การบริหารจัดการความเสี่ยง ด้านเทคโนโลยีสารสนเทศ

RISK MANAGEMENT

โรงพยาบาลเมืองจันทร์

คำนำ

ตามพระราชบัญญัติตรวจเงินแผ่นดินว่าด้วยการกำหนดมาตรฐานการควบคุมภายใน พ.ศ.2544 ที่กำหนดให้ส่วนราชการต้องมีการประเมินความเสี่ยงและปรับปรุงระบบควบคุมภายใน กลุ่มงานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์ของโรงพยาบาลเมืองจันทร์ จึงได้ดำเนินการนโยบายด้านการบริหารความเสี่ยงและการควบคุมภายในขององค์กรอย่างต่อเนื่อง ตามแนวทางการจัดวางระบบการควบคุมภายในและการประเมินการควบคุมภายใน ของสำนักงานตรวจเงินแผ่นดิน การบริหารกิจการบ้านเมืองที่ดีของรัฐบาล และการนำระบบการบริหารความเสี่ยงมา ใช้ในระบบการบริหาร โดยในปีงบประมาณ พ.ศ.2564 กลุ่มงานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์มีการดำเนินการตามกระบวนการบริหารความเสี่ยง กับประเด็นยุทธศาสตร์ และต้องดำเนินการบริหารความเสี่ยงโดยให้ครอบคลุม พันธกิจ

โรงพยาบาลเมืองจันทร์ได้จัดทำแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ประจำปี พ.ศ. 2564 - พ.ศ. 2568 ด้วยการวิเคราะห์และประเมิน ความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อที่จะบริหารจัดการความเสี่ยงตามกระบวนการบริหารความเสี่ยงตามระบบสารสนเทศการบริหารจัดการความเสี่ยงของสถานพยาบาล (Healthcare Risk Management System: HRMS) ซึ่งสอดคล้องกับมาตรฐานความมั่นคงปลอดภัยสารสนเทศ (IS027001) แผนบริหารจัดการความเสี่ยงดังกล่าว จะใช้เป็นกรอบ และแนวทำงานในการปฏิบัติงาน ของหน่วยงานต่างๆ ที่เกี่ยวข้อง ตลอดจนการกำกับดูแลการใช้งานด้านเทคโนโลยีสารสนเทศของโรงพยาบาลเมืองจันทร์ ใน พ.ศ. 2564 - พ.ศ. 2568 เพื่อให้เทคโนโลยีสารสนเทศของโรงพยาบาลเมืองจันทร์สามารถใช้งานได้อย่างต่อเนื่อง มีประสิทธิภาพและมีความมั่นคงปลอดภัยสูงสุด ทั้งนี้ จะมีการตรวจสอบและประเมินความเสี่ยงที่มีแนวโน้มอาจจะเกิดขึ้น เพื่อบริหารจัดการได้อย่างถูกต้อง ไม่เกิดเหตุการณ์ ความเสียหาย พร้อมทั้งสิ้นปีให้มีการทำการตรวจสอบหาช่องโหว่ของระบบในทุกปี และทำการทบทวนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศก่อนสิ้นสุดแผนฯ ของปีงบประมาณ

(นายแพทย์จิระวัตร วิเศษสังข์)
ผู้อำนวยการโรงพยาบาลเมืองจันทร์

สารบัญ

หน้า

บทที่ 1 บทนำ

1. หลักการและเหตุผล

ศูนย์เทคโนโลยีสารสนเทศได้นำเทคโนโลยีสารสนเทศเข้ามาใช้ในการปฏิบัติงานของโรงพยาบาลเมืองจันทร์ในหลายด้าน ดังนั้น จึงจำเป็นต้องมีการบริหารจัดการความเสี่ยงด้านสารสนเทศ เพื่อหาวิธีการป้องกันปัญหาที่อาจเกิดขึ้น อันจะส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศของโรงพยาบาล เพื่อให้การนำเทคโนโลยีสารสนเทศ มาสนับสนุนการปฏิบัติงานนั้นเกิดประโยชน์สูงสุด และเพื่อลดโอกาสความเสียหายที่อาจเกิดขึ้น แผนบริหารจัดการความเสี่ยงนั้นมีวัตถุประสงค์เพื่อเป็นแนวทางที่ใช้ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศของโรงพยาบาล ด้วยการคาดการณ์ล่วงหน้าในกรณีที่ความเสี่ยงนั้นเกิดขึ้นจริงและนำแนวทางจัดการความเสี่ยงนี้ไปใช้ในการดำเนินการ

การบริหารความเสี่ยงเป็นเครื่องมือทางกลยุทธ์ที่สำคัญตามหลักการกำกับดูแลกิจการที่ดี ที่จะช่วยให้การบริหารงานและการตัดสินใจด้านต่างๆ เช่น การวางแผน การกำหนดกลยุทธ์ การติดตามควบคุม และวัดผลการ ปฏิบัติงาน ตลอดจนการใช้ทรัพยากรต่างๆ อย่างเหมาะสม มีประสิทธิภาพมากขึ้น และลดการสูญเสียและโอกาสที่ ทำให้เกิดความเสียหายแก่องค์กร

ภายใต้สภาวะการดำเนินงานของทุกๆ องค์กรล้วนแต่มีความเสี่ยง ซึ่งเป็นความไม่แน่นอนที่อาจจะส่งผลกระทบต่อการดำเนินงานหรือเป้าหมายขององค์กร จึงจำเป็นต้องมีการจัดการความเสี่ยงเหล่านั้นอย่างเป็นระบบ โดยการระบุความเสี่ยงว่ามีปัจจัยเสี่ยงใดบ้างที่กระทบต่อการดำเนินงานหรือเป้าหมายขององค์กร วิเคราะห์ความเสี่ยงจากโอกาสและผลกระทบที่เกิดขึ้น จัดลำดับความสำคัญของความเสี่ยง กำหนดแนวทางในการจัดการความเสี่ยง และต้องคำนึงถึงความคุ้มค่าในการจัดการความเสี่ยงอย่างเหมาะสม

แผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศมีวัตถุประสงค์เพื่อเป็นแนวทำงานที่ใช้ตรวจสอบ และประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ ด้วยการคาดการณ์ล่วงหน้าในกรณีที่ความเสี่ยงเกิดขึ้นจริง และโรงพยาบาลสามารถนำแนวทำงานจัดการความเสี่ยงนี้ไปใช้ในการดำเนินการได้

2. ระบบการบริหารความเสี่ยงโรงพยาบาลเมืองจันทร์

การบริหารจัดการความเสี่ยง เป็นกิจกรรมพื้นฐานบุคลากรทุกคนของโรงพยาบาลต้องให้ความสำคัญและร่วมกันวางแผนป้องกันและดำเนินการตามแนวทางที่วางไว้ โดยใช้กระบวนการบริหารจัดการความเสี่ยงที่ประกอบด้วย การค้นหาความเสี่ยง การประเมินความเสี่ยง การจัดการความเสี่ยง การประเมินผล

นโยบายเรื่องความปลอดภัยของผู้ป่วยและบุคลากรสาธารณสุข Patient and Personnel Safety (2P Safety) เป็นโยบายสำคัญที่จะสรางระบบบริการสุขภาพที่ยั่งยืน มีความสมดุล มีการพัฒนาเชิงระบบดวยการมีสวนรวมและสรางสรรคจากทุกหน่วยงาน หวังเป็นอย่างยิ่งว่า คู่มือการบริหารจัดการความเสี่ยงเล่มนี้จะเป็นประโยชน์ต่อความปลอดภัยของผูปวยและบุคลากรสาธารณสุขจะเป็นประโยชน์นำมาซึ่งการเปลี่ยนแปลงของระบบคุณภาพด้านการบริหารจัดการความเสี่ยงของโรงพยาบาลเมืองจันทร์ ภายใตความรวมมือจากทุกหน่วยงาน บนพื้นฐานของความเขาใจกันและกัน โดยคำนึงถึงประโยชนสวนรวมขององค์กร

3. นโยบาย

3.1 พัฒนาองค์ความรู้ของบุคลากรเพื่อตอบสนองและเพิ่มประสิทธิภาพการบริหารความเสี่ยงให้เหมาะสมและสอดคล้องกับบริบทของผู้ปฏิบัติงาน

3.2 ค้นหา เฝ้าระวังและติดตามความเสี่ยงทุกประเภท เน้นเชิงรุกมากกว่าเชิงรับโดยให้ทุกหน่วยงาน/ทุกทีมรายงานอุบัติการณ์ ที่เกิดขึ้นในหน่วยงานหรือพบเห็นในโรงพยาบาลพร้อมทั้งดำเนินการตาม

ระบบการรายงานและบริหารจัดการความเสี่ยงที่ทีมบริหารความเสี่ยงกำหนดและบันทึกในโปรแกรม HRMS on Cloud

3.3 มีระบบการรายงานความเสี่ยงที่ชัดเจน

3.4 มีการจัดทำบัญชีความเสี่ยงในทุกหน่วยงาน รวมทั้งวิเคราะห์และจัดทำมาตรการป้องกันความเสี่ยงที่สำคัญโดยให้ทุกหน่วยงาน / ทุกทีมมีการทบทวนและใช้ข้อมูลที่ได้จากการบันทึกมาวางมาตรการในการป้องกันและแก้ไขความเสี่ยงอย่างเป็นระบบและให้มีการเฝ้าระวังและทบทวนความเสี่ยงอย่างสม่ำเสมอรายงานการบริหารจัดการความเสี่ยงให้หัวหน้ากลุ่ม / ทีมและกรรมการบริหารความเสี่ยงทราบตามระยะเวลาที่กำหนด

3.5 ร่วมกันสร้างวัฒนธรรมความปลอดภัยขององค์กร โดยให้ถือว่าผู้รายงานไม่มีความผิด

3.6 มีช่องทางรับรายงานความเสี่ยงและข้อร้องเรียนจากผู้รับ / ผู้ให้บริการ / ภาคีเครือข่ายภายนอก เมื่อมีข้อร้องเรียน โรงพยาบาลถือว่าเป็นเหตุการณ์ที่สำคัญและมีผลต่อชื่อเสียงของโรงพยาบาลต้องมีการรายงาน บันทึกรายงาน และตอบสนองข้อร้องเรียนอย่างเหมาะสมโดยเร็ว

3.7 มีระบบสารสนเทศที่มีประสิทธิภาพ สะท้อนสถานการณ์ความเสี่ยง ระบบเฝ้าระวัง และจัดลำดับความสำคัญ

4. ประเด็นคุณภาพที่สำคัญ

เพื่อให้ประชาชนผู้รับบริการ บุคลากรผู้ให้บริการ สิ่งแวดล้อมในโรงพยาบาลและชุมชนปลอดภัย

5. วัตถุประสงค์ของแผนบริหารความเสี่ยง

5.1 เพื่อให้ผู้บริหารและผู้ปฏิบัติงาน เข้าใจหลักการ และกระบวนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

5.2 เพื่อให้การจัดการภายในกลุ่มงานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์ข้อมูลมีประสิทธิภาพและมีความยืดหยุ่น ในการปรับตัวให้ทันต่อการเปลี่ยนแปลงของเทคโนโลยีสารสนเทศสมัยใหม่ รวมทั้งลดโอกาสที่จะก่อให้เกิดความเสียหายที่ไม่ต้องการกับระบบเทคโนโลยีสารสนเทศ

5.3 เพื่อให้ผู้ปฏิบัติงานได้รับทราบขั้นตอน และกระบวนการในการวางแผนบริหารความเสี่ยง

5.4 เพื่อให้มีการปฏิบัติตามกระบวนการบริหารความเสี่ยงอย่างเป็นระบบและต่อเนื่อง

5.5 เพื่อลดโอกาสและผลกระทบของความเสี่ยงที่จะเกิดขึ้นกับองค์กร

5.6 เพื่อเป็นแนวทำงานการดำเนินการ กำกับดูแล ตรวจสอบเกี่ยวกับการบริหารจัดการและการเผยแพร่ความรู้ความเข้าใจเกี่ยวกับการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศในโรงพยาบาล

5.7 เพื่อช่วยเพิ่มประสิทธิภาพการตัดสินใจ โดยคำนึงถึงปัจจัยเสี่ยงและความเสี่ยงในด้านต่างๆ ที่นำจะมีผลกระทบกับการดำเนินงาน วัตถุประสงค์และนโยบาย แล้วพิจารณาหาแนวทำงานในการป้องกัน หรือจัดการกับความเสี่ยงเหล่านั้น ก่อนที่จะเริ่มปฏิบัติงานหรือดำเนินงานตามแผน

6. เป้าหมาย

6.1 เกิดความปลอดภัยแก่ผู้รับบริการ ผู้ให้บริการ และสิ่งแวดล้อม

6.2 มีระบบบริหารจัดการความเสี่ยงที่มีประสิทธิภาพ

7. ประโยชน์ของการบริหารความเสี่ยง

การดำเนินการบริหารความเสี่ยงจะช่วยให้ผู้บริหารมีข้อมูลที่ใช้ในการตัดสินใจได้ดียิ่งขึ้นและทำให้องค์กรสามารถจัดการกับปัญหาอุปสรรคและอยู่รอดได้ในสถานการณ์ที่ไม่คาดคิดหรือสถานการณ์ที่อาจทำให้องค์กรเกิดความเสียหาย ประโยชน์ที่คาดหวังว่าจะได้รับจากการดำเนินการบริหารความเสี่ยง มีดังนี้

7.1 เป็นส่วนหนึ่งของหลักการบริหารกิจการบ้านเมืองที่ดี การบริหารความเสี่ยงจะช่วยคณะทำงานบริหารความเสี่ยงและผู้บริหารทุกระดับตระหนักถึงความเสี่ยงหลักที่สำคัญ และสามารถทำหน้าที่ในการกำกับดูแลองค์กรได้อย่างมีประสิทธิภาพและประสิทธิผลมากยิ่งขึ้น

7.2 สร้างฐานข้อมูลที่มีประโยชน์ต่อการบริหารและการปฏิบัติงานในองค์กร การบริหารความเสี่ยงจะเป็นแหล่งข้อมูลสำหรับผู้บริหารในการตัดสินใจด้านต่างๆ ซึ่งรวมถึงการบริหารความเสี่ยงซึ่งตั้งอยู่บนสมมุติฐานในการตอบสนองต่อเป้าหมาย และภารกิจหลักขององค์กรรวมถึงระดับความเสี่ยงที่ยอมรับได้

7.3 ช่วยสะท้อนให้เห็นภาพรวมของความเสี่ยงต่างๆ ที่สำคัญได้ทั้งหมด การบริหารความเสี่ยงจะทำให้บุคลากรภายในองค์กรมีความเข้าใจถึงเป้าหมายและภารกิจหลักขององค์กร และตระหนักถึงความเสี่ยงสำคัญที่ส่งผลกระทบในเชิงลบต่อองค์กรได้อย่างครบถ้วน ซึ่งครอบคลุมความเสี่ยงธรรมาภิบาล

7.4 เป็นเครื่องมือที่สำคัญในการบริหารงาน การบริหารความเสี่ยงเป็นเครื่องมือที่ช่วยให้ผู้บริหารสามารถมั่นใจได้ว่าความเสี่ยงได้รับการจัดการอย่างเหมาะสมและทันเวลา รวมทั้งเป็นเครื่องมือที่สำคัญของผู้บริหารในการบริหารงานและการตัดสินใจในด้านต่างๆ เช่น การวางแผนการกำหนดกลยุทธ์ การติดตามควบคุม และจัดผลการปฏิบัติงาน ซึ่งส่งผลให้การดำเนินงานของโรงพยาบาลเมืองจันทร์เป็นไปตามเป้าหมายที่กำหนด และสามารถปกป้องผลประโยชน์ รวมทั้งเพิ่มมูลค่าแก่องค์กร

7.5 ช่วยให้การพัฒนาองค์กรเป็นไปในทิศทางเดียวกัน การบริหารความเสี่ยงทำให้รูปแบบการตัดสินใจในระดับการปฏิบัติงานขององค์กรมีการพัฒนาไปในทิศทางเดียวกัน เช่น การตัดสินใจโดยที่ผู้บริหารมีความเข้าใจ ในกลยุทธ์ วัตถุประสงค์ขององค์กร และระดับความเสี่ยงอย่างชัดเจน

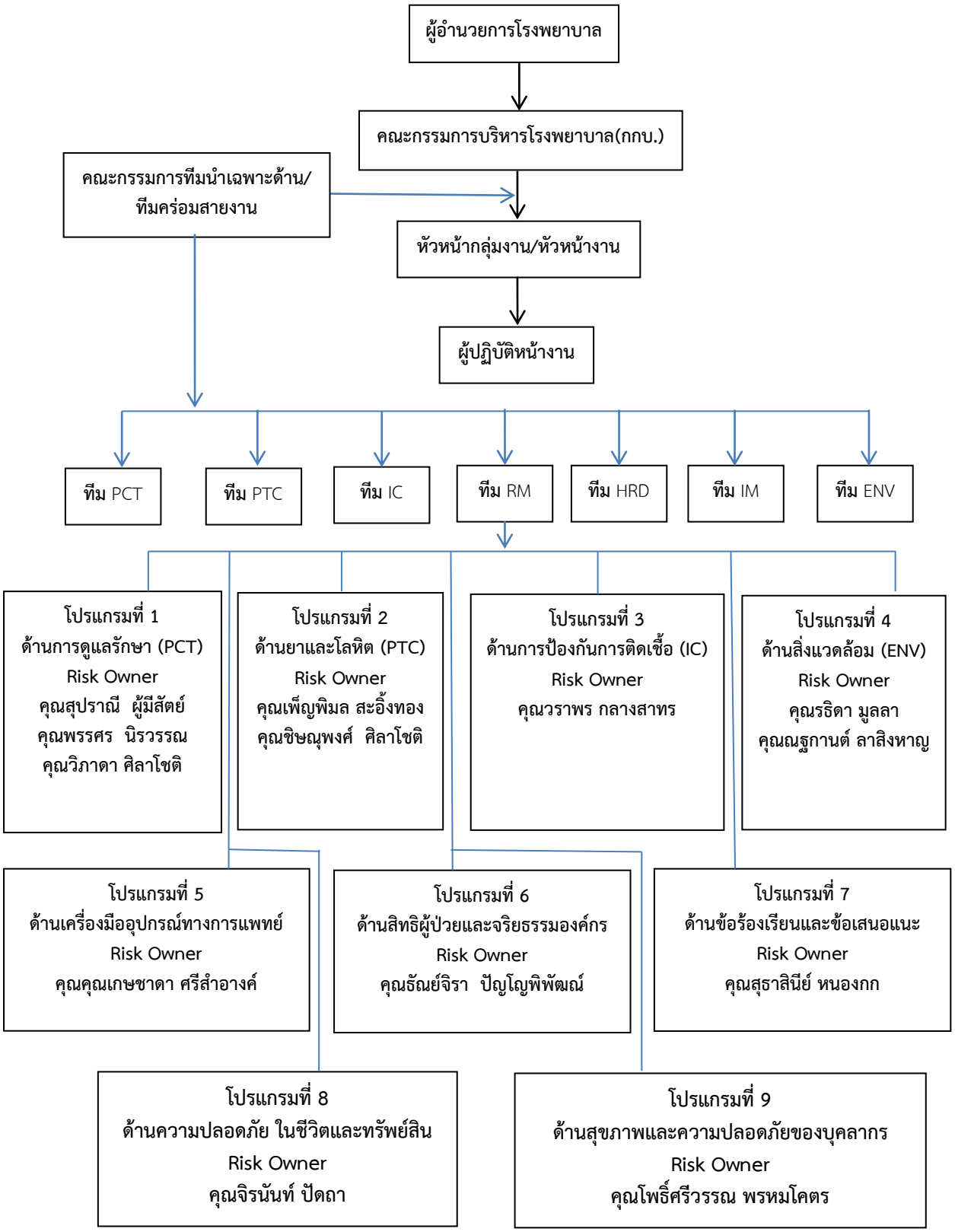
7.6 ช่วยให้การพัฒนาการบริหารและจัดสรรทรัพยากรเป็นไปอย่างมีประสิทธิภาพและประสิทธิผลการจัดสรรทรัพยากรเป็นไปอย่างเหมาะสม โดยพิจารณาถึงระดับความเสี่ยงในแต่ละกิจกรรม และการเลือกใช้ มาตรการในการบริหารความเสี่ยง เช่น การใช้ทรัพยากรสำหรับกิจกรรมที่มีความเสี่ยงต่ำและกิจกรรมที่มีความ เสี่ยงสูงย่อมแตกต่างกัน หรือการเลือกใช้มาตรการแต่ละประเภทย่อมใช้ทรัพยากรแตกต่างกัน เป็นต้น

8. ตัวชี้วัดผลการดำเนินการ

ลำดับ	รายละเอียดตัวชี้วัด	ค่าเป้าหมาย
1	ร้อยละของหน่วยงานที่มีการค้นหาและส่งรายงานความเสี่ยง	100%
2	อัตราการรายงานความเสี่ยงทันเวลาครอบคลุมทุกหน่วยงานในแต่ละเดือน	100%
3	อัตราการเกิดความเสี่ยง ระดับ Near miss : miss	เพิ่มขึ้น
4	ร้อยละความเสี่ยง/ อุบัติการณ์ที่ได้รับการแก้ไขตามเกณฑ์	100%
5	ร้อยละการเกิดอุบัติการณ์ซ้ำ ประเภท Clinic ระดับ E-F-G-H-I	น้อยกว่า20%
6	ร้อยละการเกิดอุบัติการณ์ซ้ำ ประเภท Non Clinic ระดับ ๓-๔	น้อยกว่า20%
7	ร้อยละการเกิดอุบัติการณ์ ประเภท Clinic ระดับ E-F-G-H-I ที่ได้รับการทำ RCA	100%
8	ร้อยละการเกิดอุบัติการณ์ซ้ำ ประเภท Non Clinic ระดับ ๓-๔ ที่ได้รับการทำ RCA	100%
9	ร้อยละตัวชี้วัด SIMPLE ที่ผ่านเกณฑ์	90%
10	อุบัติการณ์ที่บุคลากรติดเชื้อโควิด-19 จากการปฏิบัติงานเท่ากับ	0

บทที่ 2 แนวทางการบริหารความเสี่ยง

1. โครงสร้างการบริหารความเสี่ยง



2. บทบาทหน้าที่

2.1 บทบาทหน้าที่ของผู้อำนวยการโรงพยาบาล

1) เป็นที่ปรึกษาการวางระบบบริหารความเสี่ยงของโรงพยาบาล
2) พิจารณาสั่งการและดำเนินการกรณีที่มีความเสี่ยงหรืออุบัติการณ์สำคัญเกิดขึ้นภายในโรงพยาบาล
3) รับทราบรายงาน การประเมินผล และการตอบสนองการบริหารความเสี่ยง

2.2 บทบาทหน้าที่ของคณะกรรมการบริหารโรงพยาบาล (กกบ.)

