รายงานการนำผลการประเมินมาจัดทำแผนปรับปรุง

มีการนำผลการประเมินไปใช้ในการปรับปรุงและพัฒนา

โรงพยาบาลค่ายวีรวัฒน์โยธิน

จัดทำเพื่อสรุปผลการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และแสดงแนวทางการนำผลการประเมินไปใช้จริงในกระบวนการปฏิบัติงาน การควบคุมความเสี่ยง และการติดตามผลอย่างต่อเนื่อง ให้เกิดความปลอดภัย และความพร้อมของระบบสารสนเทศของโรงพยาบาล

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

1. บทนำ

เอกสารฉบับนี้จัดทำขึ้น โดยสรุปผลการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศของโรงพยาบาลค่ายวีรวัฒน์โยธิน และเชื่อมโยงผลการประเมินกับการดำเนินมาตรการปรับปรุงที่เป็นรูปธรรม ทั้งในด้านบุคลากร กระบวนการ และเทคโนโลยี

แนวทางดังกล่าวมุ่งให้การบริหารความเสี่ยงเป็นวงจรต่อเนื่อง เริ่มจากการระบุความเสี่ยง ประเมินระดับความรุนแรง กำหนดมาตรการควบคุมติดตามผล และทบทวนซ้ำเพื่อให้การให้บริการทางการแพทย์และบริการสนับสนุนระบบข้อมูลดำเนินไปได้อย่างปลอดภัย เชื่อถือได้ และลดผลกระทบต่อผู้รับบริการ

2. เป้าหมายของการนำผลการประเมินไปใช้

- ลดโอกาสเกิดเหตุขัดข้องของระบบสารสนเทศที่กระทบต่อการให้บริการผู้ป่วย
- ยกระดับการควบคุมการเข้าถึงข้อมูลผู้ป่วยและข้อมูลสำคัญของหน่วยงาน
- เสริมความพร้อมของโครงสร้างพื้นฐานด้านไฟฟ้า เครือข่าย และอุปกรณ์หลัก
- สร้างวัฒนธรรมการใช้งานเทคโนโลยีสารสนเทศอย่างถูกต้องและปลอดภัย

3. สรุปผลการประเมินและประเด็นที่นำมาปรับปรุง

ประเด็นความเสี่ยง	ผลการประเมิน	การนำไปใช้/แนวทางปรับปรุง	ผู้รับผิดชอบ	ระยะเวลา
ระบบไฟฟ้าและไฟสำรอง	พบความจำเป็นในการเพิ่มความมั่นคงของระบบสำรองไฟเพื่อรองรับการทำงานต่อเนื่อง	ตรวจเช็ก UPS และเครื่องกำเนิดไฟฟ้าตามรอบบำรุงรักษาเชิงป้องกัน และจัดทำแผนสำรองเมื่อไฟฟ้าขัดข้อง	งานอาคาร/IT	ต่อเนื่อง
การคุ้มครองข้อมูลส่วนบุคคล	การใช้ข้อมูลผู้ป่วยและข้อมูลบุคลากรต้องมีการควบคุมสิทธิ์อย่างเข้มงวด	อบรมทบทวน PDPA จัดระดับสิทธิ์ และกำหนดแนวปฏิบัติการเข้าถึงข้อมูลเท่าที่จำเป็น	IT/งานเวชระเบียน	ไตรมาสละ 1 ครั้ง
ความมั่นคงของห้อง Server	ต้องลดความเสี่ยงจากอุณหภูมิ ความชื้น และการเข้าถึงโดยไม่ได้รับอนุญาต	ตรวจสอบอุณหภูมิ ติดตั้ง/ปรับปรุงระบบปรับอากาศ ควบคุมการเข้าออก และติดกล้องวงจรปิด	IT/งานอาคาร	ต่อเนื่อง
ซอฟต์แวร์และลิขสิทธิ์	ยังมีความเสี่ยงจากการใช้โปรแกรมที่ไม่สอดคล้องลิขสิทธิ์	จัดหาและใช้งานซอฟต์แวร์ถูกต้องตามกฎหมาย พร้อมสร้างความตระหนักแก่ผู้ใช้งาน	IT	6 เดือน
เครือข่ายภายในและอินเทอร์เน็ต	ความต่อเนื่องของเครือข่ายมีผลต่อระบบบริการหลักของโรงพยาบาล	แยก VLAN ตรวจสอบอุปกรณ์เครือข่ายสม่ำเสมอ และประสานผู้ให้บริการเมื่อพบเหตุขัดข้อง	IT/NT	ต่อเนื่อง
อุปกรณ์พกพาและทรัพย์สิน IT	อุปกรณ์เสี่ยงต่อการสูญหายหรือถูกโจรกรรม	จัดเก็บในพื้นที่ปลอดภัย ติดระบบควบคุมการเข้าออก และตรวจนับทรัพย์สินตามรอบ	IT/เวรยาม	รายเดือน

4. แนวทางดำเนินงานหลังการประเมิน

- สรุปประเด็นความเสี่ยงที่มีระดับสูงหรือมีผลกระทบต่อการให้บริการ แล้วมอบหมายผู้รับผิดชอบชัดเจน
- กำหนดแผนแก้ไขที่มีระยะเวลา ผู้รับผิดชอบ และตัวชี้วัดติดตามผล
- นำผลการตรวจประเมินไปทบทวนในที่ประชุมงานเทคโนโลยีสารสนเทศและคณะกรรมการที่เกี่ยวข้อง
- ติดตามการปิดประเด็นทุกเดือน และรายงานความคืบหน้าในรอบประเมินถัดไป

5. ผลที่คาดว่าจะได้รับ

เมื่อมีการนำผลการประเมินไปใช้จริง โรงพยาบาลจะมีระบบบริหารความเสี่ยงที่ชัดเจนขึ้น ลดเหตุขัดข้องของระบบที่สำคัญ เพิ่มความมั่นใจในการปกป้องข้อมูลผู้ป่วย และสนับสนุนให้การบริการทางการแพทย์ดำเนินได้ต่อเนื่อง แม้เผชิญเหตุไม่คาดคิด

6. การติดตามและทบทวน

กิจกรรมติดตาม	ความถี่	ผู้รับผิดชอบ	ผลลัพธ์ที่คาดหวัง
ตรวจสอบสถานะการแก้ไขรายการความเสี่ยง	รายเดือน	หัวหน้างาน IT	เห็นความก้าวหน้าและปิดประเด็นได้ตามกำหนด
ทบทวนสิทธิ์การเข้าถึงข้อมูลสำคัญ	รายไตรมาส	IT/เวชระเบียน	ลดการเข้าถึงเกินความจำเป็น
ทดสอบแผนสำรองและแผนตอบสนองเหตุขัดข้อง	ปีละ 2 ครั้ง	IT/งานอาคาร	มั่นใจว่ากลับมาทำงานได้จริงเมื่อเกิดเหตุ