แนวปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์

(Cyber Security Operational Guideline)

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	จัดทำเอกสารสำหรับโรงพยาบาลค่ายวีรวัฒน์โยธิน เพื่อใช้เป็นแนวปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์

สารบัญ

- 1. วัตถุประสงค์ 3
- 2. ขอบเขต 3
- 3. คำจำกัดความและนิยามศัพท์ 3
- 4. หน้าที่และความรับผิดชอบ 4
- 5. แนวปฏิบัติ 4
- 6. การทบทวนและปรับปรุง 4
- 7. เอกสารที่เกี่ยวข้อง 4
- 8. เอกสารอ้างอิง 5
- 9. ผลการประเมิน 5

1. วัตถุประสงค์

เพื่อกำหนดแนวทางการปฏิบัติงานด้านความมั่นคงปลอดภัยไซเบอร์ให้เป็นมาตรฐานเดียวกัน เพื่อป้องกันการเข้าถึงระบบ ข้อมูล และอุปกรณ์ของโรงพยาบาลโดยไม่ได้รับอนุญาต เพื่อสนับสนุนการเฝ้าระวัง ตรวจสอบ และตอบสนองต่อเหตุการณ์ที่อาจกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ

2. ขอบเขต

ครอบคลุมระบบสารสนเทศ เครือข่าย อุปกรณ์คอมพิวเตอร์ บัญชีผู้ใช้งาน ข้อมูลสำคัญ และบุคลากรที่เกี่ยวข้องกับการใช้งานระบบของโรงพยาบาลใช้กับทั้งเจ้าหน้าที่ภายใน ผู้รับจ้าง ผู้ให้บริการภายนอก และผู้มีสิทธิ์เข้าถึงระบบในทุกระดับ ให้ถือปฏิบัติควบคู่กับนโยบายความมั่นคงปลอดภัยสารสนเทศ ระเบียบปฏิบัติภายใน และประกาศที่เกี่ยวข้อง

3. คำจำกัดความและนิยามศัพท์

ผู้ใช้งาน หมายถึง บุคลากรหรือผู้ที่ได้รับอนุญาตให้ใช้งานระบบสารสนเทศของโรงพยาบาล
ผู้ดูแลระบบ หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายให้กำหนดสิทธิ์ ดูแลการเข้าถึง และติดตามบันทึกการใช้งาน
เหตุการณ์ด้านความมั่นคงปลอดภัย หมายถึง เหตุผิดปกติที่อาจก่อให้เกิดการรั่วไหล แก้ไข หรือหยุดชะงักของระบบ

4. หน้าที่และความรับผิดชอบ

ระดับผู้รับผิดชอบ	หน้าที่และความรับผิดชอบด้านความมั่นคงปลอดภัยไซเบอร์
ผู้อำนวยการโรงพยาบาล	กำกับนโยบาย อนุมัติทรัพยากร และสนับสนุนการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์
หัวหน้ากลุ่มงานเทคโนโลยีสารสนเทศ	กำหนดแนวทาง ควบคุมการเข้าถึง ติดตามความเสี่ยง และประสานงานเมื่อเกิดเหตุ
ผู้ใช้งานทุกระดับ	ปฏิบัติตามแนวปฏิบัติ รักษาความลับของบัญชีผู้ใช้ และรายงานเหตุผิดปกติทันที

5. แนวปฏิบัติ

5.1 การกำหนดสิทธิ์และการยืนยันตัวตน

กำหนดสิทธิ์ตามหน้าที่งานแบบเท่าที่จำเป็น (least privilege) และทบทวนสิทธิ์เป็นระยะกำหนดให้รหัสผ่านมีความรัดกุม เปลี่ยนตามรอบที่กำหนด และไม่เปิดเผยให้ผู้อื่นทราบ ใช้การยืนยันตัวตนหลายปัจจัยสำหรับระบบสำคัญหรือข้อมูลอ่อนไหว

5.2 การเข้าถึงข้อมูลและอุปกรณ์

จำกัดการเชื่อมต่ออุปกรณ์ภายนอกตามความจำเป็น และอนุญาตเฉพาะอุปกรณ์ที่ผ่านการตรวจสอบห้ามติดตั้งซอฟต์แวร์หรือใช้งานสื่อบันทึกข้อมูลที่ไม่ได้รับอนุญาตบนเครื่องของโรงพยาบาลเมื่อใช้งานเสร็จต้องออกจากระบบ ล็อกหน้าจอ และปิดอุปกรณ์ตามระเบียบ

5.3 การบันทึกและติดตาม

บันทึกการเข้าใช้งานระบบและกิจกรรมสำคัญไว้เพื่อใช้ตรวจสอบย้อนหลัง ติดตามเหตุการณ์ผิดปกติและรายงานต่อผู้รับผิดชอบทันทีเมื่อพบความเสี่ยง เก็บรักษาหลักฐานดิจิทัลตามระยะเวลาที่หน่วยงานกำหนด

5.4 การจัดการผู้ให้บริการภายนอก

ต้องขออนุมัติก่อนเข้าถึงระบบหรือข้อมูลของโรงพยาบาล กำหนดช่วงเวลาการใช้งานและยกเลิกสิทธิ์เมื่อสิ้นสุดภารกิจ กำกับให้ปฏิบัติตามเงื่อนไขด้านความมั่นคงปลอดภัยและการรักษาความลับอย่างเคร่งครัด

6. การทบทวนและปรับปรุง

ให้ทบทวนเอกสารอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงระบบ เทคโนโลยี กฎหมาย หรือความเสี่ยงที่สำคัญ หากมีการปรับปรุง ต้องสื่อสารสาระสำคัญให้หน่วยงานที่เกี่ยวข้องรับทราบและถือปฏิบัติตามฉบับล่าสุด

7. เอกสารที่เกี่ยวข้อง

นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศของโรงพยาบาลค่ายวีรวัฒน์โยธิน ระเบียบการใช้งานระบบเทคโนโลยีสารสนเทศและเครือข่าย แบบฟอร์มขออนุมัติสิทธิ์ผู้ใช้งานและแบบบันทึกการเปลี่ยนแปลงสิทธิ์

8. เอกสารอ้างอิง

ประกาศและกรอบแนวทางด้านความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ แนวทางการควบคุมการเข้าถึงและการจัดการตัวตน หลักฐานบันทึกการเข้าถึงระบบ และรายงานการตรวจสอบด้านความปลอดภัย

9. ผลการประเมิน

โดยรวมโรงพยาบาลมีการกำหนดแนวปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์ครอบคลุมประเด็นสำคัญครบถ้วน จุดแข็งที่พบคือมีการกำหนดผู้รับผิดชอบชัดเจน การควบคุมสิทธิ์ผู้ใช้ และการติดตามเหตุผิดปกติอย่างต่อเนื่อง ข้อเสนอแนะเพื่อพัฒนาเพิ่มเติม คือการทบทวนสิทธิ์ผู้ใช้เป็นรอบสม่ำเสมอ การบันทึกหลักฐานการเข้าถึงและการซ้อมตอบสนองเหตุการณ์อย่างน้อยปีละ 1 ครั้ง