนินงานขององค์กร ทุกกิจกรรมที่เกิดขึ้นภายในองค์กรจึงล้วนมีความเกี่ยวข้องกับเทคโนโลยีสารสนเทศแทบทั้งสิ้น ในแต่ละวันข้อมูลมหาศาลถูกส่งผ่านเครือข่ายเทคโนโลยีสารสนเทศเพื่ออำนวยความสะดวกให้แก่ผู้ปฏิบัติงานของทุกหน่วยงานภายในโรงพยาบาลบ่อพลอย ในปัจจุบัน “ข้อมูล” ถือว่าเป็นทรัพย์สินอันทรงคุณค่ามหาศาลต่างตกอยู่ในสภาวะ เสี่ยงต่อการถูกล่วงละเมิด ถูกทำให้เสียหายหรือสูญหาย และถูกนำไปใช้ในทางที่ผิด ทั้งจากบุคคลภายในและ ภายนอกองค์กรโดยเจตนาหรือไม่เจตนาก็ตาม ดังนั้น หนทางที่ดีที่สุดในการแก้ปัญหานี้จึงควรเริ่มตั้งแต่การ บริหารจัดการองค์กรให้ได้มาตรฐานด้านความปลอดภัย ซึ่งก็คือ การจัดการความเสี่ยงในองค์กรนั่นเอง

1. การวิเคราะห์ปัจจัยเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ

การระบุความเสี่ยง (Risk identification) เป็นการชี้ให้เห็นถึงความเสี่ยงด้านต่างๆ ที่องค์กรเผชิญอยู่จากการกำหนดแนวทางปฏิบัติเพื่อควบคุมความเสี่ยงในระดับสูงและปานกลาง ดังต่อไปนี้

ความเสี่ยง	แนวทางปฏิบัติ
1. Fire – External	1. อบรมให้ความรู้และทักษะที่จำเป็น ให้ความรู้เกี่ยวกับอัคคีภัยใน รพ.
	2. จัดทำนโยบาย ระเบียบปฏิบัติเพื่อรักษาความมั่นคงปลอดภัย ระบบอัคคีภัย เผยแพร่ พร้อมประเมินการรับรู้ความเข้าใจของบุคคลกร รพ.
	3. ซ้อมแผนอัคคีภัยในทุกๆปี เตรียมความพร้อมอุปกรณ์ดับเพลิงครอบคลุมทุกจุด
	4. ใช้ 5 ส และ Lean มาดำเนินการ ให้ความรู้ความเข้าใจ และตระหนักถึงความสำคัญ
	5. ปรับปรุงพัฒนาระบบอัคคีภัยแบบอัตโนมัติให้ครอบคลุมทุกจุด
	6. จัดทำแผนรับสถานการณ์เพื่อให้สามารถดำเนินการได้อย่างต่อเนื่อง (Business Continuity Plan : BCP)
2. Criminal – Theft	1. จัดทำแบบการประเมินความเสี่ยงทุกจุดในโรงพยาบาลบ่อพลอย พร้อมวิเคราะห์ เพื่อหาความเสี่ยง
	2. จัดทำนโยบาย ระเบียบปฏิบัติเพื่อรักษาความมั่นคงปลอดภัย ความเสียหายอันเกิดจากการโจรกรรม พร้อมประเมินความพร้อมของบุคคลกรโรงพยาบาลบ่อพลอย
	3. ติดตั้งระบบกล้องวงจรปิดเพิ่มเติม พร้อมตรวจสอบการทำงานในทุกๆวันให้สามารถตอบสนองได้ทันที เมื่อเกิดอุบัติการณ์

