แนวทางการบริหารความเสี่ยง

1. แนวทางดำเนินงานและกลไกการบริหารความเสี่ยง

1.1 แนวทางดำเนินงาน ในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ โรงพยาบาลภูเพียง แบ่งเป็น 2 ระยะ ดังนี้

ระยะที่ 1 การเริ่มต้นและพัฒนา

1) กำหนดนโยบายหรือแนวทางในการบริหารจัดการความเสี่ยง
2) ระบุปัจจัยเสี่ยง และประเมินโอกาส ผลกระทบจากปัจจัยเสี่ยง
3) วิเคราะห์และจัดลำดับความสำคัญของปัจจัยเสี่ยงจากการดำเนินงาน
4) จัดทำแผนบริหารความเสี่ยงของปัจจัยเสี่ยงที่อยู่ในระดับสูง (High) และสูงมาก (Extreme) รวมทั้งปัจจัยเสี่ยงที่อยู่ในระดับปานกลาง (Medium) ที่มีนัยสำคัญ
5) สื่อสารทำความเข้าใจเกี่ยวกับแผนบริหารความเสี่ยงให้ผู้ปฏิบัติงานของกลุ่มงานสารสนเทศ ทาง การแพทย์ รับทราบและสามารถนำไปปฏิบัติได้
6) รายงานความก้าวหน้าของการดำเนินงานตามแผนบริหารความเสี่ยง พร้อมทั้งติดตามการ ดำเนินงาน
7) รายงานสรุปการประเมินผลความสำเร็จของการดำเนินการตามแผนบริหารความเสี่ยง

ระยะที่ 2 การพัฒนาสู่ความยั่งยืน

1) ทบทวนแผนบริหารความเสี่ยงในปีที่ผ่านมา
2) พัฒนากระบวนการบริหารความเสี่ยงสำหรับความเสี่ยงแต่ละประเภท
3) ผลักดันให้มีการบริหารความเสี่ยงทั่วทั้งองค์กร
4) พัฒนาขีดความสามารถบุคลากรในการดำเนินงานตามกระบวนการบริหารความเสี่ยง

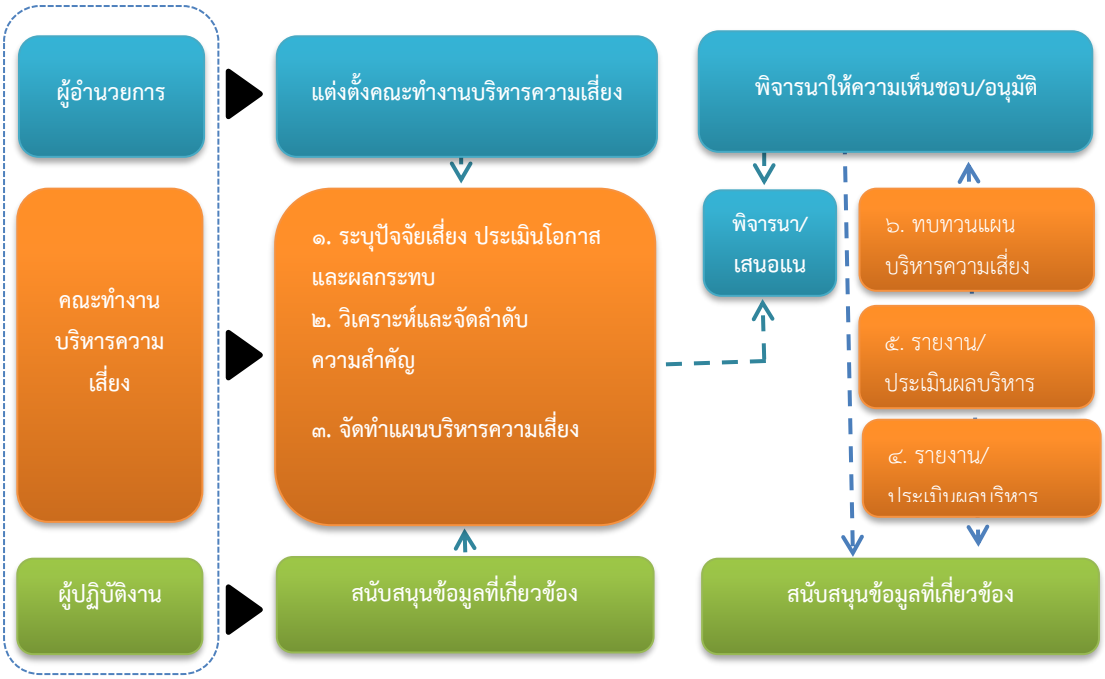
1.2 กลไกการบริหารความเสี่ยง ประกอบด้วย

1) ผู้อำนวยการ มีหน้าที่แต่งตั้งคณะทำงานบริหารความเสี่ยง ส่งเสริมให้มีการบริหารจัดการความ เสี่ยงอย่างมีประสิทธิภาพและเหมาะสม รวมทั้งพิจารณาให้ความเห็นชอบหรืออนุมัติแผนการ บริหารความเสี่ยงเพื่อนำไปปฏิบัติต่อไป

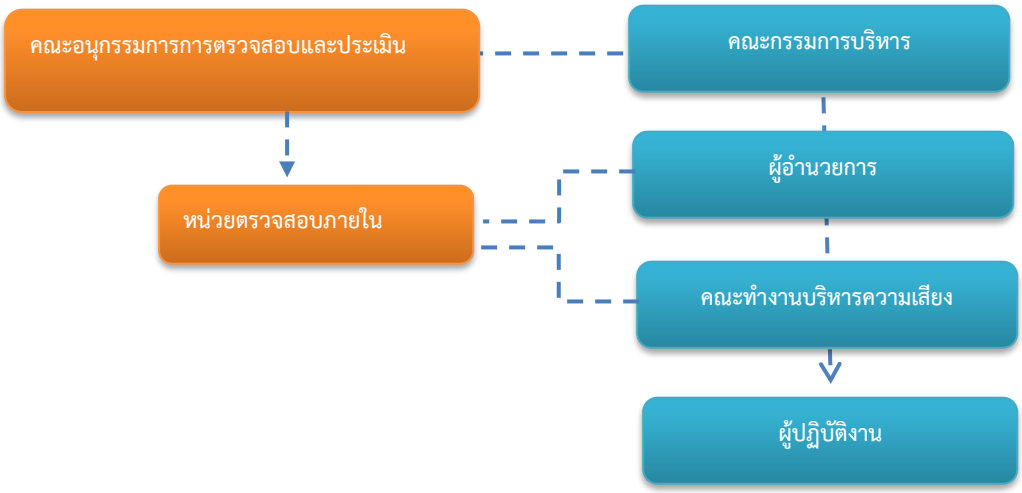
2) คณะทำงานบริหารความเสี่ยง มีหน้าที่ดำเนินการให้มีระบบการบริหารความเสี่ยง จัดทำแผน บริหารความเสี่ยง รายงานและประเมินผลการดำเนินงานตามแผนการบริหารความเสี่ยง รวมทั้ง ทบทวน แผนการบริหารความเสี่ยงเพื่อปรับปรุงการดำเนินงานต่อไปในอนาคต

3) ผู้ปฏิบัติงาน บุคลากรที่มีหน้าที่สนับสนุนข้อมูลที่เกี่ยวข้องให้กับคณะทำงานบริหารความเสี่ยง และให้ความร่วมมือในการปฏิบัติงานตามแผนบริหารความเสี่ยง

กลไกการบริหารความเสี่ยง



2. โครงสร้างการบริหารความเสี่ยง



หน้าที่ความรับผิดชอบตามโครงสร้าง

โครงสร้างการบริหารความเสี่ยง ประกอบไปด้วย การกำกับดูแล การตัดสินใจ การจัดทำแผน การดำเนินการ การติดตามประเมินผล และการสอบทาน ซึ่งในแต่ละองค์ประกอบมีอำนาจหน้าที่ดังนี้

2.1 คณะกรรมการบริหาร

1) ส่งเสริมให้มีการดำเนินงานบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ
2) ให้ความเห็นชอบและให้ข้อเสนอแนะต่อระบบและแผนการบริหารจัดการความเสี่ยง
3) รับทราบผลการบริหารความเสี่ยงและเสนอแนะแนวทางการพัฒนา

2.2 คณะอนุกรรมการตรวจสอบและประเมิน

1) ส่งเสริมและสนับสนุนให้การบริหารความเสี่ยงเป็นส่วนหนึ่งของการดำเนินงานเพื่อเพิ่มมูลค่าให้กับองค์การ
2) รับทราบผลการบริหารความเสี่ยงและให้ข้อเสนอแนะเพื่อพัฒนาระบบการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ
3) กำกับดูแลการพัฒนาและการปฏิบัติตามกรอบการบริหารความเสี่ยง

2.3 ผู้อำนวยการ

1) แต่งตั้งคณะทำงานบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ
2) ส่งเสริมและติดตามให้มีการบริหารความเสี่ยงอย่างมีประสิทธิภาพและเหมาะสม
3) พิจารณาให้ความเห็นชอบและอนุมัติแผนการบริหารความเสี่ยง
4) พิจารณาผลการบริหารความเสี่ยงและเสนอแนะแนวทางการพัฒนา

2.4 หน่วยตรวจสอบภายใน

1) สอบทานกระบวนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ
2) นำเสนอผลการบริหารความเสี่ยงให้คณะอนุกรรมการตรวจสอบและประเมินรับทราบและให้ข้อเสนอแนะ

2.5 คณะทำงานบริหารความเสี่ยง

1) จัดให้มีระบบและกระบวนการบริหารความเสี่ยงที่เป็นระบบมาตรฐานเดียวกันทั้งองค์กร
2) ดำเนินการตามกระบวนการบริหารความเสียง และการปฏิบัติตามมาตรการลดและควบคุมความเสี่ยง
3) รายงานและติดตามผลการดำเนินงานตามแผนการบริหารความเสี่ยงที่สำคัญ เสนอต่อผู้อำนวยการเพื่อพิจารณา

2.6 ผู้ปฏิบัติงาน

1) สนับสนุนข้อมูลที่เกี่ยวข้องให้กับคณะทำงานบริหารความเสี่ยง
2) ให้ความร่วมมือในการปฏิบัติงานตามแผนบริหารความเสี่ยง

กระบวนการบริหารความเสี่ยง

กระบวนการบริหารความเสี่ยง เป็นกระบวนการที่ใช้ในการระบุ วิเคราะห์ ประเมิน และจัดลำดับความเสี่ยงที่มีผลกระทบต่อการบรรลุวัตถุประสงค์ในการดำเนินงานขององค์กร รวมทั้งการจัดทำแผนบริหารจัดการความเสี่ยง โดย กำหนดแนวทางการควบคุมเพื่อป้องกันหรือลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ ซึ่งกลุ่มงานสารสนเทศทาง การแพทย์มีขั้นตอนหรือกระบวนการบริหารความเสี่ยง 6 ขั้นตอนหลัก ดังนี้

1. การระบุความเสี่ยง (Risk identification)

เป็นกระบวนการที่ผู้บริหารและผู้ปฏิบัติงาน ร่วมกันระบุความเสี่ยงและปัจจัยเสี่ยง โดยต้องคำนึงถึงความเสี่ยงที่มีสาเหตุมาจากปัจจัยทั้งภายในและภายนอก ปัจจัยเหล่านี้มีผลกระทบต่อวัตถุประสงค์และเป้าหมายขององค์กร หรือ ผลการปฏิบัติงานทั้งในระดับองค์กรและระดับกิจกรรม ในการระบุปัจจัยเสี่ยงจะต้องพิจารณาว่ามีเหตุการณ์ใดหรือ กิจกรรมใดของกระบวนการปฏิบัติงานที่อาจเกิดความผิดพลาดความเสียหายและไม่บรรลุวัตถุประสงค์ที่กำหนดรวมทั้ง มีทรัพย์สินใดที่จำเป็นต้องได้รับการดูแลป้องกันรักษา ดังนั้นจึงจำเป็นต้องเข้าใจในความหมายของ “ความเสี่ยง (Risk)” “ปัจจัยเสี่ยง (Risk Factor)” และ “ประเภทความเสี่ยง” ก่อนที่จะดำเนินการระบุความเสี่ยงได้อย่างเหมาะสม

1.1 ความเสี่ยง (Risk)

หมายถึง เหตุการณ์หรือการกระทำใดๆ ที่อาจเกิดขึ้นภายใต้สถานการณ์ที่ไม่แน่นอนและจะส่งผลกระทบหรือสร้างความเสียหาย (ทั้งที่เป็นตัวเงินและไม่เป็นตัวเงิน) หรือก่อให้เกิดความล้มเหลว หรือลดโอกาสที่จะบรรลุเป้าหมายตามภารกิจหลักขององค์กร และเป้าหมายตามแผนปฏิบัติงาน

1.2 ปัจจัยเสี่ยง (Risk Factor)

หมายถึง ต้นเหตุ หรือสาเหตุที่มาของความเสี่ยง ที่จะทำให้ไม่บรรลุวัตถุประสงค์ที่กำหนดไว้ โดยต้องระบุได้ด้วยว่าเหตุการณ์นั้นจะเกิดที่ไหน เมื่อใด และเกิดขึ้นได้อย่างไร และทำไม ทั้งนี้สาเหตุของความเสี่ยงที่ระบุควรเป็น สาเหตุที่แท้จริง เพื่อจะได้วิเคราะห์และกำหนดมาตรการลดความเสี่ยงในภายหลังได้อย่างถูกต้อง
โดยปัจจัยเสี่ยงแบ่งได้ 2 ด้าน ดังนี้

1) ปัจจัยเสี่ยงภายนอก คือ ความเสี่ยงที่ไม่สามารถควบคุมการเกิดได้โดยองค์กร เช่น เศรษฐกิจ สังคม การเมือง กฎหมาย คู่แข่ง เทคโนโลยี ภัยธรรมชาติ สิ่งแวดล้อม

2) ปัจจัยเสี่ยงภายใน คือ ความเสี่ยงที่สามารถควบคุมได้โดยองค์กร เช่น กฎระเบียบ ข้อบังคับ ภายในองค์กร วัฒนธรรมองค์กร นโยบายการบริหารและการจัดการ ความรู้/ความสามารถของบุคลากรกระบวนการทำงาน ข้อมูล/ระบบสารสนเทศ เครื่องมือ/อุปกรณ์

1.3 ประเภทความเสี่ยง

จากการวิเคราะห์ความเสี่ยงด้านสารสนเทศของโรงพยาบาลภูเพียงสามารถแยกประเภทความเสี่ยงเป็น 5 ประเภท ดังนี้

- ความเสี่ยงด้านความมั่นคงปลอดภัยของทรัพยากรในระบบเทคโนโลยีสารสนเทศ
  Hardwar , Software , Network , Data
- ความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศอาจทำให้เกิดความบกพร่องในการดูแลรักษาผู้ป่วย เป็นความเสี่ยงที่อาจเกิดขึ้นจากระบบเทคโนโลยีสารสนเทศที่ส่งผลกระทบต่อการรักษาผู้ป่วย ทำให้ข้อมูลผิดพลาด ไม่ถูกต้องตรงกัน ข้อมูลที่สำคัญไม่อยู่ระบบ ข้อมูลที่จำเป็นและสำคัญไปถึงผู้ป่วยหรือผู้ให้บริการล่าช้า จนทำให้เกิดความบกพร่องในการ ดูแลรักษาผู้ป่วย เช่น ข้อมูลผู้ป่วยคนหนึ่งไปอยู่กับผู้ป่วยคนหนึ่ง , ข้อมูลไม่ครบถ้วน ขาดหาย , ข้อมูลไปถึงผู้ป่วยล่าช้า

, การใช้ Default values ที่ผิดพลาด , ข้อมูลในคอมพิวเตอร์กับในกระดาษไม่ตรงกัน , การแก้ไขข้อมูลหลังจากมีผู้ ได้รับข้อมูลนั้นไปแล้ว เป็นต้น

● ความเสี่ยงด้านความเป็นส่วนตัวของผู้ป่วย เป็นความเสี่ยงที่อาจเกิดขึ้นจากการดำเนินการการจัดความสำคัญ ในการเข้าถึงข้อมูลไม่เหมาะสมกับการใช้งานหรือการให้บริการ โดยผู้ใช้อาจเข้าสู่ระบบเทคโนโลยีสารสนเทศของ โรงพยาบาลภูเพียง หรือใช้ข้อมูลต่างๆ ของโรงพยาบาลภูเพียง เกินกว่า อำนาจหน้าที่ของตน เองที่มีอยู่และอาจทำให้เกิดความเสียหายต่อข้อมูลสารสนเทศได้ความเสี่ยงจากผู้ปฏิบัติงาน เป็น ความเสี่ยงที่อาจเกิดขึ้น

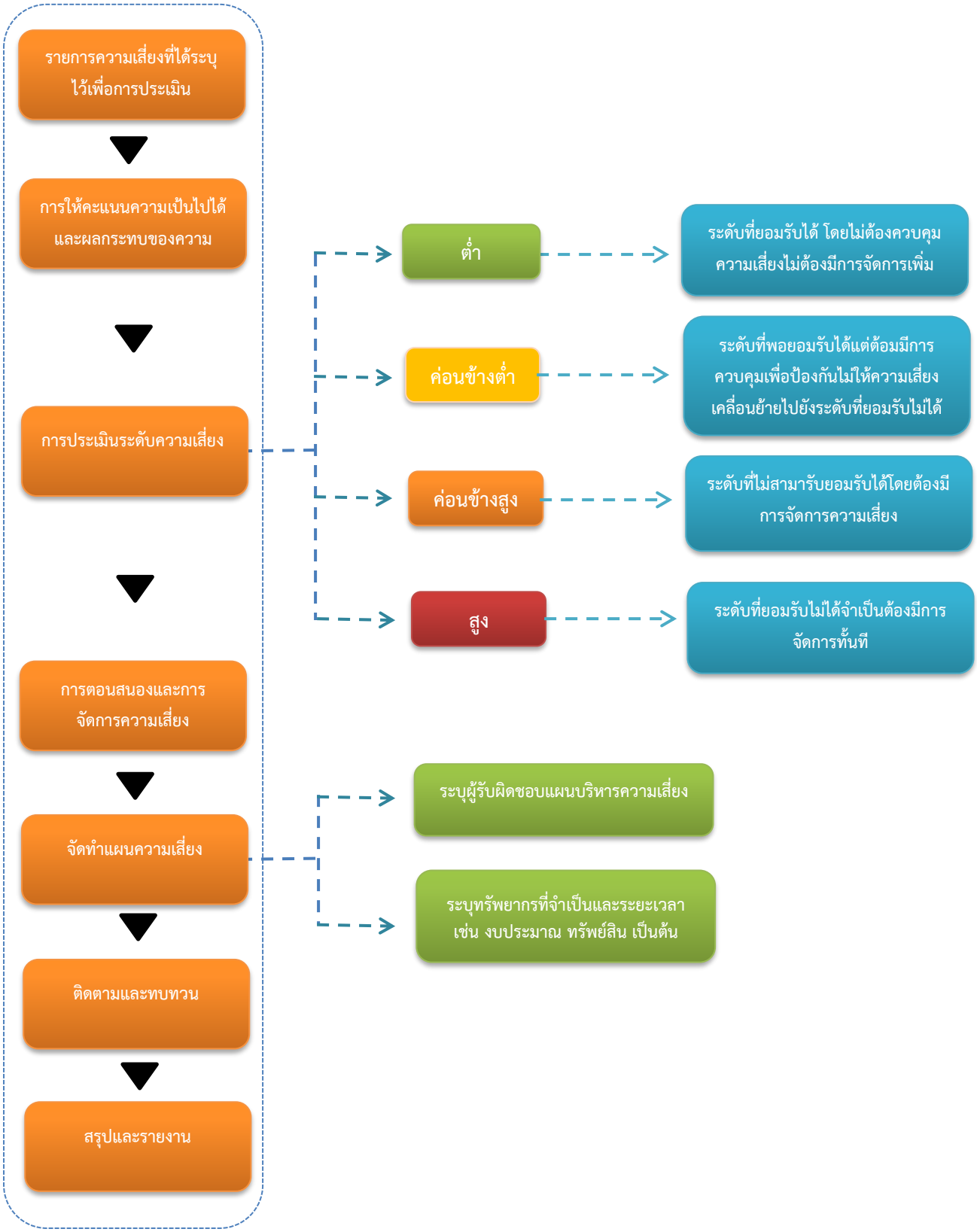
จากการดำเนินการการจัดความสำคัญในการเข้าถึงข้อมูลไม่เหมาะสมกับการใช้งานหรือการ ให้บริการ โดยผู้ใช้อาจเข้าสู่ระบบเทคโนโลยีสารสนเทศ หรือใช้ข้อมูลต่างๆ ของโรงพยาบาลภูเพียง เกินกว่าอำนาจหน้าที่ของตนเองที่มีอยู่และอาจทำให้เกิดความเสียหายต่อข้อมูลสารสนเทศได้

● ความเสี่ยงด้านภัยหรือสถานการณ์ฉุกเฉิน เป็นความเสี่ยงที่อาจเกิดจากภัยพิบัติตามธรรมชาติหรือสถานการณ์ ร้ายแรงที่ก่อให้เกิดความเสียหายร้ายแรงกับข้อมูลสารสนเทศ เช่น ไฟฟ้าขัดข้อง น้ำท่วม ไฟไหม้ อาคารถล่ม การ ชุมนุมประท้วง หรือความไม่สงบเรียบร้อยในบ้านเมือง เป็นต้น

● ความเสี่ยงด้านการบริหารจัดการ เป็นความเสี่ยงจากแนวนโยบายในการบริหารจัดการที่อาจส่งผลกระทบต่อ การดำเนินการด้านเทคโนโลยีสารสนเทศ

.