1) ส่งเสริมให้เกิดวัฒนธรรมความปลอดภัยในหน่วยงาน
2) สนับสนุนกระบวนการจัดการ และทรัพยากรเพื่อแก้ไขความเสี่ยง
3) บริหารจัดการความเสี่ยงระดับโรงพยาบาล ปัญหาความเสี่ยงที่ซับซ้อน ที่หน่วยงานหรือทีมคร่อมไม่สามารถแก้ไขได้
4) ติดตามประเมินผลการจัดการความเสี่ยง
5) กรรมการบริหารทุกท่านทำหน้าที่เป็น Risk Responder ดังนี้
   - คุณรธิดา มูลลา และคุณวิไลวรรณ กันภัย มีหน้าที่ตอบสนองความเสี่ยงด้าน ENV, โครงสร้าง,อาคาร สถานที่ ทั้งหมด
   - ทันตแพทย์หญิงมณีรัตน์ จันเทพา มีหน้าที่ตอบสนองความเสี่ยง ด้าน IC
   - คุณดวงตะวัน ภูมลี และคุณศิรดา ปะรัมย์ มีหน้าที่ตอบสนองความเสี่ยงด้าน การดูแลผู้ป่วย (PCT)
   - เภสัชกรวันชนก แก้วคะตา มีหน้าที่ตอบสนองความเสี่ยงด้านระบบยา (PTC)
   - ดร.บุษบา บุญกะนันท์ มีหน้าที่ตอบสนองความเสี่ยงด้านข้อร้องเรียน/ข้อเสนอแนะและสิทธิผู้ป่วยต่างๆ
   - คุณกรภัทร์ณิชา พิมพร มีหน้าที่ตอบสนองความเสี่ยงด้านการชันสูตร LAB , X-Ray และการตรวจวินิจฉัยโดยผู้ชำนาญกว่า

2.3 บทบาทหน้าที่ของคณะกรรมการบริหารความเสี่ยง

1) กำหนดนโยบายและแผนดำเนินงานในการบริหารจัดการความเสี่ยงระดับโรงพยาบาลเพื่อให้ทุกทีม ทุกหน่วยงานถือปฏิบัติให้เป็นแนวทางเดียวกัน
2) จัดทำคู่มือ แนวทางในการบริหารความเสี่ยง พร้อมทั้งถ่ายทอด สื่อสารให้บุคลากรทราบและสื่อสารนโยบายที่กำหนดให้ทุกหน่วยงานทราบ
3) ส่งเสริมให้เกิดกระบวนการบริหารความเสี่ยง ให้หน่วยงานเฝ้าระวังความเสี่ยงทางคลินิกและกระตุ้นการค้นหาความเสี่ยงเชิงรุก
4) รวบรวมความเสี่ยง อุบัติการณ์ และจัดทำบัญชีความเสี่ยงระดับโรงพยาบาล
5) ประสานติดตามปัญหาความเสี่ยงในระดับโรงพยาบาล ประสานระบบที่เกี่ยวข้องกับความเสี่ยงในด้านต่างๆ ของโรงพยาบาล เพื่อป้องกัน และควบคุมความเสี่ยง
6) รวบรวม วิเคราะห์ ทบทวนอุบัติการณ์ เพื่อหาแนวทางปรับปรุงและวางมาตรการป้องกันความเสี่ยงในโรงพยาบาลและวางระบบบริหารจัดการความเสี่ยงในภาพรวมของโรงพยาบาล
7) วิเคราะห์รายงานอุบัติการณ์ความเสี่ยงทางคลินิกและประเมินความรุนแรงและความสูญเสียทุกเดือน
8) สื่อสารโยบาย ระเบียบปฏิบัติที่ได้จากการทบทวน เพื่อให้ผู้เกี่ยวข้องนำไปปฏิบัติ

9) ติดตามประเมินผลการดำเนินงานด้านการบริหารจัดการความเสี่ยงของทีม และหน่วยงานต่างๆ
10) ร่วมตัดสินใจในประเด็นของความเสี่ยงหรือความสูญเสียรวมถึงเป็นผู้แก้ต่างในกรณีฟ้องร้องเรียกค่าเสียหายหรือค่าชดเชยจากโรงพยาบาล
11) ประสานงานประธานคณะกรรมการด้านบริหารความเสี่ยงด้านคลินิก (PCT)และไม่ใช่คลินิกเพื่อดำเนินการแก้ไขปรับปรุง พัฒนาตามข้อร้องเรียน
12) ให้คำปรึกษาและข้อเสนอแนะแก่หน่วยงาน ในการแก้ปัญหา วางระบบในการป้องกันการเกิดความเสี่ยงซ้ำโดยกระบวนการ Root cause analysis (RCA)
13) สรุปรายงานและประมวลผลความเสี่ยง แจ้งทุกหน่วยงานและทีมทุกทีม
14) จัดทำรายงานความเสี่ยง รายงานสถานการณ์ แนวโน้มความเสี่ยงทางคลินิกและผลการดำเนินการเสนอคณะกรรมการบริหารโรงพยาบาลทุก 1 เดือน

โดยได้แบ่งหน้าที่รับผิดชอบจัดการความเสี่ยงทั้ง 14 ข้อ โดยกรรมการทั้ง 13 ท่านมีหน้าที่ในการตอบสนองอุบัติการณ์ความเสี่ยงที่มีการรายงานเข้ามาในทุกช่องทาง RM ไม่ได้มีหน้าที่ในการแก้ไขปัญหา แต่ RM มีหน้าที่ประสานกับผู้ที่เกี่ยวข้องกับอุบัติการณ์นั้นๆ เพื่อให้เกิดการทบทวน พูดคุยกันเพื่อหาแนวทางป้องกันและฝ้าระวังไม่ให้เกิดอุบัติการณ์ซ้ำ พอถึงสิ้นเดือน ให้ RM แต่ละท่านรวบรวมรายงานอุบัติการณ์เพื่อมาวิเคราะห์และสรุปผลรายงานเพื่อนำเสนอในที่ประชุม HA ทุกวัน พุธ สัปดาห์ที่ 3 ของเดือน ให้ครอบคลุมทั้ง 9 โปรแกรม ดังนี้

<u>โปรแกรมที่ 1 ด้านการดูแลรักษา (PCT)</u> Risk Owner คือ

- คุณสุปราณี ผู้มีสัตย์
- คุณพรรศร นิรวรรณ
- คุณวิภาดา ศิลาโชติ

รับผิดชอบตอบสนองอุบัติการณ์ในเรื่องนี้พร้อมกับเป็น Risk Owner ในอุบัติการณ์ที่ต้องทำ Risk Treatment

<u>โปรแกรมที่ 2 ด้านยาและโลหิต (PTC)</u> Risk Owner คือ

- คุณเพ็ญพิมล สะอิ้งทอง
- คุณชิษณุพงศ์ ศิลาโชติ

รับผิดชอบตอบสนองอุบัติการณ์ในเรื่องนี้พร้อมกับเป็น Risk Owner ในอุบัติการณ์ที่ต้องทำ Risk Treatment

<u>โปรแกรมที่ 3 ด้าน IC</u> Risk Owner คือ

- คุณวราพร กลางสาทร

รับผิดชอบตอบสนองอุบัติการณ์ในเรื่องนี้ พร้อมกับเป็น Risk Owner ในอุบัติการณ์ที่ต้องทำ Risk Treatment

<u>โปรแกรมที่ 4 ด้านENV</u> Risk Owner คือ

- คุณรธิดา มูลลา
- คุณณฐกานต์ ลาสิงหาญ

รับผิดชอบตอบสนองอุบัติการณ์ในเรื่องนี้ พร้อมกับเป็น Risk Owner ในอุบัติการณ์ที่ต้องทำ Risk Treatment

โปรแกรมที่ 5 เครื่องมืออุปกรณ์ทางการแพทย์ Risk Owner คือ

• คุณเกษชาดา ศรีสำอาง

รับผิดชอบตอบสนองอุบัติการณ์ในเรื่องนี้ พร้อมกับเป็น Risk Owner ในอุบัติการณ์ที่ต้องทำ Risk Treatment

โปรแกรมที่ 6 ด้านสิทธิผู้ป่วยและจริยธรรมองค์กร Risk Owner คือ

• คุณธัณย์จิรา ปัญโญพิพัฒณ์

รับผิดชอบตอบสนองอุบัติการณ์ในเรื่องนี้ พร้อมกับเป็น Risk Owner ในอุบัติการณ์ที่ต้องทำ Risk Treatment

โปรแกรมที่ 7 ด้านข้อร้องเรียนและข้อเสนอแนะ Risk Owner คือ

• คุณสุธาสินีย์ หนองกก

รับผิดชอบตอบสนองอุบัติการณ์ในเรื่องนี้ พร้อมกับเป็น Risk Owner ในอุบัติการณ์ที่ต้องทำ Risk Treatment

โปรแกรมที่ 8 ด้านความปลอดภัย ในชีวิตและทรัพย์สิน Risk Owner คือ

• คุณจิรนันท์ ปัดถา

รับผิดชอบตอบสนองอุบัติการณ์ในเรื่องนี้ พร้อมกับเป็น Risk Owner ในอุบัติการณ์ที่ต้องทำ Risk Treatment

โปรแกรมที่ 9 ด้านสุขภาพและความปลอดภัยของ บุคลากร Risk Owner คือ

• คุณโพธิ์ศรีวรรณ พรหมโคตร

รับผิดชอบตอบสนองอุบัติการณ์ในเรื่องนี้ พร้อมกับเป็น Risk Owner ในอุบัติการณ์ที่ต้องทำ Risk Treatment

2.4 บทบาทหน้าที่ของหัวหน้างานและผู้รับผิดชอบความเสี่ยงในหน่วยงาน

1) วางระบบการบริหารความเสี่ยงในหน่วยงาน ค้นหา วิเคราะห์ และจัดทำบัญชีความเสี่ยงของหน่วยงาน จัดทำมาตรการการป้องกันและจัดการที่ชัดเจนในประเด็นความเสี่ยงที่สำคัญ
2) ประเมินผล ติดตาม วิเคราะห์แนวโน้มความเสี่ยง และปรับปรุงบัญชีความเสี่ยงของหน่วยงานอย่างน้อยปีละ 4 ครั้ง หรือไตรมาสละ 1 ครั้ง
3) สื่อสารให้เจ้าหน้าที่ในหน่วยงานมีความเข้าใจในประเด็นความเสี่ยงที่สำคัญ ส่งเสริมให้เกิดวัฒนธรรมความปลอดภัยอยู่ในกิจกรรมปกติประจำวัน
4) ประเมินประสิทธิภาพของระบบบริหารความเสี่ยง การดักจับความเสี่ยง การแก้ไขปัญหา การหาสาเหตุรากเหง้า สาเหตุเชิงระบบ แนวทางป้องกัน โดยป้องกันและลดความสูญเสียที่วางไว้

2.5 บทบาทหน้าที่ของผู้รับผิดชอบระบบที่เกี่ยวข้อง

มีหน้าที่ในการรายงานเหตุการณ์ / อุบัติการณ์ หรือความเสี่ยง และประเมินประสิทธิภาพของการบริหารความเสี่ยงในทีมผ่านระบบ HRMS on Cloud ดังนี้

1) ทีมดูแลผู้ป่วย (PCT) : มีหน้าที่ค้นหา รายงานความเสี่ยงและวางระบบควบคุมป้องกันความเสี่ยงเกี่ยวกับกระบวนการดูแลรักษา และสิทธิผู้ป่วยซึ่งเป็นความเสี่ยงทางคลินิก
2) ทีมพัฒนาระบบยา (PTC) : มีหน้าที่ค้นหา รายงานความเสี่ยงและวางระบบควบคุมป้องกันความเสี่ยงเกี่ยวกับความคลาดเคลื่อนทางยา และปัญหาเกี่ยวกับยา
3) ทีมป้องกันและควบคุมการติดเชื้อในโรงพยาบาล (IC) : มีหน้าที่รายงานความเสี่ยงและวางระบบควบคุมป้องกันความเสี่ยงเกี่ยวกับการติดเชื้อในโรงพยาบาลการจัดการด้านอาชีวอนามัยและความปลอดภัยที่เกี่ยวข้องกับการติดเชื้อของเจ้าหน้าที่

4) ทีมบริหารสิ่งแวดล้อมและความปลอดภัย (ENV) : มีหน้าที่ค้นหา รายงานความเสี่ยงและวางระบบควบคุมป้องกันความเสี่ยงเกี่ยวกับการรักษาความปลอดภัย การฝึกซ้อมป้องกันอัคคีภัย การเกิดอัคคีภัย การตรวจคุณภาพน้ำทิ้ง การจัดการขยะ การจัดการด้านอาชีวอนามัยและความปลอดภัยของเจ้าหน้าที่ การจัดหา เก็บรักษา แจกจ่าย ซ่อมบำรุงและจำหน่ายเครื่องมืออุปกรณ์ต่างๆ
5) ทีมเทคโนโลยีสารสนเทศ (IM) : มีหน้าที่คันหา รายงานความเสี่ยงและวางระบบควบคุมป้องกันความเสี่ยงเกี่ยวกับเวชระเบียน การตรวจสอบความสมบูรณ์ของเวชระเบียนทั้งในเชิงปริมาณและคุณภาพ การจัดการความรู้ การสื่อสาร การประชาสัมพันธ์ และระบบฐานข้อมูลต่างๆ
6) ทีมรับเรื่องร้องเรียนและเจรจาไกลเกลี่ย : มีหน้าที่ค้นหา รายงานความเสี่ยงและวางระบบควบคุมป้องกันความเสี่ยงเกี่ยวกับด้านเรื่องร้องเรียน ผลการจัดการปัญหาข้อร้องเรียน
7) ทีมบริหารและพัฒนาทรัพยากรมนุษย์ (HRD) : มีหน้าที่คันหา รายงานความเสี่ยงและวางระบบควบคุมป้องกันความเสี่ยงด้านพฤติกรรมบริการ และสมรรถนะบุคลากร

2.6 บทบาทของคณะกรรมการบริหารความเสี่ยงด้านไกล่เกลี่ย และพิจารณาข้อร้องเรียน มีหน้าที่

1) ดำเนินการไกล่เกลี่ยตามหลักสันติวิธี
2) เสนอผู้อำนวยการโรงพยาบาล พิจารณาการเยียวยาเบื้องต้น เช่น การจัดหาของเยี่ยม การลดค่ารักษาพยาบาล บริการห้องพิเศษ และการร่วมทำบุญงานศพ เป็นต้น
3) รายงานผลการไกล่เกลี่ยให้ผู้อำนวยการโรงพยาบาล ทราบเป็นระยะๆ และภายหลังสิ้นสุดกระบวนการไกล่เกลี่ย
4) สรุปรายงานการไกล่เกลี่ย ต่อผู้อำนวยการโรงพยาบาล และรายงานในที่ประชุมคณะกรรมการบริหารความเสี่ยงโรงพยาบาล

2.7 บทบาทหน้าที่ของบุคลากรทุกระดับ

1) ทำความเข้าใจแนวทาง ปฏิบัติตมคู่มือการบริหารความเสี่ยงของโรงพยาบาล
2) เป็นผู้จัดการความเสี่ยง และแก้ไขสถานการณ์เบื้องตัน
3) บันทึกอุบัติการณ์ การแก้ไข และรายงานผู้เกี่ยวข้องตามแนวทางที่กำหนด
4) ค้นหาความเสี่ยงเชิงรุก เพื่อหาแนวทางป้องกันไม่ให้เกิดอุบัติการณ์ซ้ำ

3. ขอบเขตการดำเนินการ

เป็นการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ภายในความรับผิดชอบของงานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์ โรงพยาบาลเมืองจันทร์

บทที่ 3 กระบวนการบริหารความเสี่ยง

1. คำนิยาม

1.1 ความเสี่ยง (Risk) หมายถึง โอกาสที่จะเกิดความสูญเสียหรือสิ่งไม่พึงประสงค์ เหตุการณ์ที่เกิดขึ้นที่ไม่เป็นไปตามความคาดหวัง มีโอกาสที่จะประสบกับความสูญเสียหรือสิ่งที่ไม่พึงประสงค์ ได้แก่ ความสูญเสียที่เกิดขึ้นกับผู้ป่วยและผู้รับบริการ การบาดเจ็บ การเสื่อมเสียชื่อเสียง การสูญเสียรายได้ การสูญเสียหรือเสียหายต่อทรัพย์สิน การบาดเจ็บหรืออันตรายต่อเจ้าหน้าที่ การทำลายสิ่งแวดล้อม ภาระในการชดใช้ค่าเสียหาย การไม่พิทักษ์สิทธิหรือศักดิ์ศรี เกิดความไม่แน่นอน หรือเกิดความสูญเสียจนต้องมีการชดใช้ค่าเสียหาย

1.2 การบริหารความเสี่ยง (Risk management) หมายถึง การจัดการในเรื่องการค้นหาความเสี่ยง การประเมินความเสี่ยง การจัดการความเสี่ยงและการประเมินผล รวมทั้งการดำเนินการเพื่อป้องกันความเสี่ยงและการจัดการเมื่อเกิดปัญหา

1.3 อุบัติการณ์ (Incident) หมายถึง เหตุการณ์ที่ไม่พึงประสงค์ที่เกิดขึ้นนอกเหนือความคาดหมายจากการทำงานตามปกติ เป็นเหตุการณ์ความเสี่ยงที่เกิดขึ้นแล้ว

1.4 บัญชีรายการความเสี่ยง (Risk Profile) หมายถึง รายการความเสี่ยงที่อาจเกิดขึ้นซึ่งผู้รับผิดชอบหรือหน่วยงานได้รวบรวมจัดทำขึ้นโดยอาศัยการเรียนรู้จากประสบการณ์ ข้อมูลในอดีตและหน่วยงานอื่นๆ ตลอดจนการทบทวนต่างๆ การวิเคราะห์ความเสี่ยงจากกระบวนการทำงานและการสำรวจภายในหน่วยงานของตนเอง เพื่อหาประเด็นสำคัญที่ควรมีการเฝ้าระวังทั้งในระดับหน่วยงาน ทีมคร่อมสายงานและระดับโรงพยาบาล

