แผนบริหารความเสี่ยงเทคโนโลยีสารสนเทศ

โรงพยาบาลปากพนัง

อ.ปากพนัง จ.นครศรีธรรมราช

Information security risk assessment

โรงพยาบาลปากพนัง
อ.ปากพนัง จ.นครศรีธรรมราช
ปี ๒๕๖๖

แผนบริหารความเสี่ยงเทคโนโลยีสารสนเทศ

โรงพยาบาลปากพนัง

อำเภอปากพนัง จังหวัดนครศรีธรรมราช

แผนบริหารความเสี่ยงเทคโนโลยีสารสนเทศ

หลักการและเหตุผล

การบริหารความเสี่ยงเป็นเครื่องมือทางกลยุทธ์ที่สำคัญตามหลักการกำกับดูแลกิจการที่ดี โดยจะช่วยให้การบริหารงานและการตัดสินใจด้านต่างๆ เช่น การวางแผน การกำหนดกลยุทธ์ การติดตามควบคุม และวัดผลการปฏิบัติงาน ตลอดจนการใช้ทรัพยากรต่างๆ อย่างเหมาะสมและมี ประสิทธิภาพมากขึ้น ลดการสูญเสียและโอกาสที่ทำให้เกิดความเสียหายแก่องค์กร โดยเฉพาะอย่างยิ่ง ในด้านเทคโนโลยีสารสนเทศที่เข้ามามีบทบาทสำคัญในการดำเนินงานของหน่วยงานภายในองค์กร ทั้งการจัดเก็บข้อมูล การใช้งานอุปกรณ์คอมพิวเตอร์ การติดต่อสื่อสารผ่านระบบเครือข่าย และวิธีการ ปฏิบัติงานระบบเทคโนโลยีสารสนเทศต่างๆภายใต้สภาวะการดำเนินงานของทุกๆ องค์กรล้วนแต่มีความเสี่ยง ซึ่งก็คือความไม่แน่นอนที่จะส่งผลกระทบต่อการดำเนินงานหรือเป้าหมายขององค์กรจึงจำเป็นต้องมีการจัดการความเสี่ยงเหล่านั้นอย่างเป็นระบบ โดยการระบุความเสี่ยงว่ามีปัจจัยเสี่ยง ใดบ้างที่กระทบต่อการดำเนินงานหรือเป้าหมายขององค์กรวิเคราะห์ความเสี่ยงจากโอกาสและผลกระทบที่เกิดขึ้น จัดสำดับความสำคัญของปัจจัยเสี่ยง แล้วกำหนดแนวทางในการจัดการความเสี่ยง โดยต้องคำนึงถึงความคุ้มค่าในการจัดการความเสี่ยงอย่างเหมาะสม

วัตถุประสงค์

๑. เพื่อเตรียมความพร้อมและรองรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบฐานข้อมูล สารสนเทศโรงพยาบาลปากพนัง
๒. เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศให้มีเสถียรภาพและมีความพร้อมสำหรับการใช้งาน
๓. เพื่อให้การปฏิบัติงานเป็นไปอย่างมีระบบและต่อเนื่อง และสามารถแกไขสถานการณ์ได้อย่าง ทันท่วงที กรณีเกิดสถานการณ์ความไม่แน่นอนและภัยพิบัติ

บริบท (Context)

ศูนย์สารสนเทศและเวชระเบียนอยู่ในกลุ่มงานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศ ทางการแพทย์ การแพทย์ เป็นหน่วยงานดูแลระบบ และ สนับสนุนพัฒนาระบบเทคโนโลยีสารสนเทศและเวช ระเบียน ดูแลระบบคอมพิวเตอร์ทั้งด้าน Hardware Software และ ฐานข้อมูล ให้ระบบสามารถ ทำงานได้ตลอด ๒๔ ชั่วโมง มี Server ๕ เครื่อง เครื่องคอมพิวเตอร์ตั้ง โต๊ะ ๑๓๔ เครื่อง โดย มีวัตถุประสงค์เพื่อตอบสนองความต้องการของหน่วยงานในโรงพยาบาลและผู้มีส่วนได้เสียเพื่อให้ได้ข้อมูลที่ครบล้วน ถูกต้อง รวดเร็ว ตรวจสอบได้ และลดขั้นตอนการทำงาน มีการ นำข้อมูลที่ได้มา ใช้ในการวางแผนการดำเนินงาน การแก้ปัญหาต่าง ๆ เพิ่มช่องทางการสื่อสารและ การเรียนรู้ภายในองค์กร โดยด้านโครงสร้างพื้นฐานหรือ Infrastructure มีการเชื่อมโยงเครือข่าย LAN ครอบคลุมหน่วยงานทั้งโรงพยาบาล มีการแบ่งระบบเครือข่ายออกเป็น ๒ ระบบ คือ ระบบ เครือข่ายการให้บริการผู้ป่วย HOSxP และระบบเครือข่าย Internet

ก.หน้าที่และเป้าหมาย หน้าที่

เป็นหน่วยงานสนับสนุนที่ตั้งขึ้นมาเพื่อให้บริการระบบเทคโนโลยีสารสนเทศของโรงพยาบาลปากพนัง ในงานดูแลผู้ป่วย งานบริหารและบริการเครือข่ายฯ เพื่อตอบสนองความต้องการของผู้บริหาร ผู้ ให้บริการและผู้รับบริการ อย่างถูกต้องทันเวลาและสามารถนำไปใช้ประโยชน์ได้จริง

เป้าหมาย

- โรงพยาบาลมีระบบสารสนเทศและคอมพิวเตอร์ต้องมีความถูกต้อง เพียงพอ พร้อมใช้ ปลอดภัย และได้รับความพึงพอใจ
- มีการจัดเก็บข้อมูลที่สามารถสืบค้นได้ง่าย มีความถูกต้องและทันเวลา
- มีระบบการรักษาความลับและความปลอดภัยของข้อมูล
- มีการเชื่อมโยงข้อมูลเพื่อการบริหาร บริการดูแลผู้ป่วยและการพัฒนาคุณภาพ

ข.ขอบเขตการให้บริการ (Scope of Service)

๑. ดูแลระบบให้พร้อมใช้งาน ตลอด ๒๔ ชั่วโมง
๒. สำรวจและจัดหาคอมพิวเตอร์และอุปกรณ์ต่อพ่วง
๓. บำรุงรักษาดูแลและรักษาความปลอดภัยของระบบเครือข่าย
๔. วางแผนและออกแบบระบบรายงานสารสนเทศเพื่อตอบสนองความต้องการตามคำร้องขอข้อมูลของผู้ให้กำหนดมาตรฐานและนโยบายสำหรับเวชระเบียน
๕. พัฒนาคุณภาพ ประเมิน ทบทวน ความสมบูรณ์ของเวชระเบียนปรับปรุงฐานข้อมูลให้ถูกต้องครบถ้วนก่อนส่งออก
๖. เชื่อมโยงข้อมูลสารสนเทศ เพื่อการพัฒนาคุณภาพ
๗. ให้คำปรึกษา แนะนำ อบรมงานด้านสารสนเทศและการใช้คอมพิวเตอร์ให้สอดคล้องกับสถานการณ์ปัจจุบัน
๘. รวบรวมข้อมูล วิเคราะห์ และนำเสนอข้อมูลต่อทีมนำ หน่วยงาน

นิยามความเสี่ยง

ความเสี่ยง คือ ความไม่แน่นอนที่อาจนำไปสู่ความสูญเสียทั้งที่เป็นตัวเงินและไม่ เป็นตัวเงิน ความเสี่ยงมีทั้งประเภทที่เป็นความเสี่ยงที่แท้จริงที่เป็นความเสี่ยงที่มีโดยธรรมชาติ และ ความเสี่ยงที่เกิดจากการเก็งกำไร ความหมายของความเสี่ยงอาจมีการติความแตกต่างกันไปหลายอย่างตามแต่ความเชี่ยวชาญ และอาชีพของผู้ให้คำจำกัดความ

การบริหารความเสี่ยง เป็นการบริหารปัจจัย และควบคุมกิจกรรม หรือ กระบวนการต่าง ๆ เพื่อลดโอกาสที่จะทำให้เกิดความเสียหาย หรือล้มเหลว ดังนั้นเพื่อควบคุมให้ ระดับความเสียหาย และผลกระทบที่อาจจะเกิดขึ้นใน อนาคตอยู่ในระดับที่สามารถรับได้ ประเมินได้ ควบคุมได้ และสามารถตรวจสอบได้อย่างมีระบบ โดยคำนึงถึงการบรรลุเป้าหมายตามภารกิจหลัก ตามกฎหมายจัดตั้งส่วนราชการ และเป้าหมายตามแผนปฏิบัติราชการ ประจำปี งบประมาณของส่วนราชการและเป้าหมายตามแผนปฏิบัติราชการประจำปีของส่วนราชการ

นิยาม ระบบสารสนเทศ

คือ ระบบข้อมูล การจัดเก็บข้อมูล การประมวลผลข้อมูล การไหลข้อมูลทั้งภายในและ ภายนอกองค์กร และการนำเสนอสารสนเทศ

องค์ประกอบของระบบคอมพิวเตอร์

๑. **Hardware** หมายถึง อุปกรณ์ต่างๆที่กระทำกับข้อมูล เอกสาร ทั้งที่เป็นอุปกรณ์ คอมพิวเตอร์และไม่ใช่คอมพิวเตอร์

๒. **Software** หมายถึง ชุดคำสั่งที่สั่งให้คอมพิวเตอร์ทำงาน

๓. **บุคลากร** หมายถึง กลุ่มบุคคลที่ปฏิบัติงานกับระบบสารสนเทศ คือ เป็นผู้น่า จัดการ ข้อมูลและน่าผลลัพธ์ออกจากระบบคอมพิวเตอร์

๔. **ข้อมูลและแฟ้มข้อมูล** หมายถึงข้อมูลและสารสนเทศ ที่ระบบจัดเก็บไว้ในช่วงเวลาหนึ่ง

๕. **หน้าที่การปฏิบัติงาน** หมายถึงคำสั่งหรือกฎเกณฑ์ที่ใช้ในการทำงานของระบบ

องค์ประกอบของระบบสารสนเทศ

องค์กร โครงสร้างขององค์กรระบบสารสนเทศจะทำหน้าที่ในการสนับสนุนการทำงานของ องค์กรโดยรวม ไม่ว่าจะเป็นฝ่ายต่างๆขององค์กร

บุคลากร บุคลาการที่ใช้ระบบสารสนเทศจากระบบคอมพิวเตอร์ที่ทำงานร่วมกัน บุคลากร ที่ต้องการป้อนข้อมูลไปยังระบบเพื่อส่งต่อไปยังคอมพิวเตอร์

เทคโนโลยี อุปกรณ์ที่ทำหน้าที่ในการจัดการสารสนเทศ เพื่อส่งต่อไปยังบุคลากรที่ใช้ระบบสารสนเทศ **หมายเหตุ** องค์ประกอบของระบบสารสนเทศที่ใช้ระบบคอมพิวเตอร์ในการบริหาร จึงประกอบด้วย องค์ประกอบของทั้งสองระบบรวมกัน

ความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ส่วนราชการต้องมีการวางระบบบริหารความเสี่ยงของระบบฐานข้อมูลและสารสนเทศ โดยต้องดำเนินการดังต่อไปนี้

๑. มีการบริหารความเสี่ยงเพื่อกำจัด ป้องกัน หรือลดการเกิดความเสียหายในรูปแบบต่างๆ โดย สามารถฟื้นฟูระบบสารสนเทศและการสำรองและกู้คืนข้อมูลจากความเสียหาย (Backup and Recovery)

