รายงานผลการดำเนินการตามแผนจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Execution Evidence)

โรงพยาบาลพระอาจารย์มั่น ภูริทัตโต ประจำปีงบประมาณ ๒๕๖๙

๑. วัตถุประสงค์ เพื่อรายงานความคืบหน้าและแสดงหลักฐานการปฏิบัติงานจริง (Execution Evidence) ตามแผนจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ประจำปี ๒๕๖๙ เพื่อยืนยันว่าศูนย์เทคโนโลยีสารสนเทศ โรงพยาบาลพระอาจารย์มั่น ภูริทัตโต มีมาตรการควบคุม ป้องกัน และลดผลกระทบจากความเสี่ยงทางไซเบอร์และข้อขัดข้องทางระบบโครงสร้างพื้นฐานอย่างเป็นรูปธรรม

๒. สรุปผลการดำเนินการตามแผนจัดการความเสี่ยง

๒.๑ ความเสี่ยงจากการถูกโจมตีผ่านช่องโหว่ของระบบปฏิบัติการและเครือข่าย

- มาตรการที่ดำเนินการแก้ไขและป้องกัน: (๑) ดำเนินการประเมินช่องโหว่ (VA Scan) ประจำปี ครอบคลุมระบบ DB Master, DB Slave, Web Server และ Firewall (ผลประเมินไม่พบช่องโหว่ระดับ Critical และ High) (๒) ดำเนินการปิดพอร์ตบริการที่ไม่จำเป็นบน Web Server (๓) ปรับปรุงไฟล์ sshd_config เพื่อปิดการใช้งาน Weak MAC Algorithms บนเครื่องฐานข้อมูล (๔) ปิดการส่ง TCP Timestamps ผ่าน sysctl.conf เพื่อลดการเปิดเผยข้อมูลระดับเครือข่าย
- หลักฐานที่อ้างอิง: รายงาน VA Scan จำนวน ๔ ฉบับ และภาพหน้าจอผลการรันคำสั่งตรวจสอบสถานะพอร์ตและคอนฟิกูเรชันของระบบปฏิบัติการ
- สถานะดำเนินการ : ดำเนินการแล้วเสร็จ

๒.๒ ความเสี่ยงข้อมูลสูญหายจากมัลแวร์เรียกค่าไถ่ (Ransomware) หรือระบบล่ม

- มาตรการที่ดำเนินการแก้ไขและป้องกัน: (๑) กำหนดรอบสำรองข้อมูลระดับเครื่องแม่ข่ายเสมือนเข้าสู่ระบบ Proxmox Backup Server (PBS) อัตโนมัติทุกวัน เวลา ๐๐.๐๐ น. (๒) ดำเนินการสำรองข้อมูลระดับฐานข้อมูล (HOSxP) ด้วยคำสั่ง mysqldump ทุกวัน เวลา ๒๓.๐๐ น. (๓) จัดทำ Offline Backup โดยซิงก์ข้อมูลระบบที่สำคัญลง External SSD วันละ ๒ รอบ (เวลา ๑๓.๐๐ น. และ ๒๑.๐๐ น.) โดยสลับอุปกรณ์ ๒ ชุด (๔) ดำเนินการทดสอบกู้คืนข้อมูล (Restore Test) ในวันที่ ๑ ของทุกเดือน
- หลักฐานที่อ้างอิง: ภาพหน้าจอแสดงสถานะ Job (Success/OK) ในระบบ PBS, ภาพ Log การทำงานของสคริปต์สำรองข้อมูล, และแบบฟอร์มบันทึกผลการทดสอบ Restore
- สถานะดำเนินการ : ดำเนินการแล้วเสร็จและปฏิบัติอย่างต่อเนื่อง

๒.๓ ความเสี่ยงที่ระบบจะหยุดชะงักจากฮาร์ดแวร์ขัดข้อง (Hardware Failure)

- มาตรการที่ดำเนินการแก้ไขและป้องกัน: (๑) ปรับปรุงโครงสร้างระบบเป็น Proxmox Cluster จำนวน ๓ โหนด ทำงานแบบ High Availability (HA) พร้อมตั้งค่า Watchdog Timer ที่ ๑๘๐ วินาที (๒) จัดการระบบพื้นที่เก็บข้อมูลกระจาย (Ceph Storage) โดยแก้ไขข้อขัดข้อง BLUESTORE_SLOW_OP_ALERT และปรับปรุงสคริปต์ OSD ให้ระบบทำงานสมบูรณ์ (๓) ทำการอัปเดตเฟิร์มแวร์ iDRAC เป็นเวอร์ชัน ๕.๑๐.๒๕.๐๐ และ BIOS เป็นเวอร์ชัน ๒.๒๕.๐

- หลักฐานที่อ้างอิง: ภาพหน้าจอ Proxmox VE Dashboard แสดงสถานะ Cluster ๓ Nodes และ Ceph ในสถานะ Healthy, และภาพหน้าจอระบบ iDRAC แสดงข้อมูลเวอร์ชันเฟิร์มแวร์ปัจจุบัน
- สถานะดำเนินการ : ดำเนินการแล้วเสร็จ

๒.๔ ความเสี่ยงจากการลักลอบเข้าถึงเครือข่ายและฐานข้อมูลจากภายนอก

- มาตรการที่ดำเนินการแก้ไขและป้องกัน: (๑) ปิดกั้นช่องทางการเชื่อมต่อจากภายนอกโดยตรงผ่านอุปกรณ์ Firewall FortiGate (๒) บังคับใช้ระบบเครือข่ายส่วนตัวเสมือน (WireGuard VPN) ผ่านระบบ wg-easy สำหรับผู้ดูแลระบบที่ต้องเข้าถึงเครือข่ายภายในจากระยะไกล
- หลักฐานที่อ้างอิง: ภาพหน้าจอจากระบบ wg-easy แสดงรายชื่อ Client (Peers) ที่ได้รับอนุญาต, และภาพหน้าจอแสดง Policy บน FortiGate
- สถานะดำเนินการ : ดำเนินการแล้วเสร็จและปฏิบัติอย่างต่อเนื่อง

๓. สรุปภาพรวม จากการติดตามผลการดำเนินงานตามแผนจัดการความเสี่ยง ศูนย์เทคโนโลยีสารสนเทศสามารถปฏิบัติตามมาตรการควบคุมที่กำหนดไว้ได้อย่างครบถ้วน โดยสามารถอุดช่องโหว่ที่ตรวจพบจากการประเมินได้อย่างรวดเร็ว รักษาสถานะความพร้อมใช้งานของระบบโครงสร้างพื้นฐานให้อยู่ในระดับเกณฑ์มาตรฐาน และมีระบบการสำรองข้อมูลทั้งแบบออนไลน์และออฟไลน์ที่สามารถกู้คืนได้จริง ทำให้ความเสี่ยงด้านเทคโนโลยีสารสนเทศของโรงพยาบาลอยู่ในระดับที่ยอมรับและควบคุมได้