แผนภูมิแนวทางและขั้นตอนการบริหารความเสี่ยง



ตารางที่ 1 ลักษณะรายละเอียดของความเสี่ยง (Description of risk)

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ
1. ความเสี่ยงในกาเข้าถึงข้อมูลของบุคคลอื่น	RIT01	ความเสี่ยงด้านความเป็นส่วนตัวของข้อมูลผู้ป่วย	ผู้ใช้ขาดความระมัดระวังในการเข้าใช้ระบบสารสนเทศ เช่น การมอบหมายให้ผู้อื่นใช้รหัสผ่านของตนเองเข้าใช้ระบบหรือใช้งานแทน	- การอำพรางหรือสวมรอยผู้ใช้ - การเข้าถึงข้อมูล / เปลี่ยนแปลงข้อมูล โดยไม่ได้รับอนุญาต	ผู้ใช้งาน ระบบสารสนเทศ ระบบฐานข้อมูล
2. ความเสี่ยงจากการนำเอาอุปกรณ์อื่นที่ไม่ได้รับอนุญาตมาเชื่อมต่อ	RIT02	ความเสี่ยงด้านบริหารจัดการ	ผู้ใช้ขาดความระมัดระวังในการใช้ระบบเครือข่าย เช่น การนำ wireless router หรือ switch/hub มาเชื่อมต่อกับระบบเครือข่ายไม่ได้รับอนุญาต และไม่ได้มีการตั้งค่าเครื่องที่ถูกต้อง ทำให้เครื่องคอมพิวเตอร์อื่นในระบบเครือข่ายไม่สามารถใช้งานได้ หรือ การไม่ได้ตั้งค่าการรักษาความปลอดภัย ทำให้เครื่องคอมพิวเตอร์ของบุคคลภายนอกอื่นๆที่รับสัญญาณได้ เชื่อมต่อเข้ากับระบบเครือข่ายของ ทำให้เกิดช่องโหว่กับระบบรักษาความปลอดภัย	- การนำอุปกรณ์อื่นมาเชื่อมต่อเข้าระบบ - ความล้มเหลวทางเทคนิค	ผู้ใช้งาน ผู้ดูแลระบบ ระบบสารสนเทศ ระบบฐานข้อมูล เครื่องคอมพิวเตอร์แม่ข่าย
3. ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	RIT03	ความเสี่ยงด้านภัยหรือสถานการณ์ฉุกเฉิน	การเกิดกระแสไฟฟ้าขัดข้อง หรือเกิดแรงดันไฟฟ้าไม่คงที่ ทำให้เครื่องคอมพิวเตอร์และอุปกรณ์อาจได้รับความเสียหายจากแรงดันไฟฟ้าที่ไม่คงที่ หรือเมื่อกระแสไฟฟ้าขัดข้อง ทำให้เครื่องแม่ข่ายคอมพิวเตอร์ถูกปิดไปโดยไม่สมบูรณ์ อาจทำให้ข้อมูลสารสนเทศบางส่วนเกิดการสูญหาย และการให้บริการบางประเภทไม่สามารถเปิดใช้งานได้โดยอัตโนมัติ	- แหล่งกำเนิดไฟฟ้าขัดข้องหรือแรงดันไฟฟ้าไม่คงที่	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่แม่ข่าย อุปกรณ์เครือข่าย เครื่องคอมพิวเตอร์ ระบบฐานข้อมูล ระบบสารสนเทศ

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ
4. ความเสี่ยงจากการถูกบุกรุก โดยผู้ไม่ประสงค์ดี	RIT04	ความเสี่ยงด้านด้านความมั่นคงปลอดภัยของทรัพยากรในระบบเทคโนโลยีสารสนเทศ	การบุกรุกโจมตีโดยผู้ไม่ประสงค์ดี เช่น hacker เป็นต้น การดักจับข้อมูล การส่งข้อมูลคำสั่งเจตนาร้าย การติดไวรัสหรือเวิร์ม	- แฮ็คเกอร์ - แคร็กเกอร์ - การโจมตีการให้บริการ (denial of services/ DOS) - การดักจับข้อมูล - คำสั่งเจตนาร้าย - ความผิดพลาดของซอฟต์แวร์หรือการเขียนโปรแกรม - ไวรัส/เวิร์ม	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่แม่ข่าย ระบบฐานข้อมูล ระบบสารสนเทศ
5. ความเสี่ยงจากการขาดแคลนบุคลากรผู้ปฏิบัติงาน	RIT05	ความเสี่ยงด้านการบริหารจัดการ	การขาดแคลนบุคลากรด้านสารสนเทศ ทำให้การทำงานอาจหยุดชะงัก หากบุคลากรผู้รับผิดชอบไม่สามารถมาปฏิบัติงานได้ และจำนวนบุคลากรที่มีไม่เพียงพอต่อระบบเทคโนโลยีสารสนเทศที่เพิ่มขึ้นตามความต้องการของผู้ใช้งาน ส่งผลกระทบต่อการพัฒนาและควบคุมดูแลระบบ	- นโยบายจากกระทรวง	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย ระบบฐานข้อมูล ระบบสารสนเทศ ผู้รับบริการหรือผู้ป่วย
6. ความเสี่ยงจากการเปลี่ยนแปลงนโยบายผู้บริหาร	RIT06	ความเสี่ยงด้านการบริหารจัดการ	การเปลี่ยนแปลงผู้บริหาร อาจทำให้นโยบายการบริหารจัดการสารสนเทศเปลี่ยนแปลงด้วย ทำให้การดำเนินการโครงการต่างๆได้รับผลกระทบ		ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย ระบบฐานข้อมูล ระบบสารสนเทศ

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ
7. ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ	RIT07	ความเสี่ยงด้านการบริหารจัดการ	การขาดแคลนงบประมาณในการดำเนินการให้ระบบสารสนเทศสามารถดำเนินการได้ต่อเนื่องอย่างมีประสิทธิภาพ		ผู้ใช้งาน ผู้ดูแลระบบ ระบบฐานข้อมูล ระบบสารสนเทศ
8. ความเสี่ยงจากการเกิดไฟไหม้ น้ำท่วม แผ่นดินไหว	RIT08	ความเสี่ยงด้านภัยหรือสถานการณ์ฉุกเฉิน	การเกิดไฟไหม้อาคาร แผ่นดินไหวจนอาคารถล่ม ไม่สามารถเคลื่อนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆได้ ทำให้ได้รับความเสียหายทั้งหมด	- ไฟไหม้ จากอุบัติเหตุไฟฟ้าลัดวงจร การวางเพลิง - ภัยธรรมชาติ	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย ระบบฐานข้อมูล ระบบสารสนเทศ
9. ความเสี่ยงจากสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง	RIT09	ความเสี่ยงด้านภัยหรือสถานการณ์ฉุกเฉิน	การเกิดสถานการณ์ความรุนแรง หรือความไม่สงบเรียบร้อย จนทำให้บุคลากรสามารถปฏิบัติงานได้ตามปกติ	- การชุมนุมประท้วง - การจลาจล - การก่อการร้าย	ผู้ใช้งาน ผู้ดูแลระบบ
10. ความเสี่ยงจากเครื่องคอมพิวเตอร์หรืออุปกรณ์ขัดข้อง ไม่สามารถทำงานได้ตามปกติ	RIT10	ความเสี่ยงด้านบริหารจัดการ	เครื่องคอมพิวเตอร์หรืออุปกรณ์ชำรุดหรือขัดข้องด้วยสาเหตุทางเทคนิค หรือจากสัตว์กัดแทะเช่น หนูหรือแมลง เป็นต้น	- ความล้มเหลวทางเทคนิค - สัตว์กัดแทะประเภทหนูหรือแมลง	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย
11. ความเสี่ยงจากการโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์	RIT11	ความเสี่ยงด้านความมั่นคงปลอดภัยของทรัพยากรในระบบเทคโนโลยีสารสนเทศ	การโจรกรรมเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ หรือชิ้นส่วนภายในเครื่อง เช่น CPU และ Ram ทำให้ไม่สามารถปฏิบัติงาน หรือเกิดการสูญหายของข้อมูลบนเครื่องคอมพิวเตอร์นั้นได้	- การลักทรัพย์	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ
12. ความเสี่ยงในการดูแลผู้ป่วย	RIT12	ความเสี่ยงด้านด้านระบบเทคโนโลยีสารสนเทศอาจทำให้เกิดความบกพร่องในการดูแลรักษาผู้ป่วย	เกิดจากระบบเทคโนโลยีสารสนเทศอาจทำให้เกิดความบกพร่องในการดูแลผู้ป่วย รักษาผู้ป่วย เช่น ข้อมูลผู้ป่วยคนหนึ่งไปอยู่กับผู้ป่วยคนหนึ่ง , ข้อมูลไม่ครบถ้วน ขาดหาย , ข้อมูลไปถึงผู้ป่วยล่าช้า , การใช้ Default values ที่ผิดพลาด , ข้อมูลในคอมพิวเตอร์กับในกระดาษไม่ตรงกัน , การแก้ไขข้อมูลหลังจากมีผู้ได้รับข้อมูลนั้นไปแล้ว เป็นต้น	- โปรแกรมไม่พร้อมใช้งาน/ทำงานผิดพลาด - การตั้งค่าผิดพลาด - บุคลากรทำงานผิดพลาด	ผู้ป่วย ผู้ใช้งาน ความน่าเชื่อถือโรงพยาบาล
13. ความเสี่ยงการเปิดเผยข้อมูลผู้ป่วย	RIT13	ความเสี่ยงด้านความเป็นส่วนตัวของผู้ป่วย	ผู้ใช้งานขาดความตระหนักเรื่องการเปิดเผยข้อมูลข้อมูลส่วนบุคคลของผู้ป่วย เช่น ภาพใบหน้า ชื่อ-สกุลผู้ป่วย เตียง ฯลฯ รวมไปถึงการแชร์ข้อมูลในสังคมออนไลน์	- การอำพรางหรือสวมรอยของมิจฉาชีพ - การฟ้องร้องจากผู้ป่วยเรื่องการเปิดเผยข้อมูลส่วนบุคคลก่อนได้รับอนุญาต	ผู้ป่วย ผู้ใช้งาน ความน่าเชื่อถือโรงพยาบาล
14. ความเสี่ยงระบบฐานข้อมูลล่ม/เสียหาย	RIT14	ความเสี่ยงด้านภัยหรือสถานการณ์ฉุกเฉิน	การเกิดสถานการณ์ฉุกเฉิน หรือฐานข้อมูลล่มเหลว ไม่สามารถทำงานได้ตามปกติ		ผู้ป่วย ผู้ใช้งาน ผู้ดูแลระบบ