๒. มีการจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจจะเกิดกับระบบสารสนเทศ (IT Contingency Plan)

๓. มีระบบรักษาความมั่นคงและปลอดภัย (Security) ของระบบฐานข้อมูล

๔. มีการกำหนดสิทธิให้ผู้ใช้ในแต่ละระดับ (Access Rights)

การตอบสนองความเสี่ยง

เมื่อความเสี่ยงได้รับการบ่งชี้และประเมินความสำคัญแล้วผู้บริหารต้องประเมินวิธีการจัดการ ความเสี่ยงที่สามารถนำไปปฏิบัติได้และผลของการจัดการเหล่านั้น การพิจารณาทางเลือกในการดำเนินการจะต้องคำนึงถึงความเสี่ยงที่ยอมรับได้ และต้นทุนที่เกิดขึ้นเปรียบเทียบกับผลประโยชน์ที่ จะได้รับเพื่อให้การบริหารความเสี่ยงมีประสิทธิผลผู้บริหารอาจต้องเลือกวิธีการจัดการความเสี่ยงอย่างใดอย่างหนึ่ง หรือหลายวิธีรวมกัน เพื่อลดระดับโอกาสที่อาจเกิดขึ้นและผลกระทบของเหตุการณ์ ให้อยู่ในช่วงที่องค์กรสามารถยอมรับได้ (Risk Tolerance)

หลักการตอบสนองความเสี่ยงมี ๔ ประการ คือ

๑. การหลีกเสี่ยง (Terminate) เป็นวิธีการที่ง่ายที่สุดในการบริหารความเสี่ยง คือ การเลือก ที่จะไม่รับความเสี่ยงไว้เลยอาจหยุดดำเนินการหรือยกเลิกโครงการ/กิจกรรมที่ก่อให้เกิดความเสียหายได้ การหลีกเสี่ยงความเสี่ยงเมื่อพบว่าผลประโยชน์ที่จะได้รับนั้นไม่คุ้มกับสิ่งที่จะเกิดขึ้นจึงหลีกเสี่ยงที่จะเผชิญกับกิจกรรมความเสี่ยงนั้น หรือการหลีกเสี่ยงความเสี่ยงอาจเกิดขึ้นจากหน่วยงาน เลือกที่จะหลีกเสี่ยงกิจกรรมความเสี่ยงนั้น โดยมิได้คิดทบทวนถึงผลที่จะได้รับ น่ามาซึ่งการเสียโอกาส ของหน่วยงานได้

๒. การยอมรับ (Take) เป็นการยอมรับความเสี่ยง หรือความเสียหายที่อาจจะเกิดขึ้นไว้เอง โดยไม่ทำอะไร และยอมรับในผลที่อาจตามมา เนื่องจากเห็นว่าโอกาสหรือความน่าจะเป็นที่จะเกิด ความเสียหายอยู่ในวิสัยที่หน่วยงานยอมรับได้ หรือไม่คุ้มค่าสำหรับค่าใช้จ่ายในการสร้างระบบในการ จัดการหรือป้องกันความเสี่ยง เช่น การกำหนด User/Password ในการเข้าใช้งานระบบเครือข่าย ให้กับหัวหน้างาน เมื่อหัวหน้างานได้ User/Password ที่ทางศูนย์คอมฯ ออกให้แล้ว อาจจะบอกให้ ผู้ใต้บังคับบัญชาของตนทราบ User/Password ดังกล่าวและเมื่อผู้ใต้บังคับบัญชาทราบUser/Password ชองหัวหน้างาน อาจจะเก็บไว้คนเดียวหรือน่าไปบอกให้บุคคลอื่นทราบต่อ ซึ่งใน กรณีนี้จะเกิดความเสี่ยงในการถูกเจาะหรือสักลอบ (Hack) เข้าสู่ระบบเครือข่าย ซึ่งทางศูนย์คอมฯ ต้องยอมรับความเสี่ยงหรือความเสียหายที่อาจเกิดขึ้น และกำหนด User/Password ใหม่ ให้กับหัวหน้างาน เป็นต้น

๓. การควบคุม (Treat) เป็นการปรับปรุงระบบการทำงาน หรือออกแบบวิธีการทำงานใหม่ เพื่อหาทางป้องกันมิให้มีความเสียหายเกิดขึ้น เป็นการลดโอกาสหรือจำนวนครั้งของความเสียหายที่ จะเกิด หากเราไม่สามารถป้องกันไม่ให้ความเสี่ยงเกิดขึ้นได้ ก็ควรขจัดให้หมดไป หรือลดความรุนแรง ชองความเสี่ยงลงโดยมีการจัดทำแผนหรือมาตรการควบคุมขึ้นอาจกำหนดเป็นแนวทางปฏิบัติไว้ล่วงหน้า ทั้งนี้วิธีควบคุมความสูญเสียมีสองวิธีหลัก คือ การป้องกันการเกิดความสูญเสียและการ ควบคุมขนาดชองความสูญเสียหลังเกิดความสูญเสียขึ้น

การป้องกันการเกิดความสูญเสีย เป็นวิธีการที่พยายามจะลดความถี่ชองการเกิดความสูญเสีย ก็คือการหามาตรการหรือวิธีการใด ๆ ในการป้องกันไม่ให้ความสูญเสียเกิดขึ้น เช่น การติดตั้งระบบ ป้องกันการบุกรุกระบบเครือข่าย (Firewall) เพื่อเป็นการป้องกันการถูกเจาะหรือสักลอบ (Hack) เข้า สู่ระบบเครือข่ายเป็นการป้องกันบุคคล ไวรัส มิให้เข้าถึงหรือสร้างความเสียหายแก่ข้อมูลหรือการ ทำงานของระบบคอมพิวเตอร์ เป็นต้น

การควบคุมขนาดของความสูญเสีย เป็นวิธีการที่พยายามจะลดความรุนแรงชองความสูญเสีย เมื่อเกิดความสูญเสียขึ้นแล้ว เช่น การติดตั้งอุปกรณ์ดับเพลิง อุปกรณ์เตือนไฟไหม้ เช่น เครื่อง ตรวจจับควันเครื่องตรวจจับความร้อน หรือสัญญาณเตือนภัย เพื่อป้องกันหรือระงับเหตุไฟไหม้ได้ ทันเวลา ในกรณีที่เกิดเหตุการณ์ไฟไหม้ห้อง Server เพื่อเป็นการลดความสูญเสียชองอุปกรณ์ภายใน ห้อง Server ให้มีความเสียหายน้อยที่สุด หรือไม่เกิดความเสียหายหรือกระทบต่อการทำงานชอง ระบบเครือข่าย เป็นต้น

๔. การถ่ายโอน (Transfer) การโอนย้ายหรือแบ่งความเสี่ยงไปให้ผู้อื่นช่วยรับผิดชอบ เช่น อุปกรณ์เครือข่ายเมื่อซื้อมาแล้วมีระยะประกันภัยเพียงหนึ่งปีเพื่อเป็นการรับมือในกรณีที่อุปกรณ์เครือข่ายไม่ทำงานองค์กรอาจเลือกซื้อประกันหรือสัญญาการบำรุงรักษาหลังการขาย เป็นการเพิ่มเติม

ปัจจัยเสี่ยง

ปัจจัยที่จะเกิดความเสียหายกับระบบฐานข้อมูลสารสนเทศ ได้แก่

๑. ปัจจัยภายนอก ได้ แก่

๑.๑ ภัยธรรมชาติและการเกิดสถานการณ์ความไม่สงบที่กระทำต่ออาคารสถานที่ตั้งขอเครื่องประมวลผลหลักหรือ เครื่องแม่ข่ายหลัก (Server) ชองระบบฐานข้อมูล ได้แก่ ไฟไหม้ภัยพิบัติ

๑.๒ การขโมยอุปกรณ์คอมพิวเตอร์แม่ข่ายที่เป็นส่วนของการจัดเก็บและรวบรวมข้อมูล

๑.๓ การชำรุดเสียหายของตัวเครื่องประมวลผลหลัก หรือแม่ข่ายหลัก (Server) จากการเคลื่อนย้ายหรืออื่นๆ

๑.๔ ระบบการสื่อสารของเครือข่ายคอมพิวเตอร์หลักเสียหาย/ขัดข้อง

๑.๕ ระบบกระแสไฟฟ้าขัดข้อง/ ไฟฟ้าดับ

๒. ปัจจัยภายใน ได้แก่

๒.๑ ระบบฐานข้อมูลหลักเสียหาย หรือข้อมูลถูกทำลาย

๒.๒ การถูกไวรัส (Virus) ทำลายฐานข้อมูล และโปรแกรมปฏิบัติการต่างๆ

๒.๓ การถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูลจากบุคคลภายนอก (Hacker) โดยไม่ได้รับ อนุญาต

การประเมินความเสียหาย

๑. ความเสียหายที่เกิดผลเสียหายร้ายแรงที่สุด ซึ่งจะทำให้ต้องหยุดระบบประมวลผลทั้งระบบลง ได้แก่ ภัยธรรมชาติ ตัวเครื่องประมวลผลหลักหรือแม่ข่ายเสียหาย (Server) และระบบฐานข้อมูลหลักถูกทำลายเสียหายจากไวรัส

๒.ความเสียหายที่เกิดผลเสียหายแจะต้องหยุดระบบชั่วขณะ ได้แก่ การถูกเจาะเข้าระบบฐานข้อมูล ระบบสื่อสารของเครือข่ายคอมพิวเตอร์ขัดข้อง และกระแสไฟฟ้าขัดข้อง

การติดตามและรายงานผล

กำหนดให้เจ้าหน้าที่ผู้รับผิดชอบรายงานผลการดำเนินการหรือการตรวจสอบให้ผู้กำกับดูแล ทราบเป็นประจำทุกเดือน และให้รายงานการเกิดปัญหาและผลการแก้ไขให้ทราบในทันทีที่สามารถดำเนินการได้ในทุกกรณี

ระบบรักษาความปลอดภัยบนเครือข่าย

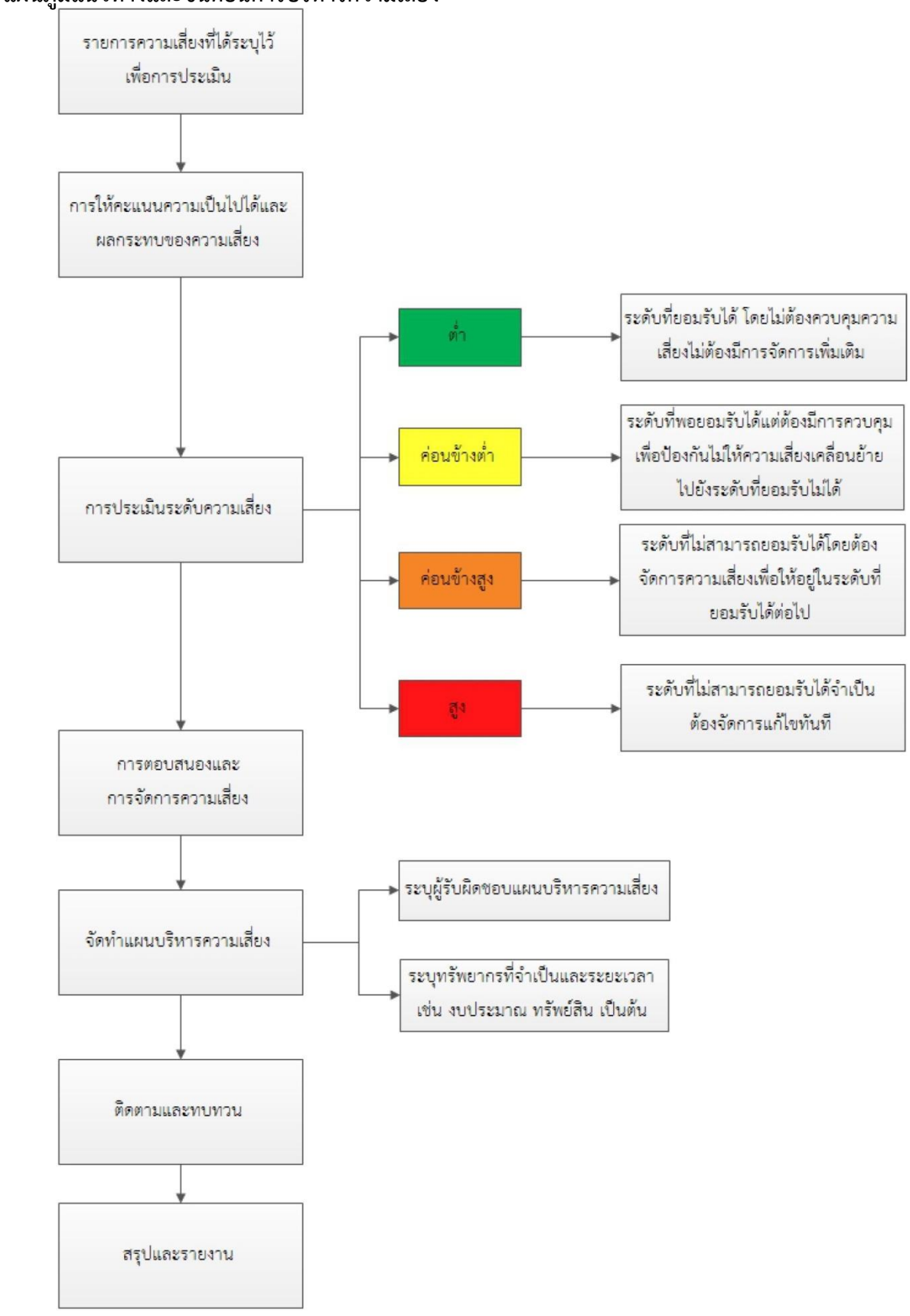
ระบบเครือข่ายคอมพิวเตอร์โรงพยาบาลปากพนัง มีการกำหนดนโยบายและมาตรการในการรักษาความปลอดภัยอย่างเข้มงวดโดยใช้ซอฟต์แวร์เพื่อป้องกันการโจมตีและบุกรุกเข้ามายังเครือข่ายโดยใช้โปรแกรมป้องกันไวรัส และ Firewall เพื่อให้คอมพิวเตอร์ทุกเครื่องที่อยู่ในระบบเครือข่ายได้รับความปลอดภัยและป้องกันความเสียหายที่อาจเกิดขึ้นกับระบบเครือข่ายทั้งหมด

ปัจจุบันเครือข่ายของโรงพยาบาลปากพนัง มีการกำหนดให้ใช้หมายเลข IP Address ประจำหน่วยงานแบบ Private เพื่อเพิ่มความปลอดภัยและสะดวกและรวดเร็วต่อการบริหารจัดการระบบกรณีเกิดปัญหาการใช้งาน

การบริหารความเสี่ยง (Risk Management)

เป็นการปฏิบัติการควบคุมความเสี่ยง ซึ่งจะประกอบด้วยการวางแผนความเสี่ยงการประเมินความเสี่ยงด้านต่างๆ การพัฒนาทางเลือกในการบริหารความเสี่ยง การตรวจสอบความ เสี่ยงเพื่อหาว่าความเสี่ยงได้เปลี่ยนแปลงไปอย่างไร

แผนภูมิแนวทางและขั้นตอนการบริหารความเสี่ยง



ตารางที่ ๑ ลักษณะรายละเอียดของความเสี่ยง (Description of risk)

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ
๑. ความเสี่ยงในการเข้าถึงข้อมูลของบุคคลอื่น	RIT ๐๑	ความเสี่ยงด้านความเป็นส่วนตัวของข้อมูลผู้ป่วย	ผู้ใช้ขาดความระมัดระวังในการเข้าใช้ระบบสารสนเทศ เช่น การมอบหมายให้ผู้อื่นใช้รหัสผ่านของตนเองเข้าใช้ระบบหรือใช้งานแทน	- การอำพรางหรือสวมรอยผู้ใช้ - การเข้าถึงข้อมูล / เปลี่ยนแปลงข้อมูล โดยไม่ได้รับอนุญาต	ผู้ใช้งาน ระบบสารสนเทศ ระบบฐานข้อมูล
๒. ความเสี่ยงจากการนำเอาอุปกรณ์อื่นที่ไม่ได้รับอนุญาตมาเชื่อมต่อ	RIT ๐๒	ความเสี่ยงด้านบริหารจัดการ	ผู้ใช้ขาดความระมัดระวังในการใช้ระบบเครือข่าย เช่น การนำ wireless router หรือ switch/hub มาเชื่อมต่อกับระบบเครือข่ายไม่ได้รับอนุญาต และไม่ได้มีการตั้งค่าเครื่องที่ถูกต้อง ทำให้เครื่องคอมพิวเตอร์อื่นในระบบเครือข่ายไม่สามารถใช้ งานได้ หรือ การไม่ได้ตั้งค่าการรักษาความ ปลอดภัย ทำให้เครื่องคอมพิวเตอร์ของ บุคคลภายนอกอื่นๆที่รับสัญญาณได้ เชื่อมต่อเข้า ลับระบบเครือข่ายของ ทำให้เกิดช่องโหวลับระบบ รักษาความปลอดภัย	- การนำอุปกรณ์อื่นมาเชื่อมต่อเข้าระบบ - ความล้มเหลวทางเทคนิค	ผู้ใช้งาน ผู้ดูแลระบบ ระบบสารสนเทศ ระบบฐานข้อมูล เครื่องคอมพิวเตอร์แม่ข่าย
๓. ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้า ดับ แรงดันไฟฟ้าไม่คงที่	RIT ๐๓	ความเสี่ยงด้านภัยหรือสถานการณ์ฉุกเฉิน	การเกิดกระแสไฟฟ้าขัดข้อง หรือเกิดแรงดันไฟฟ้า ไม่คงที่ ทำให้เครื่องคอมพิวเตอร์และอุปกรณ์อาจ ได้รับความเสียหายจากแรงดันไฟฟ้าที่ไม่คงที่ หรือเมื่อกระแสไฟฟ้าขัดข้อง ทำให้เครื่องแม่ข่ายคอมพิวเตอร์ถูกปิดไปโดยไมสมบูรณ์ อาจทำให้ข้อมูลสารสนเทศบางส่วนเกิดการสูญหาย และ การให้บริการบางประเภทไม่สามารถเปิดใช้งานได้ โดยอัตโนมัติ	- แหล่งกำเนิดไฟฟ้าขัดข้องหรือแรงดันไฟฟ้าไม่คงที่	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่แม่ข่าย อุปกรณ์เครือข่าย เครื่องคอมพิวเตอร์ ระบบฐานข้อมูล ระบบสารสนเทศ

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ
๔. ความเสี่ยงจากการถูกบุก รุกโดยผู้ไม่ประสงค์ดี	RIT ๐๔	ความเสี่ยงด้านด้านความมั่นคงปลอดภัยของทรัพยากรในระบบเทคโนโลยีสารสนเทศ	การบุกรุกโจมตีโดยผู้ไม่ประสงค์ดี เช่น hacker เป็นต้น การดักจับข้อมูล การส่งข้อมูลคำสั่งเจตนา ร้าย การติดไวรัสหรือเวิร์ม	- แฮ็คเกอร์ - แคร็กเกอร์ - การโจมตีการให้บริการ (denial of services/ DOS) - การดักจับข้อมูล - คำสั่งเจตนาร้าย - ความผิดพลาดของซอฟต์แวร์ หรือการเขียนโปรแกรม - ไวรัส/เวิริม	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่แม่ข่าย ระบบฐานข้อมูล ระบบสารสนเทศ
๔. ความเสี่ยงจากการขาด แคลนบุคลากรผู้ปฏิบัติงาน	RIT ๐๔	ความเสี่ยงด้านการบริหารจัดการ	การขาดแคลนบุคลากรด้านสารสนเทศ ทำให้การทำงานอาจหยุดชะงัก หากบุคลากรผู้รับผิดขอบไม่สามารถมาปฏิบัติงานได้ และจำนวนบุคลากรที่มี ไม่เพียงพอต่อระบบเทคโนโลยีสารสนเทศที่ เพิ่มขึ้นตามความต้องการของผู้ใช้งาน ส่งผล กระทบต่อการพัฒนาและควบคุมดูแลระบบ	- นโยบายจากกระทรวง	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย ระบบฐานข้อมูล ระบบสารสนเทศ ผู้รับบริการหรือผู้ป่วย
๖. ความเสี่ยงจากการเปลี่ยนแปลงนโยบายผู้บริหาร	RIT ๐๖	ความเสี่ยงด้านการบริหารจัดการ	การเปลี่ยนแปลงผู้บริหาร อาจทำให้นโยบายการบริหารจัดการสารสนเทศเปลี่ยนแปลงด้วย ทำให้การดำเนินการโครงการต่างๆได้รับผลกระทบ		ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย ระบบฐานข้อมูล ระบบสารสนเทศ
๗. ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ	RIT ๐๗	ความเสี่ยงด้านการบริหารจัดการ	การขาดแคลนงบประมาณในการดำเนินการให้ระบบสารสนเทศสามารถดำเนินการได้ต่อเนื่อง อย่างมีประสิทธิภาพ		ผู้ใช้งาน ผู้ดูแลระบบ ระบบฐานข้อมูล ระบบสารสนเทศ

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ
๘. ความเสี่ยงจากการเกิดไฟไหม้ น้ำท่วม แผ่นดินไหว	RIT ๐๘	ความเสี่ยงด้านภัยหรือสถานการณ์ฉุกเฉิน	การเกิดไฟไหม้อาคาร แผ่นดินไหวจนอาคารถล่ม ไม่สามารถเคลื่อนย้ายเครื่องคอมพิวเตอร์และ อุปกรณ์ต่างๆได้ ทำให้ได้รับความเสียหายทั้งหมด	- ไฟไหม้ จากอุบัติเหตุไฟฟ้า ลัดวงจร การวางเพลิง - ภัยธรรมชาติ	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย ระบบฐานข้อมูล ระบบสารสนเทศ
๙. ความเสี่ยงจากสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง	RIT ๐๙	ความเสี่ยงด้านภัยหรือสถานการณ์ฉุกเฉิน	การเกิดสถานการณ์ความรุนแรง หรือความไม่สงบเรียบร้อย จนทำให้บุคลากรสามารถปฏิบัติงานได้ตามปกติ	- การชุมนุมประท้วง - การจลาจล - การก่อการร้าย	ผู้ใช้งาน ผู้ดูแลระบบ
๑๐. ความเสี่ยงจากเครื่องคอมพิวเตอร์หรืออุปกรณ์ขัดข้อง ไม่สามารถทำงานได้ตามปกติ	RIT ๑๐	ความเสี่ยงด้านบริหารจัดการ	เครื่องคอมพิวเตอร์หรืออุปกรณ์ชำรุดหรือขัดข้องด้วยสาเหตุทางเทคนิค หรือจากสัตว์กัดแทะเช่น หนู หรือแมลง เป็นต้น	- ความล้มเหลวทางเทคนิค - สัตว์ลัดแทะประเภทหนู หรือแมลง	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย
๑๑. ความเสี่ยงจากการโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์	RIT ๑๑	ความเสี่ยงด้านความมั่นคงปลอดภัยของทรัพยากรในระบบเทคโนโลยีสารสนเทศ	การโจรกรรมเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ หรือชิ้นส่วนภายในเครื่อง เช่น CPU และ Ram ทำให้ไม่สามารถปฏิบัติงาน หรือเกิด การสูญหายของข้อมูลบนเครื่องคอมพิวเตอร์นั้นได้	- การลักทรัพย์	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย
๑๒. ความเสี่ยงในการดูแลผู้ป่วย	RIT®U	ความเสี่ยงด้านด้านระบบเทคโนโลยีสารสนเทศอาจทำให้เกิดความบกพร่องในการดูแลรักษาผู้ป่วย	เกิดจากระบบเทคโนโลยีสารสนเทศอาจทำให้เกิดความบกพร่องในการดูแลผู้ป่วย รักษาผู้ป่วย เช่น ข้อมูลผู้ป่วยคนหนึ่งไปอยู่กับผู้ป่วยคนหนึ่ง ข้อมูลไม่ครบถ้วน ขาดหาย ข้อมูลไปถึงผู้ป่วยล่าช้า การ ใช้ Default values ที่ผิดพลาด ข้อมูลใน คอมพิวเตอร์กับในกระดาษไม[1]ตรงกัน การแก้ไข ข้อมูลหลังจากมีผู้ได้รับข้อมูลนั้นไปแล้ว เป็นต้น	- โปรแกรมไม่พร้อมใช้งาน/ทำงานผิดพลาด - การตั้งค่าผิดพลาด - บุคลากรทำงานผิดพลาด	ผู้ป่วย ผู้ใช้งาน ความน่าเชื่อถือโรงพยาบาล

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ป้จจัยเสี่ยง/สิงคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ
๑๓. ความเสี่ยงการเปิดเผยข้อมูลผู้ป่วย	RIT ๑๓	ความเสี่ยงด้านความเป็นส่วนตัวของผู้ป่วย	ผู้ใช้งานขาดความตระหนักเรื่องการเป็ดเผยข้อมูลข้อมูลส่วนบุคคลของผู้ป่วย เช่น ภาพใบหน้า ชื่อ- สกุลผู้ป่วย เตียง ฯลฯ รวมไปถึงการแชร์ข้อมูลใน ลังคมออนไลน์	- การอำพรางหรือสวมรอยของมิจฉาชีพ - การฟ้องร้องจากผู้ป่วยเรื่องการเป็ดเผยข้อมูลส่วนบุคคลก่อนได้รับอนุญาต	ผู้ป่วย ผู้ใช้งาน ความน่าเชื่อถือโรงพยาบาล
๑๔. ความเสี่ยงระบบฐานข้อมูลล่ม/เสียหาย	RIT ๑๔	ความเสี่ยงด้านภัยหรือสถานการณ์ฉุกเฉิน	การเกิดสถานการณ์ฉุกเฉิน หรือฐานข้อมูลล่ม เหลว ไม่สามารถทำงานได้ตามปกติ		ผู้ป่วย ผู้ใช้งาน ผู้ดูแลระบบ

๒. การประมาณความเสี่ยง (Risk estimation)

เป็นการดูปัญหาความเสี่ยงในแง่ของโอกาสการเกิดเหตุ (Incident) หรือเหตุการณ์ (Event) ว่ามี มากน้อยเพียงไรและผลที่ติดตามมาว่ามีความรุนแรงหรือเสียหายมากน้อยเพียงใด

เกณฑ์การประมาณ เป็นการกำหนดเกณฑ์ที่จะใช้ในการประมาณความเสี่ยง ได้แก่ ระดับโอกาส ที่จะเกิดความเสี่ยง ระดับความรุนแรงของผลกระทบ และระดับความเสี่ยง ซึ่งสำนักงานจังหวัด ใช้เกณฑ์ดังนี้

ระดับโอกาสในการเกิดเหตุการณ์ต่าง ๆ (Likeihood) เชิงปริมาณ		
ระดับ	โอกาสที่จะเกิด	คำอธิบาย
๕	สูงมาก	๑ เดือนต่อครั้งหรือมากกว่า
๔	สูง	๑-๖ เดือนต่อครั้ง แต่ไม่เกิน ๕ ครั้งต่อปี
๓	ปานกลาง	๑ ปีต่อครั้ง
๒	น้อย	๒-๓ ปีต่อครั้ง
๑	น้อยมาก	๕ ปีต่อครั้ง

ระดับความรุนแรงของผลกระทบของความเสียง (Impact) เชิงคุณภาพ		
ระดับ	ผลกระทบ	คำอธิบาย
๕	สูงมาก	> ๑๐ ล้านบาท หรือ เกิดความสูญเสียต่อระบบ IT ที่สำคัญทั้งหมดและเกิดความเสียหายอย่างมากต่อความปลอดภัยของข้อมูลต่างๆ
๔	สูง	> ๕ แสนบาท - ๑๐ ล้านบาท หรือ เกิดปัญหาภัยระบบ IT ที่สำคัญ และระบบความปลอดภัยซึ่งส่งผลต่อความถูกต้องของข้อมูลบางส่วน
๓	ปานกลาง	> ๒.๕ แสนบาท - ๕ แสนบาท หรือ ระบบมีปัญหาและมีความสูญเสียไม่มาก
๒	น้อย	> ๑ แสนบาท - ๒.๕ แสนบาท หรือ เกิดเหตุร้ายเล็กน้อยที่แก้ไขได้
๑	น้อยมาก	ไม่เกิน ๑๐๐,๐๐๐ บาท หรือ เกิดเหตุร้ายที่ไม่มีความสำคัญ

ตารางที่ ๒ การประมาณความเสี่ยง (Risk estimation)

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ	โอกาส	ความรุนแรง
๑. ความเสี่ยงในการเข้าถึงข้อมูลของบุคคลอื่น	RIT๐๑	ความเสี่ยงด้านความเป็นส่วนตัวของข้อมูลผู้ป่วย	ผู้ใช้ขาดความระมัดระวังในการเข้าใช้ระบบสารสนเทศ เช่น การมอบหมายให้ผู้อื่นใช้รหัสผ่านของตนเองเข้าใช้ระบบหรือใช้งานแทน	- การอำพรางหรือสวมรอยผู้ใช้ - การเข้าถึงข้อมูล / เปลี่ยนแปลงข้อมูล โดยไม่ได้รับอนุญาต	ผู้ใช้งาน ระบบสารสนเทศ ระบบฐานข้อมูล	๕	๔
๒. ความเสี่ยงจากการนำเอาอุปกรณ์อื่นที่ไม่ได้รับอนุญาตมาเชื่อมต่อ	RIT๐๒	ความเสี่ยงด้านบริหารจัดการ	ผู้ใช้ขาดความระมัดระวังในการใช้ระบบเครือข่าย เช่น การนำ wireless router หรือ switch/hub มาเชื่อมต่อกับระบบเครือข่ายไม่ได้รับอนุญาต และไม่ได้มีการตั้งค่าเครื่องที่ถูกต้อง ทำให้เครื่องคอมพิวเตอร์อื่นในระบบเครือข่ายไม่สามารถใช้งานได้ หรือ การไม่ได้ตั้งค่าการรักษาความปลอดภัย ทำให้เครื่องคอมพิวเตอร์ของบุคคลภายนอกอื่นๆที่รับสัญญาณได้ เชื่อมต่อเข้ากับระบบเครือข่ายของ ทำให้เกิดช่องโหว่กับระบบรักษาความปลอดภัย	- การนำอุปกรณ์อื่นมาเชื่อมต่อเข้าระบบ - ความล้มเหลวทางเทคนิค	ผู้ใช้งาน ผู้ดูแลระบบ ระบบสารสนเทศ ระบบฐานข้อมูล เครื่องคอมพิวเตอร์แม่ข่าย	๔	๕
๓.ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	RIT๐๓	ความเสี่ยงด้านภัยหรือสถานการณ์ฉุกเฉิน	การเกิดกระแสไฟฟ้าขัดข้อง หรือเกิดแรงดันไฟฟ้าไม่คงที่ ทำให้เครื่องคอมพิวเตอร์และอุปกรณ์อาจได้รับความเสียหายจากแรงดันไฟฟ้าที่ไม่คงที่ หรือ เมื่อกระแสไฟฟ้าขัดข้อง ทำให้เครื่องแม่ข่ายคอมพิวเตอร์ถูกปิดไปโดยไม่สมบูรณ์ อาจทำให้ข้อมูลสารสนเทศบางส่วนเกิดการสูญหาย และการให้บริการบางประเภทไม่สามารถเปิดใช้งานได้โดยอัตโนมัติ	- แหล่งกำเนิดไฟฟ้าขัดข้องหรือแรงดันไฟฟ้าไม่คงที่	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่แม่ข่าย อุปกรณ์เครือข่าย เครื่องคอมพิวเตอร์ ระบบฐานข้อมูล ระบบสารสนเทศ	๓	๒

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ	โอกาส	ความรุนแรง
๔.ความเสี่ยงจากการถูกบุกรุก โดยผู้ไม่ประสงค์ดี	RIT๐๔	ความเสี่ยงด้านด้านความมั่นคงปลอดภัยของทรัพยากรในระบบเทคโนโลยีสารสนเทศ	การบุกรุกโจมตีโดยผู้ไม่ประสงค์ดี เช่น hacker เป็นต้น การดักจับข้อมูล การส่งข้อมูลคำสั่งเจตนาร้าย การติดไวรัสหรือเวิร์ม	- แฮ็คเกอร์ - แคร็กเกอร์ - การโจมตีการให้บริการ (denial of services/ DOS) - การดักจับข้อมูล - คำสั่งเจตนาร้าย - ความผิดพลาดของซอฟต์แวร์หรือการเขียนโปรแกรม - ไวรัส/เวิร์ม	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ แม่ข่าย ระบบฐานข้อมูล ระบบสารสนเทศ	๒	๔
๕.ความเสี่ยงจากการขาดแคลนบุคลากรผู้ปฏิบัติงาน	RIT๐๕	ความเสี่ยงด้านการบริหารจัดการ	การขาดแคลนบุคลากรด้านสารสนเทศ ทำให้การทำงานอาจหยุดชะงัก หากบุคลากรผู้รับผิดชอบไม่สามารถมาปฏิบัติงานได้ และจำนวนบุคลากรที่มีไม่เพียงพอต่อระบบเทคโนโลยีสารสนเทศที่เพิ่มขึ้นตามความต้องการของผู้ใช้งาน ส่งผลกระทบต่อการพัฒนาและควบคุมดูแลระบบ	- นโยบายจากกระทรวง	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย ระบบฐานข้อมูล ระบบสารสนเทศ ผู้รับบริการหรือผู้ป่วย	๕	๓
๖.ความเสี่ยงจากการเปลี่ยนแปลงนโยบายผู้บริหาร	RIT๐๖	ความเสี่ยงด้านการบริหารจัดการ	การเปลี่ยนแปลงผู้บริหาร อาจทำให้นโยบายการบริหารจัดการสารสนเทศเปลี่ยนแปลงด้วย ทำให้การดำเนินการโครงการต่างๆได้รับผลกระทบ		ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย ระบบฐานข้อมูล ระบบสารสนเทศ	๑	๑

