



แผนการจัดการบริหารความเสี่ยง
โรงพยาบาลน้ำเกลี้ยง

คำนำ

แผนบริการความเสี่ยงด้านระบบสารสนเทศของโรงพยาบาลน้ำเกลี้ยง ปี ๒๕๖๙-๒๕๗๐ จัดทำขึ้นเพื่อเป็นกรอบแนวทางในการดำเนินงานด้านการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศและการสื่อสารในการระบุความเสี่ยงวิเคราะห์ความเสี่ยง และการกำหนดแนวทางหรือมาตรการควบคุมเพื่อป้องกันหรือลดความเสี่ยง เพื่อให้บรรลุตามเป้าประสงค์ขององค์กร เนื่องจากความเสี่ยงอาจนำไปสู่ผลเสียหรือความสูญเสียทั้งทางตรงและทางอ้อม องค์กรจึงต้องเข้าใจประเภทของความเสี่ยงที่เผชิญอยู่เพื่อที่จะได้เลือกวิธีการที่เหมาะสมในการบริหารความเสี่ยงเหล่านั้นได้อยู่ระดับที่องค์กรสามารถรองรับได้ และทำให้องค์กรบรรลุวัตถุประสงค์ได้อย่างมีประสิทธิภาพมากขึ้น ศูนย์เทคโนโลยีสารสนเทศ หวังเป็นอย่างยิ่งว่าแผนบริการความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศของโรงพยาบาลน้ำเกลี้ยง ฉบับนี้ จะช่วยให้ผู้รับผิดชอบใช้เป็นแนวทางในการลดความเสียหายต่างๆ ที่อาจเกิดขึ้นและส่งผลต่อกระบวนการบริหารงานด้านเทคโนโลยีสารสนเทศของโรงพยาบาลน้ำเกลี้ยง ต่อไป

ศูนย์เทคโนโลยีสารสนเทศ
โรงพยาบาลน้ำเกลี้ยง
๒๕๖๙

บทที่ ๑

บทนำ

๑. หลักการและเหตุผล

การบริหารความเสี่ยงเป็นเครื่องมือทางกลยุทธ์ที่สำคัญตามหลักการกำกับดูแลกิจการที่ดีโดยจะช่วยให้การบริหารงานและการตัดสินใจในการวางแผน การกำหนดกลยุทธ์การติดตามควบคุม และวัดผล การปฏิบัติงาน ตลอดจนการใช้ทรัพยากรต่าง ๆ อย่างเหมาะสมและมีประสิทธิภาพมากขึ้น ลดการสูญเสียและโอกาสที่ทำให้เกิดความเสียหายแก่โรงพยาบาลน้ำเกลี้ยง โดยเฉพาะอย่างยิ่งในด้านเทคโนโลยีสารสนเทศที่เข้ามามีบทบาทสำคัญในการดำเนินงานของหน่วยงานภายในโรงพยาบาลน้ำเกลี้ยง ทั้งการจัดเก็บข้อมูล การใช้งานอุปกรณ์คอมพิวเตอร์การติดต่อสื่อสารผ่านระบบเครือข่าย และวิธีการ ปฏิบัติงานระบบเทคโนโลยีสารสนเทศภายใต้สภาวะการดำเนินงานของทุกหน่วยงานล้วนแต่มีความเสี่ยง ซึ่งก็คือความไม่แน่นอนที่จะส่งผลกระทบต่อการทำงานหรือเป้าหมายของโรงพยาบาลน้ำเกลี้ยง จึงจำเป็นต้องมีการจัดการความเสี่ยงเหล่านั้นอย่างเป็นระบบ โดยการระบุความเสี่ยงว่ามีปัจจัยเสี่ยงใดบ้าง ที่กระทบต่อการดำเนินงานหรือเป้าหมาย วิเคราะห์ความเสี่ยงจากโอกาส และผลกระทบที่เกิดขึ้น จัดลำดับความสำคัญของปัจจัยเสี่ยง แล้วกำหนดแนวทางในการจัดการความเสี่ยง โดยต้องคำนึงถึงความคุ้มค่าในการจัดการความเสี่ยงอย่างเหมาะสม

๒. วัตถุประสงค์ของการจัดทำแผนบริหารความเสี่ยง

๑. เพื่อเตรียมความพร้อมรองรับสถานการณ์ฉุกเฉิน ที่อาจเกิดขึ้นกับระบบฐานข้อมูลและระบบเทคโนโลยีสารสนเทศของโรงพยาบาลน้ำเกลี้ยง
๒. เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของระบบฐานข้อมูลและระบบเทคโนโลยีสารสนเทศให้มีเสถียรภาพ และพร้อมใช้งาน
๓. เพื่อให้การปฏิบัติงานเป็นไปอย่างมีระบบและต่อเนื่อง สามารถแก้ไขสถานการณ์ได้ทัน่วงทีกรณีเกิดสถานการณ์ความไม่แน่นอนและภัยพิบัติ
๔. เพื่อให้การจัดการภายในกลุ่มงานสารสนเทศทางการแพทย์ข้อมูลมีประสิทธิภาพและมีความยืดหยุ่นในการปรับตัวให้ทันต่อการเปลี่ยนแปลงของเทคโนโลยีสารสนเทศสมัยใหม่ รวมทั้งลดโอกาสที่จะก่อให้เกิดความเสียหายกับระบบเทคโนโลยีสารสนเทศ
๕. เพื่อลดโอกาสและผลกระทบของความเสี่ยงที่จะเกิดขึ้นกับองค์การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ โรงพยาบาลน้ำเกลี้ยง
๖. เพื่อเป็นแนวทางการดำเนินงาน กำกับดูแล ตรวจสอบการบริหารจัดการและการ เผยแพร่ความรู้ ความเข้าใจเกี่ยวกับการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

๓. สภาพแวดล้อมด้านเทคโนโลยีสารสนเทศ

ระบบฐานข้อมูลสารสนเทศ (Database & Software) เช่นเว็บไซต์โรงพยาบาลน้ำเกลี้ยง

ระบบฐานข้อมูลสำหรับการบริการภายใน ได้แก่ ฐานข้อมูล Him.pro ฐานข้อมูลสารบัญออนไลน์ (E-office) ฐานข้อมูลคลังยา (INVS)

ระบบให้บริการเครือข่าย ได้แก่ ระบบเครือข่ายภายใน Lan ระบบเครือข่าย Internet ระบบเครือข่ายไร้สาย (WIFI)

อุปกรณ์คอมพิวเตอร์ (Hardware) เช่น เครื่องคอมพิวเตอร์แม่ข่ายระบบฐานข้อมูล (Database Server Him.pro , INVS) เครื่องคอมพิวเตอร์แม่ข่ายที่ใช้จัดเก็บและสำรองข้อมูล (Storage Server) เครื่องคอมพิวเตอร์ชนิดพกพา (Note Book) เครื่องสแกนเนอร์ (Scanner) เครื่องพิมพ์เลเซอร์ (Laser Printer) เครื่องพิมพ์แบบพ่นหมึก (Ink-Jet Printer) อุปกรณ์สำรองไฟฟ้าสำหรับคอมพิวเตอร์ (UPS) อุปกรณ์กระจายสัญญาณเครือข่าย (Switching HUB) อุปกรณ์กระจายสัญญาณเครือข่ายชนิดไร้สาย (Wireless Access point) เป็นต้น

๔. กระบวนการบริหารความเสี่ยง

เป็นกระบวนการที่ใช้ในการระบุ วิเคราะห์ประเมิน จัดระดับความเสี่ยง ที่มีผลกระทบต่อการบรรลุวัตถุประสงค์ของกระบวนการทำงานของหน่วยงานหรือขององค์กร รวมทั้งการบริหาร/จัดการความเสี่ยง การกำหนดแนวทางการดำเนินงานหรือมาตรการควบคุมหรือป้องกันหรือลดความเสี่ยง ซึ่งมีขั้นตอนการดำเนินการหลักเกณฑ์ในการวิเคราะห์อย่างเหมาะสม โดยครอบคลุม ๕ ขั้นตอน ดังนี้

๑. การระบุความเสี่ยง
๒. การวิเคราะห์ความเสี่ยง
๓. กำหนดมาตรการ
๔. การติดตามรายงานประเมินผล
๕. ทบทวนระบุกรอบเวลา

๔.๑ การระบุความเสี่ยงหรือปัจจัยเสี่ยง

เป็นกระบวนการที่ผู้บริหารและผู้ปฏิบัติงานร่วมกันระบุความเสี่ยงและปัจจัยเสี่ยงที่เกี่ยวข้องโครงการ/กิจกรรม เพื่อให้ทราบถึงเหตุการณ์ที่เป็นความเสี่ยง ที่อาจมีผลกระทบต่อการบรรลุผลสำเร็จตามวัตถุประสงค์ซึ่งต้องคำนึงถึงสภาพแวดล้อมทั้งภายนอกและภายในองค์กร วิธีการในการระบุความเสี่ยงมีหลายวิธี เช่น

