รายงานการประเมินและบริหารความเสี่ยง

(Risk Assessment and Risk Management Report)

วันที่ประเมิน	22 มกราคม 2569	ผู้จัดทำรายงาน	กลุ่มงานเทคโนโลยีสารสนเทศ
หน่วยงาน	โรงพยาบาลค่ายวีรวัฒน์โยธิน	ชื่อระบบ	ระบบสารสนเทศเพื่อการให้บริการของโรงพยาบาล

1. สรุปสำหรับผู้บริหาร (Executive Summary)

รายงานฉบับนี้จัดทำขึ้นเพื่อประเมินความเสี่ยงของระบบสารสนเทศที่สนับสนุนการให้บริการของโรงพยาบาลค่ายวีรวัฒน์โยธิน โดยให้ความสำคัญกับการคุ้มครองข้อมูลสำคัญของผู้รับบริการ ความถูกต้องของข้อมูล และความต่อเนื่องของการให้บริการ ผลการประเมินสะท้อนว่ามีความเสี่ยงสำคัญในบางประเด็น ซึ่งควรได้รับการติดตามและยกระดับมาตรการควบคุมอย่างเป็นระบบ

- ขอบเขตการประเมินครอบคลุมระบบงานหลักที่เกี่ยวข้องกับการลงทะเบียน การให้บริการ และการสนับสนุนข้อมูล
- ประเด็นความเสี่ยงสำคัญเกี่ยวข้องกับการควบคุมปลายทาง การจัดการสิทธิ์ และความพร้อมของข้อมูลสำรอง
- ข้อเสนอแนะมุ่งเน้นการยกระดับมาตรการควบคุมที่ปฏิบัติได้จริงและเหมาะสมกับบริบทของโรงพยาบาล

2. รายละเอียดของรายงาน (Body of the Report)

2.1 วัตถุประสงค์ของการประเมินความเสี่ยง

1. ประเมินความเสี่ยงของระบบสารสนเทศที่เกี่ยวข้องกับการให้บริการและการจัดเก็บข้อมูลผู้ป่วย
2. ระบุภัยคุกคามและช่องโหว่ที่อาจกระทบต่อความลับ ความถูกต้อง และความพร้อมใช้งานของข้อมูล
3. กำหนดแนวทางควบคุมและข้อเสนอแนะเพื่อใช้ประกอบการพิจารณาของผู้บริหาร

2.2 ข้อสมมติและข้อจำกัดในการประเมิน

- ข้อมูลที่ได้รับสำหรับการประเมินถือว่าถูกต้อง ครบถ้วน และสะท้อนสภาพการใช้งานจริงในปัจจุบัน
- การประเมินครั้งนี้เป็นการประเมินเชิงบริหารและเชิงกระบวนการ ไม่ได้ทดสอบเจาะระบบเชิงเทคนิคในเชิงลึก
- ผลการประเมินเป็นภาพตามช่วงเวลาที่จัดทำรายงาน และอาจเปลี่ยนแปลงได้เมื่อบริบทภัยคุกคามหรือสภาพการใช้งานเปลี่ยนไป

2.3 การยอมรับความเสี่ยง

โรงพยาบาลค่ายวีรวัฒน์โยธินมีแนวทางยอมรับความเสี่ยงในระดับปานกลาง โดยสามารถยอมรับความเสี่ยงที่ควบคุมได้ในระดับหนึ่ง แต่จะเร่งดำเนินการต่อความเสี่ยงที่อาจกระทบต่อความต่อเนื่องของการรักษาพยาบาลหรือความปลอดภัยของข้อมูลผู้ป่วย

2.4 โมเดลความเสี่ยงและวิธีการประเมิน

ใช้กรอบการประเมินตามแนวคิด NIST SP 800-30 Rev.1 โดยพิจารณาความเป็นไปได้ของเหตุการณ์และระดับผลกระทบ จากนั้นจัดกลุ่มเป็นระดับต่ำ ปานกลาง และสูง เพื่อสนับสนุนการจัดลำดับความสำคัญของมาตรการควบคุม

3. รายละเอียดความเสี่ยง (Detailed Risk Assessment)

