	นโยบายการบริหารจัดการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Management System Policy)	**รหัสเอกสาร**	MLH-MOPH-Policy-01
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ **ชั้นความลับเอกสาร** **ของเอกสาร**	5 ม.ค 2569 ใช้ภายในเท่านั้น

การอนุมัติเอกสาร

ลงนาม	ผู้เรียบเรียง/จัดทำโดย	ผู้ตรวจทาน/ผู้ทบทวน	ผู้อนุมัติ
ลายเซ็นต์			
ลงนาม	ผู้เรียบเรียง/จัดทำโดย	ผู้ตรวจทาน/ผู้ทบทวน	ผู้อนุมัติ
ลายเซ็นต์			
ลงนาม	ผู้เรียบเรียง/จัดทำโดย	ผู้ตรวจทาน/ผู้ทบทวน	ผู้อนุมัติ

ประวัติการแก้ไข

ครั้งที่	วันที่ประกาศใช้	รายละเอียดการแก้ไข
00	5 ม.ค 2569	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

2. ขอบเขตการใช้งาน นโยบายนี้ครอบคลุมระบบเทคโนโลยีสารสนเทศทั้งหมดขององค์กร รวมถึงเครือข่าย อุปกรณ์สารสนเทศ ซอฟต์แวร์ บริการคลาวด์ และข้อมูลที่อยู่ภายในและภายนอกองค์กร ตลอดจนบุคลากรทุกระดับ ผู้รับเหมา และบุคคลภายนอกที่เกี่ยวข้องกับระบบสารสนเทศขององค์กร

3. นิยาม

- **ข้อมูลสารสนเทศ** หมายถึง ข้อมูลที่มีการจัดเก็บ ใช้งาน หรือประมวลผลผ่านระบบสารสนเทศขององค์กร 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

องค์กรดำเนินการจัดทำ ประมวลแนวทางปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์ ซึ่งมีองค์ประกอบ 3 ส่วนหลัก ได้แก่

1. **แผนการตรวจสอบ (Audit Plan)**
    - ดำเนินการตรวจสอบระบบความมั่นคงปลอดภัยไซเบอร์เป็นระยะ
    - ตรวจสอบการปฏิบัติตามมาตรฐาน เช่น ISO/IEC 27001 และ NIST CSF 2.0 และมาตรฐาน พรบ ไซเบอร์ 2562
2. **การประเมินความเสี่ยง (Risk Assessment)**
    - วิเคราะห์ภัยคุกคามและช่องโหว่ที่อาจส่งผลกระทบต่อองค์กร
    - ใช้กรอบการบริหารความเสี่ยง เช่น ISO/IEC 27005
3. **แผนการรับมือ (Incident Response Plan)**
    - จัดทำแผนรับมือเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ที่ครอบคลุม
    - ประสานงานกับหน่วยงานภายนอก เช่น ThaiCERT และ สกมช.และ สสจ

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

องค์กรดำเนินการภายใต้ 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)
    - ระบุความสัมพันธ์ของระบบและบริการภายในองค์กร
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)
    - กำหนดกระบวนการสื่อสารภายในองค์กรเมื่อเกิดเหตุการณ์ด้านความมั่นคงปลอดภัย
    - 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

เพิ่มเติม : - การใช้ทรัพยากรสารสนเทศอย่างเหมาะสม (Acceptable Use)

ความรับผิดชอบส่วนบุคคล (Individual Responsibility)

1. บุคคลใด ๆ ต้องไม่กระทำการ ดังต่อไปนี้

1.1. อนุญาตให้บุคคลอื่นใช้บัญชีผู้ใช้หรือข้อมูลรับรองของตนเองในการเข้าถึงระบบและแอปพลิเคชันของโรงพยาบาลแม่ลาว

1.2. ปล่อยให้บัญชีผู้ใช้ของตนยังคงเข้าสู่ระบบอยู่บนคอมพิวเตอร์ที่ไม่มีผู้ดูแลหรือไม่ได้ล็อกหน้าจอ

1.3. ใช้บัญชีผู้ใช้หรือข้อมูลรับรองของบุคคลอื่นในการเข้าถึงระบบหรือแอปพลิเคชันของโรงพยาบาลแม่ลาว

1.4. ดำเนินการเปลี่ยนแปลงระบบ แอปพลิเคชัน หรือข้อมูลของโรงพยาบาลแม่ลาวโดยไม่ได้รับอนุญาต

1.5. พยายามเข้าถึงข้อมูลหรือสารสนเทศที่ตนไม่ได้รับสิทธิ์ให้เข้าถึง

1.6. เชื่อมต่ออุปกรณ์ที่ไม่ได้รับอนุญาตจากโรงพยาบาลแม่ลาว เข้ากับระบบหรือแอปพลิเคชันของโรงพยาบาลแม่ลาวโดยไม่ได้รับอนุมัติ

1.7. เก็บรักษาข้อมูลของโรงพยาบาลแม่ลาว ไว้ในอุปกรณ์ที่ไม่ได้รับอนุญาตจากโรงพยาบาลแม่ลาว

