โรงพยาบาลเสาไห้เฉลิมพระเกียรติ 80 พรรษา

การบริหารจัดการความเสี่ยง (Risk Management)
ด้านเทคโนโลยีสารสนเทศ
โรงพยาบาลเสาไห้เฉลิมพระเกียรติ 80 พรรษา
ปี 2564

บทนำ

ตามพระราชบัญญัติตรวจเงินแผ่นดินว่าด้วยการกำหนดมาตรฐานการควบคุมภายใน พ.ศ.๒๕๔๔ ที่กำหนดให้ส่วนราชการต้องมีการประเมินความเสี่ยงและปรับปรุงระบบควบคุมภายใน กลุ่มงานสารสนเทศทางการแพทย์ของโรงพยาบาลแพร่จึงได้ดำเนินการนโยบายด้านการบริหารความเสี่ยงและการควบคุมภายในขององค์กรอย่างต่อเนื่อง ตามแนวทางการจัดวางระบบการควบคุมภายในและการประเมินการควบคุมภายใน ของสำนักงานตรวจเงินแผ่นดิน การบริหารกิจการบ้านเมืองที่ดีของรัฐบาล และการนำระบบการบริหารความเสี่ยงมาใช้ในระบบการบริหาร โดยในปีงบประมาณ พ.ศ.๒๕๕๙ กลุ่มงานสารสนเทศทางการแพทย์มีการดำเนินการตามกระบวนการบริหารความเสี่ยง กับประเด็นยุทธศาสตร์ และต้องดำเนินการบริหารความเสี่ยงโดยให้ครอบคลุมพันธกิจ

โรงพยาบาลแพร่ได้จัดทำแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ประจำปี พ.ศ. ๒๕๖๐-๒๕๕๖๒ ด้วยการวิเคราะห์และประเมิน ความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อที่จะบริหารจัดการความเสี่ยงตามกระบวนการบริหารความเสี่ยงตามมาตรฐาน COSO (Committee of Sponsoring Organizations of the Treadway Commission) โดยได้วิเคราะห์ความเสี่ยงให้ครอบคลุมตามหลักธรรมาภิบาลและเป็นไปตามข้อกำหนดตามเกณฑ์การพัฒนาคุณภาพการบริหารจัดการภาครัฐ (PMQA) ซึ่งสอดคล้องกับมาตรฐานความมั่นคงปลอดภัยสารสนเทศ (ISO๒๗๐๐๑) แผนบริหารจัดการความเสี่ยงดังกล่าว จะใช้เป็นกรอบและแนวทำงานในการปฏิบัติงาน ของหน่วยงานต่างๆ ที่เกี่ยวข้อง ตลอดจนการกากับดูแลการใช้งานด้านเทคโนโลยีสารสนเทศของโรงพยาบาลแพร่ ในปี ๒๕๕๙-๒๕๕๖๓ เพื่อให้เทคโนโลยีสารสนเทศของโรงพยาบาลแพร่สามารถใช้งานได้อย่างต่อเนื่อง มีประสิทธิภาพและมีความมั่นคงปลอดภัยสูงสุด ทั้งนี้ จะมีการตรวจสอบและประเมินความเสี่ยงที่มีแนวโน้มอาจจะเกิดขึ้น เพื่อบริหารจัดการได้อย่างถูกต้อง ไม่เกิดเหตุการณ์ ความเสียหาย พร้อมทั้งสิ้นปีให้มีการทำการตรวจสอบหาช่องโหว่ของระบบในทุกปี และทำการทบทวนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศก่อนสิ้นสุดแผนฯ ของปีงบประมาณ

สารบัญ

บทที่ ๑ บทนำ

๑. หลักการและเหตุผล

การบริหารความเสี่ยงเป็นเครื่องมือทางกลยุทธ์ที่สำคัญตามหลักการกำกับดูแลกิจการที่ดี ที่จะช่วยให้การบริหารงานและการตัดสินใจด้านต่างๆ เช่น การวางแผน การกำหนดกลยุทธ์ การติดตามควบคุม และวัดผลการปฏิบัติงาน ตลอดจนการใช้ทรัพยากรต่างๆ อย่างเหมาะสม มีประสิทธิภาพมากขึ้น และลดการสูญเสียและโอกาสที่ทำให้เกิดความเสียหายแก่องค์กร

ภายใต้สภาวะการดำเนินงานของทุกๆ องค์กรล้วนแต่มีความเสี่ยง ซึ่งเป็นความไม่แน่นอนที่อาจจะส่งผลกระทบต่อการดำเนินงานหรือเป้าหมายขององค์กร จึงจำเป็นต้องมีการจัดการความเสี่ยงเหล่านั้นอย่างเป็นระบบ โดยการระบุความเสี่ยงว่ามีปัจจัยเสี่ยงใดบ้างที่กระทบต่อการดำเนินงานหรือเป้าหมายขององค์กร วิเคราะห์ความเสี่ยงจากโอกาสและผลกระทบที่เกิดขึ้น จัดลำดับความสำคัญของความเสี่ยง กำหนดแนวทางในการจัดการความเสี่ยง และต้องคำนึงถึงความคุ้มค่าในการจัดการความเสี่ยงอย่างเหมาะสม

แผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศมีวัตถุประสงค์เพื่อเป็นแนวทำงานที่ใช้ตรวจสอบและ ประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ ด้วยการคาดการณ์ล่วงหน้า ในกรณีที่ความเสี่ยงเกิดขึ้นจริง และกรมฯ สามารถนำแนวทำงานจัดการความเสี่ยงนี้ไปใช้ในการดำเนินการได้

๒. วัตถุประสงค์ของแผนบริหารความเสี่ยง

๑) เพื่อให้ผู้บริหารและผู้ปฏิบัติงาน เข้าใจหลักการ และกระบวนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

๒) เพื่อให้การจัดการภายในกลุ่มงานสารสนเทศทางการแพทย์ข้อมูลมีประสิทธิภาพและมีความยืดหยุ่นในการปรับตัวให้ทันต่อการเปลี่ยนแปลงของเทคโนโลยีสารสนเทศสมัยใหม่ รวมทั้งลดโอกาสที่จะก่อให้เกิดความเสียหายที่ไม่ต้องการกับระบบเทคโนโลยีสารสนเทศ

๓) เพื่อให้ผู้ปฏิบัติงานได้รับทราบขั้นตอน และกระบวนการในการวางแผนบริหารความเสี่ยง

๔) เพื่อให้มีการปฏิบัติตามกระบวนการบริหารความเสี่ยงอย่างเป็นระบบและต่อเนื่อง

๕) เพื่อลดโอกาสและผลกระทบของความเสี่ยงที่จะเกิดขึ้นกับองค์กร

๖) เพื่อเป็นแนวทำงานการดำเนินการ กำกับดูแล ตรวจสอบเกี่ยวกับการบริหารจัดการและการเผยแพร่ ความรู้ความเข้าใจเกี่ยวกับการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศในโรงพยาบาลแพร่

๗) เพื่อช่วยเพิ่มประสิทธิภาพการตัดสินใจ โดยคำนึงถึงปัจจัยเสี่ยงและความเสี่ยงในด้านต่างๆ ที่น่าจะมีผลกระทบกับการดำเนินงาน วัตถุประสงค์และนโยบาย แล้วพิจารณาหาแนวทำงานในการป้องกันหรือจัดการ กับความเสี่ยงเหล่านั้น ก่อนที่จะเริ่มปฏิบัติงานหรือดำเนินงานตามแผน

๓. เป้าหมาย

๑) ผู้บริหารและผู้ปฏิบัติงาน มีความรู้ความเข้าใจเรื่องการบริหารความเสี่ยง เพื่อนำไปใช้ในการดำเนินงานตามยุทธศาสตร์ และแผนปฏิบัติงานประจำปีให้บรรลุตามวัตถุประสงค์และเป้าหมายที่กำหนดไว้

๒) ผู้บริหารและผู้ปฏิบัติงาน สามารถระบุความเสี่ยง วิเคราะห์ความเสี่ยง ประเมินความเสี่ยง และจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

๓) สามารถนำแผนบริหารความเสี่ยงไปใช้ในการบริหารงานที่รับผิดชอบ

๔) เพื่อพัฒนาความสามารถของบุคลากรและกระบวนการดำเนินงานภายในองค์กรอย่างต่อเนื่อง

๕) ความรับผิดชอบต่อความเสี่ยงและการบริหารความเสี่ยงถูกกำหนดขึ้นอย่างเหมาะสมทั่วทั้งองค์กร

๖) การบริหารความเสี่ยงได้รับการปลูกฝังให้เป็นวัฒนธรรมขององค์กร

๔. ประโยชน์ของการบริหารความเสี่ยง

การดำเนินการบริหารความเสี่ยงจะช่วยให้ผู้บริหารมีข้อมูลที่ใช้ในการตัดสินใจได้ดียิ่งขึ้นและทำให้องค์กรสามารถจัดการกับปัญหาอุปสรรคและอยู่รอดได้ในสถานการณ์ที่ไม่คาดคิดหรือสถานการณ์ที่อาจทำให้องค์กรเกิดความเสียหาย

ประโยชน์ที่คาดหวังว่าจะได้รับจากการดำเนินการบริหารความเสี่ยง มีดังนี้

๑) **เป็นส่วนหนึ่งของหลักการบริหารกิจการบ้านเมืองที่ดี** การบริหารความเสี่ยงจะช่วยคณะทำงานบริหารความเสี่ยงและผู้บริหารทุกระดับตระหนักถึงความเสี่ยงหลักที่สำคัญ และสามารถทำหน้าที่ในการกำกับดูแลองค์กรได้อย่างมีประสิทธิภาพและประสิทธิผลมากยิ่งขึ้น

๒) **สร้างฐานข้อมูลที่มีประโยชน์ต่อการบริหารและการปฏิบัติงานในองค์กร** การบริหารความเสี่ยงจะเป็นแหล่งข้อมูลสำหรับผู้บริหารในการตัดสินใจด้านต่างๆ ซึ่งรวมถึงการบริหารความเสี่ยง ซึ่งตั้งอยู่บนสมมุติฐานในการตอบสนองต่อเป้าหมายและภารกิจหลักขององค์กรรวมถึงระดับความเสี่ยงที่ยอมรับได้

๓) **ช่วยสะท้อนให้เห็นภาพรวมของความเสี่ยงต่างๆ ที่สำคัญได้ทั้งหมด** การบริหารความเสี่ยงจะทำให้บุคลากรภายในองค์กรมีความเข้าใจถึงเป้าหมายและภารกิจหลักขององค์กร และตระหนักถึงความเสี่ยงสำคัญที่ส่งผลกระทบในเชิงลบต่อองค์กรได้อย่างครบถ้วน ซึ่งครอบคลุมความเสี่ยงธรรมาภิบาล

๔) **เป็นเครื่องมือที่สำคัญในการบริหารงาน** การบริหารความเสี่ยงเป็นเครื่องมือที่ช่วยให้ผู้บริหารสามารถมั่นใจได้ว่าความเสี่ยงได้รับการจัดการอย่างเหมาะสมและทันเวลา รวมทั้งเป็นเครื่องมือที่สำคัญของผู้บริหารในการบริหารงานและการตัดสินใจในด้านต่างๆ เช่น การวางแผนการกำหนดกลยุทธ์ การติดตามควบคุมและวัดผลการปฏิบัติงาน ซึ่งส่งผลให้การดำเนินงานของโรงพยาบาลแพร่เป็นไปตามเป้าหมายที่กำหนด และสามารถปกป้องผลประโยชน์ รวมทั้งเพิ่มมูลค่าแก่องค์กร

๕) **ช่วยให้การพัฒนาองค์กรเป็นไปในทิศทางเดียวกัน** การบริหารความเสี่ยงทำให้รูปแบบการตัดสินใจในระดับการปฏิบัติงานขององค์กรมีการพัฒนาไปในทิศทางเดียวกัน เช่น การตัดสินใจโดยที่ผู้บริหารมีความเข้าใจในกลยุทธ์ วัตถุประสงค์ขององค์กร และระดับความเสี่ยงอย่างชัดเจน

