การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง

(Risk Assessment and Risk Management Strategy Procedure)

โรงพยาบาลค่ายวีรวัฒน์โยธิน

วันที่บังคับใช้: 4 มกราคม 2569

ลงนาม	ผู้เรียบเรียง/จัดทำโดย	ผู้ตรวจทาน/ผู้ทบทวน	ผู้อนุมัติ
ลายเซ็น			
ชื่อ-สกุล	นายนัธทวัฒน์ วสันต์กนกพัชร	ร.อ.ภาราดร บุบผาลัย	พ.อ.วงศ์สรรค์ สิริชีวเกษร
ตำแหน่ง	เจ้าพนักงานเครื่องคอมพิวเตอร์	หัวหน้าเทคโนโลยีสารสนเทศ	ผู้อำนวยการโรงพยาบาลค่ายวีรวัฒน์โยธิน
วัน เดือน ปี	4 มกราคม 2569	4 มกราคม 2569	4 มกราคม 2569

ครั้งที่	วันที่ประกาศใช้	รายละเอียดการแก้ไข
01	4 มกราคม 2569	จัดทำเอกสารครั้งแรกสำหรับโรงพยาบาลค่ายวีรวัฒน์โยธิน เพื่อใช้เป็นแนวทางประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยไซเบอร์

สารบัญ

- 1. วัตถุประสงค์ 3
- 2. ขอบเขต 3
- 3. ความรับผิดชอบในเอกสาร 4
- 4. นิยามและหลักการประเมินความเสี่ยง 4
- 5. ขั้นตอนการประเมินความเสี่ยง 4
- 6. เกณฑ์การประเมินโอกาสและผลกระทบ 6
- 7. การประเมินระดับและการจัดการความเสี่ยง 6
- 8. การติดตาม ทบทวน และรายงานผล 7
- 9. เอกสารอ้างอิง 8
- ภาคผนวก ก แบบฟอร์มทะเบียนความเสี่ยง 9

1. วัตถุประสงค์

เอกสารฉบับนี้จัดทำขึ้นเพื่อกำหนดวิธีการระบุ วิเคราะห์ ประเมิน
และจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยไซเบอร์ของโรงพยาบาลค่ายวีรวัฒน์โยธิน
ให้มีแนวทางปฏิบัติที่ชัดเจน ใช้ซ้ำได้ และตรวจสอบย้อนหลังได้

เป้าหมายสำคัญคือให้ความเสี่ยงที่อาจกระทบต่อการให้บริการผู้ป่วย ระบบงานโรงพยาบาล ข้อมูลสุขภาพ
ข้อมูลส่วนบุคคล และระบบสนับสนุนงานบริหาร อยู่ในระดับที่โรงพยาบาลยอมรับได้
พร้อมมีมาตรการควบคุมที่เหมาะสมกับภารกิจและทรัพยากรของหน่วย

- กำหนดขั้นตอนประเมินความเสี่ยงให้เป็นมาตรฐานเดียวกันทั้งหน่วยงาน
- ช่วยจัดลำดับความสำคัญของทรัพย์สินสารสนเทศและบริการสำคัญ
- กำหนดเกณฑ์ Likelihood และ Impact เพื่อใช้คำนวณระดับความเสี่ยง
- สนับสนุนการจัดทำแผนลดความเสี่ยง การติดตามผล และการรายงานต่อผู้บริหาร
- เชื่อมโยงแนวปฏิบัติกับกฎหมาย มาตรฐาน และกรอบการรักษาความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้อง

2. ขอบเขต

ขอบเขตของเอกสารนี้ครอบคลุมทรัพย์สินสารสนเทศ ระบบเครือข่าย ระบบงานบริการสุขภาพ อุปกรณ์คอมพิวเตอร์
อุปกรณ์สื่อสาร ข้อมูลผู้ป่วย ข้อมูลกำลังพล ข้อมูลการเงิน
และบริการดิจิทัลที่โรงพยาบาลค่ายวีรวัฒน์โยธินใช้ในการปฏิบัติภารกิจ

2.1 การประเมินความเสี่ยงของกลุ่มงาน

ใช้กับกลุ่มงานและหน่วยงานภายในที่มีการใช้งานหรือดูแลทรัพย์สินสารสนเทศ เช่น งานเวชระเบียน งานผู้ป่วยนอก
งานผู้ป่วยใน งานเภสัชกรรม งานการเงิน งานพัสดุ งานเทคโนโลยีสารสนเทศ และหน่วยสนับสนุนอื่น

