แผนบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ
กองสถานพยาบาลและการประกอบโรคศิลปะ
ประจำปีงบประมาณ พ.ศ.2566

กลุ่มแผนงานและประเมินผล
กองสถานพยาบาลและการประกอบโรคศิลปะ
มกราคม 2566

คำนำ

แผนบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ กองสถานพยาบาลและการประกอบโรคศิลปะ ประจำปีงบประมาณ 2566 จัดทำขึ้นโดยผ่านความเห็นชอบของคณะกรรมการพัฒนาดิจิทัลเพื่อการคุ้มครองผู้บริโภคด้านระบบบริการสุขภาพ กองสถานพยาบาลและการประกอบโรคศิลปะ ในการประชุมครั้งที่ 1/2566 เมื่อวันที่ 27 มกราคม 2566 และอนุมัติโดยผู้อำนวยการกองสถานพยาบาลและการประกอบโรคศิลปะ เพื่อเป็นกรอบแนวทางในการดำเนินงานบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ ในการระบุความเสี่ยง วิเคราะห์ความเสี่ยง และการกำหนดแนวทางหรือมาตรการควบคุมเพื่อป้องกันหรือลดความเสี่ยง โดยมีวัตถุประสงค์เพื่อลดความเสี่ยง เนื่องจากความเสี่ยงอาจนำไปสู่ผลเสียหรือความสูญเสียทั้งทางตรงและทางอ้อม หน่วยงานจึงต้องเข้าใจประเภทของความเสี่ยงที่เผชิญอยู่ เพื่อที่จะได้เลือกวิธีการที่เหมาะสมในการบริหารความเสี่ยงเหล่านั้นให้อยู่ระดับที่สามารถรองรับได้ เพื่อให้การดำเนินงานมีประสิทธิภาพและบรรลุวัตถุประสงค์ ผู้จัดทำหวังเป็นอย่างยิ่งว่าแผนบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ กองสถานพยาบาลและการประกอบโรคศิลปะฉบับนี้ จะช่วยให้ผู้รับผิดชอบใช้เป็นแนวทางในการลดความเสียหายต่างๆ ที่อาจเกิดขึ้นและส่งผลต่อกระบวนการบริหารงานด้านเทคโนโลยีสารสนเทศ กองสถานพยาบาลและการประกอบโรคศิลปะต่อไป

กลุ่มแผนงานและประเมินผล
กองสถานพยาบาลและการประกอบโรคศิลปะ
มกราคม 2566

สารบัญ

สารบัญ (ต่อ)

บทที่ 1
บทนำ

1. หลักการและเหตุผล

การบริหารความเสี่ยงเป็นเครื่องมือทางกลยุทธ์ที่สำคัญตามหลักการกำกับดูแลกิจการที่ดี โดยจะช่วยให้การบริหารงานและการตัดสินใจด้านต่างๆ เช่น การวางแผน การกำหนดกลยุทธ์ การติดตามควบคุมและวัดผลการปฏิบัติงาน ตลอดจนการใช้ทรัพยากรต่างๆ อย่างเหมาะสมและมีประสิทธิภาพมากขึ้น ลดการ สูญเสียและโอกาสที่ทำให้เกิดความเสียหายแก่หน่วยงาน โดยเฉพาะอย่างยิ่งในด้านเทคโนโลยีสารสนเทศที่เข้ามามีบทบาทสำคัญในการดำเนินงานของหน่วยงาน ทั้งการจัดเก็บข้อมูล การใช้งานอุปกรณ์ คอมพิวเตอร์ การติดต่อสื่อสารผ่านระบบเครือข่าย และวิธีการปฏิบัติงานที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศต่างๆ ภายใต้สภาวะการดำเนินงานของหน่วยงาน ล้วนแต่มีความเสี่ยง ซึ่งก็คือความไม่แน่นอนที่จะส่งผลกระทบต่อการดำเนินงานหรือเป้าหมายของหน่วยงาน จึงจำเป็นต้องมีการจัดการความเสี่ยงเหล่านั้นอย่างเป็นระบบ โดยการระบุความเสี่ยงว่ามีปัจจัยเสี่ยงใดบ้างที่กระทบต่อการดำเนินงานหรือเป้าหมายของหน่วยงาน วิเคราะห์ความเสี่ยงจากโอกาสและผลกระทบที่เกิดขึ้น จัดลำดับความสำคัญของปัจจัยเสี่ยง แล้วกำหนดแนวทางในการจัดการความเสี่ยง โดยต้องคำนึงถึงความคุ้มค่าในการจัดการความเสี่ยงอย่างเหมาะสม

2. วัตถุประสงค์

2.1 เพื่อเตรียมความพร้อมรองรับสถานการณ์ฉุกเฉิน ที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศของกองสถานพยาบาลและการประกอบโรคศิลปะ

2.2 เพื่อเป็นแนวทางในการดูแลรักษาระบบเทคโนโลยีสารสนเทศให้มีเสถียรภาพ และมีความพร้อมสำหรับการใช้งาน

2.3 เพื่อให้การปฏิบัติงานเป็นไปอย่างมีระบบและต่อเนื่อง และสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที กรณีเกิดสถานการณ์ความไม่แน่นอนและภัยพิบัติ

3. สภาพแวดล้อมด้านเทคโนโลยีสารสนเทศ

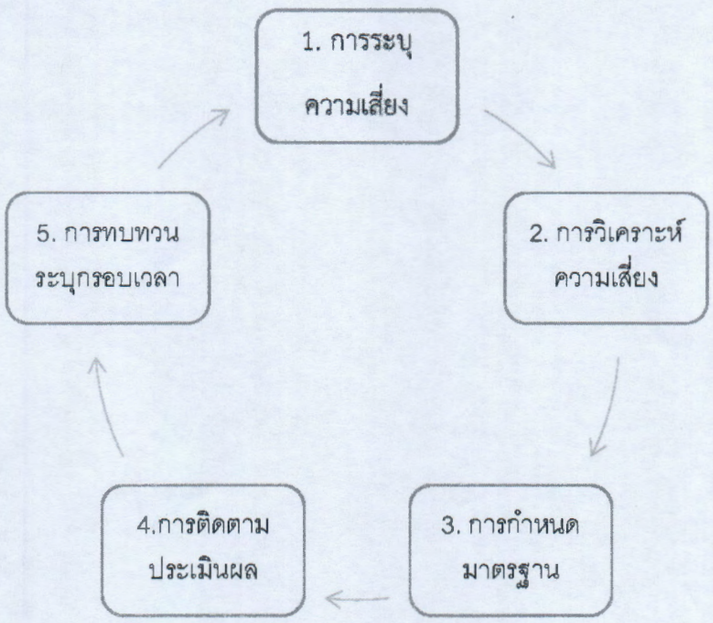
3.1 ระบบเทคโนโลยีสารสนเทศและโปรแกรมปฏิบัติการ (Database & Software) เช่น ระบบข้อมูลสารสนเทศเพื่อการคุ้มครองผู้บริโภคด้านบริการสุขภาพภาคเอกชน,ระบบ Biz Portal, เว็บไซต์กองสถานพยาบาลและการประกอบโรคศิลปะและระบบเพื่อการบริหารงานภายใน (Smart Office) เป็นต้น

3.2 ระบบให้บริการเครือข่าย ได้แก่ ระบบเครือข่ายอินเทอร์เน็ต (Internet) ระบบเครือข่ายมีสายภายใน (LAN) ระบบเครือข่ายไร้สายภายใน (WiFi)

3.3 อุปกรณ์คอมพิวเตอร์ (Hardware) เช่น เครื่องคอมพิวเตอร์ตั้งโต๊ะ (PC), เครื่องคอมพิวเตอร์ชนิดพกพา (Note Book), เครื่องสแกนเนอร์ (Scanner), เครื่องพิมพ์เลเซอร์ (Laser Printer), เครื่องพิมพ์แบบพ่นหมึก (Inkjet Printer), อุปกรณ์สำรองไฟฟ้าสำหรับคอมพิวเตอร์ (UPS)

4. กระบวนการบริหารความเสี่ยง

เป็นกระบวนการที่ใช้ในการระบุ วิเคราะห์ ประเมิน จัดระดับความเสี่ยง ที่มีผลกระทบต่อการบรรลุวัตถุประสงค์ของกระบวนการทำงานของหน่วยงานหรือขององค์กร รวมทั้งการบริหาร/จัดการความเสี่ยง และการกำหนดแนวทางการดำเนินงานหรือมาตรการควบคุมหรือป้องกันหรือลดความเสี่ยง ซึ่งมีขั้นตอนการดำเนินการ หลักเกณฑ์ในการวิเคราะห์อย่างเหมาะสม โดยครอบคลุม 5 ขั้นตอน ดังนี้



4.1 การระบุความเสี่ยงหรือปัจจัยเสี่ยง

เป็นกระบวนการที่ผู้บริหารและผู้ปฏิบัติงานร่วมกันระบุความเสี่ยงและปัจจัยเสี่ยงที่เกี่ยวข้องในโครงการ/กิจกรรม เพื่อให้ทราบถึงเหตุการณ์ที่เป็นความเสี่ยง ที่อาจมีผลกระทบต่อการบรรลุผลสำเร็จตามวัตถุประสงค์ ซึ่งต้องคำนึงถึงสภาพแวดล้อมทั้งภายนอกและภายในหน่วยงาน วิธีการในการระบุความเสี่ยงมีหลายวิธี เช่น

- การระดมสมองเพื่อให้ได้ความเสี่ยงที่หลากหลาย
- การใช้ Checklist
- การวิเคราะห์สถานการณ์จากการตั้งคำถาม “What-if”
- การวิเคราะห์ขั้นตอนการปฏิบัติงานในแต่ละขั้นตอน
- การรวบรวมปัญหาที่เกิดขึ้นมาแล้ว