๖) **ช่วยให้การพัฒนาการบริหารและจัดสรรทรัพยากรเป็นไปอย่างมีประสิทธิภาพและประสิทธิผล** การจัดสรรทรัพยากรเป็นไปอย่างเหมาะสม โดยพิจารณาถึงระดับความเสี่ยงในแต่ละกิจกรรม และการเลือกใช้มาตรการในการบริหารความเสี่ยง เช่น การใช้ทรัพยากรสำหรับกิจกรรมที่มีความเสี่ยงต่ำและกิจกรรมที่มีความเสี่ยงสูงย่อมแตกต่างกัน หรือการเลือกใช้มาตรการแต่ละประเภทย่อมใช้ทรัพยากรแตกต่างกัน เป็นต้น

๕. นิยามความเสี่ยง

๕.๑ ความเสี่ยง (Risk)

ความเสี่ยง หมายถึง เหตุการณ์หรือการกระทำใดๆ ที่อาจจะเกิดขึ้นภายในสถานการณ์ที่ไม่แน่นอน และจะส่งผล กระทบหรือสร้างความเสียหาย (ทั้งที่เป็นตัวเงินและไม่เป็นตัวเงิน) หรือก่อให้เกิดความล้มเหลวหรือ ลดโอกาสที่จะบรรลุวัตถุประสงค์และเป้าหมายขององค์กร ทั้งในด้านยุทธศาสตร์การปฏิบัติงาน การเงินและ การบริการ ซึ่งอาจเป็นผลกระทบทางบวกด้วยก็ได้ โดยวัดจากผลกระทบ (Impact) ที่ได้รับและโอกาสที่จะเกิด (Likelihood) ของเหตุการณ์

ลักษณะของความเสี่ยง สามารถแบ่งออกได้เป็น ๓ ส่วน ดังนี้

๑) ปัจจัยเสี่ยง คือ สาเหตุที่จะทำให้เกิดความเสี่ยง

๒) เหตุการณ์เสี่ยง คือ เหตุการณ์ที่ส่งผลกระทบต่อการดำเนินงาน หรือ นโยบาย

๓) ผลกระทบของความเสี่ยง คือ ความรุนแรงของความเสียหายที่น่าจะเกิดขึ้นจากเหตุการณ์เสี่ยง

๕.๒ **การประเมินความเสี่ยง (Risk Assessment)** หมายถึง กระบวนการระบุความเสี่ยง การวิเคราะห์ความเสี่ยง และจัดลาดับความเสี่ยง โดยการประเมินจากโอกาสที่จะเกิด (Likelihood) และผลกระทบ (Impact) เมื่อทำการประเมินแล้ว ทำให้ทราบระดับของความเสี่ยง (Degree of Risk) หมายถึง สถานะของความเสี่ยงที่ได้จากการประเมินโอกาสและผลกระทบของแต่ละปัจจัยเสี่ยง แบ่งออกเป็น ๔ ระดับ คือ สูงมาก สูง ปานกลาง และต่ำ

๕.๓ **การบริหารความเสี่ยง (Risk Management)** หมายถึง กระบวนการที่ใช้ในการบริหารจัดการ ให้โอกาส ที่จะเกิดเหตุการณ์ความเสี่ยงลดลง หรือผลกระทบของความเสียหายจากเหตุการณ์ความเสี่ยงลดลงอยู่ในระดับ ที่องค์กรยอมรับได้ ซึ่งการจัดการความเสี่ยง อาจแบ่งโดยสรุปได้เป็น ๔ แนวทำงานหลัก คือ การยอมรับ การลด/ควบคุมการยกเลิกและการโอนย้ายหรือแบ่งความเสี่ยง

๕.๔ **การควบคุม (Control)** หมายถึง นโยบาย แนวทำงานหรือขั้นตอนปฏิบัติต่างๆ ซึ่งกระทำเพื่อลดความเสี่ยง และทำให้การดำเนินการบรรลุวัตถุประสงค์ แบ่งได้ ๔ ประเภท คือ การควบคุมเพื่อการป้องกัน การควบคุมเพื่อให้ตรวจสอบ การควบคุมโดยการชี้แนะและการควบคุมเพื่อการแก้ไข

๕.๕ **ทรัพย์สิน (Asset)** หมายถึง ทรัพย์สินต่างๆ ขององค์กรแบ่งเป็น ๕ หมวด ได้แก่ หมวดข้อมูล หมวดบุคลากร หมวดฮาร์ดแวร์ หมวดซอฟต์แวร์ และหมวดบริการ

หลักการวิเคราะห์ ประเมิน และจัดทำความเสี่ยงอย่างเหมาะสม ตามกระบวนการบริหารความเสี่ยง ตามมาตรฐาน COSO (Committee of Sponsoring Organizations of the Tread way Commission) มีดังนี้

๑. การกำหนดเป้าหมายการบริหารความเสี่ยง (Objective Setting)
๒. การระบุความเสี่ยงต่างๆ (Event Identification)
๓. การประเมินความเสี่ยง (Risk Assessment)

๔. กลยุทธ์ที่ใช้ในการจัดการกับแต่ละความเสี่ยง (Risk Response)

๕. กิจกรรมการบริหารความเสี่ยง (Control Activities)

๖. ข้อมูลและการสื่อสารด้านบริหารความเสี่ยง (Information and Communication)

๗. การติดตามผลและเฝ้าระวังความเสี่ยงต่างๆ (Monitoring)

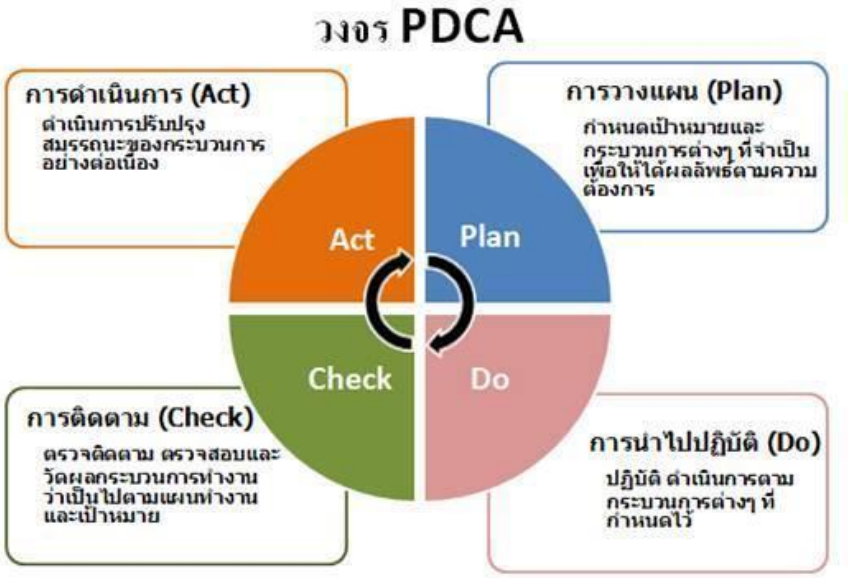
ทั้งนี้ ในการจัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ของโรงพยาบาลแพร่ ได้มีผู้เชี่ยวชาญด้านการตรวจประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ทฤษฎีที่เกี่ยงข้อง

ทฤษฎีที่เกี่ยงข้อง

๑. **BS๒๕๙๙๙ กับวงจร PCDA**

ในการบริหารความต่อเนื่องธุรกิจตามมาตรฐาน BS ๒๕๙๙๙ จะขับเคลื่อนด้วยวงจร PDCA ซึ่งประกอบด้วย การวางแผน (Plan) การลงมือทา (Do) การตรวจสอบ (Check) และ การปรับปรุง (Act)



รูปแบบจำลองวงจร PDCA

การวางแผน (Plan) ในขั้นตอนของการวางแผน จะเป็นการกำหนดนโยบายความต่อเนื่องทางธุรกิจ (Business continuity policy) รวมถึง วัตถุประสงค์ เป้าหมาย กระบวนการ และวิธีการปฏิบัติงานที่เกี่ยวข้องกับการจัดการกับความเสี่ยง และการปรับปรุงความต่อเนื่องทางธุรกิจ เพื่อให้สามารถสร้างผลลัพธ์ที่สอดคล้องกับนโยบายและวัตถุประสงค์โดยรวมขององค์กร

การดำเนินการ (Do) จะเป็นการลงมือดำเนินการ ตามนโยบาย การควบคุม กระบวนการ และวิธีการปฏิบัติงานในการรักษาความต่อเนื่องทางธุรกิจตามที่ได้กำหนดไว้

การตรวจสอบ (Check) ในขั้นตอนนี้จะเป็นการประเมิน และการวัดผลการดำเนินงานของแต่ละกระบวนการ เทียบกับนโยบายความต่อเนื่องทางธุรกิจ รวมถึงวัตถุประสงค์ในการปฏิบัติงานรวมถึงการรายงานผลลัพธ์ที่ได้ เพื่อนำไปสู่การทบทวนโดยฝ่ายบริหารต่อไป

การปรับปรุง (Act) จะเป็นการดำเนินการปฏิบัติการแก้ไขและป้องกัน จากผลของการทบทวน โดยฝ่ายบริหาร รวมถึงการดำเนินการปรับปรุงระบบการจัดการความเสี่ยง (Risk Management) ด้วย

บทที่ ๒ แนวทางการบริหารความเสี่ยง

๑. แนวทางดำเนินงานและกลไกการบริหารความเสี่ยง

๑.๑ แนวทางดำเนินงาน ในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ โรงพยาบาลแพร่ แบ่งเป็น ๒ ระยะ ดังนี้

<u>ระยะที่ ๑</u> การเริ่มต้นและพัฒนา

๑) กำหนดนโยบายหรือแนวทางในการบริหารจัดการความเสี่ยง
๒) ระบุปัจจัยเสี่ยง และประเมินโอกาส ผลกระทบจากปัจจัยเสี่ยง
๓) วิเคราะห์และจัดลำดับความสำคัญของปัจจัยเสี่ยงจากการดำเนินงาน
๔) จัดทำแผนบริหารความเสี่ยงของปัจจัยเสี่ยงที่อยู่ในระดับสูง (High) และสูงมาก (Extreme) รวมทั้งปัจจัยเสี่ยงที่อยู่ในระดับปานกลาง (Medium) ที่มีนัยสำคัญ
๕) สื่อสารทำความเข้าใจเกี่ยวกับแผนบริหารความเสี่ยงให้ผู้ปฏิบัติงานของกลุ่มงานสารสนเทศทางการแพทย์ รับทราบ และสามารถนำไปปฏิบัติได้
๖) รายงานความก้าวหน้าของการดำเนินงานตามแผนบริหารความเสี่ยง
๗) รายงานสรุปการประเมินผลความสำเร็จของการดำเนินการตามแผนบริหารความเสี่ยง

