รายงานการประเมินความเสี่ยง (Risk Assessment Report)

วันที่ทำประเมิน: 22 ธ.ค. 68

ผู้จัดทำรายงาน : นาย พรศักดิ์ ตามวงค์

ชื่อระบบ: ระบบให้บริการทุกระบบ ในโรงพยาบาลแม่ลาว

---

1. สรุปสำหรับผู้บริหาร (Executive Summary)

วันที่ทำการประเมิน: 22 ธ.ค. 68

วัตถุประสงค์: การประเมินความเสี่ยงของระบบให้บริการทุกระบบ ในโรงพยาบาลแม่ลาว เพื่อระบุความเสี่ยงที่เกี่ยวข้องกับข้อมูลผู้ใช้บริการที่สำคัญและหาวิธีการควบคุมที่เหมาะสม

ขอบเขต:

ระบบข้อมูล : ประเมินการปกป้องความลับของข้อผู้ใช้บริการ และระบบให้บริการทุกระบบ ในโรงพยาบาลแม่ลาวตั้งอยู่ในศูนย์ข้อมูลหลักขององค์กร

ประเภทของการประเมิน: การประเมินความเสี่ยงครั้งแรก

ระดับความเสี่ยงโดยรวม: ระดับความเสี่ยงโดยรวมถูกประเมินว่าอยู่ในระดับ ปานกลาง

จำนวนความเสี่ยงที่ระบุ:

ความเสี่ยงต่ำ:	2 รายการ
ความเสี่ยงปานกลาง:	11 รายการ
ความเสี่ยงสูง:	3 รายการ

2. รายละเอียดของรายงาน (Body of the Report)

2.1 วัตถุประสงค์ของการประเมินความเสี่ยง

1. ประเมินความเสี่ยงของระบบให้บริการทุกระบบ ในโรงพยาบาลแม่ลาว ที่เกี่ยวข้องกับความลับ (Confidentiality), ความถูกต้อง (Integrity), และความพร้อมใช้งาน (Availability) ของข้อมูลลูกค้า
2. ระบุความเสี่ยงที่อาจก่อให้เกิดปัญหากับระบบให้บริการในโรงพยาบาลแม่ลาว รวมถึงการจัดการข้อมูลลูกค้าหรือผู้ใช้บริการที่มีความสำคัญ
3. ตรวจสอบการใช้มาตรการควบคุมเพื่อปกป้องระบบจากภัยคุกคามไซเบอร์

2.2 ข้อสมมติและข้อจำกัดในการประเมิน

สมมติว่าข้อมูลทั้งหมดที่ให้มาสำหรับการประเมินเป็นข้อมูลที่ถูกต้องและครบถ้วน ข้อจำกัดของการประเมินคือไม่สามารถเข้าถึงเซิร์ฟเวอร์เสมือนจริงที่ใช้สำรองข้อมูลได้

2.3 การยอมรับความเสี่ยง

องค์กรมีนโยบายรับความเสี่ยงในระดับ ปานกลาง โดยยอมรับความเสี่ยงบางส่วนเพื่อรักษาประสิทธิภาพในการดำเนินงาน

2.4 โมเดลความเสี่ยงและวิธีการประเมิน

ใช้โมเดลความเสี่ยงตาม NIST SP 800-30 Rev. 1 ซึ่งประเมินตามความรุนแรงและโอกาสของความเสี่ยง โดยใช้คะแนนจาก 1 ถึง 5 (1 = ต่ำสุด, 5 = สูงสุด) และคำนวณคะแนนรวมเพื่อประเมินระดับความเสี่ยง

3. รายละเอียดความเสี่ยง (Detailed Risk Assessment)