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ	โอกาส	ความรุนแรง
๗.ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ	RIT๐๗	ความเสี่ยงด้านการบริหารจัดการ	การขาดแคลนงบประมาณในการดำเนินการให้ระบบสารสนเทศสามารถดำเนินการได้ต่อเนื่องอย่างมีประสิทธิภาพ		ผู้ใช้งาน ผู้ดูแลระบบ ระบบฐานข้อมูล ระบบสารสนเทศ	๓	๕
๘.ความเสี่ยงจากการเกิดไฟไหม้ น้ำท่วม แผ่นดินไหว	RIT๐๘	ความเสี่ยงด้านภัยหรือสถานการณ์ฉุกเฉิน	การเกิดไฟไหม้อาคาร แผ่นดินไหวจนอาคารถล่ม ไม่สามารถเคลื่อนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆได้ ทำให้ได้รับความเสียหายทั้งหมด	- ไฟไหม้ จากอุบัติเหตุไฟฟ้าลัดวงจร การวางเพลิง - ภัยธรรมชาติ	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย ระบบฐานข้อมูล ระบบสารสนเทศ	๑	๕
๙.ความเสี่ยงจากสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง	RIT๐๙	ความเสี่ยงด้านภัยหรือสถานการณ์ฉุกเฉิน	การเกิดสถานการณ์ความรุนแรง หรือความไม่สงบเรียบร้อย จนทำให้บุคลากรสามารถปฏิบัติงานได้ตามปกติ	- การชุมนุมประท้วง - การจลาจล - การก่อการร้าย	ผู้ใช้งาน ผู้ดูแลระบบ	๑	๒
๑๐.ความเสี่ยงจากเครื่องคอมพิวเตอร์หรืออุปกรณ์ขัดข้อง ไม่สามารถทำงานได้ตามปกติ	RIT๑๐	ความเสี่ยงด้านบริหารจัดการ	เครื่องคอมพิวเตอร์หรืออุปกรณ์ชำรุดหรือขัดข้องด้วยสาเหตุทางเทคนิค หรือจากสัตว์กัดแทะเช่น หนู หรือแมลง เป็นต้น	- ความล้มเหลวทางเทคนิค - สัตว์กัดแทะประเภทหนู หรือแมลง	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย	๕	๓
๑๑.ความเสี่ยงจากการโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์	RIT๑๑	ความเสี่ยงด้านความมั่นคงปลอดภัยของทรัพยากรในระบบเทคโนโลยีสารสนเทศ	การโจรกรรมเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ หรือชิ้นส่วนภายในเครื่อง เช่น CPU และ Ram ทำให้ไม่สามารถปฏิบัติงาน หรือเกิดการสูญหายของข้อมูลบนเครื่องคอมพิวเตอร์นั้นได้	- การลักทรัพย์	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย	๑	๕

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ	โอกาส	ความรุนแรง
๑๒.ความเสี่ยงในการดูแลผู้ป่วย	RIT๑๒	ความเสี่ยงด้านด้านระบบเทคโนโลยีสารสนเทศอาจทำให้เกิดความบกพร่องในการดูแลรักษาผู้ป่วย	เกิดจากระบบเทคโนโลยีสารสนเทศอาจทำให้เกิดความบกพร่องในการดูแลผู้ป่วย รักษาผู้ป่วย เช่น ข้อมูลผู้ป่วยคนหนึ่งไปอยู่กับผู้ป่วยคนหนึ่ง , ข้อมูลไม่ครบถ้วน ขาดหาย , ข้อมูลไปถึงผู้ป่วยล่าช้า , การใช้ Default values ที่ผิดพลาด , ข้อมูลในคอมพิวเตอร์กับในกระดาษไม่ตรงกัน , การแก้ไขข้อมูลหลังจากมีผู้ได้รับข้อมูลนั้นไปแล้ว เป็นต้น	- โปรแกรมไม่พร้อมใช้งาน/ทำงานผิดพลาด - การตั้งค่าผิดพลาด - บุคลากรทำงานผิดพลาด	ผู้ป่วย ผู้ใช้งาน ความน่าเชื่อถือโรงพยาบาล	๕	๔
๑๓.ความเสี่ยงการเปิดเผยข้อมูลผู้ป่วย	RIT๑๓	ความเสี่ยงด้านความเป็นส่วนตัวของผู้ป่วย	ผู้ใช้งานขาดความตระหนักเรื่องการเปิดเผยข้อมูลข้อมูลส่วนบุคคลของผู้ป่วย เช่น ภาพใบหน้า ชื่อ-สกุลผู้ป่วย เตียง ฯลฯ รวมไปถึงการแชร์ข้อมูลในสังคมออนไลน์	- การอำพรางหรือสวมรอยของมิจฉาชีพ - การฟ้องร้องจากผู้ป่วยเรื่องการเปิดเผยข้อมูลส่วนบุคคลก่อนได้รับอนุญาต	ผู้ป่วย ผู้ใช้งาน ความน่าเชื่อถือโรงพยาบาล	๔	๕
๑๔.ความเสี่ยงระบบฐานข้อมูลล่ม/เสียหาย	RIT๑๔	ความเสี่ยงด้านภัยหรือสถานการณ์ฉุกเฉิน	การเกิดสถานการณ์ฉุกเฉิน หรือฐานข้อมูลล่มเหลว ไม่สามารถทำงานได้ตามปกติ		ผู้ป่วย ผู้ใช้งาน ผู้ดูแลระบบ	๔	๕

๓. การประเมินค่าความเสี่ยง (Risk evaluation)

การประเมินค่าความเสี่ยง จะพิจารณาจากปัจจัยจากขั้นตอนที่ผ่านมาได้แก่ โอกาสที่ภัยคุกคามที่เกิดขึ้นทำให้ระบบขาดความมั่นคง, ระดับผลกระทบหรือความรุนแรงของภัยคุกคามที่มีต่อระบบ และประสิทธิภาพของแผนการควบคุมความปลอดภัยของระบบ การวัดระดับความเสี่ยงมีการกำหนด แผนภูมิความเสี่ยง ที่ได้จากการพิจารณาจัดระดับความสำคัญของความเสี่ยงจากโอกาสที่จะเกิดความเสี่ยง และผลกระทบที่เกิดขึ้น และขอบเขตของระดับความเสี่ยงที่สามารถยอมรับได้

ระดับความเสี่ยง = โอกาสที่จะเกิดหรือความถี่ (P) x ความรุนแรงหรือผลกระทบ (I)

ซึ่งเกณฑ์ในการจัดแบ่งดังนี้

ระดับคะแนนความ	สัญลักษณ์	จัดระดับความเสี่ยง	กลยุทธ์ในการจัดการความเสี่ยง	พื้นที่สี
๑ – ๕	L	ต่ำ	ยอมรับความเสี่ยง	เขียว
๖ – ๙	M	ปานกลาง	ยอมรับความเสี่ยง (มีมาตรการติดตาม)	เหลือง
๑๐ – ๑๗	H	สูง	ควบคุมความเสี่ยง (มีแผนควบคุมความ	ส้ม
๑๘ - ๒๘	HH	สูงมาก	ถ่ายโอนความเสี่ยง	แดง

๓.๑ แผนภูมิความเสี่ยง (Risk Map)

การวัดระดับความเสี่ยง

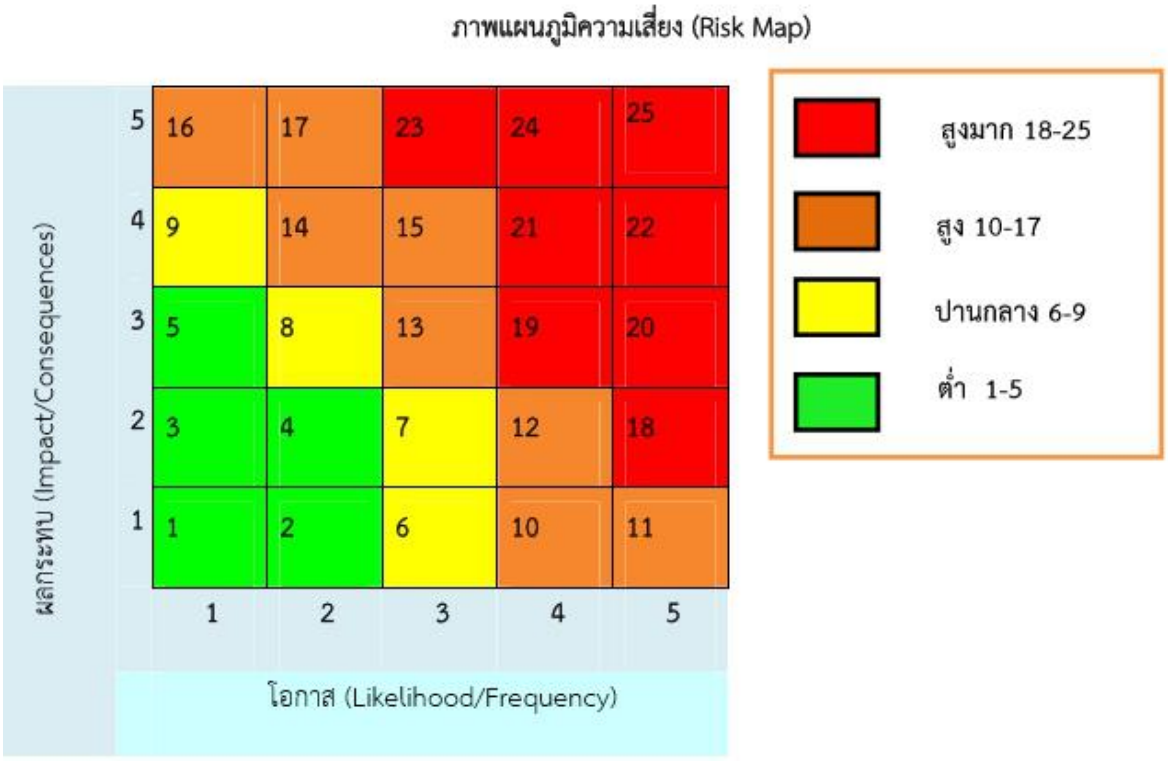
มาก

ผลกระทบ

ความเสี่ยงปานกลาง - ผลกระทบรุนแรงมาก - โอกาสเกิดน้อย	**ความเสี่ยงสูง** - ผลกระทบรุนแรงมาก - โอกาสเกิดมาก
ความเสี่ยงต่ำ - ผลกระทบน้อย - โอกาสเกิดน้อย	**ความเสี่ยงปานกลาง** - ผลกระทบน้อย - โอกาสเกิดมาก

น้อย ——— โอกาสที่จะเกิด ———→ มาก

๓.๒ การประเมินความเสี่ยง



ทั้งนี้ สามารถสรุปผลการประเมินค่าความเสี่ยง แสดงดังตารางที่ ๓ และสามารถแสดงแผนภูมิความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Risk Map) แสดงในรูปที่ ๑

