



รายงานการประเมินความเสี่ยงไซเบอร์ (Cybersecurity Risk Assessment Report)

วันที่ทำประเมิน : 24 กุมภาพันธ์ 2569

ผู้จัดทำรายงาน : นายพิทักษ์พงษ์ เพี้ยเพ็งตัน (Lead Implementer)

ชื่อระบบ : **Critical Core Application** เช่น HOSxP, LIS

1. สรุปสำหรับผู้บริหาร (Executive Summary)

วันที่ทำการประเมิน : 24 ก.พ. 69

วัตถุประสงค์ : การประเมินความเสี่ยงของระบบบริหารจัดการโรงพยาบาล (HOSxP) เพื่อระบุความเสี่ยงที่เกี่ยวข้องกับข้อมูลลูกค้าที่ใช้บริการ รวมถึงหาวิธีการควบคุมที่เหมาะสม

ประเภทของการประเมิน : การประเมินความเสี่ยงครั้งแรก

ระดับความเสี่ยงโดยรวม : ระดับความเสี่ยงโดยรวมถูกประเมินว่าอยู่ในระดับ ปานกลาง

จำนวนความเสี่ยงที่ระบุทั้งหมด : 16 รายการ

ความเสี่ยงที่ยอมรับได้ (ความเสี่ยงต่ำ) : 8 รายการ

ความเสี่ยงปานกลาง: 8 รายการ

ความเสี่ยงสูง: - รายการ

2. รายละเอียดของรายงาน (Body of the Report)

2.1 วัตถุประสงค์ของการประเมินความเสี่ยง

- ประเมินความเสี่ยงของระบบบริหารจัดการโรงพยาบาล (HOSxP) ที่เกี่ยวข้องกับความลับ (Confidentiality), ความถูกต้อง (Integrity), และความพร้อมใช้งาน (Availability) ของผู้ใช้บริการ
- ระบุความเสี่ยงที่อาจก่อให้เกิดปัญหาที่ระบบบริหารจัดการโรงพยาบาล (HOSxP) รวมถึงการจัดการข้อมูลลูกค้าที่มาใช้บริการ
- ตรวจสอบการเข้ามาตรการควบคุมเพื่อปกป้องระบบจากภัยคุกคามไซเบอร์

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	การโจมตีด้วยฟิชชิ่ง (Phishing Attacks)	ความเสี่ยงปานกลาง	เสี่ยงการโดนให้กรอกข้อมูลส่วนตัวหรือข้อมูลสำคัญจาก (Call Center) หรือจากเว็บไซต์ปลอมเลียนแบบ	แนะนำให้ความรู้และฝึกอบรมพนักงาน ตรวจสอบและควบคุมการเข้าถึงเว็บไซต์	ใช้การยืนยันตัวตนแบบหลายปัจจัย ติดตั้งระบบตรวจจับและตอบสนองต่อภัยคุกคามแบบเรียลไทม์	31 ธ.ค.69

จึงเรียนมาเพื่อทราบ

ผู้จัดทำ : นายพิทักษ์พงษ์ เพี้ยเพ็งตัน (Lead Implementer)



รับทราบ :

(นายแพทย์พิริยะ ภิบาลกุล)

ผู้อำนวยการโรงพยาบาลเชาสุกิม (CISO)