2.2 การประเมินความเสี่ยงของเครื่องมือและระบบเพื่อการจัดการภายใน

ครอบคลุมระบบงานที่ใช้สนับสนุนการบริหารจัดการ เช่น ระบบสารบรรณ ระบบจัดซื้อจัดจ้าง ระบบบัญชี
ระบบบุคลากร ระบบสำรองข้อมูล และระบบสื่อสารภายใน

2.3 การประเมินความเสี่ยงของโครงการพัฒนาหรือปรับปรุงระบบสารสนเทศ

โครงการใหม่หรือโครงการปรับปรุงระบบเดิมต้องมีการประเมินความเสี่ยงก่อนเริ่มใช้งานจริง
โดยเฉพาะระบบที่เชื่อมต่อเครือข่ายภายนอก เก็บข้อมูลส่วนบุคคลหรือข้อมูลสุขภาพ
หรือมีผลต่อความต่อเนื่องในการให้บริการ

3. ความรับผิดชอบในเอกสาร

บทบาท	หน้าที่หลัก	หลักฐาน/ผลลัพธ์
ผู้อำนวยการโรงพยาบาล	อนุมัตินโยบาย ระดับความเสี่ยงที่ยอมรับได้ และแผนจัดการความเสี่ยงที่มีผลกระทบสูง	บันทึกอนุมัติ/คำสั่ง
คณะกรรมการหรือผู้รับผิดชอบด้านความมั่นคงปลอดภัยไซเบอร์	กำกับ ทบทวน และติดตามสถานะความเสี่ยง รวมถึงเสนอแนะแนวทางควบคุม	รายงานการประชุม/รายงานความเสี่ยง
งานเทคโนโลยีสารสนเทศ	ประสานการประเมิน เก็บทะเบียนทรัพย์สิน ประเมินภัยคุกคาม ช่องโหว่ และจัดทำทะเบียนความเสี่ยง	ทะเบียนทรัพย์สิน/ทะเบียนความเสี่ยง
เจ้าของระบบหรือเจ้าของข้อมูล	ให้ข้อมูลระบบ กระบวนการทำงาน ผลกระทบ และร่วมกำหนดมาตรการควบคุม	แบบประเมิน/แผนแก้ไข

4. นิยามและหลักการประเมินความเสี่ยง

คำสำคัญ	ความหมายในการใช้งาน
ทรัพย์สินสารสนเทศ	ข้อมูล ระบบ โปรแกรม อุปกรณ์ เครือข่าย เอกสาร บุคลากร หรือบริการที่มีคุณค่าต่อภารกิจของโรงพยาบาล
ภัยคุกคาม	เหตุการณ์หรือปัจจัยที่อาจก่อให้เกิดความเสียหาย เช่น มัลแวร์ ไฟฟ้าขัดข้อง บุคคลภายนอกเข้าถึงระบบโดยไม่ได้รับอนุญาต หรือความผิดพลาดของผู้ใช้งาน
ช่องโหว่	จุดอ่อนที่ทำให้ภัยคุกคามเกิดผลกระทบได้ เช่น ระบบไม่ได้อัปเดต รหัสผ่านอ่อน ไม่มีการสำรองข้อมูล หรือไม่มีการแยกสิทธิ์ผู้ใช้งาน
Likelihood	ระดับความเป็นไปได้ที่ภัยคุกคามจะเกิดขึ้นกับช่องโหว่ที่มีอยู่
Impact	ระดับผลกระทบต่อการให้บริการ ความลับ ความถูกต้อง ความพร้อมใช้ ชื่อเสียง และการปฏิบัติตามกฎหมาย
Residual Risk	ความเสี่ยงที่ยังคงเหลือหลังจากดำเนินมาตรการควบคุมแล้ว

5. ขั้นตอนการประเมินความเสี่ยง

ขั้นที่ 1 ระบุลักษณะของทรัพย์สิน

รวบรวมรายการทรัพย์สินสารสนเทศ ระบุเจ้าของทรัพย์สิน ที่ตั้ง การเชื่อมต่อ และความสำคัญต่อภารกิจ

ขั้นที่ 2 ระบุผู้ดูแลและจัดกลุ่มทรัพย์สิน

กำหนดเจ้าของระบบ ผู้ดูแลระบบ ผู้ใช้งานหลัก และจัดกลุ่มตามบริการ เช่น บริการผู้ป่วย ระบบบริหาร ระบบเครือข่าย และระบบสนับสนุน

ขั้นที่ 3 ระบุภัยคุกคามและช่องโหว่

วิเคราะห์ภัยคุกคามที่เกี่ยวข้องกับแต่ละทรัพย์สิน พร้อมช่องโหว่ที่ทำให้เกิดเหตุได้จริง