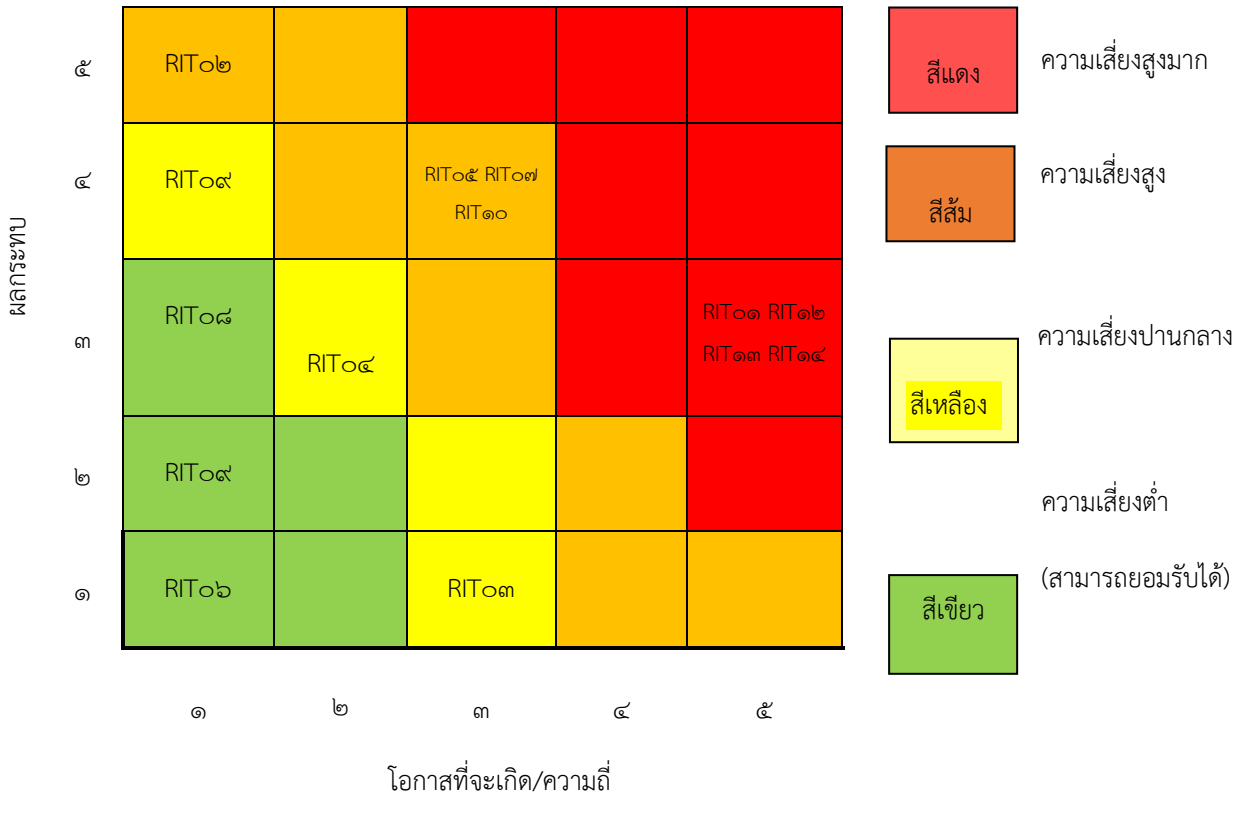
ตารางที่ ๓ สรุปผลการประเมินค่าความเสี่ยง (Risk evaluation)

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	โอกาส / ความถี่	ความรุนแรง	ระดับคะแนน	
๑. ความเสี่ยงในการเข้าถึงข้อมูลของบุคคลอื่น	RIT๐๑	ความเสี่ยงด้านความเป็นส่วนตัวของข้อมูลผู้ป่วย	ผู้ใช้งานขาดความตระหนักเรื่องการเปิดเผยข้อมูลข้อมูลส่วนบุคคลของผู้ป่วย เช่น ภาพใบหน้า ชื่อ-สกุล ผู้ป่วย เตียง ฯลฯ รวมไปถึงการแชร์ข้อมูลในสังคมออนไลน์	๕	๔	๒๐	HH
๒. ความเสี่ยงจากการนำเอาอุปกรณ์อื่นที่ไม่ได้รับอนุญาตมาเชื่อมต่อ	RIT๐๒	ความเสี่ยงด้านบริหารจัดการ	ผู้ใช้ขาดความระมัดระวังในการใช้ระบบเครือข่าย เช่น การนำ wireless router หรือ switch/hub มาเชื่อมต่อกับระบบเครือข่ายไม่ได้รับอนุญาต และไม่ได้มีการตั้งค่าเครื่องที่ถูกต้อง ทำให้เครื่องคอมพิวเตอร์อื่นในระบบเครือข่ายไม่สามารถใช้งานได้ หรือ การไม่ได้ตั้งค่าการรักษาความปลอดภัย ทำให้เครื่องคอมพิวเตอร์ของบุคคลภายนอกอื่นๆที่รับสัญญาณได้เชื่อมต่อเข้ากับระบบเครือข่ายของทำให้เกิดช่องโหว่กับระบบรักษาความปลอดภัย	๔	๔	๑๖	H
๓. ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	RIT๐๓	ความเสี่ยงด้านภัยหรือสถานการณ์ฉุกเฉิน	การเกิดกระแสไฟฟ้าขัดข้อง หรือเกิดแรงดันไฟฟ้าไม่คงที่ ทำให้เครื่องคอมพิวเตอร์และอุปกรณ์อาจได้รับความเสียหายจากแรงดันไฟฟ้าที่ไม่คงที่ หรือ เมื่อกระแสไฟฟ้าขัดข้อง ทำให้เครื่องแม่ข่ายคอมพิวเตอร์ถูกปิดไปโดยไม่สมบูรณ์ อาจทำให้ข้อมูลสารสนเทศบางส่วนเกิดการสูญหาย และการให้บริการบางประเภทไม่สามารถเปิดใช้งานได้โดยอัตโนมัติ	๓	๒	๖	M
๔. ความเสี่ยงจากการถูกบุกรุก โดยผู้ไม่ประสงค์ดี	RIT๐๔	ความเสี่ยงด้านด้านความมั่นคงปลอดภัยของทรัพยากรในระบบเทคโนโลยีสารสนเทศ	การบุกรุกโจมตีโดยผู้ไม่ประสงค์ดี เช่น hacker เป็นต้น การดักจับข้อมูล การส่งข้อมูลคำสั่งเจตนาร้าย การติดไวรัสหรือเวิร์ม	๒	๔	๘	M
๕. ความเสี่ยงจากการขาดแคลนบุคลากร	RIT๐๕	ความเสี่ยงด้านการบริหารจัดการ	การขาดแคลนบุคลากรด้านสารสนเทศ ทำให้การทำงานอาจหยุดชะงัก หากบุคลากรผู้รับผิดชอบ	๕	๓	๒๐	HH

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	โอกาส / ความถี่	ความรุนแรง	ระดับคะแนน	
ผู้ปฏิบัติงาน			ไม่สามารถมาปฏิบัติงานได้ และจำนวนบุคลากรที่มีไม่เพียงพอต่อระบบเทคโนโลยีสารสนเทศที่เพิ่มขึ้นตามความต้องการของผู้ใช้งาน ส่งผลกระทบต่อการพัฒนาและควบคุมดูแลระบบ				
๖. ความเสี่ยงจากการเปลี่ยนแปลงนโยบายผู้บริหาร	RIT๐๖	ความเสี่ยงด้านการบริหารจัดการ	การเปลี่ยนแปลงผู้บริหาร อาจทำให้นโยบายการบริหารจัดการสารสนเทศเปลี่ยนแปลงด้วย ทำให้การดำเนินการโครงการต่างๆได้รับผลกระทบ	๑	๑	๑	L
๗. ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ	RIT๐๗	ความเสี่ยงด้านการบริหารจัดการ	การขาดแคลนงบประมาณในการดำเนินการให้ระบบสารสนเทศสามารถดำเนินการได้ต่อเนื่องอย่างมีประสิทธิภาพ	๓	๕	๒๐	HH
๘. ความเสี่ยงจากการเกิดไฟไหม้ น้ำท่วม แผ่นดินไหว อาคารถล่ม	RIT๐๘	ความเสี่ยงด้านภัยหรือสถานการณ์ฉุกเฉิน	การเกิดไฟไหม้อาคาร แผ่นดินไหวจนอาคารถล่ม ไม่สามารถเคลื่อนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆได้ ทำให้ได้รับความเสียหายทั้งหมด	๑	๕	๕	L
๙. ความเสี่ยงจากสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง	RIT๐๙	ความเสี่ยงด้านภัยหรือสถานการณ์ฉุกเฉิน	การเกิดสถานการณ์ความรุนแรงหรือความไม่สงบเรียบร้อย จนทำให้บุคลากรสามารถปฏิบัติงานได้ตามปกติ	๑	๒	๒	L
๑๐. ความเสี่ยงจากเครื่องคอมพิวเตอร์หรืออุปกรณ์ขัดข้องไม่สามารถทำงานได้ตามปกติ	RIT๑๐	ความเสี่ยงด้านบริหารจัดการ	เครื่องคอมพิวเตอร์หรืออุปกรณ์ชำรุดหรือขัดข้องด้วยสาเหตุทางเทคนิค หรือจากสัตว์กัดแทะเช่น หนูหรือแมลง เป็นต้น	๕	๓	๑๕	H
๑๑. ความเสี่ยงจากการโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์	RIT๑๑	ความเสี่ยงด้านความมั่นคงปลอดภัยของทรัพยากรในระบบเทคโนโลยีสารสนเทศ	การโจรกรรมเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ หรือชิ้นส่วนภายในเครื่อง เช่น CPU และ Ram ทำให้ไม่สามารถปฏิบัติงาน หรือเกิดการสูญหายของข้อมูลบนเครื่องคอมพิวเตอร์นั้นได้	๑	๕	๕	L

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	โอกาส / ความถี่	ความรุนแรง	ระดับคะแนน	
๑๒. ความเสี่ยงในการดูแลผู้ป่วย	RIT๑๒	ความเสี่ยงด้านด้านระบบเทคโนโลยีสารสนเทศอาจทำให้เกิดความบกพร่องในการดูแลรักษาผู้ป่วย	เกิดจากระบบเทคโนโลยีสารสนเทศอาจทำให้เกิดความบกพร่องในการดูแลผู้ป่วย รักษาผู้ป่วย เช่น ข้อมูลผู้ป่วยคนหนึ่งไปอยู่กับผู้ป่วยคนหนึ่ง , ข้อมูลไม่ครบถ้วน ขาดหาย , ข้อมูลไปถึงผู้ป่วยล่าช้า , การใช้ Default values ที่ผิดพลาด , ข้อมูลในคอมพิวเตอร์กับในกระดาษไม่ตรงกัน , การแก้ไขข้อมูลหลังจากมีผู้ได้รับข้อมูลนั้นไปแล้ว เป็นต้น	๕	๔	๒๐	HH
๑๓. ความเสี่ยงการเปิดเผยข้อมูลผู้ป่วย	RIT๑๓	ความเสี่ยงด้านความเป็นส่วนตัวของข้อมูลผู้ป่วย	ผู้ใช้ขาดความระมัดระวังในการเข้าใช้ระบบสารสนเทศ เช่น การมอบหมายให้ผู้อื่นใช้รหัสผ่านของตนเองเข้าใช้ระบบหรือใช้งานแทน	๕	๔	๒๐	HH
๑๔. ความเสี่ยงฐานข้อมูลระบบล่ม/เสียหาย	RIT๑๔	ความเสี่ยงด้านด้านระบบเทคโนโลยีสารสนเทศอาจทำให้เกิดความบกพร่องในการดูแลรักษาผู้ป่วย	ระบบฐานข้อมูลล่ม หรือเสียหายไม่สามารถเชื่อมต่อระบบฐานข้อมูลได้	๔	๕	๒๐	HH

แผนภูมิความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Risk Map)



จากผลการประเมินความเสี่ยง สามารถจัดลำดับความสำคัญของความเสี่ยงด้านเทคโนโลยีสารสนเทศของโรงพยาบาลปากพนัง ในการบริหารจัดการได้อย่างมี ประสิทธิภาพดังนี้

