รายงานการประเมินความเสี่ยงไซเบอร์ (Cybersecurity Risk Assessment Report)
วันที่ทำประเมิน : 17 มีนาคม 2569
ผู้จัดทำรายงาน : นาย กำชัย เสาเวียง
ชื่อระบบ : Critical Core Application เช่น Himpro, LIS
1. สรุปสำหรับผู้บริหาร (Executive Summary)
วันที่ทำการประเมิน : 17 มีนาคม 2569
วัตถุประสงค์ : การประเมินความเสี่ยงของระบบบริหารจัดการโรงพยาบาล Himpro เพื่อระบุความเสี่ยงที่เกี่ยวข้องกับข้อมูลลูกค้าที่ใช้บริการ รวมถึงหาวิธีการควบคุมที่เหมาะสม
ประเภทของการประเมิน : การประเมินความเสี่ยงครั้งแรก
ระดับความเสี่ยงโดยรวม : ระดับความเสี่ยงโดยรวมถูกประเมินว่าอยู่ในระดับ สูง
จำนวนความเสี่ยงที่ระบุทั้งหมด : 16 รายการ
ความเสี่ยงที่ยอมรับได้ (ความเสี่ยงต่ำ) : 5 รายการ
ความเสี่ยงปานกลาง: 3 รายการ
ความเสี่ยงสูง: 3 รายการ

2. รายละเอียดของรายงาน (Body of the Report)
2.1 วัตถุประสงค์ของการประเมินความเสี่ยง
1. ประเมินความเสี่ยงของระบบบริหารจัดการโรงพยาบาล (Himpro) ที่เกี่ยวข้องกับความลับ (Confidentiality), ความถูกต้อง (Integrity), และความพร้อมใช้งาน (Availability) ของผู้ใช้บริการ
2. ระบุความเสี่ยงที่อาจก่อให้เกิดปัญหากับระบบบริหารจัดการโรงพยาบาล (Himpro) รวมถึงการจัดการข้อมูลลูกค้าที่มาใช้บริการ
3. ตรวจสอบการใช้มาตรการควบคุมเพื่อปกป้องระบบจากภัยคุกคามไซเบอร์
2.2 โมเดลความเสี่ยงและวิธีการประเมิน
ใช้โมเดลความเสี่ยงตาม NIST SP 800-30 Rev. 1 ซึ่งประเมินตามความรุนแรงและโอกาสของความเสี่ยง โดยใช้คะแนนจาก 1 ถึง 5 (1 = ต่ำสุด, 5 = สูงสุด) และคำนวณคะแนนรวมเพื่อประเมินระดับความเสี่ยง

รายละเอียดความเสี่ยง (Detailed Risk Assessment) ในแต่ละ Cluster (เน้นเฉพาะ Cluster ที่มีระดับความเสี่ยงสูง เป็นหลัก

	ความเสี่ยง	ระดับความเสี่ยง	ผลกระทบที่อาจเกิดขึ้น	การควบคุมที่มีอยู่ปัจจุบัน	คำแนะนำเพิ่มเติม	คาดว่าจะเสร็จสิ้น
1	การโจมตีด้วยมัลแวร์ (Malware Attacks)	สูง	เสี่ยงการโจรกรรมข้อมูลการเงินหรือการเรียกค่าไถ่ (Ransomware) ระบบล่มทำให้สูญเสียรายได้ ข้อมูลลูกค้าหรือผู้ใช้บริการถูกขโมยทำให้สูญเสียความเชื่อมั่นความน่าเชื่อถือขององค์กรลดลง	ติดตั้งโปรแกรมป้องกันไวรัส (Antivirus) ในทุกอุปกรณ์ใช้ระบบ Endpoint Security เพื่อสแกนหาไวรัสโดยใช้ระบบ IDS/IPS ตั้งค่าการอัปเดตอัตโนมัติ	ทดสอบระบบการป้องกันมัลแวร์อย่างสม่ำเสมอ, ดำเนินการ Penetration Testing เพื่อค้นหาช่องโหว่ที่อาจถูกใช้โจมตี, จัดอบรมเกี่ยวกับการหลีกเลี่ยงการดาวน์โหลดไฟล์หรือเข้าเว็บไซต์ที่ไม่น่าเชื่อถือ	31 ธ.ค.69
2	การโจมตีด้วย phishing attacks	สูง	นอกจากจะสูญเสียเงินจำนวนมากแล้ว เหยื่อยังต้องเผชิญกับผลกระทบทางจิตใจ ครอบครัว และความสัมพันธ์อีกด้วย บางคนเกิดความเครียด ซึมเศร้า และอับอายจนไม่กล้าพูดถึงเรื่องที่เกิดขึ้น ซึ่งอาจนำไปสู่ปัญหาสุขภาพจิตในระยะยาว นอกจากนี้ การถูกหลอกลวงยังสามารถสร้างความแตกแยกในครอบครัวและลดความเชื่อมั่นต่อสังคมอีกด้วย	จัดทำนโยบายสำหรับพนักงานในการรายงานอีเมลหรือกิจกรรมที่น่าสงสัยและให้คำแนะนำเกี่ยวกับเจ้าหน้าที่ภายในองค์กร		31 ธ.ค.69

3	การโจมตีแบบ Denial of Service (DoS) และ Distributed Denial of Service (DDoS)	สูง	ส่งผลให้เว็บไซต์หรือบริการออนไลน์ล่มชั่วคราวหรือทำงานช้าลงอย่างมาก ทำให้ลูกค้าเข้าใช้งานไม่ได้ ส่งผลให้ธุรกิจสูญเสียรายได้ทันที เสียชื่อเสียงและความเชื่อมั่น ทั้งยังทำให้องค์กรมีค่าใช้จ่ายสูงในการกู้คืนระบบ และอาจถูกโจมตีซ้ำเพื่อเรียกค่าไถ่	ใช้เครื่องมือ DDoS Mitigation เช่น Cloudflare, AWS Shield, หรือ Akamai เพื่อกรองคำขอที่เป็นอันตราย	-	31 ธ.ค.69

จึงเรียนมาเพื่อทราบ

ลงชื่อ ผู้ตรวจสอบ : นางสาว ลักขณา เสาเวียง

รับทราบ :

นาย ชำนาญ สมรมิตร
ตำแหน่ง ผู้อำนวยการ
โรงพยาบาลยางชุมน้อย (CISO)