แผนการตรวจสอบและรายงานผลการประเมินช่องโหว่ระบบสารสนเทศ
(Cybersecurity Audit Plan & Report)
โรงพยาบาลพระอาจารย์มั่น ภูริทัตโต
ประจำปีงบประมาณ ๒๕๖๙

ส่วนที่ ๑ หลักการและเหตุผล (Background and Rationale)

ในยุคปัจจุบันที่เทคโนโลยีสารสนเทศเข้ามามีบทบาทสำคัญในการให้บริการทางการแพทย์ การปกป้องข้อมูลสุขภาพส่วนบุคคลของผู้ป่วย (Patient Health Information) และข้อมูลความลับของทางราชการ ถือเป็นภารกิจที่มีความสำคัญสูงสุด โรงพยาบาลพระอาจารย์มั่น ภูริทัตโต ได้ตระหนักถึงภัยคุกคามทางไซเบอร์ (Cyber Threats) ที่มีรูปแบบการโจมตีที่ซับซ้อนและทวีความรุนแรงมากขึ้น ไม่ว่าจะเป็นมัลแวร์เรียกค่าไถ่ (Ransomware) หรือการเจาะระบบเพื่อขโมยข้อมูล

ดังนั้น เพื่อให้สอดคล้องกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (PDPA) รวมถึงมาตรฐานความปลอดภัยสารสนเทศของหน่วยงานสาธารณสุข โรงพยาบาลจึงได้กำหนดให้มี "แผนการตรวจสอบและประเมินช่องโหว่ระบบสารสนเทศ (Vulnerability Assessment)" เป็นประจำทุกปี เพื่อค้นหาจุดอ่อนของระบบเครือข่าย เครื่องแม่ข่าย และระบบฐานข้อมูล นำไปสู่การวางแผนแก้ไข (Remediation) เชิงรุก ก่อนที่ผู้ไม่หวังดีจะสามารถใช้ช่องโหว่ดังกล่าวในการโจมตีระบบของโรงพยาบาลได้

ส่วนที่ ๒ วัตถุประสงค์ของการตรวจสอบ (Audit Objectives)

๒.๑. เพื่อตรวจหาช่องโหว่ (Vulnerabilities) จุดอ่อน และการตั้งค่าที่ไม่ปลอดภัย (Misconfigurations) ในระบบเครือข่ายและเครื่องแม่ข่ายที่สำคัญของโรงพยาบาล

๒.๒. เพื่อประเมินระดับความเสี่ยง (Risk Assessment) ของช่องโหว่ที่ค้นพบ โดยอ้างอิงตามมาตรฐานสากล (เช่น CVSS - Common Vulnerability Scoring System)

๒.๓. เพื่อจัดทำแนวทางและดำเนินการแก้ไขปรับปรุง (Remediation Plan) ปิดกั้นช่องโหว่ที่ตรวจพบอย่างทันท่วงที

๒.๔. เพื่อยกระดับความมั่นคงปลอดภัยของระบบสารสนเทศให้มีความพร้อมใช้งาน (Availability) มีความถูกต้องครบถ้วน (Integrity) และรักษาความลับของข้อมูล (Confidentiality) ได้อย่างมีประสิทธิภาพ

ส่วนที่ ๓ ขอบเขตและระเบียบวิธีในการตรวจสอบ (Audit Scope & Methodology)

๓.๑. ขอบเขตการตรวจสอบ (Scope) การตรวจสอบครั้งนี้มุ่งเน้นไปที่ระบบโครงสร้างพื้นฐานหลักที่มีผลกระทบต่อการให้บริการผู้ป่วย (Critical Infrastructure) จำนวน ๔ ระบบ ได้แก่

๓.๑.๑. เครื่องแม่ข่ายฐานข้อมูลหลัก (DB Master) - IP ๑๙๒.๑๖๘.๐.๒๕๔ ระบบฐานข้อมูลศูนย์กลางสำหรับให้บริการระบบสารสนเทศโรงพยาบาล (HOSxP) และแอปพลิเคชัน MedBank

๓.๑.๒. เครื่องแม่ข่ายฐานข้อมูลสำรอง (DB Slave) - IP ๑๙๒.๑๖๘.๐.๒๕๓ ระบบสำรองข้อมูลที่ทำการ Replicate แบบ Real-time

๓.๑.๓. เครื่องแม่ข่ายให้บริการเว็บไซต์ (Web Server) - IP ๑๙๒.๑๖๘.๒.๒๔๘ ระบบให้บริการแอปพลิเคชันและหน้าเว็บพอร์ทัล