ในขั้นตอนนี้ ควรมีการเก็บข้อมูลความสูญเสียที่เกิดขึ้นในรูปของความถี่ของการเกิดความสูญเสีย และความรุนแรงของความสูญเสีย รวมทั้งข้อมูลการดำเนินการใดๆ เพื่อลดความสูญเสียที่เกิดขึ้นในอดีต ทั้งที่ประสบผลสำเร็จ และปัญหาอุปสรรคซึ่งจะเป็นประโยชน์ในการดำเนินการต่อไป

4.2 การวิเคราะห์และประเมินความเสี่ยง

การประเมินความเสี่ยงเป็นกระบวนการที่ประกอบด้วยการวิเคราะห์ การประเมิน และ การจัดระดับความเสี่ยง ประกอบด้วย 4 ขั้นตอน คือ

4.2.1 การกำหนดเกณฑ์การประเมินมาตรฐาน เป็นเกณฑ์ที่จะใช้ประเมินความเสี่ยง ได้แก่ โอกาสที่จะเกิดความเสี่ยง (Likelihood) ระดับความรุนแรงของผลกระทบ (Impact) และระดับของความเสี่ยง (Degree of Risk) คณะกรรมการบริหารความเสี่ยงต้องกำหนดเกณฑ์ของหน่วยงานขึ้น ซึ่งอาจกำหนดได้ทั้งเกณฑ์เชิงปริมาณและเชิงคุณภาพ การกำหนดเกณฑ์ของโอกาสที่เกิดความเสี่ยงอาจกำหนดเป็นเกณฑ์ 5 ระดับ (สูงมาก/รุนแรงมากที่สุด สูง/ค่อนข้างรุนแรง ปานกลาง น้อย และ น้อยมาก) ส่วนระดับของความเสี่ยงอาจกำหนดเป็นเกณฑ์ 4 ระดับ (สูงมาก สูง ปานกลาง และน้อย)

4.2.2 การประเมินโอกาสและผลกระทบของความเสี่ยง เป็นการนำความเสี่ยงและปัจจัยเสี่ยงแต่ละปัจจัยที่ระบุไว้มาประเมินโอกาสที่จะเกิดเหตุการณ์ความเสี่ยงเหล่านั้นและประเมินระดับความรุนแรงหรือมูลค่าความเสียหายจากความเสี่ยงตามเกณฑ์มาตรฐานที่กำหนดเพื่อให้เห็นระดับความเสี่ยง ซึ่งแต่ละความเสี่ยงก็จะมีความรุนแรงแตกต่างกัน ทั้งนี้การควบคุมความเสี่ยงหรือหลีกเลี่ยงความเสี่ยงนั้น ก็จะขึ้นอยู่กับมาตรการควบคุมความเสี่ยงของแต่ละหน่วยงาน โดยมีการประเมินใน 2 มิติ ได้แก่ มิติผลกระทบและมิติโอกาสของความเสี่ยงที่จะเกิดขึ้น

เกณฑ์การประเมินผลกระทบ เป็นดังนี้

ระดับ การประเมิน

1 น้อยมาก

2 น้อย

3 ปานกลาง

4 สูง

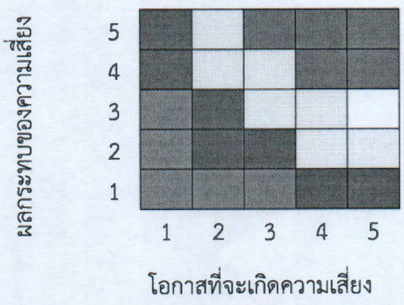
5 สูงมาก

เกณฑ์การประเมินโอกาสของการเกิดความเสี่ยงเป็นดังนี้

ระดับ	โอกาสที่จะเกิด	เชิงปริมาณ	เชิงคุณภาพ
1	น้อยมาก	ไม่เกิน 1 ครั้งต่อปี	มีโอกาสเกิดเกือบทุกครั้ง
2	น้อย	2 ครั้งต่อปี	มีโอกาสในการเกิดค่อนข้างสูงหรือบ่อยๆ
3	ปานกลาง	3 ครั้งต่อปี	มีโอกาสเกิดบางครั้ง
4	สูง	4 ครั้งต่อปี	อาจมีโอกาสเกิดแต่นานๆ ครั้ง
5	สูงมาก	มากกว่า 4 ครั้งต่อปี	มีโอกาสเกิดในกรณียกเว้น

4.2.3 การวิเคราะห์ความเสี่ยง เป็นการดูความสัมพันธ์ระหว่างโอกาสที่จะเกิดความเสี่ยงและผลกระทบของความเสี่ยงต่อองค์กรว่าจะก่อให้เกิดระดับความเสี่ยงในระดับใด โดยใช้ตารางระดับความเสี่ยงสูงสุดที่จะต้องบริหารจัดการก่อน ดังรูปต่อไปนี้ผลกระทบของความเสี่ยง

แผนผังประเมินความเสี่ยง



สีแดง หมายถึง ระดับความเสี่ยงสูง ค่าระหว่าง 15 - 25

สีเหลือง หมายถึง ระดับความเสี่ยงค่อนข้างสูง ค่าระหว่าง 8 - 14

สีเขียว หมายถึง ระดับความเสี่ยงค่อนข้างต่ำ ค่าระหว่าง 4 - 7

สีฟ้า หมายถึง ระดับความเสี่ยงต่ำ ค่าระหว่าง 1 - 3

4.2.4 การจัดลำดับความเสี่ยง เป็นการจัดลำดับความรุนแรงของความเสี่ยงที่มีผลต่อหน่วยงานเพื่อพิจารณากำหนดกิจกรรมการควบคุมในแต่ละสาเหตุของความเสี่ยงที่สำคัญให้เหมาะสมโดยพิจารณาจากระดับความเสี่ยงที่ประเมินได้ เลือกความเสี่ยงที่มีระดับสูงมาก หรือสูงมาจัดทำแผนการบริหารความเสี่ยงเป็นลำดับแรก

4.3 การกำหนดมาตรการจัดการความเสี่ยงอย่างรัดกุม

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

4.3.1 ควบคุมเพื่อการป้องกัน (Preventive Control) เป็นวิธีการควบคุมเพื่อป้องกันไม่ให้เกิดความเสี่ยงและข้อผิดพลาดตั้งแต่แรก เช่น การอนุมัติ การจัดโครงสร้างหน่วยงาน การควบคุม การเข้าถึงเอกสาร เป็นต้น

4.3.2 การควบคุมเพื่อให้ตรวจพบ (Detective Control) เป็นวิธีการควบคุม เพื่อค้นข้อผิดพลาดที่เกิดขึ้นแล้ว เช่น การวิเคราะห์ การตรวจนับ การรายงานข้อบกพร่อง เป็นต้น

4.3.3 การควบคุมโดยการชี้แนะ (Direction Control) เป็นวิธีควบคุมที่ส่งเสริมหรือกระตุ้นให้เกิดความสำเร็จตามวัตถุประสงค์

4.3.4 การควบคุมเพื่อการแก้ไข (Corrective Control) เป็นวิธีการควบคุมเพื่อแก้ไขข้อผิดพลาดที่เกิดขึ้นให้ถูกต้อง หรือหาวิธีแก้ไขไม่ให้เกิดข้อผิดพลาดนั้นซ้ำอีกในอนาคตหลังจากประเมินความเสี่ยงแล้ว จะต้องวิเคราะห์การควบคุมที่มีอยู่ว่าได้มีการจัดการควบคุมเพื่อลดความเสี่ยงดังกล่าวหรือไม่โดยนำผลการจัดระดับความเสี่ยงในระดับสูงมากและสูง มาประเมินมาตรการควบคุมเป็นอันดับแรก อาจใช้ขั้นตอนดังนี้

1) นำปัจจัยเสี่ยงที่อยู่ในระดับสูงมาก หรือสูงมากำหนดวิธีควบคุมที่ควรจะมี เพื่อป้องกันความเสี่ยงหรือปัจจัยเสี่ยงเหล่านั้น

2) พิจารณา หรือประเมินว่าในปัจจุบันความเสี่ยงหรือปัจจัยเสี่ยงนั้นมีการควบคุมอยู่แล้วหรือไม่

3) ถ้ามีการควบคุมแล้ว ให้ประเมินต่อไปว่าการควบคุมนั้นได้ผลตามความต้องการหรือไม่

4.4 การติดตาม รายงานและประเมินผลการดำเนินการตามมาตรการจัดการความเสี่ยงที่ได้กำหนดไว้

การติดตามผลการดำเนินงาน การนำกลยุทธ์ มาตรการ หรือแนวทางมาใช้ปฏิบัติ เพื่อลดโอกาสที่เกิดความเสี่ยงหรือลดความเสียหายของผลที่อาจเกิดขึ้นจากความเสี่ยง ในโครงการ/กิจกรรม ที่ยังไม่มีกิจกรรมควบคุมความเสี่ยงหรือมีแต่ไม่เพียงพอ และนำมาวางแผนจัดการความเสี่ยง ทางเลือกในการบริหารความเสี่ยงมีหลายวิธีซึ่งสามารถปรับเปลี่ยนหรือนำมาผสมผสานให้เหมาะสมกับสถานการณ์ อาจเป็นการยอมรับความเสี่ยง การลด/การควบคุมความเสี่ยง การกระจายความเสี่ยง หรือการหลีกเลี่ยงความเสี่ยง เมื่อหน่วยงานทราบความเสี่ยงที่ยังเหลืออยู่จากการประเมินความเสี่ยง และการประเมินการควบคุมแล้วให้พิจารณาความเป็นไปได้และค่าใช้จ่ายแต่ละทางเลือก เพื่อตัดสินใจเลือกมาตรการลดความเสี่ยงที่เหมาะสมโดยพิจารณาจาก