	ความเสี่ยง	ระดับความเสี่ยง	ผลกระทบที่อาจเกิดขึ้น	การควบคุมที่มีอยู่ปัจจุบัน	คำแนะนำเพิ่มเติม
1	การโจมตีด้วยมัลแวร์ (Malware Attacks)	สูง	การสูญเสียความลับของข้อมูลลูกค้าและการละเมิดข้อมูลที่สำคัญ	ใช้ Antivirus ฟรีจาก windows	จัดซื้อ Antivirus ที่ถูกลิขสิทธิ์
2	การโจมตีด้วยฟิชชิง (Phishing Attacks)	สูง	ข้อมูลสูญหาย	1.1 ให้ความรู้และฝึกอบรมพนักงาน 1.2 สร้างนโยบายรหัสผ่านที่เข้มงวด	- ตรวจสอบระบบการอัปเดตฐานข้อมูล - ให้ จนท.มีความตระหนักในการใช้งาน
3	ภัยคุกคามจากบุคคลภายใน (Insider Threats)	ปานกลาง	การสูญเสียความลับของข้อมูลลูกค้าและการละเมิดข้อมูลที่สำคัญ	การกำหนดสิทธิ์การเข้าถึง (Access Control)	ตรวจสอบสิทธิ์การเข้าถึงอย่างสม่ำเสมอ
4	การละเมิดข้อมูล (Data Breaches)	ปานกลาง	การสูญเสียความลับของข้อมูลลูกค้าและการละเมิดข้อมูลที่สำคัญ	อัปเดตระบบและซอฟต์แวร์ (Patch Management)	ตรวจสอบสิทธิ์การเข้าถึงอย่างสม่ำเสมอ
5	การโจมตีแบบ Denial of Service (DoS) และ Distributed Denial of Service (DDoS)	ปานกลาง	มีการส่งคำขอแปลกปลอมจำนวนมหาศาลทำให้ระบบหยุดชะงัก	มีการจัดการทรัพยากรระบบไม่เหมาะสม เช่น ระบบเซิร์ฟเวอร์ไม่มีแบนด์วิดท์หรือทรัพยากรเพียงพอที่จะรองรับการโจมตี	ติดตั้งระบบ WAF (Web Application Firewall) เพื่อป้องกันการโจมตีในระดับแอปพลิเคชัน

6	การโจมตีแบบ Man-in-the-Middle (MitM)	ต่ำ	ถูกปลอมแปลงเว็บไซต์ (Spoofing)	ใช้โปรโตคอล HTTPS และ TLS	บังคับให้การเชื่อมต่อทั้งหมดระหว่างเซิร์ฟเวอร์และอุปกรณ์ใช้การเข้ารหัส
7	การโจมตีด้วยแรนซัมแวร์ (Ransomware Attacks)	สูง	ถูกการโจมตีโดยใช้ช่องโหว่ในระบบหรือซอฟต์แวร์ที่ไม่ได้อัปเดต	การติดตั้งและอัปเดตซอฟต์แวร์ป้องกันแรนซัมแวร์	ใช้โปรแกรม Antivirus และ Antimalware ที่มีการตรวจจับแรนซัมแวร์โดยเฉพาะ
8	การโจมตีด้วยวิศวกรรมสังคม (Social Engineering)	ปานกลาง	ถูกการโจมตีโดยใช้ช่องโหว่ในระบบหรือซอฟต์แวร์ที่ไม่ได้อัปเดต	การติดตั้งและอัปเดตซอฟต์แวร์ป้องกันแรนซัมแวร์	ใช้โปรแกรม Antivirus และ Antimalware ที่มีการตรวจจับแรนซัมแวร์โดยเฉพาะ
9	ความเสี่ยงด้านความปลอดภัยของคลาวด์ (Cloud Security Risks)	ปานกลาง	มีการขโมยข้อมูลในระหว่างการส่งข้อมูล	การปฏิบัติตามกฎระเบียบหรือมาตรฐานความปลอดภัยของระบบคลาวด์	จำกัดการเข้าถึง API โดยการใช้ IP Whitelisting และการตั้งค่าคีย์ที่ปลอดภัย
10	ความเสี่ยงจากผู้จำหน่ายภายนอก (Third-Party Vendor Risks)	ปานกลาง	ข้อมูลระหว่างกันกับผู้จำหน่ายที่ไม่ได้มีการป้องกัน	มีข้อตกลงด้านความปลอดภัย (Security SLA)	จัดโปรแกรมการฝึกอบรมเพื่อให้ผู้จำหน่ายเข้าใจนโยบายความปลอดภัยขององค์กร
11	ความเสี่ยงของอุปกรณ์มือถือ (Mobile Device Risks) ขององค์กร	ต่ำ	มีการสูญหายหรือถูกขโมย	มีการดาวน์โหลดแอปพลิเคชันจากแหล่งที่ไม่น่าเชื่อถือ	มีการดาวน์โหลดแอปพลิเคชันจากแหล่งที่ไม่น่าเชื่อถือ
12	ซอฟต์แวร์และระบบที่มีช่องโหว่ (Vulnerable Software and Systems)	ปานกลาง	มีการสูญหายหรือถูกขโมย	มีการดาวน์โหลดแอปพลิเคชันจากแหล่งที่ไม่น่าเชื่อถือ	มีการดาวน์โหลดแอปพลิเคชันจากแหล่งที่ไม่น่าเชื่อถือ