๓.๑.๔. อุปกรณ์รักษาความปลอดภัยเครือข่าย (Firewall FortiGate) - IP ๑๙๒.๑๖๘.๙๙.๑ ด่านหน้าในการคัดกรองภัยคุกคามและจัดการการเข้าถึงเครือข่าย (Gateway)

๓.๒ เครื่องมือและวิธีการ (Tools and Methods) ดำเนินการโดยทีมบุคลากรศูนย์เทคโนโลยีสารสนเทศ (Internal Audit Team) ระหว่างวันที่ ๑๒ - ๑๓ มกราคม ๒๕๖๙ โดยใช้เครื่องมือวิเคราะห์ช่องโหว่อัตโนมัติ (Automated Vulnerability Scanner) ที่ได้รับการยอมรับในระดับสากล ทำการสแกนพอร์ต (Port Scanning) ตรวจสอบเวอร์ชันของบริการ (Service Enumeration) และเปรียบเทียบกับฐานข้อมูลช่องโหว่ (CVE Database)

ส่วนที่ ๔ สรุปผลการประเมินช่องโหว่ระบบสารสนเทศ (Executive Summary of Findings)

จากการดำเนินการสแกนช่องโหว่ (VA Scan) ตามวันและเวลาที่กำหนด ภาพรวมของระบบเทคโนโลยีสารสนเทศ โรงพยาบาลพระอาจารย์มั่น ภูริทัตโต "อยู่ในระดับที่มีความมั่นคงปลอดภัยสูงมาก" ไม่พบช่องโหว่ในระดับวิกฤต (Critical) และระดับสูง (High) ในทุกระบบที่ทำการตรวจสอบ ซึ่งแสดงให้เห็นถึงประสิทธิภาพในการบริหารจัดการระบบ การอัปเดตแพตช์ (Patch Management) และการตั้งค่าไฟร์วอลล์ที่รัดกุม อย่างไรก็ตาม ระบบยังตรวจพบข้อสังเกตและช่องโหว่ในระดับปานกลาง (Medium) และระดับต่ำ (Low) ซึ่งเป็นความเสี่ยงเชิงเทคนิคที่เกี่ยวข้องกับการเปิดเผยข้อมูลพื้นฐานของระบบ (Information Disclosure) และการใช้อัลกอริทึมการเข้ารหัสที่ควรได้รับการปรับปรุง ดังตารางสรุปต่อไปนี้

ลำดับ	ชื่อระบบ (Target)	IP Address	จำนวนช่องโหว่ที่พบ (แยกตามระดับความเสี่ยง)
๑	DB Master	๑๙๒.๑๖๘.๐.๒๕๔	Medium ๒ รายการ / Low ๓ รายการ
๒	DB Slave	๑๙๒.๑๖๘.๐.๒๕๓	Medium ๒ รายการ / Low ๒ รายการ
๓	Firewall	๑๙๒.๑๖๘.๙๙.๑	Medium ๒ รายการ / Low ๒ รายการ
๔	Web Server	๑๙๒.๑๖๘.๒.๒๔๘	Medium ๗ รายการ / Low ๒ รายการ

ส่วนที่ ๕ รายละเอียดผลการตรวจสอบและแผนการดำเนินการแก้ไข (Detailed Findings & Remediation Plan) คณะทำงานได้ทำการวิเคราะห์ผลกระทบและได้ดำเนินการแก้ไขปิดช่องโหว่ (Hardening & Remediation) เสร็จสิ้นแล้วในทุกรายการ โดยมีรายละเอียดผลการปฏิบัติงานดังนี้

๕.๑ การปรับปรุงความปลอดภัยของโปรโตคอล SSH (Weak MAC Algorithms Supported) ระบบที่พบ DB Master (๑๙๒.๑๖๘.๐.๒๕๔) และ Web Server (๑๙๒.๑๖๘.๒.๒๔๘)

- ความเสี่ยง (Medium) ระบบตรวจพบการอนุญาตให้เชื่อมต่อผ่านบริการ SSH (Port ๒๒) โดยใช้อัลกอริทึมการเข้ารหัส MAC แบบดั้งเดิม (เช่น umac-๖๔-etm@openssh.com, umac-

๖๔@openssh.com) ซึ่งแม้จะยังไม่สามารถเจาะได้ในทันที แต่มีความเสี่ยงต่อการถูกลดระดับความปลอดภัยในอนาคต

- การดำเนินการแก้ไข (Remediation) ผู้ดูแลระบบได้ทำการแก้ไขไฟล์ Configuration ของระบบปฏิบัติการ Linux (/etc/ssh/sshd_config) โดยยกเลิกการรองรับอัลกอริทึมแบบ ๖๔-bit และบังคับให้ผู้ดูแลระบบเชื่อมต่อผ่านอัลกอริทึมที่มีความปลอดภัยสูงขึ้นเท่านั้น พร้อมทั้งทำการรีสตาร์ทบริการ SSH เรียบร้อยแล้ว