2. การประมาณความเสี่ยง (Risk estimation)

เป็นการดูปัญหาความเสี่ยงในแง่ของโอกาสการเกิดเหตุ (Incident) หรือเหตุการณ์ (Event) ว่ามีมากน้อยเพียงไรและผลที่ติดตามมาว่ามีความรุนแรงหรือเสียหายมากน้อยเพียงใด

เกณฑ์การประมาณ เป็นการกำหนดเกณฑ์ที่จะใช้ในการประมาณความเสี่ยง ได้แก่ ระดับโอกาสที่จะเกิดความเสี่ยง ระดับความรุนแรงของผลกระทบ และระดับความเสี่ยง ซึ่งสำนักงานจังหวัด ใช้เกณฑ์ดังนี้

ระดับโอกาสในการเกิดเหตุการณ์ต่าง ๆ (Likeihood) เชิงปริมาณ

ระดับ	โอกาสที่จะเกิด	คำอธิบาย
5	สูงมาก	1 เดือนต่อครั้งหรือมากกว่า
4	สูง	1-6 เดือนต่อครั้ง แต่ไม่เกิน 5 ครั้งต่อปี
3	ปานกลาง	1 ปีต่อครั้ง
2	น้อย	2-3 ปีต่อครั้ง
1	น้อยมาก	5 ปีต่อครั้ง

ระดับความรุนแรงของผลกระทบของความเสี่ยง (Impact) เชิงคุณภาพ

ระดับ	ผลกระทบ	คำอธิบาย
5	สูงมาก	> 10 ล้านบาท หรือเกิดความสูญเสียต่อระบบ IT ที่สำคัญทั้งหมดและเกิดความเสียหายอย่างมากต่อความปลอดภัยของข้อมูลต่างๆ
4	สูง	> 5 แสนบาท – 10 ล้านบาทหรือเกิดปัญหากับระบบ IT ที่สำคัญ และระบบความปลอดภัยซึ่งส่งผลต่อความถูกต้องขอข้อมูลบางส่วน
3	ปานกลาง	> 2.5 แสนบาท – 5 แสนบาท หรือระบบมีปัญหาและมีความสูญเสียไม่มาก
2	น้อย	> 1 แสนบาท – 2.5 แสนบาท หรือเกิดเหตุร้ายเล็กน้อยที่แก้ไขได้
1	น้อยมาก	ไม่เกิน 100,000 บาท หรือเกิดเหตุร้ายที่ไม่มีความสำคัญ

ตารางที่ 2 การประมาณความเสี่ยง (Risk estimation)

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ	โอกาส	ความรุนแรง
1. ความเสี่ยงในการเข้าถึงข้อมูลของบุคคลอื่น	RIT01	ความเสี่ยงด้านความเป็นส่วนตัวของข้อมูลผู้ป่วย	ผู้ใช้ขาดความระมัดระวังในการเข้าใช้ระบบสารสนเทศ เช่น การมอบหมายให้ผู้อื่นใช้รหัสผ่านของตนเองเข้าใช้ระบบหรือใช้งานแทน	- การอำพรางหรือสวมรอยผู้ใช้ - การเข้าถึงข้อมูล / เปลี่ยนแปลงข้อมูล โดยไม่ได้รับอนุญาต	ผู้ใช้งาน ระบบสารสนเทศระบบฐานข้อมูล	5	4
2. ความเสี่ยงจากการนำเอาอุปกรณ์อื่นที่ไม่ได้รับอนุญาตมาเชื่อมต่อ	RIT02	ความเสี่ยงด้านบริหารจัดการ	ผู้ใช้ขาดความระมัดระวังในการใช้ระบบเครือข่าย เช่น การนำ wireless router หรือ switch/hub มาเชื่อมต่อกับระบบเครือข่ายไม่ได้รับอนุญาต และไม่ได้มีการตั้งค่าเครื่องที่ถูกต้อง ทำให้เครื่องคอมพิวเตอร์อื่นในระบบเครือข่ายไม่สามารถใช้งานได้ หรือ การไม่ได้ตั้งค่าการรักษาความปลอดภัย ทำให้เครื่องคอมพิวเตอร์ของบุคคลภายนอกอื่นๆที่รับสัญญาณได้ เชื่อมต่อเข้ากับระบบเครือข่ายของทำให้เกิดช่องโหว่กับระบบรักษาความปลอดภัย	- การนำอุปกรณ์อื่นมาเชื่อมต่อเข้าระบบ - ความล้มเหลวทางเทคนิค	ผู้ใช้งาน ผู้ดูแลระบบ ระบบสารสนเทศ ระบบฐานข้อมูล เครื่องคอมพิวเตอร์แม่ข่าย	4	5
3.ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	RIT03	ความเสี่ยงด้านภัยหรือสถานการณ์ฉุกเฉิน	การเกิดกระแสไฟฟ้าขัดข้อง หรือเกิดแรงดันไฟฟ้าไม่คงที่ ทำให้เครื่องคอมพิวเตอร์และอุปกรณ์อาจได้รับความเสียหายจากแรงดันไฟฟ้าที่ไม่คงที่ หรือเมื่อกระแสไฟฟ้าขัดข้อง ทำให้เครื่องแม่ข่ายคอมพิวเตอร์ถูกปิดไปโดยไม่สมบูรณ์ อาจทำให้ข้อมูลสารสนเทศบางส่วนเกิดการสูญหาย และการให้บริการบางประเภทไม่สามารถเปิดใช้งานได้โดยอัตโนมัติ	- แหล่งกำเนิดไฟฟ้าขัดข้องหรือแรงดันไฟฟ้าไม่คงที่	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย เครื่องคอมพิวเตอร์ ระบบฐานข้อมูล ระบบสารสนเทศ	3	2

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ	โอกาส	ความรุนแรง
4.ความเสี่ยงจากการถูกบุกรุกโดยผู้ไม่ประสงค์ดี	RIT04	ความเสี่ยงด้านด้านความมั่นคงปลอดภัยของทรัพยากรในระบบเทคโนโลยีสารสนเทศ	การบุกรุกโจมตีโดยผู้ไม่ประสงค์ดี เช่น hacker เป็นต้น การดักจับข้อมูล การส่งข้อมูลคำสั่งเจตนาร้าย การติดไวรัสหรือเวิร์ม	- แฮ็คเกอร์ - แคร็กเกอร์ - การโจมตีการให้บริการ (denial ofservices/ DOS) - การดักจับข้อมูล - คำสั่งเจตนาร้าย - ความผิดพลาดของซอฟต์แวร์หรือการเขียนโปรแกรม - ไวรัส/เวิร์ม	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่ายระบบฐานข้อมูล ระบบสารสนเทศ	2	4
5.ความเสี่ยงจากการขาดแคลนบุคลาผู้ปฏิบัติงาน	RIT05	ความเสี่ยงด้านการบริหารจัดการ	การขาดแคลนบุคลากรด้านสารสนเทศ ทำให้การทำงานอาจหยุดชะงัก หากบุคลากรผู้รับผิดชอบไม่สามารถมาปฏิบัติงานได้ และจำนวนบุคลากรที่มีไม่เพียงพอต่อระบบเทคโนโลยีสารสนเทศที่เพิ่มขึ้นตามความต้องการของผู้ใช้งาน ส่งผลกระทบต่อการพัฒนาและควบคุมดูแลระบบ	- นโยบายจากกระทรวง	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย ระบบฐานข้อมูล ระบบสารสนเทศ ผู้รับบริการหรือผู้ป่วย	5	3

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ	โอกาส	ความรุนแรง
6.ความเสี่ยงจากการเปลี่ยนแปลงนโยบายผู้บริหาร	RIT06	ความเสี่ยงด้านการบริหารจัดการ	การเปลี่ยนแปลงผู้บริหาร อาจทำให้นโยบายการบริหารจัดการสารสนเทศเปลี่ยนแปลงด้วย ทำให้การดำเนินการโครงการต่างๆได้รับผลกระทบ		ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย ระบบฐานข้อมูล ระบบสารสนเทศ	1	1
7.ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ	RIT07	ความเสี่ยงด้านการบริหารจัดการ	การขาดแคลนงบประมาณในการดำเนินการให้ระบบสารสนเทศสามารถดำเนินการได้ต่อเนื่องอย่างมีประสิทธิภาพ		ผู้ใช้งาน ผู้ดูแลระบบ ระบบฐานข้อมูล ระบบสารสนเทศ	3	5
8.ความเสี่ยงจากการเกิดไฟไหม้ น้ำท่วม แผ่นดินไหว	RIT08	ความเสี่ยงด้านภัยหรือสถานการณ์ฉุกเฉิน	การเกิดไฟไหม้อาคาร แผ่นดินไหวจนอาคารถล่ม ไม่สามารถเคลื่อนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆได้ ทำให้ได้รับความเสียหายทั้งหมด	- ไฟไหม้ จากอุบัติเหตุไฟฟ้าลัดวงจร การวางเพลิง - ภัยธรรมชาติ	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย ระบบฐานข้อมูล	1	5
9.ความเสี่ยงจากสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง	RIT09	ความเสี่ยงด้านภัยหรือสถานการณ์ฉุกเฉิน	การเกิดสถานการณ์ความรุนแรง หรือความไม่สงบเรียบร้อย จนทำให้บุคลากรสามารถปฏิบัติงานได้ตามปกติ	- การชุมนุมประท้วง - การจลาจล - การก่อการร้าย	ผู้ใช้งาน ผู้ดูแลระบบ	1	2

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ	โอกาส	ความรุนแรง
10.ความเสี่ยงจากเครื่องคอมพิวเตอร์หรืออุปกรณ์ขัดข้อง ไม่สามารถทำงานได้ตามปกติ	RIT10	ความเสี่ยงด้านบริหารจัดการ	เครื่องคอมพิวเตอร์หรืออุปกรณ์ชำรุดหรือขัดข้องด้วยสาเหตุทางเทคนิค หรือจากสัตว์กัดแทะเช่น หนูหรือแมลง เป็นต้น	- ความล้มเหลวทางเทคนิค - สัตว์กัดแทะประเภทหนู หรือแมลง	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย	5	3
11.ความเสี่ยงจากการโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์	RIT11	ความเสี่ยงด้านความมั่นคงปลอดภัยของทรัพยากรในระบบเทคโนโลยีสารสนเทศ	การโจรกรรมเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ หรือชิ้นส่วนภายในเครื่อง เช่น CPU และ Ram ทำให้ไม่สามารถปฏิบัติงาน หรือเกิดการสูญหายของข้อมูลบนเครื่องคอมพิวเตอร์นั้นได้	- การลักทรัพย์	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย	1	5
12.ความเสี่ยงในการดูแลผู้ป่วย	RIT12	ความเสี่ยงด้านด้านระบบเทคโนโลยีสารสนเทศอาจทำให้เกิดความบกพร่องในการดูแลรักษาผู้ป่วย	เกิดจากระบบเทคโนโลยีสารสนเทศอาจทำให้เกิดความบกพร่องในการดูแลผู้ป่วย รักษาผู้ป่วย เช่น ข้อมูลผู้ป่วยคนหนึ่งไปอยู่กับผู้ป่วยคนหนึ่ง , ข้อมูลไม่ครบถ้วน ขาดหาย , ข้อมูลไปถึงผู้ป่วยล่าช้า , การใช้ Default values ที่ผิดพลาด , ข้อมูลในคอมพิวเตอร์กับในกระดาษไม่ตรงกัน , การแก้ไขข้อมูลหลังจากมีผู้ได้รับข้อมูลนั้นไปแล้ว เป็นต้น	- โปรแกรมไม่พร้อมใช้งาน/ทำงานผิดพลาด - การตั้งค่าผิดพลาด - บุคลากรทำงานผิดพลาด	ผู้ป่วย ผู้ใช้งาน ความน่าเชื่อถือโรงพยาบาล	5	4

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ	โอกาส	ความรุนแรง
13.ความเสี่ยงการเปิดเผยข้อมูลผู้ป่วย	RIT13	ความเสี่ยงด้านความเป็นส่วนตัวของผู้ป่วย	ผู้ใช้งานขาดความตระหนักเรื่องการเปิดเผยข้อมูลข้อมูลส่วนบุคคลของผู้ป่วย เช่น ภาพใบหน้า ชื่อ-สกุลผู้ป่วย เตียง ฯลฯ รวมไปถึงการแชร์ข้อมูลในสังคมออนไลน์	- การอำพรางหรือสวมรอยของมิจฉาชีพ - การฟ้องร้องจากผู้ป่วยเรื่องการเปิดเผยข้อมูลส่วนบุคคลก่อนได้รับอนุญาต	ผู้ป่วย ผู้ใช้งาน ความน่าเชื่อถือโรงพยาบาล	4	5
14.ความเสี่ยงระบบฐานข้อมูลล่ม/เสียหาย	RIT14	ความเสี่ยงด้านภัยหรือสถานการณ์ฉุกเฉิน	การเกิดสถานการณ์ฉุกเฉิน หรือฐานข้อมูลล่มเหลว ไม่สามารถทำงานได้ตามปกติ		ผู้ป่วย ผู้ใช้งาน ผู้ดูแลระบบ	4	5

3. การประเมินค่าความเสี่ยง (Risk evaluation)

การประเมินค่าความเสี่ยง จะพิจารณาจากปัจจัยจากขั้นตอนที่ผ่านมาได้แก่ โอกาสที่ภัยคุกคามที่เกิดขึ้นทำให้ระบบขาดความมั่นคง, ระดับผลกระทบหรือความรุนแรงของภัยคุกคามที่มีต่อระบบ และประสิทธิภาพของแผนการควบคุมความปลอดภัยของระบบ การวัดระดับความเสี่ยงมีการกำหนด แผนภูมิความเสี่ยง ที่ได้จากการพิจารณาจัดระดับความสำคัญของความเสี่ยงจากโอกาสที่จะเกิดความเสี่ยง และผลกระทบที่เกิดขึ้น และขอบเขตของระดับความเสี่ยงที่สามารถยอมรับได้

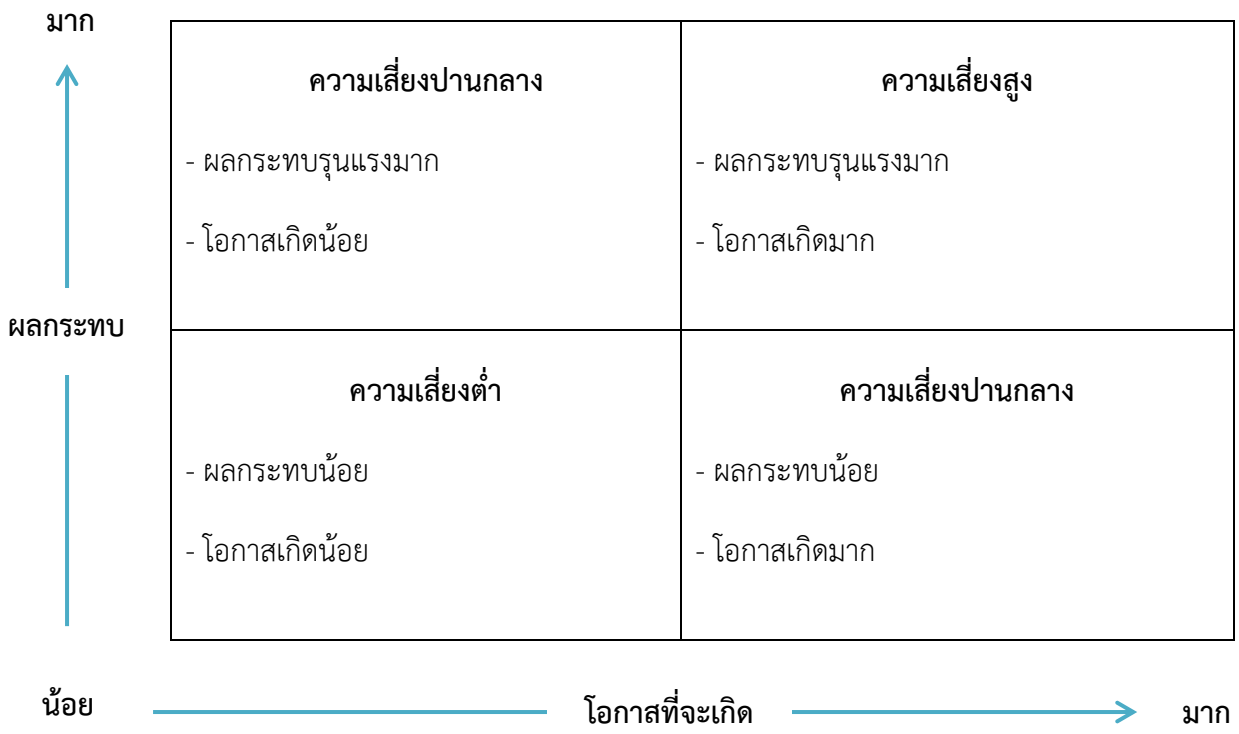
ระดับความเสี่ยง = โอกาสที่จะเกิดหรือความถี่ (P) x ความรุนแรงหรือผลกระทบ (I)

ซึ่งเกณฑ์ในการจัดแบ่งดังนี้

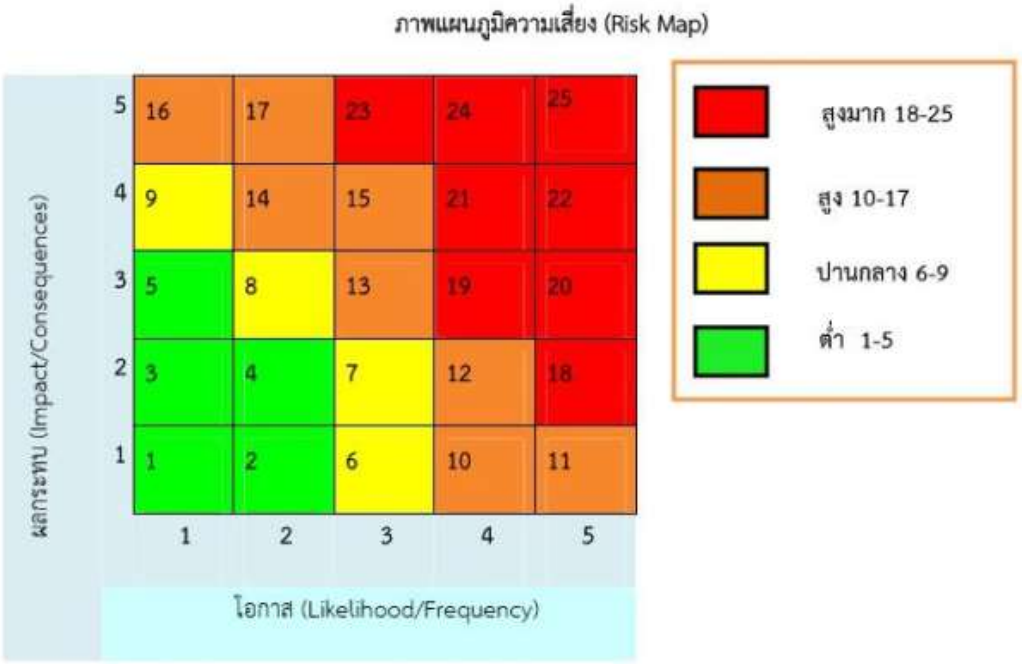
ระดับคะแนนความ	สัญลักษณ์	จัดระดับความเสี่ยง	กลยุทธ์ในการจัดการความเสี่ยง	พื้นที่สี
1 –5	L	ต่ำ	ยอมรับความเสี่ยง	เขียว
6 –9	M	ปานกลาง	ยอมรับความเสี่ยง (มีมาตรการติดตาม)	เหลือง
10 –17	H	สูง	ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)	ส้ม
18-28	HH	สูงมาก	ถ่ายโอนความเสี่ยง	แดง