4.4.1 พิจารณาว่ายอมรับความเสี่ยง หรือจะกำหนดกิจกรรมควบคุมเพื่อลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

4.4.2 เปรียบเทียบค่าใช้จ่ายหรือต้นทุนในการจัดการให้มีมาตรการควบคุมกับผลประโยชน์ที่จะได้รับจากมาตรการดังกล่าวว่าคุ้มค่าหรือไม่

4.4.3 กรณีเลือกกำหนดกิจกรรมควบคุมเพื่อลดความเสี่ยงให้กำหนดวิธีควบคุมในแผนบริหารความเสี่ยง

4.4.4 ในรอบปีต่อไป ให้พิจารณาผลการติดต่อการบริหารความเสี่ยงในงวดก่อนที่ดำเนินการมาบริหารความเสี่ยงตามกระบวนการเหล่านั้น หากพบว่ายังมีความเสี่ยงที่มีนัยสำคัญซึ่งอาจมีผลต่อการบรรลุวัตถุประสงค์และ

เป้าหมายตามแผนปฏิบัติงานของหน่วยงาน ให้นำมาระบุการควบคุมในแผนบริหารความเสี่ยงด้วยการรายงานผลการวิเคราะห์ประเมินและบริหารจัดการความเสี่ยง ว่ามีความเสี่ยงที่ยังเหลืออยู่หรือไม่ ถ้าไม่มีเหลืออยู่ มีอยู่ในระดับความเสี่ยงสูงมากเพียงใด และมีวิธีการจัดการความเสี่ยงนั้นอย่างไร โดยเสนอต่อผู้บริหารเพื่อทราบและสั่งการ

4.5 การทบทวนการบริหารความเสี่ยงโดยระบุกรอบเวลาในการทบทวนอย่างชัดเจน

เป็นการติดตามภายหลังจากได้ดำเนินการตามแผนการบริหารความเสี่ยง ว่ามีความเสี่ยงแล้วเพื่อให้มั่นใจว่าแผนการบริหารความเสี่ยงนั้นมีประสิทธิภาพ ทั้งนี้ เพื่อประเมินคุณภาพและความเหมาะสมของวิธีการจัดการความเสี่ยงที่ใช้ และเป็นการตรวจสอบความคืบหน้าของมาตรการควบคุม โดยอาจติดตามผลเป็นรายครั้งตามรอบระยะเวลาหรือการติดตามผลในระหว่างการปฏิบัติงาน

5. ความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ประเภทความเสี่ยงด้านเทคโนโลยีสารสนเทศ ตามแนวทางของ COSO (Committee of Sponsoring Organization) แบ่งออกเป็น 8 ประเภท ดังนี้

5.1 ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)

หมายถึง ความเสี่ยงที่เกิดจากภัยคุกคามทั้งภัยจากธรรมชาติ และภัยที่มนุษย์ทำขึ้น เช่น วาตภัย อุทกภัย อัคคีภัย ฟ้าผ่า กระแสไฟฟ้าขัดข้อง การชุมนุมประท้วง การก่อการร้าย รวมถึงการไม่มีระบบรักษาความปลอดภัยห้องปฏิบัติการระบบเครือข่ายและคอมพิวเตอร์ เครื่องคอมพิวเตอร์แม่ข่าย และระบบสื่อสารที่มีประสิทธิภาพเพียงพอ

5.2 ความเสี่ยงด้านบุคลากร (Human Risk)

หมายถึง ความเสี่ยงที่เกิดจากบุคลากรที่เกี่ยวข้องกับการดำเนินงานด้านเทคโนโลยีสารสนเทศทั้งในด้านการวางแผน การตรวจสอบการทำงาน การมอบหมายหน้าที่และสิทธิ์ของบุคลากรและคณะทำงานที่มีส่วนเกี่ยวข้องกับการดำเนินการทุกฝ่ายอย่างละเอียด เพื่อให้บุคลากรมีความรู้ ความเข้าใจในการใช้งาน การดูแลรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งบุคลากรภายนอกที่เกี่ยวข้องทั้งทางตรงและทางอ้อม ซึ่งล้วนแต่เป็นความเสี่ยงทั้งสิ้น

5.3 ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร (Hardware and Data Communication Risk)

หมายถึง ความเสี่ยงที่เกิดจากความผิดพลาดของอุปกรณ์ การเคลื่อนย้ายตัวเครื่องอุปกรณ์ การติดตั้งอุปกรณ์ในพื้นที่ไม่เหมาะสม การถูกภัยคุกคามจากภัยต่างๆ เช่น ไวรัสคอมพิวเตอร์ Malware, Trojan, Adware เป็นต้น ทั้งที่เป็นการโจมตีจากภายใน และมาจากภายนอกโดยผ่านทางเครือข่าย(Networks) หรือจากคอมพิวเตอร์โดยตรง เช่น จาก USB Flash Drive หรือ USB External Hard Disk Drive เป็นต้น

5.4 ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk)

หมายถึง ความเสี่ยงที่เกิดจากระบบการทำงานของโปรแกรมต่างๆ เช่น การใช้โปรแกรมที่ไม่มีการอัพเดทให้ทันสมัย เพื่อลดช่องโหว่ที่อาจเกิดจาก Bug ของซอฟต์แวร์นั้นๆ หรือการถูกผู้ไม่หวังดี (Hacker) เข้ามาทำลายระบบหรือการใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ ซึ่งสำนักงานฯ อาจถูกฟ้องร้องให้ต้องชำระค่าละเมิดลิขสิทธิ์ เป็นต้น

5.5 ความเสี่ยงด้านระบบข้อมูล (Database Risk)

หมายถึง ความเสี่ยงที่เกิดจากฐานข้อมูลต่างๆ ในระบบสารสนเทศและการสื่อสารอันอาจจะก่อให้เกิดความเสียหาย เนื่องจากข้อมูลถูกทำลาย ความเสี่ยงจากผู้บุกรุกข้อมูล เพื่อการโจรกรรมข้อมูลที่สำคัญการลักลอบเข้ามาแก้ไขเปลี่ยนแปลงข้อมูล ทำให้เกิดความเสียหาย ขาดความน่าเชื่อถือและสร้างความเสื่อมเสียแก่หน่วยงาน ความเสี่ยงเหล่านี้ทำให้มีความจำเป็นที่จะต้องมีการบริหารจัดการความเสี่ยงด้านข้อมูล ดังนั้น การรักษาความปลอดภัยของข้อมูลจึงเป็นเรื่องสำคัญ เนื่องจากข้อมูลสารสนเทศและการสื่อสารเป็นปัจจัยสำคัญสำหรับผู้บริหาร ผู้มีส่วนได้ส่วนเสีย

โดยตรง รวมถึงประชาชนทั่วไป ดังนั้น การรักษาความปลอดภัยของระบบข้อมูลและคอมพิวเตอร์จากภัยต่างๆ ทั้งภัยจากคน ภัยจากธรรมชาติ หรือเหตุการณ์ใดๆ จึงมีความสำคัญและจำเป็นที่จะต้องมีการป้องกัน เพื่อให้เกิดความมั่นคงต่อระบบเทคโนโลยีสารสนเทศ

5.6 ความเสี่ยงด้านกลยุทธ์ (Strategic Risk)

หมายถึง ความเสี่ยงที่เกิดจากการเปลี่ยนแปลงของนโยบายรัฐบาล ผู้บริหารหน่วยงาน เนื่องจากการเปลี่ยนแปลงรัฐบาล และผู้บริหารหน่วยงานต่างๆ ในด้านเทคโนโลยีสารสนเทศและการสื่อสาร ทำให้การกำหนดยุทธศาสตร์และกลยุทธ์เปลี่ยนแปลงไป

5.7 ความเสี่ยงด้านการเงิน (Financial Risk)

หมายถึง ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ และต่อการเบิกจ่ายงบประมาณไม่ทันตามกำหนดเวลา

5.8 ความเสี่ยงในด้านการบริหารจัดการ (Management Risk)

หมายถึง ความเสี่ยงเนื่องมาจากการบริหารที่ไม่รัดกุม ไม่มีแผนงานในการดำเนินการที่ดี

6. การตอบสนองความเสี่ยง

เมื่อความเสี่ยงได้รับการบ่งชี้และประเมินความสำคัญแล้วผู้บริหารต้องประเมินวิธีการจัดการความเสี่ยงที่สามารถนำไปปฏิบัติได้และผลของการจัดการเหล่านั้น การพิจารณาทางเลือกในการดำเนินการจะต้องคำนึงถึงความเสี่ยงที่ยอมรับได้ และต้นทุนที่เกิดขึ้นเปรียบเทียบกับผลประโยชน์ที่จะได้รับเพื่อให้การบริหารความเสี่ยงมีประสิทธิผล ผู้บริหารอาจต้องเลือกวิธีการจัดการความเสี่ยงอย่างใดอย่างหนึ่ง หรือหลายวิธีรวมกัน เพื่อลดระดับโอกาสที่อาจเกิดขึ้นและผลกระทบของเหตุการณ์ให้อยู่ในช่วงที่หน่วยงานสามารถยอมรับได้ (Risk Tolerance) หลักการตอบสนองความเสี่ยงมี 4 ประการ คือ

6.1 การหลีกเลี่ยง (Terminate) เป็นวิธีการที่ง่ายที่สุดในการบริหารความเสี่ยง คือ การเลือกที่จะไม่รับความเสี่ยงไว้เลย อาจหยุดดำเนินการ หรือยกเลิกโครงการ /กิจกรรมที่ก่อให้เกิดความเสียหายได้ การหลีกเลี่ยงความเสี่ยงเมื่อพบว่าผลประโยชน์ที่จะได้รับนั้นไม่คุ้มกับสิ่งที่จะเกิดขึ้นจึงหลีกเลี่ยงที่จะเผชิญกับกิจกรรมความเสี่ยงนั้น หรือการหลีกเลี่ยงความเสี่ยงอาจเกิดขึ้นจากหน่วยงานเลือกที่จะหลีกเลี่ยงกิจกรรมความเสี่ยงนั้น โดยมิได้คิดทบทวนถึงผลที่จะได้รับ นำมาซึ่งการเสียโอกาสของหน่วยงานได้