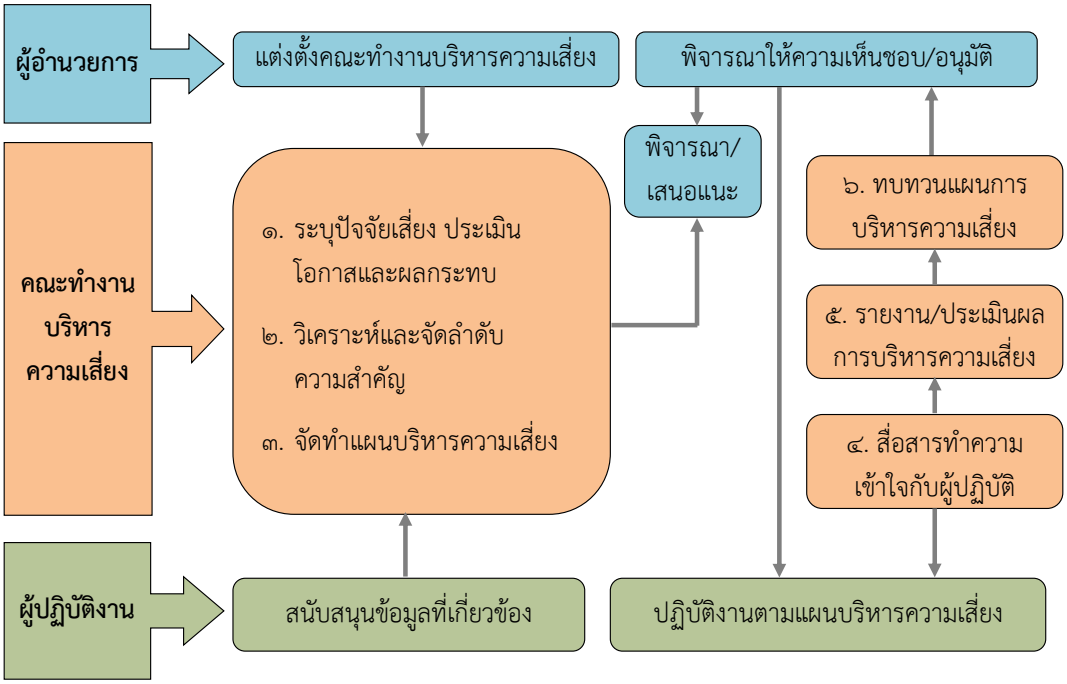
<u>ระยะที่ ๒</u> การพัฒนาสู่ความยั่งยืน

๑) ทบทวนแผนบริหารความเสี่ยงในปีที่ผ่านมา
๒) พัฒนากระบวนการบริหารความเสี่ยงสำหรับความเสี่ยงแต่ละประเภท
๓) ผลักดันให้มีการบริหารความเสี่ยงทั่วทั้งองค์กร
๔) พัฒนาขีดความสามารถบุคลากรในการดำเนินงานตามกระบวนการบริหารความเสี่ยง

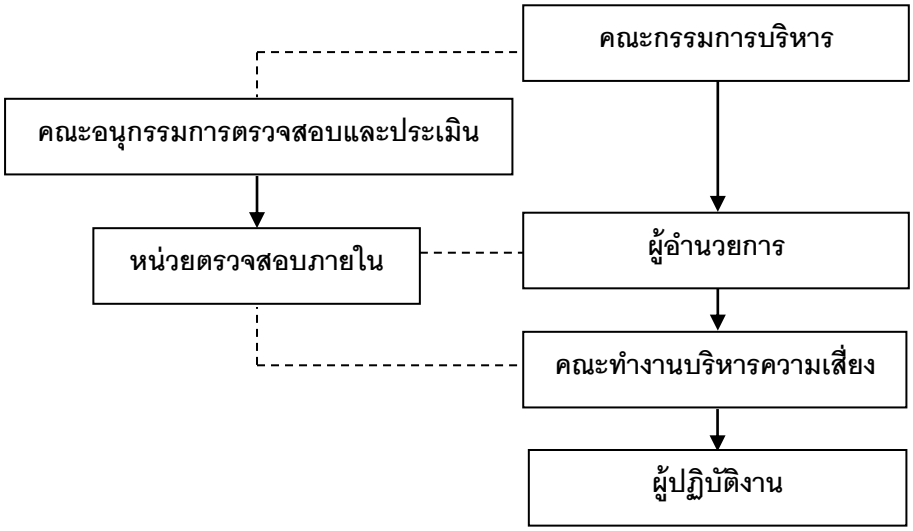
๑.๒ กลไกการบริหารความเสี่ยง ประกอบด้วย

๑) **ผู้อำนวยการ** มีหน้าที่แต่งตั้งคณะทำงานบริหารความเสี่ยง ส่งเสริมให้มีการบริหารจัดการความเสี่ยงอย่างมีประสิทธิภาพและเหมาะสม รวมทั้งพิจารณาให้ความเห็นชอบหรืออนุมัติแผนการบริหารความเสี่ยงเพื่อนำไปปฏิบัติต่อไป
๒) **คณะทำงานบริหารความเสี่ยง** มีหน้าที่ดำเนินการให้มีระบบการบริหารความเสี่ยง จัดทำแผนบริหารความเสี่ยง รายงานและประเมินผลการดำเนินงานตามแผนการบริหารความเสี่ยง รวมทั้งทบทวนแผนการบริหารความเสี่ยงเพื่อปรับปรุงการดำเนินงานต่อไปในอนาคต
๓) **ผู้ปฏิบัติงาน** บุคลากรที่มีหน้าที่สนับสนุนข้อมูลที่เกี่ยวข้องให้กับคณะทำงานบริหารความเสี่ยง และให้ความร่วมมือในการปฏิบัติงานตามแผนบริหารความเสี่ยง

กลไกการบริหารความเสี่ยง



๒. โครงสร้างการบริหารความเสี่ยง



หน้าที่ความรับผิดชอบตามโครงสร้าง

โครงสร้างการบริหารความเสี่ยง ประกอบไปด้วย การกำกับดูแล การตัดสินใจ การจัดทำแผน การดำเนินการ การติดตามประเมินผล และการสอบทาน ซึ่งในแต่ละองค์ประกอบมีอำนาจหน้าที่ดังนี้

๒.๑ คณะกรรมการบริหาร

๑) ส่งเสริมให้มีการดำเนินงานบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ
๒) ให้ความเห็นชอบและให้ข้อเสนอแนะต่อระบบและแผนการบริหารจัดการความเสี่ยง
๓) รับทราบผลการบริหารความเสี่ยงและเสนอแนะแนวทางการพัฒนา

๒.๒ คณะอนุกรรมการตรวจสอบและประเมิน

๑) ส่งเสริมและสนับสนุนให้การบริหารความเสี่ยงเป็นส่วนหนึ่งของการดำเนินงานเพื่อเพิ่มมูลค่าให้กับองค์การ
๒) รับทราบผลการบริหารความเสี่ยงและให้ข้อเสนอแนะเพื่อพัฒนาระบบการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ
๓) กำกับดูแลการพัฒนาและการปฏิบัติตามกรอบการบริหารความเสี่ยง

๒.๓ ผู้อำนวยการ

๑) แต่งตั้งคณะทำงานบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ
๒) ส่งเสริมและติดตามให้มีการบริหารความเสี่ยงอย่างมีประสิทธิภาพและเหมาะสม
๓) พิจารณาให้ความเห็นชอบและอนุมัติแผนการบริหารความเสี่ยง
๔) พิจารณาผลการบริหารความเสี่ยงและเสนอแนะแนวทางการพัฒนา

๒.๔ หน่วยตรวจสอบภายใน

๑) สอบทานกระบวนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ
๒) นำเสนอผลการบริหารความเสี่ยงให้คณะอนุกรรมการตรวจสอบและประเมินรับทราบและให้ข้อเสนอแนะ

๒.๕ คณะทำงานบริหารความเสี่ยง

๑) จัดให้มีระบบและกระบวนการบริหารความเสี่ยงที่เป็นระบบมาตรฐานเดียวกันทั้งองค์กร
๒) ดำเนินการตามกระบวนการบริหารความเสี่ยง และการปฏิบัติตามมาตรการลดและควบคุมความเสี่ยง
๓) รายงานและติดตามผลการดำเนินงานตามแผนการบริหารความเสี่ยงที่สำคัญ เสนอต่อผู้อำนวยการเพื่อพิจารณา

๒.๖ ผู้ปฏิบัติงาน

๑) สนับสนุนข้อมูลที่เกี่ยวข้องให้กับคณะทำงานบริหารความเสี่ยง
๒) ให้ความร่วมมือในการปฏิบัติงานตามแผนบริหารความเสี่ยง

บทที่ ๓ กระบวนการบริหารความเสี่ยง

กระบวนการบริหารความเสี่ยง เป็นกระบวนการที่ใช้ในการระบุ วิเคราะห์ ประเมิน และจัดลำดับความเสี่ยงที่มีผลกระทบต่อการบรรลุวัตถุประสงค์ในการดำเนินงานขององค์กร รวมทั้งการจัดทำแผนบริหารจัดการความเสี่ยง โดยกำหนดแนวทางการควบคุมเพื่อป้องกันหรือลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ ซึ่งกลุ่มงานสารสนเทศทางการแพทย์ มีขั้นตอนหรือกระบวนการบริหารความเสี่ยง ๖ ขั้นตอนหลัก ดังนี้

๑. การระบุความเสี่ยง (Risk identification)

เป็นกระบวนการที่ผู้บริหารและผู้ปฏิบัติงาน ร่วมกันระบุความเสี่ยงและปัจจัยเสี่ยง โดยต้องคำนึงถึงความเสี่ยงที่มีสาเหตุมาจากปัจจัยทั้งภายในและภายนอก ปัจจัยเหล่านี้มีผลกระทบต่อวัตถุประสงค์และเป้าหมายขององค์กร หรือผลการปฏิบัติงานทั้งในระดับองค์กรและระดับกิจกรรม ในการระบุปัจจัยเสี่ยงจะต้องพิจารณาว่ามีเหตุการณ์ใดหรือกิจกรรมใดของกระบวนการปฏิบัติงานที่อาจเกิดความผิดพลาดความเสียหายและไม่บรรลุวัตถุประสงค์ที่กำหนด รวมทั้งมีทรัพย์สินใดที่จำเป็นต้องได้รับการดูแลป้องกันรักษา ดังนั้นจึงจำเป็นต้องเข้าใจในความหมายของ “ความเสี่ยง (Risk)” “ปัจจัยเสี่ยง (Risk Factor)” และ “ประเภทความเสี่ยง” ก่อนที่จะดำเนินการระบุความเสี่ยงได้อย่างเหมาะสม

๑.๑ ความเสี่ยง (Risk)

หมายถึง เหตุการณ์หรือการกระทำใดๆ ที่อาจเกิดขึ้นภายใต้สถานการณ์ที่ไม่แน่นอนและจะส่งผลกระทบหรือสร้างความเสียหาย (ทั้งที่เป็นตัวเงินและไม่เป็นตัวเงิน) หรือก่อให้เกิดความล้มเหลว หรือลดโอกาสที่จะบรรลุเป้าหมายตามภารกิจหลักขององค์กร และเป้าหมายตามแผนปฏิบัติงาน

๑.๒ ปัจจัยเสี่ยง (Risk Factor)

หมายถึง ต้นเหตุ หรือสาเหตุที่มาของความเสี่ยง ที่จะทำให้ไม่บรรลุวัตถุประสงค์ที่กำหนดไว้ โดยต้องระบุได้ด้วยว่าเหตุการณ์นั้นจะเกิดที่ไหน เมื่อใด และเกิดขึ้นได้อย่างไร และทำไม ทั้งนี้สาเหตุของความเสี่ยงที่ระบุควรเป็นสาเหตุที่แท้จริง เพื่อจะได้วิเคราะห์และกำหนดมาตรการลดความเสี่ยงในภายหลังได้อย่างถูกต้อง โดยปัจจัยเสี่ยงแบ่งได้ ๒ ด้าน ดังนี้