๕.๒ การป้องกันการเปิดเผยข้อมูลระดับเครือข่าย (TCP Timestamps Information Disclosure) ระบบที่พบ ตรวจพบในทุกระบบ (DB Master, DB Slave, Firewall, Web Server)

-ความเสี่ยง (Low) ระบบปฏิบัติการมีการตอบสนองแพ็กเก็ต TCP Timestamps ตามมาตรฐาน RFC๑๓๒๓ ซึ่งผู้โจมตีอาจนำข้อมูลความหน่วงเวลาไปคำนวณระยะเวลาการเปิดเครื่อง (Uptime) เพื่อเดาเวอร์ชันของระบบปฏิบัติการ (OS Fingerprinting) ได้

-การดำเนินการแก้ไข (Remediation) ผู้ดูแลระบบได้ดำเนินการปรับแต่ง Kernel Parameters ของระบบปฏิบัติการ Linux โดยเพิ่มคำสั่ง net.ipv๔.tcp_timestamps = ๐ ลงในไฟล์ /etc/sysctl.conf เพื่อปิดการส่งข้อมูล Timestamps ออกสู่ภายนอก

๕.๓ การลดพื้นที่การโจมตีบนเครื่องให้บริการเว็บไซต์ (Attack Surface Reduction on Web Server) ระบบที่พบ Web Server (๑๙๒.๑๖๘.๒.๒๔๘)

-ความเสี่ยง (Medium) ตรวจพบการเปิดให้บริการพอร์ตที่ไม่จำเป็นต่อการแสดงผลเว็บไซต์หลายรายการ ได้แก่ พอร์ต ๒๑ (FTP), ๑๑๐ (POP๓), ๑๔๓ (IMAP) ซึ่งการเปิดพอร์ตทิ้งไว้จะเป็นการเพิ่มพื้นที่เสี่ยง (Attack Surface) ให้ผู้ไม่หวังดีทำการสแกนและหาจุดอ่อนได้

- การดำเนินการแก้ไข (Remediation) ดำเนินการปิดเซอร์วิสที่ไม่ได้ใช้งานในระดับระบบปฏิบัติการ และปรับปรุงกฎของไฟร์วอลล์ (Firewall Policy) ให้บล็อกการเข้าถึงพอร์ตดังกล่าวจากภายนอก อนุญาตเฉพาะพอร์ต ๘๐ (HTTP) และ ๔๔๓ (HTTPS) เท่านั้น

๕.๔ การควบคุมการเข้าถึงอุปกรณ์รักษาความปลอดภัย (Firewall Access Control) ระบบที่พบ Firewall FortiGate (๑๙๒.๑๖๘.๙๙.๑)

- ความเสี่ยง (Medium) พบการเปิดรับการเชื่อมต่อบนพอร์ต ๘๕๓/tcp ซึ่งเป็นบริการ DNS over TLS

- การดำเนินการแก้ไข (Remediation) ได้ทำการตรวจสอบและจำกัดสิทธิ์ (Access Control List - ACL) ให้บริการดังกล่าวสามารถถูกเรียกใช้งานได้เฉพาะจากเครือข่ายย่อย (Subnet) ของเซิร์ฟเวอร์ภายในองค์กรที่ได้รับอนุญาตเท่านั้น ป้องกันการร้องขอจากไอพีแปลกปลอม

ส่วนที่ ๖ บทสรุป (Conclusion)

การประเมินความมั่นคงปลอดภัยไซเบอร์ประจำปีงบประมาณ ๒๕๖๙ บรรลุผลตามวัตถุประสงค์ทุกประการ ผลการตรวจประเมินยืนยันว่าโครงสร้างพื้นฐานของโรงพยาบาลพระอาจารย์มั่น ภูริทัตโต มีความแข็งแกร่ง ไม่พบช่องโหว่ระดับวิกฤตที่ส่งผลกระทบต่อข้อมูลผู้ป่วย

อย่างไรก็ตาม ทางคณะทำงานศูนย์เทคโนโลยีสารสนเทศ จะยังคงเฝ้าระวัง ติดตามข่าวสารด้านภัยคุกคามอย่างต่อเนื่อง และกำหนดให้มีการสแกนระบบย่อยๆ เป็นประจำ เพื่อรักษามาตรฐานความมั่นคงปลอดภัย ให้ระบบของโรงพยาบาลพร้อมให้บริการประชาชนได้อย่างมีประสิทธิภาพและปลอดภัยสูงสุด