- ๑) การระดมสมองเพื่อให้ได้ความเสี่ยงที่หลากหลาย
- ๒) การใช้ Checklist
- ๓) การวิเคราะห์สถานการณ์จากการตั้งคำถาม “What-if”
- ๔) การวิเคราะห์ขั้นตอนการปฏิบัติงานในแต่ละขั้นตอน
- ๕) การรวบรวมปัญหาที่เกิดขึ้นมาแล้ว ในขั้นตอนนี้ควรมีการเก็บข้อมูลความสูญเสียที่เกิดขึ้นในรูปของสถิติของการเกิดความสูญเสียและความรุนแรงของความสูญเสีย รวมทั้งข้อมูลการดำเนินการใด ๆ เพื่อลดความสูญเสียที่เกิดขึ้นในอดีตทั้งที่ ประสบผลสำเร็จ และปัญหาอุปสรรคซึ่งจะเป็นประโยชน์ในการดำเนินการต่อไป

๔.๒ การวิเคราะห์และประเมินความเสี่ยง

การประเมินความเสี่ยงเป็นกระบวนการที่ประกอบด้วยการวิเคราะห์การประเมิน และการจัดระดับความเสี่ยง ประกอบด้วย ๔ ขั้นตอน คือ

๔.๒.๑ การกำหนดเกณฑ์การประเมินมาตรฐาน

เป็นเกณฑ์ที่จะใช้ประเมินความเสี่ยง ได้แก่ โอกาสที่จะเกิดความเสี่ยง (Likelihood) ระดับความรุนแรงของผลกระทบ (Impact) และระดับของความเสี่ยง (Degree of Risk) คณะกรรมการบริหาร ความเสี่ยงต้องกำหนดเกณฑ์ของหน่วยงานขึ้น ซึ่งอาจกำหนดได้ทั้ง เกณฑ์เชิงปริมาณและเชิงคุณภาพ การกำหนดเกณฑ์ของโอกาสที่เกิิดความเสี่ยงอาจกำหนดเป็นเกณฑ์ ๕ ระดับ (สูงมาก สูงปานกลาง น้อย และ น้อยมาก) ส่วนระดับของความเสี่ยงอาจกำหนดเป็นเกณฑ์ ๕ ระดับ (สูงมาก สูงปานกลาง น้อย และน้อยมาก)

๔.๒.๒ การประเมินโอกาสและผลกระทบของความเสี่ยง

เป็นการดูปัญหาความเสี่ยงในแง่ของโอกาสการเกิดเหตุ (incident) หรือเหตุการณ์ (event) ว่ามีมากน้อยเพียงไรและผลที่ติดตามมาว่ามีความรุนแรงหรือเสียหายมากน้อยเพียงใด เกณฑ์การประเมิน เป็นการกำหนดเกณฑ์ที่จะใช้ในการประเมินความเสี่ยง ได้แก่ ระดับ โอกาสที่จะเกิดความเสี่ยง ระดับความรุนแรงของผลกระทบ และระดับความเสี่ยง ซึ่งใช้เกณฑ์ดังนี้

ขั้นตอนที่ ๑ ระดับโอกาสในการเกิดเหตุการณ์ต่างๆ (Likelihood) กำหนดเกณฑ์ไว้ ๕ ระดับ ดังนี้

ระดับโอกาสในการเกิดเหตุการณ์ต่างๆ (Likelihood) เชิงปริมาณ		
ระดับ	โอกาสที่จะเกิดขึ้น	คำอธิบาย
๕	รุนแรงสูง (High Risk)	๑ เดือน / ครั้ง หรือมากกว่า
๔	รุนแรงมาก (High Risk)	๑ - ๖ เดือน / ครั้ง แต่ไม่เกิน ๕ ครั้ง
๓	รุนแรงปานกลาง (Moderate Risk)	๑ ปี / ครั้ง
๒	รุนแรงน้อย (Low Risk)	๒ - ๓ ปี / ครั้ง
๑	เกือบพลาด (Near Miss)	๕ ปี / ครั้ง

ระดับโอกาสในการเกิดเหตุการณ์ต่างๆ (Likelihood) เชิงคุณภาพ		
ระดับ	โอกาสที่จะเกิดขึ้น	คำอธิบาย
๕	รุนแรงสูง (High Risk)	มีโอกาสในการเกิดแทบทุกครั้ง
๔	รุนแรงมาก (High Risk)	มีโอกาสในการเกิดค่อนข้างสูงหรือบ่อยๆ
๓	รุนแรงปานกลาง (Moderate Risk)	มีโอกาสบางครั้ง
๒	รุนแรงน้อย (Low Risk)	มีโอกาสเกิดแต่นานๆ ครั้ง
๑	เกือบพลาด (Near Miss)	มีโอกาสเกิดในกรณียกเว้น

ขั้นตอนที่ ๒ ระดับความรุนแรงของผลกระทบของความเสี่ยง (Impact) กำหนดเกณฑ์ไว้ ๕ ระดับ ดังนี้

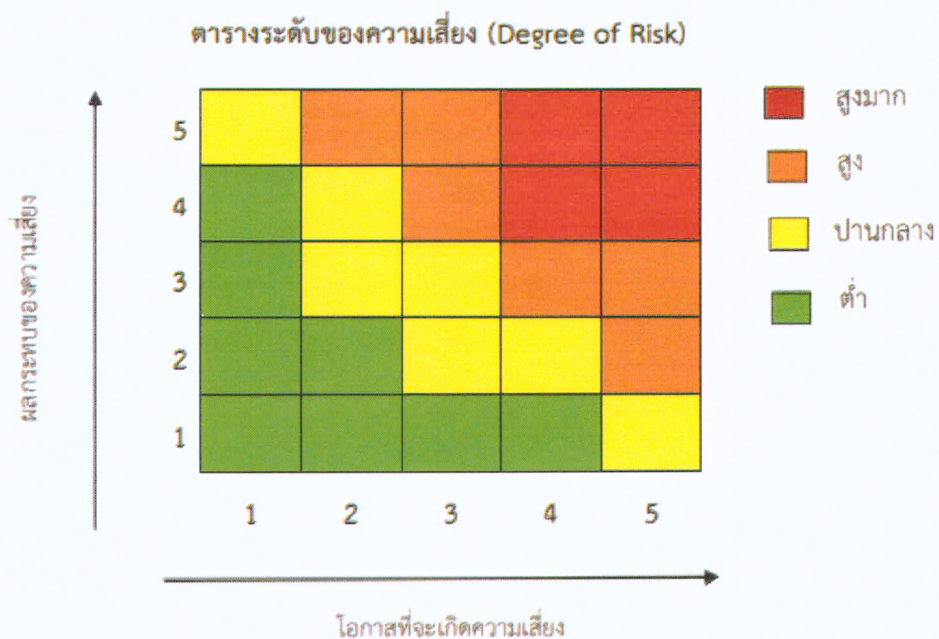
ระดับโอกาสในการเกิดเหตุการณ์ต่างๆ (Likelihood) เจริงปริมาณ		
ระดับ	โอกาสที่จะเกิดขึ้น	คำอธิบาย
๕	รุนแรงสูง (High Risk)	มูลค่าความเสียหาย มากกว่า ๑๐,๐๐๑ บาทขึ้นไป
๔	รุนแรงมาก (High Risk)	มูลค่าความเสียหาย ๕,๐๐๑ - ๑๐,๐๐๐ บาท
๓	รุนแรงปานกลาง (Moderate Risk)	มูลค่าความเสียหาย ๓,๐๐๑ - ๕,๐๐๐ บาท
๒	รุนแรงน้อย (Low Risk)	มูลค่าความเสียหาย ๑,๐๐๑ - ๓,๐๐๐ บาท
๑	เกือบพลาด (Near Miss)	มูลค่าความเสียหาย น้อยกว่า ๑,๐๐๐ บาท

ระดับโอกาสในการเกิดเหตุการณ์ต่างๆ (Likelihood) เจริงปริมาณ		
ระดับ	โอกาสที่จะเกิดขึ้น	คำอธิบาย
๕	รุนแรงสูง (High Risk)	เกิดเหตุการณ์ผิดพลาดแล้วแล้วเกิดการฟ้องร้อง แก้ไขไม่ได้
๔	รุนแรงมาก (High Risk)	เกิดเหตุการณ์ผิดพลาดแล้ว เสียชื่อเสียง/ความเชื่อถือ/เสียลูกค้า แก้ไขไม่ได้ อาจถูกฟ้องร้อง สูญเสียเงิน
๓	รุนแรงปานกลาง (Moderate Risk)	เกิดเหตุการณ์ผิดพลาดแล้ว มีผลกระทบต่อคน
๒	รุนแรงน้อย (Low Risk)	เกิดเหตุการณ์แล้ว แต่ยังไม่มืผลกระทบ
๑	เกือบพลาด (Near Miss)	เสี่ยง/ยังไม่เกิดเหตุการณ์/มีโอกาศเกิด