ความเสี่ยง	ระดับ	ผลกระทบที่อาจเกิดขึ้น	การควบคุม / ข้อเสนอแนะ
การโจมตีด้วยมัลแวร์	สูง	อาจทำให้ข้อมูลผู้ป่วยและระบบบริการสำคัญหยุดชะงักหรือถูกเข้ารหัส	ติดตั้งซอฟต์แวร์ป้องกันมัลแวร์ที่ได้รับอนุญาต อัปเดตฐานข้อมูลภัยคุกคามและทบทวนสิทธิ์การใช้งานอุปกรณ์ปลายทาง
การโจมตีแบบฟิชชิง	สูง	อาจนำไปสู่การรั่วไหลของรหัสผ่าน การปลอมตัวผู้ใช้งาน และการเข้าถึงระบบโดยไม่ได้รับอนุญาต	จัดอบรมสร้างความตระหนัก ตรวจสอบอีเมลต้องสงสัย และบังคับใช้รหัสผ่านที่รัดกุมร่วมกับการยืนยันตัวตนหลายปัจจัย
ภัยคุกคามจากบุคคลภายใน	ปานกลาง	อาจเกิดการเข้าถึงหรือเปิดเผยข้อมูลเกินสิทธิ์โดยไม่ตั้งใจหรือโดยเจตนา	ทบทวนสิทธิ์ตามบทบาทงาน ตรวจสอบบันทึกเหตุการณ์เป็นประจำ และใช้หลักการให้สิทธิน้อยที่สุด
การละเมิดข้อมูล	ปานกลาง	อาจทำให้ข้อมูลสุขภาพส่วนบุคคลรั่วไหลและกระทบชื่อเสียงองค์กร	กำหนดกระบวนการแจ้งเหตุและตอบสนองเหตุผิดปกติ รวมถึงการเข้ารหัสข้อมูลสำคัญ
การโจมตีแบบ Denial of Service	ปานกลาง	ระบบบริการอาจช้าหรือใช้งานไม่ได้ในช่วงเวลาสำคัญ	เตรียมแผนรองรับเหตุขัดข้อง ใช้การเฝ้าระวังทราฟฟิก และพิจารณา WAF หรือ rate limiting
การโจมตีแบบ Man-in-the-Middle	ต่ำ	อาจถูกดักฟังหรือปลอมแปลงข้อมูลระหว่างทาง	บังคับใช้ HTTPS/TLS และตรวจสอบใบรับรองดิจิทัลของระบบอย่างสม่ำเสมอ
การโจมตีด้วยแรนซัมแวร์	สูง	อาจทำให้ฐานข้อมูลและเอกสารสำคัญไม่สามารถใช้งานได้	สำรองข้อมูลแบบออฟไลน์ ทดสอบการกู้คืน และควบคุมการปรับปรุงแพตช์ของระบบปฏิบัติการ
วิศวกรรมสังคม	ปานกลาง	ผู้ใช้ถูกหลอกให้เปิดเผยข้อมูลหรืออนุญาตการเข้าถึงโดยไม่เหมาะสม	จัดทำแนวปฏิบัติการตรวจสอบตัวตนและซ้อมสถานการณ์หลอกลวงภายในองค์กร
ความเสี่ยงด้านคลาวด์	ปานกลาง	อาจเกิดการตั้งค่าที่ไม่ปลอดภัยหรือการเข้าถึงข้ามระบบโดยไม่เหมาะสม	ใช้การกำหนดสิทธิ์แบบจำกัด ตรวจสอบการตั้งค่าบริการ และทบทวนคีย์และข้อมูลลับของระบบ

ความเสี่ยงจากผู้จำหน่ายภายนอก	ปานกลาง	ความปลอดภัยของข้อมูลอาจได้รับผลกระทบจากระบบของคู่ค้า	กำหนด SLA ด้านความปลอดภัย และประเมินผู้ให้บริการก่อนเชื่อมต่อระบบ
อุปกรณ์เคลื่อนที่ขององค์กร	ต่ำ	อุปกรณ์สูญหายอาจทำให้ข้อมูลรั่วไหลหรือถูกเข้าถึงโดยมิชอบ	เปิดใช้รหัสผ่าน การจัดการอุปกรณ์เคลื่อนที่ (MDM) และการล้างข้อมูลระยะไกลเมื่ออุปกรณ์สูญหาย
ซอฟต์แวร์และระบบที่มีช่องโหว่	ปานกลาง	ช่องโหว่อาจถูกใช้เป็นทางผ่านเข้าสู่เครือข่ายภายใน	ทบทวนบัญชีทรัพย์สินระบบ การบริหารแพตช์ และการสแกนช่องโหว่เป็นรอบ

4. ข้อเสนอแนะเพื่อการปรับปรุง

- ยกระดับการสำรองข้อมูลและการทดสอบกู้คืนอย่างสม่ำเสมอ เพื่อรองรับเหตุขัดข้องหรือการโจมตีด้วยแรนซัมแวร์
- เพิ่มการอบรมความปลอดภัยไซเบอร์แก่บุคลากรทุกระดับ โดยเฉพาะการสังเกตอีเมลและการขออนุมัติที่ผิดปกติ
- ทบทวนสิทธิ์ผู้ใช้และการเข้าถึงระบบสำคัญตามรอบเวลา พร้อมจัดทำบัญชีผู้ใช้งานที่เป็นปัจจุบัน
- ตั้งค่ามาตรการเฝ้าระวังเหตุการณ์และบันทึกเหตุการณ์ให้เพียงพอสำหรับการสืบค้นเหตุและการตอบสนอง

ลงนาม	ผู้เรียบเรียง / จัดทำโดย	ผู้ตรวจทาน / ผู้ทบทวน	ผู้อนุมัติ
ลายเซ็น			
ชื่อ-สกุล	นายกัมปนาท สมกล้า	ร.อ.ภาราดร บุบผาลัย	พ.อ.วงศ์สรรค์ สิริชีวเกษร
ตำแหน่ง	นักวิชาการคอมพิวเตอร์	หัวหน้าเทคโนโลยีสารสนเทศ	ผู้อำนวยการโรงพยาบาลค่ายวีรวัฒน์โยธิน
วัน เดือน ปี	22 มกราคม 2569	22 มกราคม 2569	22 มกราคม 2569

ครั้งที่	วันที่ประกาศใช้	รายละเอียดการแก้ไข
01	22 มกราคม 2569	จัดทำเอกสารฉบับแรกสำหรับโรงพยาบาลค่ายวีรวัฒน์โยธิน เพื่อใช้เป็นแนวทางประเมินและทบทวนความเสี่ยงด้านเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยไซเบอร์