	นโยบายการบริหารจัดการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Management System Policy)	**รหัสเอกสาร**	KSC MOPH-Policy-01
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ **ชั้นความลับเอกสาร** **ของเอกสาร**	1 ธ.ค.68 ใช้ภายในเท่านั้น

การอนุมัติเอกสาร

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

ประวัติการแก้ไข

ครั้งที่	วันที่ประกาศใช้	รายละเอียดการแก้ไข
00	1 ธันวาคม 2568	**จัดทำเอกสารครั้งแรก พร้อมขึ้นระบบ พรบ ไซเบอร์**

นโยบายการบริหารจัดการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Management System Policy)

อ้างอิง : พรบ ไซเบอร์ (ม.43, ม.44, ม.45, ม.46, ม.54, ม.56), นโยบาย [ข้อ 1.1, ข้อ 1.3, ข้อ 2.1, ข้อ 2.2, ข้อ 2.3, ข้อ 3.1, ข้อ 3.2], ประมวลและกรอบ [ข้อ 18]

1. วัตถุประสงค์ นโยบายฉบับนี้จัดทำขึ้นเพื่อกำหนดแนวทางและมาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์และข้อมูลสารสนเทศ ให้เป็นไปตามมาตรฐานที่กำหนดใน แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกระทรวงสาธารณสุข และ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 รวมถึงแนวปฏิบัติที่เกี่ยวข้องกับมาตรฐานสากล เช่น ISO/IEC 27001:2022

2. ขอบเขตการใช้งาน นโยบายนี้ครอบคลุมระบบเทคโนโลยีสารสนเทศทั้งหมดของโรงพยาบาลเกาะสีชังรวมถึงเครือข่าย อุปกรณ์สารสนเทศ ซอฟต์แวร์ บริการคลาวด์ และข้อมูลที่อยู่ภายในและภายนอกโรงพยาบาลเกาะสีชัง ตลอดจนบุคลากรทุกระดับ ผู้รับเหมา และบุคคลภายนอกที่เกี่ยวข้องกับระบบสารสนเทศของโรงพยาบาลเกาะสีชัง

3. นิยาม

- **ข้อมูลสารสนเทศ** หมายถึง ข้อมูลที่มีการจัดเก็บ ใช้งาน หรือประมวลผลผ่านระบบสารสนเทศของโรงพยาบาลเกาะสีชัง ไม่ว่าจะอยู่ในรูปแบบอิเล็กทรอนิกส์หรือกายภาพ
- **ระบบสารสนเทศ** หมายถึง โครงสร้างพื้นฐานทางเทคโนโลยี รวมถึงฮาร์ดแวร์ ซอฟต์แวร์ เครือข่าย และฐานข้อมูล
- **ความมั่นคงปลอดภัยสารสนเทศ (Information Security)** หมายถึง การปกป้องข้อมูลจากการเข้าถึงโดยไม่ได้รับอนุญาต การถูกเปิดเผย การถูกเปลี่ยนแปลง หรือการถูกทำลาย

- **ภัยคุกคามไซเบอร์** หมายถึง กิจกรรมหรือเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ เช่น การโจมตีแบบมัลแวร์ ฟิชชิ่ง หรือการรั่วไหลของข้อมูล
- **เจ้าของข้อมูล** หมายถึง บุคคลหรือหน่วยงานที่รับผิดชอบดูแลข้อมูลให้มีความปลอดภัย

4. ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

4.1 การจัดทำประมวลแนวทางปฏิบัติ ตาม พ.ร.บ. ไซเบอร์ เพื่อให้เป็นไปตามมาตรา ๕๐ ของ พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562
โรงพยาบาลเกาะสีชังดำเนินการจัดทำ ประมวลแนวทางปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์ ซึ่งมีองค์ประกอบ 3 ส่วนหลัก ได้แก่

1. **แผนการตรวจสอบ (Audit Plan)**
    - ดำเนินการตรวจสอบระบบความมั่นคงปลอดภัยไซเบอร์เป็นระยะ
    - ตรวจสอบการปฏิบัติตามมาตรฐาน เช่น ISO/IEC 27001 และ NIST CSF 2.0
2. **การประเมินความเสี่ยง (Risk Assessment)**
    - วิเคราะห์ภัยคุกคามและช่องโหว่ที่อาจส่งผลกระทบต่อโรงพยาบาลเกาะสีชัง
    - ใช้กรอบการบริหารความเสี่ยง เช่น ISO/IEC 27005
3. **แผนการรับมือ (Incident Response Plan)**
    - จัดทำแผนรับมือเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ที่ครอบคลุม
    - ประสานงานกับหน่วยงานภายนอก เช่น ThaiCERT และ สกมช.