3.1 แผนภูมิความเสี่ยง (Risk Map)

การวัดระดับความเสี่ยง



3.2 การประเมินความเสียง



ทั้งนี้ สามารถสรุปผลการประเมินค่าความเสี่ยง แสดงดังตารางที่ 3 และสามารถแสดงแผนภูมิความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Risk Map) แสดงในรูปที่ 1

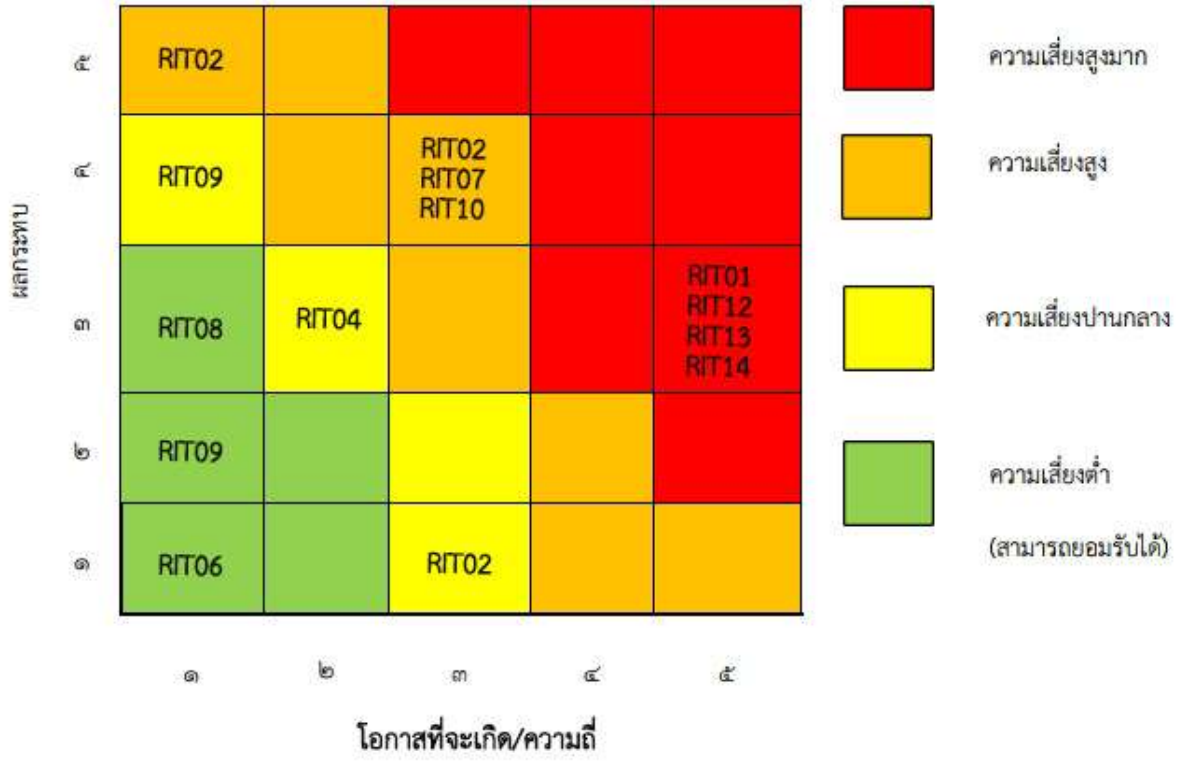
ตารางที่ 3 สรุปผลการประเมินค่าความเสี่ยง (Risk evaluation)

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	โอกาส/ความถี่	ความรุนแรง	ระดับคะแนน	
1. ความเสี่ยงในการเข้าถึงข้อมูลของบุคคลอื่น	RIT01	ความเสี่ยงด้านความเป็นส่วนตัวของข้อมูลผู้ป่วย	ผู้ใช้งานขาดความตระหนักเรื่องการเปิดเผยข้อมูลข้อมูลส่วนบุคคลของผู้ป่วย เช่น ภาพใบหน้า ชื่อ-สกุลผู้ป่วย เตียง ฯลฯ รวมไปถึงการแชร์ข้อมูลในสังคมออนไลน์	5	4	20	HH
2. ความเสี่ยงจากการนำเอาอุปกรณ์อื่นที่ไม่ได้รับอนุญาตมาเชื่อมต่อ	RIT02	ความเสี่ยงด้านบริหารจัดการ	ผู้ใช้ขาดความระมัดระวังในการใช้ระบบเครือข่าย เช่น การนำ wireless router หรือ switch/hubมาเชื่อมต่อกับระบบเครือข่ายไม่ได้รับอนุญาต และไม่ได้มีการตั้งค่าเครื่องที่ถูกต้อง ทำให้เครื่องคอมพิวเตอร์อื่นในระบบเครือข่ายไม่สามารถใช้งานได้ หรือ การไม่ได้ตั้งค่าการรักษาความปลอดภัย ทำให้เครื่องคอมพิวเตอร์ของบุคคลภายนอกอื่นๆที่รับสัญญาณได้ เชื่อมต่อเข้ากับระบบเครือข่ายของ ทำให้เกิดช่องโหว่กับระบบรักษาความปลอดภัย	4	4	16	H
3. ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	RIT03	ความเสี่ยงด้านภัยหรือสถานการณ์ฉุกเฉิน	การเกิดกระแสไฟฟ้าขัดข้อง หรือเกิดแรงดันไฟฟ้าไม่คงที่ ทำให้เครื่องคอมพิวเตอร์และอุปกรณ์อาจได้รับความเสียหายจากแรงดันไฟฟ้าที่ไม่คงที่หรือเมื่อกระแสไฟฟ้าขัดข้อง ทำให้เครื่องแม่ข่ายคอมพิวเตอร์ถูกปิดไปโดยไม่สมบูรณ์ อาจทำให้ข้อมูลสารสนเทศบางส่วนเกิดการสูญหาย และการให้บริการบางประเภทไม่สามารถเปิดใช้งานได้โดยอัตโนมัติ	3	2	6	M
4. ความเสี่ยงจากการถูกบุกรุก โดยผู้ไม่ประสงค์ดี	RIT04	ความเสียงด้านด้านความมั่นคงปลอดภัยของทรัพยากรในระบบเทคโนโลยีสารสนเทศ	การบุกรุกโจมตีโดยผู้ไม่ประสงค์ดี เช่น hacker เป็นต้น การดักจับข้อมูล การส่งข้อมูลคำสั่งเจตนาร้าย การติดไวรัสหรือเวิร์ม	2	4	8	M
5. ความเสี่ยงจากการขาดแคลนบุคลากร	RIT05	ความเสี่ยงด้านการบริหารจัดการ	การขาดแคลนบุคลากรด้านสารสนเทศ ทำให้การทำงานอาจหยุดชะงัก หากบุคลากรผู้รับผิดชอบ	5	3	20	HH

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	โอกาส/ความถี่	ความรุนแรง	ระดับคะแนน	
ผู้ปฏิบัติงาน			ไม่สามารถมาปฏิบัติงานได้ และจำนวนบุคลากรที่มีไม่เพียงพอต่อระบบเทคโนโลยีสารสนเทศที่เพิ่มขึ้นตามความต้องการของผู้ใช้งาน ส่งผลกระทบต่อการพัฒนาและควบคุมดูแลระบบ				
6. ความเสี่ยงจากการเปลี่ยนแปลงนโยบายผู้บริหาร	RIT06	ความเสี่ยงด้านการบริหารจัดการ	การเปลี่ยนแปลงผู้บริหาร อาจทำให้นโยบายการบริหาจัดการสารสนเทศเปลี่ยนแปลงด้วย ทำให้การดำเนินการโครงการต่างๆ ได้รับผลกระทบ	1	1	1	L
7. ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ	RIT07	ความเสี่ยงด้านการบริหารจัดการ	การขาดแคลนงบประมาณในการดำเนินการให้ระบบสารสนเทศสามารถดำเนินการได้ต่อเนื่องอย่างมีประสิทธิภาพ	3	5	20	HH
8. ความเสี่ยงจากการเกิดไฟไหม้ น้ำท่วม แผ่นดินไหว อาคารถล่ม	RIT08	ความเสี่ยงด้านภัยหรือสถานการณ์ฉุกเฉิน	การเกิดไฟไหม้อาคาร แผ่นดินไหวจนอาคารถล่ม ไม่สามารถเคลื่อนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆ ได้ ทำให้ได้รับความเสียหายทั้งหมด	1	5	5	L
9. ความเสี่ยงจาก สถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง	RIT09	ความเสี่ยงด้านภัยหรือสถานการณ์ฉุกเฉิน	การเกิดสถานการณ์ความรุนแรงหรือความไม่สงบเรียบร้อย จนทำให้บุคลากรสามารปฏิบัติงานได้ตามปกติ	1	2	2	L
10. ความเสี่ยงจากเครื่องคอมพิวเตอร์หรืออุปกรณ์ขัดข้อง ไม่สามารถทำงานได้ตามปกติ	RIT10	ความเสี่ยงด้านบริหารจัดการ	เครื่องคอมพิวเตอร์หรืออุปกรณ์ชำรุดหรือขัดข้องด้วยสาเหตุทางเทคนิค หรือจากสัตว์กัดแทะ เช่น หนูหรือแมลง เป็นต้น	5	3	15	H