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

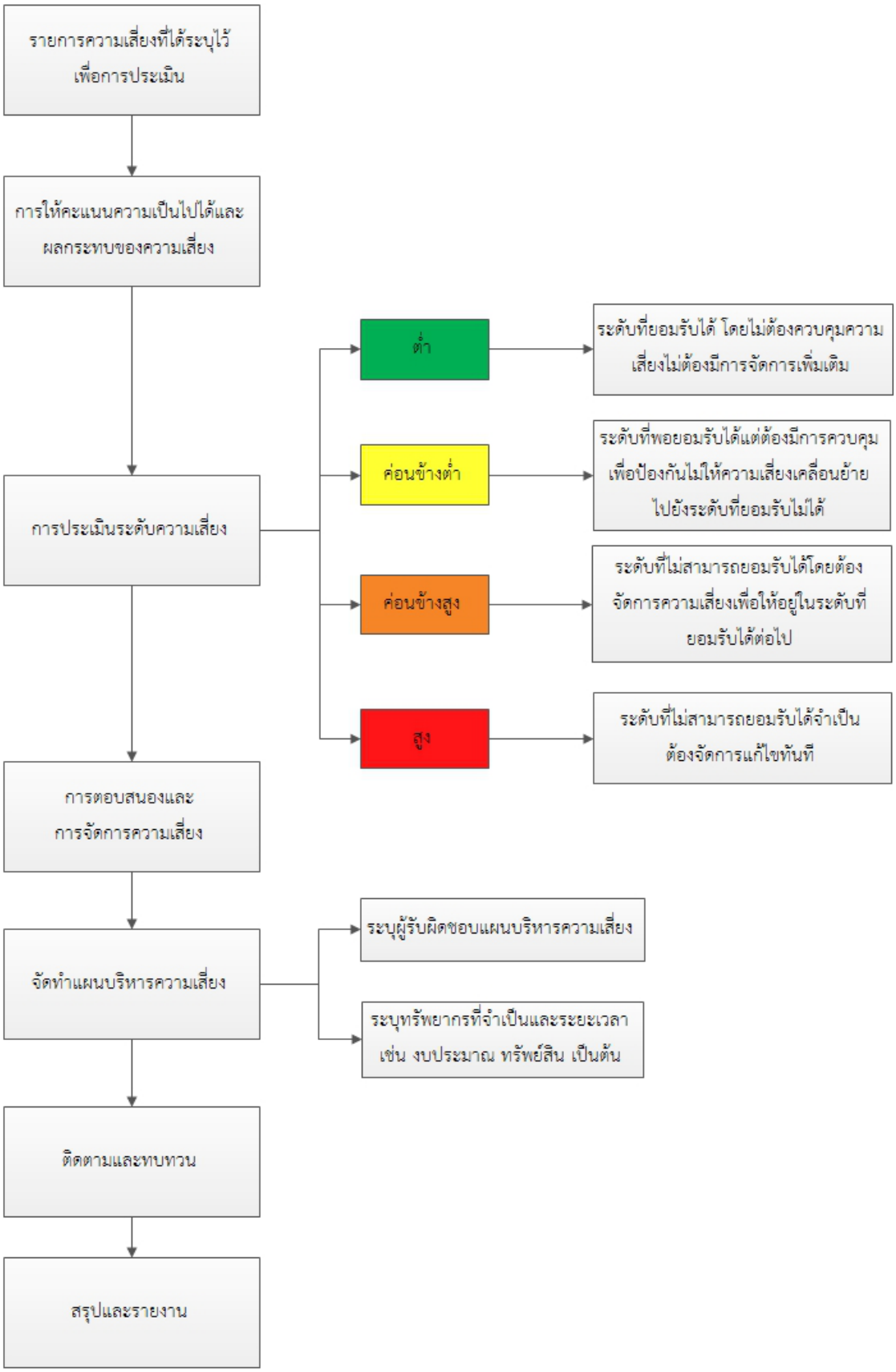
๒) ปัจจัยเสี่ยงภายใน คือ ความเสี่ยงที่สามารถควบคุมได้โดยองค์กร เช่น กฎระเบียบ ข้อบังคับภายในองค์กร วัฒนธรรมองค์กร นโยบายการบริหารและการจัดการ ความรู้/ความสามารถของบุคลากร กระบวนการทำงาน ข้อมูล/ระบบสารสนเทศ เครื่องมือ/อุปกรณ์

๑.๓ ประเภทความเสี่ยง

จากการวิเคราะห์ความเสี่ยงด้านสารสนเทศของโรงพยาบาลแพร่สามารถแยกประเภทความเสี่ยงเป็น ๕ ประเภท ดังนี้

- **ความเสี่ยงด้านความมั่นคงปลอดภัยของทรัพยากรในระบบเทคโนโลยีสารสนเทศ**
  - Hardware ,Software ,Network , Data
- **ความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศอาจทำให้เกิดความบกพร่องในการดูแลรักษาผู้ป่วย** เป็นความเสี่ยงที่อาจเกิดขึ้นจากระบบเทคโนโลยีสารสนเทศที่ส่งผลกระทบต่อการรักษาผู้ป่วย ทำให้ข้อมูลผิดพลาด ไม่ถูกต้องตรงกัน ข้อมูลที่สำคัญไม่อยู่ระบบ ข้อมูลที่จำเป็นและสำคัญไปถึงผู้ป่วยหรือผู้ให้บริการล่าช้า จนทำให้เกิดความบกพร่องในการดูแลรักษาผู้ป่วย เช่น ข้อมูลผู้ป่วยคนหนึ่งไปอยู่กับผู้ป่วยคนหนึ่ง , ข้อมูลไม่ครบถ้วน ขาดหาย , ข้อมูลไปถึงผู้ป่วยล่าช้า , การใช้ Default values ที่ผิดพลาด , ข้อมูลในคอมพิวเตอร์กับในกระดาษไม่ตรงกัน , การแก้ไขข้อมูลหลังจากมีผู้ได้รับข้อมูลนั้นไปแล้ว เป็นต้น
- **ความเสี่ยงด้านความเป็นส่วนตัวของผู้ป่วย** เป็นความเสี่ยงที่อาจเกิดขึ้นจากการดำเนินการการจัดความสำคัญในการเข้าถึงข้อมูลไม่เหมาะสมกับการใช้งานหรือการให้บริการ โดยผู้ใช้อาจเข้าสู่ระบบเทคโนโลยีสารสนเทศของโรงพยาบาลแพร่ หรือใช้ข้อมูลต่างๆ ของโรงพยาบาลแพร่เกินกว่าอำนาจหน้าที่ของตนเองที่มีอยู่และอาจทำให้เกิดความเสียหายต่อข้อมูลสารสนเทศได้ความเสี่ยงจากผู้ปฏิบัติงาน เป็นความเสี่ยงที่อาจเกิดขึ้นจากการดำเนินการการจัดความสำคัญในการเข้าถึงข้อมูลไม่เหมาะสมกับการใช้งานหรือการให้บริการ โดยผู้ใช้อาจเข้าสู่ระบบเทคโนโลยีสารสนเทศ หรือใช้ข้อมูลต่างๆ ของโรงพยาบาลแพร่ เกินกว่าอำนาจหน้าที่ของตนเองที่มีอยู่และอาจทำให้เกิดความเสียหายต่อข้อมูลสารสนเทศได้
- **ความเสี่ยงด้านภัยหรือสถานการณ์ฉุกเฉิน** เป็นความเสี่ยงที่อาจเกิดจากภัยพิบัติตามธรรมชาติหรือสถานการณ์ร้ายแรงที่ก่อให้เกิดความเสียหายร้ายแรงกับข้อมูลสารสนเทศ เช่น ไฟฟ้าขัดข้อง น้ำท่วม ไฟไหม้ อาคารถล่ม การชุมนุมประท้วง หรือความไม่สงบเรียบร้อยในบ้านเมือง เป็นต้น
- **ความเสี่ยงด้านการบริหารจัดการ** เป็นความเสี่ยงจากแนวนโยบายในการบริหารจัดการที่อาจส่งผลกระทบต่อการดำเนินการด้านเทคโนโลยีสารสนเทศ

แผนภูมิแนวทางและขั้นตอนการบริหารความเสี่ยง



ตารางที่ ๑ ลักษณะรายละเอียดของความเสี่ยง (Description of risk)

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ
๑. ความเสี่ยงในการเข้าถึงข้อมูลของบุคคลอื่น	RIT๐๑	ความเสี่ยงด้านความเป็นส่วนตัวของข้อมูลผู้ป่วย	ผู้ใช้ขาดความระมัดระวังในการเข้าใช้ระบบสารสนเทศ เช่น การมอบหมายให้ผู้อื่นใช้รหัสผ่านของตนเองเข้าใช้ระบบหรือใช้งานแทน	- การอำพรางหรือสวมรอยผู้ใช้ - การเข้าถึงข้อมูล / เปลี่ยนแปลงข้อมูล โดยไม่ได้รับอนุญาต	ผู้ใช้งาน ระบบสารสนเทศ ระบบฐานข้อมูล
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
๓. ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	RIT๐๓	ความเสี่ยงด้านภัยหรือสถานการณ์ฉุกเฉิน	การเกิดกระแสไฟฟ้าขัดข้อง หรือเกิดแรงดันไฟฟ้าไม่คงที่ ทำให้เครื่องคอมพิวเตอร์และอุปกรณ์อาจได้รับความเสียหายจากแรงดันไฟฟ้าที่ไม่คงที่ หรือ เมื่อกระแสไฟฟ้าขัดข้อง ทำให้เครื่องแม่ข่ายคอมพิวเตอร์ถูกปิดไปโดยไม่สมบูรณ์ อาจทำให้ข้อมูลสารสนเทศบางส่วนเกิดการสูญหาย และการให้บริการบางประเภทไม่สามารถเปิดใช้งานได้โดยอัตโนมัติ	- แหล่งกำเนิดไฟฟ้าขัดข้องหรือแรงดันไฟฟ้าไม่คงที่	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่แม่ข่าย อุปกรณ์เครือข่าย เครื่องคอมพิวเตอร์ ระบบฐานข้อมูล ระบบสารสนเทศ

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ
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 เครื่องคอมพิวเตอร์แม่แม่ข่าย ระบบฐานข้อมูล ระบบสารสนเทศ
๕. ความเสี่ยงจากการขาดแคลนบุคลากรผู้ปฏิบัติงาน	RIT๐๕	ความเสี่ยงด้านการบริหารจัดการ	การขาดแคลนบุคลากรด้านสารสนเทศ ทำให้การทำงานอาจหยุดชะงัก หากบุคลากรผู้รับผิดชอบไม่สามารถมาปฏิบัติงานได้ และจำนวนบุคลากรที่มีไม่เพียงพอต่อระบบเทคโนโลยีสารสนเทศที่เพิ่มขึ้นตามความต้องการของผู้ใช้งาน ส่งผลกระทบต่อการพัฒนาและควบคุมดูแลระบบ	- นโยบายจากกระทรวง	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย ระบบฐานข้อมูล ระบบสารสนเทศ ผู้รับบริการหรือผู้ป่วย
๖. ความเสี่ยงจากการเปลี่ยนแปลงนโยบายผู้บริหาร	RIT๐๖	ความเสี่ยงด้านการบริหารจัดการ	การเปลี่ยนแปลงผู้บริหาร อาจทำให้นโยบายการบริหารจัดการสารสนเทศเปลี่ยนแปลงด้วย ทำให้การดำเนินการโครงการต่างๆได้รับผลกระทบ		ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย ระบบฐานข้อมูล ระบบสารสนเทศ
๗. ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ	RIT๐๗	ความเสี่ยงด้านการบริหารจัดการ	การขาดแคลนงบประมาณในการดำเนินการให้ระบบสารสนเทศสามารถดำเนินการได้ต่อเนื่องอย่างมีประสิทธิภาพ		ผู้ใช้งาน ผู้ดูแลระบบ ระบบฐานข้อมูล ระบบสารสนเทศ

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

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ
๑๓. ความเสี่ยงการเปิดเผยข้อมูลผู้ป่วย	RIT๑๓	ความเสี่ยงด้านความเป็นส่วนตัวของผู้ป่วย	ผู้ใช้งานขาดความตระหนักเรื่องการเปิดเผยข้อมูลข้อมูลส่วนบุคคลของผู้ป่วย เช่น ภาพใบหน้า ชื่อ-สกุลผู้ป่วย เตียง ฯลฯ รวมไปถึงการแชร์ข้อมูลในสังคมออนไลน์	- การอำพรางหรือสวมรอยของมิจฉาชีพ - การฟ้องร้องจากผู้ป่วยเรื่องการเปิดเผยข้อมูลส่วนบุคคลก่อนได้รับอนุญาต	ผู้ป่วย ผู้ใช้งาน ความน่าเชื่อถือโรงพยาบาล
๑๔. ความเสี่ยงระบบฐานข้อมูลล่ม/เสียหาย	RIT๑๔	ความเสี่ยงด้านภัยหรือสถานการณ์ฉุกเฉิน	การเกิดสถานการณ์ฉุกเฉิน หรือฐานข้อมูลล่มเหลว ไม่สามารถทำงานได้ตามปกติ		ผู้ป่วย ผู้ใช้งาน ผู้ดูแลระบบ