4.2 กรอบมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อให้สอดคล้องกับ แนวทางของ พ.ร.บ. ไซเบอร์ พ.ศ. 2562

โรงพยาบาลเกาะสีชังดำเนินการภายใต้ 6 องค์ประกอบหลัก ได้แก่

1. **การกำกับดูแล (Governance)**
   - กำหนดโครงสร้างการบริหารจัดการด้านความมั่นคงปลอดภัยไซเบอร์
   - ปฏิบัติตามมาตรฐานและกฎหมายที่เกี่ยวข้อง เช่น พ.ร.บ. ไซเบอร์ และ พ.ร.บ. คอมพิวเตอร์
   - ดำเนินการตรวจสอบและประเมินผลอย่างต่อเนื่องเพื่อให้มั่นใจว่ามาตรการที่กำหนดสามารถป้องกันภัยคุกคามไซเบอร์ได้
2. **การระบุความเสี่ยง (Identify)**
   - กำหนดขอบเขตของสินทรัพย์สารสนเทศที่ต้องคุ้มครอง
   - จัดทำทะเบียนสินทรัพย์สารสนเทศ (Asset Inventory) และกำหนดระดับความสำคัญ
   - ประเมินความเสี่ยงด้านไซเบอร์อย่างต่อเนื่อง (Cyber Risk Assessment)
   - วิเคราะห์ผลกระทบจากภัยคุกคามไซเบอร์ (Impact Analysis)
   - ระบุความสัมพันธ์ของระบบและบริการภายในโรงพยาบาลเกาะสีชัง
3. **การป้องกัน (Protect)**
   - กำหนดมาตรการควบคุมการเข้าถึงข้อมูล (Access Control)
   - ใช้ Zero Trust Architecture เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต
   - ใช้การเข้ารหัสข้อมูล (Encryption) ในการปกป้องข้อมูลที่สำคัญ
   - กำหนดนโยบายรหัสผ่านที่แข็งแกร่ง และบังคับใช้ Multi-Factor Authentication (MFA)
   - ฝึกอบรมพนักงานเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์อย่างสม่ำเสมอ

4. **การเฝ้าระวัง (Detect)**
   - ใช้ ระบบเฝ้าระวังภัยคุกคาม (Security Information and Event Management – SIEM)
   - ติดตั้ง **ระบบตรวจจับและป้องกันการบุกรุก** (IPS/IDS)
   - วิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์ (Log Analysis) เพื่อตรวจจับพฤติกรรมที่ผิดปกติ
   - ใช้ Threat Intelligence ในการติดตามและคาดการณ์ภัยคุกคามล่วงหน้า
5. **การตอบสนอง (Respond)**
   - จัดทำ แผนรับมือเหตุการณ์ไซเบอร์ (Incident Response Plan – IRP)
   - กำหนดกระบวนการสื่อสารภายในโรงพยาบาลเกาะสีชังเมื่อเกิดเหตุการณ์ด้านความมั่นคงปลอดภัย
   - มีการรายงานและประสานงานกับหน่วยงานที่เกี่ยวข้อง เช่น ThaiCERT และ สกมช.
   - ฝึกอบรมพนักงานเกี่ยวกับกระบวนการตอบสนองต่อเหตุการณ์เป็นระยะ
   - จัดทำ แผนรับมือเหตุการณ์ไซเบอร์ (Incident Response Plan – IRP)
   - กำหนดแนวทางการสื่อสารเมื่อเกิดเหตุการณ์ด้านความมั่นคงปลอดภัย
   - ฝึกอบรมและซักซ้อมแผนตอบสนองภัยคุกคามอย่างสม่ำเสมอให้กับบุคลากร
   - การคัดกรองบุคลากรที่เกี่ยวข้องกับระบบสารสนเทศ (Background Check)
   - การควบคุมการเข้าถึงและกำหนดสิทธิ์ของผู้ใช้งานตามหน้าที่ความรับผิดชอบ (Least Privilege Access)
   - การดำเนินการเมื่อพนักงานลาออกหรือเปลี่ยนหน้าที่ (Offboarding & Role Change Security)
6. **การฟื้นฟู (Recover)**
   - **จัดทำ** แผนกู้คืนระบบ (Disaster Recovery Plan – DRP) และแผนดำเนินธุรกิจต่อเนื่อง (Business Continuity Plan – BCP)
   - กำหนด Recovery Time Objective (RTO) และ Recovery Point Objective (RPO)

