	แผนงานการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring Plan)	**รหัสเอกสาร**	KSC MOPH-Detect -04
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ ชั้นความลับของเอกสาร	1 ธ.ค.2568 ใช้ภายในเท่านั้น

การอนุมัติเอกสาร

ลงนาม	ผู้เรียบเรียง/จัดทำโดย	ผู้ตรวจทาน/ผู้ทบทวน	ผู้อนุมัติ
ลายเซ็นต์			
ชื่อ-สกุล	นางสาวศิรดา สว่างสุข	นายชัพ ธิราขันธิ์	นายภูจิตต์ ตรีบำเพ็ญ
ตำแหน่ง	นักสาธารณสุขปฏิบัติการ	นักจัดการงานทั่วไปชำนาญการ	ผู้อำนวยการโรงพยาบาลเกาะสีชัง
วันเดือนปี	24 พฤศจิกายน 2568	28 พฤศจิกายน 2568	28 พฤศจิกายน 2568

ประวัติการแก้ไข

ครั้งที่	วันที่ประกาศใช้	รายละเอียดการแก้ไข
00	1 ธ.ค. 2568	**จัดทำเอกสารครั้งแรก พร้อมขึ้นระบบ พรบ ไซเบอร์**

แผนงานการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์
(Cyber Threat Detection and Monitoring Plan)

1. วัตถุประสงค์ (Objective)
แผนงานนี้มีวัตถุประสงค์เพื่อกำหนดกลไกและกระบวนการในการตรวจจับ วิเคราะห์ และจัดการกับภัยคุกคามทางไซเบอร์ที่อาจส่งผลกระทบต่อบริการที่สำคัญของหน่วยงานของรัฐและโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

2. ขอบเขต (Scope)
แผนงานนี้ครอบคลุมการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ที่เกี่ยวข้องกับบริการที่สำคัญของหน่วยงานของรัฐและโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

3. กลไกและกระบวนการตรวจจับและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Mechanisms and Processes for Cyber Threat Detection and Monitoring)

3.1 การตรวจจับเหตุการณ์ (Event Detection)

- **กลไก**
  - ใช้ระบบ SIEM (Security Information and Event Management) ในการรวบรวมและวิเคราะห์ข้อมูลจากแหล่งต่าง ๆ เพื่อระบุเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์
  - ใช้เครื่องมือ IDS/IPS (Intrusion Detection/Prevention System) ในการตรวจจับและป้องกันการโจมตีทางไซเบอร์
- **กระบวนการ**
  - ตั้งค่าการแจ้งเตือนอัตโนมัติเมื่อพบเหตุการณ์ที่น่าสงสัยหรือมีความเสี่ยงสูง
  - จัดทำรายการเหตุการณ์ที่ต้องเฝ้าระวังเป็นพิเศษตามประเภทของภัยคุกคาม

3.2 การจัดประเภทและวิเคราะห์เหตุการณ์ (Event Classification and Analysis)

- **กลไก**
  - จัดทำกระบวนการในการจัดประเภทเหตุการณ์ตามความรุนแรงและผลกระทบที่อาจเกิดขึ้น
  - ใช้ระบบอัตโนมัติในการวิเคราะห์เหตุการณ์และระบุแนวโน้มของภัยคุกคาม
- **กระบวนการ**
  - แยกประเภทเหตุการณ์เป็นกลุ่มตามระดับความรุนแรง เช่น ต่ำ กลาง สูง
  - ใช้ข้อมูลจาก Threat Intelligence เพื่อสนับสนุนการวิเคราะห์และการตอบสนอง

3.3 การระบุและตอบสนองต่อภัยคุกคาม (Threat Identification and Response)

- **กลไก**
  - ใช้ระบบการแจ้งเตือนและการจัดการเหตุการณ์ (Incident Response) เพื่อจัดการกับภัยคุกคามที่ตรวจพบ
  - จัดตั้งทีม CSIRT (Computer Security Incident Response Team) เพื่อรับผิดชอบการตอบสนองต่อภัยคุกคาม
- **กระบวนการ:**
  - ทบทวนและวิเคราะห์เหตุการณ์ที่เกิดขึ้นเพื่อระบุว่าเป็นภัยคุกคามจริงหรือไม่
  - หากพบว่ามีภัยคุกคาม ให้ดำเนินการตามแผนการตอบสนองที่กำหนดไว้ เช่น การกักกัน การวิเคราะห์ การแก้ไข และการฟื้นฟู

4. **การทบทวนกลไกและกระบวนการ** (Review of Mechanisms and Processes)
   - **ความถี่:** ดำเนินการทบทวนกลไกและกระบวนการตรวจจับและเฝ้าระวังภัยคุกคามทางไซเบอร์อย่างน้อยปีละ 1 ครั้ง
   - **ขั้นตอน**
     - ตรวจสอบประสิทธิภาพของกลไกและกระบวนการที่มีอยู่
     - ปรับปรุงและอัปเดตตามความจำเป็นเพื่อให้มั่นใจว่ายังคงมีประสิทธิภาพในการเฝ้าระวังและตอบสนองต่อภัยคุกคามใหม่ ๆ
     - จัดทำรายงานผลการทบทวนและนำเสนอให้กับผู้บริหารเพื่อการอนุมัติและดำเนินการต่อไป

5. **ความรับผิดชอบ** (Responsibilities)
   - **ทีม IT:** รับผิดชอบการตรวจจับเหตุการณ์และการแจ้งเตือนอัตโนมัติ
   - **ทีมความมั่นคงปลอดภัยไซเบอร์:** รับผิดชอบการจัดประเภทและวิเคราะห์เหตุการณ์
   - **ทีม CSIRT:** รับผิดชอบการระบุและตอบสนองต่อภัยคุกคาม รวมถึงการทบทวนและปรับปรุงกระบวนการ

6. **การบันทึกและรายงาน** (Documentation and Reporting)
   - **การบันทึก:** จัดทำบันทึกเหตุการณ์ที่เกิดขึ้นและผลการวิเคราะห์ในระบบการจัดการเหตุการณ์
   - **การรายงาน:** รายงานผลการตรวจจับและวิเคราะห์เหตุการณ์ให้กับผู้บริหารเป็นระยะ ๆ และเมื่อมีเหตุการณ์สำคัญที่ส่งผลต่อความมั่นคงปลอดภัยไซเบอร์