ระดับโอกาสในการเกิดเหตุการณ์ต่างๆ (Likelihood) เจริงคุณภาพ		
ระดับ	โอกาสที่จะเกิดขึ้น	คำอธิบาย
๕	รุนแรงสูง (High Risk)	เกิดเหตุการณ์ผิดพลาดแล้วแล้วเกิดการฟ้องร้อง แก้ไขไม่ได้
๔	รุนแรงมาก (High Risk)	เกิดเหตุการณ์ผิดพลาดแล้ว เสียชื่อเสียง/ความเชื่อถือ/เสียลูกค้า แก้ไขไม่ได้ อาจถูกฟ้องร้อง สูญเสียเงิน
๓	รุนแรงปานกลาง (Moderate Risk)	เกิดเหตุการณ์ผิดพลาดแล้ว มีผลกระทบต่อคน
๒	รุนแรงน้อย (Low Risk)	เกิดเหตุการณ์แล้ว แต่ยังไม่มืผลกระทบ
๑	เกือบพลาด (Near Miss)	เสี่ยง/ยังไม่เกิดเหตุการณ์/มีโอกาศเกิด

ระดับความรุนแรงของผลกระทบของความเสี่ยงเทคโนโลยีสารสนเทศ		
ระดับ	โอกาสที่จะเกิดขึ้น	คำอธิบาย
๕	รุนแรงสูง (High Risk)	เกิดความสูญเสียต่อระบบ IT ที่สำคัญทั้งหมดและเกิดความเสียหายอย่างมากต่อความปลอดภัยของข้อมูลต่างๆ
๔	รุนแรงมาก (High Risk)	เกิดปัญหากับระบบ IT ที่สำคัญ และระบบความปลอดภัย ซึ่ง ส่งผลต่อความถูกต้องของข้อมูลบางส่วน
๓	รุนแรงปานกลาง (Moderate Risk)	ระบบมีปัญหาและมีความสูญเสียไม่มาก
๒	รุนแรงน้อย (Low Risk)	เกิดเหตุการณ์เล็กน้อยแก้ไขได้
๑	เกือบพลาด (Near Miss)	เกิดเหตุการณ์ที่ไม่มีความสำคัญ

๔.๒.๓ การวิเคราะห์ความเสี่ยง เป็นการดูความสัมพันธ์ระหว่างโอกาสที่จะเกิดความเสี่ยง และผลกระทบของความเสี่ยงต่อ โรงพยาบาลน้ำเกลือ ว่าจะก่อให้เกิดระดับความเสี่ยงในระดับใด โดยใช้ตารางระดับความเสี่ยงสูงสุด ที่จะต้องบริหารจัดการก่อน ดังรูปด้านล่าง



๔.๒.๔ การจัดลำดับความเสี่ยง

เป็นการจัดลำดับความรุนแรงของความเสี่ยงที่มีผลต่อโรงพยาบาลน้ำเกลี้ยง เพื่อ พิจารณา กำหนดกิจกรรมการควบคุมในแต่ละสาเหตุของความเสี่ยงที่สำคัญให้เหมาะสมโดยพิจารณาจากระดับความเสี่ยงที่ประเมินได้ เลือกความเสี่ยงที่มีระดับสูงมาก หรือสูงมาจัดทำแผนการบริหารความเสี่ยงเป็นลำดับแรก

๔.๓ การกำหนดมาตรการจัดการความเสี่ยงอย่างรัดกุม

มีการวางแผนโดยกำหนดมาตรการเพื่อควบคุมผลกระทบของความเสี่ยงเพื่อให้สามารถบรรลุ เป้าหมาย หรือใกล้เคียงกับเป้าหมายที่กำหนดไว้ในการวางแผน จะต้องมีการกำหนดกลยุทธ์ในการควบคุม ผลกระทบของความเสี่ยงที่อาจเกิดขึ้น เพื่อที่จะลดและตรวจหาความเสี่ยงที่ได้ประเมินเอาไว้โดยให้มีการแต่งตั้งเจ้าหน้าที่ผู้รับผิดชอบเป็นผู้ดูแลรักษาความมั่นคงปลอดภัยของระบบ และป้องกัน/แก้ไข/ควบคุม ความเสี่ยงไม่ให้มีผลกระทบต่อระบบที่วางไว้โดยสามารถดำเนินการตามแผนได้การควบคุมอาจแบ่งได้เป็น ๔ ประเภท คือ

๔.๓.๑ ควบคุมเพื่อป้องกัน (Preventive Control)

เป็นวิธีการควบคุมเพื่อป้องกันไม่ให้เกิดความเสี่ยงและข้อผิดพลาดตั้งแต่แรก เช่น การอนุมัติ การจัดโครงสร้างองค์กร การควบคุม การเข้าถึงเอกสาร เป็นต้น

๔.๓.๒ การควบคุมเพื่อให้อัตราพบ (Detective Control)

เป็นวิธีการควบคุมเพื่อค้นหาข้อผิดพลาดที่เกิดขึ้นแล้ว เช่น การวิเคราะห์การตรวจนับ การรายงาน ข้อบกพร่อง เป็นต้น

๔.๓.๓ การควบคุมโดยการชี้แนะ (Direction Control) เป็นวิธีควบคุมที่ส่งเสริมหรือกระตุ้นให้เกิดความสำเร็จตามวัตถุประสงค์

๔.๓.๔ การควบคุมเพื่อการแก้ไข (Corrective Control) เป็นวิธีการควบคุมเพื่อแก้ไขข้อผิดพลาด ที่เกิดขึ้นให้ถูกต้อง หรือหาวิธีแก้ไขไม่ให้เกิด ข้อผิดพลาดนั้นซ้ำอีกในอนาคตหลังจากประเมินความเสี่ยงแล้ว จะต้องวิเคราะห์การควบคุมที่มีอยู่ว่าได้มี การจัดการควบคุมเพื่อลดความเสี่ยงดังกล่าวหรือไม่ โดยนำผลการ จัดระดับความเสี่ยงในระดับสูงมากและสูง มาประเมินมาตรการควบคุมเป็นอันดับแรก อาจใช้ขั้นตอนดังนี้

๑) นำปัจจัยเสี่ยงที่อยู่ในระดับสูงมาก หรือสูงมากกำหนดวิธีควบคุมที่ควรจะมีเพื่อป้องกัน ความเสี่ยง หรือปัจจัยเสี่ยงเหล่านั้น

๒) พิจารณา หรือประเมินว่าในปัจจุบันความเสี่ยงหรือปัจจัยเสี่ยงนั้นมีการควบคุมอยู่แล้ว หรือไม่

๓) ถ้ามีการควบคุมแล้ว ให้ประเมินต่อไปว่าการควบคุมนั้นได้ผลตามความต้องการหรือไม่

๔.๔ การติดตาม รายงานและประเมินผลการดำเนินการตามมาตรการจัดการความเสี่ยงที่ได้ กำหนดไว้

การติดตามผลการดำเนินงาน การนำกลยุทธ์มาตรการ หรือแนวทางมาใช้ปฏิบัติเพื่อลดโอกาสที่เกิด ความเสี่ยง หรือลดความเสียหายของผลที่อาจเกิดขึ้นจากความเสี่ยง ในโครงการ/กิจกรรมที่ยังไม่มีกิจกรรม ควบคุมความเสี่ยง หรือมีแต่ไม่เพียงพอ และนำมาวางแผนจัดการความเสี่ยง ทางเลือกในการบริหารความเสี่ยง มีหลายวิธีซึ่งสามารถปรับเปลี่ยนหรือนำมาผสมผสานให้เหมาะสมกับสถานการณ์อาจเป็นการยอมรับ ความเสี่ยง การลด/การควบคุมความเสี่ยง การกระจายความเสี่ยง หรือการหลีกเลี่ยงความเสี่ยงเมื่อองค์กร ทราบ ความเสี่ยงที่ยังเหลืออยู่จากการประเมินความเสี่ยง และการประเมินการควบคุมแล้วให้พิจารณาความ เป็นไป ได้และค่าใช้จ่ายแต่ละทางเลือก เพื่อตัดสินใจเลือกมาตรการลดความเสี่ยงที่เหมาะสมโดยพิจารณาจาก

๔.๔.๑ พิจารณาวายอมรับความเสี่ยง หรือจะกำหนดกิจกรรมควบคุมเพื่อลดความเสี่ยงให้อยู่ในระดับ ที่ยอมรับได้

๔.๔.๒ เปรียบเทียบค่าใช้จ่ายหรือต้นทุนในการจัดการให้มีมาตรการควบคุมกับผลประโยชน์ที่จะได้รับจากมาตรการดังกล่าวว่าคุ้มค่าหรือไม่

๔.๔.๓ กรณีเลือกกำหนดกิจกรรมควบคุมเพื่อลดความเสี่ยงให้กำหนดวิธีควบคุมในแผนบริหารความเสี่ยง