1.8. มอบหมาย ส่งต่อ หรือถ่ายโอนข้อมูลหรือซอฟต์แวร์ของโรงพยาบาลแม่ลาว ให้แก่บุคคลหรือองค์กรภายนอก โดยไม่ได้รับอนุมัติจากฝ่ายบริหาร (Management)

2. บุคคลต้องรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศทั้งหมดโดยทันที ตามขั้นตอนที่กำหนดไว้ในเอกสาร

2.1. การเข้าถึงระบบโดยไม่ได้รับอนุญาต (Unauthorized Access) ความพยายามหลอกลวงทางอีเมล (Phishing Attempts) และกิจกรรมที่น่าสงสัย (Suspicious Activities) ต้องได้รับการแจ้งเตือนและส่งต่อให้หน่วยงานที่เกี่ยวข้องโดยไม่ชักช้า

อินเตอร์เน็ตและการใช้อีเมล (Internet and Email Usage)

3. การใช้งานอินเทอร์เน็ตและอีเมลของโรงพยาบาลแม่ลาว มีวัตถุประสงค์เพื่อใช้ในการดำเนินงานทางธุรกิจของโรงพยาบาลแม่ลาวเท่านั้น

3.1. การใช้งานส่วนบุคคลสามารถกระทำได้ในกรณีที่ไม่ส่งผลกระทบต่อประสิทธิภาพการทำงานของบุคคลนั้น ไม่ก่อให้เกิดความเสียหายต่อโรงพยาบาลแม่ลาว ในทางใดทางหนึ่ง, ไม่ขัดต่อเงื่อนไขการจ้างงาน และไม่ก่อให้เกิดการละเมิดกฎหมาย ข้อบังคับ หรือพันธกรณีทางกฎหมายใด ๆ ทั้งต่อบุคคลหรือโรงพยาบาลแม่ลาว

4. บุคคลทุกคนต้องรับผิดชอบต่อการกระทำของตนในการใช้งานอินเทอร์เน็ตและระบบอีเมลของโรงพยาบาลแม่ลาว

5. ห้ามใช้อินเทอร์เน็ตหรืออีเมลเพื่อการคุกคาม ล่วงละเมิด หรือส่งข้อความหยาบคาย ดูหมิ่น หรือใช้ถ้อยคำไม่เหมาะสมในช่องทางการสื่อสาร

6. ห้ามเข้าถึง ดาวน์โหลด ส่งต่อ หรือรับข้อมูล (รวมถึงภาพและวิดีโอ) ที่โรงพยาบาลแม่ลาว เห็นว่าไม่เหมาะสม เช่น เนื้อหาลามกอนาจาร การเลือกปฏิบัติ การหมิ่นประมาท หรือข้อมูลที่มีลักษณะใส่ร้ายผู้อื่น
7. ห้ามใช้อีเมลของโรงพยาบาลแม่ลาว เพื่อแสวงหาผลประโยชน์ส่วนตน ดำเนินธุรกิจส่วนตัว หรือเล่นการพนัน
8. ห้ามใช้อีเมลในลักษณะที่อาจกระทบต่อความน่าเชื่อถือหรือประสิทธิภาพของระบบ เช่น การส่งต่อจดหมายลูกโซ่ (Chain Letters) หรือสแปม (Spam)
9. ห้ามเผยแพร่ข้อมูลใด ๆ ที่เกี่ยวข้องกับโรงพยาบาลแม่ลาว บนอินเทอร์เน็ต เว้นแต่ได้รับอนุญาตอย่างเป็นทางการ
10. ห้ามส่งข้อมูลภายในหรือข้อมูลลับของโรงพยาบาลแม่ลาว ออกไปภายนอกโดยไม่มีการป้องกัน (Unprotected Transmission)
11. ห้ามดาวน์โหลด ติดตั้ง หรือแจกจ่ายซอฟต์แวร์จากอินเทอร์เน็ตโดยไม่ได้รับอนุมัติจากฝ่าย IT
12. ห้ามเชื่อมต่ออุปกรณ์ของโรงพยาบาลแม่ลาว เข้ากับอินเทอร์เน็ตโดยใช้การเชื่อมต่อที่ไม่ได้มาตรฐานหรือไม่ได้รับอนุญาต
13. ห้ามดาวน์โหลดหรือใช้ผลงานที่มีลิขสิทธิ์โดยไม่ได้รับอนุญาต หรือกระทำการละเมิดทรัพย์สินทางปัญญาในทุกรูปแบบ
14. ทรัพย์สินทางปัญญาทั้งหมด เช่น เอกสาร รายงาน แบบร่าง บันทึก สเปรดชีต หรือข้อมูลอื่นใดที่บุคคลจัดทำขึ้นในระหว่างการปฏิบัติงาน ถือเป็นกรรมสิทธิ์ของโรงพยาบาลแม่ลาว ตั้งแต่เวลาที่สร้างหรือพัฒนา
15. ห้ามโอนหรือเก็บข้อมูลลับของโรงพยาบาลแม่ลาว หรือของลูกค้าไว้ในอุปกรณ์ส่วนตัว หรือบริการของบุคคลที่สาม โดยไม่ได้รับอนุมัติจากฝ่าย IT
16. ห้ามใช้แอปพลิเคชันของบุคคลที่สามที่ไม่ได้รับอนุมัติ (รวมถึงบริการคลาวด์ เช่น Dropbox หรืออีเมลส่วนตัว) เพื่อจัดการหรือประมวลผลข้อมูลลับของโรงพยาบาลแม่ลาว