13	ความเสี่ยงด้านความปลอดภัยของเครือข่าย (Network Security Risks)	ปานกลาง	มีการสูญหายหรือถูกขโมย	มีการดาวน์โหลดแอปพลิเคชันจากแหล่งที่ไม่น่าเชื่อถือ	มีการดาวน์โหลดแอปพลิเคชันจากแหล่งที่ไม่น่าเชื่อถือ
14	ความเสี่ยงด้านความปลอดภัยทางกายภาพ (Physical Security Risks)	ปานกลาง	เสี่ยงอุปกรณ์สูญหาย การใช้งานอุปกรณ์จากการใช้งาน	มีการเข้าถึงพื้นที่สำคัญโดยใช้ Keycard, Biometric Authentication หรือ PIN ตรวจสอบ ถังดับเพลิง กล้อง CCTV เป็นระยะ	ปรับปรุงห้องให้ได้มาตรฐานด้าน Cyber
15	ความเสี่ยงจากการไม่ปฏิบัติตามกฎระเบียบและข้อบังคับ (Regulatory and Compliance Risks)	ปานกลาง	ผลต่อข้อมูล ระบบ	กำหนดนโยบายการจัดการข้อมูลส่วนบุคคล	ฝึกอบรมให้ความรู้ PDPA แก่ จนท.ในรพ.
16	การสูญหายหรือการรั่วไหลของข้อมูล (Data Loss or Data Leakage)	ปานกลาง	ขาดการควบคุม	สร้างนโยบายองค์กรให้ตรวจสอบชื่อผู้รับอีเมล หรือผู้รับข้อมูล	จัดอบรมให้ความรู้แก่จนท. รพ ทุกท่าน

4. ภาคผนวกสนับสนุน (Supporting Appendices)

4.1 ผลการประเมินโดยละเอียด

ระบบให้บริการในโรงพยาบาลแม่ลาว ได้รับการปกป้องจากการเข้าถึงโดยไม่ได้รับอนุญาตผ่านการควบคุมการเข้าถึงที่เหมาะสม อย่างไรก็ตาม จำเป็นต้องทดสอบและอัพเดตมาตรการเป็นระยะเพื่อป้องกันภัยคุกคามใหม่ ๆ

4.2 ระยะเวลาความถูกต้องของการประเมิน

ผลการประเมินนี้มีอายุการใช้งาน 1 ปี หรือจนกว่าจะมีการเปลี่ยนแปลงระบบ จัดซื้อและจัดหา Antivirus ถูกลิขสิทธิ์

4.3 การจำแนกความเสี่ยง

ภัยคุกคามที่เกิดจากบุคคลภายนอก (Adversarial Threats): โจมตีด้วยการพยายามเข้าถึงข้อมูลที่ไม่ได้รับอนุญาต

4.4 ข้อเสนอแนะในการใช้งบประมาณ จากการที่ประเมินความเสี่ยงที่ได้ประเมินเจอความเสี่ยงสูง และปานกลาง จะต้องใช้งบประมาณในการดำเนินการแก้ไขเป็นเงินจำนวน 500,000 บาท

ภัยคุกคามที่ไม่เกิดจากบุคคลภายนอก (Non-Adversarial Threats): การสูญหายของข้อมูลจากข้อผิดพลาดในการจัดเก็บข้อมูล