๔.๔.๔ ในรอบปีต่อไป ให้พิจารณาผลการติดต่อการบริหารความเสี่ยงในงวดก่อนที่ดำเนินการ มาบริหารความเสี่ยงตามกระบวนการเหล่านั้น หากพบว่ายังมีความเสี่ยงที่มีนัยสำคัญซึ่งอาจมีผลต่อการบรรลุวัตถุประสงค์และเป้าหมายตามแผนปฏิบัติงานขององค์กรให้นำมาระบุการควบคุมในแผนบริหารความเสี่ยงด้วยการรายงานผลการวิเคราะห์ประเมินและบริหารจัดการความเสี่ยง ว่ามีความเสี่ยงที่ยังเหลืออยู่หรือไม่ ถ้าไม่มีเหลืออยู่ มีอยู่ในระดับความเสี่ยงสูงมากเพียงใด และมีวิธีการจัดการความเสี่ยงนั้นอย่างไรเสนอต่อผู้บริหารเพื่อทราบและสั่งการ

๔.๕ การทบทวนการบริหารความเสี่ยงโดยระบุรอบเวลาในการทบทวนอย่างชัดเจน

เป็นการติดตามภายหลังจากได้ดำเนินการตามแผนการบริหารความเสี่ยง ว่ามีความเสี่ยงแล้วเพื่อให้มั่นใจว่าแผนการบริหารความเสี่ยงนั้นมีประสิทธิภาพ ทั้งนี้เพื่อประเมินคุณภาพและความเหมาะสมของวิธีการจัดการความเสี่ยงที่ใช้และเป็นการตรวจสอบความคืบหน้าของมาตรการควบคุม โดยอาจติดตามผลเป็น รายครั้งตามรอบระยะเวลา หรือการติดตามผลในระหว่างการปฏิบัติงาน

๕. ความเสี่ยงด้านเทคโนโลยีสารสนเทศ

โรงพยาบาลน้ำเกลี้ยงได้กำหนดประเภทความเสี่ยงด้านเทคโนโลยีสารสนเทศ ออกได้เป็น ๕ ประเภท ดังนี้

ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)

หมายถึง ความเสี่ยงที่เกิดขึ้นและส่งผลกระทบโดยตรงต่อระบบคอมพิวเตอร์ และห้อง คอมพิวเตอร์ ศูนย์แม่ข่ายกลาง เช่น ไฟไหม้กระแสไฟฟ้าขัดข้อง รวมถึงการไม่มีระบบรักษาความปลอดภัย ห้องปฏิบัติการ ระบบเครือข่ายและคอมพิวเตอร์เครื่องคอมพิวเตอร์แม่ข่าย และระบบสื่อสารที่มีประสิทธิภาพ เพียงพอ

ความเสี่ยงด้านบุคลากร (Human Risk)

หมายถึง ความเสี่ยงที่เกิดจากบุคลากรที่เกี่ยวข้องกับการดำเนินงานด้านเทคโนโลยี สารสนเทศ ทั้งในด้านการวางแผน การตรวจสอบการทำงาน การมอบหมายหน้าที่และสิทธิ์ของบุคลากร และ คณะทำงานที่มีส่วนเกี่ยวข้องกับการดำเนินการทุกฝ่ายอย่างละเอียด เพื่อให้บุคลากรมีความรู้ความเข้าใจ ในการใช้งาน การดูแลรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งบุคลากร ภายนอกที่เกี่ยวข้องทั้งทางตรงและทางอ้อม ซึ่งล้วนแต่เป็นความเสี่ยงทั้งสิ้น

ความเสี่ยงด้านระบบคอมพิวเตอร์และระบบเครือข่าย (Computer and Network Risk)

หมายถึง ความเสี่ยงที่เกิดจากความผิดพลาดของอุปกรณ์การเคลื่อนย้ายตัวเครื่องอุปกรณ์ การติดตั้งอุปกรณ์ในพื้นที่ไม่เหมาะสม การถูกภัยคุกคามจากไวรัสคอมพิวเตอร์ Malware, Trojan, Adware เป็นต้น ทั้งที่เป็นการโจมตีจากภายใน และมาจากภายนอกโดยผ่านทางเครือข่าย (Networks) หรือจาก คอมพิวเตอร์ โดยตรง เช่น จาก USB Flash Drive หรือ USB External Hard Disk Drive เป็นต้น

ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk)

หมายถึง ความเสี่ยงที่เกิดจากระบบการทำงานของโปรแกรมต่าง ๆ เช่น การใช้โปรแกรม ที่ไม่มีการอัปเดตให้ทันสมัย เพื่อลดช่องโหว่ที่อาจเกิดจาก Bug ของซอฟต์แวร์นั้น ๆ หรือการถูกผู้ไม่หวังดี (Hacker)

เข้ามาทำลายระบบ หรือการใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ซึ่งกรมฝนหลวงและการบินเกษตร อาจถูกฟ้องร้องให้ต้องชำระค่าละเมิดลิขสิทธิ์เป็นต้น

ความเสี่ยงด้านระบบฐานข้อมูล (Database Risk)

หมายถึง ความเสี่ยงที่เกิดจากระบบฐานข้อมูลต่าง ๆ ในระบบสารสนเทศ อันอาจจะก่อให้เกิดความเสียหาย เนื่องจากข้อมูลถูกทำลาย ความเสี่ยงจากผู้นุกรกข้อมูล เพื่อการโจรกรรมข้อมูลที่สำคัญ การลักลอบเข้ามาแก้ไขเปลี่ยนแปลงข้อมูล ทำให้เกิดความเสียหาย ขาดความน่าเชื่อถือและสร้างความเสื่อมเสียแก่โรงพยาบาลน้ำเกลี้ยง ความเสี่ยงเหล่านี้ทำให้มีความจำเป็นที่จะต้องมีการบริหารจัดการ ความเสี่ยงด้านข้อมูล ดังนั้น การรักษาความปลอดภัยของข้อมูลจึงเป็นเรื่องสำคัญ เนื่องจากข้อมูลสารสนเทศ เป็นปัจจัยสำคัญสำหรับผู้บริหาร ผู้มีส่วนได้ส่วนเสียโดยตรง รวมถึงประชาชนทั่วไป ดังนั้น การรักษาความปลอดภัยของระบบข้อมูลและคอมพิวเตอร์จากภัยต่างๆ ทั้งภัยจากคน ภัยจากธรรมชาติหรือเหตุการณ์ใดๆ จึงมีความสำคัญและจำเป็นที่จะต้องมีการป้องกัน เพื่อให้เกิดความมั่นคงต่อระบบข้อมูลสารสนเทศ

๖. การตอบสนองความเสี่ยง

เมื่อความเสี่ยงได้รับการบ่งชี้และประเมินความสำคัญแล้วผู้บริหารต้องประเมินวิธีการจัดการ ความเสี่ยงที่สามารถนำไปปฏิบัติได้และผลของการจัดการเหล่านั้น การพิจารณาทางเลือกในการดำเนินการ จะต้องคำนึงถึงความเสี่ยงที่ยอมรับได้และต้นทุนที่เกิดขึ้นเปรียบเทียบกับผลประโยชน์ที่จะได้รับเพื่อให้ การบริหารความเสี่ยงมีประสิทธิภาพ ผู้บริหารอาจต้องเลือกวิธีการจัดการความเสี่ยงอย่างใดอย่างหนึ่ง หรือ หลายวิธีรวมกัน เพื่อลดระดับโอกาสที่อาจเกิดขึ้นและผลกระทบของเหตุการณ์ให้อยู่ในช่วงที่องค์กรสามารถ ยอมรับได้ (Risk Tolerance) หลักการตอบสนองความเสี่ยงมี ๔ ประการ คือ

การหลีกเลี่ยง (Terminate) เป็นวิธีการที่ง่ายที่สุดในการบริหารความเสี่ยง คือ การเลือกที่จะไม่รับความเสี่ยงไว้เลย อาจหยุดดำเนินการ หรือยกเลิกโครงการ/กิจกรรมที่ก่อให้เกิดความเสียหายได้การหลีกเลี่ยงความเสี่ยงเมื่อพบว่าผลประโยชน์ที่จะได้รับนั้นไม่คุ้มกับสิ่งที่เกิดขึ้นจึงหลีกเลี่ยงที่จะเผชิญกับกิจกรรม ความเสี่ยงนั้น หรือการหลีกเลี่ยงความเสี่ยงอาจเกิดขึ้นจากหน่วยงานเลือกที่จะหลีกเลี่ยงกิจกรรมความเสี่ยงนั้น โดยมิได้คิดทบทวนถึงผลที่จะได้รับ นำมาซึ่งการเสียโอกาสของหน่วยงานได้

การยอมรับ (Take) เป็นการยอมรับความเสี่ยง หรือความเสียหายที่อาจจะเกิดขึ้นไว้เองโดยไม่ทำอะไร และยอมรับในผลที่อาจตามมา เนื่องจากเห็นว่าโอกาสหรือความน่าจะเป็นที่จะเกิดความเสียหายอยู่ในวิสัย ที่โรงพยาบาลน้ำเกลี้ยง ยอมรับได้หรือไม่คุ้มค่าสำหรับค่าใช้จ่ายในการสร้างระบบในการจัดการหรือป้องกันความเสี่ยง

