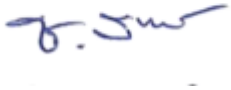
	แผนการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise Plan)	**รหัสเอกสาร**	**YCN MOPH Respond -04**
		แก้ไขครั้งที่	**00**
		วันที่บังคับใช้	**23 มี.ค. 2569**
		ชั้นความลับของเอกสาร	**ใช้ภายในเท่านั้น**

การอนุมัติเอกสาร

ลงนาม	ผู้เรียบเรียง/จัดทำโดย	**ผู้ตรวจทาน/ผู้ทบทวน**	**ผู้อนุมัติ**
ลายเซ็นต์			
ชื่อ-สกุล	นาย กำชัย เสาเวียง	นางสาว ลักขณา เสาเวียง	นพ ชำนาญ สมรมิตร
ตำแหน่ง	นักวิชาการคอมพิวเตอร์	นักวิชาการสาธารณสุชำนาญการ (Lead Implementer)	ผอ.โรงพยาบาลยางชุมน้อย (CISO)
วันเดือนปี	16 มีนาคม 2569	20 มีนาคม 2569	23 มีนาคม 2569

ประวัติการแก้ไข

ครั้งที่	**วันที่ประกาศใช้**	**รายละเอียดการแก้ไข**
00	**23 มี.ค. 2569**	**จัดทำเอกสารครั้งแรก พร้อมขึ้นระบบ พรบ ไซเบอร์**

แผนการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise Plan)

1. จัดทีมร่วมการฝึกซ้อม (Exercise Security Team)

	ตำแหน่ง	หน้าที่รับผิดชอบ	ชื่อและติดต่อ
1	หัวหน้าทีมฝึกซ้อม	กำหนดทิศทางและเป้าหมายของการฝึกซ้อม รวมถึงประสานงานกับคณะกรรมการที่เกี่ยวข้อง	นายแพทย์ ชำนาญ สมรมิตร 089-849-8162
2	ผู้เชี่ยวชาญด้านความปลอดภัยไซเบอร์	จัดทำและออกแบบสถานการณ์จำลองภัยคุกคาม รวมถึงให้คำแนะนำด้านเทคนิค	นาย กำชัย เสาเวียง 092-454-0342
3	ผู้จัดการการสื่อสาร	จัดการการสื่อสารกับพนักงานและทีมงานทั้งหมดที่มีส่วนเกี่ยวข้องในการฝึกซ้อม	นาง รัตนาภรณ์ กองสะดี 081-321-3900
4	ผู้จัดการด้าน IT	รับผิดชอบในการจัดการและตรวจสอบระบบเทคโนโลยีสารสนเทศที่เกี่ยวข้องในสถานการณ์จำลอง	นาย เสฏฐวุฒิ บุญสนิท 065-097-8559

2. การวางแผนการฝึกซ้อม (Exercise Planning)

	ขั้นตอน	รายละเอียด
1	**การรับคำสั่งและเริ่มต้นการวางแผน**	รับคำสั่งเป็นลายลักษณ์อักษรจากคณะกรรมการเพื่อเริ่มต้นการวางแผน
2	**การระบุเป้าหมายการฝึกซ้อม**	ระบุเป้าหมาย เช่น การทดสอบการตอบสนองต่อ Ransomware การตรวจสอบแผนการสื่อสารในภาวะวิกฤต
3	**การรวบรวมข้อมูลและการวิเคราะห์**	รวบรวมข้อมูลจากหน่วยงาน เช่น แผนรับมือภัยคุกคามไซเบอร์ แผนการสื่อสารในภาวะวิกฤต ข้อมูลเกี่ยวกับบริการสำคัญ
4	**การออกแบบสถานการณ์จำลอง**	ออกแบบสถานการณ์ที่เหมาะสมกับเป้าหมาย โดยคำนึงถึงความเป็นไปได้และระดับความซับซ้อนของภัยคุกคาม
5	**การกำหนดบทบาทและความรับผิดชอบ**	กำหนดบทบาทของบุคลากรที่ร่วมการฝึกซ้อม รวมถึงการกำหนดความรับผิดชอบ เช่น หัวหน้าฝ่าย IT เป็นผู้นำทีมตอบสนอง หัวหน้าฝ่ายประชาสัมพันธ์เป็นโฆษกหลักในการฝึกซ้อม

3. การดำเนินการฝึกซ้อม (Exercise Execution)

	ขั้นตอน	รายละเอียด
1	การเตรียมพร้อมก่อนการฝึกซ้อม	เตรียมความพร้อม เช่น การแจ้งเตือนทีมงานที่เกี่ยวข้องและจัดเตรียมเครื่องมือ
2	การเริ่มต้นฝึกซ้อม	แจ้งให้ทีมงานทราบถึงสถานการณ์จำลองและเริ่มต้นการฝึกซ้อม เช่น ส่งแจ้งเตือนการโจมตีแบบ Ransomware ให้ทีม IT เพื่อตอบสนองทันที
3	การตรวจสอบและบันทึกการดำเนินการ	ตรวจสอบการดำเนินงานของทีมงานและบันทึกเพื่อใช้ในการประเมินผลหลังการฝึกซ้อม
4	การดำเนินการปรับปรุงทันที	หากพบปัญหาในการฝึกซ้อม ต้องดำเนินการแก้ไขทันทีและแจ้งให้ทีมงานที่เกี่ยวข้องทราบ
5	การสรุปการฝึกซ้อม	ประเมินผลการดำเนินงานของทีมต่าง ๆ และจัดทำรายงานสรุปผลเพื่อวิเคราะห์ข้อดีและข้อผิดพลาดที่เกิดขึ้นในการฝึกซ้อม

4. การประเมินผลและการปรับปรุง (Post-exercise Evaluation and Improvement)

	ขั้นตอน	รายละเอียด
1	การประเมินผลการตอบสนอง	ประเมินความพร้อมและความเร็วในการตอบสนองของบุคลากร เช่น การรับมือกับการโจมตีแบบ Ransomware
2	การวิเคราะห์ข้อผิดพลาดและจุดที่ต้องปรับปรุง	วิเคราะห์ข้อผิดพลาดและปัญหาที่เกิดขึ้นในระหว่างการฝึกซ้อม เช่น การประสานงานที่ล่าช้าระหว่างทีม IT และฝ่ายกฎหมาย
3	การจัดทำรายงานสรุปและข้อเสนอแนะ	จัดทำรายงานสรุปและข้อเสนอแนะในการปรับปรุงแผนการรับมือภัยคุกคาม
4	การปรับปรุงแผนการรับมือภัยคุกคาม	ปรับปรุงแผนรับมือภัยคุกคามตามข้อเสนอแนะที่ได้จากการฝึกซ้อม เช่น การปรับปรุงแผนการสื่อสารในภาวะวิกฤต
5	การติดตามผลการปรับปรุง	ติดตามผลการปรับปรุงที่ดำเนินการและประเมินผลในการฝึกซ้อมครั้งถัดไป

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)