คำนำ

แผนบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศของโรงพยาบาลปาย ประจำปี 2566-2570 จัดทำขึ้นเพื่อเป็นกรอบแนวทางในการ ดำาเนินงานบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ ในการระบุความเสี่ยง วิเคราะห์ ความเสี่ยง และการกำหนดแนวทางหรือมาตรการควบคุมเพื่อป้องกันหรือลดความเสี่ยง โดยมุ่งหวังให้โรงพยาบาลบรรลุผลตามเป้าประสงค์ขององค์กร เนื่องจากความเสี่ยงอาจนำาไปสู่ผลเสียหรือความสูญเสียทั้ง ทางตรงและทางอ้อม โรงพยาบาลจึงต้องเข้าใจประเภทของความเสี่ยงที่เผชิญอยู่เพื่อที่จะได้เลือกวิธีการที่เหมาะสม ในการบริหารความเสี่ยงเหล่านั้นได้อยู่ระดับที่โรงพยาบาลสามารถรองรับได้ และทำให้โรงพยาบาลบรรลุวัตถุประสงค์ได้ อย่างมีประสิทธิภาพมากขึ้น ศูนย์คอมพิวเตอร์โรงพยาบาลปาย หวังเป็นอย่างยิ่งว่าแผนบริหารความ เสี่ยงด้านระบบเทคโนโลยีสารสนเทศของโรงพยาบาลปาย ฉบับนี้ จะช่วยให้ผู้รับผิดชอบใช้เป็นแนวทางในการลดความ เสียหายต่างๆ ที่อาจเกิดขึ้นและส่งผลต่อกระบวนการบริหารงานด้านเทคโนโลยีสารสนเทศของโรงพยาบาลปายต่อไป

ศูนย์คอมพิวเตอร์โรงพยาบาลปาย

ตุลาคม 2565

สารบัญ

บทที่ 3

สรุปและข้อเสนอแนะ

1. การวิเคราะห์ปัจจัยเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ

2.สรุป

3.ข้อเสนอแนะ

บทที่ 1

1. หลักการและเหตุผล

การบริหารความเสี่ยงเป็นเครื่องมือทางกลยุทธ์ที่สำคัญตามหลักการกำกับดูแลกิจการที่ดี โดยจะ ช่วยให้การบริหารงานและการตัดสินใจด้านต่างๆ เช่น การวางแผน การกำหนดกลยุทธ์ การติดตามควบคุม และวัดผลการปฏิบัติงาน ตลอดจนการใช้ทรัพยากรต่างๆ อย่างเหมาะสมและมีประสิทธิภาพมากขึ้น ลดการสูญเสียและโอกาสที่ทำให้เกิดความเสียหายแก่องค์กร โดยเฉพาะอย่างยิ่งในด้านเทคโนโลยีสารสนเทศที่เข้ามามีบทบาทสำคัญในการดำเนินงานของหน่วยงานภายในองค์กร ทั้งการจัดเก็บข้อมูล การใช้งานอุปกรณ์คอมพิวเตอร์ การติดต่อสื่อสารผ่านระบบเครือข่าย และวิธีการปฏิบัติงานระบบเทคโนโลยีสารสนเทศต่างๆ ภายใต้สภาวะการดำเนินงานของทุกๆ องค์กรล้วนแต่มีความเสี่ยง ซึ่งก็คือความไม่แน่นอนที่จะส่งผลกระทบต่อการดำเนินงานหรือเป้าหมายขององค์กร จึงจำเป็นต้องมีการจัดการความเสี่ยงเหล่านั้นอย่างเป็นระบบ โดยการระบุความเสี่ยงว่ามีปัจจัยเสี่ยงใดบ้างที่กระทบต่อการดำเนินงานหรือเป้าหมายขององค์กรวิเคราะห์ความเสี่ยงจากโอกาสและผลกระทบที่เกิดขึ้น จัดลำดับความสำคัญของปัจจัยเสี่ยง แล้วกำหนดแนวทางในการจัดการความเสี่ยง โดยต้องคำนึงถึงความคุ้มค่าในการจัดการความเสี่ยงอย่างเหมาะสม

2. วัตถุประสงค์ของการจัดทำแผนบริหารความเสี่ยง

1. เพื่อเตรียมความพร้อมรองรับสถานการณ์ฉุกเฉิน ที่อาจจะเกิดขึ้นกับระบบฐานข้อมูลและ ระบบเทคโนโลยีสารสนเทศของโรงพยาบาลปาย

2. เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของระบบฐานข้อมูลและระบบเทคโนโลยีสารสนเทศให้มีเสถียรภาพ และมีความพร้อมสำหรับการใช้งาน

3. เพื่อให้การปฏิบัติงานเป็นไปอย่างมีระบบและต่อเนื่อง และสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที กรณีเกิดสถานการณ์ความไม่แน่นอนและภัยพิบัติ

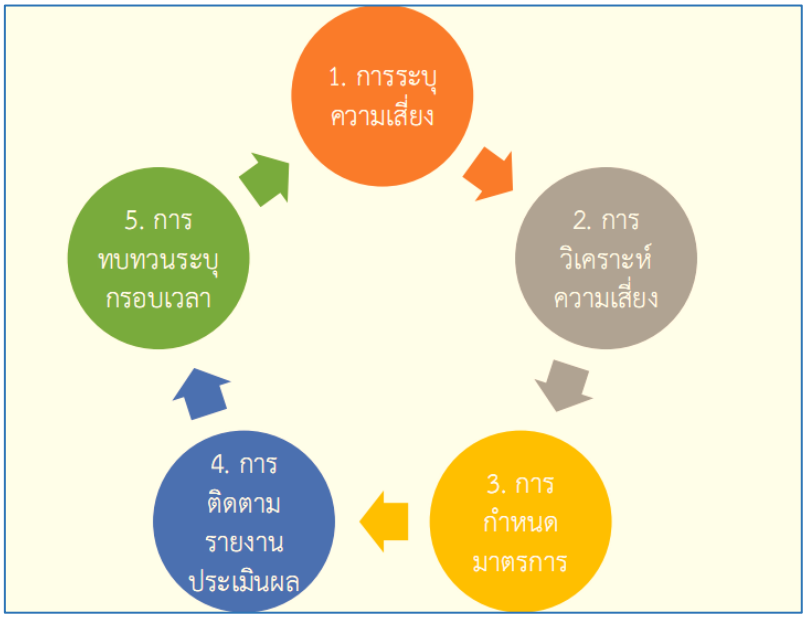
3. สภาพแวดล้อมด้านเทคโนโลยีสารสนเทศ

ระบบฐานข้อมูลสารสนเทศและโปรแกรมปฏิบัติการ (Database & Software) เช่น เว็บไซต์โรงพยาบาลปาย ฐานข้อมูลเว็บไซต์โรงพยาบาลปาย ฐานข้อมูลโปรแกรม HOSXP XE เป็นต้น ระบบฐานข้อมูลบริหารงานภายใน (Back Office) ได้แก่ โปรแกรม Smart OFFICE ระบบให้บริการเครือข่าย ได้แก่ โปรแกรมป้องกันไวรัสและการถูกโจมตีจากบุคคลภายนอก (Antivirus) โปรแกรมระบบปฏิบัติการจัดการเครือข่าย (Network Software) และโปรแกรมปฏิบัติการบน หน้าจอเว็บไซต์โรงพยาบาลปาย เป็นต้น อุปกรณ์คอมพิวเตอร์ (Hardware) เช่น เครื่องคอมพิวเตอร์แม่ข่ายระบบเน็ตเวิร์ค (Network Server) เครื่องคอมพิวเตอร์แม่ข่ายระบบฐานข้อมูล (Database Server) เครื่องคอมพิวเตอร์แม่ข่ายที่ใช้ จัดเก็บและสำรอง

ข้อมูล (Storage Server) เครื่องแม่ข่ายสำหรับให้บริการเว็บไซต์(Web Server) เครื่องคอมพิวเตอร์ป้องกันการจู่โจมข้อมูลจากบุคคลภายนอก (Firewall) เครื่องคอมพิวเตอร์ชนิดพกพา (Note Book) เครื่องสแกนเนอร์ (Scanner) เครื่องพิมพ์เลเซอร์ (Laser Printer)เครื่องพิมพ์แบบพ่นหมึก (Ink-Jet Printer) อุปกรณ์สำรองไฟฟ้าสำหรับ คอมพิวเตอร์ (UPS) อุปกรณ์กระจายสัญญาณเครือข่าย (Switching HUB) อุปกรณ์กระจายสัญญาณเครือข่าย ชนิดไร้สาย (Wireless Access point) เป็นต้น

4. กระบวนการบริหารความเสี่ยง

เป็นกระบวนการที่ใช้ในการระบุ วิเคราะห์ ประเมิน จัดระดับความเสี่ยง ที่มีผลกระทบต่อการ บรรลุวัตถุประสงค์ของกระบวนการทำงานของหน่วยงานหรือขององค์กร รวมทั้งการบริหาร/จัดการความเสี่ยง รวมทั้งการกำหนดแนวทางการดำเนินงานหรือมาตรการควบคุมหรือป้องกันหรือลดความเสี่ยง ซึ่งมีขั้นตอนการดำเนินการ หลักเกณฑ์ในการวิเคราะห์อย่างเหมาะสม โดยครอบคลุม 5 ขั้นตอน ดังนี้



รูปภาพกระบวนการบริหารความเสี่ยง

1. การระบุความเสี่ยงหรือปัจจัยเสี่ยง

เป็นกระบวนการที่ผู้บริหารและผู้ปฏิบัติงานร่วมกันระบุความเสี่ยงและปัจจัยเสี่ยงที่เกี่ยวข้องโครงการ/กิจกรรม เพื่อให้ทราบถึงเหตุการณ์ที่เป็นความเสี่ยง ที่อาจมีผลกระทบต่อการบรรลุผลสำเร็จตามวัตถุประสงค์ ซึ่งต้องคำนึงถึงสภาพแวดล้อมทั้งภายนอกและภายในองค์กร วิธีการในการระบุความเสี่ยงมีหลายวิธี เช่น

1. การระดมสมองเพื่อให้ได้ความเสี่ยงที่หลากหลาย

2. การใช้Checklist

3. การวิเคราะห์สถานการณ์จากการตั้งคำถาม “What-if”

4. การวิเคราะห์ขั้นตอนการปฏิบัติงานในแต่ละขั้นตอน

5. การรวบรวมปัญหาที่เกิดขึ้นมาแล้ว

ในขั้นตอนนี้ ควรมีการเก็บข้อมูลความสูญเสียที่เกิดขึ้นในรูปของความถี่ของการเกิดความสูญเสียและความ รุนแรงของความสูญเสีย รวมทั้งข้อมูลการดำเนินการใด ๆ เพื่อลดความสูญเสียที่เกิดขึ้นในอดีตทั้งที่ประสบผลสำเร็จ และปัญหาอุปสรรคซึ่งจะเป็นประโยชน์ในการดำเนินการต่อไป

2. การวิเคราะห์และประเมินความเสี่ยง

การประเมินความเสี่ยงเป็นกระบวนการที่ประกอบด้วยการวิเคราะห์ การประเมิน และ การจัดระดับความเสี่ยง ประกอบด้วย 4 ขั้นตอน คือ

2.1 การกำหนดเกณฑ์การประเมินมาตรฐาน เป็นเกณฑ์ที่จะใช้ประเมินความเสี่ยง ได้แก่ โอกาสที่จะเกิดความเสี่ยง (Likelihood) ระดับความรุนแรงของผลกระทบ (Impact) และระดับของความเสี่ยง (Degree of Risk) คณะกรรมการบริหารความเสี่ยงต้องกำหนดเกณฑ์ของหน่วยงานขึ้น ซึ่งอาจกำหนดได้ทั้ง เกณฑ์เชิงปริมาณและเชิงคุณภาพ การกำหนดเกณฑ์ของโอกาสที่เกิดความเสี่ยงอาจกำหนดเป็นเกณฑ์ 5 ระดับ (สูงมาก/รุนแรงมากที่สุด สูง/ค่อนข้างรุนแรง ปานกลาง น้อย และ น้อยมาก) ส่วนระดับของความ เสี่ยงอาจกำหนดเป็นเกณฑ์4 ระดับ (สูงมาก สูง ปานกลาง และ น้อย)

2.2 กำรประเมินโอกาสและผลกระทบของความเสี่ยง เป็นการนำความเสี่ยงและปัจจัย เสี่ยงแต่ละปัจจัยที่ระบุไว้มาประเมินโอกาสที่จะเกิดเหตุการณ์ความเสี่ยงเหล่านั้นและประเมินระดับความ รุนแรงหรือมูลค่าความเสียหายจากความเสี่ยงตามเกณฑ์มาตรฐานที่กำหนดเพื่อให้เห็นระดับความเสี่ยง ซึ่งแต่ ละความเสี่ยงก็จะมีความรุนแรงแตกต่างกัน ทั้งนี้การควบคุมความเสี่ยงหรือหลีกเลี่ยงความเสี่ยงนั้น ก็จะขึ้นอยู่ กับมาตรการควบคุมความเสี่ยงของแต่ละหน่วยงาน โดยมีการประเมินใน 2 มิติ ได้แก่ มิติผลกระทบ และมิติโอกาสของความเสี่ยงที่จะเกิดขึ้น