การควบคุม (Treat) เป็นการปรับปรุงระบบการทำงาน หรือออกแบบวิธีการทำงานใหม่เพื่อหาทางป้องกันมิให้ความเสียหายเกิดขึ้น เป็นการลดโอกาสหรือจำนวนครั้งของความเสียหายที่จะเกิดหากเรา ไม่สามารถป้องกันมิให้ความเสี่ยงเกิดขึ้นได้ก็ควรขจัดให้หมดไป หรือลดความรุนแรงของความเสี่ยงลงโดยมี การจัดทำแผนหรือมาตรการควบคุมขึ้น อาจกำหนดเป็นแนวทางปฏิบัติไว้ล่วงหน้า ทั้งนี้วิธีควบคุมความสูญเสีย มีสองวิธีหลัก คือ การป้องกันการเกิดความสูญเสีย และการควบคุมขนาดของความสูญเสียหลังเกิดความ สูญเสียขึ้นการป้องกันการเกิดความสูญเสีย เป็นวิธีการที่พยายามจะลดความถี่ของการเกิดความสูญเสียก็คือ การหา มาตรการหรือวิธีการใด ๆ ในการป้องกันมิให้ความสูญเสียเกิดขึ้น

การถ่ายโอน (Transfer) การโอนย้ายหรือแบ่งความเสี่ยงไปให้ผู้อื่นช่วยรับผิดชอบ เช่น อุปกรณ์ เครือข่ายเมื่อซื้อมาแล้วมีระยะประกันภัยเพียงหนึ่งปีเพื่อเป็นการรับมือในกรณีที่อุปกรณ์เครือข่ายไม่ทำงาน องค์กรอาจเลือกซื้อประกัน หรือสัญญาการบำรุงรักษาหลังการขาย

๗. ปัจจัยเสี่ยง

๑) ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk) แบ่งออกเป็น

- ๑.๑) ความเสี่ยงจากการเกิดไฟไหม้ห้องศูนย์คอมพิวเตอร์แม่ข่ายกลาง (Data Center)
- ๑.๒) ความเสี่ยงจากระบบกระแสไฟฟ้าขัดข้องของห้องศูนย์คอมพิวเตอร์แม่ข่ายกลาง (Data Center)
- ๑.๓) ความเสี่ยงจากอุณหภูมิและความชื้น ของศูนย์คอมพิวเตอร์แม่ข่ายกลางผิดปกติ (Data Center)
- ๑.๔) ความเสี่ยงจากแมลง สัตว์กัดแทะ อุปกรณ์เครือข่ายและระบบไฟฟ้า
- ๑.๕) ความเสี่ยงจากการโจรกรรมอุปกรณ์คอมพิวเตอร์เครื่องแม่ข่าย เครื่องลูกข่ายและอุปกรณ์ต่อ

พ่วง

๒) ความเสี่ยงด้านบุคลากร (Human Risk) แบ่งออกเป็น

- ๒.๑) ความเสี่ยงจากผู้ดูแลระบบ
- ๒.๒) ความเสี่ยงจากผู้ใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่าย

๓) ความเสี่ยงด้านระบบคอมพิวเตอร์และระบบเครือข่าย (Computer and Network Risk) แบ่งออกเป็น

- ๓.๑) ความเสี่ยงจากระบบคอมพิวเตอร์แม่ข่ายหลักเสียหาย
- ๓.๒) ความเสี่ยงจากการติดไวรัสคอมพิวเตอร์หรือมัลแวร์
- ๓.๓) ความเสี่ยงจากการถูกบุกรุก และถูกโจมตีระบบเครือข่ายจากภายในและภายนอกองค์กร
- ๓.๔) ความเสี่ยงจากการเชื่อมต่อระบบเครือข่ายอินเทอร์เน็ต และอินเทอร์เน็ตภายในและ ภายนอก

สถานที่ทำงาน

๔) ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk) แบ่งออกเป็น

- ๔.๑) ความเสี่ยงจากการใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์
- ๔.๒) ความเสี่ยงจากช่องโหว่จากการพัฒนาโปรแกรมประยุกต์ภายในองค์กร

๕) ความเสี่ยงด้านระบบฐานข้อมูล (Database Risk) แบ่งออกเป็น

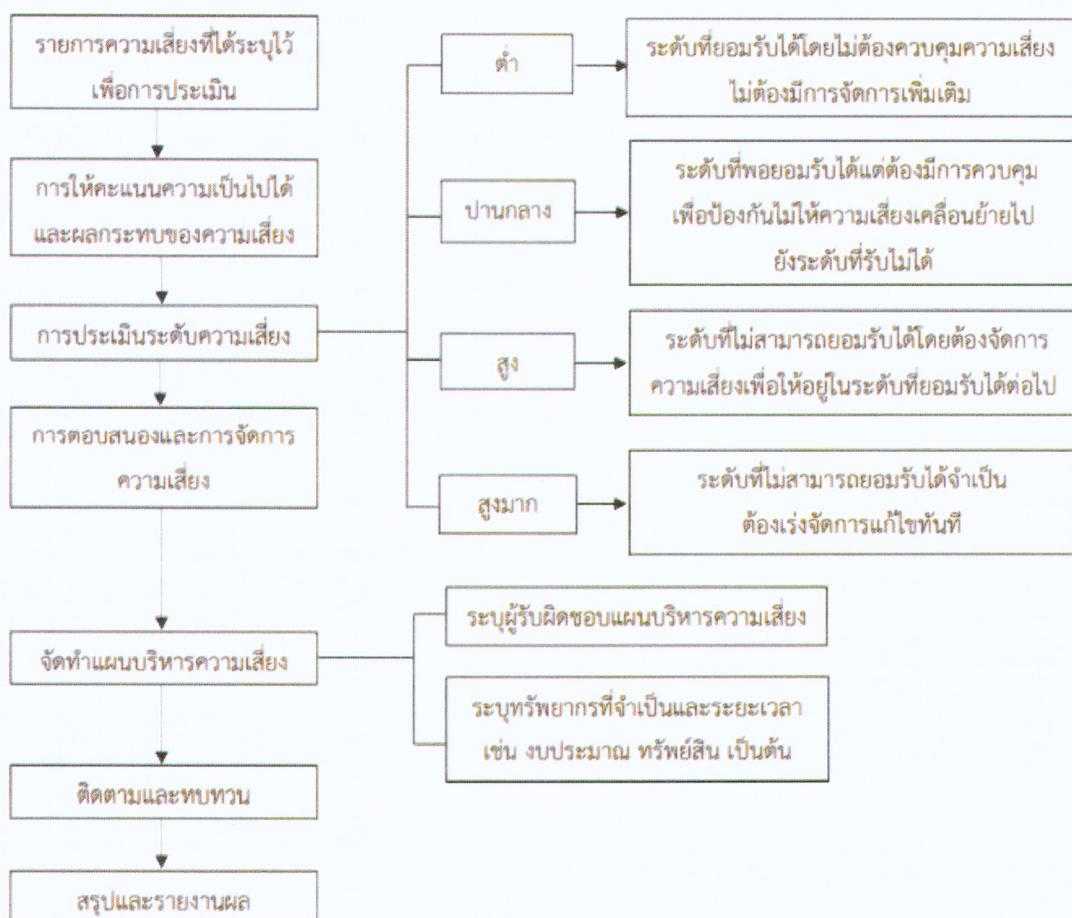
- ๕.๑) ความเสี่ยงจากระบบฐานข้อมูลไม่ถูกต้อง ไม่เป็นปัจจุบัน และไม่ครบถ้วน
- ๕.๒) ความเสี่ยงจากการไม่สำรองข้อมูล และไม่สามารถกู้คืนระบบฐานข้อมูล
- ๕.๓) ความเสี่ยงจากการถูกโจมตีระบบฐานข้อมูล