ลำดับ	ความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ค่าระดับความเสี่ยง
๑	RIT๑๒ ความเสี่ยงในการดูแลผู้ป่วย	ความเสี่ยงด้านด้านระบบเทคโนโลยีสารสนเทศอาจทำให้เกิดความบกพร่องในการดูแลรักษาผู้ป่วย	เกิดจากระบบเทคโนโลยีสารสนเทศอาจทำให้เกิดความบกพร่องในการดูแลผู้ป่วย รักษาผู้ป่วย เช่น ข้อมูลผู้ป่วยคนหนึ่งไปอยู่กับผู้ป่วยคนหนึ่ง ข้อมูลไม่ครบถ้วน ขาดหาย ข้อมูลไปถึงผู้ป่วยล่าช้า การใช้ Default values ที่ผิดพลาด ข้อมูลในคอมพิวเตอร์ลับในกระดาษไม่ตรงกัน การแก้ไขข้อมูลหลังจากมีผู้ได้รับข้อมูลนั้นไปแล้ว เป็นต้น	HH
๒	RIT๑๓ ความเสี่ยงในการเข้าถึง ข้อมูลของบุคคลอื่น	ความเสี่ยงด้านด้านความมั่นคงปลอดภัยของทรัพยากรในระบบเทคโนโลยีสารนเทศ	ผู้ใช้ขาดความระมัดระวังในการเข้าใช้ระบบสารสนเทศ เช่น การมอบหมายให้ผู้อื่นใช้รหัสผ่านของ ตนเองเข้าใช้ระบบหรือใช้งานแทน	HH
๓	RIT๑๔ ความเสี่ยงการเปิดเผยข้อมูลผู้ป่วย	ความเสี่ยงด้านความเป็นส่วนตัวของข้อมูลผู้ป่วย	ผู้ใช้ขาดความระมัดระวังในการเข้าใช้ระบบสารลนเทศ เช่น การมอบหมายให้ผู้อื่นใช้รหัสผ่านของ ตนเองเข้าใช้ระบบหรือใช้งานแทน	HH
๔	RIT ๑๔ ความเสี่ยงระบบฐานข้อมูลล่ม/เลียหาย	ด้านระบบเทคโนโลยีสารลนเทศ	ระบบฐานข้อมูลล่ม หรือเลียหายไม่ลามารถเชื่อมต่อระบบฐานข้อมูลได้	HH
๕	RIT๐๗ ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ	ความเสี่ยงด้านการบริหารจัดการ	การขาดแคลนงบประมาณในการดำเนินการให้ระบบสารลนเทศลามารถดำเนินการได้ต่อเนื่องอย่างมีประสิทธิภาพ	H
๖	RIT๐๒ ความเสี่ยงจากการนำเอาอุปกรณ์อื่นที่ไม่ได้รับอนุญาตมาเชื่อมต่อ	ความเสี่ยงด้านการบริหารจัดการ	ผู้ใช้ขาดความระมัดระวังในการใช้ระบบเครือข่าย เช่น การนำ wireless router หรือ switch/hub มาเชื่อมต่อลับระบบเครือข่ายล่านักงานจังหวัด (มหาดไทย) โดยไม่ได้รับอนุญาต และไม่ได้มีการตั้งค่าเครื่องที่ถูกต้อง ทำให้เครื่องคอมพิวเตอร์อื่นในระบบเครือข่ายไม่ลามารถใช้งานได้หรือ การไม[1]ได้ตั้งค่าการรักษาความปลอดลัย ทำให้เครื่องคอมพิวเตอร์ของบุคคลภายนอกอื่นๆที่ รับสัญญาณได้ เชื่อมต่อเข้าลับระบบเครือข่าย	H
๗	RIT๐๕ ความเสี่ยงจากการขาดแคลนบุคลากรผู้ปฏิบัติงาน	ความเสี่ยงด้านการบริหารจัดการ	การขาดแคลนบุคลากรด้านสารสนเทศ ทำให้การทำงานอาจหยุดชะงัก หากบุคลากรผู้รับผิดขอบไม่สามารถมาปฏิบัติงานได้ และจำนวนบุคลากรที่มีไม[1]เพียงพอต่อระบบเทคโนโลยีสารสนเทศที่เพิ่มขึ้นตามความต้องการของผู้ใช้งาน ส่งผลกระทบต่อการพัฒนาและควบคุมดูแลระบบ	H

ลำดับ	ความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ค่าระดับความเสี่ยง
๘	RIT๑๐ ความเสียงจากเครื่องคอมพิวเตอร์หรืออุปกรณ์ขัดข้องไม่สามารถทำงานได้ตามปกติ	ความเสียงจากภัยหรือสถานการณ์ฉุกเฉิน	เครื่องคอมพิวเตอร์หรืออุปกรณ์ชำรุดหรือขัดข้องด้วยสาเหตุทางเทคนิค หรือจากสัตว์ลัดแทะเช่น หนู หรือแมลง เป็นต้น	H
๙	RIT ๐๔ ความเสี่ยงจากการถูก บุกรุก โดยผู้ไม่ประสงค์ดี	ความเสี่ยงด้านด้านความ มั่นคงปลอดภัยของทรัพยากร ในระบบเทคโนโลยีสารสนเทศ	การบุกรุกโจมตีโดยผู้ไม[1]ประสงค์ดี เช่น hacker เป็นต้น การดักจับข้อมูล การส่งข้อมูลคำสั่งเจตนาร้าย การติดไวรัส หรือ เวิร์ม	M
๑๐	RIT๐๓ ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดกระแสไฟฟ้าขัดข้อง หรือเกิดแรงดันไฟฟ้าไม[1]คงที่ ทำให้เครื่องคอมพิวเตอร์และอุปกรณ์อาจได้รับความเสียหายจากแรงดันไฟฟ้าที่ไม่คงที่ หรือ	M
๑๑	RIT๐๘ ความเสี่ยงจากการเกิด ไฟไหม้ แผ่นดินไหว อาคารถล่ม	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดไฟไหม้อาคาร แผ่นดินไหวจนอาคารถล่ม ไม่สามารถเคลื่อนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆได้ ทำให้ได้รับความเสียหายทั้งหมด	L
๑๒	RIT๑๑ ความเสี่ยงจากการโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์	ความเสี่ยงด้านด้านความ มั่นคงปลอดภัยของทรัพยากร ในระบบเทคโนโลยีสารสนเทศ	การโจรกรรมเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ หรือชิ้นส่วนภายในเครื่อง เช่น CPU และ Ram ทำให้ไม่สามารถปฏิบัติงาน หรือเกิดการสูญหายของข้อมูลบนเครื่องคอมพิวเตอร์นั้นได้	L
๑๓	RIT ๐๙ ความเสี่ยงจากสถานการณ์ความไม่สงบ เรียบร้อยในบ้านเมือง	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดสถานการณ์ความรุนแรง หรือความไม[1]สงบเรียบร้อย จนทำให้บุคลากรไม่สามารถปฏิบัติงานได้ตามปกติ	L
๑๔.	RIT๐๖ ความเสี่ยงจากการเปลี่ยนแปลงนโยบายผู้บริหาร	ความเสี่ยงด้านการบริหารจัดการ	การเปลี่ยนแปลงผู้บริหาร อาจทำให้นโยบายการบริหารจัดการสารสนเทศเปลี่ยนแปลงด้วย ทำให้การดำเนินการโครงการต่างๆได้รับผลกระทบ	L

๕. การจัดการความเสี่ยง (Risk management)

นโยบายของกลุ่มงานเทคโนโลยีสารสนเทศทางการแพทย์โรงพยาบาลปากพนัง ระดับความเสี่ยงคงเหลือที่ยอมรับได้ < ๕

กำหนดให้ความเสี่ยงที่จำเป็นต้องนำมาดำเนินการจัดการความเสี่ยงคือ ความเสี่ยงที่มีระดับความเสี่ยงสูง ตั้งแต่ ๑๕ขึ้นไปส่วนความเสี่ยงที่มีระดับความเสี่ยงต่ำกว่า ๑๕ ลือว่ามีความเสี่ยงค่อนข้างต่ำอาจจะนำมาดำเนินการจัดการความสี่ยงในแผนบริหารความสี่ยงหรือไม่ก็ได้ การดำเนินการจัดการความสี่ยงเป็นดังตารางที่ ๕

๑. หลีกเสี่ยงความเสี่ยง (Risk Avoidance = RA) การหลีกเสี่ยงความเสี่ยง เช่น เมื่อพบว่าปัจจุบันโรงพยาบาล มีการสำรองข้อมูลเพียง ๑ ขุดและจัดเป็นความ เสี่ยงต่อการสูญเลีย การเสี่ยงความเสี่ยงนี้อาจได้แก่การทำสำรองข้อมูล ๒ ขุด และแยกเก็บในสถานที่ต่างกัน การบริหารจัดการการเชื่อมโยงสู่เครือข่ายผ่านโมเด็ม ถ้าเป็น การยากต่อการควบคุมหรือบริหารจัดการ องค์กรอาจเลือกทางออกโดยการยกเลิกไม่ให้ใช้บริการ และแนะนำให้พนักงานใช้บริการผ่านทาง ISP ในช่วงที่มีการระบาดของ ไวรัสอย่างหนัก องค์กรอาจมีเลือกระงับไม่ให้ใช้คอมพิวเตอร์ที่ไม่ได้ติดตั้ง Antivirus เป็นต้น

๒. การโอนย้ายความเสี่ยง (Risk Transfer = RF) เช่น อุปกรณ์เครือข่ายเมื่อซื้อมาแล้วมีระยะประกันเพียงหนึ่งปี เพื่อเป็นการรับมือในกรณ์ที่อุปกรณ์เครือข่าย ไม่ทำงาน องค์กรอาจ เลือกซื้อประกัน หรือสัญญาการบำรุงรักษาหลังขาย (Maintenance service) เป็นต้น

๓. การยอมรับความเสี่ยง (Risk acceptance = RC) เป็นการยอมรับในความเสี่ยงโดยไม่ทำอะไร และยอมรับในผลที่อาจตามมา เช่น การพิสูจน์ตัวจริงเพียงใช้ id/ password มีความเสี่ยงเพราะอาจมีการขโมยไปใช้ได้ การให้มีใช้ชีวมาตร (biometrics) เช่น การตรวจลายนิ้วมือหรือม่านตา อาจมีค่าใช้จ่ายสูงไม่คุ้มค่า โรงพยาบาล อาจยอมรับความเสี่ยงของระบบปีจจุบันและทำงานต่อไปโดยไม่ทำอะไร

๔. การลดความเสี่ยง (Loss Reduction = LR) ได้แก่ การมีมาตรการควบคุมมากชนิดขึ้น หรือชนิดที่เข้มงวดมากขึ้นเพื่อลดความเสี่ยง เช่น การใช้ชีวมาตร (biometrics) เพื่อใช้ในการพิสูจน์ตัวจริงนอกเหนือไปจากการใช้ id/ password ที่มีอยู่เดิม

ตารางที่ ๔ การจัดการความเสี่ยง (Risk management)