เกณฑ์การประเมินผลกระทบ เป็นดังนี้

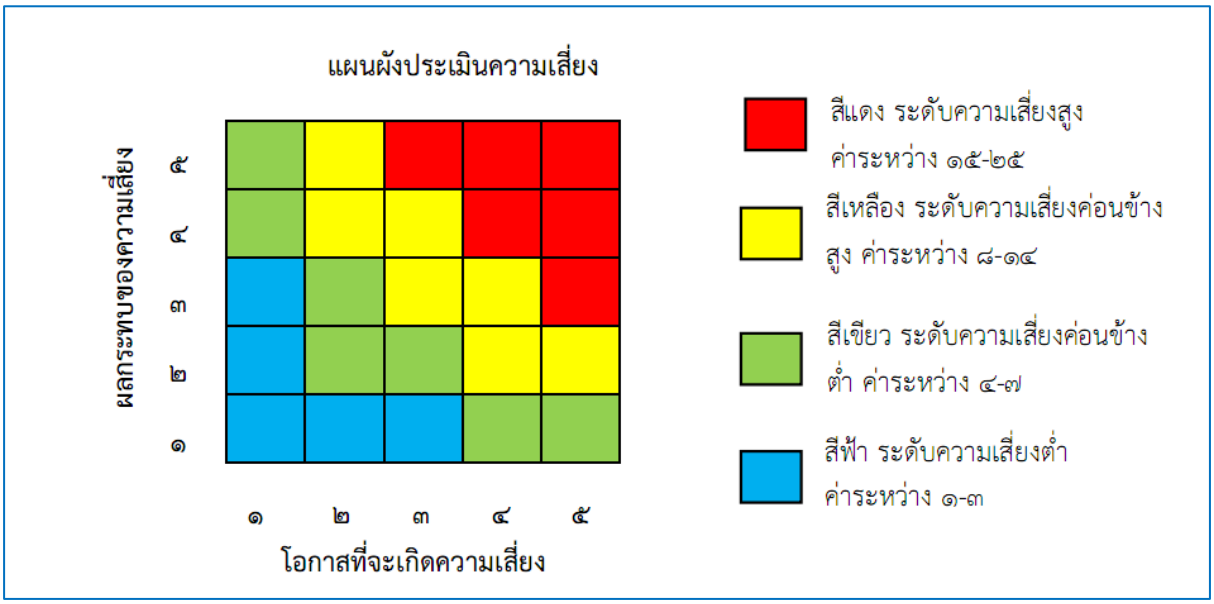
ระดับ	การประเมิน
1	น้อยมาก
2	น้อย

3	ปานกลาง
4	สูง
5	สูงมาก

เกณฑ์การประเมินโอกาสของการเกิดความเสี่ยงเป็นดังนี้

ระดับ	การประเมิน
1	เกิดขึ้นน้อยมาก
2	เกิดขึ้นน้อย
3	เกิดขึ้นปานกลาง
4	เกิดขึ้นสูง
5	เกิดขึ้นสูงมาก

2.3 การวิเคราะห์ความเสี่ยง เป็นการดูความสัมพันธ์ระหว่างโอกาสที่จะเกิดความเสี่ยงและผลกระทบของความเสี่ยงต่อองค์กร ว่าจะก่อให้เกิดระดับความเสี่ยงในระดับใด โดยใช้ตารางระดับความเสี่ยง สูงสุดที่จะต้องบริหารจัดการก่อน ดังภาพประกอบ



รูปภาพแผนผังประเมินความเสี่ยง

2.4 การจัดลำดับความเสี่ยง เป็นการจัดลำดับความรุนแรงของความเสี่ยงที่มีผลต่อองค์กร เพื่อพิจารณากำหนดกิจกรรมการควบคุมในแต่ละสาเหตุของความเสี่ยงที่สำคัญให้เหมาะสมโดยพิจารณาจาก ระดับความเสี่ยงที่ประเมินได้ เลือกความเสี่ยงที่มีระดับสูงมาก หรือสูงมาจัดทำแผนการบริหารความเสี่ยงเป็น ลำดับแรก

3. การกำหนดมาตรการจัดการความเสี่ยงอย่างรัดกุม

มีการวางแผนโดยกำหนดมาตรการเพื่อควบคุมผลกระทบของความเสี่ยงเพื่อให้สามารถบรรลุเป้าหมาย หรือใกล้เคียงกับเป้าหมายที่กำหนดไว้ในการวางแผน จะต้องมีการกำหนดกลยุทธ์ในการควบคุมผลกระทบของความเสี่ยงที่อาจเกิดขึ้น เพื่อที่จะลดและตรวจหาความเสี่ยงที่ได้ประเมินเอาไว้ โดยให้มีการแต่งตั้งเจ้าหน้าที่ผู้รับผิดชอบเป็นผู้ดูแลรักษาความมั่นคงปลอดภัยของระบบ และป้องกัน/แก้ไข/ควบคุมความเสี่ยงไม่ให้มีผลกระทบต่อระบบที่วางไว้ โดยสามารถด าเนินการตามแผนได้ การควบคุมอาจแบ่งได้เป็น 4 ประเภท คือ

3.1 ควบคุมเพื่อกำรป้องกัน (Preventive Control) เป็นวิธีการควบคุมเพื่อป้องกันไม่ให้ เกิดความเสี่ยงและข้อผิดพลาดตั้งแต่แรก เช่น การอนุมัติ การจัดโครงสร้างองค์กร การควบคุม การเข้าถึง เอกสาร เป็นต้น

3.2 กำรควบคุมเพื่อให้ตรวจพบ (Detective Control) เป็นวิธีการควบคุมเพื่อค้น ข้อผิดพลาดที่เกิดขึ้นแล้ว เช่น การวิเคราะห์ การตรวจนับ การรายงานข้อบกพร่อง เป็นต้น

3.3 กำรควบคุมโดยกำรชี้แนะ (Direction Control) เป็นวิธีควบคุมที่ส่งเสริมหรือกระตุ้น ให้เกิดความส าเร็จตามวัตถุประสงค์

3.4 กำรควบคุมเพื่อการแก้ไข (Corrective Control) เป็นวิธีการควบคุมเพื่อแก้ไข ข้อผิดพลาดที่เกิดขึ้นให้ถูกต้อง หรือหาวิธีแก้ไขไม่ให้เกิดข้อผิดพลาดนั้นซ้ำอีกในอนาคตหลังจากประเมินความ เสี่ยงแล้ว จะต้องวิเคราะห์การควบคุมที่มีอยู่ว่าได้มีการจัดการควบคุมเพื่อลดความเสี่ยงดังกล่าวหรือไม่

โดยนำผลการจัดระดับความเสี่ยงในระดับสูงมากและสูง มาประเมินมาตรการควบคุมเป็นอันดับแรก อาจใช้ ขั้นตอนดังนี้

1) นำปัจจัยเสี่ยงที่อยู่ในระดับสูงมาก หรือสูงมากำหนดวิธีควบคุมที่ควรจะมี เพื่อป้องกัน ความเสี่ยงหรือปัจจัยเสี่ยงเหล่านั้น

2) พิจารณา หรือประเมินว่าในปัจจุบันความเสี่ยงหรือปัจจัยเสี่ยงนั้นมีการควบคุมอยู่แล้ว หรือไม่

3) ถ้ามีการควบคุมแล้ว ให้ประเมินต่อไปว่าการควบคุมนั้นได้ผลตามความต้องการหรือไม่

4. การติดตามรายงานและประเมินผลการดำเนินการตามมาตรฐานการจัดความเสี่ยงที่ได้กำหนดไว้

การติดตามผลการดำเนินงาน การนำกลยุทธ์ มาตรการ หรือแนวทางมาใช้ปฏิบัติ เพื่อลดโอกาส ที่เกิดความเสี่ยง หรือลดความเสียหายของผลที่อาจเกิดขึ้นจากความเสี่ยง ในโครงการ/กิจกรรม ที่ยังไม่มีกิจกรรมควบคุมความเสี่ยง หรือมีแต่ไม่เพียงพอ และนำมาวางแผนจัดการความเสี่ยง ทางเลือกในการ บริหารความเสี่ยงมีหลายวิธีซึ่งสามารถปรับเปลี่ยนหรือนำมาผสมผสานให้เหมาะสมกับสถานการณ์ อาจเป็น การยอมรับความเสี่ยง การลด/การควบคุมความเสี่ยง การกระจายความเสี่ยง หรือการหลีกเลี่ยงความเสี่ยง เมื่อองค์กรทราบความเสี่ยงที่ยังเหลืออยู่จากการประเมินความเสี่ยง และการประเมินการควบคุมแล้วให้ พิจารณาความเป็นไปได้และค่าใช้จ่ายแต่ละทางเลือก เพื่อตัดสินใจเลือกมาตรการลดความเสี่ยงที่เหมาะสมโดย พิจารณาจาก

4.1 พิจารณาว่ายอมรับความเสี่ยง หรือจะกำหนดกิจกรรมควบคุมเพื่อลดความเสี่ยงให้อยู่ใน ระดับที่ยอมรับได้

4.2 เปรียบเทียบค่าใช้จ่ายหรือต้นทุนในการจัดการให้มีมาตรการควบคุมกับผลประโยชน์ที่ จะได้รับจากมาตรการดังกล่าวว่าคุ้มค่าหรือไม่

4.3 กรณีเลือกกำหนดกิจกรรมควบคุมเพื่อลดความเสี่ยงให้กำหนดวิธีควบคุมในแผนบริหาร ความเสี่ยง

4.4 ในรอบปีต่อไป ให้พิจารณาผลการติดต่อการบริหารความเสี่ยงในงวดก่อนที่ดำเนินการ มาบริหารความเสี่ยงตามกระบวนการเหล่านั้น หากพบว่ายังมีความเสี่ยงที่มีนัยสำคัญซึ่งอาจมีผลต่อการบรรลุวัตถุประสงค์และเป้าหมายตามแผนปฏิบัติงานขององค์กร ให้นำมาระบุการควบคุมในแผนบริหารความเสี่ยงด้วยการรายงานผลการวิเคราะห์ประเมินและบริหารจัดการความเสี่ยง ว่ามีความเสี่ยงที่ยังเหลืออยู่หรือไม่ถ้าไม่มีเหลืออยู่ มีอยู่ในระดับความเสี่ยงสูงมากเพียงใด และมีวิธีการจัดการความเสี่ยงนั้นอย่างไรเสนอต่อผู้บริหารเพื่อทราบและสั่งการ

5. การทบทวนการบริหารความเสี่ยงโดยระบุกรอบเวลาในการทบทวนอย่างชัดเจน

เป็นการติดตามภายหลังจากได้ดำเนินการตามแผนการบริหารความเสี่ยง ว่ามีความเสี่ยงแล้ว เพื่อให้มั่นใจว่าแผนการบริหารความเสี่ยงนั้นมีประสิทธิภาพ ทั้งนี้ เพื่อประเมินคุณภาพและความเหมาะสมของวิธีการจัดการความเสี่ยงที่ใช้ และเป็นการตรวจสอบความคืบหน้าของมาตรการควบคุม โดยอาจติดตามผลเป็นรายครั้งตามรอบระยะเวลา หรือการติดตามผลในระหว่างการปฏิบัติงาน

6. ความเสี่ยงด้านเทคโนโลยีสารสนเทศ

โรงพยาบาลปายได้กำหนดประเภทความเสี่ยงด้านเทคโนโลยีสารสนเทศ ตามแนวทางของ COSO (Committee of Sponsoring Organization) ออกได้ เป็น 8 ประเภท ดังนี้

- ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk) หมายถึง ความเสี่ยงที่เกิดจากภัยคุกคามทั้งภัยจากธรรมชาติ และภัยที่มนุษย์ทำขึ้น เช่น วาตภัย อุทกภัย อัคคีภัย ฟ้าผ่า กระแสไฟฟ้าขัดข้อง การชุมนุมประท้วง การก่อการร้าย รวมถึงการไม่มีระบบรักษา ความปลอดภัยห้องปฏิบัติการระบบเครือข่ายและคอมพิวเตอร์ เครื่องคอมพิวเตอร์แม่ข่าย และระบบสื่อสารที่ มีประสิทธิภาพเพียงพอ

- ความเสี่ยงด้านบุคลากร (Human Risk) หมายถึง ความเสี่ยงที่เกิดจากบุคลากรที่เกี่ยวข้องกับการดำเนินงานด้านเทคโนโลยีสารสนเทศ และการสื่อสาร ทั้งในด้านการวางแผน การตรวจสอบการท างาน การมอบหมายหน้าที่และสิทธิ์ของบุคลากร และคณะทำงานที่มีส่วนเกี่ยวข้องกับการดำเนินการทุกฝ่ายอย่างละเอียด เพื่อให้บุคลากรมีความรู้ ความเข้าใจ ในการใช้งาน การดูแลรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งบุคลากร ภายนอกที่เกี่ยวข้องทั้งทางตรงและทางอ้อม ซึ่งล้วนแต่เป็นความเสี่ยงทั้งสิ้น

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

- ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk) หมายถึง ความเสี่ยงที่เกิดจากระบบการทำงานของโปรแกรมต่างๆ เช่น การใช้โปรแกรมที่ไม่มี การอัพเดทให้ทันสมัย เพื่อลดช่องโหว่ที่อาจเกิดจาก Bug ของซอฟต์แวร์นั้นๆ หรือการถูกผู้ไม่หวังดี (Hacker) เข้ามาทำลายระบบ หรือการใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ซึ่งโรงพยาบาล อาจถูกฟ้องร้องให้ต้องชำระค่าละเมิด ลิขสิทธิ์ เป็นต้น