บทที่ ๒

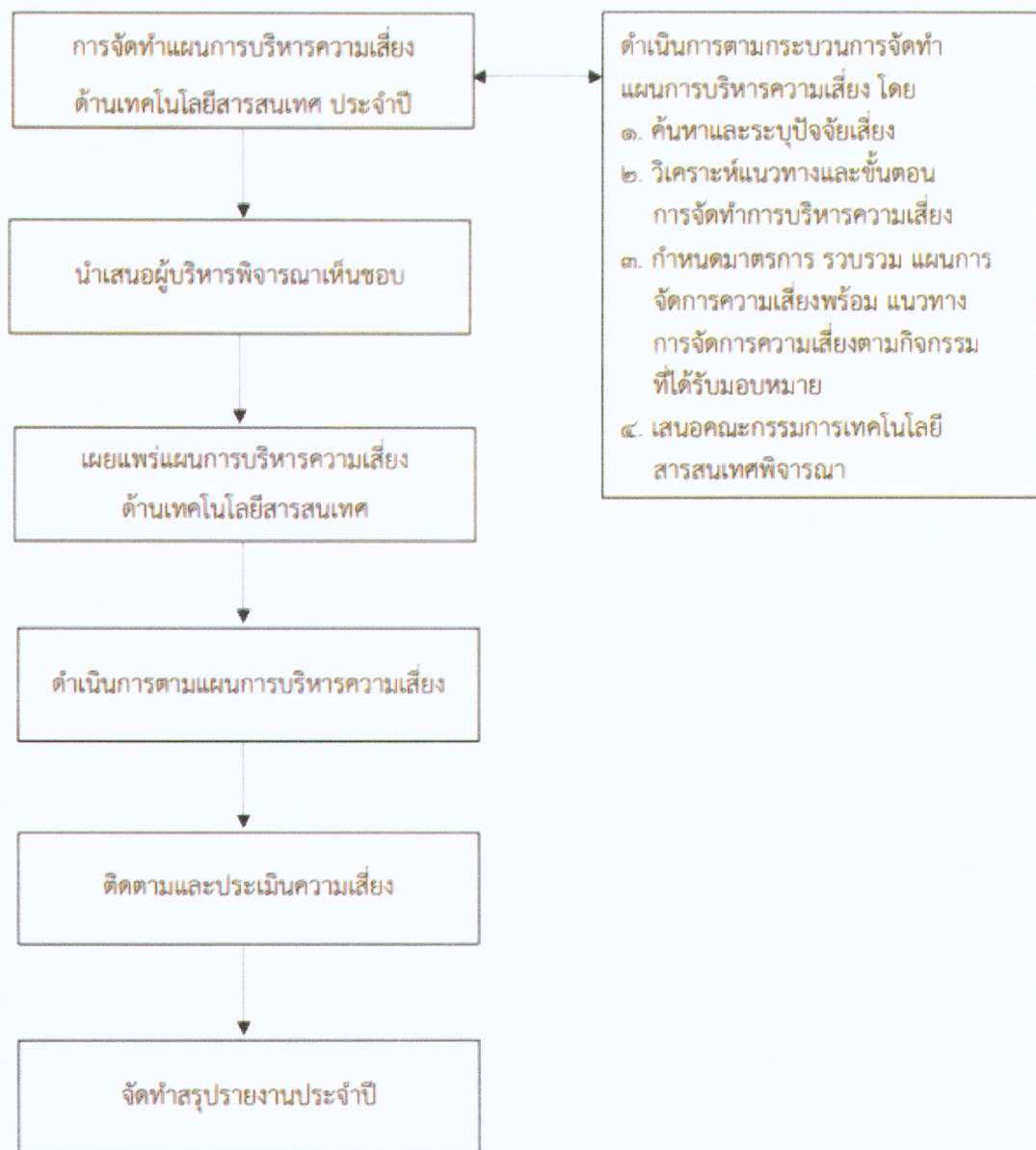
การวิเคราะห์และจัดทำแผนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

โรงพยาบาลน้ำเกลี้ยงได้ตระหนักถึงความสำคัญของข้อมูลที่อาจประสบกับความเสียหาย จากปัจจัยเสี่ยงหลายด้าน จึงมอบหมายให้ศูนย์เทคโนโลยีสารสนเทศ จัดทำแผนการบริหารความเสี่ยง ด้านเทคโนโลยีสารสนเทศ พ.ศ.๒๕๖๖ โดยกระบวนการบริหารจัดการความเสี่ยงของหน่วยงานเริ่มต้นจากการรวบรวมข้อมูลที่เกี่ยวข้องกับกิจกรรม การวิเคราะห์ปัจจัยเสี่ยง และกระบวนการที่มีผลต่อการดำเนินงานด้านสารสนเทศ โดยมีรายละเอียดดังนี้

๑. แผนภูมิแนวทางและขั้นตอนการบริหารความเสี่ยง



๒. กระบวนการจัดทำแผนการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ



๓. การวิเคราะห์ปัจจัยเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ

จากการวิเคราะห์ความเสี่ยงด้านคอมพิวเตอร์และสารสนเทศของโรงพยาบาลน้ำเกลี้ยง สามารถสรุปความเสี่ยงได้ ๕ ด้าน ดังนี้

๑) ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)

- ๑.๑) ความเสี่ยงจากการเกิดไฟไหม้ห้องศูนย์คอมพิวเตอร์แม่ข่ายกลาง (Data Center)
- ๑.๒) ความเสี่ยงจากระบบกระแสไฟฟ้าขัดข้องของห้องศูนย์คอมพิวเตอร์แม่ข่ายกลาง (Data Center)
- ๑.๓) ความเสี่ยงจากอุณหภูมิและความชื้น ของศูนย์คอมพิวเตอร์แม่ข่ายกลางผิดปกติ (Data Center)
- ๑.๔) ความเสี่ยงจากแมลง สัตว์กัดแทะ อุปกรณ์เครือข่ายและระบบไฟฟ้า
- ๑.๕) ความเสี่ยงจากการโจรกรรมอุปกรณ์คอมพิวเตอร์เครื่องแม่ข่าย เครื่องลูกข่าย และ อุปกรณ์ต่อ

พ่วง

๒) ความเสี่ยงด้านบุคลากร (Human Risk)

- ๒.๑) ความเสี่ยงจากผู้ดูแลระบบ
- ๒.๒) ความเสี่ยงจากผู้ใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่าย

๓) ความเสี่ยงด้านระบบคอมพิวเตอร์และระบบเครือข่าย (Computer and Network Risk)

- ๓.๑) ความเสี่ยงจากระบบคอมพิวเตอร์แม่ข่ายหลักเสียหาย
- ๓.๒) ความเสี่ยงจากการติดไวรัสคอมพิวเตอร์หรือมัลแวร์
- ๓.๓) ความเสี่ยงจากการถูกบุกรุก และถูกโจมตีระบบเครือข่ายจากภายในและภายนอกองค์กร
- ๓.๔) ความเสี่ยงจากการเชื่อมต่อระบบเครือข่ายอินเทอร์เน็ต และอินเทอร์เน็ตภายในและ ภายนอก

สถานที่ทำงาน

๔) ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk)

- ๔.๑) ความเสี่ยงจากการใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์
- ๔.๒) ความเสี่ยงจากช่องโหว่จากการพัฒนาโปรแกรมประยุกต์ภายในองค์กร

๕) ความเสี่ยงด้านระบบฐานข้อมูล (Database Risk)

- ๕.๑) ความเสี่ยงจากระบบฐานข้อมูลไม่ถูกต้อง ไม่เป็นปัจจุบัน และไม่ครบถ้วน
- ๕.๒) ความเสี่ยงจากการไม่สำรองข้อมูล และไม่สามารถกู้คืนระบบฐานข้อมูล
- ๕.๓) ความเสี่ยงจากการถูกโจมตีระบบฐานข้อมูล

ตารางการประมาณความเสี่ยง (Risk estimation)

ลำดับ	ความเสี่ยง	โอกาส	ผลกระทบ	คะแนน	ระดับ
๑. ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)					
๑.๑	ความเสี่ยงจากการเกิดไฟไหม้ห้องศูนย์คอมพิวเตอร์แม่ข่าย	๑	๕	๕	ปานกลาง
๑.๒	ความเสี่ยงจากระบบกระแสไฟฟ้าขัดข้องของห้องศูนย์คอมพิวเตอร์แม่ข่าย	๓	๒	๖	ปานกลาง
๑.๓	ความเสี่ยงจากอุณหภูมิลและความชื้น ของศูนย์คอมพิวเตอร์แม่ข่ายกลางผิดปกติ	๒	๕	๑๐	เสี่ยงสูง
๑.๔	ความเสี่ยงจากแมลง สัตว์กัดแทะ อุปกรณ์เครือข่ายและระบบไฟฟ้า	๑	๓	๓	ต่ำ
๑.๕	ความเสี่ยงจากการโจรกรรมอุปกรณ์คอมพิวเตอร์เครื่องแม่ข่ายเครื่องลูกข่าย และ อุปกรณ์ต่อ	๑	๓	๓	ต่ำ
๒. ความเสี่ยงด้านบุคลากร (Human Risk)					
๒.๑	ความเสี่ยงจากผู้ดูแลระบบ	๑	๓	๓	ต่ำ
๒.๒	ความเสี่ยงจากผู้ใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่าย	๓	๓	๙	เสี่ยงสูง
๓. ความเสี่ยงด้านระบบคอมพิวเตอร์และระบบเครือข่าย (Computer and Network Risk)					
๓.๑	ความเสี่ยงจากระบบคอมพิวเตอร์แม่ข่ายหลักเสียหาย	๓	๕	๑๕	สูงมาก
๓.๒	ความเสี่ยงจากการติดไวรัสคอมพิวเตอร์หรือมัลแวร์	๓	๒	๖	ปานกลาง
๓.๓	ความเสี่ยงจากการถูกบุกรุก และถูกโจมตีระบบเครือข่ายจากภายในและภายนอกองค์กร	๔	๓	๑๒	สูง
๓.๔	ความเสี่ยงจากการเชื่อมต่อระบบเครือข่ายอินเทอร์เน็ต และ อินเทอร์เน็ตภายในและ ภายนอกสถานที่ทำงาน	๓	๒	๖	ปานกลาง
๔. ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk)					
๔.๑	ความเสี่ยงจากการใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์	๑	๓	๓	ต่ำ
๔.๒	ความเสี่ยงจากช่องโหว่จากการพัฒนาโปรแกรมประยุกต์ภายในองค์กร	๒	๓	๖	ปานกลาง
๕. ความเสี่ยงด้านระบบฐานข้อมูล					
๕.๑	ความเสี่ยงจากระบบฐานข้อมูลไม่ถูกต้อง ไม่เป็นปัจจุบัน และไม่ครบถ้วน	๒	๓	๖	ปานกลาง
๕.๒	ความเสี่ยงจากการไม่สำรองข้อมูล และไม่สามารถกู้คืนระบบฐานข้อมูล	๑	๓	๓	ต่ำ
๕.๓	ความเสี่ยงจากการถูกโจมตีระบบฐานข้อมูล	๑	๓	๓	ต่ำ