ลำดับ	ความเสี่ยง	ค่าระดับความเสี่ยง	กลยุทธ์การจัดการความ เสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง	กลยุทธ์
๑	RIT๑๒ ความเสี่ยงในการดูแลผู้ป่วย	๒๐	- ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)	๑. มีระบบติดตามเฝ้าระวัง ได้แก่ ๑.๑ ระบบ Log file ๑.๒ ระบบ Alert แจ้งเตือนต่างๆ ให้ทราบ ได้แก่ ■ ข้อมูลการแพ้ยา ■ ระบบ Drug Interaction ■ นโยบายกำหนดสิทธิการสั่งจ่ายยาโดยแพทย์เฉพาะทาง และบางกรณีต้องผ่านการขออนุมัติก่อนใช้ยา ๒. ควบคุม กำกับ ดูแล โดยคณะกรรมทีมบริหารความเสี่ยงโรงพยาบาลปากพนัง ๓. จัดทำแผนรับสถานการณ์เพื่อให้สามารถดำเนินการได้อย่างต่อเนื่อง	LR
๒	RIT๑๔ ความเสี่ยงระบบฐานข้อมูล ล่ม/เลียหาย	๒๐	- ยอมรับความเสี่ยง - ถ่ายโอนความเสี่ยง - หลีกเลี่ยงความเสี่ยง	๑. ระบบฐานข้อมูลและการบำรุงรักษาหลังขาย (Maintenance service) ได้แก่ ระบบฐานข้อมูลผู้ป่วย HOSxP, ระบบภาพรังสี (PACs) ๒. มีระบบสารองข้อมูลมากกว่า ๑ ชุด กรณีระบบฐานข้อมูลผู้ป่วย	RC RF RA
๓	RIT๑๓ ความเสี่ยงการเปิดเผยข้อมูลผู้ป่วย	๒๐	- ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)	๑. สร้างความตระหนักในเรื่องของข้อมูลส่วนบุคคล ในการพึงรักษาลิทธิในส่วน ของข้อมูลส่วนบุคคล ๒. กำกับดูแลการปฏิบัติตามระเบียบปฏิบัติด้านการรักษาความมั่นคงปลอดภัย สารลนเทศอย่างเคร่งครัด	LR
๔	RIT๐๑ ความเสี่ยงในการเข้าถึงข้อมูลของบุคคลอื่น	๒๐	- ควบคุมความเสี่ยง (มีแผนควบคุมความเลี่ยง)	๑. สร้างความตระหนักในเรื่องของข้อมูลส่วนบุคคล ในการพึงรักษาลิทธิในส่วน ของข้อมูลส่วนบุคคล ๒. กำกับดูแลการปฏิบัติตามระเบียบปฏิบัติด้านการรักษาความมั่นคงปลอดภัย สารลนเทศอย่างเคร่งครัด	LR

ลำดับ	ความเสี่ยง	ค่าระดับความเสี่ยง	กลยุทธ์การจัดการความ เสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง	กลยุทธ์
๕	RIT๐๒ ความเสี่ยงจากการนำเอาอุปกรณ์อื่นที่ไม่ได้รับอนุญาตมาเชื่อมต่อ	๑๖	- ยอมรับความเสี่ยง (มีมาตรการติดตาม)	๑. สร้างความตระหนักในเรื่องนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารลนเทศ ๒. กระตุ้นให้เกิดการปฏิบัติตามแนวนโยบายหรือระเบียบด้านสารสนเทศอย่างจริงจัง ๓. ใช้อุปกรณ์เครือข่ายที่ลามารถจำกัดสิทธิการเข้าถึงลำหรับอุปกรณ์ที่ไม่ได้รับอนุญาตให้เชื่อมต่อเข้าเครือข่าย	RC LR
๖	RIT ๐๔ ความเสี่ยงจากการขาดแคลนบุคลากรผู้ปฏิบัติงาน	๑	- ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)	๑. ปรับปรุงโครงสร้างศูนย์สารสนเทศ และสรรหาบุคลากรเพื่อรองรับงานอย่างเหมาะลม ๒. จัดทำคู่มือกระบวนการทำงานเพื่อให้บุคลากรอื่นลามารถปฏิบัติตามคู่มือได้ กรณีที่บุคลากรผู้รับผิดขอบไม่สามารถมาปฏิบัติงานได้ ๓. จัดตารางเวรและช่องทางการติดต่อลื่อสารตลอด ๒๔ ชั่วโมง	LR
๗	RIT๐๗ ความเสียงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ	๑๕	- ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)	๑. จัดทำแผนแม่บทเทคโนโลยีสารลนเทศ เพื่อแลดงความจำเป็นในการขอสนับสนุนงบประมาณในการดำเนินการต้านเทคโนโลยีสารสนเทศ	LR
๘	RIT๑๐ ความเสี่ยงจากเครื่องคอมพิวเตอร์หรืออุปกรณ์ขัดข้อง ไม่สามารถทำงานได้ตามปกติ	๕	- ยอมรับความเสี่ยง (มีมาตรการติดตาม)	๑. หาทางบีองกันสัตว์กัดแทะอุปกรณ์ ๒. จัดหาเครื่องและอุปกรณ์ลำรองเพื่อให้ลามารถใช้ทดแทนชั่วคราว เพื่อสามารถปฏิบัติงานได้ ๓. จัดทำแผนการตรวจลอบและจัดจ้างบำรุงรักษาเครื่องและอุปกรณ์อย่างสม่ำเสมอ	RC RA
๙	RIT๐๔ ความเสี่ยงจากการถูกบุกรุกโดยผู้ไม่ประสงค์	๘	- ยอมรับความเสี่ยง	- ตรวจลอบการตั้งค่าของ firewall อย่างสม่ำเสมอ - ติดตั้งระบบตรวจลอบการบุกรุกเครือข่าย และติดตามเพื่อปรับปรุงอย่างสม่ำเสมอ - ติดตั้งโปรแกรมป้องกันไวรัส และ patch อย่างสม่ำเสมอ - ติดตั้ง patch ของระบบปฏิบัติการอย่างสม่ำเสมอ - เปลี่ยนรหัสผ่านตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ	RC RA
๑๐	RIT๐๓ ความเสียงจากกระแสไฟฟ้า	๖	- ยอมรับความเสี่ยง	- จัดหาเครื่องกำเนิดไฟฟ้า และเครื่องสำรองไฟฟ้าแบบป้องกันปัญหา	RC

ลำดับ	ความเสี่ยง	ค่าระดับความเสี่ยง	กลยุทธ์การจัดการความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง	กลยุทธ์
	ขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่		(มีมาตรการติดตาม)	แรงดันไฟฟ้าไม่คงที่ - โรงพยาบาลมีระบบไฟฉุกเฉินอัตโนมัติใช้(เวลา ๕ วินาที) - จัดทำแผนรับสถานการณ์เพื่อให้สามารถดำเนินการได้อย่างต่อเนื่อง (Business Continuity Plan : BCP)	RA
๑๑	RIT๐๘ ความเสี่ยงจากการเกิดไฟไหม้ แผ่นดินไหว อาคารถล่ม	๕	- ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)	๑. จัดทำแผนรับสถานการณ์เพื่อให้สามารถดำเนินการได้อย่างต่อเนื่อง (Business Continuity Plan : BCP) , แผนกู้คืนระบบ DRP ๒. จัดหาระบบสำรองเพื่อให้ระบบสารสนเทศสามารถทำงานได้ ๓. สำรองข้อมูลระบบ และฐานข้อมูลเก็บไว้ในสถานที่อื่นอีกหนึ่งชุด	RC
๑๒	RIT๑๑ ความเสี่ยงจากการโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์	๕	- ยอมรับความเสี่ยง	- ตรวจสอบการเข้าออกของบุคคลภายนอก - ตรวจสอบระบบการป้องกันรักษาความปลอดภัยของสถานที่ให้อยู่ในสภาพปกติ - ติดตั้งกล้องวงจรปิดเพื่อเฝ้าระวัง	RC
๑๓	RIT๐๙ ความเสี่ยงจากสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง	๒	- ยอมรับความเสี่ยง	- จัดทำแผนรับสถานการณ์เพื่อให้สามารถดำเนินการได้อย่างต่อเนื่อง (Business Continuity Plan : BCP) - จัดหาระบบสำรองเพื่อให้ระบบสารสนเทศสามารถทำงานได้	RC
๑๔	RIT๐๖ ความเสี่ยงจากการเปลี่ยนแปลงนโยบายผู้บริหาร	๑	- ยอมรับความเสี่ยง		RC

แผนการดูแลจัดการรักษาและแก้ไขปัญหาระบบข้อมูลสารสนเทศ

แผนการดูแลจัดการรักษาและแก้ไขปัญหาระบบข้อมูลสารสนเทศ

ประเภทความเสี่ยง/กิจกรรม	แนวทางการควบคุม	ระยะเวลาเริ่มต้น/สิ้นสุด	ปีงบประมาณ												หมายเหตุ
			ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	
๑. ความเสี่ยงด้านความเสียหายของระบบสารสนเทศและข้อมูลสารสนเทศ															
๑.๑ ระบบฐานข้อมูล/โปรแกรมที่ให้บริการเกิดความเสียหาย	- จัดทำการสำรอง ข้อมูลแบบอัตโนมัติ - จัดทำการสำรอง ข้อมูลแบบไม่อัตโนมัติ - ทดสอบการกู้คืน ฐานข้อมูลและระบบสารสนเทศ	- ทุกวัน/ทุกสัปดาห์ - ทุกวัน/ทุกสัปดาห์ - ทุกเดือน	←											→	
๑.๒ ข้อมูลเสียหายเกิดจากอุปกรณ์บันทึกข้อมูล (Hard disk) ชำรุด	- จัดทำการสำรอง ข้อมูลแบบอัตโนมัติ - จัดทำการสำรอง ข้อมูลแบบไม่อัตโนมัติ -ทดสอบการกู้คืน ฐานข้อมูลและระบบสารสนเทศ	-ทุกวัน/ทุก สัปดาห์ -ทุกเดือน -ทุกเดือน	←											→	

แผนการดูแลจัดการรักษาและแก้ไขปัญหาระบบข้อมูลสารสนเทศ

ประเภทความเสี่ยง/กิจกรรม	แนวทางการควบคุม	ระยะเวลาเริ่มต้น/สิ้นสุด	ปีงบประมาณ												หมายเหตุ
			ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	
๒. ความเสี่ยงด้านภัยพิบัติระบบสารสนเทศ															
๒.๑ ไฟไหม้ห้อง Server	- ตรวจสอบความพร้อมของการใช้งานอุปกรณ์ดับเพลิง	- ทุกเดือน	←											→	
๒.๒ ระบบเครือข่ายสื่อสารหลักเสียหาย/ ขัดข้อง	- ตรวจสอบระบบเครือข่ายสื่อสารหลัก -	- ทุกเดือน	←											→	
๓. ความเสี่ยงด้านความมั่นคง และปลอดภัยของระบบฐานข้อมูล															
๓.๑ ระบบกระแสไฟฟ้าขัดข้อง /ไฟฟ้าดับ	- ตรวจสอบระบบสำรองไฟฟ้า (UPS)	- ทุกเดือน	←											→	
๓.๒ การถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบประมวลผลของเครื่อง Server	- ตรวจสอบระบบป้องกันการบุกรุกระบบเครือข่าย (Firewall)	- ทุกเดือน	←											→	
๓.๓ การถูกเจาะหรือลักลอบ (Hack) ระบบฐานข้อมูล	- ตรวจสอบระบบป้องกันการบุกรุก ระบบเครือข่าย(Firewall)	- ทุกเดือน	←											→	

แผนการดูแลจัดการรักษาและแก้ไขปัญหาระบบข้อมูลสารสนเทศ

ประเภทความเสี่ยง/กิจกรรม	แนวทางการควบคุม	ระยะเวลาเริ่มต้น/สิ้นสุด	ปีงบประมาณ												หมายเหตุ
			ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	
๔. ความเสี่ยงด้านสิทธิการใช้งานของผู้ใช้งานในแต่ละระดับ															
๔.๑ การเข้าใช้ระบบเครือข่ายคอมพิวเตอร์ภายในองค์กรโดยไม่ได้รับอนุญาต	- กำหนดสิทธิ์ในการ เข้าถึงข้อมูล	- เมื่อแต่งตั้ง /โยกย้าย / ลาออก / เกษียณอายุ ราชการ	←											→	
๕. อุปกรณ์คอมพิวเตอร์เสียหาย															
๕.๑ คอมพิวเตอร์ไม่สามารถใช้งานได้	- บำรุงรักษา คอมพิวเตอร์ เช่น เป่าฝุ่น สแกน ฮาร์ดดิสค์ disk cleanup และ disk defragmenter	- ทุก ๓ เดือน			✓			✓			✓			✓	