แผนเผชิญเหตุและรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan - IRP)

โรงพยาบาลพระอาจารย์มั่น ภูริทัตโต ประจำปี ๒๕๖๙

๑. วัตถุประสงค์ เพื่อให้ศูนย์เทคโนโลยีสารสนเทศและบุคลากรของโรงพยาบาลพระอาจารย์มั่น ภูริทัตโต มีแนวทางปฏิบัติที่ชัดเจนในการรับมือกับเหตุการณ์ละเมิดความมั่นคงปลอดภัยทางไซเบอร์ (เช่น มัลแวร์เรียกค่าไถ่ Ransomware, ข้อมูลรั่วไหล, หรือระบบถูกโจมตี) สามารถระงับเหตุได้อย่างรวดเร็ว ลดผลกระทบต่อการให้บริการผู้ป่วย และกู้คืนระบบให้กลับมาใช้งานได้ตามปกติอย่างปลอดภัย

๒. โครงสร้างทีมรับมือเหตุฉุกเฉิน (Incident Response Team)

๒.๑ ผู้บัญชาการเหตุการณ์ (Incident Commander)

- นางศิริกัญญา ถาบุตร (หัวหน้ากลุ่มงานฯ) มีหน้าที่ประเมินสถานการณ์ระดับความรุนแรง สั่งการอนุมัติตัดระบบเครือข่ายหลัก และเป็นผู้รายงานสถานการณ์ต่อผู้อำนวยการโรงพยาบาล ตลอดจนหน่วยงานภายนอก

๒.๒ ทีมผู้ปฏิบัติการทางเทคนิค (Technical Responders)

- เจ้าหน้าที่ผู้ปฏิบัติหน้าที่เวร On Call (ตรวจสอบตารางเวรได้ที่หน้าเว็บไซต์หลักของโรงพยาบาล) มีหน้าที่เข้าระงับเหตุเบื้องต้น กักกันความเสียหาย และดำเนินการกู้คืนข้อมูล

๓. ช่องทางการแจ้งเหตุฉุกเฉิน (Incident Reporting) เมื่อบุคลากรทางการแพทย์หรือผู้ใช้งานพบความผิดปกติ เช่น หน้าจอถูกล็อกไฟล์ (Ransomware), เครื่องคอมพิวเตอร์ทำงานผิดปกติอย่างรุนแรง, หรือไม่สามารถเข้าถึงฐานข้อมูล HOSxP ได้ ให้ดำเนินการแจ้งเหตุทันทีตามลำดับดังนี้ ๑. ตรวจสอบรายชื่อผู้ปฏิบัติหน้าที่เวร On Call ประจำวัน ผ่านหน้าเว็บไซต์โรงพยาบาล ๒. โทรศัพท์แจ้งเหตุโดยตรงไปยังเบอร์มือถือของเจ้าหน้าที่เวร หรือทีมงานศูนย์เทคโนโลยีสารสนเทศ ดังรายชื่อต่อไปนี้

- นางศิริกัญญา ถาบุตร โทร. ๐๙๕-๒๒๓-๙๒๖๙
- นายพงษ์ดนัย วรสาร โทร. ๐๘๐-๙๘๙-๖๙๒๒
- น.ส.ขวัญฤดี นามนนท์ โทร. ๐๖๓-๑๖๒-๖๓๒๘
- น.ส.พัชราภรณ์ แสงหาญ โทร. ๐๘๒-๐๓๗-๒๙๒๕
- น.ส.วรรณนิดา นามแสง โทร. ๐๙๕-๓๖๕-๐๓๘๐
- นายอภิวัฒน์ อินธิกาย โทร. ๐๖๔-๙๙๓-๘๘๗๕
- นายชนุดม อาษา โทร. ๐๙๒-๘๘๒-๓๗๕๐
- นายวชิรวิทย์ อุดมฉวี โทร. ๐๖๓-๘๑๐-๙๓๑๐

๔. ขั้นตอนการปฏิบัติเมื่อเกิดเหตุฉุกเฉิน (Standard Operating Procedures - SOP)

ระยะที่ ๑ การจำกัดความเสียหายเบื้องต้น (Containment)

- สำหรับผู้ใช้งาน/พยาบาลประจำจุด เมื่อสงสัยว่าเครื่องติดไวรัสหรือ Ransomware ให้ทำการ "ถอดสาย LAN" หรือ "ปิดสวิตช์ Wi-Fi" ทันที เพื่อป้องกันการแพร่กระจายผ่านระบบเครือข่าย (ห้าม Shut down หรือรีสตาร์ทเครื่อง เพื่อรักษา Log และข้อมูลในหน่วยความจำชั่วคราว)
- สำหรับทีม IT หากพบการโจมตีระดับเซิร์ฟเวอร์ ให้ดำเนินการระงับช่องทางการเชื่อมต่อ (Isolate) ผ่าน Firewall FortiGate หรือตัดการเชื่อมต่อโหนด (Node) ที่มีปัญหาออกจากระบบ Proxmox Cluster ทันที

ระยะที่ ๒ การตรวจสอบและกำจัดภัยคุกคาม (Eradication)

- ทีม IT ดำเนินการตรวจสอบหาสาเหตุ ช่องโหว่ หรือเครื่องที่เป็นต้นทางของการโจมตี (Patient Zero)
- นำฮาร์ดดิสก์หรืออุปกรณ์ที่ติดเชื้อออกจากระบบ ทำความสะอาด (Wipe) หรือฟอร์แมตเพื่อติดตั้งระบบปฏิบัติการใหม่ทั้งหมด ห้ามนำอุปกรณ์ที่ยังไม่ผ่านการฆ่าเชื้อกลับเข้าเครือข่ายโดยเด็ดขาด

ระยะที่ ๓ การกู้คืนระบบ (Recovery)

- นำข้อมูลที่สำรองไว้ (Backup) จากระบบ Proxmox Backup Server (PBS) หรือจาก External SSD แบบ Offline (ที่แยกไว้ต่างหากและปลอดภัยจากการโจมตี) มาทำการ Restore เข้าสู่เครื่องแม่ข่ายหรือระบบทดแทน
- ทดสอบความสมบูรณ์ของระบบฐานข้อมูล HOSxP ก่อนเปิดให้บริการ (Go-Live) ตามปกติ

ระยะที่ ๔ การรายงานและทบทวน (Reporting & Post-Incident Activity)

- การรายงานภายใน นางศิริกัญญา ถาบุตร ดำเนินการสรุปสถานการณ์ สาเหตุ และผลกระทบรายงานต่อผู้อำนวยการโรงพยาบาล ภายใน ๒๔ ชั่วโมงหลังเกิดเหตุ
- การรายงานภายนอก (ตามมาตรฐาน PDPA และ สกมช.) หากเหตุการณ์ดังกล่าวส่งผลกระทบให้ข้อมูลสุขภาพผู้ป่วย (PHI) รั่วไหล หรือระบบโครงสร้างพื้นฐานสำคัญของโรงพยาบาลล่ม หัวหน้ากลุ่มงานฯ ต้องดำเนินการแจ้ง สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) และ สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (PDPC) ภายใน ๗๒ ชั่วโมง นับตั้งแต่ทราบเหตุการณ์