6.2 การยอมรับ (Take) เป็นการยอมรับความเสี่ยง หรือความเสียหายที่อาจจะเกิดขึ้นไว้เองโดยไม่ทำอะไรและยอมรับในผลที่อาจตามมา เนื่องจากเห็นว่าโอกาสหรือความน่าจะเป็นที่จะเกิดความเสียหายอยู่ในวิสัยที่หน่วยงานยอมรับได้ หรือไม่คุ้มค่าสำหรับค่าใช้จ่ายในการสร้างระบบในการจัดการหรือป้องกันความเสี่ยง

6.3 การควบคุม (Treat) เป็นการปรับปรุงระบบการทำงาน หรือออกแบบวิธีการทำงานใหม่เพื่อหาทางป้องกันมิให้มีความเสียหายเกิดขึ้น เป็นการลดโอกาสหรือจำนวนครั้งของความเสียหายที่จะเกิด หากเราไม่สามารถป้องกันไม่ให้ความเสี่ยงเกิดขึ้นได้ ก็ควรขจัดให้หมดไป หรือลดความรุนแรงของความเสี่ยงลงโดยมีการจัดทำแผนหรือมาตรการควบคุมขึ้น อาจกำหนดเป็นแนวทางปฏิบัติไว้ล่วงหน้า ทั้งนี้วิธีควบคุมความสูญเสียมีสองวิธีหลัก คือ การป้องกันการเกิดความสูญเสีย และการควบคุมขนาดของความสูญเสียหลังเกิดความสูญเสียขึ้น การป้องกันการเกิดความสูญเสียเป็นวิธีการที่พยายามจะลดความถี่ของการเกิดความสูญเสีย โดยการหามาตรการหรือวิธีการใดๆ ในการป้องกันไม่ให้ความสูญเสียเกิดขึ้น

6.4 การถ่ายโอน (Transfer) การโอนย้ายหรือแบ่งความเสี่ยงไปให้ผู้อื่นช่วยรับผิดชอบ เช่น อุปกรณ์เครือข่ายเมื่อซื้อมาแล้วมีระยะประกันภัยเพียงหนึ่งปี เพื่อเป็นการรับมือในกรณีที่อุปกรณ์เครือข่ายไม่ทำงานหน่วยงานอาจเลือกซื้อประกัน หรือสัญญาการบำรุงรักษาหลังการขาย

7. ปัจจัยเสี่ยง

ปัจจัยที่จะเกิดความเสียหายกับระบบฐานข้อมูลสารสนเทศของกองสถานพยาบาลและการประกอบโรคศิลปะ ได้แก่

7.1 ปัจจัยภายนอก ได้แก่

7.1.1 ภัยธรรมชาติ และการเกิดสถานการณ์ความไม่สงบที่กระทบต่ออาคารสถานที่ตั้งของเครื่องประมวลผลหลัก หรือ เครื่องแม่ข่ายหลัก (Server) ของระบบฐานข้อมูล ได้แก่ ไฟไหม้ ภัยพิบัติ

7.1.2 การขโมยอุปกรณ์คอมพิวเตอร์แม่ข่ายที่เป็นส่วนของการจัดเก็บและรวบรวมข้อมูล

7.1.3 การชำรุดเสียหายของตัวเครื่องประมวลผลหลัก หรือแม่ข่ายหลัก (Server)

7.1.4 ระบบการสื่อสารของเครือข่ายคอมพิวเตอร์หลักเสียหายหรือขัดข้อง

7.1.5 ระบบกระแสไฟฟ้าขัดข้องหรือไฟฟ้าดับ

7.1.6 การถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูลจากบุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาต

7.2 ปัจจัยภายใน ได้แก่

7.2.1 ระบบฐานข้อมูลหลักเสียหาย หรือข้อมูลถูกทำลาย

7.2.2 การถูกไวรัสโจมตี (Virus) ทำลายข้อมูลสำคัญ และโปรแกรมปฏิบัติการต่างๆ จากผู้ใช้ภายในหน่วยงาน

7.2.3 เจ้าหน้าที่หรือบุคลากรของหน่วยงานขาดความรู้ความเข้าใจในการใช้เครื่องมือ อุปกรณ์คอมพิวเตอร์ทั้งด้านฮาร์ดแวร์ และซอฟท์แวร์ อันอาจทำให้ระบบเทคโนโลยีสารสนเทศ และการสื่อสารเสียหาย ใช้งานไม่ได้ หรือหยุดการทำงาน

8. การประเมินความเสียหาย

8.1 ความเสียหายที่เกิดผลเสียหายร้ายแรงที่สุด ซึ่งจะทำให้ต้องหยุดระบบประมวลผลทั้งระบบลงได้แก่ ภัยธรรมชาติ ตัวเครื่องประมวลผลหลักหรือแม่ข่ายเสียหาย (Server) และระบบฐานข้อมูลหลักถูกทำให้เสียหายจากไวรัส

8.2 ความเสียหายที่เกิดผลเสียหายและต้องหยุดระบบชั่วขณะ ได้แก่ การถูกเจาะเข้าระบบฐานข้อมูลระบบสื่อสารของเครือข่ายคอมพิวเตอร์ขัดข้อง และกระแสไฟฟ้าขัดข้อง

9. การติดตามและรายงานผล

กำหนดให้เจ้าหน้าที่ผู้รับผิดชอบรายงานผลการดำเนินการหรือการตรวจสอบให้ผู้กำกับดูแลทราบเป็นประจำทุกเดือน และให้รายงานการเกิดปัญหาและผลการแก้ไขให้ทราบในทันทีที่สามารถดำเนินการได้ในทุกกรณีตามที่ระบุ

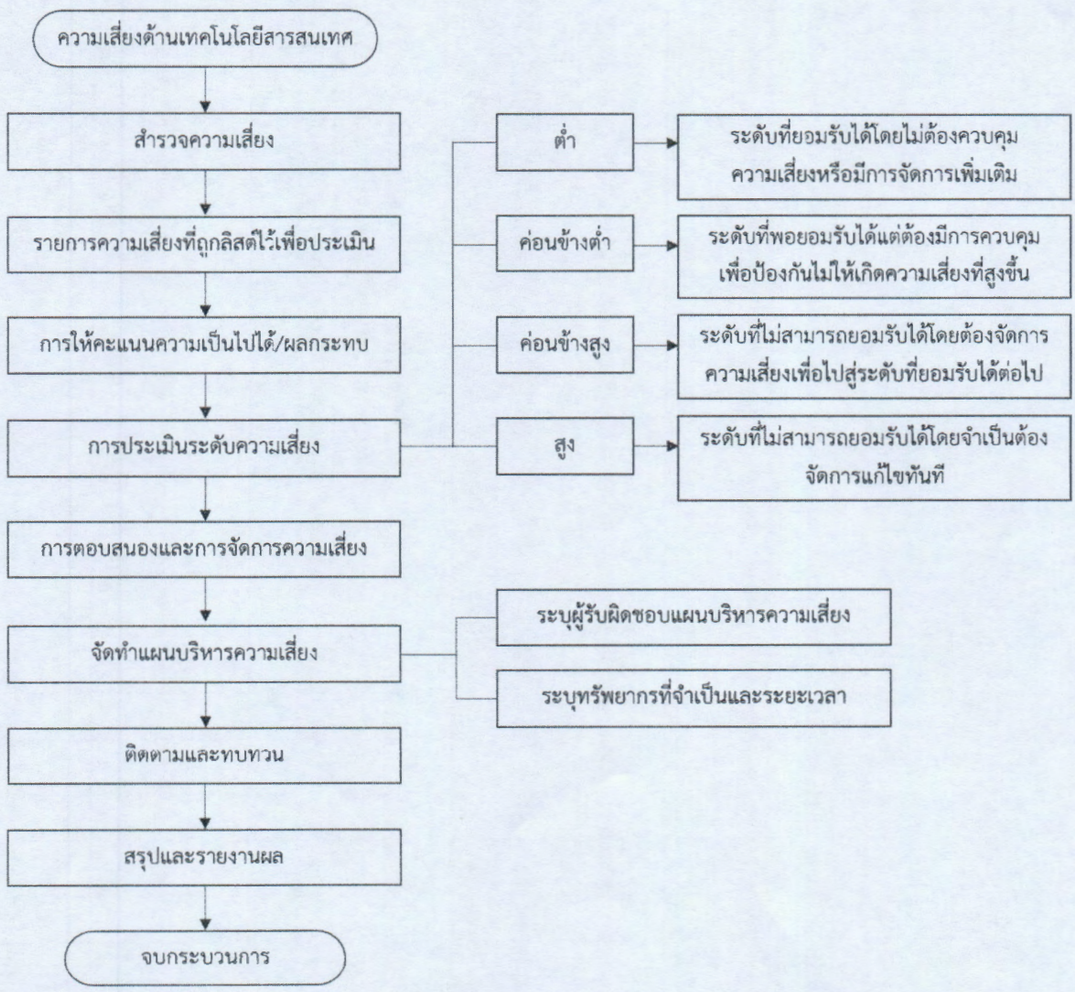
10. ระบบรักษาความปลอดภัยบนเครือข่าย

ระบบคอมพิวเตอร์และเครือข่ายของกองสถานพยาบาลและการประกอบโรคศิลปะได้รับการปรับปรุง และบำรุงรักษาเป็นประจำเพื่อให้การทำงานผ่านระบบคอมพิวเตอร์และเครือข่ายของหน่วยงาน เป็นไปอย่างรวดเร็วและมีประสิทธิภาพ โดยมีการติดตั้งระบบอยู่ภายในอาคารสำนักงานกองสถานพยาบาลและการประกอบโรคศิลปะซึ่งมีการปิดล็อคและกำหนดสิทธิ การเข้าถึงระบบ