๒. การประมาณความเสี่ยง (Risk estimation)

เป็นการดูปัญหาความเสี่ยงในแง่ของโอกาสการเกิดเหตุ (Incident) หรือเหตุการณ์ (Event) ว่ามีมากน้อยเพียงไรและผลที่ติดตามมาว่ามีความรุนแรงหรือเสียหายมากน้อยเพียงใด

เกณฑ์การประมาณ เป็นการกำหนดเกณฑ์ที่จะใช้ในการประมาณความเสี่ยง ได้แก่ ระดับโอกาสที่จะเกิดความเสี่ยง 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	๒-๓ปีต่อครั้ง
๑	น้อยมาก	๕ปีต่อครั้ง

ระดับความรุนแรงของผลกระทบของความเสี่ยง (Impact) เชิงคุณภาพ		
ระดับ	ผลกระทบ	คำอธิบาย
๕	สูงมาก	> ๑๐ ล้านบาท หรือ เกิดความสูญเสียต่อระบบ IT ที่สำคัญทั้งหมดและเกิดความเสียหายอย่างมากต่อความปลอดภัยของข้อมูลต่างๆ
๔	สูง	> ๕ แสนบาท – ๑๐ ล้านบาท หรือ เกิดปัญหากับระบบ 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 เครื่องคอมพิวเตอร์แม่แม่ข่าย 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

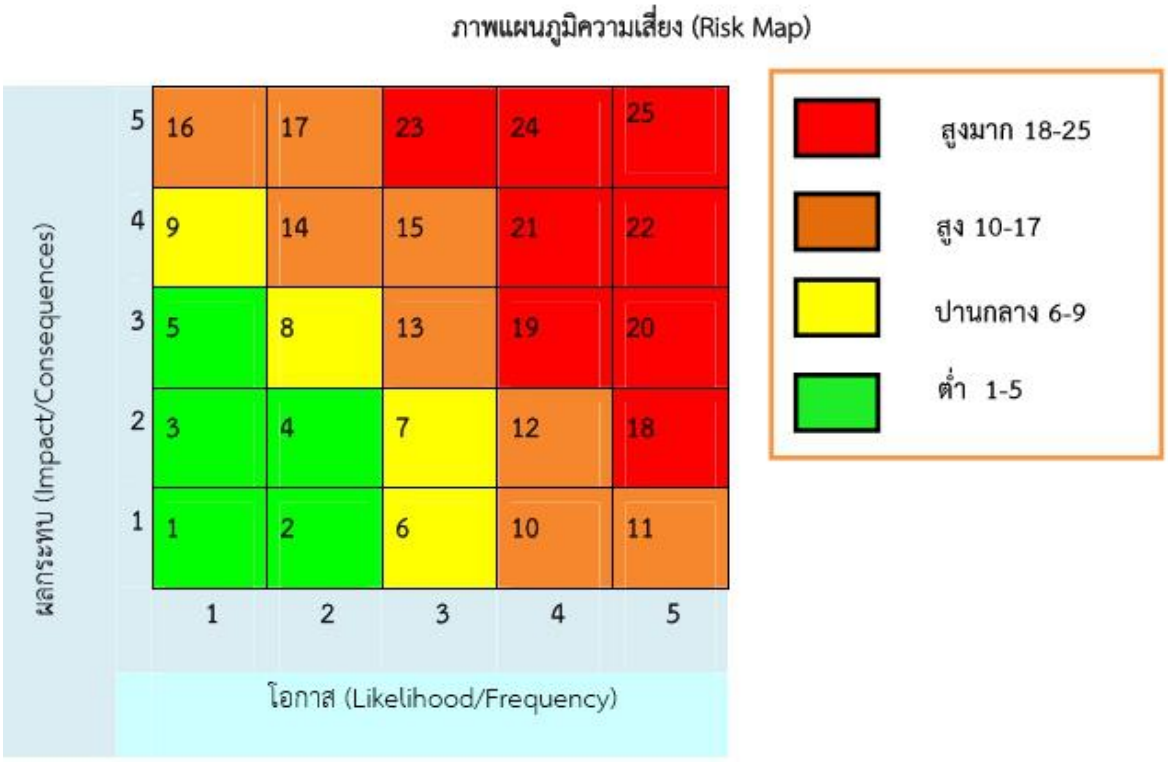
มาก

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

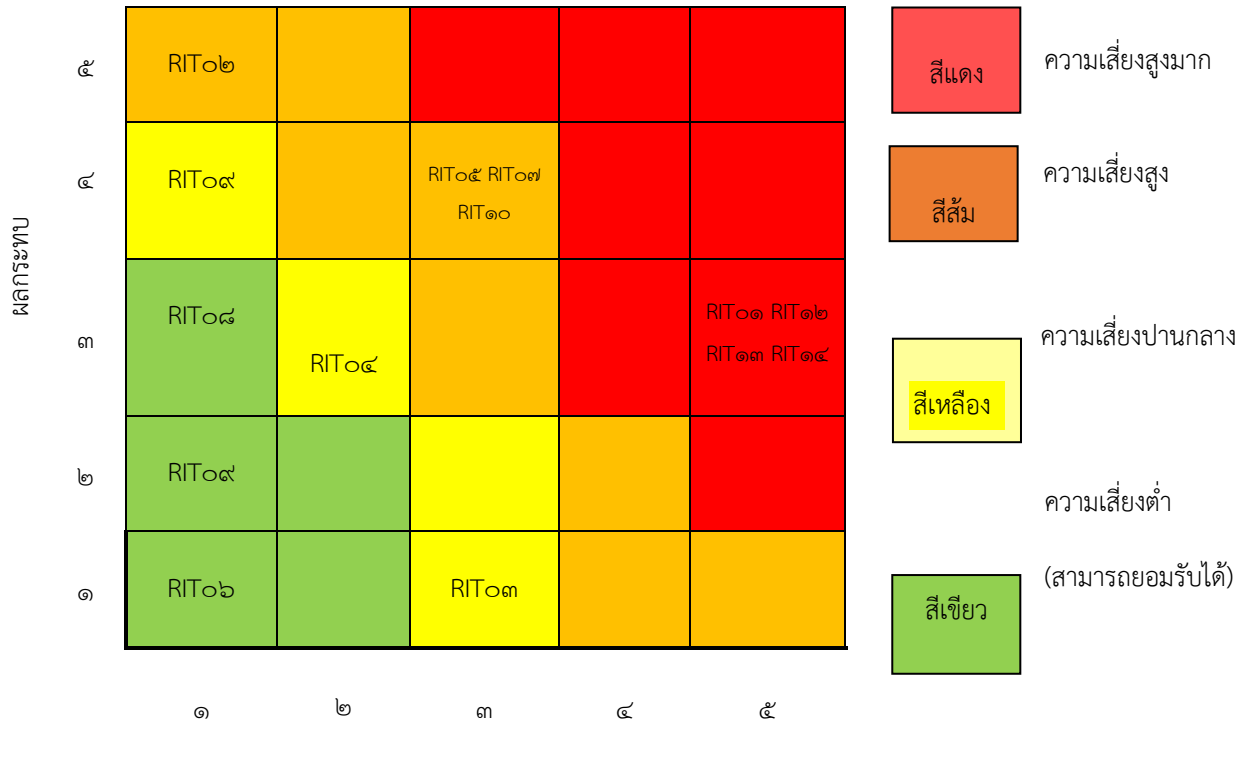
ตารางที่ ๓ สรุปผลการประเมินค่าความเสี่ยง (Risk evaluation)

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)



การรายงานผลการวิเคราะห์ความเสี่ยง (Risk reporting)

จากผลการประเมินความเสี่ยง สามารถจัดลำดับความสำคัญของความเสี่ยงด้านเทคโนโลยีสารสนเทศของโรงพยาบาลแพร่ ในการบริหารจัดการได้อย่างมีประสิทธิภาพดังนี้

ลำดับ	ความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ค่าระดับความเสี่ยง
๑	RIT๑๒ ความเสี่ยงในการดูแลผู้ป่วย	ความเสี่ยงด้านด้านระบบเทคโนโลยีสารสนเทศอาจทำให้เกิดความบกพร่องในการดูแลรักษาผู้ป่วย	เกิดจากระบบเทคโนโลยีสารสนเทศอาจทำให้เกิดความบกพร่องในการดูแลผู้ป่วย รักษาผู้ป่วย เช่น ข้อมูลผู้ป่วยคนหนึ่งไปอยู่กับผู้ป่วยคนหนึ่ง , ข้อมูลไม่ครบถ้วน ขาดหาย , ข้อมูลไปถึงผู้ป่วยล่าช้า , การใช้ Default values ที่ผิดพลาด , ข้อมูลในคอมพิวเตอร์กับในกระดาษไม่ตรงกัน , การแก้ไขข้อมูลหลังจากมีผู้ได้รับข้อมูลนั้นไปแล้ว เป็นต้น	**HH**
๒	RIT๐๑ ความเสี่ยงในการเข้าถึงข้อมูลของบุคคลอื่น	ความเสี่ยงด้านด้านความมั่นคงปลอดภัยของทรัพยากรในระบบเทคโนโลยีสารสนเทศ	ผู้ใช้ขาดความระมัดระวังในการเข้าใช้ระบบสารสนเทศ เช่น การมอบหมายให้ผู้อื่นใช้รหัสผ่านของตนเองเข้าใช้ระบบหรือใช้งานแทน	HH
๓	RIT๑๓ ความเสี่ยงการเปิดเผยข้อมูลผู้ป่วย	ความเสี่ยงด้านความเป็นส่วนตัวของข้อมูลผู้ป่วย	ผู้ใช้ขาดความระมัดระวังในการเข้าใช้ระบบสารสนเทศ เช่น การมอบหมายให้ผู้อื่นใช้รหัสผ่านของตนเองเข้าใช้ระบบหรือใช้งานแทน	**HH**
๔	RIT๑๔ ความเสี่ยงระบบฐานข้อมูลล่ม/เสียหาย	ด้านระบบเทคโนโลยีสารสนเทศ	ระบบฐานข้อมูลล่ม หรือเสียหายไม่สามารถเชื่อมต่อระบบฐานข้อมูลได้	**HH**
๕	RIT๐๗ ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ	ความเสี่ยงด้านการบริหารจัดการ	การขาดแคลนงบประมาณในการดำเนินการให้ระบบสารสนเทศสามารถดำเนินการได้ต่อเนื่องอย่างมีประสิทธิภาพ	**H**
๖	RIT๐๒ ความเสี่ยงจากการนำเอาอุปกรณ์อื่นที่ไม่ได้รับอนุญาตมาเชื่อมต่อ	ความเสี่ยงด้านการบริหารจัดการ	ผู้ใช้ขาดความระมัดระวังในการใช้ระบบเครือข่าย เช่น การนำ wireless router หรือ switch/hub มาเชื่อมต่อกับระบบเครือข่ายสำนักงานจังหวัด (มหาดไทย) โดยไม่ได้รับอนุญาต และไม่ได้มีการตั้งค่าเครื่องที่ถูกต้อง ทำให้เครื่องคอมพิวเตอร์อื่นในระบบเครือข่ายไม่สามารถใช้งานได้ หรือ การไม่ได้ตั้งค่าการรักษาความปลอดภัย ทำให้เครื่องคอมพิวเตอร์ของบุคคลภายนอกอื่นๆที่รับสัญญาณได้ เชื่อมต่อเข้ากับระบบเครือข่าย	H
๗	RIT๐๕ ความเสี่ยงจากการขาด	ความเสี่ยงด้านการบริหาร	การขาดแคลนบุคลากรด้านสารสนเทศ ทำให้การทำงานอาจหยุดชะงัก หากบุคลากรผู้รับผิดชอบ	H