1.5 เหตุการณ์ไม่พึงประสงค์ (Adverse Event) หมายถึง การบาดเจ็บที่เกิดจากกระบวนการดูแลรักษาโดยไม่ตั้งใจ (มีเหตุการณ์เกิดขึ้นแล้ว) อันตรายที่ผู้ป่วยได้รับ ซึ่งเกิดจากการรักษาและไม่ได้เป็นผลสืบเนื่องมาจากโรคหรือความผิดปกติเดิมของผู้ป่วย อันตรายดังกล่าวส่งผลให้ระยะเวลาการรักษานานขึ้น นอนโรงพยาบาลนานขึ้นหรือเกิดความพิการตามมา ลักษณะของสิ่งที่ไม่พึงประสงค์ ได้แก่ การบาดเจ็บ เหตุร้าย ภัยอันตราย การคุกคามก่อให้เกิดความรู้สึกไม่มั่นคง ความไม่แน่นอน การถูกเปิดเผย เป็นต้น

1.6 เหตุการณ์พึงสังวรณ์ (Sentinel Event) หมายถึง เหตุการณ์สำคัญรุนแรงและไม่พึงประสงค์เป็นเหตุการณ์ที่ไม่ได้คาดหมายที่อาจเกิดขึ้นได้ มีผลต่อชีวิต ร่างกาย การสูญเสียหน้าที่ของอวัยวะของผู้ป่วย ทรัพย์สิน หรือมีผลกระทบต่อชื่อเสียงของโรงพยาบาลตามที่โรงพยาบาลกำหนดไว้ (ควรมีการเฝ้าระวังเชิงรุก) ก่อให้เกิดความเสียหายอย่างร้ายแรง ซึ่งผู้ที่ทราบข้อมูลต้องรายงานให้ผู้บังคับบัญชาทราบอย่างเร่งด่วน เช่น

- การเสียชีวิตของผู้ป่วยโดยไม่คาดหมาย(ทุกสาเหตุ)
- การเกิดทุพพลภาพถาวร(ทุกสาเหตุ)เกิดความเสียหายร้ายแรงแก่ผู้ป่วย ได้แก่ ผ่าตัดผิดคน/ผิดอวัยวะ/ผิดที่ การลักพาทารก/ผู้ป่วย ผู้ป่วยพยายามฆ่าตัวตาย/ฆ่าตัวตาย
- อุบัติการณ์ของการติดเชื้อแพร่ระบาดในโรงพยาบาล
- ความผิดพลาด/ความเสียหายใดๆที่มีโอกาสนำไปฟ้องร้อง/การเสื่อมเสีย เสียชื่อเสียง

1.7 การวิเคราะห์สาเหตุราก (Root Cause Analysis) หมายถึง การวิเคราะห์เพื่อค้นหาสาเหตุที่แท้จริงของอุบัติการณ์หรือความเสี่ยงที่เกิดขึ้น เพื่อให้สามารถพัฒนาแนวทางแก้ไขป้องกันได้อย่างเหมะสมและตรงกับสาเหตุที่แท้จริง โดยมีวิธีการที่หลากหลายที่จะใช้เป็นเครื่องมือในการวิเคราะห์

1.8 โปรแกรมรายงานความเสี่ยง HRMS on Cloud ย่อมาจาก HRMS: Healthcare Risk Management System on Cloud เป็นระบบบริหารจัดการความเสี่ยงของสถานพยาบาล ประกอบด้วยส่วนของข้อมูลและตัวช่วยในการประเมิน ซึ่งเป็นช่องทางในการรายงานความเสี่ยงของโรงพยาบาลเมืองจันทร์

1.9 ระบบ NRLS: National Reporting and Learning System เป็นระบบฐานข้อมูลอุบัติการณ์ความเสี่ยงภาพรวมของประเทศ ซึ่งใช้ในการแลกเปลี่ยนเรียนรู้จาก เหตุการณ์ไม่พึงประสงค์และความผิดพลาดที่เกิดขึ้น ตามนโยบายความปลอดภัยของผู้ป่วยและบุคลากรสาธารณสุข (Patient and Personnel Safety: 2P Safety)

2. การแบ่งประเภทความเสี่ยง

2.1 ความเสี่ยงทั่วไป (Non Clinic Risk) เป็นความเสี่ยงหรือโอกาสที่จะประสบกับความสูญเสียหรือสิ่งไม่พึงประสงค์ที่ไม่เกี่ยวข้องกับการดูแลรักษาผู้ป่วย เป็นความเสี่ยงที่เกิดขึ้นนอกเหนือจากกระบวนการรักษา ซึ่งสามารถพบได้โดยทั่วไป เช่น การตัดสินใจที่ผิดพลาดจากการใช้ข้อมูลที่ไม่ถูกต้อง ไม่สมบูรณ์ หรือไม่เป็นปัจจุบัน การบันทึกบัญชีผิดพลาด/เกิดการทุจริตในองค์กร/รายงานทางการเงินไม่น่าเชื่อถือ การปฏิบัติงานไม่มีประสิทธิภาพและประสิทธิผล การสูญเสียทรัพยากร/การใช้ทรัพยากรอย่างไม่ประหยัด เกิดความเสียหายต่อชื่อเสียงของหน่วยงาน การไม่ปฏิบัติตามกฎหมาย ระเบียบ วิธีปฏิบัติงาน เช่น สิ่งแวดล้อม อัคคีภัย เครื่องมือ ข้อร้องเรียน เป็นต้น

2.2 ความเสี่ยงทางคลินิก (Clinical Risk) เป็นความเสี่ยงหรือเหตุการณ์ที่ไม่พึงประสงค์ที่เกี่ยวข้องกับการดูแลรักษาผู้ป่วย อันมีเหตุเกิดขึ้นกับผู้ป่วย เป็นความเสี่ยงในการดูแลผู้ป่วย อาจพบร่วมในหลายคลินิกบริการ เช่น ความผิดพลาดของการวินิจฉัย ความผิดพลาดของการวางแผนการดูแลรักษาพยาบาล ความผิดพลาดหรืออุบัติเหตุในการให้การรักษาพยาบาล อาการข้างเคียงจากการใช้ยาหรือการให้เลือด การติดเชื้อในโรงพยาบาล ความผิดพลาดในการบันทึกข้อมูลที่สำคัญทางคลินิก การละเลยในการให้การดูแลสุขภาพผู้ป่วยอย่างต่อเนื่อง แบ่งเป็น 2 กลุ่ม ได้แก่

1) ความเสี่ยงทางคลินิกทั่วไป (Common Clinical Risk) เหตุการณ์หรือการดูแลรักษาที่อาจเกิดอันตรายหรือเหตุการณ์ไม่พึงประสงค์กับผู้ป่วยทั่วไปรายใดก็ได้ไม่จำเพาะโรค

2) ความเสี่ยงเฉพาะโรค (Specific Clinical Risk) ความเสี่ยงใดๆที่เกี่ยวข้องกับการดูแลรักษาผู้ป่วยและอาจเกิดภาวะไม่พึงประสงค์หรือเสียชีวิตโดยระบุจำเพาะโรคและภาวะเสี่ยงที่อาจเกิดขึ้นกับโรคนั้นๆ

ระดับความรุนแรงความเสี่ยงทางคลินิก (Clinic) แบ่งเป็น 9 ระดับ คือ A – I

ระดับ	ลักษณะอุบัติการณ์	ผลกระทบ	ความหมาย
A	Near Miss	เหตุการณ์ที่มีโอกาสผิดพลาด	เสี่ยงแต่ยังไม่เกิด
B	Near Miss	ความผิดพลาดเกิดขึ้นแต่ยังไม่ถึงตัวผู้ป่วยและ/หรือบุคลากร	เกิดแต่ยังไม่ถึง
C	Miss	ความผิดพลาดเกิดขึ้นถึงตัวผู้ป่วยแต่ไม่ถึงอันตราย	ถึงแต่ไม่เป็นไร
D	Miss	ความผิดพลาดถึงผู้ป่วยและต้องให้การดูแลเฝ้าระวังเป็นพิเศษ	ต้องเฝ้าระวังไว้
E	Miss	ความผิดพลาดถึงผู้ป่วยและเกิดอันตรายชั่วคราวแก่ผู้ป่วยและต้องให้การรักษาเพิ่มมากขึ้น	ต้องให้การรักษา

F	Miss	ความผิดพลาดถึงผู้ป่วยและมีผลทำให้ผู้ป่วยต้องได้รับการรักษาและต้องนอนโรงพยาบาลนานขึ้น	ต้องเสียเวลานอนนาน
G	Miss	ความผิดพลาดถึงผู้ป่วยและมีผลทำให้ผู้ป่วยเกิดความพิการถาวร	ต้องพิการถาวร
H	Miss	ความผิดพลาดถึงผู้ป่วยและมีผลทำให้ผู้ป่วยต้องได้รับการช่วยชีวิต	ต้องช่วยชีวิต
I	Miss	ความผิดพลาดถึงผู้ป่วยและเป็นสาเหตุให้ผู้ป่วยเสียชีวิต	เสียชีวิต

ระดับความรุนแรงความเสี่ยงทั่วไป (Non Clinic) ระดับความรุนแรงความเสี่ยงทั่วไป แบ่งเป็น 5 ระดับ

ระดับ	ระดับความรุนแรง	ผลกระทบ
1	เกือบพลาด (Near Miss)	ยังไม่เกิดความผิดพลาด แต่มีแนวโน้มหรือโอกาสที่ทำให้เกิดอุบัติการณ์ได้
2	รุนแรงน้อย (Low Risk)	มีความผิดพลาดเกิดขึ้น แต่ไม่เป็นอันตราย เกิดความเสียหายเล็กน้อยมูลค่าความเสียหายน้อยกว่า 3,000 บาท
3	รุนแรงปานกลาง (Moderate Risk)	มีความผิดพลาดเกิดขึ้น เกิดอันตรายหรือความเสียหายต่อผู้รับบริการ/จ้าหน้าที่/อุปกรณ์เครื่องมือ มูลค่าความเสียหายมากกว่า 3,001-5,000 บาท
4	รุนแรงมาก (High Risk)	มีความผิดพลาดเกิดขึ้น เกิดอันตรายหรือความเสียหายมีโอกาสถูกร้องเรียน/ฟ้องร้อง มูลค่าความเสียหายมากกว่า 5,001-10,000 บาท
5	รุนแรงสูง (High Risk)	มีความผิดพลาดเกิดขึ้น เกิดอันตรายหรือความเสียหายมีโอกาสถูกร้องเรียน/ฟ้องร้อง มูลค่าความเสียหายมากกว่า 10,001 บาทขึ้นไป

2.3 การบริหารความเสี่ยงประกอบด้วย 4 ขั้นตอน ได้แก่

ขั้นตอนที่ 1 การค้นหาความเสี่ยง (Risk Identification) มีขั้นตอน ดังนี้

1.1 การค้นหาความเสี่ยงเชิงรุก ได้แก่ การทบทวนเวชระเบียน การเดินสำรวจกระบวนการทำงาน การรับ-ส่งเวร การเยี่ยมสำรวจภายใน/ภายนอก

1.2 การค้นหาความเสี่ยงเชิงรับ ได้แก่ ข้อมูลจากการรายงานอุบัติการณ์ การทบทวน12 กิจกรรม ข้อร้องเรียน หรือความคิดเห็นของผู้รับบริการ ข้อมูลจากสื่อต่างๆ

1) การค้นหาจากอดีต เช่น ศึกษาความสูญเสียของหน่วยงานที่ผ่านมา เรียนรู้จากประสบการณ์ หรือความผิดพลาดของคนอื่น ทบทวนข้อร้องเรียน
2) การศึกษาจากการสำรวจสภาพการณ์ในปัจจุบัน มี 2 ประเภท คือ
   - การค้นหาเชิงรุกจากการตรวจสอบ เช่น ENV Round, IC Round, Risk Round, การทบทวนเวชระเบียน การค้นหาจากกระบวนการทำงาน
   - การค้นหาเชิงรับจากรายงานต่างๆ เช่น รายงานอุบัติการณ์ รายงานเวรตรวจการบันทึกประจำวันของหน่วยงาน เป็นต้น

3) การจัดทำบัญชีความเสี่ยงของหน่วยงาน (Risk Profile)
4) การจัดบัญชีความเสี่ยงเข้าโปรแกรมความเสี่ยง เพื่อแยกเป็นหมวดหมู่ สะดวกในการวิเคราะห์ แก้ไข ปรับปรุง

ขั้นตอนที่ 2 การประเมินและวิเคราะห์ความเสี่ยง (Risk Assessment)

2.1 ประเภทของความเสี่ยง

1) ความเสี่ยงทางคลินิก หมายถึง ความเสี่ยงเกี่ยวกับการดูแลรักษาซึ่งส่งผลต่อสภาพร่างกายหรืออันตรายต่อผู้ป่วย/เจ้าหน้าที่ ได้แก่ ความปลอดภัยจากการใช้ยา การควบคุมและป้องกันการติดเชื้อ กระบวนการดูแลผู้ป่วย

2) ความสี่ยงทั่วไป หมายถึง ความเสี่ยงที่ไม่ได้มีสาเหตุจากการรักษาพยาบาล แต่เกิดจากปัจจัยอื่นๆ ที่มีผลทำให้เกิดความเสียหาย ได้แก่

- ความเสี่ยงด้านสิ่งแวดล้อม อาชีวอนามัย และความปลอดภัย หมายถึง อุบัติการณ์เกี่ยวกับอาคาร สถานที่ สิ่งอำนวยความสะดวก อุบัติการณ์เกี่ยวกับผลที่เกิดจากการปฏิบัติงานที่มีต่อสุขภาพของบุคลากร ความปลอดภัยด้านทรัพย์สิน อุบัติการณ์เกี่ยวกับเครื่องมือ อุปกรณ์ ที่ใช้ในการดูแลรักษา
- ความเสี่ยงด้านข้อร้องเรียน และสิทธิผู้ป่วย หมายถึง อุบัติการณ์เกี่ยวกับการพิทักษ์สิทธิผู้ป่วย เช่น การให้ข้อมูลก่อนลงนามยินยอมรับการรักษา การเปิดเผยข้อมูลผู้ป่วย การตัดสินใจรับ หรือไม่รับการรักษา อุบัติการณ์ข้อร้องเรียนด้านต่างๆ เช่น พฤติกรรมบริการ
- ความเสี่ยงด้านเทคโนโลยีสารสนเทศและเวชระเบียน หมายถึง อุบัติการณ์เกี่ยวกับคอมพิวเตอร์ ความไม่พร้อมใช้ของคอมพิวเตอร์ โปรแกรมการสื่อสาร บันทึก การจัดเก็บข้อมูล และเกี่ยวกับข้อมูลสถิติต่างๆ อุบัติการณ์เกี่ยวกับเอกสารประวัติของผู้ป่วย เช่นการบันทึก การจัดเก็บ การค้นหา การระบุตัวผู้ป่วย การบันทึกสิทธิ์ การรักษา การบันทึกค่ารักษาพยาบาล การบันทึกที่แสดงถึงคุณภาพ การรักษาพยาบาล การป้องกันโรค การฟื้นฟูสภาพ การสื่อสารของสหวิชาชีพ
- ด้านการสนับสนุนบริการ หมายถึง การช่วยเหลืออำนวยความสะดวกจากงานสนับสนุนอุบัติการณ์เกี่ยวกับการสูญเสียรายได้ ทรัพย์สินของทางราชการต่างๆ

2.2 การแบ่งระดับความรุนแรง

1) ระดับความรุนแรงของความเสี่ยงทางคลินิก แบ่งเป็น 9 ระดับ

ระดับ A : ไม่มีอุบัติการณ์เกิดขึ้น แต่มีโอกาสเกิดอุบัติการณ์ขึ้นได้ หรือถ้าไม่ให้ความสนใจก็อาจมีอุบัติการณ์เกิดขึ้น

ระดับ B : มีอุบัติการณ์เกิดขึ้น แต่ไม่เป็นอันตราย หรือ ไม่เกิดความเสียหายต่อผู้ป่วย/เจ้าหน้าที่ เนื่องจากอุบัติการณ์นั้นไม่ถึงตัวผู้ป่วย

ระดับ C : มีอุบัติการณ์เกิดขึ้นแต่ไม่เป็นอันตราย หรือเกิด ไม่เกิดความเสียหาย แต่อุบัติการณ์ที่เกิดขึ้นนั้นถึงตัวผู้ป่วย/เจ้าหน้าที่

ระดับ D : มีอุบัติการณ์เกิดขึ้นแต่ไม่เป็นอันตราย หรือเกิด ไม่เกิดความเสียหายต่อผู้ป่วย/เจ้าหน้าที่ แต่ยังจำเป็นต้องได้รับการติดตามดูแลและเฝ้าระวังเพิ่มเติม

ระดับ E : มีอุบัติการณ์เกิดขึ้นและเป็นอันตราย หรือเกิดความเสียหายต่อผู้ป่วย/เจ้าหน้าที่เพียงชั่วคราว รวมถึงจำเป็นต้องได้รับการดูแลรักษา และแก้ไขเพิ่มเติม

ระดับ F : มีอุบัติการณ์เกิดขึ้นถึง และเป็นอันตราย หรือเกิดความเสียหายต่อผู้ป่วย/เจ้าหน้าที่ เพียงชั่วคราว รวมถึงต้องได้รับการดูแลรักษาในโรงพยาบาล หรือยืดระยะเวลาในการรักษาตัวในโรงพยาบาลออกไป

ระดับ G : มีอุบัติการณ์เกิดขึ้นถึง และเป็นอันตราย หรือเกิดความเสียหายต่อผู้ป่วย/เจ้าหน้าที่ ต้องส่งต่อ หรือเกิดความพิการอย่างถาวร

ระดับ H : มีอุบัติการณ์เกิดขึ้นถึง และเป็นอันตรายต่อผู้ป่วย/เจ้าหน้าที่จนเกือบถึงแก่ชีวิตต้องช่วยชีวิต

ระดับ I : มีอุบัติการณ์เกิดขึ้นถึง และเป็นอันตรายต่อผู้ป่วย/จ้าหน้าที่จนถึงแก่ชีวิต

2) ระดับความรุนแรงของความเสี่ยงทั่วไป มี 5 ระดับ คือ

ระดับ 1 : **Near Miss** เป็นเรื่องปกติ อาจก่อกวน หรือสร้างความรำคาญ ยังไม่เกิดความเสียหาย หรือมีโอกาสสูญเสียทรัพย์สินแต่ยังไม่สูญเสีย

ระดับ 2 : **Low Risk** มีความผิดพลาดเกิดขึ้น แต่ไม่เป็นอันตราย เกิดความเสียหายเล็กน้อยมูลค่าความเสียหายน้อยกว่า 3,000 บาท ก่อให้เกิดความเสียหายต่อทรัพย์สิน แต่สามารถแก้ไขปัญหาได้ หรือผู้ป่วยไม่พอใจแจ้งเจ้าหน้าที่

ระดับ 3 : **Moderate Risk** มีความผิดพลาดเกิดขึ้น เกิดอันตรายหรือความเสียหายต่อผู้รับบริการ/จ้าหน้าที่/อุปกรณ์เครื่องมือมูลค่าความเสียหายมากกว่า 3,001-5,000 บาทซึ่งสามารถแก้ไขปัญหาได้ แต่ต้องสูญเสียบางอย่างไป หรือผู้ป่วยไม่พอใจต้องให้โรงพยาบาลรับผิดชอบโดยแจ้งหัวหน้างาน หรือผู้อำนวยการโดยตรง

ระดับ 4 : **High Risk** มีความผิดพลาดเกิดขึ้น เกิดอันตรายหรือความเสียหาย มีโอกาสถูกร้องเรียน/ฟ้องร้องมูลค่าความเสียหายมากกว่า 5,001-10,000 บาท หรือเสียชื่อเสียงต่อโรงพยาบาลอย่างรุนแรง

ไม่สามารถแก้ไขได้ หรือผู้ป่วยไม่พอใจอย่างมากต้องให้โรงพยาบาลรับผิดชอบโดยฟ้องร้องผ่านองค์กรภายนอก

ระดับ 5 : High Risk มีความผิดพลาดเกิดขึ้น เกิดอันตรายหรือความเสียหาย มีโอกาสถูกร้องเรียน/ฟ้องร้องมูลค่าความเสียหายมากกว่า 10,001 บาทขึ้นไป หรือเสียชื่อเสียงต่อโรงพยาบาลอย่างรุนแรง ไม่สามารถแก้ไขได้ หรือผู้ป่วยไม่พอใจอย่างมากต้องให้โรงพยาบาลรับผิดชอบโดยฟ้องร้องผ่านองค์กรภายนอก