- ความเสี่ยงด้านระบบข้อมูล (Database Risk) หมายถึง ความเสี่ยงที่เกิดจากฐานข้อมูลต่างๆ ในระบบสารสนเทศและการสื่อสารอันอาจจะ ก่อให้เกิดความเสียหาย เนื่องจากข้อมูลถูกทำลาย ความเสี่ยงจากผู้บุกรุกข้อมูล เพื่อการโจรกรรมข้อมูลที่สำคัญการลักลอบเข้ามาแก้ไขเปลี่ยนแปลงข้อมูล ทำให้เกิดความเสียหาย ขาดความน่าเชื่อถือและสร้างความ เสื่อมเสียแก่องค์กร ความเสี่ยงเหล่านี้ทำให้มีความจำเป็นที่จะต้องมีการบริหารจัดการความเสี่ยงด้านข้อมูล ดังนั้น การรักษาความปลอดภัยของข้อมูลจึงเป็นเรื่องสำคัญ

เนื่องจากข้อมูลสารสนเทศและการสื่อสารเป็น ปัจจัยสำคัญสำหรับผู้บริหาร ผู้มีส่วนได้ส่วนเสียโดยตรง รวมถึงประชาชนทั่วไป ดังนั้น การรักษาความ ปลอดภัยของระบบข้อมูลและคอมพิวเตอร์จากภัยต่างๆ ทั้งภัยจากคน ภัยจากธรรมชาติ หรือเหตุการณ์ใดๆ จึงมีความสำคัญและจำเป็นที่จะต้องมีการป้องกัน เพื่อให้เกิดความมั่นคงต่อระบบข้อมูลสารสนเทศและเทคโนโลยี

- ความเสี่ยงด้านกลยุทธ์(Strategic Risk) หมายถึง ความเสี่ยงที่เกิดจากการเปลี่ยนแปลงของนโยบายรัฐบาล ผู้บริหารองค์กร เนื่องจาก การเปลี่ยนแปลงรัฐบาล และผู้บริหารองค์กรต่างๆ ในด้านเทคโนโลยีสารสนเทศและการสื่อสาร ทำให้การ กำหนดยุทธศาสตร์และกลยุทธ์เปลี่ยนแปลงไป

- ความเสี่ยงด้านการเงิน (Financial Risk) หมายถึง ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ และต่อการเบิกจ่าย งบประมาณไม่ทันตามกำหนดเวลา

- ความเสี่ยงในการด้านการบริหารจัดการ (Management Risk) หมายถึง ความเสี่ยง เนื่องมาจากการบริหารที่ไม่รัดกุม ไม่มีแผนงานในการดำเนินการที่ดี

7. การตอบสนองความเสี่ยง

เมื่อความเสี่ยงได้รับการบ่งชี้และประเมินความสำคัญแล้วผู้บริหารต้องประเมินวิธีการจัดการ ความเสี่ยงที่สามารถนำไปปฏิบัติได้และผลของการจัดการเหล่านั้น การพิจารณาทางเลือกในการดำเนินการ จะต้องคำนึงถึงความเสี่ยงที่ยอมรับได้ และต้นทุนที่เกิดขึ้นเปรียบเทียบกับผลประโยชน์ที่จะได้รับเพื่อให้การ บริหารความเสี่ยงมีประสิทธิผล ผู้บริหารอาจต้องเลือกวิธีการจัดการความเสี่ยงอย่างใดอย่างหนึ่ง หรือหลายวิธีรวมกัน เพื่อลดระดับโอกาสที่อาจเกิดขึ้นและผลกระทบของเหตุการณ์ให้อยู่ในช่วงที่องค์กรสามารถยอมรับได้ (Risk Tolerance) หลักการตอบสนองความเสี่ยงมี4 ประการ คือ

- การหลีกเลี่ยง (Terminate) เป็นวิธีการที่ง่ายที่สุดในการบริหารความเสี่ยง คือ การเลือกที่จะ ไม่รับความเสี่ยงไว้เลย อาจหยุดดำเนินการ หรือยกเลิกโครงการ/กิจกรรมที่ก่อให้เกิดความเสียหายได้ การหลีกเลี่ยงความเสี่ยงเมื่อพบว่าผลประโยชน์ที่จะได้รับนั้นไม่คุ้มกับสิ่งที่จะเกิดขึ้นจึงหลีกเลี่ยงที่จะเผชิญกับกิจกรรมความเสี่ยงนั้น หรือการหลีกเลี่ยงความเสี่ยงอาจเกิดขึ้นจากหน่วยงานเลือกที่จะหลีกเลี่ยงกิจกรรมความเสี่ยงนั้น โดยมิได้คิดทบทวนถึงผลที่จะได้รับ นำมาซึ่งการเสียโอกาสของหน่วยงานได้

- การยอมรับ (Take) เป็นการยอมรับความเสี่ยง หรือความเสียหายที่อาจจะเกิดขึ้นไว้เองโดยไม่ ทำอะไร และยอมรับในผลที่อาจตามมา เนื่องจากเห็นว่าโอกาสหรือความน่าจะเป็นที่จะเกิดความเสียหายอยู่ในวิสัยที่หน่วยงานยอมรับได้ หรือไม่คุ้มค่าส าหรับค่าใช้จ่ายในการสร้างระบบในการจัดการหรือป้องกันความเสี่ยง

- การควบคุม (Treat) เป็นการปรับปรุงระบบการทำงาน หรือออกแบบวิธีการทำงานใหม่ เพื่อหาทางป้องกันมิให้มีความเสียหายเกิดขึ้น เป็นการลดโอกาสหรือจำนวนครั้งของความเสียหายที่จะเกิด หากเราไม่สามารถป้องกันไม่ให้ความเสี่ยงเกิดขึ้นได้ ก็ควรขจัดให้หมดไปหรือลดความรุนแรงของความเสี่ยงลง โดยมีการจัดทำแผนหรือมาตรการควบคุมขึ้น อาจกำหนดเป็นแนวทางปฏิบัติไว้ล่วงหน้า ทั้งนี้วิธีควบคุมความสูญเสียมีสองวิธีหลัก คือ การป้องกันการเกิดความสูญเสีย และการควบคุมขนาดของความสูญเสียหลังเกิดความสูญเสียขึ้นการป้องกันการเกิดความสูญเสีย เป็นวิธีการที่พยายามจะลดความถี่ของการเกิดความสูญเสีย ก็คือการหามาตรการหรือวิธีการใด ๆ ในการป้องกันไม่ให้ความสูญเสียเกิดขึ้น

- การถ่ายโอน (Transfer) การโอนย้ายหรือแบ่งความเสี่ยงไปให้ผู้อื่นช่วยรับผิดชอบ เช่นอุปกรณ์เครือข่ายเมื่อซื้อมาแล้วมีระยะประกันภัยเพียงหนึ่งปี เพื่อเป็นการรับมือในกรณีที่อุปกรณ์เครือข่ายไม่ทำงาน องค์กรอาจเลือกซื้อประกัน หรือสัญญาการบำรุงรักษาหลังการขาย

8. ปัจจัยเสี่ยง

ปัจจัยที่จะเกิดความเสียหายกับระบบฐานข้อมูลสารสนเทศของโรงพยาบาลปายได้แก่

1. ปัจจัยภายนอก ได้แก่

1.1 ภัยธรรมชาติ และการเกิดสถานการณ์ความไม่สงบที่กระท าต่ออาคารสถานที่ตั้งของเครื่องประมวลผลหลัก หรือ เครื่องแม่ข่ายหลัก (Server) ของระบบฐานข้อมูล ได้แก่ ไฟไหม้ ภัยพิบัติ

1.2 การขโมยอุปกรณ์คอมพิวเตอร์แม่ข่ายที่เป็นส่วนของการจัดเก็บและรวบรวมข้อมูล

1.3 การชำรุดเสียหายของตัวเครื่องประมวลผลหลัก หรือแม่ข่ายหลัก (Server)

1.4 ระบบการสื่อสารของเครือข่ายคอมพิวเตอร์หลักเสียหายหรือขัดข้อง

1.5 ระบบกระแสไฟฟ้าขัดข้องหรือไฟฟ้าดับ

1.6 การถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูลจากบุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาต

2. ปัจจัยภายใน ได้แก่

2.1 ระบบฐานข้อมูลหลักเสียหาย หรือข้อมูลถูกทำลาย

2.2 การถูกไวรัส (Virus) ท าลายฐานข้อมูล และโปรแกรมปฏิบัติการต่างๆ จากผู้ใช้ ภายในองค์กร

2.3 เจ้าหน้าที่หรือบุคลการของหน่วยงานขาดความรู้ความเข้าใจในการใช้เครื่องมือ อุปกรณ์คอมพิวเตอร์ทั้งด้านฮาร์ดแวร์ และซอฟท์แวร์ อันอาจทำให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารเสียหาย ใช้งานไม่ได้ หรือหยุดการทำงาน

9. การประเมินความเสียหาย

1. ความเสียหายที่เกิดผลเสียหายร้ายแรงที่สุด ซึ่งจะทำให้ต้องหยุดระบบประมวลผลทั้งระบบลง ได้แก่ ภัยธรรมชาติ ตัวเครื่องประมวลผลหลักหรือแม่ข่ายเสียหาย (Server) และระบบฐานข้อมูลหลักถูกทำลายเสียหายจากไวรัส

2. ความเสียหายที่เกิดผลเสียหายและต้องหยุดระบบชั่วขณะ ได้แก่ การถูกเจาะเข้าระบบ ฐานข้อมูล ระบบสื่อสารของเครือข่ายคอมพิวเตอร์ขัดข้อง และกระแสไฟฟ้าขัดข้อง

10. การติดตามและรายงานผล

กำหนดให้เจ้าหน้าที่ผู้รับผิดชอบรายงานผลการดำเนินการหรือการตรวจสอบให้ผู้กำกับดูแล ทราบเป็นประจำทุกเดือน และให้รายงานการเกิดปัญหาและผลการแก้ไขให้ทราบในทันทีที่สามารถดำเนินการ ได้ในทุกกรณีตามที่ระบุ

11. ระบบรักษาความปลอดภัยบนเครือข่าย

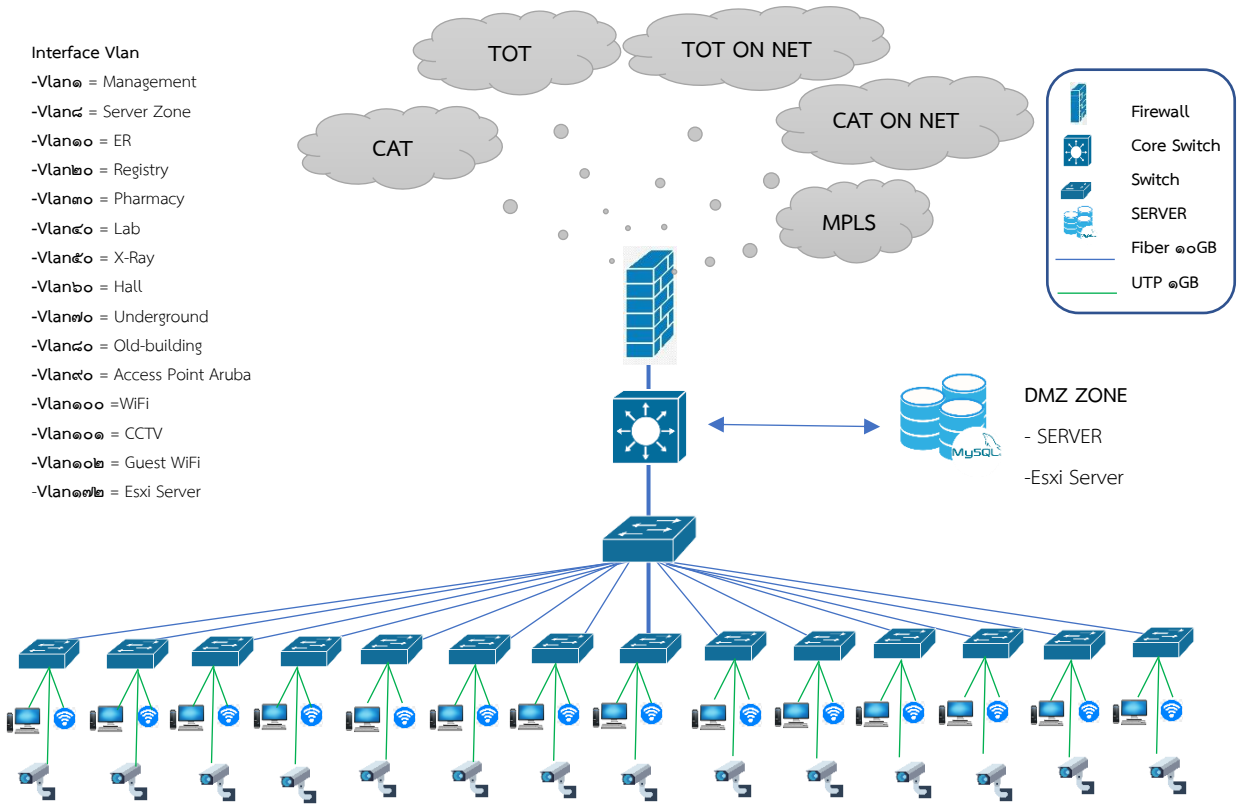
ระบบคอมพิวเตอร์และเครือข่ายของโรงพยาบาลปายได้พัฒนาอย่าง ต่อเนื่อง เพื่อให้การทำงานผ่านระบบคอมพิวเตอร์และเครือข่าย โรงพยาบาลปายเป็นไปอย่างรวดเร็วและมีประสิทธิภาพ ตั้งอยู่ที่อาคารผู้ป่วยนอกใหม่ ชั้นใต้ดิน โรงพยาบาลปาย ถนนชัยสงคราม ตำบลเวียงใต้ อำเภอปาย จังหวัดแม่ฮ่องสอน