ลำดับ	ความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ค่าระดับความเสี่ยง
	แคลนบุคลากรผู้ปฏิบัติงาน	จัดการ	ไม่สามารถมาปฏิบัติงานได้ และจำนวนบุคลากรที่มีไม่เพียงพอต่อระบบเทคโนโลยีสารสนเทศที่เพิ่มขึ้นตามความต้องการของผู้ใช้งาน ส่งผลกระทบต่อการพัฒนาและควบคุมดูแลระบบ	
๘	RIT๑๐ ความเสี่ยงจากเครื่องคอมพิวเตอร์หรืออุปกรณ์ขัดข้อง ไม่สามารถทำงานได้ตามปกติ	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	เครื่องคอมพิวเตอร์หรืออุปกรณ์ชำรุดหรือขัดข้องด้วยสาเหตุทางเทคนิค หรือจากสัตว์กัดแทะเช่น หนูหรือแมลง เป็นต้น	H
๙	RIT๐๔ ความเสี่ยงจากการถูกบุกรุก โดยผู้ไม่ประสงค์ดี	ความเสี่ยงด้านด้านความมั่นคงปลอดภัยของทรัพยากรในระบบเทคโนโลยีสารสนเทศ	การบุกรุกโจมตีโดยผู้ไม่ประสงค์ดี เช่น hacker เป็นต้น การดักจับข้อมูล การส่งข้อมูลคำสั่งเจตนาร้าย การติดไวรัส หรือ เวิร์ม	M
๑๐	RIT๐๓ ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดกระแสไฟฟ้าขัดข้อง หรือเกิดแรงดันไฟฟ้าไม่คงที่ ทำให้เครื่องคอมพิวเตอร์และอุปกรณ์อาจได้รับความเสียหายจากแรงดันไฟฟ้าที่ไม่คงที่ หรือ เมื่อกระแสไฟฟ้าขัดข้อง ทำให้เครื่องแม่ข่ายคอมพิวเตอร์ถูกปิดไปโดยไม่สมบูรณ์ อาจทำให้ข้อมูลสารสนเทศบางส่วนเกิดการสูญหาย และการให้บริการบางประเภทไม่สามารถเปิดใช้งานได้โดยอัตโนมัติ	M
๑๑	RIT๐๘ ความเสี่ยงจากการเกิดไฟไหม้ แผ่นดินไหว อาคารถล่ม	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดไฟไหม้อาคาร แผ่นดินไหวจนอาคารถล่ม ไม่สามารถเคลื่อนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆได้ ทำให้ได้รับความเสียหายทั้งหมด	L
๑๒	RIT๑๑ ความเสี่ยงจากการโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์	ความเสี่ยงด้านด้านความมั่นคงปลอดภัยของทรัพยากรในระบบเทคโนโลยีสารสนเทศ	การโจรกรรมเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ หรือชิ้นส่วนภายในเครื่อง เช่น CPU และ Ram ทำให้ไม่สามารถปฏิบัติงาน หรือเกิดการสูญหายของข้อมูลบนเครื่องคอมพิวเตอร์นั้นได้	L
๑๓	RIT๐๙ ความเสี่ยงจากสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดสถานการณ์ความรุนแรง หรือความไม่สงบเรียบร้อย จนทำให้บุคลากรไม่สามารถปฏิบัติงานได้ตามปกติ	L
๑๔	RIT๐๖ ความเสี่ยงจากการเปลี่ยนแปลงนโยบายผู้บริหาร	ความเสี่ยงด้านการบริหารจัดการ	การเปลี่ยนแปลงผู้บริหาร อาจทำให้นโยบายการบริหารจัดการสารสนเทศเปลี่ยนแปลงด้วย ทำให้การดำเนินการโครงการต่างๆได้รับผลกระทบ	L

๕. การจัดการความเสี่ยง (Risk management)

นโยบายของกลุ่มงานเทคโนโลยีสารสนเทศทางการแพทย์ โรงพยาบาลแพร่ ระดับความเสี่ยงคงเหลือที่ยอมรับได้ ≤ ๕

กำหนดให้ความเสี่ยงที่จำเป็นต้องนำมาดำเนินการจัดการความเสี่ยง คือ ความเสี่ยงที่มีระดับความเสี่ยงสูง ตั้งแต่ ๑๕ ขึ้นไป ส่วนความเสี่ยงที่มีระดับความเสี่ยงต่ำกว่า ๑๕ ถือว่ามีความเสี่ยงค่อนข้างต่ำอาจจะนำมาดำเนินการจัดการความเสี่ยงในแผนบริหารความเสี่ยงหรือไม่ก็ได้ การดำเนินการจัดการความเสี่ยงเป็นดังตารางที่ ๕

๑. หลีกเลี่ยงความเสี่ยง (Risk Avoidance = RA) การหลีกเลี่ยงความเสี่ยง เช่น เมื่อพบว่าปัจจุบันโรงพยาบาล มีการสำรองข้อมูลเพียง ๑ ชุดและจัดเป็นความเสี่ยงต่อการสูญเสีย การเลี่ยงความเสี่ยงนี้อาจได้แก่การทำสำรองข้อมูล ๒ ชุด และแยกเก็บในสถานที่ต่างกัน การบริหารจัดการการเชื่อมโยงสู่เครือข่ายผ่านโมเด็ม ถ้าเป็นการยากต่อการควบคุมหรือบริหารจัดการ องค์กรอาจเลือกทางออกโดยการยกเลิกไม่ให้ใช้บริการ และแนะนำให้พนักงานใช้บริการผ่านทาง ISP ในช่วงที่มีการระบาดของไวรัสอย่างหนัก องค์กรอาจมีเลือกระงับไม่ให้ใช้คอมพิวเตอร์ที่ไม่ได้ติดตั้ง Antivirus เป็นต้น

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

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

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

ตารางที่ ๔ การจัดการความเสี่ยง (Risk management)

ลำดับ	ความเสี่ยง	ค่าระดับความเสี่ยง	กลยุทธ์การจัดการความเสี่ยง	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 โดยคณะกรรมทีมบริหารความเสี่ยงโรงพยาบาลแพร่ ๓. จัดทำแผนรับสถานการณ์เพื่อให้สามารถดำเนินการได้อย่างต่อเนื่อง (Business Continuity Plan : BCP)	**LR**
๒	RIT๑๔ ความเสี่ยงระบบฐานข้อมูลล่ม/เสียหาย	๒๐	- ยอมรับความเสี่ยง - ถ่ายโอนความเสี่ยง - หลีกเลี่ยงความเสี่ยง	๑. ระบบฐานข้อมูล สัญญาการบำรุงรักษาหลังขาย (Maintenance service) ได้แก่ ระบบฐานข้อมูลผู้ป่วย **HOSxP,**ระบบเวชระเบียนอิเล็กทรอนิกส์ **Binary** , ระบบสำนักงาน **(Express),**ระบบภาพรังสี **(PACs)** ๒. มีระบบสำรองข้อมูลมากกว่า ๑ ชุด กรณีระบบฐานข้อมูลผู้ป่วย	**RC** **RF** **RA**
๓	RIT๑๓ ความเสี่ยงการเปิดเผยข้อมูลผู้ป่วย	๒๐	- ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)	๑. สร้างความตระหนักในเรื่องของข้อมูลส่วนบุคคล ในการพึงรักษาสิทธิ์ในส่วนของข้อมูลส่วนบุคคล ๒. กำกับดูแลการปฏิบัติตามระเบียบปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศอย่างเคร่งครัด	**LR**
๔	RIT๐๑ ความเสี่ยงในการเข้าถึงข้อมูลของบุคคลอื่น	**๒๐**	- ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)	๑. สร้างความตระหนักในเรื่องของข้อมูลส่วนบุคคล ในการพึงรักษาสิทธิ์ในส่วนของข้อมูลส่วนบุคคล ๒. กำกับดูแลการปฏิบัติตามระเบียบปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศอย่างเคร่งครัด	**LR**

ลำดับ	ความเสี่ยง	ค่าระดับความเสี่ยง	กลยุทธ์การจัดการความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง	กลยุทธ์
๕	RIT๐๒ ความเสี่ยงจากการนำเอาอุปกรณ์อื่นที่ไม่ได้รับอนุญาตมาเชื่อมต่อ	๑๖	- ยอมรับความเสี่ยง (มีมาตรการติดตาม)	๑. สร้างความตระหนักในเรื่องนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ ๒. กระตุ้นให้เกิดการปฏิบัติตามแนวนโยบายหรือระเบียบด้านสารสนเทศอย่างจริงจัง ๓. ใช้อุปกรณ์เครือข่ายที่สามารถจำกัดสิทธิ์การเข้าถึงสำหรับอุปกรณ์ที่ไม่ได้รับอนุญาตให้เชื่อมต่อเข้าเครือข่าย	RC LR
๖	RIT๐๕ ความเสี่ยงจากการขาดแคลนบุคลากรผู้ปฏิบัติงาน	๑๕	- ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)	๑. ปรับปรุงโครงสร้างศูนย์สารสนเทศ และสรรหาบุคลากรเพื่อรองรับงานอย่างเหมาะสม ๒. จัดทำคู่มือกระบวนการทำงานเพื่อให้บุคลากรอื่นสามารถปฏิบัติตามคู่มือได้กรณีที่บุคลากรผู้รับผิดชอบไม่สามารถมาปฏิบัติงานได้ ๓. จัดตารางเวรและช่องทางการติดต่อสื่อสารตลอด ๒๔ ชั่วโมง	LR
๗	RIT๐๗ ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ	๑๕	- ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)	๑. จัดทำแผนแม่บทเทคโนโลยีสารสนเทศ เพื่อแสดงความจำเป็นในการขอสนับสนุนงบประมาณในการดำเนินการด้านเทคโนโลยีสารสนเทศ	LR
๘	RIT๑๐ ความเสี่ยงจากเครื่องคอมพิวเตอร์หรืออุปกรณ์ขัดข้อง ไม่สามารถทำงานได้ตามปกติ	๑๕	- ยอมรับความเสี่ยง (มีมาตรการติดตาม)	๑. หาทางป้องกันสัตว์กัดแทะอุปกรณ์ ๒. จัดหาเครื่องและอุปกรณ์สำรองเพื่อให้สามารถใช้ทดแทนชั่วคราว เพื่อสามารถปฏิบัติงานได้ ๓. จัดทำแผนการตรวจสอบและจัดจ้างบำรุงรักษาเครื่องและอุปกรณ์อย่างสม่ำเสมอ	RC RA
๙	RIT๐๔ ความเสี่ยงจากการถูกบุกรุกโดยผู้ไม่ประสงค์ดี	๘	- ยอมรับความเสี่ยง	- ตรวจสอบการตั้งค่าของ firewall อย่างสม่ำเสมอ - ติดตั้งระบบตรวจสอบการบุกรุกเครือข่าย และติดตามเพื่อปรับปรุงอย่างสม่ำเสมอ - ติดตั้งโปรแกรมป้องกันไวรัสและ patch อย่างสม่ำเสมอ - ติดตั้ง patch ของระบบปฏิบัติการอย่างสม่ำเสมอ - เปลี่ยนรหัสผ่านตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ	RC RA
๑๐	RIT๐๓ ความเสี่ยงจากกระแสไฟฟ้า	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

๖. แผนปฏิบัติการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

จากการจัดการความเสี่ยง สามารถนำมาจัดทำแผนปฏิบัติบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร โดยมีหน่วยงานรับผิดชอบคือกลุ่มงานสารสนเทศทางการแพทย์โรงพยาบาลแพร่ ระยะเวลาดำเนินการระหว่างเดือน ตุลาคม ๒๕๖๑ – ๒๕๖๓

โครงการ/กิจกรรม/กระบวนการ แผนปฏิบัติการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ๒๕๖๑ - ๒๕๖๓

ประเภทความเสี่ยง	แนวทางการควบคุม	ระยะเวลาเริ่มต้น/สิ้นสุด	ปีงบ ๒๕๖๑				ปีงบ ๒๕๖๒				ปีงบ ๒๕๖๓				งบประมาณ	ผู้รับผิดชอบ
			Q๑	Q๒	Q๓	Q๔	Q๑	Q๒	Q๓	Q๔	Q๑	Q๒	Q๓	Q๔		
๑. ความเสี่ยงจากการเกิดไฟไหม้ น้ำท่วม แผ่นดินไหว อาคารถล่ม	- ตรวจสอบความพร้อมใช้ของอุปกรณ์ดับเพลิง - จัดทำแผนในการเคลื่อนย้ายอุปกรณ์ตามลำดับความสำคัญ - จัดทำแผนรับสถานการเพื่อให้สามารถดำเนินการได้อย่างต่อเนื่อง (Business Continuity Plan : BCP) และ DRP	- ทุก ๖ เดือน - เดือน ต.ค. - ทุกปี		●		●		●		●		●		●	NA	ฝ่ายบริหาร กลุ่มสารสนเทศทางการแพทย์

**** โครงการ/กิจกรรม/กระบวนการ แผนปฏิบัติการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (ต่อ)*

ประเภทความเสี่ยง	แนวทางการควบคุม	ระยะเวลาเริ่มต้น/สิ้นสุด	ปีงบ ๒๕๖๑				ปีงบ ๒๕๖๒				ปีงบ ๒๕๖๓				งบประมาณ	ผู้รับผิดชอบ
			Q๑	Q๒	Q๓	Q๔	Q๑	Q๒	Q๓	Q๔	Q๑	Q๒	Q๓	Q๔		
๒. ความเสี่ยงจากผู้ใช้งานสารสนเทศขาดความระมัดระวังและการตระหนักถึงความสำคัญของความปลอดภัยด้านเทคโนโลยีสารสนเทศ	- ฝึกอบรม เผยแพร่และประชาสัมพันธ์เรื่องความมั่งคงปลอดภัยเทคโนโลยีสารสนเทศ - กำกับดูแลการปฏิบัติตามแนวปฏิบัติด้านการรักษาความมั่งคงปลอดภัยด้านเทคโนโลยีสารสนเทศอย่างเคร่งครัด	- ตลอดปี - ตลอดปี	←											→	NA	กลุ่มสารสนเทศทางการแพทย์ กลุ่มสารสนเทศทางการแพทย์, คณะกรรมการ MIS
๓. ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	- ถ่ายโอนความเสี่ยง ๑. แจ้งให้กลุ่มงานไฟฟ้าดำเนินการปรับปรุงระบบไฟฟ้า ๒.ตรวจสอบความพร้อมของระบบสำรองไฟฟ้า	- เดือน ต.ค. ๒๕๖๑ - ทุกปี				●								←		NA	กลุ่มบริหารส่วนกลาง (ไฟฟ้า)

**** โครงการ/กิจกรรม/กระบวนการ แผนปฏิบัติการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (ต่อ)*

ประเภทความเสี่ยง	แนวทางการควบคุม	ระยะเวลาเริ่มต้น/สิ้นสุด	ปีงบ ๒๕๖๑				ปีงบ ๒๕๖๒				ปีงบ ๒๕๖๓				งบประมาณ	ผู้รับผิดชอบ
			Q๑	Q๒	Q๓	Q๔	Q๑	Q๒	Q๓	Q๔	Q๑	Q๒	Q๓	Q๔		
๔.ความเสี่ยงจากการการถูกบุกรุก โดยผู้ไม่ประสงค์ดี	- ตรวจสอบการตั้งค่าของ Firewall, PS อย่างสม่ำเสมอ	- ตลอดปี	←											→	NA	กลุ่มสารสนเทศทางการแพทย์
	- บริหารจัดการระบบตรวจสอบการบุกรุกเครือข่ายและติดตามเพื่อปรับปรุงอย่างสม่ำเสมอ	- ตลอดปี	←											→		กลุ่มสารสนเทศทางการแพทย์
	- ติดตั้งโปรแกรมป้องกันไวรัสและ Patch ของระบบ	- ทุก ๖ ปี				●										
	- ติดตั้ง patch ของระบบปฏิบัติการอย่างสม่ำเสมอ	เดือน มิ.ย. ๒๕๖๑		●											๒๘,๖๐๐๐	
	- จัดทำแผนจัดซื้อ Firewall ทดแทน															
	- อับเดท Firmware content ของระบบ Firewall															

ประเภทความเสี่ยง	แนวทางการควบคุม	ระยะเวลาเริ่มต้น/สิ้นสุด	ปีงบ ๒๕๖๑				ปีงบ ๒๕๖๒				ปีงบ ๒๕๖๓				งบประมาณ	ผู้รับผิดชอบ
			Q๑	Q๒	Q๓	Q๔	Q๑	Q๒	Q๓	Q๔	Q๑	Q๒	Q๓	Q๔		
๕.ความเสี่ยงจากการเชื่อมต่อเครือข่ายอินเทอร์เน็ตล้มเหลวหรือไม่สามารถใช้งานได้	- สำรวจและจัดหาระบบเครือข่ายอินเทอร์เน็ตสำรองเพื่อเป็นช่องทางให้ระบบอินเทอร์เน็ตใช้งานได้อย่างต่อเนื่อง - ตรวจสอบการเชื่อมต่อเครือข่ายอินเทอร์เน็ต	- เดือนต.ค.	←			→								→	NA	กลุ่มสารสนเทศทางการแพทย์ กลุ่มสารสนเทศทางการแพทย์
๖. ความเสี่ยงด้านภัยหรือสถานการณ์ฉุกเฉินร้ายแรงมากที่สุด	- จัดทำแผน ขั้นตอนการอนุมัติ การติดตั้งเพื่อให้สามารถดำเนินการได้อย่างต่อเนื่อง (Business Continuity Plan : BCP) และ DRP - จัดทำคู่มือแผนบริหารความต่อเนื่อง (BCP) และแผนกู้คืนระบบ DRP	ทบทวนแผนทุกปี ทบทวนแผนทุกปี				●				●				●	๓,๐๒๐,๐๐๐	กลุ่มงานสารสนเทศทางการแพทย์, คณะกรรมการ MIS

**** โครงการ/กิจกรรม/กระบวนการ แผนปฏิบัติการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (ต่อ)*

ประเภทความเสี่ยง	แนวทางการควบคุม	ระยะเวลาเริ่มต้น/สิ้นสุด	ปีงบ ๒๕๖๑				ปีงบ ๒๕๖๒				ปีงบ ๒๕๖๓				งบประมาณ	ผู้รับผิดชอบ
			Q๑	Q๒	Q๓	Q๔	Q๑	Q๒	Q๓	Q๔	Q๑	Q๒	Q๓	Q๔		
๗. ความเสี่ยงจากการไม่ได้รับงบประมาณในการบำรุงรักษาระบบสารสนเทศและระบบคอมพิวเตอร์อย่างต่อเนื่องและเพียงพอ	- มีการสำรวจและรวบรวมความต้องการอย่างต่อเนื่อง เพื่อการจัดทำงบประมาณในแต่ละปี - มีการหารือ ชี้แจ้งและทำความเข้าใจกับผู้บังคับบัญชาในเรื่องงบประมาณที่ต้องการใช้อย่างชัดเจน	- เดือน มิ.ย. ถึง ก.ย. - เดือนก.ย.		←	→ ●			←	→ ●			←	→ ●		NA	กลุ่มงานสารสนเทศทางการแพทย์, คณะกรรมการ MIS
๘. ความเสี่ยงระบบเทคโนโลยีอาจทำให้เกิดความบกพร่องในการดูแลผู้ป่วย	- เมื่อพบเหตุอุบัติการณ์ให้รายงานทุกครั้ง - ควบคุม ติดตาม ดูแลโดยคณะกรรการความเสี่ยงรพ.แพร่	- ตลอดปี - ตลอดปี	←	—	—	→	←	—	—	→	←	—	—	→	NA	คณะกรรมการความเสี่ยง รพ.แพร่, คณะกรรมการ MIS

ประเภทความเสี่ยง	แนวทางการควบคุม	ระยะเวลาเริ่มต้น/สิ้นสุด	ปีงบ ๒๕๖๑				ปีงบ ๒๕๖๒				ปีงบ ๒๕๖๓				งบประมาณ	ผู้รับผิดชอบ
			Q๑	Q๒	Q๓	Q๔	Q๑	Q๒	Q๓	Q๔	Q๑	Q๒	Q๓	Q๔		
๙. ความเสี่ยงด้านการการเปิดเผยข้อมูลผู้ป่วย	- จัดทำแผนโครงการกระตุ้นผู้ใช้งานให้ตระหนักในความเสี่ยงของการเปิดเผยข้อมูลหรือแชร์ข้อมูลในสื่อสังคมออนไลน์ ทุกชนิด	- ตลอดปี	←											→	NA	กลุ่มงานสารสนเทศทางการแพทย์
	- ปรับปรุงระเบียบปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของรพ.แพร่	- เดือน ส.ค. ๖๑				●									NA	คณะกรรมการ MIS
	- ประกาศใช้นโยบายเรื่องระเบียบปฏิบัติในการปฏิบัติการส่งข้อมูลผู้ป่วยทางโปรแกรม LINE	- เดือน พ.ย. ๖๑					●								NA	คณะกรรมการ MIS
	- เพิ่มกระบวนการให้ผู้ป่วยยินยอมให้เปิดเผยข้อมูลเพื่อการวินิจฉัยและรักษาในช่องทางต่าง ๆ (*ผู้ป่วยในใช้แบบฟอร์ม Informed Consent, *ผู้ป่วยนอกใช้ตรายาง)	- เดือน พ.ย. ๖๑					●								NA	อนุกรรมการทีมเวชระเบียน

**** โครงการ/กิจกรรม/กระบวนการ แผนปฏิบัติการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (สุดท้าย)*

บทที่ ๔ สรุปผลและข้อเสนอแนะ

๔.๑ การประเมินปัจจัยเสี่ยง

นโยบายของกลุ่มสารสนเทศทางการแพทย์ ระดับคามเสี่ยงที่ยอมรับได้ <=๕

สำนักงาน ก.พ.ร. กำหนดให้ ความเสี่ยงที่จำเป็นต้องนำมาดำเนินการจัดการความเสี่ยง คือความเสี่ยงที่มีระดับความเสี่ยงสูง ตั้งแต่ ๑๐ ส่วนความเสี่ยงในแผนบริหารความเสี่ยงต่ำกว่า ๑๐ ถือว่ามีความเสี่ยงค่อนข้างต่ำอาจจะนำมาดำเนินการจัดการความเสี่ยงในแผนบริหารความเสี่ยงหรือไม่ก็ได้ การดำเนินการจัดการความเสี่ยง กิจกรรมที่ดำเนินการต่อไป

๑. สร้างความตระหนักในเรื่องนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ โดยจัดทำแผนโครงการกระตุ้นผู้ใช้งานให้ตระหนักในความเสี่ยงของการเปิดเผยข้อมูล หรือแชร์ข้อมูลในสื่อสังคมออนไลน์ ทุกชนิด

๒. กระตุ้นให้เกิดการปฏิบัติตามแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศอย่างเคร่งครัด

๓. จัดทำ KM เผื่อแพร่ข้อมูล ข่าวสารเกี่ยวต่างๆ ที่มีอยู่

๔.๒ ปัจจัยที่ทำให้ระบบบริหารความเสี่ยงประสบผลสำเร็จ

๑. แรงผลักดันจากผู้บริหารหน่วยงานที่ให้ความสนับสนุน

๒. เทคโนโลยีสารสนเทศที่ช่วยในการจัดเก็บข้อมูล การส่งถ่ายข้อมูลและการตรวจสอบย้อนกลับได้อย่างรวดเร็ว

๓. ความร่วมมือร่วมใจของบุคลากรภายในเทคโนโลยีสารสนเทศทางการแพทย์ที่จะผลักดันให้การบริหารความเสี่ยงประสบผลสำเร็จ

รายการความเสี่ยง		๒๕๕๙	๒๕๖๐	๒๕๖๑	โอกาส/ความถี่	ความรุนแรงและผลกระทบ
ด้านความมั่นคงปลอดภัยของทรัพยากรในระบบเทคโนโลยีสารสนเทศ						
๑	การถูกบุกรุกโดยผู้ไม่ประสงค์ดี	**๒X๔**	**๒X๔**	**๓X๔**	ปี ๒๕๕๙-๖๐(ไม่เคยพบ), ปี ๒๕๖๑ (๑ครั้ง) เว็บไซต์บุกรุก	-เว็บไซต์ใช้งานได้ปกติ ดำเนินการแก้ไขปัญหาได้ ๑๕ ชั่วโมง ไม่พบความเสียหาย/มีแผนจัดการ**
๒	การโจรกรรม	**๑X๕**	**๑X๕**	**๑X๕**	ไม่เคยเกิดขึ้น	ไม่เคยเกิดขึ้น
ด้านระบบเทคโนโลยีสารสนเทศอาจทำให้เกิดความบกพร่องในการดูแลผู้ป่วย						
๓	โปรแกรมทำงานผิดพลาด/ตั้งค่าผิดพลาด/ฐานข้อมูลเสียหาย/ข้อมูลถูกแก้ไขหลังจากมีผู้ได้รับข้อมูลไปแล้ว	**๕X๔**	**๔X๔**	**๔X๔**	การแพ้ยาซ้ำ ข้อมูลค่าใช้จ่ายสูญหาย การเปลี่ยน HN ข้อมูล LAB ผิด Visit ผู้ป่วยใส่ TUBE ยาก	ควบคุม ติดตาม ดูแลโดยคณะกรรมการความเสี่ยงโรงพยาบาลแพร่รายงานอุบัติการณ์ใน HRMS on Cloud
ด้านความเป็นส่วนตัวของผู้ป่วย						
๔	การเข้าถึงข้อมูลของบุคคลอื่น	**๕X๔**	**๕X๔**	**๓X๔**	ปี ๒๕๕๙-๒๕๖๐ เกิดขึ้นบ่อย/ ปี ๒๕๖๑ ผู้ใช้งานเริ่มมีความตระหนัก	-มีแนวทางปฏิบัติและและควบคุมโดยใช้ระเบียบปฏิบัติฯระเบียบปฏิบัติฯข้อนี้ - ตรวจสอบ สำรวจให้ลงทะเบียน Login ครบทุกคน -เฝ้าระบบโดยผู้ดูแลระบบ Monitor ปี ๒๕๖๑
๕	การเปิดเผยข้อมูลผู้ป่วย	**๔X๕**	**๔X๔**	**๓X๓**	ปี ๒๕๕๙-๒๕๖๐ เกิดขึ้นบ่อยผู้ใช้งานบางคนไม่ทราบระเบียบปฏิบัติ/ปี ๒๕๖๑ มีการละเมิดลดลง	มีแนวทางปฏิบัติและและควบคุมโดยใช้ระเบียบปฏิบัติฯ

รายการความเสี่ยง		๒๕๕๙	๒๕๖๐	๒๕๖๑	โอกาส/ความถี่	ความรุนแรงและผลกระทบ
ด้านบริหารจัดการ						
๖	การขาดแคลนบุคลากรปฏิบัติงาน	**๕X๓**	**๔X๓**	**๒X๓**	๒๕๕๙-๒๕๖๐ FTE(ขาด๒), ๒๕๖๑ พอเพียง**รับใหม่๒คน	จัดเจ้าหน้าที่อยู่เวร ๒๔ ชั่วโมง
๗	การสนับสนุนงบประมาณไม่เพียงพอ	**๓X๕**	**๓X๔**	**๓X๓**	มีโครงการที่ได้ล่าช้า	ทำการสำรวจ และแผนให้ทันตามระยะเวลากำหนด
๘	การนำอุปกรณ์อื่นที่ไม่ได้อนุญาตมาเชื่อมต่อ	**๔X๔**	**๔X๔**	**๓X๔**	เกิดขึ้นน้อยมาก	ป้องกันโดยปิดกั้นช่องทางการเชื่อมต่ออุปกรณ์ดังกล่าว และควบคุมโดยใช้ระเบียบปฏิบัติฯ
๙	เครื่องคอมพิวเตอร์หรืออุปกรณ์ขัดข้อง	**๕X๓**	**๔X๓**	**๒X๓**	๒๕๕๙ จำนวน ๑๑๕ ครั้ง, ๒๕๖๐ จำนวน ๙๖ครั้ง, ๒๕๖๑ จำนวน ๕๒ครั้ง	- สามารถแก้ไขปัญหาได้และใช้งานต่อเนื่องได้/จัดซื้อครุภัณฑ์ฯ ประจำปีและมีแผนจัดซื้อทดแทนทุกปี
ด้านภัยหรือสถานการณ์ฉุกเฉิน						
๑๐	Server/ระบบฐานข้อมูลล่ม/เสียหาย	**๔X๕**	**๔X๕**	**๓X๕**	๒๕๕๙ ระบบ Binary (๓ครั้ง), ๒๕๖๐ ระบบ Binary (๒ครั้ง), ๒๕๖๑ ระบบ Binary (๑ครั้ง),	-สามารถแก้ไขและใช้งานต่อเนื่องได้ภายใน ๒ ชั่วโมง -สามารถแก้ไขและใช้งานต่อเนื่องได้ภายใน ๑ ชั่วโมง -สามารถแก้ไขและใช้งานต่อเนื่องได้ภายใน ๔๕ นาที - แผนรองรับสถานการณ์ฉุกเฉิน (BCP,DRP)

รายการความเสี่ยง		๒๕๕๙	๒๕๖๐	๒๕๖๑	โอกาส/ความถี่	ความรุนแรงและผลกระทบ
๑๑	ไฟฟ้าขัดข้อง ไฟฟ้าดับ	**๓x๒**	**๓x๒**	**๓x๒**	เกิดความขัดข้องน้อย ส่วนใหญ่มีไฟสำรอง	สามารถแก้ไขได้และใช้งานต่อเนื่องมีระบบสำรองไฟฟ้า
๑๒	ไฟไหม้ น้ำท่วม แผ่นดินไหว อาคารถล่ม	**๑x๕**	**๑x๕**	**๑x๕**	ไม่เคยเกิด	- ไม่เคยเกิด - มีแผน DRP รองรับเหตุการณ์ดังกล่าว
๑๓	ความเสี่ยงจากสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง	**๑x๒**	**๑x๒**	**๑x๒**	การเกิดสถานการณ์ความรุนแรงหรือความไม่สงบเรียบร้อย จนทำให้ บุคลากรไม่สามารถปฏิบัติงานได้ตามปกติ	
๑๔	ความเสี่ยงจากการเปลี่ยนแปลงนโยบายผู้บริหาร	**๑x๑**	**๑x๑**	**๑x๑**	นโยบายกระทรวง	

๔.๓ ผลการประเมิน / ข้อสรุป

ผู้บริหารได้สร้างบรรยากาศสภาพแวดล้อมการควบคุมภายในเพื่อให้บุคลากรทุกคนมีทัศนคติที่ดีต่อการควบคุมภายในโดยใช้หลักธรรมาภิบาลส่งเสริม สนับสนุน และสื่อสารให้ทุกคนเข้าใจขอบเขตหน้าที่ รวมทั้งสามารถ ทักษาในการปฏิบัติงาน กฎ ระเบียบ ข้อบังคับที่เกียงข้อง รวมตลอดถึงจรรยาบรรณการทำงานของการดูแลผู้ป่วยเพื่อให้การควบคุมภายในหน่วยงานมีประสิทธิผลสามารถปฏิบัติงานตามภารกิจและตามที่ได้มอบหมายได้อย่างมีประสิทธิภาพ

จากการประเมินองค์ประกอบของการควบคุมภายในด้านการประเมินความเสี่ยงพบว่าในภาพรวมมีความเหมาะสมแล้ว แต่ต้องมีการปรับปรุงให้เหมาะสมยิ่งขึ้น ความเสี่ยงอยู่ในระดับที่ยอมรับได้และส่งเสริมให้บุคลากรมีความรู้ความชำนาญในการวิเคราะห์ความเสี่ยง

ระดับความเสี่ยง	**คะแนน**	**ปี ๒๕๕๙ -๒๕๖๐ (เรื่อง)**	**๒๕๖๑ (เรื่อง)**	**+/- (เรื่อง)**
ความเสี่ยงสูงมาก	**๑๘-๒๕**	**๔**	-	**-๔**
ความเสี่ยงสูง	**๑๐– ๑๗**	**๔** (ดำเนินการแก้ไขกลยุทธ์ลดความเสี่ยง)	**๔** (เรื่องใหม่ ลดลงสูงมากจาก ๓ เพิ่มมาจาก ปานกลาง ๑)	-
ความเสี่ยงปานกลาง	**๖ – ๙**	**๒** (ดำเนินการแก้ไขกลยุทธ์ลดความเสี่ยง)	**๖** (เรื่องเดิม ๑ ลดลงมาจากสูงมาก ๑ ลดลงมาจากสูงมาก ๔)	**+๔**
ความเสี่ยงต่ำ	**๑ – ๕**	**๔**	**๔** (เรื่องเดิม ๔)	-

ใบสรุปทางเลือกที่เหมาะสมในการจัดการความเสี่ยง

ลำดับ	ความเสี่ยง	ระดับความเสี่ยง	วิธีการจัดการที่เหมาะสม	กลยุทธ์
๑	**ด้านความปลอดภัยระบบสารสนเทศ**			
๑.๑	RIT๐๔ ความเสี่ยงจากการถูกบุกรุก โดยผู้ไม่ประสงค์ดี	๑๒	ควบคุม	LR
๑.๒	RIT๑๑ ความเสี่ยงจากการโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์	๕	ยอมรับ	RC
๒	**ด้านระบบเทคโนโลยีสารสนเทศอาจทำให้เกิดความบกพร่องในการดูแลผู้ป่วย**			
๒.๑	RIT๑๒ ความเสี่ยงในการดูแลผู้ป่วย	**๑๖**	ควบคุม	LR
๓	**ด้านความเป็นส่วนตัวของผู้ป่วย**			
๓.๑	RIT๐๑ ความเสี่ยงในการเข้าถึงข้อมูลของบุคคลอื่น	๑๒	ควบคุม	LR
	RIT๑๓ ความเสี่ยงการเปิดเผยข้อมูลผู้ป่วย	๙	ควบคุม	LR
๔	**ด้านบริหารจัดการ**			
๔.๑	RIT๐๒ ความเสี่ยงจากการนำเอาอุปกรณ์อื่นที่ไม่ได้รับอนุญาตมาเชื่อมต่อ	๑๒	ควบคุม	LR
๔.๒	RIT๐๗ ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ	๙	ควบคุม	LR
๔.๓	RIT๑๐ ความเสี่ยงจากเครื่องคอมพิวเตอร์หรืออุปกรณ์ขัดข้อง ไม่สามารถทำงานได้ตามปกติ	๖	หลีกเลี่ยง	RA
๔.๔	RIT๐๕ ความเสี่ยงจากการขาดแคลนบุคลากรผู้ปฏิบัติงาน	๖	ยอมรับ	LR
๔.๕	RIT๐๖ ความเสี่ยงจากการเปลี่ยนแปลงนโยบายผู้บริหาร	๑	ยอมรับ	RC
๕	**ด้านภัยหรือสถานการณ์ฉุกเฉิน**			
๕.๑	RIT๑๔ ความเสี่ยงระบบฐานข้อมูลล่ม/เสียหาย	๑๕	หลีกเลี่ยง	RA
๕.๒	RIT๐๓ ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	๖	ถ่ายโอน	RF
๕.๓	RIT๐๘ ความเสี่ยงจากการเกิดไฟไหม้ แผ่นดินไหว อาคารถล่ม	๕	ควบคุม	LR
๕.๔	RIT๐๙ ความเสี่ยงจากสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง	๒	ยอมรับ	RC

เกณฑ์ระดับความเสี่ยงที่ยอมรับได้ มีดังนี้

- ระดับความเสี่ยงด้านความปลอดภัยระบบสารสนเทศ (๑ เรื่อง) มีค่าตั้งแต่ ๑ – ๕
- ระดับความเสี่ยงด้านบริหารจัดการ (๑ เรื่อง) มีค่าตั้งแต่ ๑ – ๕
- ระดับความเสี่ยงด้านภัยหรือสถานการณ์ฉุกเฉิน (๒ เรื่อง) มีค่าตั้งแต่ ๑ - ๘