ขั้นตอนที่ 3 การจัดการกับความเสี่ยง (Action to Manage Risk)

3.1 กลยุทธ์การควบคุมการสูญเสีย

1) การหลีกเลี่ยงความเสี่ยง เช่น การส่งต่อ การผ่องถ่ายความเสี่ยง เช่น จ้างเหมาบริษัทเพื่อดูแลเครื่องมือทางการแพทย์ และห้องปฏิบัติการ
2) การป้องกันความเสี่ยง เช่น ใส่ของมีคมในกล่องที่หนา การมีระบบบำรุงรักษาเชิงป้องกัน เช่น การตรวจสอบเครื่องมือ การสอบเทียบเครื่องมือต่างๆ มีระเบียบปฏิบัติในการทำงาน เช่น การให้ยา การตรวจอุปกรณ์ในรถฉุกเฉิน การให้ความรู้เจ้าหน้าที่
3) มีระบบเฝ้าระวังความเสี่ยง ได้แก่ ทุกหน่วยงานมีระบบการรายงานความเสี่ยงหลายช่องทางสะดวก มีการสื่อสารย้อนกลับ ไม่เปิดเผยข้อมูลแก่ผู้ไม่เกี่ยวข้อง

3.2 การจัดการหลังเกิดเหตุ

1) ลดความสูญเสียหลังเกิดเหตุการณ์ เป็นการดูแลแก้ปัญหาฉับพลัน โดยการเอาใจใส่ให้ข้อมูลตรงไปตรงมา ภายใต้คำแนะนำ การสื่อสาร ความเข้าใจที่ดีต่อกัน ประคับประคองจิตใจ ขวัญกำลังใจทั้งผู้ป่วย ญาติ และเจ้าหน้าที่ รายงานผู้บริหารสูงสุดและคณะกรรมการบริหารโรงพยาบาล ติดตามประเมินผล
2) การบริหารเงินค่าชดเชยกรณีต้องชดเชยค่าเสียหาย ทีมควบคุมค่าเสียหาย/ไกลเกลี่ยจะเป็นผู้สรุปข้อมูลปัญหา นำเสนอต่อผู้บริหารสูงสุดและทีมกรรมการบริหารโรงพยาบาลร่วมกันพิจารณา
3) การรายงานอุบัติการณ์/ความเสี่ยง (Incident Report)

ความเสี่ยงทางคลินิกระดับ A-B หรือความเสี่ยงทั่วไประดับ 1 (Near Miss)

1) ผู้ที่พบเห็นเหตุการณ์ประเมินสถานการณ์ / เหตุการณ์ที่เกิดขึ้นแจ้งหัวหน้าเวร/หัวหน้าหน่วยงานรับทราบ เพื่อหาแนวทางป้องกันแก้ไขโดยหัวหน้างานเป็นความเสี่ยงระดับหน่วยงาน
2) ผู้พบเห็นเหตุการณ์ บันทึกรายงานในโปรแกรม HRMS on Cloud
3) ผู้รับผิดชอบ RM ในหน่วยงาน สรุปอุบัติการณ์ประจำเดือน ส่งเลขาทีมบริหารความเสี่ยงภายใน 1 เดือน

ความเสี่ยงทางคลินิกระดับ C-D หรือความเสี่ยงทั่วไประดับ 2 (Low Risk)

1) ผู้ที่พบเห็นเหตุการณ์ประเมินสถานการณ์ / เหตุการณ์ที่เกิดขึ้น แจ้งหัวหน้าเวร/หัวหน้าหน่วยงานรับทราบ เพื่อหาแนวทางป้องกันแก้ไขโดยหัวหน้างาน เป็นความเสี่ยงระดับหน่วยงาน
2) ผู้พบเห็นเหตุการณ์ บันทึกรายงานในโปรแกรม HRMS on Cloud
3) ผู้รับผิดชอบ RM ในหน่วยงาน สรุปอุบัติการณ์ประจำเดือน ส่งเลขาทีมบริหารความเสี่ยง ภายใน 1 สัปดาห์

ความเสี่ยงทางคลินิกระดับ E- F หรือความเสี่ยงทั่วไประดับ 3 (Moderate Risk)

1) ผู้ที่พบเห็นเหตุการณ์ประเมินสถานการณ์ / เหตุการณ์ที่เกิดขึ้นพร้อมกับแก้ไขเหตุการณ์เบื้องต้น แจ้งหัวหน้าเวร/หัวหน้าหน่วยงานรับทราบภายใน 24 ชั่วโมง เพื่อหาแนวทางป้องกันแก้ไขโดยหัวหน้างาน เป็นความเสี่ยงระดับหน่วยงาน
2) ผู้พบเห็นเหตุการณ์ บันทึกรายงานในโปรแกรม HRMS on Cloud
3) ผู้รับผิดชอบ RM ในหน่วยงาน สรุปอุบัติการณ์ประจำเดือน ส่งเลขาทีมบริหารความเสี่ยง ภายใน 72 ชั่วโมง (3 วัน)
4) ผู้รับผิดชอบ RM ในหน่วยงาน สรุปอุบัติการณ์ประจำเดือน ส่งเลขาทีมบริหารความเสี่ยง ทุกเดือน

ความเสี่ยงทางคลินิกระดับ G – H - I หรือความเสี่ยงทั่วไประดับ 4-5 (High Risk) และsentinelevent (เหตุการณ์พึงสังวรณ์)

1) ผู้ที่พบเห็นเหตุการณ์ประเมินสถานการณ์/เหตุการณ์ที่เกิดขึ้นพร้อมกับแก้ไขเหตุการณ์เบื้องต้น แจ้งหัวหน้าเวร/หัวหน้าหน่วยงานรับทราบทันที
2) กรณีในเวลาราชการ หัวหน้าหน่วยงานต้องรายงานผู้อำนวยการโรงพยาบาลและหรือผู้จัดการความเสี่ยงโปรแกรมที่เกี่ยวข้องทันที
3) กรณีนอกเวลาราชการ หัวหน้าเวรรายงานแพทย์เวรทันที แล้วแพทย์เวรรายงานผู้อำนวยการทันที
4) ผู้พบเห็นเหตุการณ์ บันทึกรายงานในโปรแกรม HRMS on Cloud
5) ผู้รับผิดชอบ RM ในหน่วยงาน สรุปอุบัติการณ์ประจำเดือน ส่งเลขาทีมบริหารความเสี่ยง ภายใน 24 ชั่วโมง (1 วัน)
6) ผู้รับผิดชอบ RM ในหน่วยงาน สรุปอุบัติการณ์ประจำเดือน ส่งเลขาทีมบริหารความเสี่ยง ทุกเดือน

สรุปเปรียบเทียบคำจำกัดความระดับความรุนแรงของความเสี่ยงแต่ละประเภทเพื่อให้เข้าใจง่าย

ความเสี่ยงด้านคลินิก (Clinical risk)	**ความเสี่ยงทั่วไป (Non clinical risk)**	**ผลกระทบ**
A = เสี่ยง/ยังไม่เกิดเหตุการณ์/มีโอกาสเกิด	1 = เสี่ยง/ยังไม่เกิดเหตุการณ์/มีโอกาสเกิด	ไม่มีผลกระทบ (Near miss)
B = เกิดเหตุการณ์แล้ว แต่ยังไม่มีผลกระทบต่อผู้ป่วย	2 = เกิดเหตุการณ์แล้ว แต่ยังไม่มีผลกระทบสูญเสียเงิน ค่าใช้จ่ายน้อยกว่า 3,000 บาท	ไม่มีผลกระทบหรือมีผลกระทบน้อย (Near miss)
C = เกิดเหตุการณ์แล้ว มีผลกระทบต่อคน หน่วยงาน, โรงพยาบาล แต่ไม่ทำให้เกิดความเสียหาย/อันตรายต่อผู้ป่วย	3 = เกิดเหตุการณ์ผิดพลาดแล้ว มีผลกระทบต่อคน มูลค่าความเสียหายมากกว่า 3,001-5,000 บาท	มีผลกระทบปานกลาง
D = เกิดเหตุการณ์แล้ว มีผลกระทบต่อคน, หน่วยงาน, โรงพยาบาล ต้องมีการเฝ้าระวังต่อเพื่อให้มั่นใจว่าไม่เกิดอันตรายต่อผู้ป่วย		
E = เกิดเหตุการณ์แล้ว มีผลกระทบต่อคน, หน่วยงาน, โรงพยาบาล เกิดความเสียหาย/อันตรายชั่วคราวต่อผู้ป่วย ต้องแก้ไขหรือรักษาให้หายได้เป็นปกติ	4 = เกิดเหตุการณ์ผิดพลาดแล้ว เสียชื่อเสียง/ความเชื่อถือ,เสียลูกค้า, แก้ไขไม่ได้ อาจถูกฟ้องร้อง สูญเสียเงิน มูลค่าความเสียหายมากกว่า 5,001-10,000 บาท	มีผลกระทบมาก
F = เกิดเหตุการณ์แล้ว มีผลกระทบต่อคน, หน่วยงาน, โรงพยาบาล ต้องใช้เวลารักษาผู้ป่วยนานเกินกำหนด ต้องส่งต่อการรักษา		
G = เกิดเหตุการณ์แล้ว มีผลกระทบทำให้เสียชื่อเสียง, เสียงความเชื่อถือ, อาจถูกฟ้องร้องเรียกค่าเสียหายรักษาไม่ได้ มีความพิการถาวรหรือมีผลเสียที่ร้ายแรงระยะยาวต่อผู้ป่วย	5 = เกิดเหตุการณ์ผิดพลาดแล้ว แล้วเกิดการฟ้องร้อง แก้ไขไม่ได้ มูลค่าความเสียหายมากกว่า 10,001 บาทขึ้นไป	มีผลกระทบรุนแรงละเลยไม่ได้
H = เกิดเหตุการณ์หรือความคลาดเคลื่อนขึ้นแล้ว มีผลกระทบทำให้เสียชื่อเสียง, เสียความเชื่อถือ, แก้ไขไม่ได้ถูกฟ้องร้อง, เป็นอันตรายจนเกือบถึงชีวิตต้องทำการช่วยชีวิตผู้ป่วย(CPR)		
I = เกิดเหตุการณ์แล้ว มีผลทำให้เสียชื่อเสียง, เสียความเชื่อถือ, แก้ไขไม่ได้ เกิดการฟ้องร้อง, เป็นอันตรายต่อผู้ป่วยจนเกิดการเสียชีวิต		

3.3 ข้อร้องเรียนจากผู้รับบริการ

1) รายงานหัวหน้างานและเลขาทีมบริหารความเสี่ยง ประสานทีมดำเนินการไกล่เกลี่ย/ลดความเสี่ยง/สอบสวนและแจ้งผู้อำนวยการทราบภายใน 24 ชม.
2) ทีมบริหารความเสี่ยงประเมินและติดตามผลการดำเนินการแก้ไข สรุปผลหลังเกิดเหตุการณ์รายงานต่อผู้อำนวยการโรงพยาบาลภายใน 1 สัปดาห์

3.4 การจำแนกความเสี่ยงและการจัดการ

1) ทีม PCT : การดูแลผู้ป่วยทางคลินิก
2) ทีม PTC : ความคลาดเคลื่อนทางยา
3) ทีม IC : การควบคุมป้องกันและเฝ้าระวังการติดเชื้อ
4) ทีม ENV : อุปกรณ์และเครื่องมือทางการแพทย์
5) ทีม IM : เทคโนโลยีและสารสนเทศ
6) ทีม HRD : บุคลากร การสนับสนุนบริการ และประสานงาน
7) ทีมเจรจาไกลเกลี่ย : ข้อร้องเรียนและสิทธิผู้ป่วย

3.5 เรื่องที่ต้องประสานกับหน่วยงานอื่น / เรื่องที่ต้องวิเคราะห์ RCA

1) ความเสี่ยงทางคลินิกระดับ E ขึ้นไป / ความเสี่ยงทั่วไประดับ 3 ขึ้นไป
2) ความเสี่ยงทางคลินิกระดับ C,D / ความเสี่ยงทั่วไประดับ 2 ที่เกิดขึ้นซ้ำมากกว่า 3 ครั้ง/เดือน

3.6 การสรุปข้อมูลอุบัติการณ์/ความเสี่ยง

1) ทีมบริหารความเสี่ยงสรุปข้อมูลทุกเดือน เสนอที่ประชุมคณะกรรมการบริหารโรงพยาบาลและสรุปข้อมูลรวมทุก 3 เดือน
2) ส่งกลับให้ทุกหน่วยงานรับทราบเพื่อนำไปวิเคราะห์ในหน่วยงาน หาแนวทางแก้ไข ป้องกันต่อไป เรื่องที่ต้องวิเคราะห์ RCA ส่งข้อมูลกลับคณะกรรมการบริหารความเสี่ยง โรงพยาบาลภายใน 30 วัน

ขั้นตอนที่ 4 ประเมินผล (Evaluation) เป็นการประเมินประสิทธิผลของระบบบริหารความเสี่ยงและความปลอดภัยอย่างสม่ำเสมอ นำไปสู่การปรับปรุงระบบให้ดีขึ้น

1) ประเมินระบบ/กระบวนการที่วางไว้ /ความเสี่ยงที่เกิดขึ้นใหม่
2) ประเมินประสิทธิภาพของระบบบริหารความเสี่ยง
   - การบันทึกรายงานอุบัติการณ์ตามระยะเวลาที่กำหนด
   - จำนวน / ประเภท ของความเสี่ยง, อุบัติการณ์
   - อัตราของความเสี่ยง / อุบัติการณ์ตามกลุ่มประเภทความเสี่ยง, ความรุนแรง
   - ระดับความรุนแรง
   - อัตราการเกิดอุบัติการณ์ซ้ำ

4.1 การประเมินความเสี่ยง หรับการประเมินความเสี่ยงจากอุบัติการณ์ มีแนวทางดังนี้

1) ให้แต่ละหน่วยงานวิเคราะห์ว่าความเสี่ยงนั้นอยู่ในความเสี่ยงประเภทใด (Clinical Risk or Non-Clinical Risk)
2) ประเมินระดับความรุนแรง
3) รายงานความเสี่ยงตามช่องทางการรายงานอุบัติการณ์

4) การประเมินเพื่อจัดทำบัญชีความเสี่ยง มีแนวทางดังนี้

- นำความเสี่ยงของหน่วยงาน ทั้งที่เกิดขึ้นแล้ว และยังไม่เกิดขึ้น (ความเสี่ยงจากกระบวนการหลัก และความเสี่ยงจากอุบัติการณ์) มาประเมินความเสี่ยงในตาราง Risk Matrix
- หลังจากประเมินความเสี่ยงแล้วให้นำมาจัดเรียงความเสี่ยง 5 อันดับของหน่วยงาน เพื่อจัดลำดับความสำคัญของความเสี่ยงนั้น เพื่อนำมาวิเคราะห์หาสาเหตุ และหาทางแก้ไขเชิงระบบอย่างเหมาะสม รวมทั้งเป็นการวางแนวทางป้องกันความเสี่ยงที่อาจเกิดซ้ำ
- การวิเคราะห์หาสาเหตุที่แท้จริงของปัญหา RCA : Root Cause Analysis เป็นเครื่องมือที่จะช่วยให้การแก้ปัญหาหรือการพัฒนาคุณภาพมีความยั่งยืน ไม่เกิดเหตุการณ์ที่ไม่พึงประสงค์ซ้ำขึ้นอีก ด้วยการวิเคราะห์เพื่อให้เข้าไปจัดการกับสาเหตุที่เป็นต้นตอของปัญหาจริงๆ มิใช่แก้ปัญหาแต่ปลายเหตุ

4.2 เมื่อไร จะต้องทำ RCA

เมื่อเหตุการณ์ > มีความรุนแรง มีผลกระทบสูง > ควรทำ RCA ทุกรายเป็นรายกรณี

> มีความรุนแรงต่ำ ให้ดูแนวโน้ม หากเกิดซ้ำ > ควรทำ RCA ในภาพรวม

> หากมองเห็นแนวทางแก้ปัญหาชัดเจน > แก้ไขปัญหา > ไม่ต้องทำ RCA

บทที่ 4 ความเสี่ยงด้านความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ

1. รหัสและรายการอุบัติการณ์

รายการอุบัติการณ์ความเสี่ยงในกลุ่มอุบัติการณ์ความเสี่ยงทั่วไป (General Risk Incident: G)
หมวดอุบัติการณ์ความเสี่ยง Personnel Safety Goals: P

ประเภทอุบัติการณ์ความเสี่ยง S: Social Media and Communication มี 2 ประเภทย่อย ได้แก่
S1 : Security and Privacy of Information
S2 : Social Media and Communication Professionalism

ลำดับ	รหัสอุบัติการณ์	ชื่ออุบัติการณ์ความเสี่ยง	SIMPER
1	GPS101	เกิดอุบัติการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ทำให้ข้อมูลความลับของสถานพยาบาลรั่วไหล (Confidentiality Failure)	S1
2	GPS102	เกิดอุบัติการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ทำให้ข้อมูลสารสนเทศของสถานพยาบาลถูกแก้ไข/ลบ/เพิ่มเติม/ทำให้เสียหายหรือสูญหายโดยมิชอบ (Integrity Failure)	S1
3	GPS103	เกิดอุบัติการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ทำให้ระบบสารสนเทศของสถานพยาบาลขัดข้อง/ใช้การไม่ได้/ทำงานช้าหรือไม่ปกติ (Availability Failure)	S1
4	GPS104	เกิดอุบัติการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ทำให้เกิดความเสียหายต่อข้อมูลหรือระบบสารสนเทศของสถานพยาบาลมากกว่าหนึ่งด้าน (Multiple Failures) ระหว่าง Confidentiality Failure, Integrity Failure และ Availability Failure	S1
5	GPS105	เกิดอุบัติการณ์การละเมิดความเป็นส่วนตัว (Privacy) ของข้อมูลส่วนบุคคลของบุคลากรหรือนักศึกษาของสถานพยาบาล ที่ไม่ใช่อุบัติการณ์ด้านความมั่นคงปลอดภัยไซเบอร์	S1
6	GPS106	เกิดอุบัติการณ์ความละเมิดความเป็นส่วนตัว (Privacy) ของข้อมูลส่วนบุคคลของผู้ป่วย/ผู้รับบริการ หรือบุคคลภายนอก ที่ไม่ใช่อุบัติการณ์ด้านความมั่นคงปลอดภัยไซเบอร์	S1
7	GPS201	บุคลากรถูกกล่าวถึงหรือวิพากษ์วิจารณ์ในทางลบบนสื่อสังคมออนไลน์หรือสื่อสาธารณะที่เกี่ยวข้องกับการปฏิบัติหน้าที่	S2
8	GPS202	บุคลากรถูกกล่าวถึงหรือวิพากษ์วิจารณ์ในทางลบบนสื่อสังคมออนไลน์หรือสื่อสาธารณะที่ไม่ได้เกี่ยวข้องกับการปฏิบัติหน้าที่	S2
9	GPS203	บุคลากรใช้สื่อสังคมออนไลน์ไม่เหมาะสม เกิดผลกระทบทางลบต่อตนเอง บุคลากรคนอื่น สถานพยาบาล ผู้ป่วย/ผู้รับบริการ หรือบุคคลภายนอก	S2
10	GPS204	เกิดอุบัติการณ์ที่ส่งผลกระทบทางลบต่อสถานพยาบาลบนสื่อสังคมออนไลน์ เช่น Drama, Fake News แต่ไม่ได้เกิดจากบุคลากร และไม่กระทบบุคลากรคนใดคนหนึ่งโดยตรง	S2

รายการอุบัติการณ์ความเสี่ยงในกลุ่มอุบัติการณ์ความเสี่ยงทั่วไป (General Risk Incident:. G)
หมวดอุบัติการณ์ความเสี่ยง Organization Safety Goals: O

ประเภทอุบัติการณ์ความเสี่ยง I: Information Technology & Communication, Internal control & Inventory มี 2 ประเภทย่อย ได้แก่