ผลการวิเคราะห์ความเสี่ยงด้านเทคโนโลยีสารสนเทศและแนวทางการควบคุมที่มีอยู่

ความเสี่ยง	การประเมินความเสี่ยง			วิธีการบริหารความเสี่ยง			
	ผลกระทบ	โอกาส	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีการกำจัดความเสี่ยง	ผู้รับผิดชอบ
๑. ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)							
๑. ความเสี่ยงจากการเกิดไฟไหม้ห้องศูนย์คอมพิวเตอร์แม่ข่ายกลาง (Data Center)	๑. เครื่องคอมพิวเตอร์แม่ข่ายเสียหาย ๒. ระบบสารสนเทศและระบบฐานข้อมูลถูกทำลาย	๑	๕	๕	๑. ตรวจสอบความพร้อมใช้งานถึงดับเพลิงทุกเดือน ๒. ตรวจสอบเครื่องสำรองข้อมูลแบบ Realtime ทุกวัน ๓. สำรองฐานข้อมูลเป็นก้อน SQL ทุกวัน วัน ละ ๒ รอบ	การควบคุม	งานเทคโนโลยีสารสนเทศ
	๒. ความเสี่ยงจากระบบกระแสไฟฟ้าขัดข้องของห้องศูนย์คอมพิวเตอร์แม่ข่ายกลาง (Data Center)	๑. ไม่สามารถใช้โปรแกรม Him.pro ได้ ๒. ไม่สามารถใช้งานระบบคอมพิวเตอร์และระบบเครือข่ายได้ ๓. ระบบปฏิบัติการและระบบฐานข้อมูลเกิดความเสียหายเนื่องจากปิดไม่ถูกวิธี	๓	๒	๖		
๓. ความเสี่ยงจากอุณหภูมิและความชื้นของศูนย์คอมพิวเตอร์แม่ข่ายกลางผิดปกติ	๑. เครื่องคอมพิวเตอร์แม่ข่ายทำงานหนักและอาจทำให้อุปกรณ์เสียหาย	๒	๕	๑๐	๑. ตรวจสอบเครื่องปรับอากาศและที่วัดอุณหภูมิทุกวัน ๒. ล้างแผ่นกรองเครื่องปรับอากาศทุกเดือน เดือนละ ๑ ครั้ง	การควบคุม	งานเทคโนโลยีสารสนเทศ
๔. ความเสี่ยงจากแมลงสัตว์กัดแทะ อุปกรณ์	๑. ไม่สามารถใช้งานระบบเครือข่ายได้ ๒. ไม่สามารถให้บริการระบบเครือข่ายได้	๑	๓	๓	๑. แบ่ง V-LAN Network ๒. ตรวจสอบอุปกรณ์เครือข่ายและระบบไฟฟ้าเดือนละ ๑ ครั้ง	การยอมรับ	งานเทคโนโลยีสารสนเทศ

ความเสี่ยง	การประเมินความเสี่ยง				วิธีการบริหารความเสี่ยง		
	ผลกระทบ	โอกาส	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีการกำจัดความเสี่ยง	ผู้รับผิดชอบ
เครือข่ายและระบบไฟฟ้า							
๕. ความเสี่ยงจากการโจรกรรมอุปกรณ์คอมพิวเตอร์เครื่องแม่ข่าย เครื่องลูกข่าย และอุปกรณ์ต่อพ่วง	๑. ไม่สามารถใช้งานระบบสารสนเทศได้ ๒. อุปกรณ์และข้อมูลสำคัญหาย	๑	๓	๓	๑. ติดตั้งระบบกล้องวงจรปิดภายในห้อง Data Center ๒. ติดตั้งระบบรักษาความปลอดภัยการเข้าออกห้อง Data Center ๓. ระบบสำรองข้อมูลแบบ Realtime เก็บคนละตึก ๔. สำรองข้อมูลเป็นก้อน SQL ๑ วัน ๒ รอบ	การควบคุม	งานเทคโนโลยีสารสนเทศ
๒. ความเสี่ยงด้านบุคลากร (Human Risk)							
๑. ความเสี่ยงจากผู้ดูแลระบบ	ข้อมูลที่อยู่ในชั้นความลับ รั่วไหล ทำให้เสียหายต่อความน่าเชื่อถือของหน่วยงาน	๑	๓	๓	๑. มีการทำ Authentication การใช้งานระบบสารสนเทศ และยกเลิกการใช้งานระบบสารสนเทศ (เกษียณอายุ ลาออก) ๒. มีการกำหนดสิทธิ์ในการเข้าถึงชั้นข้อมูลของแต่ละระดับ	การควบคุม	งานเทคโนโลยีสารสนเทศ
๒. ความเสี่ยงจากผู้ใช้งานเครื่อง	๑. สูญเสีย Bandwidth ในระบบเครือข่ายทำให้ต้องเพิ่ม Bandwidth	๓	๓	๔	๑. กำหนด Policy ของ Firewall ให้เหมาะสมต่อการใช้งาน	การควบคุม	งานเทคโนโลยีสารสนเทศ

ความเสี่ยง	การประเมินความเสี่ยง				วิธีการบริหารความเสี่ยง		
	ผลกระทบ	โอกาส	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีการกำจัดความเสี่ยง	ผู้รับผิดชอบ
คอมพิวเตอร์และระบบเครือข่าย	ให้มากขึ้น เนื่องจากการใช้งานนอกเหนือจากงานราชการ ๒. เครื่องคอมพิวเตอร์เสียหายและเสื่อมอายุการใช้งานเร็วกว่าปกติ				๒. มีการกำหนดสิทธิ์การเข้าถึงงาน Internet โดยผ่าน Authentication ทุกครั้งก่อนเข้าใช้งาน ๓. ห้ามนำอุปกรณ์ Access point, Switch, Computer เข้ามาเชื่อมต่อในระบบโดยไม่ได้รับอนุญาต		
๓. ความเสี่ยงด้านระบบคอมพิวเตอร์และระบบเครือข่าย (Computer and Network Risk)							
๑. ความเสี่ยงจากระบบคอมพิวเตอร์แม่ข่ายหลักเสียหาย	๑. เกิดความเสียหายต่อระบบสารสนเทศและระบบฐานข้อมูล ๒. ไม่สามารถใช้งานระบบสารสนเทศที่สำคัญได้และต้องใช้งานอย่างเร่งด่วน	๓	๕	๑๕	๑. ตรวจสอบเครื่องแม่ข่ายทุกวันก่อนปฏิบัติงาน ๒. มีระบบสำรองข้อมูลแบบ Realtime เก็บคนละตึก ๓. สำรองข้อมูลเป็นก้อน SQL ๑ วัน ๒ รอบ	การควบคุม	งานเทคโนโลยีสารสนเทศ
๒. ความเสี่ยงจากการติดไวรัสคอมพิวเตอร์หรือมัลแวร์	๑. ไฟล์งานข้อมูลเสียหายหรือถูกเข้ารหัส ๒. ไม่สามารถใช้งานโปรแกรมหรือระบบปฏิบัติการได้ตามปกติ ๓. เครื่องคอมพิวเตอร์ช้า	๓	๒	๖	๑. อัปเดตโปรแกรมป้องกันไวรัสให้สามารถป้องกันไวรัส ได้ทุกรูปแบบ ๒. จัดทำแผนขอจัดซื้อ license Antivirus ๓. ปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัย ของระบบ	การควบคุม	งานเทคโนโลยีสารสนเทศ