- ทดสอบการกู้คืนข้อมูลและระบบเป็นระยะ
- ปรับปรุงกระบวนการฟื้นฟูให้มีประสิทธิภาพมากขึ้นหลังจากเกิดเหตุการณ์ความมั่นคงปลอดภัย

ในขณะที่ ISO/IEC 27001 : 2022 นั้น โรงพยาบาลเกาะสีชังดำเนินการภายใต้ 4 องค์ประกอบหลัก ได้แก่

1. **มาตรการควบคุมด้านองค์กร (Organizational Controls)**
   - การกำหนดนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ
   - การบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์
   - การบริหารจัดการความต่อเนื่องทางธุรกิจและการกู้คืนระบบ (BCP & DRP)
   - การบริหารจัดการซัพพลายเชนและบุคคลภายนอกที่เกี่ยวข้องกับระบบสารสนเทศ
   - การดำเนินการตรวจสอบและติดตามการปฏิบัติตามข้อกำหนด
2. **มาตรการควบคุมด้านกายภาพ (Physical Controls)**
   - การกำหนดมาตรการควบคุมการเข้าถึงอาคาร สำนักงาน และศูนย์ข้อมูล (Data Center Security)
   - การป้องกันการเข้าถึงอุปกรณ์สารสนเทศที่ไม่ได้รับอนุญาต (Unauthorized Physical Access)
   - การจัดทำมาตรการป้องกันภัยธรรมชาติ เช่น ไฟไหม้ น้ำท่วม แผ่นดินไหว (Disaster Prevention)
   - การกำหนดมาตรการป้องกันการโจรกรรมอุปกรณ์และสื่อบันทึกข้อมูล
   - การตรวจสอบและบันทึกการเข้าถึงสถานที่ที่มีข้อมูลสำคัญ (Access Logs & Surveillance)

3. **มาตรการควบคุมด้านเทคโนโลยี (Technological Controls)**
   - การใช้ การเข้ารหัสข้อมูล (Data Encryption) เพื่อปกป้องข้อมูลที่สำคัญ
   - การกำหนด นโยบายรหัสผ่านที่แข็งแกร่ง (Strong Password Policy) และ Multi-Factor Authentication (MFA)
   - การติดตั้ง ระบบตรวจจับและป้องกันการบุกรุก (IPS/IDS – Intrusion Prevention & Detection System)
   - การใช้ ไฟร์วอลล์ (Firewall) และ ระบบเฝ้าระวังความปลอดภัย (SIEM – Security Information and Event Management)
   - การจัดทำ นโยบายหรือคู่มือการสำรองข้อมูล (Backup & Recovery Policy) และทดสอบการกู้คืนข้อมูลเป็นระยะ

5. การปฏิบัติตามกฎหมายและมาตรฐาน (Compliance with Laws and Standards)

- การปฏิบัติตามข้อกำหนด (Regulatory Compliance): โรงพยาบาลเกาะสีชังจะปฏิบัติตามกฎหมาย ข้อบังคับ และมาตรฐานที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์อย่างเคร่งครัด
- การประเมินและตรวจสอบ (Assessment and Audits): โรงพยาบาลเกาะสีชังจะดำเนินการประเมินและตรวจสอบภายในเป็นระยะเพื่อให้มั่นใจว่าการปฏิบัติตามข้อกำหนดและนโยบายด้านความมั่นคงปลอดภัยไซเบอร์เป็นไปอย่างเหมาะสม

6. การจัดทำเอกสารและการจัดเก็บข้อมูล (Documentation and Record Keeping)

- การจัดทำเอกสาร (Documentation): โรงพยาบาลเกาะสีชังจะดำเนินการจัดทำเอกสารที่เกี่ยวข้องกับการดำเนินการด้านความมั่นคงปลอดภัยไซเบอร์อย่างครบถ้วนและถูกต้อง
- การจัดเก็บและเข้าถึงข้อมูล (Record Keeping and Access): เอกสารและข้อมูลทั้งหมดจะถูกจัดเก็บอย่างปลอดภัย และจะต้องสามารถเข้าถึงได้เมื่อจำเป็นสำหรับการตรวจสอบหรือใช้งานในอนาคต

การทบทวนนโยบาย (Policy Review)

นโยบายนี้จะได้รับการทบทวนเป็นประจำทุกปีหรือตามความจำเป็นเพื่อให้มั่นใจในประสิทธิภาพและและถ้ามีการเปลี่ยนแปลงนโยบายนี้จะต้องมีการสื่อสารไปยังทุกฝ่ายที่ได้รับผลกระทบหรือทุกฝ่ายที่เกี่ยวข้องทราบ