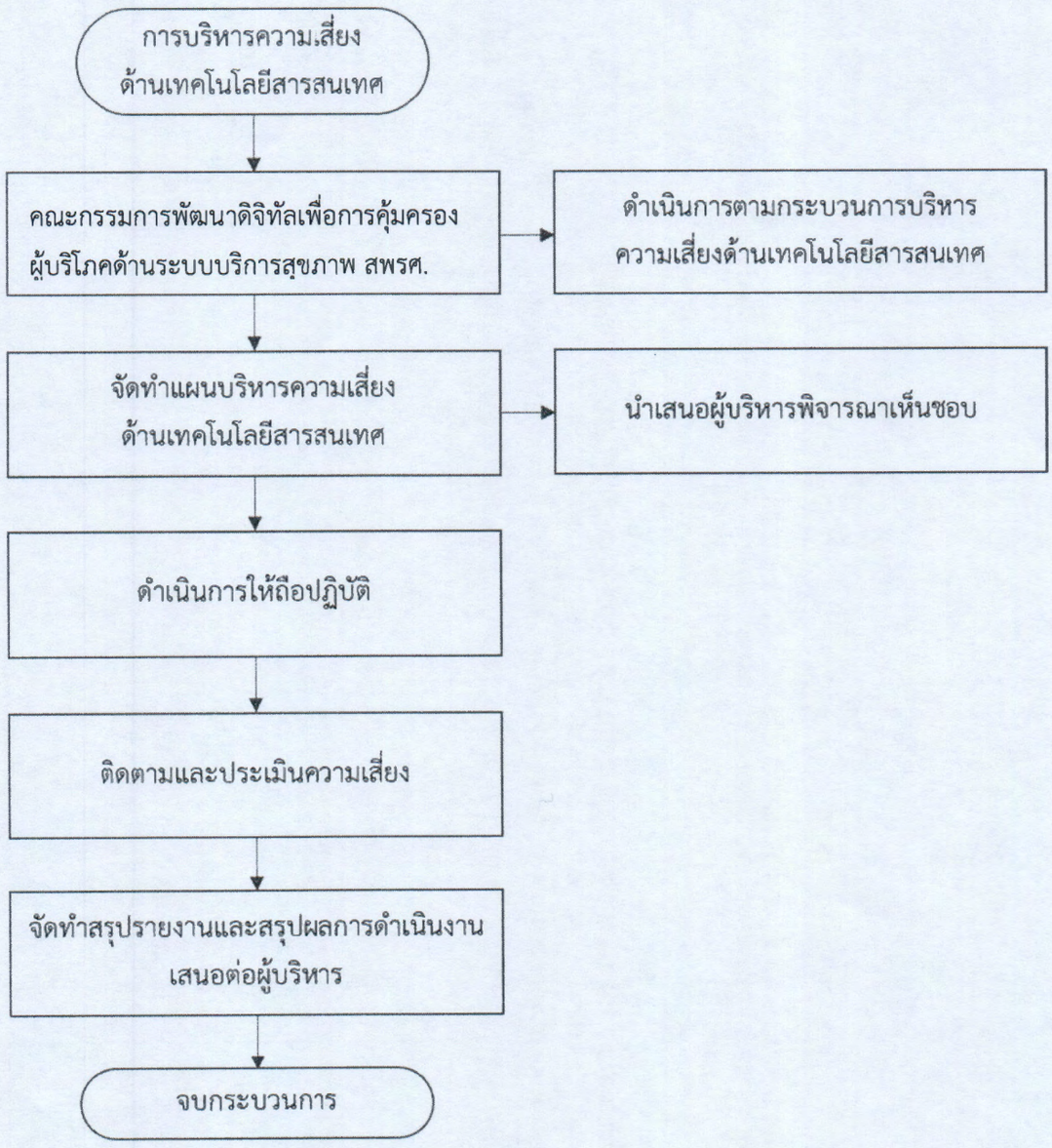
บทที่ 2
การวิเคราะห์การบริหารจัดการความเสี่ยง

กองสถานพยาบาลและการประกอบโรคศิลปะได้ตระหนักถึงความสำคัญของข้อมูลและการทำงานของระบบเทคโนโลยีสารสนเทศที่สนับสนุนการปฏิบัติงานของหน่วยงานที่อาจประสบกับความเสียหายจากปัจจัยเสี่ยงต่างๆ จึงได้จัดทำแผนบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ กองสถานพยาบาลและการประกอบโรคศิลปะ ประจำปีงบประมาณ พ.ศ.2566 ให้สอดคล้องกับนโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของกรมสนับสนุนบริการสุขภาพ โดยกระบวนการบริหารจัดการความเสี่ยงของหน่วยงานเริ่มต้นจากการรวบรวมข้อมูลที่เกี่ยวข้องกับกิจกรรม/ปัจจัยเสี่ยง หรือกระบวนงานที่มีผลต่อการดำเนินงานด้านเทคโนโลยีสารสนเทศ และการศึกษาข้อมูล ระดมความคิดเห็นร่วมกับผู้ปฏิบัติงานด้านกิจกรรมนั้น ๆ ดังตาราง การบริหารจัดการความเสี่ยง ที่ได้จัดทำการวิเคราะห์โดยแยกการวิเคราะห์ออกเป็นกิจกรรมต่าง ๆ ดังต่อไปนี้

1. แผนภูมิแนวทางและขั้นตอนการบริหารความเสี่ยง



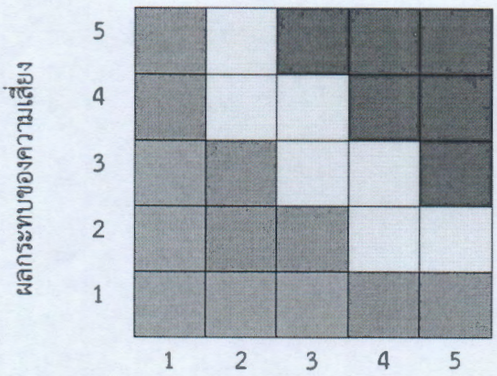
2. กระบวนการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศและการสื่อสาร



3. การวิเคราะห์ปัจจัยเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ

การระบุความเสี่ยง (Risk identification) เป็นการชี้ให้เห็นถึงความเสี่ยงด้านต่างๆ ที่หน่วยงานเผชิญอยู่ ผลสรุปการกำหนดประเด็นความเสี่ยงด้านเทคโนโลยีสารสนเทศ รวมทั้งการประเมินระดับความเป็นไปได้ และผลกระทบ มีดังนี้

แผนผังประเมินความเสี่ยง



โอกาสที่จะเกิดความเสี่ยง

	สีแดง	หมายถึง ระดับความเสี่ยงสูง ค่าระหว่าง 15 - 25
	สีเหลือง	หมายถึง ระดับความเสี่ยงค่อนข้างสูง ค่าระหว่าง 8 - 14
	สีเขียว	หมายถึง ระดับความเสี่ยงค่อนข้างต่ำ ค่าระหว่าง 4 - 7
	สีฟ้า	หมายถึง ระดับความเสี่ยงต่ำ ค่าระหว่าง 1 - 3

ประเด็นความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ลำดับ	ความเสี่ยง	ความน่าจะเป็นที่จะเกิด	ผลกระทบ	คะแนน
1	ผู้ใช้งานขาดความตระหนักในการใช้งานระบบเทคโนโลยีสารสนเทศให้ปลอดภัย	4	4	16
2	การถูกนำสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศของหน่วยงานที่ไม่ได้รับอนุญาตไปใช้ในทางที่ผิดกฎหมาย	3	5	15
3	ความเสี่ยงจากระบบคอมพิวเตอร์หลักและอุปกรณ์เสียหาย	3	5	15
4	การถูกบุกรุกจากผู้ไม่ประสงค์ดีหรือไวรัสคอมพิวเตอร์	3	5	15
5	ระบบกระแสไฟฟ้าขัดข้อง	4	3	12
6	การนำอุปกรณ์เคลื่อนที่ (Smart Phone, Tablet, PC) ส่วนบุคคลเข้ามาเชื่อมต่อกับระบบเครือข่าย	5	2	10
7	การสูญหายของข้อมูล	2	5	10

ลำดับ	ความเสี่ยง	ความน่าจะเป็นที่จะเกิด	ผลกระทบ	คะแนน
8	การติดตั้งและใช้งานซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ถูกต้องตามกฎหมาย	3	4	12
9	การเชื่อมต่อระบบเครือข่ายอินเตอร์เน็ตขัดข้อง	2	4	8
10	ข้อมูลรั่วไหลจากการเปลี่ยนผู้รับผิดชอบหรือผู้ใช้ระบบ	2	4	8
11	เกิดความเสียหายจากภัยธรรมชาติ และอุบัติเหตุ เช่น เกิดไฟไหม้ น้ำท่วม แผ่นดินไหว อาคารถล่ม ฯลฯ	1	5	5
12	การจลาจล/สถานการณ์ความสงบเรียบร้อยในบ้านเมือง	1	4	4
13	แมลงหรือสัตว์กัดแทะคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ สายไฟฟ้าหรือสายสัญญาณ	1	4	4
14	การถูกโจมตีระบบจากเครือข่ายภายใน	1	4	4
15	การถูกโจรกรรมอุปกรณ์คอมพิวเตอร์ และอุปกรณ์ต่อพ่วง	1	5	5

4. ผลการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง
ความเสี่ยงด้านบุคลากร (Human Risk)	ความเสี่ยงจากการที่ผู้ใช้งานขาดความตระหนักในการใช้งานเทคโนโลยีสารสนเทศให้ปลอดภัย	1. เจ้าหน้าที่หรือบุคลากรของหน่วยงานขาดความรู้ความเข้าใจในเครื่องมืออุปกรณ์คอมพิวเตอร์ทั้งด้าน Hardware และ Software อย่างปลอดภัย 2. การใช้งานโปรแกรมผิดกฎหมาย เช่น การดาวน์โหลดโปรแกรมที่ไม่มีลิขสิทธิ์	1. ระบบเสียหาย และการทำงานหยุดชะงัก 2. สูญเสีย Bandwidth ในเครือข่าย ทำให้ต้องจัดสรรเพิ่มทำให้สิ้นเปลืองทรัพยากรด้านงบประมาณในการจัดสรร Bandwidth 3. อาจถูกร้องเรียนหรือฟ้องร้องจากบุคคลภายนอก	สูง 4x4 = 16	1. อบรม สร้างความรู้ความเข้าใจการใช้ งานระบบเทคโนโลยีสารสนเทศที่ถูกวิธี 2. กำหนด แนวทางปฏิบัติ/มาตรการในการใช้งานอุปกรณ์ พร้อมทั้งรักษาความปลอดภัยของระบบให้มีความปลอดภัยและตรวจสอบการทางานของระบบอย่างสม่ำเสมอ และเปิดสิทธิเข้าใช้งานเท่าที่จำเป็น 3. กำกับดูแลการปฏิบัติตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศอย่างเคร่งครัด	การควบคุม (Treat)
ความเสี่ยงด้านบุคลากร (Human Risk)	ความเสี่ยงจากการถูกนำสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศของหน่วยงานที่ไม่ได้รับอนุญาตไปใช้ในทางที่ผิดกฎหมาย	สิทธิการใช้งานระบบเทคโนโลยีสารสนเทศ และสิทธิการเข้าถึงข้อมูลของผู้ใช้งานไม่เป็นปัจจุบัน เนื่องจากผู้ใช้งานมีการลาออก โอน ย้าย สิ้นสุดการจ้างตลอดเวลา	1. หน่วยงาน/ผู้บริหาร/ผู้ใช้งาน อาจได้รับความเสียหายจากการถูกนำสิทธิ์การเข้าถึงระบบไปใช้ในทางผิดกฎหมาย รวมทั้งต้องรับโทษทางกฎหมาย 2. ข้อมูลที่เป็นความลับถูกเผยแพร่หรือนำไปใช้จะนำมาซึ่งการขาดความเชื่อถือของหน่วยงานฯ และอาจเกิดข้อร้องเรียนซึ่งทำให้เกิดข้อพิพาททางกฎหมาย	สูง 3x5 = 15	หน่วยงานต้องดำเนินการตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยฯ ในกรณีผู้ใช้งานของหน่วยงานลาออก โอน ย้าย หรือสิ้นสุดการจ้าง ให้งานเจ้าหน้าที่/กลุ่มงานแจ้งผู้ดูแลระบบให้ทราบทันที เพื่อปรับปรุงฐานข้อมูลผู้มีสิทธิ์เข้าใช้งานระบบเทคโนโลยีสารสนเทศให้เป็นปัจจุบัน	การควบคุม (Treat)

ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง
ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร (Hardware and Data Communication Risk)	ความเสี่ยงจากระบบคอมพิวเตอร์หลักและอุปกรณ์เสียหาย ทำให้ไม่สามารถใช้ระบบงานได้เต็มประสิทธิภาพ	การทำงานของอุปกรณ์คอมพิวเตอร์ที่เป็นส่วนสำคัญของระบบเกิดการขัดข้อง จากการใช้งานและอายุการใช้งาน	1. ระบบงานไม่สามารถดำเนินต่อไปได้ตามปกติ 2. ข้อมูลที่ถูกบันทึกไว้ในอุปกรณ์เกิดความเสียหาย	สูง 3x5 = 15	1. ตรวจสอบอุปกรณ์คอมพิวเตอร์ที่อยู่ในความรับผิดชอบขององค์กร/กลุ่มงาน/บุคคล อย่างสม่ำเสมอ 2. สำรองข้อมูลสำคัญไว้ที่ระบบขององค์กร หรือ External Hard disk ส่วนบุคคล 3. แจ้งเจ้าหน้าที่ IT กรมฯ	การถ่ายโอน (Transfer)
ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร (Hardware and Data Communication Risk)	ความเสี่ยงจากการบุกรุกจากผู้ไม่ประสงค์ดี/ไวรัสคอมพิวเตอร์ เช่น Hacker Virus Malware เป็นต้น	การถูกโจมตีจากภายนอกผ่านเครือข่ายอินเทอร์เน็ต	1. อาจทำให้เครื่องแม่ข่าย หรือเครื่องลูกข่ายติดไวรัส และแพร่กระจายสู่เครื่องอื่นๆ ทั้งหมดในเครือข่าย 2. ระบบ/ข้อมูลอาจถูกแก้ไขหรือเปลี่ยนแปลง เช่น ข้อมูลบนเว็บไซต์ของสำนักงาน 3. อาจถูกโจรกรรมข้อมูลที่เป็นความลับ	สูง 3x5 = 15	1. ตรวจสอบการติดตั้งโปรแกรมป้องกันไวรัส และทำการอัพเดทอย่างสม่ำเสมอ 2. อัพเดทระบบปฏิบัติการให้เป็นเวอร์ชันปัจจุบันและสม่ำเสมอ 3. จัดเจ้าหน้าที่รับผิดชอบตรวจสอบและเฝ้าระวัง	การควบคุม (Treat)
ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)	ความเสี่ยงจากการเกิดไฟฟ้าขัดข้องทำไม่สามารถใช้งานระบบเทคโนโลยีสารสนเทศได้ อุปกรณ์คอมพิวเตอร์ถูก Shutdown อย่างเหมาะสม อาจทำให้อุปกรณ์คอมพิวเตอร์ในระบบเกิดความเสียหาย	1. ระบบไฟฟ้าขัดข้อง 2. ไม่มีระบบสำรองไฟในสำนักงาน กรณีที่เกิดไฟฟ้าดับ 3. ไม่มีระบบแจ้งเตือนไฟฟ้าขัดข้อง 4. UPS ไม่สามารถทำงานได้อย่างเต็มประสิทธิภาพเนื่องจากหมดอายุการใช้งาน	1.ระบบไม่สามารถทำงานได้ 2.ข้อมูล/อุปกรณ์เสียหาย 3.ระบบปฏิบัติโปรแกรม ข้อมูลเสียหาย ต้องมีการ Recovery หรือติดตั้งใหม่	ค่อนข้างสูง 4x3 = 12	1.วางแผนการจัดหาและติดตั้ง UPS 2.ตรวจสอบการทำงานของเครื่องสำรองไฟฟ้า (UPS) อย่างสม่ำเสมอ	การควบคุม (Treat)

ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง
ความเสี่ยงด้านบุคลากร (Human Risk)	ความเสี่ยงจากการนำอุปกรณ์เคลื่อนที่ (Smart phone, Tablet, PC) ส่วนตัวเข้ามาเชื่อมต่อกับระบบเครือข่ายของหน่วยงานโดยขาดความระมัดระวังในการใช้งาน	1. ระบบเทคโนโลยีสารสนเทศไม่มีการรักษาความปลอดภัยที่ถูกต้องและเพียงพอ 2. การไม่ตระหนักต่อความเสี่ยงที่อาจเกิดขึ้นในการใช้งานระบบของผู้ใช้	อาจเกิดช่องโหว่ของระบบรักษาความปลอดภัยของหน่วยงาน และอาจมีการโจมตี ทำให้ระบบ ไม่สามารถทำงานได้	ค่อนข้างสูง 4x3 = 12	1.อบรมเผยแพร่ประชาสัมพันธ์ข้อมูลเพื่อสร้างความตระหนักในเรื่องความมั่นคงปลอดภัยสารสนเทศให้กับบุคลากรของหน่วยงาน 2.กำกับดูแลการปฏิบัติตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศอย่างเคร่งครัด	การควบคุม (Treat)
ความเสี่ยงด้านระบบข้อมูล (Database Risk)	ความเสี่ยงต่อการสูญหายของข้อมูล ในขั้นเล็กน้อยหรือมากจนไม่สามารถดำเนินการกู้คืนข้อมูลได้หากระบบเกิดเหตุขัดข้อง	ระบบสารสนเทศที่ไม่มีการสำรองข้อมูล หรือ ไม่มีการสำรองข้อมูลอย่างต่อเนื่อง	ระบบเกิดขัดข้อง/ข้อมูลเสียหาย ไม่สามารถกู้คืนข้อมูลได้	ค่อนข้างสูง 2x5 = 10	1.หน่วยงานต้องมีการสำรองข้อมูล (Backup) อย่างสม่ำเสมอ 2.ผู้ใช้งานต้องมีการสำรองข้อมูล (Backup) ไว้ที่ระบบขององค์กร หรือ External Harddisk ส่วนบุคคลอย่างสม่ำเสมอ	การควบคุม (Treat)
ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk)	การติดตั้งและใช้งานซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ถูกต้องตามกฎหมาย	ผู้ใช้ติดตั้งและใช้งานซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ถูกต้องตามกฎหมาย	หน่วยงานอาจถูกฟ้องร้องเรียกค่าเสียหายจากผู้เป็นเจ้าของลิขสิทธิ์นั้นๆ	ค่อนข้างสูง 3x4 = 12	1. การจัดหาซอฟต์แวร์ที่ถูกกฎหมายมาใช้งานตามความจำเป็น 2. สร้างความตระหนักในการใช้งานซอฟต์แวร์มีลิขสิทธิ์และถูกต้องตามกฎหมาย	ยอมรับ (Accept)
ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร (Hardware and Data Communication Risk)	ความเสี่ยงจากการเชื่อมต่อระบบเครือข่ายอินเตอร์เน็ตขัดข้อง	ไม่สามารถเชื่อมต่อเครือข่ายอินเตอร์เน็ตภายนอกสำนักงานได้	ผู้ใช้ไม่สามารถเชื่อมต่อเครือข่ายอินเตอร์เน็ตภายนอกสำนักงานได้ ทำให้ขาดการติดต่อสื่อสาร และรับ-ส่งข้อมูล	ค่อนข้างสูง 2x4 = 8	1. แจ้งเจ้าหน้าที่ IT กรมฯ เพื่อตรวจสอบระบบเครือข่าย เพื่อแก้ไขปัญหาที่เกิดขึ้น 2. ตรวจสอบการทำงานของอุปกรณ์เครือข่าย อย่างสม่ำเสมอ หากพบปัญหาให้ดำเนินการแก้ไขอย่างรวดเร็วหรือแจ้งเจ้าหน้าที่ IT กรมฯ เพื่อซ่อมแซมหรือจัดหาใหม่	ยอมรับ (Accept)

ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง
ความเสี่ยงด้านระบบข้อมูล (Database Risk)	ความเสี่ยงจากข้อมูลรั่วไหลเนื่องจากการเปลี่ยนผู้รับผิดชอบหรือผู้ใช้ระบบ	ข้อมูลที่สำคัญมีการรั่วไหลจากการซ่อมแซมเครื่องที่เสีย เช่น Hard Disk หรืออุปกรณ์สำรองข้อมูลประเภทต่างๆ	1. ข้อมูลที่อยู่ในชั้นความลับรั่วไหลส่งผลต่อความน่าเชื่อถือ 2. ข้อมูลที่รั่วไหลอาจทำให้ฝ่ายใดฝ่ายหนึ่งนำไปใช้ประโยชน์ได้โดยไม่ถูกต้องตามกฎหมาย	ค่อนข้างสูง 2x4 = 8	มีการบริหารจัดการอุปกรณ์เก็บข้อมูล เช่น Hard Disk อุปกรณ์สำรองข้อมูลประเภทต่างๆ ให้แน่ใจว่าข้อมูลได้ถูกลบทิ้งอย่างถาวร หรือได้ทำลายอุปกรณ์นั้นๆทิ้งก่อนการจำหน่าย	ยอมรับ (Accept)
ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)	ความเสี่ยงจากการเกิดไฟไหม้ น้ำท่วม แผ่นดินไหว อาคารถล่มจนไม่สามารถเคลื่อนย้ายเครื่องคอมพิวเตอร์แลอุปกรณ์ต่างๆได้ส่งผลให้ระบบไม่สามารถทำงานได้	ไฟฟ้าลัดวงจร การวางเพลิง ภัยธรรมชาติ อุบัติเหตุฉุกเฉิน	1. สูญเสียงบประมาณในการจัดหาระบบทดแทน 2. ไม่สามารถใช้งานระบบระหว่างที่มีการจัดหาระบบทดแทนได้	ค่อนข้างต่ำ 1x5 = 5	1. จัดทำแผนป้องกันและแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติต่อระบบเทคโนโลยีสารสนเทศ (IT Contingency Plan) 2.ตรวจสอบระบบตรวจจับควัน	การควบคุม (Treat)
ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)	ความเสี่ยงจากสถานการณ์ความสงบเรียบร้อยในบ้านเมือง	- การชุมนุมประท้วง - การจลาจล/ก่อการร้าย - การสูญหายและถูกทำลายของอุปกรณ์ และข้อมูลที่เป็นส่วนสำคัญขององค์กร	การเกิดสถานการณ์ความรุนแรงหรือความไม่สงบเรียบร้อย จนทำให้บุคลากรไม่สามารถปฏิบัติงานได้ตามปกติ	ค่อนข้างต่ำ 1x4 = 4	1. จัดทำแผนป้องกันและแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติต่อระบบเทคโนโลยีสารสนเทศ (IT Contingency Plan) 2. สำรองข้อมูลระบบและฐานข้อมูลเก็บไว้ในสถานที่อื่นอีกหนึ่งชุด	การควบคุม (Treat)
ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)	ความเสี่ยงจากแมลงหรือสัตว์กัดแทะคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ สายไฟฟ้าหรือสายสัญญาณ	เสี่ยงต่อการอุปกรณ์/ระบบไม่สามารถใช้งานได้ปกติ	1. เสียงบประมาณในการซ่อมแซมหรือจัดหาทดแทน 2. ไม่สามารถให้บริการระบบได้อย่างต่อเนื่อง	ค่อนข้างต่ำ 1x4 = 4	1. ไม่ปล่อยให้มีสายไฟฟ้าหรือสายสัญญาณไม่มีท่อห่อหุ้ม 2. ไม่นำอาหาร/เครื่องดื่มมาทานหรือเก็บไว้ในบริเวณที่มีความเสี่ยง	การควบคุม (Treat)

ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง
ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร (Hardware and Data Communication Risk)	ความเสี่ยงจากการถูกโจมตีระบบจากเครือข่ายภายใน	เสี่ยงต่อการถูกโจมตีจากโปรแกรมต่างๆโดยเฉพาะประเภทTrojan ที่มีการติดตั้งที่เครื่องลูกข่ายโดยผู้ใช้งานภายในทั้งที่ไม่ได้ตั้งใจและตั้งใจ	อาจส่งผลให้ระบบเครือข่ายไม่สามารถใช้ได้อย่างปกติ	ค่อนข้างต่ำ 1x4 = 4	กำหนดแนวปฏิบัติการจำกัดและควบคุมการใช้งานโปรแกรมอรรถประโยชน์	การควบคุม (Treat)
ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)	ความเสี่ยงจากการถูกโจรกรรมอุปกรณ์คอมพิวเตอร์และอุปกรณ์ต่อพ่วง	เสี่ยงต่อการสูญหายของอุปกรณ์และข้อมูลที่มีความสำคัญเสี่ยงต่อการสูญหายของอุปกรณ์ และข้อมูลที่มีความสำคัญ	1. เสียงบประมาณในการจัดหาอุปกรณ์ทดแทน 2. เสียเวลาในการกู้ระบบ	ค่อนข้างต่ำ 1x4 = 4	1. ล็อคประตูห้องทำงานทุกครั้ง เมื่อเลิกงาน หรือเจ้าหน้าที่ไม่อยู่ 2. จัดเก็บเครื่องคอมพิวเตอร์ที่สามารถเคลื่อนย้ายได้สะดวก เช่น Notebook ไว้ในที่มิดชิดเมื่อไม่ได้ใช้งาน	การควบคุม (Treat)

แผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

กองสถานพยาบาลและการประกอบโรคศิลปะ
กรมสนับสนุนบริการสุขภาพ

ผู้รับผิดชอบหลัก
หน่วยงาน กองสถานพยาบาลและการประกอบโรคศิลปะ
ระยะเวลา ปีงบประมาณ 2566

วัตถุประสงค์ : เพื่อให้การดำเนินงานด้านการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศของกองสถานพยาบาลและการประกอบโรคศิลปะ
บรรลุเป้าประสงค์ของการบริหารความเสี่ยง

ประเภทความเสี่ยง/กิจกรรม	แผนปฏิบัติ	ระยะเวลา	ไตรมาสที่ 1	ไตรมาสที่ 2	ไตรมาสที่ 3	ไตรมาสที่ 4	ผู้รับผิดชอบ
ความเสี่ยงจากการที่ผู้ใช้งานขาดความตระหนักในการใช้งานเทคโนโลยีสารสนเทศให้ปลอดภัย	1. อบรม สร้างความรู้ความเข้าใจการใช้งานระบบเทคโนโลยีสารสนเทศที่ถูกวิธี	1 ครั้ง/ปี			/		-กลุ่มงานแผนงานฯ -คณะกรรมการพัฒนาดิจิทัลเพื่อการคุ้มครองผู้บริโภคด้านบริการสุขภาพฯ
	2. กำหนด แนวปฏิบัติในการใช้งานอุปกรณ์พร้อมทั้งรักษาความปลอดภัยของระบบให้มีความปลอดภัยและตรวจสอบการทำงานของระบบอย่างสม่ำเสมอ และเปิดสิทธิเข้าใช้งานเท่าที่จำเป็น	1 ครั้ง/ปี	/				
	3. กำกับดูแลการปฏิบัติตามแนวปฏิบัติ ด้านการรักษาความมั่นคงปลอดภัยสารสนเทศอย่างเคร่งครัด	1 ครั้ง/เดือน	/	/	/	/	-นายนัธทวัฒน์ อมรไทยสุนทร
ความเสี่ยงจากการถูกนำสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศของหน่วยงานที่ไม่ได้รับอนุญาตไปใช้ในทางที่ผิดกฎหมาย	หน่วยงานต้องดำเนินการตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยฯ ในกรณีผู้ใช้งานของหน่วยงานลาออก โอน ย้าย หรือสิ้นสุดการจ้าง ให้งานเจ้าหน้าที่/กลุ่มงานแจ้งผู้ดูแลระบบให้ทราบทันที เพื่อปรับปรุงฐานข้อมูล	ทุกครั้งที่มีการเปลี่ยนแปลงผู้ใช้งาน	/	/	/	/	-นายนัธทวัฒน์ อมรไทยสุนทร