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	โอกาส/ความถี่	ความรุนแรง	ระดับคะแนน	
11. ความเสี่ยงจากการโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์	RIT11	ความเสี่ยงด้านความมั่นคงปลอดภัยของทรัพยากรในระบบเทคโนโลยีสารสนเทศ	การโจรกรรมเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ หรือชิ้นส่วนภายในเครื่อง เช่น CPU และ Ram ทำให้ไม่สามารถปฏิบัติงาน หรือเกิดการสูญหายของข้อมูลบนเครื่องคอมพิวเตอร์นั้นได้	1	5	5	L
12. ความเสี่ยงในการดูแลผู้ป่วย	RIT12	ความเสี่ยงด้านด้านระบบเทคโนโลยีสารสนเทศอาจทำให้เกิดความบกพร่องในการดูแลรักษาผู้ป่วย	เกิดจากระบบเทคโนโลยีสารสนเทศอาจทำให้เกิดความบกพร่องในการดูแลผู้ป่วย รักษาผู้ป่วย เช่น ข้อมูลผู้ป่วยคนหนึ่งไปอยู่กับผู้ป่วยคนหนึ่ง , ข้อมูลไม่ครบถ้วน ขาดหาย , ข้อมูลไปถึงผู้ป่วยล่าช้า , การใช้ Default values ที่ผิดพลาด , ข้อมูลในคอมพิวเตอร์กับในกระดาษไม่ตรงกัน , การแก้ไขข้อมูลหลังจากมีผู้ได้รับข้อมูลนั้นไปแล้ว เป็นต้น	5	4	20	HH
13. ความเสี่ยงการเปิดเผยข้อมูลผู้ป่วย	RIT13	ความเสี่ยงด้านความเป็นส่วนตัวของข้อมูลผู้ป่วย	ผู้ใช้ขาดความระมัดระวังในการเข้าใช้ระบบสารสนเทศ เช่น การมอบหมายให้ผู้อื่นใช้รหัสผ่านของตนเองเข้าใช้ระบบหรือใช้งานแทน	5	4	20	HH
14. ความเสี่ยงฐานข้อมูลระบบล่ม/เสียหาย	RIT14	ความเสี่ยงด้านด้านระบบเทคโนโลยีสารสนเทศอาจทำให้เกิดความบกพร่องในการดูแลรักษาผู้ป่วย	ระบบฐานข้อมูลล่ม หรือเสียหายไม่สามารถเชื่อมต่อระบบฐานข้อมูลได้	4	5	20	HH

แผนภูมิความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Risk Map)



การรายงานผลการวิเคราะห์ความเสี่ยง (Risk reporting)

จากผลการประเมินความเสี่ยง สามารถจัดลำดับความสำคัญของความเสี่ยงด้านเทคโนโลยีสารสนเทศของโรงพยาบาลสมเด็จพระยุพราชเลิงนกทา ในการบริหารจัดการได้อย่างมีประสิทธิภาพดังนี้

ลำดับ	ความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ค่าระดับความเสี่ยง
1	RIT12 ความเสี่ยงในการดูแลผู้ป่วย	ความเสี่ยงด้านด้านระบบเทคโนโลยีสารสนเทศอาจทำให้เกิดความบกพร่องในการดูแลรักษาผู้ป่วย	เกิดจากระบบเทคโนโลยีสารสนเทศอาจทำให้เกิดความบกพร่องในการดูแลผู้ป่วย รักษาผู้ป่วย เช่น ข้อมูลผู้ป่วยคนหนึ่งไปอยู่กับผู้ป่วยคนหนึ่ง , ข้อมูลไม่ครบถ้วน ขาดหาย , ข้อมูลไปถึงผู้ป่วยล่าช้า , การใช้ Default values ที่ผิดพลาด , ข้อมูลในคอมพิวเตอร์กับในกระดาษไม่ตรงกัน , การแก้ไขข้อมูลหลังจากมีผู้ได้รับข้อมูลนั้นไปแล้ว เป็นต้น	**HH**
2	RIT01 ความเสี่ยงในการเข้าถึงข้อมูลของบุคคลอื่น	ความเสี่ยงด้านด้านความมั่นคงปลอดภัยของทรัพยากรในระบบเทคโนโลยีสารสนเทศ	ผู้ใช้ขาดความระมัดระวังในการเข้าใช้ระบบสารสนเทศ เช่น การมอบหมายให้ผู้อื่นใช้รหัสผ่านของตนเองเข้าใช้ระบบหรือใช้งานแทน	HH
3	RIT13 ความเสี่ยงการเปิดเผยข้อมูลผู้ป่วย	ความเสี่ยงด้านความเป็นส่วนตัวของข้อมูลผู้ป่วย	ผู้ใช้ขาดความระมัดระวังในการเข้าใช้ระบบสารสนเทศ เช่น การมอบหมายให้ผู้อื่นใช้รหัสผ่านของตนเองเข้าใช้ระบบหรือใช้งานแทน	**HH**
4	RIT14 ความเสี่ยงระบบฐานข้อมูลล่ม/เสียหาย	ด้านระบบเทคโนโลยีสารสนเทศ	ระบบฐานข้อมูลล่ม หรือเสียหายไม่สามารถเชื่อมต่อระบบฐานข้อมูลได้	**HH**
5	RIT07 ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ	ความเสี่ยงด้านการบริหารจัดการ	การขาดแคลนงบประมาณในการดำเนินการให้ระบบสารสนเทศสามารถดำเนินการได้ต่อเนื่องอย่างมีประสิทธิภาพ	**H**
6	RIT02 ความเสี่ยงจากการนำเอาอุปกรณ์อื่นที่ไม่ได้รับอนุญาตมาเชื่อมต่อ	ความเสี่ยงด้านการบริหารจัดการ	ผู้ใช้ขาดความระมัดระวังในการใช้ระบบเครือข่าย เช่น การนำ wireless router หรือ switch/hub มาเชื่อมต่อกับระบบเครือข่ายสำนักงานจังหวัด (มหาดไทย) โดยไม่ได้รับอนุญาต และไม่ได้มีการตั้งค่าเครื่องที่ถูกต้อง ทำให้เครื่องคอมพิวเตอร์อื่นในระบบ	H

ลำดับ	ความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ค่าระดับความเสี่ยง
			เครือข่ายไม่สามารถใช้งานได้ หรือ การไม่ได้ตั้งค่าการรักษาความปลอดภัย ทำให้เครื่องคอมพิวเตอร์ของบุคคลภายนอกอื่นๆที่ รับสัญญาณได้ เชื่อมต่อเข้ากับระบบเครือข่าย	
7	RIT05 ความเสี่ยงจากการขาดแคลนบุคลากรผู้ปฏิบัติงาน	ความเสี่ยงด้านการบริหารจัดการ	การขาดแคลนบุคลากรด้านสารสนเทศ ทำให้การทำงานอาจหยุดชะงัก หากบุคลากรผู้รับผิดชอบ ไม่สามารถมาปฏิบัติงานได้ และจำนวนบุคลากรที่มีไม่เพียงพอต่อระบบเทคโนโลยีสารสนเทศที่เพิ่มขึ้นตามความต้องการของผู้ใช้งาน ส่งผลกระทบต่อการพัฒนาและควบคุมดูแลระบบ	H
8	RIT10 ความเสี่ยงจากเครื่องคอมพิวเตอร์หรืออุปกรณ์ขัดข้อง ไม่สามารถทำงานได้ตามปกติ	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	เครื่องคอมพิวเตอร์หรืออุปกรณ์ชำรุดหรือขัดข้องด้วยสาเหตุทางเทคนิค หรือจากสัตว์กัดแทะเช่น หนูหรือแมลง เป็นต้น	H
9	RIT04 ความเสี่ยงจากการถูกบุกรุก โดยผู้ไม่ประสงค์ดี	ความเสี่ยงด้านด้านความมั่นคงปลอดภัยของทรัพยากรในระบบเทคโนโลยีสารสนเทศ	การบุกรุกโจมตีโดยผู้ไม่ประสงค์ดี เช่น hacker เป็นต้น การดักจับข้อมูล การส่งข้อมูลคำสั่งเจตนาร้าย การติดไวรัส หรือ เวิร์ม	M
10	RIT03 ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดกระแสไฟฟ้าขัดข้อง หรือเกิดแรงดันไฟฟ้าไม่คงที่ ทำให้เครื่องคอมพิวเตอร์และอุปกรณ์อาจได้รับความเสียหายจากแรงดันไฟฟ้าที่ไม่คงที่หรือเมื่อกระแสไฟฟ้าขัดข้อง ทำให้เครื่องแม่ข่ายคอมพิวเตอร์ถูกปิดไปโดยไม่สมบูรณ์ อาจทำให้ข้อมูลสารสนเทศบางส่วนเกิดการสูญหาย และการให้บริการบางประเภทไม่สามารถเปิดใช้งานได้โดยอัตโนมัติ	M
11	RIT08 ความเสี่ยงจากการเกิดไฟไหม้ แผ่นดินไหว อาคารถล่ม	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดไฟไหม้อาคาร แผ่นดินไหวจนอาคารถล่ม ไม่สามารถเคลื่อนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆได้ ทำให้ได้รับความเสียหายทั้งหมด	L

ลำดับ	ความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ค่าระดับความเสี่ยง
12	RIT11 ความเสี่ยงจากการโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์	ความเสี่ยงด้านด้านความมั่นคงปลอดภัยของทรัพยากรในระบบเทคโนโลยีสารสนเทศ	การโจรกรรมเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ หรือชิ้นส่วนภายในเครื่อง เช่น CPU และRam ทำให้ไม่สามารถปฏิบัติงาน หรือเกิดการสูญหายของข้อมูลบนเครื่องคอมพิวเตอร์นั้นได้	L
13	RIT09 ความเสี่ยงจากสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดสถานการณ์ความรุนแรง หรือความไม่สงบเรียบร้อย จนทำให้บุคลากรไม่สามารถปฏิบัติงานได้ตามปกติ	L
14	RIT06 ความเสี่ยงจากการเปลี่ยนแปลงนโยบายผู้บริหาร	ความเสี่ยงด้านการบริหารจัดการ	การเปลี่ยนแปลงผู้บริหาร อาจทำให้นโยบายการบริหารจัดการสารสนเทศเปลี่ยนแปลงด้วย ทำให้การดำเนินการโครงการต่างๆได้รับผลกระทบ	L

5. การจัดการความเสี่ยง (Risk management)

นโยบายของกลุ่มงานเทคโนโลยีสารสนเทศทางการแพทย์ โรงพยาบาลภูเพียง ระดับ ความเสี่ยงคงเหลือที่ยอมรับได้ ≤ 5 กำหนดให้ความเสี่ยงที่จำเป็นต้องนำมาดำเนินการจัดการความเสี่ยง คือความเสี่ยง ที่มีระดับความเสี่ยงสูง ตั้งแต่ 15 ขึ้นไป ส่วนความเสี่ยงที่มีระดับความเสี่ยงต่ำกว่า 15 ถือว่ามีความเสี่ยงค่อนข้างต่ำ อาจจะนำมาดำเนินการจัดการความเสี่ยงในแผนบริหารความเสี่ยงหรือไม่ก็ได้ การดำเนินการจัดการความเสี่ยงเป็นดัง ตารางที่ 5

