แผนรับมือภัยคุกคามทางไซเบอร์หรือระบบล่ม

(Cybersecurity & System Outage Response Plan)

โรงพยาบาลค่ายวีรวัฒน์โยธิน | รหัสเอกสาร KWT-9-2-2 | แก้ไขครั้งที่ 01 | วันที่บังคับใช้ 4 มกราคม 2569 | ใช้ภายในเท่านั้น

ลงนาม	ผู้เรียบเรียง/จัดทำโดย	ผู้ตรวจทาน/ผู้ทบทวน	ผู้อนุมัติ
ลายเซ็นต์			
ชื่อ-สกุล	นายกัมปนาท สมกล้า	ร.อ.ภาราดร บุบผาลัย	พ.อ.วงศ์สรรค์ สิริชีวเกษร
ตำแหน่ง	นักวิชาการคอมพิวเตอร์	หัวหน้าเทคโนโลยีสารสนเทศ	ผู้อำนวยการโรงพยาบาลค่ายวีรวัฒน์โยธิน
วัน เดือน ปี	4 มกราคม 2569	4 มกราคม 2569	4 มกราคม 2569

ประวัติการแก้ไข

ครั้งที่	วันที่ประกาศใช้	รายละเอียดการแก้ไข
01	4 มกราคม 2569	จัดทำเอกสารครั้งแรก เพื่อใช้เป็นแนวทางการรับมือเหตุการณ์และภัยคุกคามทางไซเบอร์ของโรงพยาบาลค่ายวีรวัฒน์โยธิน


โรงพยาบาลค่ายวีรวัฒน์โยธิน
FORT WEERAWATYOTHIN HOSPITAL
ขั้นตอนการปฏิบัติเมื่อระบบล่ม
1. จุดคัดกรอง
1.1 กรอกเลขบัตรประชาชนในใบนำทาง
1.2 ลง นน. สส. ความดัน และอื่นๆ
2. จุดลงทะเบียน
2.1 ตรวจสอบสิทธิ์จากเลขบัตร
2.2 เปิด Visit คนไข้
2.3 ปริ้นหรือ ถ่ายรูปประวัติการรักษาที่หน้าเวชระเบียน
3. จุดซักประวัติ
3.1 เพิ่มใบนำทางออฟไลน์ และลงข้อมูลซักประวัติ
3.2 เย็บใบนำทางสองแผ่นส่งไปที่จุดส่งคิว
3.3 เซ็นชื่อ ผู้ซักประวัติ
4. จุดส่งคิว
4.1 จุดส่งคิวทำการส่งคิวเข้าที่ห้องแพทย์
5. แพทย์ตรวจรักษา
5.1 เขียนชื่อยา จำนวนยา และหัตถการ โดยไม่ต้องใส่ราคา
5.2 ลงผลวินิจฉัย รหัส ICD และชื่อโรค (โรคหลัก และ ร่วม)
5.3 เซ็นชื่อ ส่งให้ จนท ที่จุดออกใบนัด
6. จุดออกใบนัด
6.1 ทำการออกใบนัดคนไข้
6.2 ให้คนไข้นำเอกสารทั้งหมด ยกเว้นใบนัดยื่นที่ห้องยา
7. ห้องจ่ายยา
7.1 ลงราคายาทั้งหมด ยกเว้นหัตถการ
7.2 เซ็นชื่อเจ้าหน้าที่ผู้จ่ายยา
7.3 ส่งเอกสารให้คนไข้ยื่นที่ห้องเก็บเงิน
7.4.1 จ.น.ท. ห้องยาจ่ายยาให้คนไข้พร้อมใบเสร็จ
7.4.2 จ.น.ท. ห้องยาเก็บรวบรวมเอกสารทั้งหมด เพื่อนำข้อมูลเข้ามาลงในระบบจริงย้อนหลังใหม่ทั้งหมดตามขั้นตอนข้างต้น
8. ห้องเก็บเงิน
8.1 ทำการตรวจสอบค่ารักษาพยาบาลทั้งหมด
8.2 รวมราคาค่าใช้จ่าย คิดเงิน ออกใบเสร็จ
8.3 เซ็นชื่อเจ้าหน้าที่เรียกเก็บเงิน
8.4 ให้คนไข้นำเอกสารทั้งหมด ยกเว้นใบนัดยื่นที่ห้องยาเพื่อรับยา
โรงพยาบาลค่ายวีรวัฒน์โยธิน
Fort Weerawatyothin Hospital
โรงพยาบาลคุณธรรม
MORAL HOSPITAL
ดูแลด้วยใจ ห่วงใยดุจครอบครัว