ระบบคอมพิวเตอร์และเครือข่าย โรงพยาบาลปายมีการกำหนด นโยบายและมาตรการในการรักษาความปลอดภัยอย่างเข้มงวด โดยใช้ทั้งระบบฮาร์ดแวร์ และซอฟต์แวร์ ทำงานร่วมกันเพื่อป้องกันการโจมตีและบุกรุกเข้ามายังเครือข่าย โดยในส่วนของฮาร์ดแวร์มีการกำหนด มาตรการ (Policy) ผ่านอุปกรณ์ Firewall ของ FortiGate 100F ซึ่งใช้ในการกรอง (Filter Package) ที่ผ่านเข้ามาภายใน ระบบของโรงพยาบาลปายจากเครือข่ายภายนอก เช่น เครือข่ายอินเทอร์เน็ต นอกจากนั้นยังมีการกำหนดมาตรการ (Policy) ให้ทำหน้าที่ป้องกันการบุกรุกในส่วนของ DMZ ที่ดูแลเครื่อง แม่ข่ายทั้งหมดของโรงพยาบาลปายรวมถึงการใช้โปรแกรมป้องกันไวรัสแบบ Client-Server ในการตรวจสอบเครื่อง

คอมพิวเตอร์ทุกเครื่องที่อยู่ในระบบเครือข่ายของโรงพยาบาลปาย มี การกำหนดนโยบายและมาตรการในการรักษาความมั่นคงปลอดภัยอย่างเข้มงวด เพื่อให้มีความปลอดภัย และ ป้องกันความเสียหายที่

อาจเกิดขึ้นกับระบบเครือข่ายทั้งหมด ปัจจุบันเครือข่ายของโรงพยาบาลปาย มีการแบ่งโซนออกตามอาคารจุดต่างๆ เพื่อเพิ่ม ความปลอดภัยและสะดวกและรวดเร็วต่อการบริหารจัดการระบบ กรณีเกิดปัญหาการใช้งาน

ระบบเครือข่ายหลักของโรงพยาบาลปาย (Core Network) ตั้งอยู่ที่ ศูนย์คอมพิวเตอร์ เป็นศูนย์กลางการเชื่อมต่อทำหน้าที่เชื่อมโยงระบบเครือข่ายภายในโรงพยาบาลปาย ในความเร็วระดับ 10 GB และ 1,000 Mbps และระบบเครือข่ายภายนอก เช่น อินเทอร์เน็ต มี Core Switch ที่ออกแบบติดตั้งในลักษณะระบบเครือข่ายที่สามารถทดแทนกันได้ (Redundant Network) เพื่อแก้ปัญหาระบบเครือข่ายศูนย์กลางล่ม (Single Point of Failure) และแก้ปัญหา คอขวดในการเข้าถึงข้อมูล (Bottleneck)เพื่อรองรับภารกิจของโรงพยาบาลปายซึ่งลักษณะงานต้องใช้อุปกรณ์เครือข่ายคอมพิวเตอร์ที่มีประสิทธิภาพสูงสามารถรองรับการเชื่อมต่อกับระบบ เครือข่ายภายในและภายนอก เพื่อใช้ระบบงานฐานข้อมูลที่สำคัญของโรงพยาบาลปาย พร้อมทั้งเชื่อมโยงไปยังอุปกรณ์ Core Switch (L3) และ Access Switch(L2) ไปยังอาคารต่างๆ ซึ่งเป็นที่ตั้งของหน่วยงานในโรงพยาบาลปาย



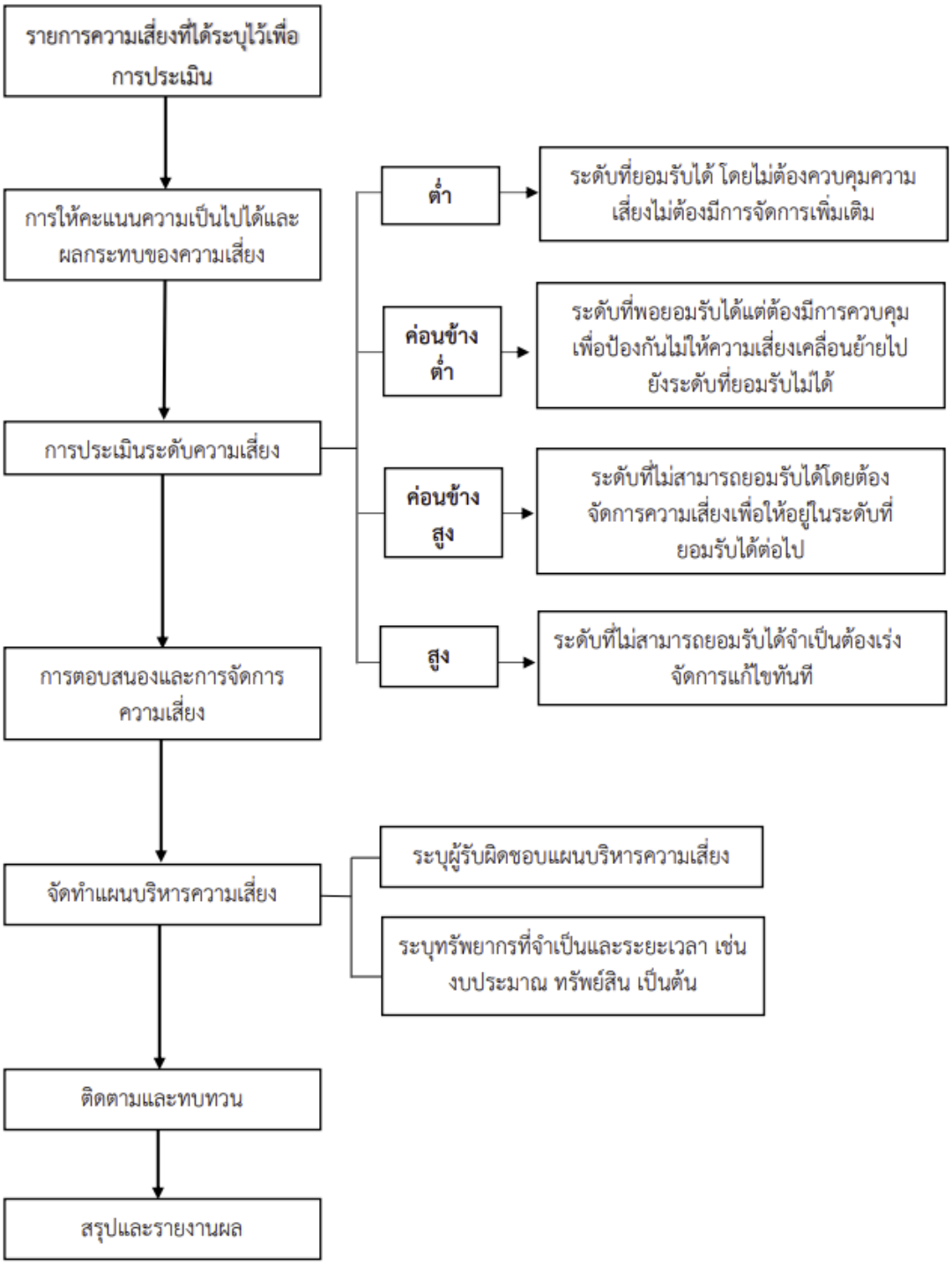
รูปภาพแสดงระบบโครงข่ายคอมพิวเตอร์สารสนเทศของโรงพยาบาลปาย

บทที่ 2

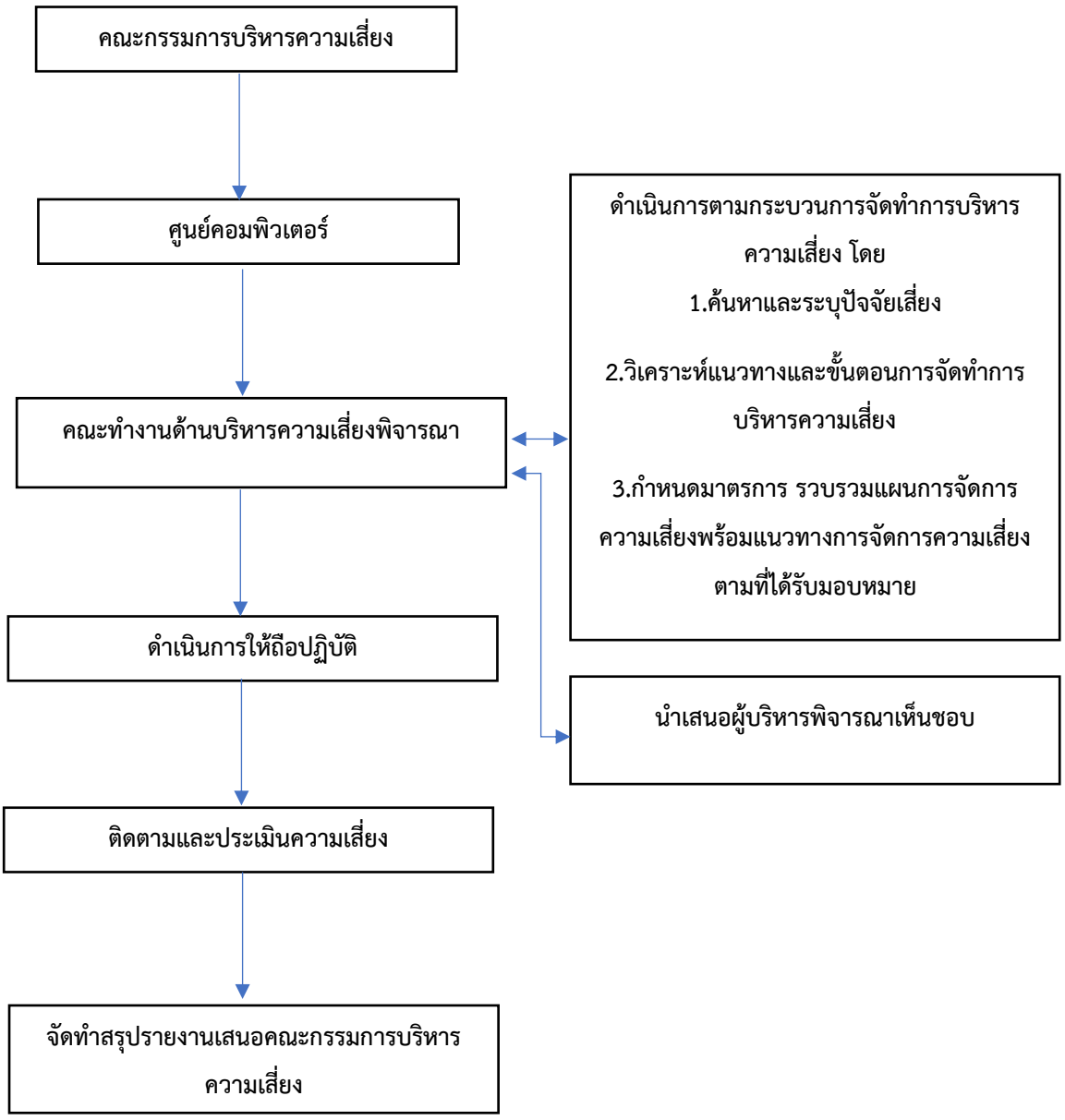
การวิเคราะห์ความเสี่ยง

โรงพยาบาลปายได้ตระหนักถึงความสำคัญของข้อมูลที่อาจประสบกับความเสียหายจากปัจจัยเสี่ยงต่างๆ จึงมอบหมายให้ศูนย์คอมพิวเตอร์ทำาแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ พ.ศ. 2566-2570 ให้สอดคล้องกับแผน บริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ของกระทรวงสาธารณสุข กระบวนการบริหารจัดการความเสี่ยงของหน่วยงานเริ่มต้นจากการรวบรวมข้อมูลที่เกี่ยวข้องกับกิจกรรม/ปัจจัยเสี่ยง หรือกระบวนงานที่มี ผลต่อการดำเนินงานด้านเทคโนโลยีสารสนเทศ และทำการศึกษาข้อมูล ระดมความคิดเห็นร่วมกับผู้ปฏิบัติงาน ด้านกิจกรรมนั้นๆ ดังตารางการบริหารจัดการความเสี่ยง ที่ได้จัดทำการวิเคราะห์โดยแยกการวิเคราะห์ ออกเป็นกิจกรรมต่างๆ ดังต่อไปนี้

1.แผนภูมิแนวทางและขั้นตอนการบริหารความเสี่ยง

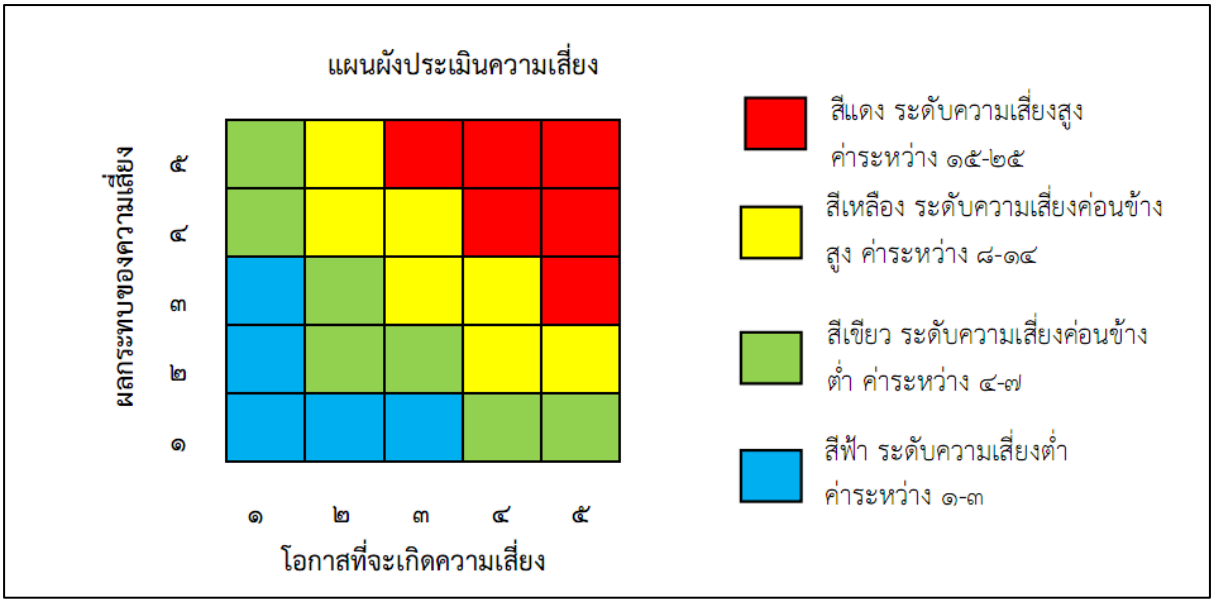


2.กระบวนการจัดทำการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ



3. การวิเคราะห์ปัจจัยเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ

การระบุความเสี่ยง (Risk identification) เป็นการชี้ให้เห็นถึงความเสี่ยงด้านต่างๆ ที่องค์กรเผชิญอยู่ ผลสรุป การกำหนดประเด็นความเสี่ยงด้านเทคโนโลยีสารสนเทศ รวมทั้งการประเมินระดับ ความเป็นไปได้ และผลกระทบมีดังนี้



ตารางที่ 1 ประเด็นความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ลำดับ	ความเสี่ยง	ความน่าจะเป็นที่จะเกิดขึ้น	ผลกระทบ	คะแนน
1	ความเสี่ยงจากอัคคีภัย	3	5	15
2	ความเสี่ยงจากระบบคอมพิวเตอร์แม่ข่ายหลักเสียหาย	4	5	20
3	ความเสี่ยงจากความชื้น อุณหภูมิ	3	4	12
4	การไม่สำรองข้อมูล/ การสำรองข้อมูลขาดการอัพเดท	3	5	15
5	ช่องโหว่จากการพัฒนาโปรแกรมประยุกต์ภายในองค์กร	3	5	15
6	การใช้โปรแกรมที่พัฒนาโดย Outsource ขาดแผนบริหารความต่อเนื่อง	3	5	15
7	ระบบกระแสไฟฟ้าขัดข้อง	4	5	20
8	การเชื่อมต่อระบบอินเทอร์เน็ต/ อินทราเน็ตขัดข้อง	4	4	16
9	การบุกรุกโจมตีจากภายนอก	4	5	20
10	ลิขสิทธิ์ซอฟต์แวร์	2	5	10
11	ไวรัสคอมพิวเตอร์/ Malware	4	5	20
12	ความเสี่ยงจากการถูก Black List จาก Search Engine /Spamhaus	2	3	6
13	ความเสี่ยงจากข้อมูลรั่วไหลจากการเปลี่ยนมือผู้ใช้	2	5	10
14	เจ้าหน้าที่ใช้คอมพิวเตอร์/เครือข่ายผิดวัตถุประสงค์	2	4	8
15	ความเสี่ยงจากแมลง/สัตว์กัดแทะ	1	5	5

16	การโจรกรรมอุปกรณ์คอมพิวเตอร์แม่ข่าย/อุปกรณ์	1	5	5
17	การโจมตี Server ของหน่วยงานไม่ให้สามารถ ให้บริการ ได้ (Denial of Service-DoS)	3	5	15
18	ความเสี่ยงจากการใช้Wireless เข้าเครือข่าย อินเตอร์เน็ต	3	5	15
19	วินาศภัย/การก่อการร้าย	1	5	5
20	การโจรกรรมฐานข้อมูล	3	5	15
21	ความเสี่ยงจากไฟกระชากจากปลั๊กพ่วง	2	2	4
22	ความเสี่ยงจากแผ่นดินไหว	1	4	4
23	ความเสี่ยงจากอุทกภัย	1	4	4

4. ผลการประเมินแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ประเภทความเสี่ยง	ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	แนวทางควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
ความเสี่ยงสูง							
ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)	1.ความเสี่ยงจากอัคคีภัย	1.คอมพิวเตอร์และเครือข่ายถูกทำลาย 2.ข้อมูลถูกทำลาย 3.การบาดเจ็บหรือเสียชีวิตของเจ้าหน้าที่หรือลูกจ้างภายในอาคาร	1. เสียงบประมาณใน การจัดหาระบบทดแทน 2.การไม่สามารถใช้งาน ระบบระหว่างที่มีการจัดหาระบบทดแทน	สูง 3*5 = 15	1.ตรวจสอบความพร้อมของการใช้งานอุปกรณ์ดับเพลิง 2.วางแผนจัดหาและติดตั้งระบบตรวจจับควันแจ้งเตือนไฟไหม้ระบบดับเพลิง 3.มีแผนในการเคลื่อนย้ายอุปกรณ์ตามลำดับความสำคัญ	การควบคุม (Treat)	ศูนย์คอมพิวเตอร์
ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร (Hardware and Data Communication Risk)	2.ความเสี่ยงจากระบบคอมพิวเตอร์แม่ข่ายหลักเสียหาย	1.ไม่สามารถใช้ระบบงานได้เต็มประสิทธิภาพ 2.เสี่ยงต่อความเสียหายของข้อมูลและการกู้คืนข้อมูล	1.การใช้งานระบบงาน ไม่สามารถใช้ได้ตามปกติ	สูง 4*5 = 20	1.ตรวจสอบระบบคอมพิวเตอร์แม่ ข่ายและสำรองฐานข้อมูล 2.จัดตั้งศูนย์สำรอง ข้อมูล(Backup Site)	การควบคุม (Treat)	ศูนย์คอมพิวเตอร์

ความเสี่ยงด้านระบบข้อมูล(Database Risk)	3. ความเสี่ยงจากการ สำรองข้อมูลการทำงานระบบไม่มีความเสถียรภาพ หรือทำการสำรองข้อมูลแต่ขาดการอัพเดท	1.เสี่ยงต่อการสูญหายของข้อมูล ในขั้นเล็กน้อยหรือมากจนไม่สามารถดำเนินงานได้ตามปกติ 2.เสี่ยงต่อการมีข้อมูลที่ ไม่ถูกต้องกับความเป็นจริง	1.เสียค่าใช้จ่ายในการกู้ คืนข้อมูล หรือ การจัดทำขึ้นมาใหม่ 2.ไม่สามารถนำข้อมูลที่มีอยู่ไปใช้งานได้เนื่องจากขาดความมั่นใจ ในข้อมูล	สูง 4*5 = 20	1.มีการบริหารจัดการในการทำการสำรองข้อมูล (Backup)เป็นประจำอย่างสม่ำเสมอ 2.มีการทดสอบการนำข้อมูลกลับคืนสู่ระบบ (Restore)	การควบคุม (Treat)	ศูนย์คอมพิวเตอร์
ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk)	4.ความเสี่ยงจากช่องโหว่จากการพัฒนาโปรแกรมประยุกต์ภายในองค์กร	1.การถูกขโมยข้อมูล 2.โปรแกรมเสียหาย 3.การใช้ช่องโหว่ของโปรแกรมหรือซ่อน Scriptไว้เพื่วัตถุประสงค์แอบแฝง	1. ลดความน่าเชื่อถือต่อรพ.ปายหากข้อมูลถูกขโมยไปและนำไปเผยแพร่ 2.กรณีที่เป็นข้อมูลลับอาจสร้างความเสียหายต่อ รพ.ปายเป็นอย่างยิ่ง	สูง 3*5 = 15	1.ตั้งมาตรฐานในการพัฒนาซอฟต์แวร์ตามคำแนะนำของ OWASP-Top10 Web Application Security Risks เพื่อลดความเสี่ยง 2.มีมาตรการกำหนดชั้นความลับของข้อมูลและการเข้าถึงข้อมูลที่เป็นความลับ 3.ตรวจสอบช่องโหว่ และดำเนินการปิดช่องโหว่	การควบคุม (Treat)	ศูนย์คอมพิวเตอร์และหน่วยงานที่พัฒนาใช้เอง
ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk)	5. ความเสี่ยงจากการจัดจ้างพัฒนาโปรแกรมหรือ ดูแลระบบโดยผู้รับจ้าง ภายนอก (Outsource)การขาดแผนบริหารความต่อเนื่อง	1.เสี่ยงต่อการถูกขโมยข้อมูล 2.เสี่ยงต่อการทำความเสียหายแก่โปรแกรม 3.ไม่สามารถแก้ไขข้อบกพร่องได้เอง	1. ลดความน่าเชื่อถือต่อรพ.ปายหากข้อมูลถูกขโมยไปและนำไปเผยแพร่ 2.กรณีที่เป็นข้อมูลลับอาจสร้างความ	สูง 3*5 = 15	1.การออกแบบระบบให้อิงมาตรฐาน Data Flow Diagram (DFD) Level 2.การออกแบบอ้างอิงแผนผังความสัมพันธ์ระหว่างกลุ่มข้อมูล–ER Diagram 3.ให้มีการส่งมอบ Source Code ในรูปแบบDVD, Flash Drive ในฟอร์แมต	การควบคุม (Treat)	ศูนย์คอมพิวเตอร์และหน่วยงานที่พัฒนาใช้เอง

		4.ขาดการดูแล บ ารุงรักษาโปรแกรม และข้อมูลทำให้ไม่สามารถใช้งานได้ในระยะยาว 5. เสียค่าใช้จ่ายสูง	เสียหายต่อหน่วยงานเป็นอย่างยิ่ง 3. จัดหางบประมาณ เพื่อทำการบำรุงรักษาโปรแกรมและข้อมูลพร้อมกับการทำการบำรุงรักษาเครื่องแม่ข่ายและอุปกรณ์ที่เกี่ยวข้องที่ต้องมีการอัพเดทอยู่ เสมอ		ที่ไม่เข้ารหัสใดๆและสามารถปรับปรุงแก้ไขได้ 4.หากมีการพัฒนา Library ด้วยตนเอง ต้องส่งSource Code Library ที่สามารถแก้ไขได้ 5.มีการถ่ายทอดความรู้ เทคโนโลยี ในการพัฒนาระบบให้กับเจ้าหน้าที่ 6.มีมาตรการในการกำหนดให้นำข้อมูลใดๆออกไปนอกสถานที่ได้ให้ชัดเจนและมีการควบคุมอย่างรัดกุม 7.จัดทำข้อตกลงการรักษาข้อมูลความลับของหน่วยงานระหว่างผู้รับจ้างกับผู้ว่าจ้าง 8.มีแผนการบำรุงรักษาระบบงานที่ดี รวมถึงการแก้ไขข้อผิดพลาดในการเขียนโปรแกรม (Bug)การอัพเดทเมื่อมี Versionหรือ Release ใหม่ การแก้ไขเมื่อเกิดการ Crashของโปรแกรมหรือฐานข้อมูล (Database)เกิดความเสียหาย เป็นต้น		

ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)	6.ความเสี่ยงจากการระบบกระแสไฟฟ้าขัดข้อง	1. ไม่สามารถใช้งานเครื่องแม่ข่ายและเครือข่ายได้ 2.ความเสี่ยงต่อการ Crash ของเครื่องแม่ข่ายทั้งส่วนระบบปฏิบัติการ (Operating System) ระบบฐานข้อมูล (RDBMS)อันเนื่องมาจากเครื่องไม่ได้ถูกทำการ Shutdownอย่างเหมาะสม	1.ข้อมูลเสียหาย 2.ระบบปฏิบัติการโปรแกรมหรือฐานข้อมูลเสียหายต้องมีการติดตั้งใหม่	สูง 4*5 = 20	1. ตรวจสอบระบบสำรองไฟฟ้า (UPS) 2.วางแผนการจัดหาและติดตั้งเครื่องกำเนิดไฟฟ้า (Electrical Generator) สำหรับรพ.ปาย ที่สามารถรองรับการใช้งานได้ตลอด24ชั่วโมง 3.วางแผนต่อไฟตรงอีกเฟสสำหรับห้องศูนย์คอมพิวเตอร์โดยเฉพาะ	การควบคุม (Treat)	ศูนย์คอมพิวเตอร์
ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร (Hardware and Data Communication Risk)	7.ความเสี่ยงจากการ เชื่อมต่อระบบเครือข่าย อินเทอร์เน็ต และ อินทราเน็ตขัดข้อง	1.ไม่สามารถใช้งานระบบงานหน่วยงานผ่านเครือข่ายอินทราเน็ตได้ 2. ไม่สามารถเชื่อมต่อภายนอกหน่วยงานผ่านเครือข่ายอินเทอร์เน็ตได้	1.ขัดขวางการทำงาน ของเจ้าหน้าที่และผู้บริหารงานในหน่วยงาน 2.บุคคลภายนอกไม่สามารถเข้าใช้ Web Serverหรือค้นหาข้อมูล ที่ต้องการได	สูง 4*4 = 16	ตรวจสอบระบบเครือข่ายสื่อสารหลัก	การควบคุม (Treat)	ศูนย์คอมพิวเตอร์

ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร (Hardware and Data Communication Risk)	8.การบุกรุกโจมตีจากภายนอก	เสี่ยงต่อการถูกโจมตีจากภายนอกผ่านเครือข่ายอินเทอร์เน็ต	1.ทำให้ระบบเครื่องแม่ข่ายหรือลูกข่ายติดไวรัสและแพร่กระจายสู่เครื่อง อื่นๆ ทั้งหมดในเครือข่าย 2.ถูกแก้ไขหรือเปลี่ยนแปลงข้อมูลหรือรูปภาพบน Web Site ของส า นักงานฯ 3. ถูกโจรกรรมข้อมูลที่เป็นความลับ	สูง 4*5 = 20	1.ติดตั้งระบบเครือข่ายเพื่อป้องกันและเตือนภัย 2.จัดทำแผนหรือขั้นตอนปฏิบัติที่จำเป็น ตามลำดับ 3. ตรวจสอบ Policy และ Log ของระบบ ป้องกันการบุกรุกระบบเครือข่าย	การควบคุม (Treat)	ศูนย์คอมพิวเตอร์
ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร (Hardware and Data Communication Risk)	9.ความเสี่ยงจากการติดไวรัสคอมพิวเตอร์หรือ Malware	1.โปรแกรมหรือข้อมูลถูกทำลาย 2.ไม่สามารถเรียกใช้โปรแกรมหรือระบบงาน ได้ตามปกติ 3. การถูกขโมยข้อมูล	1.ใช้คอมพิวเตอร์ไม่ได้ 2.ใช้ระบบงานไม่ได้ 3.ข้อมูลที่สำคัญสูญหาย	สูง 4*5 = 20	1.จัดหาและติดตั้งระบบป้องกันไวรัสกับเครื่องแม่ข่าย 2.จัดหาและติดตั้งระบบป้องกันไวรัสกับเครื่องลูกข่าย 3.อัพเดทข้อมูลไวรัสอย่างสม่ำเสมอ	การควบคุม (Treat)	ศูนย์คอมพิวเตอร์

ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร (Hardware and Data Communication Risk)	10.ความเสี่ยงจากการโจมตีเครื่องแม่ข่ายของโรงพยาบาลไม่ให้สามารถให้บริการได้ (Denial of Service-DoS)						
	10.1 ความเสี่ยงจากการถูกโจมตีระบบจากเครือข่ายภายนอก	เสี่ยงต่อการถูกโจมตีได้ จากภายนอก โดยโจมตีทั้งเครื่องแม่ข่ายและ/หรือเครือข่ายในทุกรูปแบบซึ่งจะมีการพัฒนาวิธีการอยู่ตลอดเวลา	ไม่สามารถใช้งานเครือข่ายได้หรือใช้ได้แต่ช้ามาก	สูง 3*5 = 15	1.ติดตั้งระบบป้องกันและเตือนภัย Spam,Virus, Malware, Trojan และมีเจ้าหน้าที่คอยดูแลตรวจสอบและอัพเดทฐานข้อมูลของอุปกรณ์นั้นๆ อยู่เป็นประจำเพื่อลดหรือสามารถแก้ไขได้ทันเมื่อถูกโจมตี 2. หมั่นตรวจสอบ Policy และ Log ของ Firewall และ IPS/ IDS อย่างสม่ำเสมอ	การควบคุม (Treat)	ศูนย์คอมพิวเตอร์
	10.2 ความเสี่ยงจากการถูกโจมตีระบบจากเครือข่ายภายใน	เสี่ยงต่อการถูกโจมตีจากโปรแกรมต่างๆ โดยเฉพาะประเภท Trojan ที่มีการติดตั้งที่เครื่องลูกข่ายโดยผู้ใช้งานภายในทั้งที่ไม่ได้ตั้งใจและตั้งใจ	ไม่สามารถใช้งานเครือข่ายได้หรือใช้ได้แต่ช้ามาก	สูง 3*5 = 15	1.มีมาตรการและกฎระเบียบในการควบคุมมิให้มีการติดตั้งโปรแกรม ต่างๆ ลงบนเครื่องลูกข่ายที่เชื่อมโยง กับเครือข่ายอินทราเน็ตของโรงพยาบาล 2.การควบคุมด้วยระบบDesktop Management	การควบคุม (Treat)	ศูนย์คอมพิวเตอร์

ความเสี่ยงด้านระบบข้อมูล(Database Risk)	11.ความเสี่ยงจากการโจรกรรมฐานข้อมูล	ข้อมูลที่สำคัญรั่วไหลสู่ภายนอกหรือสาธารณะ	1.เสียชื่อเสียงและความ น่าเชื่อถือที่มีต่อหน่วยงาน 2.การสูญหายหรือถูกทำลายของข้อมูล	สูง 3*5 = 15	1.มีการบริหารจัดการด้านการป้องกันข้อมูล 2.มีการบริหารจัดการด้านการเข้าถึงข้อมูล (Access) 3. มีการบริหารสื่อจัดเก็บข้อมูล เช่น Hard disk 4. Disk ม้วนเทป (Cartridge Tape) แผ่น DVD/CDให้แน่ใจว่าข้อมูลได้ถูกลบทิ้งอย่างถาวรหรือได้ทำลายอุปกรณ์หรือสื่อเก็บข้อมูลนั้นๆ ทิ้ง แล้ว หากทำได้	การควบคุม (Treat)	ศูนย์คอมพิวเตอร์
ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร (Hardware and Data Communication Risk)	12.ความเสี่ยงจากการใช้ Wirelessเข้าเครือข่ายอินเตอร์เน็ต	เสี่ยงต่อผู้ที่ไม่มีสิทธิ์เข้าถึงข้อมูลเข้าใช้เครือข่าย อินทราเน็ตผ่านทาง WIFI	ข้อมูลที่เป็นความลับถูกเผยแพร่หรือนำไปใช้อันจะนำมาซึ่งการขาดความเชื่อถือของหน่วยงานฯ	สูง 3*5 = 15	1.ควบคุมการเข้าใช้เครือข่าย 2.เพิ่มความปลอดภัยในการใช้งานเพิ่มขึ้นโดยิดตั้งระบบยืนยันตน (Authentication)	การควบคุม (Treat)	ศูนย์คอมพิวเตอร์
ความเสี่ยงค่อนข้างสูง							

ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)	1. ความเสี่ยงจากความชื้นอุณหภูมิ	ห้องคอมพิวเตอร์แม่ข่ายไม่มีระบบปรับอากาศที่สามารถความคุมอุณหภูมิความชื้นได้	อายุของเครื่องและอุปกรณ์สั้นลง	สูง 3x4=12	1.ตรวจสอบการทำงาน/อุณหภูมิเครื่องปรับอากาศที่มีอยู่เดิมอย่างสม่ำเสมอ 2.จัดหาระบบปรับอากาศชนิดที่สามารถควบคุมได้ทั้งอุณหภูมิและความชื้นให้อยู่ในสภาวะที่เหมาะสมและสามารถทำงานสลับกันได้	การยอมรับ (Take)	ศูนย์คอมพิวเตอร์
ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk)	2.ความเสี่ยงจากการใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์	1.การสูญหายของข้อมูล 2.การถูกฟ้องร้องและเสื่อมเสียชื่อเสียงและความน่าเชื่อถือของหน่วยงานฯ	1.การใช้งานอาจไม่ได้ประสิทธิภาพตามความสามารถของซอฟต์แวร์นั้นๆ 2. โรงพยาบาล อาจถูกฟ้องร้องเรียกค่าเสียหายจากผู้เป็นเจ้าของลิขสิทธิ์นั้นๆ 3.ความไม่สะดวกหากไม่ใช้งานด้วยซอฟต์แวร์ที่ไม่จำเป็นต้องมีลิขสิทธิ์ (Open Source)	ค่อนข้างสูง 2x5=10	1. การจัดหาซอฟต์แวร์ที่ถูกกฎหมายมาใช้งานตามความจำเป็น 2 .การรณรงค์ขอความร่วมมือเจ้าหน้าที่ในการใช้งานซอฟต์แวร์ที่ถูกกฎหมาย	การควบคุม (Treat)	ศูนย์คอมพิวเตอร์

ความเสี่ยงด้านระบบข้อมูล(Database Risk)	3.ความเสี่ยงจากข้อมูลรั่วไหลจากการเปลี่ยนมือ ผู้ใช้	ข้อมูลที่สำคัญมีการรั่วไหลจากการซ่อมแซมเครื่องที่เสีย เช่น Hard Disk หรือม้วนเทป(Cartridge Tape)แผ่น DVD/ CD	1.ข้อมูลที่อยู่ในชั้นความลับรั่วไหลทำให้เสียหายต่อความเชื่อถือของโรงพยาบาล 2.ข้อมูลที่รั่วไหลอาจทำให้ฝ่ายใดฝ่ายหนึ่ง นำไปใช้ประโยชน์ได้	ค่อนข้างสูง 2x5=10	มีการบริหารจัดการ ต่ออุปกรณ์เก็บข้อมูล เช่น Hard Disk ม้วนเทป (Cartridge Tape) แผ่น DVD/ CD ให้แน่ใจว่าข้อมูลได้ถูกลบทิ้งอย่างถาวร หรือได้ท าลายอุปกรณ์นั้นๆ ทิ้งแล้วหากท าได้	การยอมรับ (Take)	ศูนย์คอมพิวเตอร์
ความเสี่ยงด้านบุคลากร (Human Risk)	4.ความเสี่ยงจากการที่เจ้าหน้าที่ใช้คอมพิวเตอร์/เครือข่ายผิดวัตถุประสงค์	1. เสี่ยงต่อการใช้งานในทางที่ผิดหรือเปล่าประโยชน์ เช่น การฟังวิทยุหรือดูโทรทัศน์ออนไลน์ เป็นต้น 2. การใช้ Resource ทำผิดกฎหมาย เช่น การดาวน์โหลดโปรแกรม ภาพยนตร์ หรือเพลงที่ไม่มีลิขสิทธิ์ เป็นต้น	1.สูญเสีย Bandwidth ในเครือข่ายทำให้ ต้องจัดเพิ่ม Bandwidth ให้มากขึ้นทุกๆ ปี 2. อาจถูกร้องเรียนหรือ ฟ้องร้องจากบุคคลภายนอก	ค่อนข้างสูง 2x5=10	1.บริหารจัดการด้วยข้อแนะนำ Ten Ways to Protect Your Network From Insider Threats เพื่อลดความเสี่ยง 2.กำหนด Policy ของFirewall ให้เหมาะสมอย่างสม่ำเสมอ เปิด Port เท่าที่จำเป็น 3.การมีข้อตกลงที่ผู้ใช้งานต้องเป็นผู้รับผิดชอบในการนำอุปกรณ์เครื่องคอมพิวเตอร์ หรือ Resources ต่างๆ ไปใช้ในทางที่ผิด รวมถึงการบันทึก การใช้งานและรายงานการใช้งานของ ผู้ใช้ที่ฝ่าฝืนต่อผู้บังคับบัญชา	การควบคุม (Treat)	ศูนย์คอมพิวเตอร์
ความเสี่ยงค่อนข้างต่ำ							

ความเสี่ยงด้านบุคลากรHuman Risk) และความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร (Hardware and Data Communication Risk)	1.ความเสี่ยงจากการถูก Black List โดยSearch Engine หรือ Spamhaus (http://www.spamhaus.org	1.ผู้ใช้งานที่ต้องการข้อมูลของโรงพยาบาล หรือประชาชนทั่วไปไม่สามารถเข้าใช้งาน Web Server ได้ 2.ไม่สามารถใช้งานเครือข่ายหรือ e-mail ได้	1.ลดความน่าเชื่อถือหรือข้อมูลของโรงพยาบาล 2. โรงพยาบาล อาจถูก ฟ้องร้อง โดยผู้มีส่วนได้ส่วนเสีย	ค่อนข้างต่ า 2x3=6	1. ติดตั้งโปรแกรมเพื่อตรวจสอบให้แน่ใจว่าไม่มีอุปกรณ์ใดในเครือข่ายสำนักงานฯ ได้ส่ง Spam ออกไปยังเครือข่ายอินเทอร์เน็ต 2.ติดตั้งระบบการตรวจสอบแฟ้มข้อมูลก่อนการอัพโหลดข้อมูลขึ้น Web Server หรือ FTP Server 3.มีการอัพเดทตัวโปรแกรมและ Signature อย่างสม่ำเสมอ และการทำการบำรุงรักษา (Maintenance) ทั้งฮาร์ดแวร์และซอฟต์แวร์พร้อมทั้ง Update Licenses	การควบคุม (Treat)	ศูนย์คอมพิวเตอร์
ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)	2.ความเสี่ยงจากแมลงหรือสัตว์กัดแทะคอมพิวเตอร์อุปกรณ์หรือสายไฟฟ้า/สายสัญญาณ	เสี่ยงต่อการไม่สามารถใช้งานได้ปกติ	1.เสียงบประมาณในการซ่อมแซมหรือจัดหาทดแทน 2.ไม่สามารถให้บริการระบบได้อย่างต่อเนื่อง	ค่อนข้างต่ า 1x5=5	1.ไม่ปล่อยให้มีสายไฟฟ้าหรือสายสัญญาณไม่มีท่อห่อหุ้มจนถึงจุดทางเข้าตู้ Rack 2.ไม่นำอาหารหรือเครื่องดื่มมาทานหรือเก็บไว้ในบริเวณที่มีความเสี่ยง	การควบคุม (Treat)	ศูนย์คอมพิวเตอร์

ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)	3.ความเสี่ยงจากการโจรกรรมอุปกรณ์ คอมพิวเตอร์แม่ข่าย หรือเครื่องลูกข่ายและอุปกรณ์ ต่อพ่วง						
	3.1เครื่องแม่ข่ายสูญหาย	เสี่ยงต่อการสูญหายของอุปกรณ์และข้อมูลที่มีความสำคัญ	1. เสียงบประมาณใน การจัดหาเครื่องแม่ข่ายทดแทนที่มีมูลค่าสูง 2.เสียเวลาในการกู้ระบบ 3.เสียภาพลักษณ์ของหน่วยงานฯ	ค่อนข้างต่ำ 1x5=5	1. ติดตั้งระบบรักษาความปลอดภัยในการควบคุมการเข้า-ออกห้องคอมพิวเตอร์แม่ข่าย 2. ตู้ Rack ที่ติดตั้งอุปกรณ์ เช่น เครื่องแม่ข่าย (Server) อุปกรณ์ จัดเก็บข้อมูล (Disk Array) และอุปกรณ์เครือข่าย ต้องมีการล็อคด้วยกุญแจตลอดเวลา 3.จัดเก็บเครื่องคอมพิวเตอร์ที่สามารถเคลื่อนย้ายได้สะดวก เช่น Notebook ไว้ในที่มิดชิดเมื่อไม่ได้ใช้งาน	การควบคุม (Treat)	ศูนย์คอมพิวเตอร์
	3.2 เครื่องลูกข่ายและอุปกรณ์ต่อพ่วงสูญหาย	เสี่ยงต่อการสูญหายของอุปกรณ์และข้อมูลที่มีความสำคัญ	1. เสียงบประมาณใน การจัดหาอุปกรณ์ ทดแทน 2. เสียภาพลักษณ์ของหน่วยงานฯ	ค่อนข้างต่ำ 1x5=5	1.ควบคุมการเข้าออกอาคาร 2.ควบคุมการขนย้ายเครื่องคอมพิวเตอร์เข้า-ออก อาคาร ตลอดเวลา 3. ติดตั้งกล้องวงจรปิดให้ครอบคลุม ทุกที่ๆ มีเครื่องคอมพิวเตอร์และอุปกรณ์ติดตั้งอยู่	การควบคุม (Treat)	ศูนย์คอมพิวเตอร์

ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)	4.ความเสี่ยงจากวินาศภัย/การก่อการร้าย	การสูญหายและถูกทำลายของอุปกรณ์และข้อมูลที่เป็นส่วนสำคัญขององค์กร	ไม่สามารถใช้ระบบงานหรือข้อมูลได้เป็นปกติ	ค่อนข้างต่ำ า 1x5=5	1. ทำการสำรองข้อมูลไว้ต่างสถานที่กัน 2. จัดทำแผนสำรองฉุกเฉิน 3. จัดทำศูนย์สำรอง (Backup Site)	การยอมรับ (Take)	ศูนย์คอมพิวเตอร์
ความเสี่ยงด้านบุคลากร (Human Risk)	5.ความเสี่ยงจากไฟกระชากจากสายพ่วง (Extension Cord)	เสี่ยงต่อไฟไหม้ ไฟดูดไฟย้อนกลับทำให้อุปกรณ์เครื่องคอมพิวเตอร์เสียหายทั้งหมดได้	1. ไม่สามารถใช้งานเครื่องคอมพิวเตอร์ได้ตามปกติ 2. ไฟอาจลัดวงจรทาให้ เครื่องเสียหาย	ค่อนข้างต่ า 2x2=4	1.งดใช้สายพ่วงหรืองดใช้สายพ่วงที่ไม่ได้มาตรฐาน ม.อ.ก. และไม่มีสายดิน 2. ไม่ใช้อุปกรณ์ที่ไม่มีสายดิน (ปลั๊ก ๒ ขา หรือ ๓ ขาแต่หักสายดิน ออก) ต่อเข้ากับสายพ่วงหรือเต้าไฟฟ้า (Receptacle) 3. ต่อสายพ่วงเข้ากับอุปกรณ์ที่มี ระบบ Stabilize	การควบคุม (Treat)	ศูนย์คอมพิวเตอร์
ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)	6.ความเสี่ยงจากแผ่นดินไหว	ความเสียหายด้านโครงสร้างอาจทำลายระบบเครื่องและข้อมูล	ไม่สามารถใช้ระบบงานหรือข้อมูลได้เป็นปกติ	ค่อนข้างต่ า 1x4=4	1.ทำการสำรองข้อมูลไว้ต่างสถานที่กัน 2.จัดทำแผนสำรองฉุกเฉิน เพื่อ รับมือว่ามีขั้นตอนปฏิบัติอย่างไร และ จะใช้เครื่องทดแทนจากที่ใด เพื่อ สามารถจะใช้งานได้อย่างต่อเนื่อง 3.จัดทำศูนย์สำรอง (Backup Site)	การยอมรับ (Take)	ศูนย์คอมพิวเตอร์

ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)	7.ความเสี่ยงจากการเกิดอุทกภัย	ความเสียหายของเครื่องคอมพิวเตอร์และอุปกรณ์	การให้บริการระบบขาดความต่อเนื่อง	ค่อนข้างต่ า 1x4=4	1.มีแผนในการเคลื่อนย้ายอุปกรณ์ตามลำาดับความสำคัญ	การยอมรับ (Take)	ศูนย์คอมพิวเตอร์

แผนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศโรงพยาบาลปาย

ศูนย์คอมพิวเตอร์โรงพยาบาลปาย **ผู้รับผิดชอบหลัก ศูนย์คอมพิวเตอร์โรงพยาบาลปาย**

ระยะเวลาการด่าเนินการ ตุลาคม 2566 - ตุลาคม 2570

วัตถุประสงค์ : เพื่อให้การด่าเนินงานด้านการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศของโรงพยาบาลปายบรรลุเป้าประสงค์ของการบริหารความเสี่ยง

ประเภทความเสี่ยง/กิจกรรม	แผนปฏิบัติ	ระยะเวลา	2566	2567			2568			2569			2570			ผลลัพธ์/ความก้าวหน้า
			10-12	1-4	5-8	9-12	1-4	5-8	9-12	1-4	5-8	9-12	1-4	5-8	9-12	
1. ความเสี่ยงจากการเกิด อัคคีภัย	ตรวจสอบความพร้อมของการใช้งานอุปกรณ์ ดับเพลิง	- ทุกวันที่ 30 ก.ย. ของทุกปี	↔			↔			↔			↔			↔	
2. ความเสี่ยงจากการระบบคอมพิวเตอร์แม่ข่ายหลักเสียหาย	- ตรวจสอบระบบคอมพิวเตอร์แม่ข่าย	- ทุก 3 เดือน	↔			↔			↔			↔			↔	
3. ความเสี่ยงจากการระบบกระแสไฟฟ้าขัดข้อง	- ตรวจสอบการทำงานระบบไฟฟ้าไฟสำรอง UPS ที่มีอยู่เดิมอย่างสม่ำเสมอ	- ทุกวัน	←												→	
4. ความเสี่ยงจากการสำรอง ข้อมูล การทำงานระบบไม่มีความเสถียรภาพหรือทำการสำรองข้อมูลแต่ขาดการอัพเดท	- จัดทำการสำรองข้อมูล แบบอัตโนมัติ - มีการทดสอบการนำข้อมูล กลับคืนสู่ระบบ (Restore)	- ทุกวัน -2 ระบบต่อปี	← ↔			↔			↔			↔			→ ↔	

ประเภทความเสี่ยง/กิจกรรม	แผนปฏิบัติ	ระยะเวลา	2566	2567			2568			2569			2570			ผลลัพธ์/ความก้าวหน้า
			10-12	1-4	5-8	9-12	1-4	5-8	9-12	1-4	5-8	9-12	1-4	5-8	9-12	
5. ความเสี่ยงจากช่องโหว่ จากการพัฒนาโปรแกรมประยุกต์ภายในองค์กร	ตรวจสอบช่องโหว่ และดำเนินการปิดช่องโหว่	ปีละครั้ง	↔			↔			↔			↔			↔	
6. ความเสี่ยงจากการจัด จ้างพัฒนาโปรแกรมหรือ ดูแลระบบโดยผู้รับจ้างภายนอก (outsource) ขาดแผนบริหารความต่อเนื่อง	- จัดทำข้อตกลงการรักษาข้อมูลความลับของหน่วยงาน ระหว่างผู้รับจ้างกับผู้ว่าจ้าง	ปีละครั้ง	↔			↔			↔			↔			↔	
7.ความเสี่ยงจากการ เชื่อมต่อระบบเครือข่ายอินเทอร์เน็ตและอินทราเน็ตขัดข้อง	- ตรวจสอบระบบสัญญาณอินเตอร์เน็ตอย่างสม่ำเสมอ	- ทุกวัน	←	—	—	—	—	—	—	—	—	—	—	—	→	
8.การบุกรุกโจมตีจากภายนอก	-ตรวจสอบสถานะการทำงานของ firewall อย่างสม่ำเสมอ	- ทุกวัน	←	—	—	—	—	—	—	—	—	—	—	—	→	
9.ความเสี่ยงจากการติดไวรัสคอมพิวเตอร์หรือ Malware	-ตรวจสอบและอัพเดทระบบปฏิบัติและแอนตี้ไวรัส	- ทุกเดือนๆ ละครั้ง	←	—	—	—	—	—	—	—	—	—	—	—	→	

ประเภทความเสี่ยง/กิจกรรม	แผนปฏิบัติ	ระยะเวลา	2566	2567			2568			2569			2570			ผลลัพธ์/ความก้าวหน้า
			10-12	1-4	5-8	9-12	1-4	5-8	9-12	1-4	5-8	9-12	1-4	5-8	9-12	
10.ความเสี่ยงจากการโจมตีเครื่องแม่ข่ายของโรงพยาบาลไม่ให้สามารถให้บริการได้ (Denial of Service-DoS)	ตรวจสอบช่องโหว่ และดำเนินการปิดช่องโหว่	ทุก 6 เดือน	↔		↔		↔		↔		↔			↔		
11.ความเสี่ยงจากการโจรกรรมฐานข้อมูล	- ตรวจสอบ log การทำงานของระบบต่างๆ	ทุก 6 เดือน	↔			↔			↔			↔			↔	
12.ความเสี่ยงจากการใช้ Wireless เข้าเครือข่ายอินเตอร์เน็ต	-จัดทำคู่มือการใช้งานระบบอินเตอร์เน็ตและไวไฟ		↔													

บทที่ 3

สรุปและข้อเสนอแนะ

การจัดการความเสี่ยง (Risk Management) คือ กระบวนการในการระบุ วิเคราะห์ ประเมิน ดูแล ตรวจสอบ และควบคุมความเสี่ยงที่สัมพันธ์กับกิจกรรม หน้าที่ และกระบวนการทำงานเพื่อให้องค์กร ลดความเสียหายจากความเสี่ยงมากที่สุด อันเนื่องมาจากภัยที่องค์กรต้องเผชิญในช่วงเวลาใดเวลาหนึ่ง เมื่อเทคโนโลยีสารสนเทศก้าวเข้ามามีบทบาทสำคัญในฐานะกลไกอันทรงพลังในการขับเคลื่อน การดำเนินงาน ขององค์กร ทุกกิจกรรมที่เกิดขึ้นภายในองค์กรจึงล้วนมีความเกี่ยวข้องกับเทคโนโลยีสารสนเทศแทบทั้งสิ้น ในแต่ละวัน ข้อมูลมหาศาลถูกส่งผ่านเครือข่ายเทคโนโลยีสารสนเทศเพื่ออำนวยความสะดวกให้แก่ผู้ปฏิบัติงาน ของทุกหน่วยงานภายในโรงพยาบาลปาย ในปัจจุบัน “ข้อมูล” ถือว่าเป็นทรัพย์สิน อันทรงคุณค่ามหาศาลต่างตกอยู่ในสภาวะเสี่ยงต่อการถูกล่วงละเมิด ถูกทำให้เสียหายหรือเสียหาย และถูก นำไปใช้ในทางที่ผิด ทั้งจากบุคคลภายในและภายนอกองค์กรโดยเจตนาหรือไม่เจตนาก็ตาม ดังนั้น หนทางที่ดี ที่สุดในการแก้ปัญหานี้จึงควรเริ่มตั้งแต่การบริหารจัดการองค์กรให้ได้มาตรฐานด้านความปลอดภัย ซึ่งก็คือ การจัดการความเสี่ยงในองค์กรนั่นเอง

1. การวิเคราะห์ปัจจัยเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ

การระบุความเสี่ยง (Risk identification) เป็นการชี้ให้เห็นถึงความเสี่ยงด้านต่างๆ ที่องค์กร เผชิญอยู่ จากการกำหนดแนวทางปฏิบัติเพื่อควบคุมความเสี่ยงที่มีผลคะแนนสูงสุด 12 อันดับแรก ได้ข้อสรุป ดังนี้

1.ความเสี่ยงจากอัคคีภัย มีแนวทางปฏิบัติดังนี้

- ตรวจสอบความพร้อมของการใช้งานอุปกรณ์ดับเพลิง
- ติดตั้งระบบตรวจจับควัน แจ้งเตือนไฟไหม้ระบบดับเพลิง
- มีแผนในการเคลื่อนย้ายอุปกรณ์ตามลำดับความสำคัญ

2.ความเสี่ยงจากระบบคอมพิวเตอร์แม่ข่ายหลักเสียหาย มีแนวทางปฏิบัติดังนี้

- ตรวจสอบระบบคอมพิวเตอร์แม่ข่ายฐานข้อมูลหลักและสำรองฐานข้อมูล
- ควรมีการจัดตั้งศูนย์สำรองข้อมูล (Backup Site)
- จัดหาอุปกรณ์สำหรับสำรองข้อมูล เช่น (Hard disk External, Synology, Veem backup)

3. ความเสี่ยงจากการสำรองข้อมูลการทำงานระบบไม่มีความเสถียรภาพ หรือทำการสำรองข้อมูลแต่ขาดการอัพเดท มีแนวทางปฏิบัติดังนี้

- การบริหารจัดการในการทำการส ารองข้อมูล (Backup) เป็นประจำอย่างสม่ำเสมอ

- มีการทดสอบการนำข้อมูลกลับคืนสู่ระบบ (Restore)

4.ความเสี่ยงจากช่องโหว่จากการพัฒนาโปรแกรมประยุกต์ภายในองค์กร มีแนวทางปฏิบัติดังนี้

- ตั้งมาตรฐานในการพัฒนาซอฟต์แวร์ตามค าแนะน าของ OWASP- Top 10 Web Application Security Risks เพื่อลดความเสี่ยง

- มาตรการกำหนดชั้นความลับของข้อมูลและการเข้าถึงข้อมูลที่เป็นความลับ

- ตรวจสอบช่องโหว่ และดำเนินการปิดช่องโหว่

5. ความเสี่ยงจากการจัดจ้างพัฒนาโปรแกรมหรือ ดูแล ระบบโดยผู้รับจ้าง ภายนอก (Outsource)การขาดแผนบริหารความต่อเนื่อง มีแนวทางปฏิบัติดังนี้

- การออกแบบระบบให้อิงมาตรฐาน Data Flow Diagram (DFD) Level

- การออกแบบอ้างอิงแผนผังความสัมพันธ์ระหว่างกลุ่มข้อมูล

– ER Diagram

- ให้มีการส่งมอบ Source Code ในรูปแบบ DVD ในฟอร์แมตที่ไม่เข้ารหัสใดๆ และ สามารถปรับปรุงแก้ไขได้

- หากมีการพัฒนา Library ด้วยตนเอง ต้องส่ง Source Code Library ที่สามารถแก้ไขได้

- มีการถ่ายทอดความรู้ เทคโนโลยีในการพัฒนาระบบให้กับเจ้าหน้าที่

- มีมาตรการในการกำหนดให้นำข้อมูลใด ออกไปนอกสถานที่ได้ให้ชัดเจนและมีการ ควบคุมอย่างรัดกุม

- จัดทำข้อตกลงการรักษาข้อมูลความลับของหน่วยงานระหว่างผู้รับจ้างกับผู้ว่าจ้าง

- มีแผนการบำรุงรักษาระบบงานที่ดี รวมถึงการแก้ไขข้อผิดพลาดในการเขียนโปรแกรม (Bug) การอัพเดท เมื่อมี Version หรือ Release ใหม่ การแก้ไขเมื่อเกิดการ Crashของโปรแกรมหรือฐานข้อมูล (Database) เกิดความเสียหาย เป็นต้น

6.ความเสี่ยงจากการระบบกระแสไฟฟ้าขัดข้อง มีแนวทางปฏิบัติดังนี้

- ตรวจสอบเครื่องกำเนิดไฟฟ้าสำรองให้สามารถใช้งานได้สม่ำเสมอ

- ตรวจสอบเครื่องสำรองไฟ UPS ให้พร้อมใช้งานตลอดเวลา

7.ความเสี่ยงจากการเชื่อมต่อระบบเครือข่าย อินเทอร์เน็ตขัดข้อง มีแนวทางปฏิบัติดังนี้

- ตรวจสอบอุปกรณ์ต่อเชื่อมระบบต่างๆ
- ประสานผู้ให้บริการให้ตรวจสอบสัญญาณอินเตอร์เน็ต

8.การบุกรุกโจมตีจากภายนอก มีแนวทางปฏิบัติดังนี้

- จัดหาอุปกรณ์ป้องกัน next gen firewall

- จัดอบรมให้กับบุคลากรด้านคอมพิวเตอร์ในหน่วยงานให้มีความพร้อมด้านการตรวจสอบและรับมือภายคุกคามต่างๆ

9.ความเสี่ยงจากการติดไวรัสคอมพิวเตอร์หรือ Malware มีแนวทางปฏิบัติดังนี้

-ติดตั้งโปรแกรมป้องกันไวรัสและอัปเดตข้อมูลไวรัสอยู่เสมอ

- ติดตั้งโปรแกรมอุดช่องโหว่(patch) โดยการอัปเดตซอฟต์แวร์และโปรแกรมประยุกต์ต่าง ๆ ให้ใหม่อยู่เสมอ

- ปรับแต่งให้ซอฟต์แวร์ที่ใช้งานปลอดภัยสูงที่สุด เช่น ปรับแต่งไม่ให้โปรแกรมที่ใช้อ่าน E-mail รันไฟล์แนบ(Attachment) โดยอัตโนมัติ

- ระวังภัยจากการเปิดไฟล์จากสื่อบันทึกข้อมูล(Media) ต่าง ๆ
- ใช้ความระมัดระวังในการเปิดอ่าน E-mail

- ตระหนักถึงความเสี่ยงของไฟล์ที่ดาวน์โหลด หรือได้รับจากทางอินเตอร์เน็ต ไม่ดาวน์โหลดไฟล์ต่าง ๆ จากเว็บไซต์ที่ไม่มั่นใจ หรือไม่น่าเชื่อถือ

- กำหนดนโยบายด้านการบริหารจัดการไวรัสคอมพิวเตอร์ขององค์กร

10.ความเสี่ยงจากการโจมตีเครื่องแม่ข่ายของโรงพยาบาลไม่ให้สามารถให้บริการได้ (Denial of Service-DoS) มีแนวทางปฏิบัติดังนี้

10.1 ความเสี่ยงจากการถูกโจมตีระบบจากเครือข่ายภายนอก

- จัดหาและติดตั้งอุปกรณ์ป้องกัน next gen firewall เพื่อป้องกันการโดนโจมตีระบบเพื่อรับ Traffic ขนาดใหญ่

- จัดอบรมให้กับบุคลากรด้านคอมพิวเตอร์ในหน่วยงานให้มีความพร้อมด้านการตรวจสอบและรับมือภายคุกคามต่างๆ

- แนะนำให้ใช้บริการป้องกัน DDoS ขนาดใหญ่ https://www.cloudflare.com

- แนะนำให้เปิด Ports ที่จำเป็นสำหรับการใช้งานของลูกค้าเพื่อลดความเสี่ยงในการโดนเจาะระบบ

- ติดตั้ง Tools ที่ช่วยในการ block จาก connection ที่เชื่อมต่อแบบผิดปกติเช่น fail2ban, apacheModsecurity หรือใช้ Nginx ทำ rate limit

10.2 ความเสี่ยงจากการถูกโจมตีระบบจากเครือข่ายภายใน

-ติดตั้งโปรแกรมป้องกันไวรัสและอัปเดตข้อมูลไวรัสอยู่เสมอ

- ติดตั้งโปรแกรมอุดช่องโหว่(patch) โดยการอัปเดตซอฟต์แวร์และโปรแกรมประยุกต์ต่าง ๆ ให้ใหม่อยู่เสมอ

- ปรับแต่งให้ซอฟต์แวร์ที่ใช้งานปลอดภัยสูงที่สุด เช่น ปรับแต่งไม่ให้โปรแกรมที่ใช้อ่าน E-mail รันไฟล์แนบ(Attachment) โดยอัตโนมัติ

- ระวังภัยจากการเปิดไฟล์จากสื่อบันทึกข้อมูล(Media) ต่าง ๆ

- ใช้ความระมัดระวังในการเปิดอ่าน E-mail

- ตระหนักถึงความเสี่ยงของไฟล์ที่ดาวน์โหลด หรือได้รับจากทางอินเตอร์เน็ต ไม่ดาวน์โหลดไฟล์ต่าง ๆ จากเว็บไซต์ที่ไม่มั่นใจ หรือไม่น่าเชื่อถือ

- กำหนดนโยบายด้านการบริหารจัดการไวรัสคอมพิวเตอร์ขององค์กร

- จัดหาซอฟต์ที่มีลิขสิทธิ์ถูกต้อง เช่น ระบบปฏิบัติการ windows, Microsoft office, antivirus เป็นต้น

11.ความเสี่ยงจากการโจรกรรมฐานข้อมูล มีแนวทางปฏิบัติดังนี้

- รับการปกป้องด้วยข้อมูลที่ละเอียดอ่อน อย่าใส่ข้อมูลที่ละเอียดอ่อนในอีเมล สื่อสังคม หรือข้อความตัวอักษร วิธีการเหล่านี้อาจไม่ปลอดภัย มองหาสัญญาณว่าเว็บเพจมีความปลอดภัยและถูกต้อง ก่อนที่คุณจะใส่ข้อมูลที่ละเอียดอ่อน ให้ตรวจสอบให้แน่ใจว่าที่อยู่เว็บเริ่มต้นด้วย https ("s" ย่อมาจากการรักษาความปลอดภัย) และแสดงแม่กุญแจปิด (ล็อกอาจอยู่ที่มุมล่างขวาของหน้าต่าง)

- สร้างรหัสผ่านที่คาดเดายากและเก็บเป็นความลับ รหัสผ่านที่คาดเดายากจะมีความยาว (วลีหรือประโยค) ที่ประกอบด้วยตัวพิมพ์ใหญ่และตัวพิมพ์เล็ก ตัวเลข และสัญลักษณ์ ตามหลักแล้ว รหัสผ่านของคุณควรมีความยาวอย่างน้อย 14 อักขระ

ปกป้องบัญชีของคุณ ไม่แชร์รหัสผ่านของคุณ ไม่จดรหัสผ่านไว้บนหน้าจอคอมพิวเตอร์

- เพิ่มความปลอดภัยของคอมพิวเตอร์ โดยการติดตั้งซอฟต์แวร์ป้องกันไวรัสและป้องกันสปายแวร์ที่ถูกต้อง Windows มาพร้อมกับโปรแกรมป้องกันไวรัส Microsoft Defender ติดตั้งและเปิดใช้งานอยู่แล้ว และไม่ปิดไฟร์วอลล์

12.ความเสี่ยงจากการใช้ Wirelessเข้าเครือข่ายอินเตอร์เน็ต มีแนวทางปฏิบัติดังนี้

-จัดทำคู่มือและวิธีการใช้งานระบบอินเตอร์เน็ตและไวไฟ

- การจะเข้าใช้งานไวไฟต้องผ่านระบบพิสูจน์ยืนยันตัวตนเท่านั้น (Authentication)

- ปิด Wi-Fi หรือ logout ออกจากระบบทุกครั้งเมื่อคุณไม่ได้ใช้งาน

2. สรุป

แผนการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ ได้ดำเนินการจัดทำเพื่อ

2.1 เตรียมความพร้อมและรองรับสถานการณ์ฉุกเฉิน ที่อาจจะเกิดขึ้นกับระบบฐานข้อมูลสารสนเทศ

2.2 เป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศให้ มีเสถียรภาพ และมีความพร้อมสำหรับการใช้งาน

2.3 ให้การปฏิบัติงานเป็นไปอย่างมีระบบและต่อเนื่อง และสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงทีกรณีเกิดสถานการณ์ความไม่แน่นอนและภัยพิบัติ

3. ข้อเสนอแนะ

3.1 การควบคุมนโยบายและกระบวนการปฏิบัติงานถือเป็นสำคัญ เพื่อให้มั่นใจว่าได้มีการจัดการความเสี่ยง ดังนั้น ควรมีการกำหนดบุคลากรภายในหน่วยงานเพื่อรับผิดชอบการควบคุมนั้น โดยบุคลากรแต่ละคนที่ได้รับมอบหมายในการควบคุมควรมีความรับผิดชอบ ดังนี้

3.1.1 พิจารณาประสิทธิผลของการจัดการความเสี่ยงที่ได้ดำเนินการอยู่ในปัจจุบัน

3.1.2 พิจารณาการปฏิบัติเพิ่มเติมที่จำเป็น เพื่อเพิ่มประสิทธิผลของการจัดการความเสี่ยงนั้น

3.1.3 กำกับกิจกรรมลดความเสี่ยงให้แล้วเสร็จตามกำหนดวันตามแผนที่วางไว้

3.2 การติดตามการบริหารคววมเสี่ยงเพื่อให้มั่นใจว่าการจัดการความเสี่ยงมีคุณภาพ และมีความเหมาะสม ดังนั้น จึงควรมีการติดตามการบริหารความเสี่ยงอย่างต่อเนื่องและดำเนินการอย่าง สม่ำเสมอเพื่อตอบสนองต่อการเปลี่ยนแปลงอย่างทันท่วงที และถือเป็นส่วนหนึ่งของการปฏิบัติงาน รวมถึงการติดตามการดำเนินการภายหลังจากเกิดเหตุการณ์ขึ้น เพื่อวิเคราะห์ถึงปัญหาที่เกิดขึ้นและการแก้ไขอย่าง ถูกต้องได้อย่างมีประสิทธิภาพ