1. หลีกเลี่ยงความเสี่ยง (Risk Avoidance = RA) การหลีกเลี่ยงความเสี่ยง เช่น เมื่อพบว่าปัจจุบันโรงพยาบาล มีการสำรองข้อมูลเพียง 1 ชุดและจัดเป็นความเสี่ยงต่อการสูญเสีย การเลี่ยงความเสี่ยงนี้อาจได้แก่การทำสำรองข้อมูล 2 ชุด และแยกเก็บในสถานที่ต่างกัน การบริหารจัดการการเชื่อมโยงสู่เครือข่ายผ่านโมเด็ม ถ้าเป็นการยากต่อการควบคุมหรือบริหารจัดการ องค์กรอาจเลือกทางออกโดยการยกเลิกไม่ให้ใช้บริการ และแนะนำให้พนักงานใช้บริการผ่านทาง ISP ในช่วงที่มีการระบาดของไวรัสอย่างหนัก องค์กรอาจมีเลือกระงับไม่ให้ใช้คอมพิวเตอร์ที่ไม่ได้ติดตั้ง Antivirus เป็นต้น

2. การโอนย้ายความเสี่ยง (Risk Transfer = RF) เช่น อุปกรณ์เครือข่ายเมื่อซื้อมาแล้วมีระยะประกันเพียงหนึ่งปี เพื่อเป็นการรับมือในกรณีที่อุปกรณ์เครือข่ายไม่ทำงาน องค์กรอาจเลือกซื้อประกัน หรือสัญญาการบำรุงรักษาหลังขาย (Maintenance service) เป็นต้น

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

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

ตารางที่ 4 การจัดการความเสี่ยง (Risk management)

ลำดับ	ความเสี่ยง	ค่าระดับความเสี่ยง	กลยุทธ์การจัดการความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง	กลยุทธ์
1	RIT12 ความเสี่ยงในการดูแลผู้ป่วย	**20**	- ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)	1. มีระบบติดตามเฝ้าระวัง ได้แก่ 1.1 ระบบ Log file 1.2 ระบบ Alert แจ้งเตือนต่างๆ ให้ทราบ ได้แก่ - ข้อมูลการแพ้ยา - ระบบ Drug Interaction - นโยบายกำหนดสิทธิการสั่งจ่ายยาโดยแพทย์เฉพาะทาง และบางกรณีต้องผ่านการขออนุมัติก่อนใช้ยา 2. ควบคุม กำกับ ดูแล โดยคณะกรรมทีมบริหารความเสี่ยงโรงพยาบาลสมเด็จพระยุพราชเลิงนกทา 3. จัดทำแผนรับสถานการณ์เพื่อให้สามารถดำเนินการได้อย่างต่อเนื่อง (Business Continuity Plan : BCP)	**LR**
2	RIT14 ความเสี่ยงระบบฐานข้อมูลล่ม/เสียหาย	20	- ยอมรับความเสี่ยง - ถ่ายโอนความเสี่ยง - หลีกเลี่ยงความเสี่ยง	1. ระบบฐานข้อมูล สัญญาการบำรุงรักษาหลังขาย (Maintenance service)ได้แก่ ระบบฐานข้อมูลผู้ป่วย **HOSxP,**ระบบเวชระเบียนอิเล็กทรอนิกส์ **Binary** ,ระบบสำนักงาน **(Express),**ระบบภาพรังสี **(PACs)** 2. มีระบบส ารองข้อมูลมากกว่า 1 ชุด กรณีระบบฐานข้อมูลผู้ป่วย	**RC** **RF** **RA**
3	RIT13 ความเสี่ยงการเปิดเผยข้อมูลผู้ป่วย	20	- ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)	1. สร้างความตระหนักในเรื่องของข้อมูลส่วนบุคคล ในการพึงรักษาสิทธิ์ในส่วนของข้อมูลส่วนบุคคล 2. กำกับดูแลการปฏิบัติตามระเบียบปฏิบัติด้านการรักษาความมั่นคงปลอดภัย สารสนเทศอย่างเคร่งครัด	**LR**

ลำดับ	ความเสี่ยง	ค่าระดับความเสี่ยง	กลยุทธ์การจัดการความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง	กลยุทธ์
4	RIT01 ความเสี่ยงในการเข้าถึงข้อมูลของบุคคลอื่น	20	- ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)	1. สร้างความตระหนักในเรื่องของข้อมูลส่วนบุคคล ในการพึงรักษาสิทธิ์ในส่วนของข้อมูลส่วนบุคคล 2. กำกับดูแลการปฏิบัติตามระเบียบปฏิบัติด้านการรักษาความมั่นคงปลอดภัย สารสนเทศอย่างเคร่งครัด	LR
5	RIT02 ความเสี่ยงจากการนำเอาอุปกรณ์อื่นที่ไม่ได้รับอนุญาตมาเชื่อมต่อ	16	- ยอมรับความเสี่ยง (มีมาตรการติดตาม)	1. สร้างความตระหนักในเรื่องนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ 2. กระตุ้นให้เกิดการปฏิบัติตามแนวนโยบายหรือระเบียบด้านสารสนเทศอย่างจริงจัง 3. ใช้อุปกรณ์เครือข่ายที่สามารถจำกัดสิทธิ์การเข้าถึงสำหรับอุปกรณ์ที่ไม่ได้รับอนุญาตให้เชื่อมต่อเข้าเครือข่าย	RC LR
6	RIT05 ความเสี่ยงจากการขาดแคลนบุคลากรผู้ปฏิบัติงาน	15	- ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)	1. ปรับปรุงโครงสร้างศูนย์สารสนเทศ และสรรหาบุคลากรเพื่อรองรับงานอย่างเหมาะสม 2. จัดทำคู่มือกระบวนการทำงานเพื่อให้บุคลากรอื่นสามารถปฏิบัติตามคู่มือได้กรณีที่บุคลากรผู้รับผิดชอบไม่สามารถมาปฏิบัติงานได้ 3. จัดตารางเวรและช่องทางการติดต่อสื่อสารตลอด 24 ชั่วโมง	LR
7	RIT07 ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ	15	- ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)	1. จัดทำแผนแม่บทเทคโนโลยีสารสนเทศ เพื่อแสดงความจำเป็นในการขอสนับสนุนงบประมาณในการดำเนินการด้านเทคโนโลยีสารสนเทศ	LR

ลำดับ	ความเสี่ยง	ค่าระดับความเสี่ยง	กลยุทธ์การจัดการความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง	กลยุทธ์
8	RIT10 ความเสี่ยงจากเครื่องคอมพิวเตอร์หรืออุปกรณ์ขัดข้อง ไม่สามารถทำงานได้ตามปกติ	15	- ยอมรับความเสี่ยง (มีมาตรการติดตาม)	1. หาทางป้องกันสัตว์กัดแทะอุปกรณ์ 2. จัดหาเครื่องและอุปกรณ์สำรองเพื่อให้สามารถใช้ทดแทนชั่วคราว เพื่อสามารถปฏิบัติงานได้ 3. จัดทำแผนการตรวจสอบและจัดจ้างบำรุงรักษาเครื่องและอุปกรณ์อย่างสม่ำเสมอ	RC RA
9	RIT04 ความเสี่ยงจากการถูกบุกรุกโดยผู้ไม่ประสงค์ดี	8	- ยอมรับความเสี่ยง	- ตรวจสอบการตั้งค่าของ firewall อย่างสม่ำเสมอ - ติดตั้งระบบตรวจสอบการบุกรุกเครือข่าย และติดตามเพื่อปรับปรุงอย่างสม่ำเสมอ - ติดตั้งโปรแกรมป้องกันไวรัสและ patch อย่างสม่ำเสมอ - ติดตั้ง patch ของระบบปฏิบัติการอย่างสม่ำเสมอ - เปลี่ยนรหัสผ่านตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ	RC RA
10	RIT03 ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที	6	- ยอมรับความเสี่ยง (มีมาตรการติดตาม)	- จัดหาเครื่องกำเนิดไฟฟ้า และเครื่องสำรองไฟฟ้าแบบป้องกันปัญหาแรงดันไฟฟ้าไม่คงที่ - โรงพยาบาลมีระบบไฟฉุกเฉินอัตโนมัติใช้ (เวลา 3 วินาที) - จัดทำแผนรับสถานการณ์เพื่อให้สามารถดำเนินการได้อย่างต่อเนื่อง (Business Continuity Plan : BCP)	RC
11	RIT08 ความเสี่ยงจากการเกิดไฟไหม้ แผ่นดินไหว อาคารถล่ม	5	- ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)	1. จัดทำแผนรับสถานการณ์เพื่อให้สามารถดำเนินการได้อย่างต่อเนื่อง (Business Continuity Plan : BCP) , แผนกู้คืนระบบ DRP 2. จัดหาระบบสำรองเพื่อให้ระบบสารสนเทศสามารถทำงานได้ 3. สำรองข้อมูลระบบ และฐานข้อมูลเก็บไว้ในสถานที่อื่นอีกหนึ่งชุด	RC

ลำดับ	ความเสี่ยง	ค่าระดับความเสี่ยง	กลยุทธ์การจัดการความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง	กลยุทธ์
12	RIT11 ความเสี่ยงจากการโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์	5	- ยอมรับความเสี่ยง	- ตรวจสอบการเข้าออกของบุคคลภายนอก - ตรวจสอบระบบการป้องกันรักษาความปลอดภัยของสถานที่ให้อยู่ในสภาพปกติ - ติดตั้งกล้องวงจรปิดเพื่อเฝ้าระวัง	RC
13	RIT09 ความเสี่ยงจากสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง	2	- ยอมรับความเสี่ยง	- จัดทำแผนรับสถานการณ์เพื่อให้สามารถดำเนินการได้อย่างต่อเนื่อง (Business Continuity Plan : BCP) - จัดหาระบบส ารองเพื่อให้ระบบสารสนเทศสามารถทำงานได้	RC
14	RIT06 ความเสี่ยงจากการเปลี่ยนแปลงนโยบายผู้บริหาร	1	- ยอมรับความเสี่ยง		RC

นายชรินทร์ ดีปินตา
นายแพทย์เชี่ยวชาญ(ด้านเวชกรรมป้องกัน)
รักษาการในตำแหน่งผู้อำนวยการโรงพยาบาลภูเพียง