I1 : Information Technology & Communication

I2 : Internal Control & Inventory

ลำดับ	รหัสอุบัติการณ์	ชื่ออุบัติการณ์ความเสี่ยง	มาตรฐาน
1	GOI101	เกิดปัญหาด้าน Hardware เช่น ไม่มีแผนบริหารจัดการ/ไม่เพียงพอ/ไม่พร้อมใช้/ใช้ไม่ตรงวัตถุประสงค์/ใช้ผิดวิธี - เทคนิค	ตอนที่ I-4/ I1
2	GOI102	เกิดปัญหาด้าน Network & Security เช่น ไม่พร้อมใช้/ระบบล่ม/มีการเข้าถึงโดยผู้ไม่มีสิทธิ์	ตอนที่ I-4/ I1
3	GOI103	เกิดปัญหาด้าน Software เช่น ไม่เข้ากับ hardware/ไม่พร้อมใช้/ไม่ตอบสนองความต้องการ/ใช้ผิดวิธี-เทคนิค	ตอนที่ I-4/ I1
4	GOI104	เกิดปัญหาด้าน User & IT Team เช่น ไม่มอบหมายผู้รับผิดชอบ/ไม่พร้อม/ไม่ครอบคลุมบทบาทหน้าที่/ขาดความรู้และทักษะ	ตอนที่ I-4/ I1
5	GOI105	เกิดปัญหาด้านข้อมูล สารสนเทศ เช่น ไม่ถูกต้อง/ไม่ครบถ้วน/ไม่น่าเชื่อถือ/ไม่เป็นปัจจุบัน	ตอนที่ I-4/ I1
6	GOI106	เกิดปัญหาด้านระบบ/กระบวนการสื่อสาร เช่น ไม่มีแผน/วิธีการหรือช่องทางการสื่อสาร, ไม่สื่อสารหรือสื่อสารไม่ต่อเนื่อง/ไม่ครบถ้วน, ขาดการติดตามประเมินผลการสื่อสาร	ตอนที่ I-3/ I1
7	GOI201	เกิดปัญหาด้านการควบคุมทรัพย์สิน เช่น ไม่กำหนดระเบียบ/ผู้รับผิดชอบ, ไม่มีทะเบียนคุม/เอกสารหลักฐานกำกับ, ขาดการตรวจสอบหรือสอบทาน	ตอนที่ I-1/ I2
8	GOI202	เกิดปัญหาด้านระบบบริหารการพัสดุ เช่น ไม่กำหนดระเบียบ/แผนความต้องการและการจัดหา,ไม่มีทะเบียนคุม/การตรวจรับ/การบำรุงรักษา,ขาดการควบคุมการแจกจ่าย/การจำหน่าย	ตอนที่ I-1/ I2
9	GOI203	เกิดปัญหาด้านการควบคุมการใช้ทรัพยากร เช่น จัดสรรไม่เหมาะสม/ใช้ไม่คุ้ม-ไม่ถูกตามมาตรฐาน/บุคลากรไม่ปฏิบัติตามข้อกำหนด-ขาดทักษะการใช้	ตอนที่ II-3/ I2

2. การประมาณความเสี่ยง (Risk estimation)

เป็นการดูปัญหาความเสี่ยงในแง่ของโอกาสการเกิดเหตุ (Incident) หรือเหตุการณ์ (Event) ว่ามีมากน้อยเพียงไรและผลที่ติดตามมาว่ามีความรุนแรงหรือเสียหายมากน้อยเพียงใด

เกณฑ์การประมาณ เป็นการกำหนดเกณฑ์ที่จะใช้ในการประมาณความเสี่ยง ได้แก่ ระดับโอกาสที่จะเกิดความเสี่ยง ระดับความรุนแรงของผลกระทบ และระดับความเสี่ยง ซึ่งใช้เกณฑ์ดังนี้

ขั้นตอนที่ 1 ระดับโอกาสในการเกิดเหตุการณ์ต่างๆ (Likelihood) กำหนดเกณฑ์ไว้ 5 ระดับ ดังนี้

ระดับโอกาสในการเกิดเหตุการณ์ต่างๆ (Likelihood) เชิงปริมาณ		
ระดับ	**โอกาสที่จะเกิด**	**คำอธิบาย**
5	รุนแรงสูง (High Risk)	1 เดือน / ครั้ง หรือมากกว่า
4	รุนแรงมาก (High Risk)	1 - 6 เดือน / ครั้ง แต่ไม่เกิน 5 ครั้ง
3	รุนแรงปานกลาง (Moderate Risk)	1 ปี / ครั้ง
2	รุนแรงน้อย (Low Risk)	2 – 3 ปี / ครั้ง
1	เกือบพลาด (Near Miss)	5 ปี / ครั้ง

ระดับโอกาสในการเกิดเหตุการณ์ต่างๆ (Likelihood) เชิงคุณภาพ		
ระดับ	**โอกาสที่จะเกิด**	**คำอธิบาย**
5	รุนแรงสูง (High Risk)	มีโอกาสในการเกิดแทบทุกครั้ง
4	รุนแรงมาก (High Risk)	มีโอกาสในการเกิดค่อนข้างสูงหรือบ่อยๆ
3	รุนแรงปานกลาง (Moderate Risk)	มีโอกาสบางครั้ง
2	รุนแรงน้อย (Low Risk)	มีโอกาสเกิดแต่นานๆ ครั้ง
1	เกือบพลาด (Near Miss)	มีโอกาสเกิดในกรณียกเว้น

ขั้นตอนที่ 2 ระดับความรุนแรงของผลกระทบของความเสี่ยง (Impact) กำหนดเกณฑ์ไว้ 5 ระดับ ดังนี้

ระดับความรุนแรงของผลกระทบของความเสี่ยง (Impact) เชิงปริมาณ		
ระดับ	**โอกาสที่จะเกิด**	**คำอธิบาย**
5	รุนแรงสูง (High Risk)	มูลค่าความเสียหาย มากกว่า 10,001 บาทขึ้นไป
4	รุนแรงมาก (High Risk)	มูลค่าความเสียหาย 5,001 - 10,000 บาท
3	รุนแรงปานกลาง (Moderate Risk)	มูลค่าความเสียหาย 3,001 - 5,000 บาท
2	รุนแรงน้อย (Low Risk)	มูลค่าความเสียหาย 1,001 - 3,000 บาท
1	เกือบพลาด (Near Miss)	มูลค่าความเสียหาย น้อยกว่า 1,000 บาท

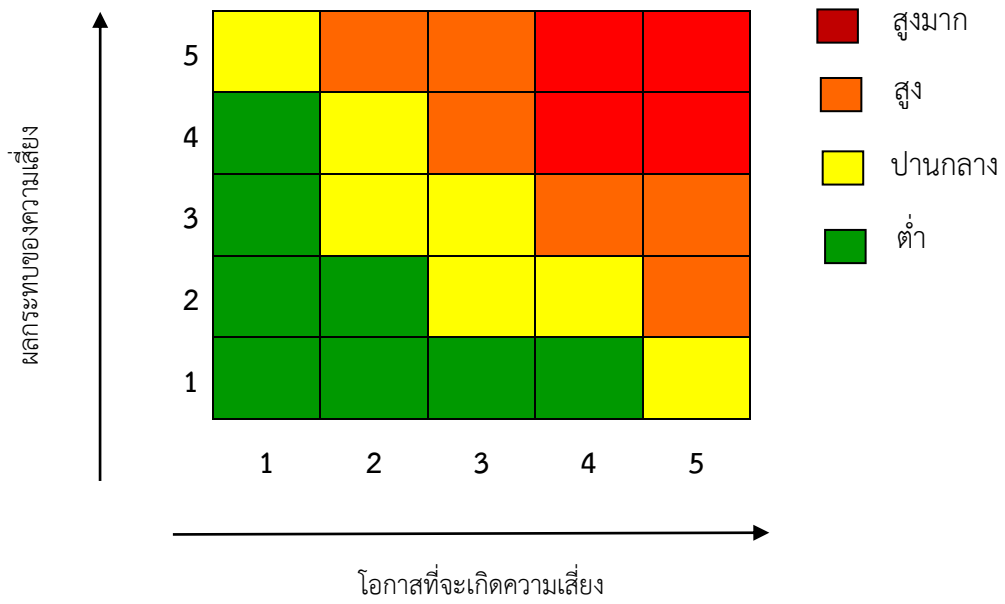
ระดับความรุนแรงของผลกระทบของความเสี่ยง (Impact) **เชิงคุณภาพ**		
ระดับ	**โอกาสที่จะเกิด**	**คำอธิบาย**
5	รุนแรงสูง (High Risk)	เกิดเหตุการณ์ผิดพลาดแล้วแล้วเกิดการฟ้องร้อง แก้ไขไม่ได้
4	รุนแรงมาก (High Risk)	เกิดเหตุการณ์ผิดพลาดแล้ว เสียชื่อเสียง/ความเชื่อถือ/เสียลูกค้า แก้ไขไม่ได้ อาจถูกฟ้องร้อง สูญเสียเงิน
3	รุนแรงปานกลาง (Moderate Risk)	เกิดเหตุการณ์ผิดพลาดแล้ว มีผลกระทบต่อคน
2	รุนแรงน้อย (Low Risk)	เกิดเหตุการณ์แล้ว แต่ยังไม่มีผลกระทบ
1	เกือบพลาด (Near Miss)	เสี่ยง/ยังไม่เกิดเหตุการณ์/มีโอกาสเกิด

ระดับความรุนแรงของผลกระทบของความเสี่ยงต่อระบบเทคโนโลยีสารสนเทศ		
ระดับ	**ระดับความรุนแรง**	**ผลกระทบ**
5	รุนแรงสูง (High Risk)	เกิดความสูญเสียต่อระบบ IT ที่สำคัญทั้งหมดและเกิดความเสียหายอย่างมากต่อความปลอดภัยของข้อมูลต่างๆ
4	รุนแรงมาก (High Risk)	เกิดปัญหากับระบบ IT ที่สำคัญ และระบบความปลอดภัยซึ่งส่งผลต่อความถูกต้องของข้อมูลบางส่วน
3	รุนแรงปานกลาง (Moderate Risk)	ระบบมีปัญหาและมีความสูญเสียไม่มาก
2	รุนแรงน้อย (Low Risk)	เกิดเหตุการณ์เล็กน้อยแก้ไขได้
1	เกือบพลาด (Near Miss)	เกิดเหตุการณ์ที่ไม่มีความสำคัญ

ขั้นตอนที่ 3 ระดับความเสี่ยง (Degree of Risk)

กำหนดเกณฑ์ไว้ 4 ระดับ ได้แก่ สูงมาก สูง ปานกลาง และต่ำ

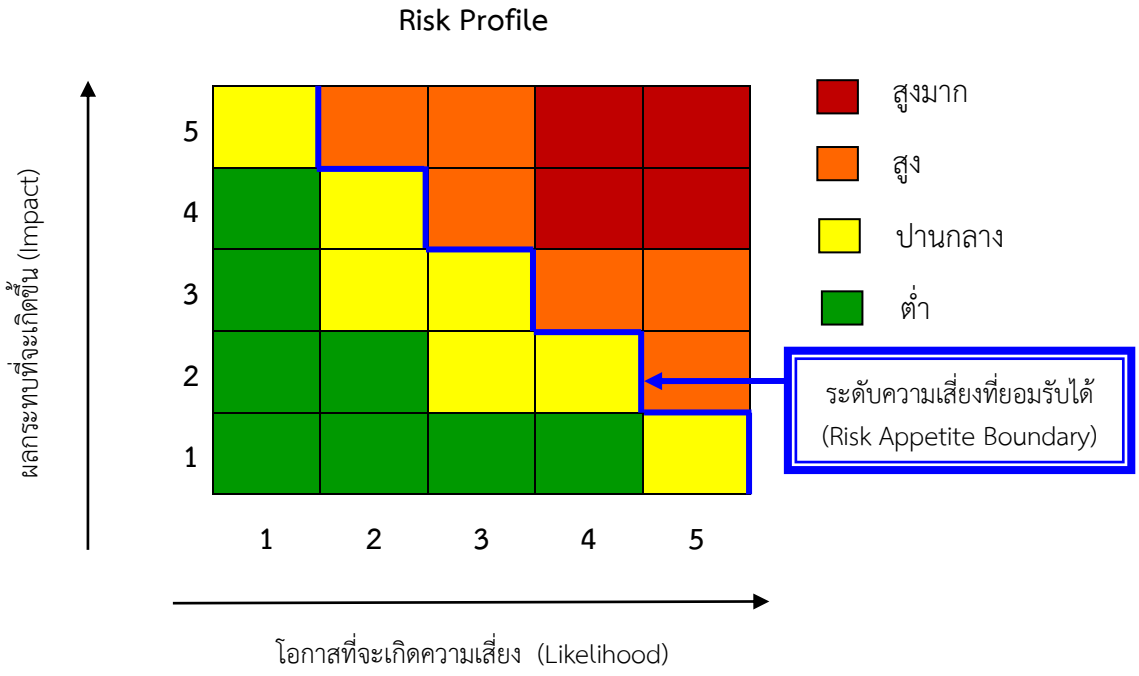
ตารางระดับของความเสี่ยง (Degree of Risk)



1) **การประเมินโอกาสและผลกระทบของความเสี่ยง** เป็นการนำความเสี่ยงและปัจจัยเสี่ยงแต่ละปัจจัยที่ระบุไว้มาประเมินโอกาสที่จะเกิดเหตุการณ์ความเสี่ยงต่างๆ และประเมินระดับความรุนแรงหรือมูลค่า ความเสียหายจากความเสี่ยง เพื่อให้เห็นถึงระดับของความเสี่ยงที่แตกต่างกัน ทำให้สามารถกำหนด ควบคุมความเสี่ยงได้อย่างเหมาะสม ซึ่งจะช่วยให้หน่วยงานสามารถวางแผนและจัดสรรทรัพยากรได้อย่างถูกต้องภายใต้งบประมาณ กำลังคน หรือเวลาที่มีจำกัด โดยอาศัยเกณฑ์มาตรฐานที่กำหนดไว้ข้างต้น ซึ่งมีขั้นตอนดำเนินการ ดังนี้
   - พิจารณาโอกาสและความถี่ในการเกิดเหตุการณ์ต่างๆ ว่ามีโอกาสและความถี่ที่จะเกิดนั้นมากน้อยเพียงใด ตามเกณฑ์มาตรฐานที่กำหนด
   - พิจารณาความรุนแรงของผลกระทบของความเสี่ยงที่มีผลต่อองค์กรหรือหน่วยงานว่ามีระดับความรุนแรง หรือมีความเสียหายเพียงใดตามเกณฑ์มาตรฐานที่กำหนด
2) **การวิเคราะห์ระดับความเสี่ยง** เมื่อพิจารณาโอกาสและความถี่ที่จะเกิดเหตุการณ์และความรุนแรงของผลกระทบของแต่ละปัจจัยเสี่ยง แล้วให้นำผลที่ได้มาพิจารณาความสัมพันธ์ระหว่างโอกาสที่จะเกิดความเสี่ยง และผลกระทบของความเสี่ยงต่อองค์กรหรือหน่วยงานว่าก่อให้เกิดระดับของความเสี่ยงในระดับใด
3) **การจัดลำดับความเสี่ยง** เมื่อได้ค่าระดับความเสี่ยงแล้ว จะนำมาจัดลำดับความรุนแรงของความเสี่ยงที่มีผลต่อองค์กร เพื่อพิจารณากำหนดกิจกรรมการควบคุมในแต่ละสาเหตุของความเสี่ยงที่สำคัญให้เหมาะสม โดยพิจารณาจากระดับของความเสี่ยงที่เกิดจากความสัมพันธ์ระหว่างโอกาสที่จะเกิดความเสี่ยง และผลกระทบของความเสี่ยงที่ประเมินได้ตามตารางการประเมินความเสี่ยง โดยจัดเรียงตามลำดับ จากระดับสูงมาก สูง ปานกลาง ต่ำ และเลือกความเสี่ยงที่มีระดับสูงมากและสูง มาจัดทำแผนการบริหารความเสี่ยงในขั้นตอนต่อไป

ในการประเมินความเสี่ยงจะต้องมีการกำหนด แผนภูมิความเสี่ยง (Risk Profile) ที่ได้จากการพิจารณาจัดระดับความสำคัญของความเสี่ยงจากโอกาสที่จะเกิดความเสี่ยง (Likelihood) และผลกระทบที่เกิดขึ้น (Impact) และขอบเขตของระดับความเสี่ยงที่สามารถยอมรับได้ (Risk Appetite Boundary) โดยระดับความเสี่ยง = โอกาสในการเกิดเหตุการณ์ต่างๆ X ความรุนแรงของเหตุการณ์ต่างๆ (Likelihood X Impact) ซึ่งจัดแบ่งเป็น 4 ระดับ สามารถแสดงเป็น Risk Profile แบ่งพื้นที่เป็น 4 ส่วน (4 Quadrant) ซึ่งใช้เกณฑ์ในการจัดแบ่ง ดังนี้

- ระดับความเสี่ยงต่ำ (Low) คะแนนระดับความเสี่ยง 1-4 คะแนน ยอมรับความเสี่ยงกำหนดเป็นสีเขียว ( )
- ระดับความเสี่ยงปานกลาง (Medium) คะแนนระดับความเสี่ยง 5-9 คะแนน ยอมรับความเสี่ยงแต่มีมาตรการควบคุม กำหนดเป็น สีเหลือง ( )
- ระดับความเสี่ยงสูง (High) คะแนนระดับความเสี่ยง 10-15 คะแนน มีแผนลดความเสี่ยง กำหนดเป็นสีส้ม ( )
- ระดับความเสี่ยงสูงมาก (Extreme) คะแนนระดับความเสี่ยง 16-25 คะแนน มีแผนลดและประเมินซ้ำหรือถ่ายโอนความเสี่ยง กำหนดเป็น สีแดง ( )



ขั้นตอนที่ 4 แนวทางการตอบสนองความเสี่ยง

การกำหนดแนวทางการตอบสนองความเสี่ยงมุ่งเน้นให้องค์กรสามารถบริหารความเสี่ยงให้อยู่ในระดับ ที่ยอมรับได้โดยการกำหนดแนวทางการตอบสนองความเสี่ยงสามารถทำได้หลายวิธี และสามารถปรับเปลี่ยนให้เหมาะสมกับสถานการณ์ ขึ้นอยู่กับดุลยพินิจของผู้รับผิดชอบ แต่อย่างไรก็ตาม แนวทางการบริหารจัดการความเสี่ยงต้องคุ้มค่ากับการลดระดับผลกระทบความเสี่ยงทางเลือกหรือกลยุทธ์ในการจัดการความเสี่ยงแบ่งได้ 4 แนวทางหลัก คือ

1) **การยอมรับ (Take, Accept)** หมายถึง การที่ความเสี่ยงนั้นสามารถยอมรับได้ภายใต้การควบคุมที่มีอยู่ในปัจจุบัน ซึ่งไม่ต้องดำเนินการใดๆ เช่น กรณีที่มีความเสี่ยงในระดับไม่รุนแรงและไม่คุ้มค่าที่จะดำเนินการใดๆ ให้ขออนุมัติหลักการรับความเสี่ยงไว้และไม่ดำเนินการใดๆ
2) **การลด/ควบคุม (Reduction)** หมายถึง เป็นการปรับปรุงระบบการทำงานหรือการออกแบบวิธีการทำงานใหม่ เพื่อลดโอกาสที่จะเกิด หรือลดผลกระทบให้อยู่ในระดับที่องค์กรยอมรับได้
3) **การยกเลิก (Terminate) หรือหลีกเสี่ยง (Avoid)** คือ ความเสี่ยงที่ไม่สามารถยอมรับและต้องจัดการให้ความเสี่ยงนั้นไปอยู่นอกเงื่อนไขการดำเนินงาน โดยมีวิธีการจัดการความเสี่ยงในกลุ่มนี้ เช่น การหยุดดำเนินงานหรือกิจกรรมที่ก่อให้เกิดความเสี่ยงนั้น การเปลี่ยนแปลงวัตถุประสงค์ในการดำเนินงาน การลดขนาดของงานที่จะดำเนินการหรือกิจกรรมลง เป็นต้น
4) **การถ่ายโอนความเสี่ยง (Transfer) หรือแบ่ง (Share)** คือ ความเสี่ยงที่สามารถโอนไปให้ผู้อื่นได้ เช่น การทำประกันภัย/ประกันทรัพย์สินกับบริษัทประกัน การจ้างบุคคลภายนอกหรือการจ้างบริษัทภายนอกมาจัดการในงานบางอย่างแทน เช่น งานรักษาความปลอดภัย เป็นต้น

ขั้นตอนที่ 5 กิจกรรมการบริหารความเสี่ยง (Control Activities)

เมื่อได้ประเมินความเสี่ยงและกำหนดกลยุทธ์ในการจัดการความเสี่ยงแล้วจึงดำเนินการกำหนดกิจกรรม หรือมาตรการในการจัดการความเสี่ยงให้หมดไป หรือลดลงในระดับที่ยอมรับกิจกรรมเดิมที่เคยปฏิบัติอยู่แล้ว แต่ไม่สามารถควบคุมความเสี่ยงได้ นอกจากนั้นยังต้องกำหนดระยะเวลาที่ใช้ในการดำเนินการแต่ละกิจกรรม ตลอดจนหน่วยงานผู้รับผิดชอบในแผนบริหารความเสี่ยงขององค์กรได้ โดยกิจกรรมที่กำหนด ต้องเป็นกิจกรรมที่หน่วยงานยังไม่เคยปฏิบัติหรือเป็นกิจกรรมที่กำหนดเพิ่มเติม

ขั้นตอนที่ 6 ข้อมูลและการสื่อสารด้านบริหารความเสี่ยง (Information and Communication)

การสื่อสารถือได้ว่าเป็นหัวใจของการบริหารความเสี่ยงในทุกๆ ขั้นตอนมีวัตถุประสงค์เพื่อต้องการให้ทุกฝ่ายที่เกี่ยวข้องได้รับความเข้าใจที่ตรงกันอย่างทั่วถึง โดยมีการเปิดช่องทางการสื่อสารข้อมูลด้านการบริหารความเสี่ยงให้กับผู้บริหาร คณะทำงาน และบุคลากรของหน่วยงานได้เข้าถึง และรับทราบข้อมูลด้านการบริหารความเสี่ยงให้กับผู้บริหาร คณะทำงาน และบุคลากรของหน่วยงานได้เข้าถึงและทราบข้อมูลผ่านช่องทางต่างๆ เช่น ระบบอินทราเน็ต หนังสือเวียน การประชุมชี้แจงโดยผู้บริหาร หรือการฝึกอบรม เป็นต้น

ขั้นตอนที่ 7 การติดตาม และเฝ้าระวังความเสี่ยงต่างๆ (Monitoring)

การติดตามและเฝ้าระวังความเสี่ยงโดยการกำหนดให้มีการติดตามและประเมินผล ว่าแต่ละหน่วยงานมีการประเมินประสิทธิผลของการจัดการความเสี่ยงที่กำหนดไว้อย่างต่อเนื่อง และสม่ำเสมอ เพื่อให้เกิดความ มั่นใจว่ามาตรการในการปรับปรุงความเสี่ยงที่วางไว้เพียงพอ เหมาะสม มีประสิทธิภาพ ประสิทธิผล และมีการปฏิบัติจริงสามารถลด หรือป้องกันความเสี่ยงที่อาจเกิดขึ้น

ตารางการประมาณความเสี่ยง (Risk estimation)

SIMPLE	ความเสี่ยง	โอกาสที่จะเกิด	ความรุนแรง
Personnel Safety Goals **S :** Security and Privacy of Information	GPS101 : เกิดอุบัติการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ทำให้ข้อมูลความลับของสถานพยาบาลรั่วไหล (Confidentiality Failure)	1	5
	GPS102 : เกิดอุบัติการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ทำให้ข้อมูลสารสนเทศของสถานพยาบาลถูกแก้ไข/ลบ/เพิ่มเติม/ทำให้เสียหายหรือสูญหายโดยมิชอบ (Integrity Failure)	1	5
	GPS103 : เกิดอุบัติการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ทำให้ระบบสารสนเทศของสถานพยาบาลขัดข้อง/ใช้การไม่ได้/ทำงานช้าหรือไม่ปกติ (Availability Failure)	1	5
	GPS104 : เกิดอุบัติการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ทำให้เกิดความเสียหายต่อข้อมูลหรือระบบสารสนเทศของสถานพยาบาลมากกว่าหนึ่งด้าน (Multiple Failures) ระหว่าง Confidentiality Failure, Integrity Failure และ Availability Failure	1	5
	GPS105 : เกิดอุบัติการณ์การละเมิดความเป็นส่วนตัว (Privacy) ของข้อมูลส่วนบุคคลของบุคลากรหรือนักศึกษาของสถานพยาบาล ที่ไม่ใช่อุบัติการณ์ด้านความมั่นคงปลอดภัยไซเบอร์	2	4
	GPS106 : เกิดอุบัติการณ์ความละเมิดความเป็นส่วนตัว (Privacy) ของข้อมูลส่วนบุคคลของผู้ป่วย/ผู้รับบริการหรือบุคคลภายนอก ที่ไม่ใช่อุบัติการณ์ด้านความมั่นคงปลอดภัยไซเบอร์	2	4
	GPS201 : บุคลากรถูกกล่าวถึงหรือวิพากษ์วิจารณ์ในทางลบบนสื่อสังคมออนไลน์หรือสื่อสาธารณะที่เกี่ยวข้องกับการปฏิบัติหน้าที่	2	3
	GPS202 : บุคลากรถูกกล่าวถึงหรือวิพากษ์วิจารณ์ในทางลบบนสื่อสังคมออนไลน์หรือสื่อสาธารณะที่ไม่ได้เกี่ยวข้องกับการปฏิบัติหน้าที่	2	3
	GPS203 : บุคลากรใช้สื่อสังคมออนไลน์ไม่เหมาะสมเกิดผลกระทบทางลบต่อตนเอง บุคลากรคนอื่น สถานพยาบาลผู้ป่วย/ผู้รับบริการ หรือบุคคลภายนอก	2	4
	GPS204 : เกิดอุบัติการณ์ที่ส่งผลกระทบทางลบต่อสถานพยาบาลบนสื่อสังคมออนไลน์ เช่น Drama, Fake News แต่ไม่ได้เกิดจากบุคลากร และไม่กระทบบุคลากรคนใดคนหนึ่งโดยตรง	2	4

SIMPLE	ความเสี่ยง	โอกาสที่จะเกิด	ความรุนแรง
Organization Safety Goals **I :** Information Technology & Communication, Internal control & Inventory	GOI101 : เกิดปัญหาด้าน Hardware เช่น ไม่มีแผนบริหารจัดการ/ไม่เพียงพอ/ไม่พร้อมใช้/ใช้ไม่ตรงวัตถุประสงค์/ใช้ผิดวิธี - เทคนิค	2	3
	GOI102 : เกิดปัญหาด้าน Network & Security เช่น ไม่พร้อมใช้/ระบบล่ม/ มีการเข้าถึงโดยผู้ไม่มีสิทธิ์	2	5
	GOI103 : เกิดปัญหาด้าน Software เช่น ไม่เข้ากับ hardware/ไม่พร้อมใช้/ไม่ตอบสนองความต้องการ/ใช้ผิดวิธี-เทคนิค	2	3
	GOI104 : เกิดปัญหาด้าน User & IT Team เช่น ไม่มอบหมายผู้รับผิดชอบ/ไม่พร้อม/ไม่ครอบคลุมบทบาทหน้าที่/ขาดความรู้และทักษะ	2	3
	GOI105 : เกิดปัญหาด้านข้อมูล สารสนเทศ เช่น ไม่ถูกต้อง/ไม่ครบถ้วน/ไม่น่าเชื่อถือ/ไม่เป็นปัจจุบัน	5	3
	GOI106 : เกิดปัญหาด้านระบบ/กระบวนการสื่อสาร เช่น ไม่มีแผน/วิธีการหรือช่องทางการสื่อสาร, ไม่สื่อสารหรือสื่อสารไม่ต่อเนื่อง/ไม่ครบถ้วน, ขาดการติดตามประเมินผลการสื่อสาร	2	2
	GOI201 : เกิดปัญหาด้านการควบคุมทรัพย์สิน เช่น ไม่กำหนดระเบียบ/ผู้รับผิดชอบ, ไม่มีทะเบียนคุม/เอกสารหลักฐานกำกับ, ขาดการตรวจสอบหรือสอบทาน	2	3
	GOI202 : เกิดปัญหาด้านระบบบริหารการพัสดุ เช่น ไม่กำหนดระเบียบ/แผนความต้องการและการจัดหา,ไม่มีทะเบียนคุม/การตรวจรับ/การบำรุงรักษา,ขาดการควบคุมการแจกจ่าย/การจำหน่าย	2	3
	GOI203 : เกิดปัญหาด้านการควบคุมการใช้ทรัพยากร เช่น จัดสรรไม่เหมาะสม/ใช้ไม่คุ้ม-ไม่ถูกตามมาตรฐาน/บุคลากรไม่ปฏิบัติตามข้อกำหนด-ขาดทักษะการใช้	2	3

3. การประเมินค่าความเสี่ยง (Risk evaluation)

การประเมินค่าความเสี่ยง จะพิจารณาจากปัจจัยจากขั้นตอนที่ผ่านมาได้แก่ โอกาสที่ภัยคุกคามที่เกิดขึ้นทำให้ระบบขาดความมั่นคง ระดับผลกระทบหรือความรุนแรงของภัยคุกคามที่มีต่อระบบและประสิทธิภาพของแผนการควบคุมความปลอดภัยของระบบ การวัดระดับความเสี่ยงมีการกำหนดแผนภูมิความเสี่ยง ที่ได้จากการพิจารณาจัดระดับความสำคัญของความเสี่ยงจากโอกาสที่จะเกิดความเสี่ยงและผลกระทบที่เกิดขึ้น และขอบเขตของระดับความเสี่ยงที่สามารถยอมรับได้

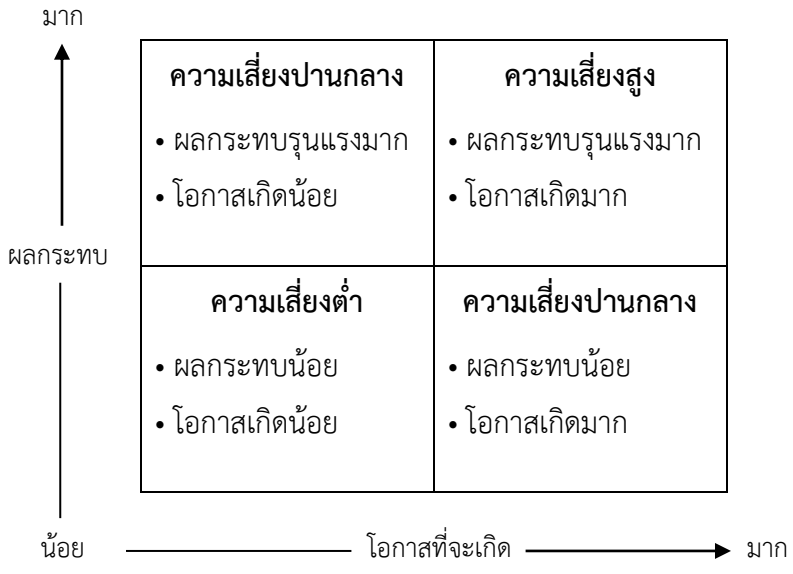
ระดับความเสี่ยง = โอกาสที่จะเกิดหรือความถี่ (P) x ความรุนแรงหรือผลกระทบ (I)

เกณฑ์ในการจัด แบ่งดังนี้

ระดับคะแนนความเสี่ยง	สัญลักษณ์	จัดระดับความเสี่ยง	กลยุทธ์ในการจัดการความเสี่ยง	พื้นที่สี
1 - 4	L	ต่ำ	ยอมรับความเสี่ยง	เขียว
5 - 9	M	ปานกลาง	ยอมรับความเสี่ยง (มีมาตรการ)	เหลือง
10 - 15	H	สูง	ควบคุมความเสี่ยง (มีแผนควบคุม)	ส้ม
16 - 25	HH	สูงมาก	ถ่ายโอนความเสี่ยง	แดง

3.1 แผนภูมิความเสี่ยง (Risk Map)

การวัดระดับความเสี่ยง



3.2 การประเมินความเสี่ยง

การวิเคราะห์ความเสี่ยงจากการวิเคราะห์ความเสี่ยงด้านสารสนเทศ สามารถแยกประเภทอุบัติการณ์ความเสี่ยงหลัก เป็น 2 ประเภท และ 4 ประเภทย่อย ดังนี้

1) รายการอุบัติการณ์ความเสี่ยงในกลุ่มอุบัติการณ์ความเสี่ยงทั่วไป (General Risk Incident:G) หมวดอุบัติการณ์ความเสี่ยง Personnel Safety Goals: P

ประเภทอุบัติการณ์ความเสี่ยง S: Social Media and Communication มี 2 ประเภทย่อย ได้แก่

S1 : Security and Privacy of Information (ความปลอดภัยและความเป็นส่วนตัวของข้อมูล)

S2 : Social Media and Communication Professionalism (ความเป็นมืออาชีพด้านโซเชียลมีเดียและการสื่อสาร)

ลำดับ	รหัสอุบัติการณ์	ชื่ออุบัติการณ์ความเสี่ยง	SIMPER
1	GPS101	เกิดอุบัติการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ทำให้ข้อมูลความลับของสถานพยาบาลรั่วไหล (Confidentiality Failure)	S1
2	GPS102	เกิดอุบัติการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ทำให้ข้อมูลสารสนเทศของสถานพยาบาลถูกแก้ไข/ลบ/เพิ่มเติม/ทำให้เสียหายหรือสูญหายโดยมิชอบ (Integrity Failure)	S1
3	GPS103	เกิดอุบัติการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ทำให้ระบบสารสนเทศของสถานพยาบาลขัดข้อง/ใช้การไม่ได้/ทำงานช้าหรือไม่ปกติ (Availability Failure)	S1
4	GPS104	เกิดอุบัติการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ทำให้เกิดความเสียหายต่อข้อมูลหรือระบบสารสนเทศของสถานพยาบาลมากกว่าหนึ่งด้าน (Multiple Failures) ระหว่าง Confidentiality Failure, Integrity Failure และ Availability Failure	S1
5	GPS105	เกิดอุบัติการณ์การละเมิดความเป็นส่วนตัว (Privacy) ของข้อมูลส่วนบุคคลของบุคลากรหรือนักศึกษาของสถานพยาบาล ที่ไม่ใช่อุบัติการณ์ด้านความมั่นคงปลอดภัยไซเบอร์	S1
6	GPS106	เกิดอุบัติการณ์ความละเมิดความเป็นส่วนตัว (Privacy) ของข้อมูลส่วนบุคคลของผู้ป่วย/ผู้รับบริการ หรือบุคคลภายนอก ที่ไม่ใช่อุบัติการณ์ด้านความมั่นคงปลอดภัยไซเบอร์	S1
7	GPS201	บุคลากรถูกกล่าวถึงหรือวิพากษ์วิจารณ์ในทางลบบนสื่อสังคมออนไลน์หรือสื่อสาธารณะที่เกี่ยวข้องกับการปฏิบัติหน้าที่	S2
8	GPS202	บุคลากรถูกกล่าวถึงหรือวิพากษ์วิจารณ์ในทางลบบนสื่อสังคมออนไลน์หรือสื่อสาธารณะที่ไม่ได้เกี่ยวข้องกับการปฏิบัติหน้าที่	S2
9	GPS203	บุคลากรใช้สื่อสังคมออนไลน์ไม่เหมาะสม เกิดผลกระทบทางลบต่อตนเอง บุคลากรคนอื่น สถานพยาบาล ผู้ป่วย/ผู้รับบริการ หรือบุคคลภายนอก	S2
10	GPS204	เกิดอุบัติการณ์ที่ส่งผลกระทบทางลบต่อสถานพยาบาลบนสื่อสังคมออนไลน์ เช่น Drama, Fake News แต่ไม่ได้เกิดจากบุคลากร และไม่กระทบบุคลากรคนใดคนหนึ่งโดยตรง	S2

2) รายการอุบัติการณ์ความเสี่ยงในกลุ่มอุบัติการณ์ความเสี่ยงทั่วไป (General Risk Incident:G) หมวดอุบัติการณ์ความเสี่ยง Organization Safety Goals: O

ประเภทอุบัติการณ์ความเสี่ยง I: Information Technology & Communication, Internal control & Inventory มี 2 ประเภทย่อย ได้แก่

I1 : Information Technology & Communication (เทคโนโลยีสารสนเทศและการสื่อสาร)

I2 : Internal Control & Inventory (การควบคุมภายในและสินค้าคงคลัง)

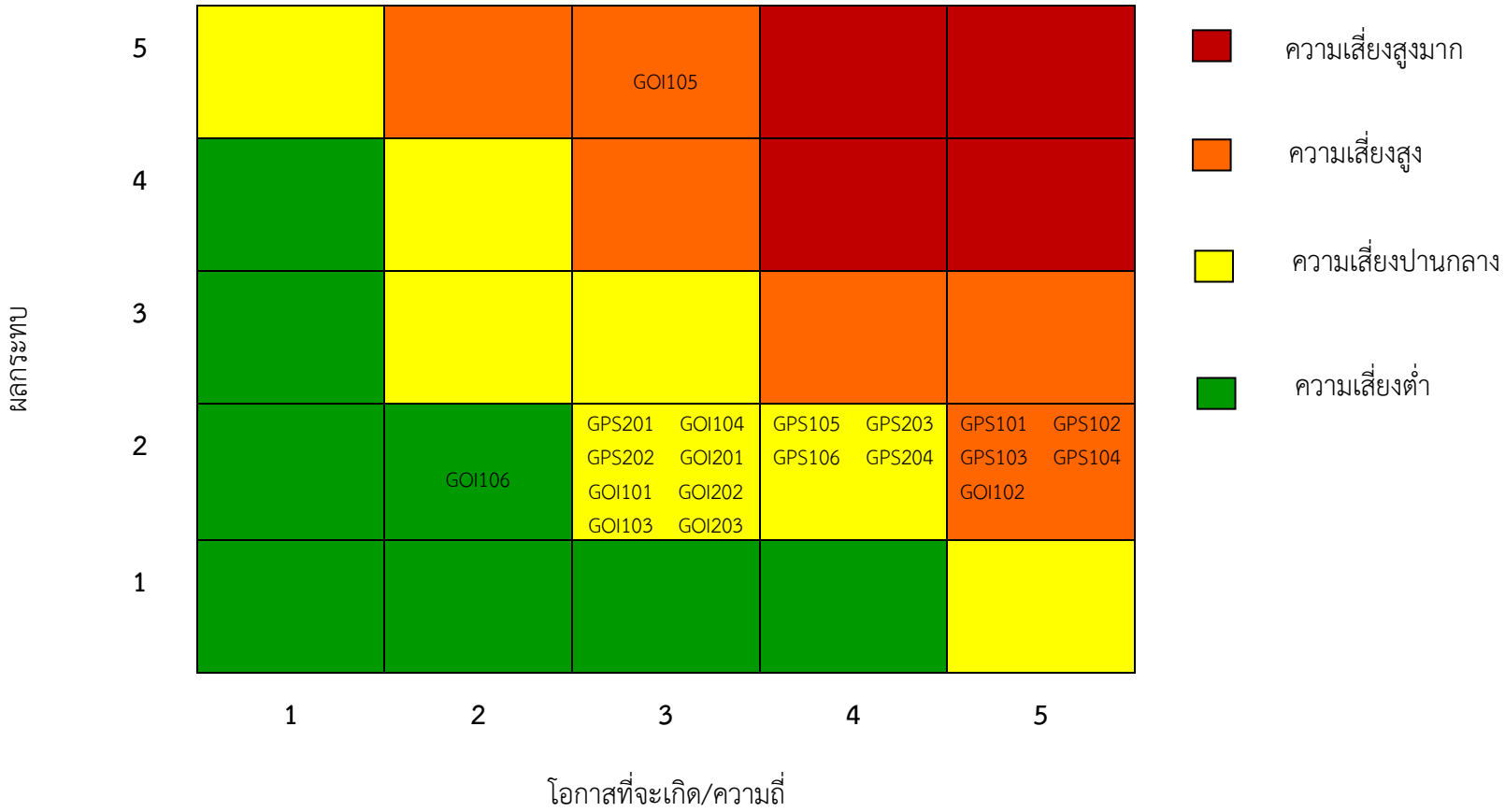
ลำดับ	รหัสอุบัติการณ์	ชื่ออุบัติการณ์ความเสี่ยง	มาตรฐาน
1	GOI101	เกิดปัญหาด้าน Hardware เช่น ไม่มีแผนบริหารจัดการ/ไม่เพียงพอ/ไม่พร้อมใช้/ใช้ไม่ตรงวัตถุประสงค์/ใช้ผิดวิธี - เทคนิค	ตอนที่ I-4/ I1
2	GOI102	เกิดปัญหาด้าน Network & Security เช่น ไม่พร้อมใช้/ระบบล่ม/มีการเข้าถึงโดยผู้ไม่มีสิทธิ์	ตอนที่ I-4/ I1
3	GOI103	เกิดปัญหาด้าน Software เช่น ไม่เข้ากับ hardware/ไม่พร้อมใช้/ไม่ตอบสนองความต้องการ/ใช้ผิดวิธี-เทคนิค	ตอนที่ I-4/ I1
4	GOI104	เกิดปัญหาด้าน User & IT Team เช่น ไม่มอบหมายผู้รับผิดชอบ/ไม่พร้อม/ไม่ครอบคลุมบทบาทหน้าที่/ขาดความรู้และทักษะ	ตอนที่ I-4/ I1
5	GOI105	เกิดปัญหาด้านข้อมูล สารสนเทศ เช่น ไม่ถูกต้อง/ไม่ครบถ้วน/ไม่น่าเชื่อถือ/ไม่เป็นปัจจุบัน	ตอนที่ I-4/ I1
6	GOI106	เกิดปัญหาด้านระบบ/กระบวนการสื่อสาร เช่น ไม่มีแผน/วิธีการหรือช่องทางการสื่อสาร, ไม่สื่อสารหรือสื่อสารไม่ต่อเนื่อง/ไม่ครบถ้วน, ขาดการติดตามประเมินผลการสื่อสาร	ตอนที่ I-3/ I1
7	GOI201	เกิดปัญหาด้านการควบคุมทรัพย์สิน เช่น ไม่กำหนดระเบียบ/ผู้รับผิดชอบ, ไม่มีทะเบียนคุม/เอกสารหลักฐานกำกับ, ขาดการตรวจสอบหรือสอบทาน	ตอนที่ I-1/ I2
8	GOI202	เกิดปัญหาด้านระบบบริหารการพัสดุ เช่น ไม่กำหนดระเบียบ/แผนความต้องการและการจัดหา,ไม่มีทะเบียนคุม/การตรวจรับ/การบำรุงรักษา,ขาดการควบคุมการแจกจ่าย/การจำหน่าย	ตอนที่ I-1/ I2
9	GOI203	เกิดปัญหาด้านการควบคุมการใช้ทรัพยากร เช่น จัดสรรไม่เหมาะสม/ใช้ไม่คุ้ม-ไม่ถูกตามมาตรฐาน/บุคลากรไม่ปฏิบัติตามข้อกำหนด-ขาดทักษะการใช้	ตอนที่ II-3/ I2