ความเสี่ยง	การประเมินความเสี่ยง				วิธีการบริหารความเสี่ยง		
	ผลกระทบ	โอกาส	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีการกำจัดความเสี่ยง	ผู้รับผิดชอบ
๓. ความเสี่ยงจากการถูกบุกรุก และถูกโจมตีระบบเครือข่ายจากภายในและภายนอกองค์กร	๑. ระบบสารสนเทศของหน่วยงานไม่สามารถให้บริการได้ ๒. ทำให้ระบบเครื่องแม่ข่าย หรือลูกข่ายติดไวรัส และแพร่กระจายสู่เครื่องอื่นๆ ทั้งหมดในเครือข่าย ๓. ถูกแก้ไขหรือเปลี่ยนแปลงข้อมูล หรือ รูปภาพ บน Web Site ของหน่วยงาน ๔. ถูกโจรกรรมข้อมูลที่เป็นความลับ ๕. ไม่สามารถเข้าใช้ระบบสารสนเทศได้	๔	๓	๑๒	สารสนเทศและ ให้มีผลบังคับใช้ ๑. ตรวจสอบ Policy และ การทำงานของระบบ ป้องกันการบุกรุก และระบบเฝ้าระวัง เครือข่ายทุกวัน ๒. อัปเดตโปรแกรมป้องกันไวรัส ให้สามารถป้องกันไวรัส ได้ทุกรูปแบบ ๓. จัดทำแผนขอจัดซื้อ Firewall ในปีงบประมาณ ๒๕๖๖	การควบคุม	งานเทคโนโลยีสารสนเทศ
๔. ความเสี่ยงจากการเชื่อมต่อระบบเครือข่าย อินเทอร์เน็ต และ อินเทอร์เน็ตภายในและภายนอกสถานที่ทำงาน	๑. ไม่สามารถเข้าใช้งาน VPN ได้ ๒. ไม่สามารถเข้าใช้งานระบบสารสนเทศได้	๑	๓	๓	๑. ตรวจสอบเครื่องลูกข่ายเชื่อมต่อ Internet ๒. ควบคุมการเข้าใช้ เครือข่าย อินเทอร์เน็ต และ อินเทอร์เน็ต โดยใช้ระบบยืนยันตน (Authentication)	การควบคุม	งานเทคโนโลยีสารสนเทศ
๔. ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk)							
๑. ความเสี่ยงจากการใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์	๑. การใช้งานโปรแกรมไม่ได้เต็มประสิทธิภาพ	๑	๓	๓	๑. จัดหาซอฟต์แวร์แวร์ที่ถูกต้องกฎหมาย	การยอมรับ	งานเทคโนโลยีสารสนเทศ

ความเสี่ยง	การประเมินความเสี่ยง				วิธีการบริหารความเสี่ยง		
	ผลกระทบ	โอกาส	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีการกำจัดความเสี่ยง	ผู้รับผิดชอบ
๒. ความเสี่ยงจากช่องโหว่จาก การพัฒนาโปรแกรมประยุกต์ภายในองค์กร	๑. สร้างความเสียหายต่อระบบคอมพิวเตอร์แม่ข่าย ระบบสารสนเทศ และระบบฐานข้อมูล ๒. ผล Lab หาย เนื่องจากมีการเปิดใบส่งยาค้างไว้ HN เดี่ยวกันหลายเครื่อง พอลผล lab ออก ทำให้ Code Check Result เปลี่ยน	๒	๓	๖	๑. มีการตรวจสอบ Log การเข้าใช้งานระบบเครือข่าย ๒. ชี้แจงเรื่องการลงบันทึกข้อมูล ๓. มีการตรวจสอบ band with ถ้ามีการรับส่งข้อมูลเยอะเกิน ผิดปกติจะมีการแจ้งเตือนเข้าไปที่ไลน์กลุ่มผู้ดูแลระบบ	การยอมรับ	งานเทคโนโลยีสารสนเทศ
๕. ความเสี่ยงด้านระบบฐานข้อมูล							
๑. ความเสี่ยงจากระบบฐานข้อมูลไม่ถูกต้อง ไม่เป็นปัจจุบัน และไม่ครบถ้วน	๑. ระบบฐานข้อมูลไม่สามารถนำไปใช้ ๒. สนับสนุนการปฏิบัติงานได้อย่างมีประสิทธิภาพ	๒	๓	๖	๑. จัดทำรายการข้อมูลและความถี่ในการปรับปรุง ๒. กำหนดมาตรการการ แนวทางการปรับปรุง และ ช่องทางการเข้าถึงข้อมูล เพื่อให้ผู้ดูแลข้อมูลถือปฏิบัติ	การยอมรับ	งานเทคโนโลยีสารสนเทศ
๒. ความเสี่ยงจากการไม่สำรอง ข้อมูล และไม่สามารถกู้คืนระบบฐานข้อมูล	๑. เกิดความเสียหายของข้อมูลส่งผลกระทบต่อการให้บริการผู้ป่วย ๒. ไม่สามารถนำข้อมูลที่มีอยู่มาใช้ในการให้บริการเจ้าหน้าที่และผู้ป่วยได้	๑	๓	๓	๑. ตรวจสอบการทำงานของเครื่องแม่ข่ายสำรองทุกวันก่อนปฏิบัติงาน ๒. ตรวจสอบเครื่อง Backup database ทุกวัน	การยอมรับ	งานเทคโนโลยีสารสนเทศ
๓. ความเสี่ยงจากการโจรกรรม ระบบฐานข้อมูล	๑. ข้อมูลที่สำคัญรั่วไหลสู่ภายนอกหรือสาธารณะ ๒. ข้อมูลที่สำคัญสูญหายและถูกทำลาย	๑	๓	๓	๑. ตรวจสอบระบบป้องกัน การบุกรุกและระบบ ตรวจสอบและ	การยอมรับ	งานเทคโนโลยีสารสนเทศ

ความเสี่ยง	การประเมินความเสี่ยง				วิธีการบริหารความเสี่ยง		
	ผลกระทบ	โอกาส	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีการกำจัดความเสี่ยง	ผู้รับผิดชอบ
					เผื่อระวัง เครือข่าย เป็นประจำทุกวัน ๒. ตรวจสอบ Policy และ Log ของระบบป้องกัน การบุกรุกและระบบ เผื่อระวังเครือข่าย เป็นประจำทุกวัน		

[illegible]

บทที่ ๓

สรุปผลข้อเสนอแนะ

๓.๑ การประเมินปัจจัยเสี่ยง

นโยบายของกลุ่มสารสนเทศทางการแพทย์ ระดับความเสี่ยงที่ยอมรับได้ ≤ 5 ความเสี่ยงที่จำเป็นต้องนำมาดำเนินการจัดการความเสี่ยง คือความเสี่ยงที่มีระดับความเสี่ยงสูง ตั้งแต่ ๑๐ ส่วนความเสี่ยงในแผนบริหารความเสี่ยงต่ำกว่า ๑๐ ถือว่ามีความเสี่ยงค่อนข้างต่ำอาจจะนำมาดำเนินการ จัดการความเสี่ยงในแผนบริหารความเสี่ยงหรือไม่ก็ได้ การดำเนินการจัดการความเสี่ยง กิจกรรมที่ดำเนินการ ต่อไป

๑. สร้างความตระหนักในเรื่องนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ โดยจัดทำแผนโครงการกระตุ้นผู้ใช้งานให้ตระหนักในความเสี่ยงของการเปิดเผยข้อมูล หรือแชร์ข้อมูลในสื่อสังคม ออนไลน์ ทุกชนิด
๒. กระตุ้นให้เกิดการปฏิบัติตามแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศอย่างเคร่งครัด
๓. จัดทำ KM เพื่อแพร่ข้อมูล ข่าวสารเกี่ยวกับภัย ที่มีอยู่

๓.๒ ปัจจัยที่ทำให้ระบบบริหารความเสี่ยงประสบผลสำเร็จ

๑. แรงผลักดันจากผู้บริหารหน่วยงานที่ให้ความสนับสนุน
๒. เทคโนโลยีสารสนเทศที่ช่วยในการจัดเก็บข้อมูล การส่งถ่ายข้อมูลและการตรวจสอบย้อนกลับได้ อย่างรวดเร็ว
๓. ความร่วมมือร่วมใจของบุคลากรภายในเทคโนโลยีสารสนเทศทางการแพทย์ที่จะผลักดันให้การ บริหารความเสี่ยงประสบผลสำเร็จ

๔.๓ ผลการประเมิน / ข้อเสนอสรุป

ผู้บริหารได้สร้างบรรยากาศสภาพแวดล้อมการควบคุมภายในเพื่อให้บุคลากรทุกคนมีทัศนคติที่ดีต่อการควบคุมภายในโดยใช้หลักธรรมาภิบาลส่งเสริม สนับสนุน และสื่อสารให้ทุกคนเข้าใจขอบเขตหน้าที่ รวมทั้งความสามารถ ทักษะในการปฏิบัติงาน กฎ ระเบียบ ข้อบังคับที่เกี่ยวข้อง รวมถึงตลอดถึงจรรยาบรรณการทำงานของบุคลากรผู้เกี่ยวข้อง เพื่อให้การควบคุมภายในหน่วยงานมีประสิทธิภาพสามารถปฏิบัติงานตามภารกิจและตามที่ได้มอบหมายได้อย่างมีประสิทธิภาพ จาก การประเมินองค์ประกอบของการควบคุมภายในด้านการประเมินความเสี่ยงพบว่าในภาพรวมมีความเหมาะสมแล้ว แต่ต้องมีการปรับปรุงให้เหมาะสมยิ่งขึ้น ความเสี่ยงอยู่ในระดับที่ยอมรับได้และส่งเสริมให้บุคลากรมีความรู้ความชำนาญในการวิเคราะห์ความเสี่ยง



นายต่อกระกุล ศรีทา

นายแพทย์ชำนาญการ รักษาการในตำแหน่ง

ผู้อำนวยการโรงพยาบาลน้ำเกลี้ยง