17. ห้ามติดตั้ง เปิดใช้งาน หรือใช้อุปกรณ์หรือบริการใด ๆ ที่มีเจตนาในการบันทึกเสียง ภาพ หรือถ่ายทอดข้อมูลการประชุมลับของ**โรงพยาบาลแม่ลาว** หรือของลูกค้าผู้ใช้บริการโดยไม่ได้รับอนุญาต
18. ห้ามสอดแนมหรือบันทึกภาพ/เสียงบุคคลอื่นโดยไม่ได้รับอนุญาต รวมถึงการบันทึกที่ทำขึ้นเพื่อใช้จัดทำรายงานการประชุมหรือเพื่อเผยแพร่ให้บุคคลที่ได้รับอนุญาตสามารถรับชมภายหลังได้ ถือว่าได้รับอนุญาตตามนโยบายนี้ แต่ต้องมีการแจ้งให้ทราบล่วงหน้าก่อนเริ่มการประชุมทุกครั้ง

การใช้เทคโนโลยีปัญญาประดิษฐ์ (AI use)

19. การใช้งานเครื่องมือหรือบริการคลาวด์ที่ขับเคลื่อนด้วยปัญญาประดิษฐ์ (AI) ต้องจำกัดอยู่เฉพาะวัตถุประสงค์ที่ถูกต้องตามกฎหมายและกำหนดไว้อย่างชัดเจนเท่านั้น
20. ห้ามใช้เครื่องมือหรือบริการ AI เพื่อกระทำการละเมิดกฎหมาย ทำลายความมั่นคงของระบบ หรือสร้างความเสียหายต่อผู้ใช้งานทั้งภายในและภายนอกโรงพยาบาลแม่ลาว
21. ห้ามนำข้อมูลที่เป็นความลับหรือข้อมูลอ่อนไหวของโรงพยาบาลแม่ลาวไปป้อนหรือแบ่งปันให้กับระบบ AI ที่สร้างเนื้อหา (Generative AI) เว้นแต่เป็นส่วนหนึ่งของกระบวนการที่ได้รับอนุมัติจากหน่วยงานหรือแผนกที่เกี่ยวข้อง
22. ห้ามใช้เทคโนโลยี AI ในการสร้าง ปลอมแปลง หรือเผยแพร่ข้อมูลที่บิดเบือน หลอกลวง หรืออาจทำให้เกิดความเข้าใจผิดในทุกกรณี

การตรวจสอบกิจกรรม (Monitoring)

23. ข้อมูลทั้งหมดที่ถูกสร้างขึ้นหรือจัดเก็บอยู่ในอุปกรณ์ของโรงพยาบาลแม่ลาว ถือเป็นทรัพย์สินของโรงพยาบาลแม่ลาว แต่เพียงผู้เดียว
24. โรงพยาบาลแม่ลาว มีสิทธิ์ในการตรวจสอบกิจกรรมทั้งหมดที่เกิดขึ้นบนระบบและอุปกรณ์ของโรงพยาบาลแม่ลาว รวมถึงการใช้งานอินเทอร์เน็ตและอีเมล เพื่อให้มั่นใจในความมั่นคงปลอดภัยของระบบ การดำเนินงานที่มีประสิทธิภาพ และเพื่อป้องกันการใช้งานในทางที่ผิดหรือไม่ได้รับอนุญาต

การปฏิบัติตามกฎหมายและมาตรฐาน (Compliance with Laws and Standards)

- การปฏิบัติตามข้อกำหนด (Regulatory Compliance): โรงพยาบาลแม่ลาว จะปฏิบัติตามกฎหมาย ข้อบังคับ และมาตรฐานที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์อย่างเคร่งครัด
- การประเมินและตรวจสอบ (Assessment and Audits): โรงพยาบาลแม่ลาว จะดำเนินการประเมินและตรวจสอบภายในเป็นระยะเพื่อให้มั่นใจว่าการปฏิบัติตามข้อกำหนดและนโยบายด้านความมั่นคงปลอดภัยไซเบอร์เป็นไปอย่างเหมาะสม

การทบทวนนโยบาย (Policy Review)

นโยบายนี้จะได้รับการทบทวนเป็นประจำทุกปีหรือตามความจำเป็นเพื่อให้มั่นใจในประสิทธิภาพและและถ้ามีการเปลี่ยนแปลงนโยบายนี้จะต้องมีการสื่อสารไปยังทุกฝ่ายที่ได้รับผลกระทบหรือทุกฝ่ายที่เกี่ยวข้องทราบ