ขั้นที่ 4 ระบุผลกระทบด้านความมั่นคงปลอดภัย

ประเมินผลต่อความลับ ความถูกต้อง ความพร้อมใช้ การบริการผู้ป่วย ความน่าเชื่อถือ และข้อกำหนดตามกฎหมาย

ขั้นที่ 5 ระบุการควบคุมในปัจจุบัน

บันทึกมาตรการที่มีอยู่ เช่น การสำรองข้อมูล การควบคุมสิทธิ์ การติดตั้งโปรแกรมป้องกันไวรัส การบันทึก Log และการอบรมผู้ใช้งาน

ขั้นที่ 6 ประเมินโอกาสเกิด

ให้คะแนน Likelihood จากข้อมูลเหตุการณ์ที่ผ่านมา สภาพช่องโหว่ ความถี่การใช้งาน และระดับการเปิดเผยต่อเครือข่ายภายนอก

ขั้นที่ 7 ประเมินผลกระทบ

ให้คะแนน Impact โดยพิจารณาผลกระทบต่อผู้ป่วย การหยุดชะงักของบริการ ข้อมูลรั่วไหล ค่าใช้จ่าย และข้อกำหนดของหน่วยเหนือ

ขั้นที่ 8 คำนวณระดับความเสี่ยง

คำนวณ Risk Score = Likelihood x Impact และจัดระดับตามเกณฑ์ที่กำหนด

ขั้นที่ 9 กำหนดแนวทางจัดการความเสี่ยง

เลือกวิธีลด ยอมรับ หลีกเลี่ยง หรือถ่ายโอนความเสี่ยง พร้อมผู้รับผิดชอบและกำหนดแล้วเสร็จ

ขั้นที่ 10 ประเมินความเสี่ยงคงเหลือ

ประเมินคะแนนหลังดำเนินมาตรการควบคุม เพื่อให้แน่ใจว่าอยู่ในระดับที่ยอมรับได้

ขั้นที่ 11 ติดตามและทบทวน

ทบทวนมาตรการควบคุมอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงสำคัญ

ขั้นที่ 12 รายงานผล

รายงานผลต่อผู้บริหารหรือคณะกรรมการที่เกี่ยวข้อง พร้อมประเด็นเร่งด่วนและข้อเสนอแนะ

6. เกณฑ์การประเมินโอกาสและผลกระทบ

6.1 เกณฑ์โอกาสเกิดเหตุการณ์ (LIKELIHOOD)

คะแนน	ระดับ	คำอธิบาย
1	น้อยมาก	แทบไม่เคยเกิด มีมาตรการควบคุมรัดกุม และโอกาสเกิดต่ำมาก
2	น้อย	อาจเกิดได้แต่ไม่บ่อย มีช่องโหว่จำกัดและมีการเฝ้าระวัง
3	ปานกลาง	มีโอกาสเกิดเป็นครั้งคราว หรือเคยเกิดในหน่วยงานใกล้เคียง
4	สูง	มีช่องโหว่ชัดเจน เคยเกิดมาก่อน หรือระบบเปิดให้เข้าถึงจากหลายจุด
5	สูงมาก	มีแนวโน้มเกิดได้บ่อย มีช่องโหว่รุนแรง หรือมีภัยคุกคามต่อเนื่อง

6.2 เกณฑ์ผลกระทบ (IMPACT)

คะแนน	ระดับ	คำอธิบาย
1	น้อยมาก	กระทบงานเฉพาะจุด แก้ไขได้ทันที ไม่มีผลต่อบริการผู้ป่วย
2	น้อย	กระทบงานบางส่วน ใช้เวลาฟื้นฟูไม่นาน ไม่มีข้อมูลสำคัญเสียหาย
3	ปานกลาง	กระทบบริการบางหน่วย ต้องใช้แผนสำรองหรือกำลังคนเพิ่มเติม
4	สูง	กระทบบริการสำคัญ ข้อมูลสำคัญอาจรั่วไหลหรือสูญหาย ต้องรายงานผู้บริหาร
5	สูงมาก	กระทบการดูแลผู้ป่วยหรือบริการหลักอย่างรุนแรง มีผลต่อกฎหมาย ชื่อเสียง หรือความต่อเนื่องของโรงพยาบาล

7. การประเมินระดับและการจัดการความเสี่ยง

7.1 ตารางประเมินระดับความเสี่ยง

Likelihood / Impact	1 น้อยมาก	2 น้อย	3 ปานกลาง	4 สูง	5 สูงมาก
5 สูงมาก	5	10	15	20	25
4 สูง	4	8	12	16	20
3 ปานกลาง	3	6	9	12	15
2 น้อย	2	4	6	8	10
1 น้อยมาก	1	2	3	4	5