ความเสี่ยง	แนวทางปฏิบัติ
	4. จัดทำแผนรับสถานการณ์เพื่อให้สามารถดำเนินการได้อย่างต่อเนื่อง (Business Continuity Plan : BCP)
3. IT Hacking Unauthorized Intrusions	1. อบรมให้ความรู้และทักษะที่จำเป็น ให้ความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์
	2. จัดทำนโยบาย ระเบียบปฏิบัติเพื่อรักษาความมั่นคงปลอดภัย ในระบบเทคโนโลยี
	3. จัดทำระบบ Domain Controller เพื่อนำมาบริหาร จัดการในระบบเครือข่าย
	4. จัดหา ติดตั้งโปรแกรม ชุดโปรแกรมป้องกันไวรัส และปรับปรุงโปรแกรมให้ทันสมัย
	5. จัดหาซอฟแวร์ลิขสิทธิ์
	6. ตรวจสอบการทำงานของ Firewall ที่ระบบคอมพิวเตอร์ส่วนกลางที่เป็นทางผ่านเข้าออกไปยังระบบเครือข่ายภายนอก (Internet) และ Update Patch
	7. ปรับปรุงพัฒนาระบบเครือข่าย ออกแบบระบบ VLAN และ IP Network ให้สอดรับกับความจำเป็นในการใช้งาน
	8. จัดทำแผนรับสถานการณ์เพื่อให้สามารถดำเนินการได้อย่างต่อเนื่อง (Business Continuity Plan : BCP)
4. IT- .Server and Main Switches Crash or Failure	1.ทำแบบประเมินการทำงานของอุปกรณ์ Computer Server ,UPS, Main Switches
	2. ปรับปรุงพัฒนาระบบเครือข่าย ให้ทันสมัยพร้อมรองรับ การพัฒนาในอนาคต
	3. จัดหาอุปกรณ์วัดอุณหภูมิและความชื้น พร้อม บันทึกผล
	4. ติดตั้งระบบเครือข่ายสำรองที่ สามารถใช้งานจริงได้ในทันทีเมื่อเครือข่ายหยุดทำงาน โดยติดตั้งไว้อิสระจากระบบจริง
	5. จัดทำแผนรับสถานการณ์เพื่อให้สามารถดำเนินการได้อย่างต่อเนื่อง (Business Continuity Plan : BCP)
5.Data Protection Policy and Regulations การป้องกันความลับและความเป็นส่วนตัวของข้อมูล	1. จัดทำแนวปฏิบัติ ในการจัดการการป้องกันความลับและความเป็นส่วนตัวของข้อมูล

ความเสี่ยง	แนวทางปฏิบัติ
6. Utilities – Electricity	1. ป้องกันความเสี่ยงเสียหายจากไฟฟ้าตกหรือกระชาก รวมถึงทบทวนมาตรการ และแนวปฏิบัติ
	2. ปรับปรุงระบบไฟฟ้าเป็น 3 เฟส และแยกระบบไฟฟ้าออกจากระบบภายในโรงพยาบาล
	3.จัดทำโครงการจัดซื้อเครื่องสำรองไฟให้กับจุดบริการให้ครอบคลุมการใช้งาน ที่จำเป็น และเหมาะสม

2. สรุปแผนการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ ได้ดำเนินการจัดทำเพื่อ

- เตรียมความพร้อมและรองรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบฐานข้อมูลสารสนเทศ
- เป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศ ให้มีเสถียรภาพ และมีความพร้อมสำหรับการใช้งาน
- ให้การปฏิบัติงานเป็นไปอย่างมีระบบและต่อเนื่อง และสามารถแก้ไขสถานการณ์ได้อย่าง ทันท่วงที กรณีเกิดสถานการณ์ความไม่แน่นอนและภัยพิบัติ

3. ข้อเสนอแนะ

- การควบคุมนโยบายและกระบวนการปฏิบัติงานถือเป็นสำคัญ เพื่อให้มั่นใจว่าได้มีการจัดการความเสี่ยง ดังนั้น ควรมีการกำหนดบุคลากรภายในหน่วยงานเพื่อรับผิดชอบการควบคุม โดยบุคลากรแต่ละคนที่ได้รับมอบหมายในการควบคุมควรมีความรับผิดชอบ ดังนี้
  1) พิจารณาประสิทธิผลของการจัดการความเสี่ยงที่ได้ดำเนินการอยู่ในปัจจุบัน
  2) พิจารณาการปฏิบัติเพิ่มเติมที่จำเป็น เพื่อเพิ่มประสิทธิผลของการจัดการความเสี่ยงนั้น
  3) กำกับกิจกรรมลดความเสี่ยงให้แล้วเสร็จตามกำหนดวันตามแผนที่วางไว้
- การติดตามการบริหารความเสี่ยงเพื่อให้มั่นใจว่าการจัดการความเสี่ยงมีคุณภาพเหมาะสม ดังนั้น จึงควรมีการติดตามการบริหารความเสี่ยงอย่างต่อเนื่องและดำเนินการอย่างสม่ำเสมอ เพื่อตอบสนองต่อการเปลี่ยนแปลงอย่างทันท่วงที และถือเป็นส่วนหนึ่งของการปฏิบัติงาน รวมถึงการติดตามการดำเนินการภายหลังจากเกิดเหตุการณ์ขึ้น