ประเภทความเสี่ยง/กิจกรรม	แผนปฏิบัติ	ระยะเวลา	ไตรมาสที่ 1	ไตรมาสที่ 2	ไตรมาสที่ 3	ไตรมาสที่ 4	ผู้รับผิดชอบ
	ผู้มีสิทธิ์เข้าใช้งานระบบเทคโนโลยีสารสนเทศให้เป็นปัจจุบัน						
ความเสี่ยงจากระบบคอมพิวเตอร์หลักและอุปกรณ์เสียหาย ทำให้ไม่สามารถใช้ระบบงานได้เต็มประสิทธิภาพ	1. ตรวจสอบอุปกรณ์คอมพิวเตอร์ที่อยู่ในความรับผิดชอบขององค์กร/กลุ่มงาน/บุคคล อย่างสม่ำเสมอ	ทุกสัปดาห์	/	/	/	/	-นายนัธทวัฒน์ อมรไทยสุนทร
	2. สำรองข้อมูลสำคัญไว้ที่ระบบขององค์กร หรือ External Hard disk ส่วนบุคคล	ทุกสัปดาห์	/	/	/	/	-จนท.ทุกคน
	3. แจ้งเจ้าหน้าที่ IT กรมฯ	ทุกครั้ง	/	/	/	/	-นายนัธทวัฒน์ อมรไทยสุนทร
ความเสี่ยงจากการบุกรุกจากผู้ไม่ประสงค์ดี/ไวรัสคอมพิวเตอร์ เช่น Hacker Virus Malware เป็นต้น	1. ตรวจสอบการติดตั้งโปรแกรมป้องกันไวรัสและทำการอัพเดทอย่างสม่ำเสมอ	2 ครั้ง/ปี	/			/	-นายนัธทวัฒน์ อมรไทยสุนทร
	2. อัพเดทระบบปฏิบัติการให้เป็นเวอร์ชั่นปัจจุบันและสม่ำเสมอ	2 ครั้ง/ปี	/			/	
	3. จัดเจ้าหน้าที่รับผิดชอบตรวจสอบ และเฝ้าระวัง	1 ครั้ง/ปี	/				
ความเสี่ยงจากการเกิดไฟฟ้าขัดข้องทำไม่สามารถใช้งานระบบเทคโนโลยีสารสนเทศได้ อุปกรณ์คอมพิวเตอร์ถูก Shutdown อย่างเหมาะสม อาจทำให้อุปกรณ์คอมพิวเตอร์ในระบบเกิดความเสียหาย	1.วางแผนการจัดหาและติดตั้ง UPS	1 ครั้ง/ปี	/				-นายนัธทวัฒน์ อมรไทยสุนทร
	2.ตรวจสอบการทำงานของเครื่องสำรองไฟฟ้า (UPS) อย่างสม่ำเสมอ	1 ครั้ง/ปี	/				

ประเภทความเสี่ยง/กิจกรรม	แผนปฏิบัติ	ระยะเวลา	ไตรมาสที่ 1	ไตรมาสที่ 2	ไตรมาสที่ 3	ไตรมาสที่ 4	ผู้รับผิดชอบ
ความเสี่ยงจากการนำอุปกรณ์เคลื่อนที่ (Smart phone, Tablet, PC) ส่วนตัวเข้ามาเชื่อมต่อกับระบบเครือข่ายของหน่วยงานโดยขาดความระมัดระวังในการใช้งาน	1.อบรม เผยแพร่ประชาสัมพันธ์ข้อมูลเพื่อสร้างความตระหนักในเรื่องความมั่นคงปลอดภัยสารสนเทศให้กับบุคลากรของหน่วยงาน	1 ครั้ง/ปี			/		-กลุ่มงานแผนงานฯ
	2.กำกับดูแลการปฏิบัติตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศอย่างเคร่งครัด	2 ครั้ง/ปี	/			/	
ความเสี่ยงต่อการสูญหายของข้อมูล ในขั้นเล็กน้อยหรือมากจนไม่สามารถดำเนินการกู้คืนข้อมูลได้หากระบบเกิดเหตุขัดข้อง	1. หน่วยงานต้องมีการสำรองข้อมูล (Backup) อย่างสม่ำเสมอ	ทุกเดือน	/	/	/	/	-นายนัธทวัฒน์ อมรไทยสุนทร
	2. ผู้ใช้งานต้องมีการสำรองข้อมูล (Backup) ไว้ที่ระบบ Cloud ขององค์กร หรือ External Hard disk ส่วนบุคคลอย่างสม่ำเสมอ	ทุกวัน	/	/	/	/	-จนท.ทุกคน
การติดตั้งและใช้งานซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ถูกต้องตามกฎหมาย	1. การจัดหาซอฟต์แวร์ที่ถูกกฎหมายมาใช้งานตามความจำเป็น	1 ครั้ง/ปี	/				-สพรศ.
	2. สร้างความตระหนักในการใช้งานซอฟต์แวร์มีลิขสิทธิ์และถูกต้องตามกฎหมาย	ทุกเดือน	/	/	/	/	-กลุ่มแผนงานฯ

บทที่ 3
สรุปและข้อเสนอแนะ

การจัดการความเสี่ยง (Risk Management คือ กระบวนการในการระบุ วิเคราะห์ ประเมินดูแลตรวจสอบและควบคุมความเสี่ยงที่สัมพันธ์กับกิจกรรม หน้าที่ และกระบวนการทำงาน เพื่อให้หน่วยงาน ลดความเสียหายจากความเสี่ยงมากที่สุด อันเนื่องมาจากภัยที่หน่วยงานต้องเผชิญในช่วงเวลาใดเวลาหนึ่งเมื่อเทคโนโลยีสารสนเทศก้าวเข้ามามีบทบาทสำคัญในฐานะกลไกอันทรงพลังในการขับเคลื่อน การดำเนินงานของหน่วยงาน ทุกกิจกรรมที่เกิดขึ้นภายในหน่วยงานจึงล้วนมีความเกี่ยวข้องกับเทคโนโลยีสารสนเทศแทบทั้งสิ้น ในแต่ละวันข้อมูลมหาศาลถูกส่งผ่านเครือข่ายเทคโนโลยีสารสนเทศเพื่ออำนวยความสะดวกให้แก่ผู้ปฏิบัติงานของทุกหน่วยงานภายในหน่วยงาน ในปัจจุบัน "ข้อมูล" ถือว่าเป็นทรัพย์สินอันทรงคุณค่ามหาศาลต่างตกอยู่ในสภาวะเสี่ยงต่อการถูกล่วงละเมิด ถูกทำให้เสียหายและถูกนำไปใช้ในทางที่ผิด ทั้งจากบุคคลภายในและภายนอกหน่วยงานโดยเจตนาหรือไม่เจตนาก็ตาม ดังนั้น หนทางที่ดีที่สุดในการแก้ปัญหานี้จึงควรเริ่มตั้งแต่การบริหารจัดการหน่วยงานให้ได้มาตรฐานด้านความปลอดภัย ซึ่งก็คือการจัดการความเสี่ยงในหน่วยงาน นั่นเอง

1. การวิเคราะห์ปัจจัยเสี่ยงด้านระบบเทคโนโลยีสารสนเทศการระบุความเสี่ยง (Risk identification) เป็นการชี้ให้เห็นถึงความเสี่ยงด้านต่างๆ ที่หน่วยงานเผชิญอยู่จากการกำหนดแนวทางปฏิบัติเพื่อควบคุมความเสี่ยงที่มีระดับสูง โดยได้ข้อสรุปตามตารางแสดงผลการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ

2. สรุป แผนการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศและการสื่อสาร ได้ดำเนินการจัดทำโดยมีวัตถุประสงค์ ดังนี้

2.1 เตรียมความพร้อมและรองรับสถานการณ์ฉุกเฉิน ที่อาจจะเกิดขึ้นกับระบบฐานข้อมูลสารสนเทศ

2.2 เป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศให้มีเสถียรภาพ และมีความพร้อมสำหรับการใช้งาน

2.3 ให้การปฏิบัติงานเป็นไปอย่างมีระบบและต่อเนื่อง และสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงทีกรณีเกิดสถานการณ์ความไม่แน่นอนและภัยพิบัติ

3. ข้อเสนอแนะ

3.1 การควบคุมนโยบายและกระบวนการปฏิบัติงานถือเป็นสำคัญ เพื่อให้มั่นใจว่าได้มีการจัดการความเสี่ยง ดังนั้นควรมีการกำหนดบุคลากรภายในหน่วยงานเพื่อรับผิดชอบการควบคุมนั้นโดยบุคลากรแต่ละคนที่ได้รับมอบหมายในการควบคุมควรมีความรับผิดชอบ ดังนี้

3.3.1 พิจารณาประสิทธิผลของการจัดการความเสี่ยงที่ได้ดำเนินการอยู่ในปัจจุบัน

3.3.2 พิจารณาการปฏิบัติเพิ่มเติมที่จำเป็น เพื่อเพิ่มประสิทธิผลของการจัดการความเสี่ยงนั้น

3.3.3 กำกับกิจกรรมลดความเสี่ยงให้แล้วเสร็จตามกำหนดวันตามแผนที่วางไว้

3.2 การติดตามการบริหารความเสี่ยงเพื่อให้มั่นใจว่าการจัดการความเสี่ยงมีคุณภาพและมีความเหมาะสม ดังนั้นจึงควรมีการติดตามการบริหารความเสี่ยงอย่างต่อเนื่องและดำเนินการอย่างสม่ำเสมอเพื่อตอบสนองต่อการเปลี่ยนแปลงอย่างทันท่วงที และถือเป็นส่วนหนึ่งของการปฏิบัติงาน รวมถึงการติดตามการดำเนินการภายหลังจากเกิดเหตุการณ์ขึ้นเพื่อวิเคราะห์ถึงปัญหาที่เกิดขึ้นและการแก้ไขอย่างถูกต้องได้อย่างมีประสิทธิภาพ

ผู้เสนอแผน.....

(นางพรพีศ กาลนาน)

หัวหน้ากลุ่มแผนงานและประเมินผล

วันที่ ๑๗ ก.พ. ๖๕

ผู้อนุมัติ.....

(นางนลินา ตันตินิรามัย)

ผู้อำนวยการกองสถานพยาบาลและการประกอบโรคศิลปะ

๑๗ ก.พ. ๖๕