7.2 เกณฑ์การจัดการความเสี่ยง

คะแนน	ระดับ	แนวทาง	ระยะเวลาดำเนินการ
20-25	สูงมาก	ลด/ควบคุมทันที	เริ่มดำเนินการทันที และควรแล้วเสร็จภายใน 3 เดือน หรือเร็วกว่านั้นตามความเร่งด่วน
12-19	สูง	ลด/ควบคุม	จัดทำแผนและดำเนินการภายใน 3-6 เดือน
6-11	ปานกลาง	ยอมรับโดยมีมาตรการหรือจัดทำแผน	ติดตามและปรับปรุงภายใน 6-12 เดือน
1-5	ต่ำ	ยอมรับความเสี่ยง	เฝ้าระวังตามรอบปกติ หรือดำเนินมาตรการต้นทุนต่ำตามความเหมาะสม

7.3 แนวทางตอบสนองความเสี่ยง

- ลดความเสี่ยง: ปรับปรุงกระบวนการหรือเพิ่มมาตรการควบคุม เช่น อัปเดตระบบ แยกสิทธิ์ สำรองข้อมูล หรือเพิ่มการตรวจสอบ Log
- ยอมรับความเสี่ยง: ใช้เมื่อคะแนนอยู่ในระดับที่ยอมรับได้ และมีผู้มีอำนาจอนุมัติพร้อมเหตุผล
- หลีกเลี่ยงความเสี่ยง: ยกเลิกหรือเปลี่ยนวิธีดำเนินกิจกรรมที่ก่อให้เกิดความเสี่ยงสูงเกินรับได้
- ถ่ายโอนความเสี่ยง: ส่งต่อความรับผิดชอบบางส่วนให้ผู้ให้บริการภายนอกหรือหน่วยงานที่มีความเชี่ยวชาญ โดยต้องมีข้อตกลงด้านความมั่นคงปลอดภัยชัดเจน

8. การติดตาม ทบทวน และรายงานผล

งานเทคโนโลยีสารสนเทศร่วมกับเจ้าของระบบต้องติดตามความคืบหน้าของแผนจัดการความเสี่ยงอย่างต่อเนื่อง และรายงานความเสี่ยงระดับสูงขึ้นไปต่อผู้บริหารตามรอบที่กำหนด

- ทบทวนทะเบียนความเสี่ยงอย่างน้อยปีละ 1 ครั้ง
- ทบทวนทันทีเมื่อเกิดเหตุการณ์สำคัญ เช่น ระบบล่ม ข้อมูลรั่วไหล มัลแวร์ระบาด หรือมีการเปลี่ยนแปลงโครงสร้างระบบ
- จัดเก็บหลักฐานการประเมิน แผนแก้ไข ผลการติดตาม และการอนุมัติไว้ในระบบเอกสารของโรงพยาบาล
- สรุปรายงานความเสี่ยงที่หลงเหลือและข้อเสนอแนะต่อคณะกรรมการหรือผู้บริหารที่ได้รับมอบหมาย

9. เอกสารอ้างอิง

1. พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และแนวทางที่เกี่ยวข้องกับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
2. ISO/IEC 27001:2022 Information Security Management Systems - Requirements
3. ISO/IEC 27002:2022 Information Security Controls
4. NIST Cybersecurity Framework 2.0, National Institute of Standards and Technology
5. ข้อมูลประกอบจากรายชื่อโรงพยาบาลในประเทศไทย: Fort Weerawatyothin Hospital, Royal Thai Army, Surin, Mueang, 60 beds
6. เอกสารต้นแบบ: การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy Procedure), โรงพยาบาลแม่ลาว

ภาคผนวก ก แบบฟอร์มทะเบียนความเสี่ยง

ลำดับ	ทรัพย์สิน/ระบบ	ภัยคุกคาม	ช่องโหว่	L	I	ระดับ	มาตรการ/ผู้รับผิดชอบ
1	ระบบเวชระเบียน	เข้าถึงข้อมูลโดยไม่ได้รับอนุญาต	กำหนดสิทธิ์ไม่เหมาะสม				
2	เครื่องแม่ข่ายฐานข้อมูล	ระบบหยุดให้บริการ	ไม่มีแผนสำรองหรือทดสอบกู้คืน				
3	เครื่องลูกข่าย	มัลแวร์/ฟิชชิง	ผู้ใช้งานเปิดไฟล์แนบไม่ปลอดภัย				
4	เครือข่ายภายใน	อุปกรณ์ขัดข้อง	ไม่มีอุปกรณ์สำรองหรือการเฝ้าระวัง				
5	ระบบสำรองข้อมูล	สำรองไม่สำเร็จ	ไม่มีการตรวจสอบผลการสำรอง				