ตารางสรุปผลการประเมินค่าความเสี่ยง (Risk Evaluation)

ประเภทอุบัติการณ์ความเสี่ยง	รหัสอุบัติการณ์	ชื่ออุบัติการณ์	โอกาส/ความถี่	ความรุนแรง	ระดับคะแนน
S1 : Security and Privacy of Information (ความปลอดภัยและความเป็นส่วนตัวของข้อมูล)	GPS101	เกิดอุบัติการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ทำให้ข้อมูลความลับของสถานพยาบาลรั่วไหล (Confidentiality Failure)	2	5	10
	GPS102	เกิดอุบัติการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ทำให้ข้อมูลสารสนเทศของสถานพยาบาลถูกแก้ไข/ลบ/เพิ่มเติม/ทำให้เสียหายหรือสูญหายโดยมิชอบ (Integrity Failure)	2	5	10
	GPS103	เกิดอุบัติการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ทำให้ระบบสารสนเทศของสถานพยาบาลขัดข้อง/ใช้การไม่ได้/ทำงานช้าหรือไม่ปกติ (Availability Failure)	2	5	10
	GPS104	เกิดอุบัติการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ทำให้เกิดความเสียหายต่อข้อมูลหรือระบบสารสนเทศของสถานพยาบาลมากกว่าหนึ่งด้าน (Multiple Failures) ระหว่าง Confidentiality Failure, Integrity Failure และ Availability Failure	2	5	10
	GPS105	เกิดอุบัติการณ์การละเมิดความเป็นส่วนตัว (Privacy) ของข้อมูลส่วนบุคคลของบุคลากรหรือนักศึกษาของสถานพยาบาล ที่ไม่ใช่อุบัติการณ์ด้านความมั่นคงปลอดภัยไซเบอร์	2	4	8
	GPS106	เกิดอุบัติการณ์ความละเมิดความเป็นส่วนตัว (Privacy) ของข้อมูลส่วนบุคคลของผู้ป่วย/ผู้รับบริการ หรือบุคคลภายนอก ที่ไม่ใช่อุบัติการณ์ด้านความมั่นคงปลอดภัยไซเบอร์	2	4	8
S2 : Social Media and Communication Professionalism (ความเป็นมืออาชีพด้านโซเชียล)	GPS201	บุคลากรถูกกล่าวถึงหรือวิพากษ์วิจารณ์ในทางลบบนสื่อสังคมออนไลน์หรือสื่อสาธารณะที่เกี่ยวข้องกับการปฏิบัติหน้าที่	2	3	6
	GPS202	บุคลากรถูกกล่าวถึงหรือวิพากษ์วิจารณ์ในทางลบบนสื่อสังคมออนไลน์หรือสื่อสาธารณะที่ไม่ได้เกี่ยวข้องกับการปฏิบัติหน้าที่	2	3	6
	GPS203	บุคลากรใช้สื่อสังคมออนไลน์ไม่เหมาะสม เกิดผลกระทบทางลบต่อตนเอง บุคลากรคนอื่น สถานพยาบาล ผู้ป่วย/ผู้รับบริการ หรือบุคคลภายนอก	2	4	8
	GPS204	เกิดอุบัติการณ์ที่ส่งผลกระทบทางลบต่อสถานพยาบาลบนสื่อสังคมออนไลน์ เช่น Drama, Fake News แต่ไม่ได้เกิดจากบุคลากร และไม่กระทบบุคลากรคนใดคนหนึ่งโดยตรง	2	4	8

ประเภทอุบัติการณ์ความเสี่ยง	รหัสอุบัติการณ์	ชื่ออุบัติการณ์	โอกาส/ความถี่	ความรุนแรง	ระดับคะแนน
I1 : Information Technology & Communication (เทคโนโลยีสารสนเทศและการสื่อสาร)	GOI101	เกิดปัญหาด้าน Hardware เช่น ไม่มีแผนบริหารจัดการ/ ไม่เพียงพอ/ไม่พร้อมใช้/ใช้ไม่ตรงวัตถุประสงค์/ใช้ผิดวิธี - เทคนิค	2	3	6
	GOI102	เกิดปัญหาด้าน Network & Security เช่น ไม่พร้อมใช้/ระบบล่ม/มีการเข้าถึงโดยผู้ไม่มีสิทธิ์	2	5	10
	GOI103	เกิดปัญหาด้าน Software เช่น ไม่เข้ากับ hardware/ไม่พร้อมใช้/ไม่ตอบสนองความต้องการ/ใช้ผิดวิธี-เทคนิค	2	3	6
	GOI104	เกิดปัญหาด้าน User & IT Team เช่น ไม่มอบหมายผู้รับผิดชอบ/ไม่พร้อม/ไม่ครอบคลุมบทบาทหน้าที่/ขาดความรู้และทักษะ	2	3	6
	GOI105	เกิดปัญหาด้านข้อมูล สารสนเทศ เช่น ไม่ถูกต้อง/ไม่ครบถ้วน/ ไม่น่าเชื่อถือ/ไม่เป็นปัจจุบัน	5	3	15
	GOI106	เกิดปัญหาด้านระบบ/กระบวนการสื่อสาร เช่น ไม่มีแผน/วิธีการหรือช่องทางการสื่อสาร, ไม่สื่อสารหรือสื่อสารไม่ต่อเนื่อง/ ไม่ครบถ้วน, ขาดการติดตามประเมินผลการสื่อสาร	2	2	4
I2 : Internal Control & Inventory (การควบคุมภายในและสินค้าคงคลัง)	GOI201	เกิดปัญหาด้านการควบคุมทรัพย์สิน เช่น ไม่กำหนดระเบียบ/ผู้รับผิดชอบ, ไม่มีทะเบียนคุม/เอกสารหลักฐานกำกับ, ขาดการตรวจสอบหรือสอบทาน	2	3	6
	GOI202	เกิดปัญหาด้านระบบบริหารการพัสดุ เช่น ไม่กำหนดระเบียบ/แผนความต้องการและการจัดหา,ไม่มีทะเบียนคุม/การตรวจรับ/การบำรุงรักษา,ขาดการควบคุมการแจกจ่าย/การจำหน่าย	2	3	6
	GOI203	เกิดปัญหาด้านการควบคุมการใช้ทรัพยากร เช่น จัดสรรไม่เหมาะสม/ใช้ไม่คุ้ม-ไม่ถูกตามมาตรฐาน/บุคลากรไม่ปฏิบัติตามข้อกำหนด-ขาดทักษะการใช้	2	3	6

แผนภูมิความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Risk Map)



4. การจัดการความเสี่ยง (Risk management)

นโยบายของกลุ่มงานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์โรงพยาบาลเมืองจันทร์ระดับความเสี่ยงคงเหลือที่ยอมรับได้ ≤ 5

กำหนดให้ความเสี่ยงที่จำเป็นต้องนำมาดำเนินการจัดการความเสี่ยง คือความเสี่ยงที่มีระดับความเสี่ยงสูงตั้งแต่ 15 ขึ้นไป ส่วนความเสี่ยงที่มีระดับความเสี่ยงต่ำกว่า 15 ถือว่ามีความเสี่ยงค่อนข้างต่ำอาจจะนำมาดำเนินการจัดการความเสี่ยงในแผนบริหารความเสี่ยงหรือไม่ก็ได้

4.1 การยอมรับ (Take, Accept) หมายถึง การที่ความเสี่ยงนั้นสามารถยอมรับได้ภายใต้การควบคุมที่มีอยู่ในปัจจุบันซึ่งไม่ต้องดำเนินการใดๆ เช่น กรณีที่มีความเสี่ยงในระดับไม่รุนแรงและไม่คุ้มค่าที่จะดำเนินการใดๆ ให้ขออนุมัติหลักการรับความเสี่ยงไว้และไม่ดำเนินการใดๆ

4.2 การลด/ควบคุม (Reduction) หมายถึง เป็นการปรับปรุงระบบการทำงานหรือการออกแบบวิธีการทำงานใหม่เพื่อลดโอกาสที่จะเกิดหรือลดผลกระทบให้อยู่ในระดับที่องค์กรยอมรับได้

4.3 การยกเลิก (Terminate) หรือหลีกเลี่ยง (Avoid) คือ ความเสี่ยงที่ไม่สามารถยอมรับและต้องจัดการให้ความเสี่ยงนั้นไปอยู่นอกเงื่อนไขการดำเนินงาน โดยมีวิธีการจัดการความเสี่ยงในกลุ่มนี้ เช่น การหยุดดำเนินงานหรือกิจกรรมที่ก่อให้เกิดความเสี่ยงนั้นการเปลี่ยนแปลงวัตถุประสงค์ในการดำเนินงาน การลดขนาดของงานที่จะดำเนินการหรือกิจกรรมลงเป็นต้น

4.4 การถ่ายโอนความเสี่ยง (Transfer) หรือแบ่ง (Share) คือความเสี่ยงที่สามารถโอนไปให้ผู้อื่นได้ เช่น การทำประกันภัย/ประกันทรัพย์สินกับบริษัทประกัน การจ้างบุคคลภายนอกหรือการจ้างบริษัทภายนอกมาจัดการในงานบางอย่างแทนเช่นงานรักษาความปลอดภัยเป็นต้น

ตารางการจัดการความเสี่ยง (Risk Management)

ลำดับ	รหัสอุบัติการณ์	ชื่ออุบัติการณ์	ค่าระดับความเสี่ยง	กลยุทธ์จัดการความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง
1	GOI105	เกิดปัญหาด้านข้อมูลสารสนเทศ เช่น ไม่ถูกต้อง/ไม่ครบถ้วน/ ไม่น่าเชื่อถือ/ไม่เป็นปัจจุบัน	15	• ควบคุมความเสี่ยง (มีแผนควบคุม)	1. สร้างความตระหนัก การรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ 2. มีการตรวจสอบ กำกับ ติดตาม
2	GPS101	เกิดอุบัติการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ทำให้ข้อมูลความลับของสถานพยาบาลรั่วไหล (Confidentiality Failure)	10	• ควบคุมความเสี่ยง (มีแผนควบคุม)	1. สร้างความตระหนัก การรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ 2. ตรวจสอบระบบคอมพิวเตอร์แม่ข่ายและสำรองฐานข้อมูล 3. ตรวจสอบการทำงานอุปกรณ์เครือข่ายอย่างสม่ำเสมอ
3	GPS102	เกิดอุบัติการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ทำให้ข้อมูลสารสนเทศของสถานพยาบาลถูกแก้ไข/ลบ/เพิ่มเติม/ทำให้เสียหายหรือสูญหายโดยมิชอบ (Integrity Failure)	10	• ควบคุมความเสี่ยง (มีแผนควบคุม)	1. สร้างความตระหนัก การรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ 2. มีการตรวจสอบ กำกับ ติดตาม
4	GPS103	เกิดอุบัติการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ทำให้ระบบสารสนเทศของสถานพยาบาลขัดข้อง/ใช้การไม่ได้/ทำงานช้าหรือไม่ปกติ (Availability Failure)	10	• ควบคุมความเสี่ยง (มีแผนควบคุม)	1. สร้างความตระหนัก การรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ 2. ตรวจสอบการทำงานของระบบเครือข่ายอย่างสม่ำเสมอ

ลำดับ	รหัสอุบัติการณ์	ชื่ออุบัติการณ์	ค่าระดับความเสี่ยง	กลยุทธ์จัดการความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง
5	GPS104	เกิดอุบัติการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ทำให้เกิดความเสียหายต่อข้อมูลหรือระบบสารสนเทศของสถานพยาบาลมากกว่าหนึ่งด้าน (Multiple Failures) ระหว่าง Confidentiality Failure, Integrity Failure และ Availability Failure	10	• ควบคุมความเสี่ยง (มีแผนควบคุม)	1. ตรวจสอบระบบคอมพิวเตอร์แม่ข่ายและสำรองฐานข้อมูล อย่างสม่ำเสมอ 2. สร้างความตระหนัก การรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ
6	GOI102	เกิดปัญหาด้าน Network & Security เช่น ไม่พร้อมใช้/ระบบล่ม/มีการเข้าถึงโดยผู้ไม่มีสิทธิ์	10	• ควบคุมความเสี่ยง (มีแผนควบคุม)	1. ตรวจสอบระบบเครือข่ายสื่อสารหลัก/ผู้ให้บริการอินเทอร์เน็ต 2. ตรวจสอบการทำงานอุปกรณ์เครือข่ายอย่างสม่ำเสมอ 3. ดำเนินการปฏิบัติตามระเบียบปฏิบัติการรักษาความมั่นคงปลอดภัยฯ ในกรณีผู้ใช้งานของหน่วยงานภานใน ลาออก โอน ย้าย หรือสิ้นสุดการจ้าง ให้หน่วยงานแจ้งผู้ดูแลระบบทันทีเพื่อปรับปรุงฐานข้อมูล ผู้มีสิทธิ์เข้าใช้งานให้เป็นปัจจุบัน
7	GPS105	เกิดอุบัติการณ์การละเมิดความเป็นส่วนตัว (Privacy) ของข้อมูลส่วนบุคคลของบุคลากรหรือนักศึกษาของสถานพยาบาล ที่ไม่ใช่อุบัติการณ์ด้านความมั่นคงปลอดภัยไซเบอร์	8	• ยอมรับความเสี่ยง (มีมาตรการ)	1. สร้างความตระหนักในเรื่องของข้อมูลส่วนบุคคลในการพึงรักษาสิทธิในส่วนของข้อมูลส่วนบุคคล 2. กระตุ้นให้เกิดการปฏิบัติตามระเบียบปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศอย่างเคร่งครัด

ลำดับ	รหัสอุบัติการณ์	ชื่ออุบัติการณ์	ค่าระดับความเสี่ยง	กลยุทธ์จัดการความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง
8	GPS106	เกิดอุบัติการณ์ความละเมิดความเป็นส่วนตัว (Privacy) ของข้อมูลส่วนบุคคลของผู้ป่วย/ผู้รับบริการ หรือบุคคลภายนอก ที่ไม่ใช่อุบัติการณ์ด้านความมั่นคงปลอดภัยไซเบอร์	8	• ยอมรับความเสี่ยง (มีมาตรการ)	1. สร้างความตระหนักในเรื่องของข้อมูลส่วนบุคคลในการพึงรักษาสิทธิในส่วนของข้อมูลส่วนบุคคล 2. สร้างความตระหนัก การรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ
9	GPS203	บุคลากรใช้สื่อสังคมออนไลน์ไม่เหมาะสม เกิดผลกระทบทางลบต่อตนเอง บุคลากรคนอื่น สถานพยาบาล ผู้ป่วย/ผู้รับบริการ หรือบุคคลภายนอก	8	• ยอมรับความเสี่ยง (มีมาตรการ)	1. สร้างความตระหนักในเรื่องของข้อมูลส่วนบุคคลในการพึงรักษาสิทธิในส่วนของข้อมูลส่วนบุคคล 2. ดำเนินการปฏิบัติตามระเบียบปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศอย่างจริงจัง
10	GPS204	เกิดอุบัติการณ์ที่ส่งผลกระทบทางลบต่อสถานพยาบาลบนสื่อสังคมออนไลน์ เช่น Drama, Fake News แต่ไม่ได้เกิดจากบุคลากร และไม่กระทบบุคลากรคนใดคนหนึ่งโดยตรง	8	• ยอมรับความเสี่ยง (มีมาตรการ)	1. สร้างความตระหนักในเรื่องของข้อมูลส่วนบุคคลในการพึงรักษาสิทธิในส่วนของข้อมูลส่วนบุคคล 2. สร้างความตระหนัก การรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ
11	GPS201	บุคลากรถูกกล่าวถึงหรือวิพากษ์วิจารณ์ในทางลบบนสื่อสังคมออนไลน์หรือสื่อสาธารณะที่เกี่ยวข้องกับการปฏิบัติหน้าที่	6	• ยอมรับความเสี่ยง (มีมาตรการ)	1. สร้างความตระหนักในเรื่องของข้อมูลส่วนบุคคลในการพึงรักษาสิทธิในส่วนของข้อมูลส่วนบุคคล 2. สร้างความตระหนัก การรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ
12	GPS202	บุคลากรถูกกล่าวถึงหรือวิพากษ์วิจารณ์ในทางลบบนสื่อสังคมออนไลน์หรือสื่อสาธารณะที่ไม่ได้เกี่ยวข้องกับการปฏิบัติหน้าที่	6	• ยอมรับความเสี่ยง (มีมาตรการ)	1. สร้างความตระหนักในเรื่องของข้อมูลส่วนบุคคลในการพึงรักษาสิทธิในส่วนของข้อมูลส่วนบุคคล 2. สร้างความตระหนัก การรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

ลำดับ	รหัสอุบัติการณ์	ชื่ออุบัติการณ์	ค่าระดับความเสี่ยง	กลยุทธ์จัดการความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง
13	GOI101	เกิดปัญหาด้าน Hardware เช่น ไม่มีแผนบริหารจัดการ/ ไม่เพียงพอ/ไม่พร้อมใช้/ใช้ไม่ตรงวัตถุประสงค์/ใช้ผิดวิธี - เทคนิค	6	• ยอมรับความเสี่ยง (มีมาตรการ)	1. จัดหาคอมพิวเตอร์และอุปกรณ์สำรองที่สามารถใช้ทดแทนได้ทันที สามารถปฏิบัติงานได้อย่างต่อเนื่อง 2. ตรวจสอบ บำรุงรักษาคอมพิวเตอร์และอุปกรณ์อย่างสม่ำเสมอ
14	GOI103	เกิดปัญหาด้าน Software เช่น ไม่เข้ากับ hardware/ไม่พร้อมใช้/ไม่ตอบสนองความต้องการ/ใช้ผิดวิธี-เทคนิค	6	• ยอมรับความเสี่ยง (มีมาตรการ)	1. จัดหา Software เตรียมพร้อมไว้สำหรับการใช้งาน
15	GOI104	เกิดปัญหาด้าน User & IT Team เช่น ไม่มอบหมายผู้รับผิดชอบ/ไม่พร้อม/ไม่ครอบคลุมบทบาทหน้าที่/ขาดความรู้และทักษะ	6	• ยอมรับความเสี่ยง (มีมาตรการ)	1. สร้างความตระหนัก การรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ
16	GOI201	เกิดปัญหาด้านการควบคุมทรัพย์สิน เช่น ไม่กำหนดระเบียบ/ผู้รับผิดชอบ, ไม่มีทะเบียนคุม/เอกสารหลักฐานกำกับ,ขาดการตรวจสอบหรือสอบทาน	6	• ยอมรับความเสี่ยง (มีมาตรการ)	1. สร้างความตระหนัก การรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ
17	GOI202	เกิดปัญหาด้านระบบบริหารการพัสดุ เช่น ไม่กำหนดระเบียบ/แผนความต้องการและการจัดหา,ไม่มีทะเบียนคุม/การตรวจรับ/การบำรุงรักษา,ขาดการควบคุมการแจกจ่าย/การจำหน่าย	6	• ยอมรับความเสี่ยง (มีมาตรการ)	1. สร้างความตระหนัก การรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