แผนรับมือภัยคุกคามทางไซเบอร์หรือระบบล่ม (Cybersecurity & System Outage Response Plan)

อ้างอิง: แนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานภาครัฐ
และกรอบการตอบสนองเหตุการณ์ฉุกเฉินด้านสารสนเทศ

1. หลักการและเหตุผล

- โรงพยาบาลค่ายวีรวัฒน์โยธินจำเป็นต้องมีแนวทางรับมือเหตุการณ์ทางไซเบอร์ที่ชัดเจน เพื่อให้การตอบสนองเป็นระบบ ลดผลกระทบต่อการรักษาพยาบาล และรักษาความพร้อมใช้งานของระบบสารสนเทศของโรงพยาบาล
- เอกสารฉบับนี้ใช้เป็นแนวทางปฏิบัติเมื่อพบเหตุผิดปกติ เช่น ระบบใช้งานไม่ได้ ข้อมูลถูกแก้ไขโดยไม่ได้รับอนุญาต พบมัลแวร์ หรือมีการเข้าถึงระบบโดยมิชอบ

2. วัตถุประสงค์

- เพื่อกำหนดขั้นตอนรับแจ้ง ตรวจสอบ ยืนยันเหตุการณ์ ควบคุมความเสียหาย กู้คืนระบบ และสรุปบทเรียนหลังเหตุการณ์
- เพื่อให้บุคลากรทุกระดับปฏิบัติได้สอดคล้องกัน และประสานงานกับผู้บริหารหรือหน่วยงานภายนอกได้ทันเวลา

3. ขอบเขต

- ใช้กับระบบคอมพิวเตอร์ เครือข่าย ข้อมูลดิจิทัล และบัญชีผู้ใช้งานของโรงพยาบาลค่ายวีรวัฒน์โยธิน
- ครอบคลุมเหตุการณ์สำคัญที่อาจกระทบต่อการให้บริการ เช่น Phishing, Malware, Ransomware, ระบบล่ม, และการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

4. ขั้นตอนการรับมือ

1. รับแจ้งเหตุและบันทึกเวลา สถานที่ ผู้พบเหตุ และอาการผิดปกติที่สังเกตได้
2. ตรวจสอบเบื้องต้นเพื่อแยกแยะว่าเป็นเหตุจริงหรือความขัดข้องทั่วไป
3. จำกัดความเสียหาย เช่น ตัดการเชื่อมต่อเครื่องที่สงสัย เปลี่ยนรหัสผ่านชั่วคราว หรือปิดบริการที่เสี่ยง
4. เก็บหลักฐานที่จำเป็น เช่น ภาพหน้าจอ ไฟล์บันทึก และข้อมูลเครือข่าย
5. กู้คืนระบบจากสำเนาข้อมูลที่เชื่อถือได้ และทดสอบก่อนเปิดใช้งาน
6. สรุปผลและปรับปรุงมาตรการป้องกันไม่ให้เกิดซ้ำ

5. บทบาทหน้าที่

- หัวหน้าเทคโนโลยีสารสนเทศ: ควบคุมการตอบสนอง ประสานหน่วยงานที่เกี่ยวข้อง และเสนอแนวทางแก้ไขต่อผู้บริหาร
- ผู้ดูแลระบบ: ตรวจสอบสาเหตุ ตัดวงจรความเสียหาย กู้คืนระบบ และเฝ้าระวังหลังเหตุการณ์
- ผู้ใช้งาน: แจ้งเหตุทันทีเมื่อพบความผิดปกติ และปฏิบัติตามคำแนะนำของเจ้าหน้าที่

6. การทบทวนและปรับปรุง

- ทบทวนแผนอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีเหตุการณ์สำคัญ/การเปลี่ยนแปลงด้านระบบสารสนเทศ
- นำข้อเสนอแนะจากการซ้อมแผนหรือเหตุการณ์จริงมาปรับปรุงเอกสารและการฝึกอบรมบุคลากร