ลำดับ	รหัสอุบัติการณ์	ชื่ออุบัติการณ์	ค่าระดับความเสี่ยง	กลยุทธ์จัดการความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง
18	GOI203	เกิดปัญหาด้านการควบคุมการใช้ทรัพยากร เช่น จัดสรรไม่เหมาะสม/ใช้ไม่คุ้ม-ไม่ถูกตามมาตรฐาน/บุคลากรไม่ปฏิบัติตามข้อกำหนด-ขาดทักษะการใช้	6	• ยอมรับความเสี่ยง (มีมาตรการ)	1. สร้างความตระหนัก การรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ
19	GOI106	เกิดปัญหาด้านระบบ/กระบวนการสื่อสาร เช่น ไม่มีแผน/วิธีการหรือช่องทางการสื่อสาร, ไม่สื่อสารหรือสื่อสารไม่ต่อเนื่อง/ ไม่ครบถ้วน, ขาดการติดตามประเมินผลการสื่อสาร	4	• ยอมรับความเสี่ยง	1. สร้างความตระหนัก การรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

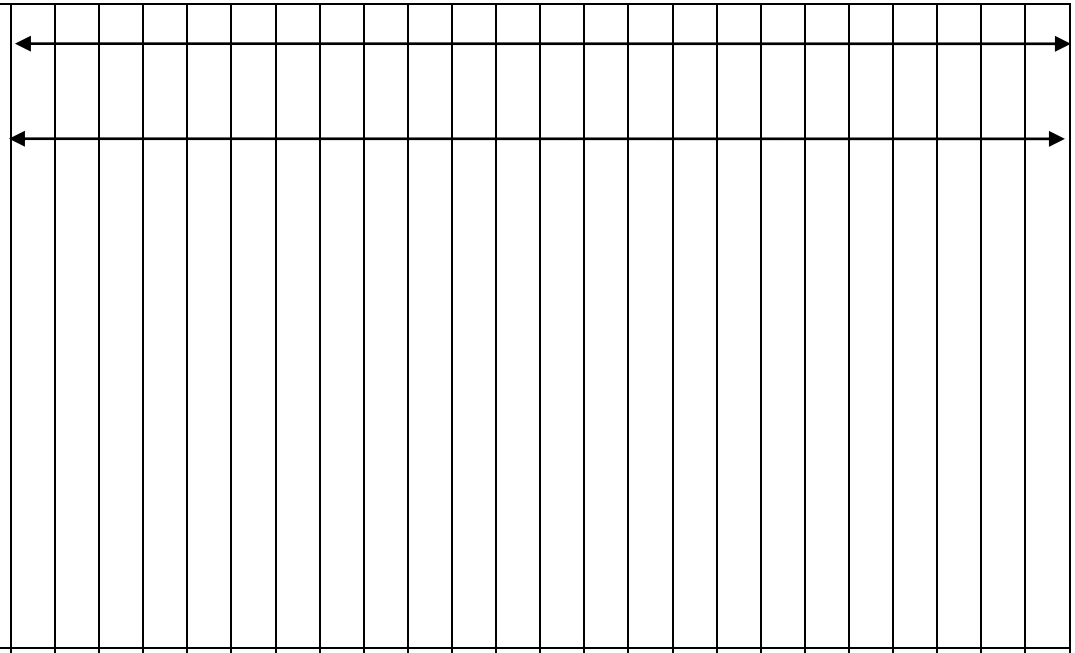
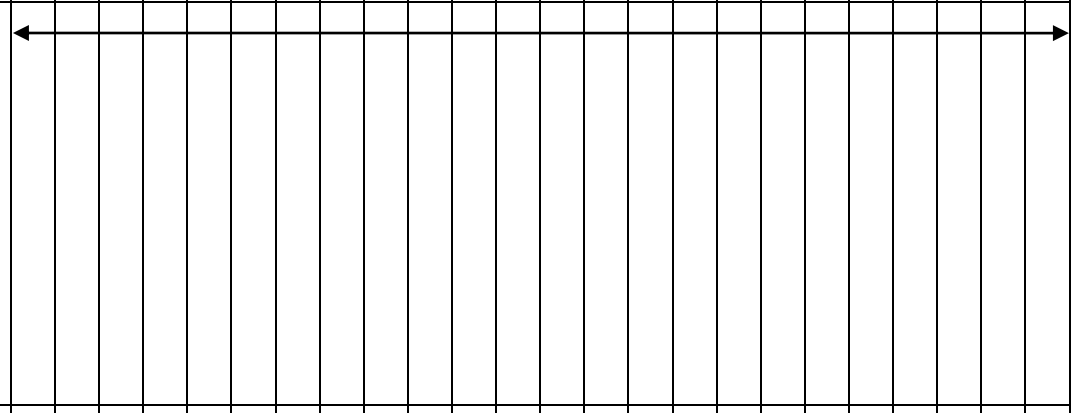
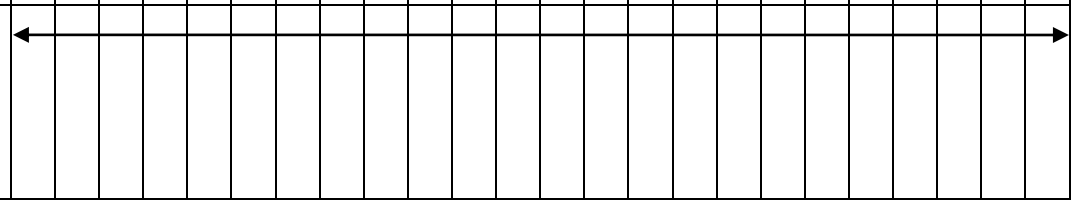
5. แผนปฏิบัติการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

จากการจัดการความเสี่ยง สามารถนำมาจัดทำแผนปฏิบัติบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร โดยมีหน่วยงานรับผิดชอบคืองานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์ โรงพยาบาลเมืองจันทร์ ระยะเวลาดำเนินการระหว่างเดือนตุลาคม 2563 – เดือนตุลาคม 2568

แผนปฏิบัติการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

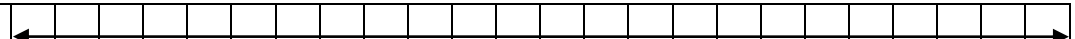
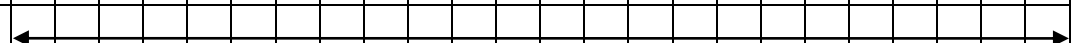
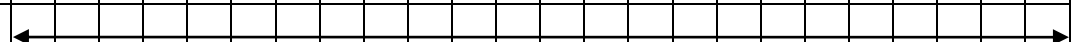
ประเภทความเสี่ยง	แนวทางการควบคุม	ระยะเวลา	ปีงบ 2564				ปีงบ 2565				ปีงบ 2565				ปีงบ 2566				ปีงบ 2567				ปีงบ 2568			
			Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
GOI105 : เกิดปัญหาด้านข้อมูลสารสนเทศ เช่น ไม่ถูกต้อง/ไม่ครบถ้วน/ไม่น่าเชื่อถือ/ไม่เป็นปัจจุบัน	1. มีการตรวจสอบ กำกับติดตาม	1ครั้ง/สัปดาห์	←	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	→
GPS101 : เกิดอุบัติการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ทำให้ข้อมูลความลับของสถานพยาบาลรั่วไหล (Confidentiality Failure)	1. ตรวจสอบระบบคอมพิวเตอร์แม่ข่ายและสำรอง ฐานข้อมูล 2. ตรวจสอบการทำงานอุปกรณ์เครือข่ายอย่างสม่ำเสมอ	1ครั้ง/สัปดาห์ 1ครั้ง/สัปดาห์	←	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	→
GPS102 : เกิดอุบัติการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ทำให้ข้อมูลสารสนเทศของสถานพยาบาลถูกแก้ไข/	1. สร้างความตระหนักการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ	1 ครั้ง/ปี	←	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	→

ลบ/เพิ่มเติม/ทำให้เสียหาย หรือสูญหายโดยมิชอบ (Integrity Failure)	2. มีการตรวจสอบ กำกับติดตาม	1 ครั้ง/สัปดาห์	← →
GPS103 : เกิดอุบัติการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ทำให้ระบบสารสนเทศของสถานพยาบาลขัดข้อง/ใช้การไม่ได้/ทำงานช้าหรือไม่ปกติ (Availability Failure)	1. ตรวจสอบการทำงานของระบบเครือข่ายอย่างสม่ำเสมอ	1 ครั้ง/สัปดาห์	← →
GPS104 : เกิดอุบัติการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ทำให้เกิดความเสียหายต่อข้อมูลหรือระบบสารสนเทศของสถานพยาบาลมากกว่าหนึ่งด้าน (Multiple Failures) ระหว่าง Confidentiality Failure, Integrity Failure และ Availability Failure	1. ตรวจสอบระบบคอมพิวเตอร์แม่ข่ายและสำรองฐานข้อมูลอย่างสม่ำเสมอ 2. สร้างความตระหนักการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ	1 ครั้ง/สัปดาห์ 1 ครั้ง/ปี	← → ← →
GOI102 : เกิดปัญหาด้าน Network & Security เช่น ไม่พร้อมใช้/ระบบล่ม/มี	1. ตรวจสอบระบบเครือข่ายสื่อสารหลัก/ผู้ให้บริการอินเทอร์เน็ต	1ครั้ง/วัน	← →

การเข้าถึงโดยผู้ไม่มีสิทธิ์	2. ตรวจสอบการทำงานอุปกรณ์เครือข่ายอย่างสม่ำเสมอ 3. ดำเนินการปฏิบัติตามระเบียบปฏิบัติการรักษาความมั่นคงปลอดภัยฯ ในกรณีผู้ใช้งานของหน่วยงานภานใน ลาออก โอน ย้าย หรือสิ้นสุดการจ้าง ให้หน่วยงานแจ้งผู้ดูแลระบบทันทีเพื่อปรับปรุงฐานข้อมูล ผู้มีสิทธิ์เข้าใช้งานให้เป็นปัจจุบัน	1ครั้ง/วัน ทุกครั้งที่มีการเปลี่ยนแปลงผู้ใช้งาน	
GPS105 : เกิดอุบัติการณ์การละเมิดความเป็นส่วนตัว (Privacy) ของข้อมูลส่วนบุคคลของบุคลากรหรือนักศึกษาของสถานพยาบาล ที่ไม่ใช่อุบัติการณ์ด้านความมั่นคงปลอดภัยไซเบอร์	1. สร้างความตระหนักในเรื่องของข้อมูลส่วนบุคคลในการพึงรักษาสิทธิในส่วนของข้อมูลส่วนบุคคล 2. สร้างความตระหนักการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ	1 ครั้ง/ปี	
GPS106 : เกิดอุบัติการณ์ความละเมิดความเป็นส่วนตัว (Privacy) ของข้อมูลส่วนบุคคลของ	1. สร้างความตระหนักในเรื่องของข้อมูลส่วนบุคคลในการพึงรักษาสิทธิในส่วนของข้อมูลส่วนบุคคล	1 ครั้ง/ปี	

ผู้ป่วย/ผู้รับบริการ หรือบุคคลภายนอก ที่ไม่ใช่อุบัติการณ์ด้านความมั่นคงปลอดภัยไซเบอร์	2. สร้างความตระหนักการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ																							
GPS203 : บุคลากรใช้สื่อสังคมออนไลน์ไม่เหมาะสม เกิดผลกระทบทางลบต่อตนเอง บุคลากรคนอื่น สถานพยาบาล ผู้ป่วย/ผู้รับบริการ หรือบุคคลภายนอก	1. สร้างความตระหนักในเรื่องของข้อมูลส่วนบุคคลในการพึงรักษาสิทธิในส่วนของข้อมูลส่วนบุคคล 2. สร้างความตระหนักการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ	1 ครั้ง/ปี	←	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	→
GPS204 : เกิดอุบัติการณ์ที่ส่งผลกระทบทางลบต่อสถานพยาบาลบนสื่อสังคมออนไลน์ เช่น Drama, Fake News แต่ไม่ได้เกิดจากบุคลากร และไม่กระทบบุคลากรคนใดคนหนึ่งโดยตรง	1. สร้างความตระหนักในเรื่องของข้อมูลส่วนบุคคลในการพึงรักษาสิทธิในส่วนของข้อมูลส่วนบุคคล 2. สร้างความตระหนักการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ	1 ครั้ง/ปี	←	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	→
GPS201 : บุคลากรถูกกล่าวถึงหรือวิพากษ์วิจารณ์ในทางลบบนสื่อสังคมออนไลน์หรือสื่อสาธารณะ	1. สร้างความตระหนักในเรื่องของข้อมูลส่วนบุคคลในการพึงรักษาสิทธิในส่วนของข้อมูลส่วนบุคคล	1 ครั้ง/ปี	←	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	→

ที่เกี่ยวข้องกับการปฏิบัติหน้าที่	2. สร้างความตระหนักการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ		
GPS202 : บุคลากรถูกกล่าวถึงหรือวิพากษ์วิจารณ์ในทางลบบนสื่อสังคมออนไลน์หรือสื่อสาธารณะที่ไม่ได้เกี่ยวข้องกับการปฏิบัติหน้าที่	1. สร้างความตระหนักในเรื่องของข้อมูลส่วนบุคคลในการพึงรักษาสิทธิในส่วนของข้อมูลส่วนบุคคล 2. สร้างความตระหนักการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ	1 ครั้ง/ปี	← →
GOI101 : เกิดปัญหาด้าน Hardware เช่น ไม่มีแผนบริหารจัดการ/ ไม่เพียงพอ/ไม่พร้อมใช้/ใช้ไม่ตรงวัตถุประสงค์/ใช้ผิดวิธี - เทคนิค	1. จัดหาคอมพิวเตอร์และอุปกรณ์สำรอง ที่สามารถใช้ทดแทนได้ทันที สามารถปฏิบัติงาน ได้อย่างต่อเนื่อง 2. ตรวจสอบ บำรุงรักษาคอมพิวเตอร์และอุปกรณ์อย่างสม่ำเสมอ	1 ครั้ง/ปี 3 เดือน/ครั้ง	← →
GOI103 : เกิดปัญหาด้าน Software เช่น ไม่เข้ากับ hardware/ไม่พร้อมใช้/ไม่ตอบสนองความต้องการ/ใช้ผิดวิธี-เทคนิค	1. จัดหา Software เตรียมพร้อมไว้สำหรับ การใช้งาน	1 ครั้ง/ปี	← →

GOI104 : เกิดปัญหาด้าน User & IT Team เช่น ไม่มอบหมายผู้รับผิดชอบ/ไม่พร้อม/ไม่ครอบคลุมบทบาทหน้าที่/ขาดความรู้และทักษะ	1. สร้างความตระหนัก การรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ	1 ครั้ง/ปี	
GOI201 : เกิดปัญหาด้านการควบคุมทรัพย์สิน เช่น ไม่กำหนดระเบียบ/ผู้รับผิดชอบ, ไม่มีทะเบียนคุม/เอกสารหลักฐานกำกับ, ขาดการตรวจสอบหรือสอบทาน	1. สร้างเครื่องมือในการกำหนดทะเบียนคุม/เอกสารหลักฐานกำกับ	1 ครั้ง/ปี	
GOI202 : เกิดปัญหาด้านระบบบริหารการพัสดุ เช่น ไม่กำหนดระเบียบ/แผนความต้องการและการจัดหา,ไม่มีทะเบียนคุม/การตรวจรับ/การบำรุงรักษา, ขาดการควบคุมการแจกจ่าย/การจำหน่าย	1. สร้างเครื่องมือในการกำหนดทะเบียนคุม/เอกสารหลักฐานกำกับ	1 ครั้ง/ปี	
GOI203 : เกิดปัญหาด้านการควบคุมการใช้ทรัพยากร เช่น จัดสรรไม่	1. สร้างเครื่องมือในการกำหนดทะเบียนคุม/เอกสารหลักฐานกำกับ	1 ครั้ง/ปี	

เหมาะสม/ใช้ไม่คุ้ม-ไม่ถูกตามมาตรฐาน/บุคลากรไม่ปฏิบัติตามข้อกำหนด-ขาดทักษะการใช้																									
GOI106 : เกิดปัญหาด้านระบบ/กระบวนการสื่อสาร เช่น ไม่มีแผน/วิธีการหรือช่องทางการสื่อสาร, ไม่สื่อสารหรือสื่อสารไม่ต่อเนื่อง/ไม่ครบถ้วน, ขาดการติดตามประเมินผลการสื่อสาร	1. จัดทำคู่มือการปฏิบัติงาน กระบวนการการบริการ ระเบียบปฏิบัติ (สำหรับผู้ใช้งาน)	1 ครั้ง/ปี	◄																						►

บทที่ 5 สรุปผลและข้อเสนอแนะ

1. การประเมินปัจจัยเสี่ยง

นโยบายของกลุ่มงานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์ ระดับคามเสี่ยงที่ยอมรับได้ <=5 ความเสี่ยงที่จำเป็นต้องนำมาดำเนินการจัดการความเสี่ยง คือความเสี่ยงที่มีระดับความเสี่ยงสูงตั้งแต่ 10 ส่วนความเสี่ยงในแผนบริหารความเสี่ยงต่ำกว่า 10 ถือว่ามีความเสี่ยงค่อนข้างต่ำอาจจะนำมาดำเนินการจัดการความเสี่ยงในแผนบริหารความเสี่ยงหรือไม่ก็ได้ การดำเนินการจัดการความเสี่ยง กิจกรรมที่ดำเนินการต่อไป

1) สร้างความตระหนักในเรื่องนโยบายและระเบียบปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ โดยจัดทำแผนโครงการกระตุ้นผู้ใช้งานให้ตระหนักในความเสี่ยงของการเปิดเผยข้อมูล หรือแชร์ข้อมูลในสื่อสังคมออนไลน์ทุกชนิด
2) กระตุ้นให้เกิดการปฏิบัติตามนโยบายและระเบียบปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ อย่างเคร่งครัด
3) จัดทำสื่อต่างๆ และเผยแพร่เพื่อให้ความรู้

2. ปัจจัยที่ทำให้ระบบบริหารความเสี่ยงประสบผลสำเร็จ

1) แรงผลักดันจากผู้บริหารหน่วยงานที่ให้ความสนับสนุน
2) เทคโนโลยีสารสนเทศที่ช่วยในการจัดเก็บข้อมูล การส่งถ่ายข้อมูลและการตรวจสอบย้อนกลับได้อย่างรวดเร็ว
3) ความร่วมมือร่วมใจของบุคลากรภายในกลุ่มงานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์ที่จะผลักดันให้การบริหารความเสี่ยงประสบผลสำเร็จ

3. ผลการประเมิน / ข้อสรุป

ผู้บริหารได้สร้างบรรยากาศสภาพแวดล้อมการควบคุมภายในเพื่อให้บุคลากรทุกคนมีทัศนคติที่ดีต่อการควบคุมภายในโดยใช้หลักธรรมาภิบาล ส่งเสริม สนับสนุน และสื่อสารให้ทุกคนเข้าใจขอบเขตหน้าที่ รวมทั้งทักษะในการปฏิบัติงาน กฎ ระเบียบ ข้อบังคับที่เกี่ยวข้อง ตลอดถึงจรรยาบรรณการทำงานของการดูแลผู้ป่วย เพื่อให้การควบคุมภายในหน่วยงานมีประสิทธิผล สามารถปฏิบัติงานตามภารกิจและตามที่ได้มอบหมายได้อย่างมีประสิทธิภาพ

จากการประเมินองค์ประกอบของการควบคุมภายในด้านการประเมินความเสี่ยงพบว่าในภาพรวมมีความเหมาะสมแล้ว แต่ต้องมีการปรับปรุงให้เหมาะสมยิ่งขึ้น ความเสี่ยงอยู่ในระดับที่ยอมรับได้และส่งเสริมให้บุคลากรมีความรู้ความชำนาญในการวิเคราะห์ความเสี่ยง