	นโยบายการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Management Policy)	**รหัสเอกสาร**	MLH-MOPH - Policy-02
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ ชั้นความลับของเอกสาร	5 ม.ค 2569 ใช้ภายในเท่านั้น

การอนุมัติเอกสาร

ลงนาม	ผู้เรียบเรียง/จัดทำโดย	ผู้ตรวจทาน/ผู้ทบทวน	ผู้อนุมัติ
ลายเซ็นต์			
ชื่อ-สกุล	นายสุทธิชัย เสาว์สิงห์	นายพรศักดิ์ ตามวงค์	นพ.สุขชัย เธียรเศวตตระกูล
ตำแหน่ง	นักวิชาการคอมพิวเตอร์	นักวิชาการคอมพิวเตอร์ชำนาญการ	ผู้อำนวยการโรงพยาบาลแม่ลาว
วันเดือนปี	22 ธันวาคม 2568	30 ธันวาคม 2568	5 มกราคม 2569

ประวัติการแก้ไข

ครั้งที่	วันที่ประกาศใช้	รายละเอียดการแก้ไข
00	5 ม.ค 2569	จัดทำเอกสารครั้งแรก พร้อมขึ้นระบบ พรบ ไซเบอร์

นโยบายการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Management Policy)

อ้างอิง : พรบ ไซเบอร์ (ม.43, ม.44, ม.54), นโยบาย (ข้อ 2.1, ข้อ 2.2, ข้อ 2.3, ข้อ 3.1, ข้อ 3.2), ประมวลและกรอบ [ข้อ 18, ข้อ 18.1(ก), ข้อ 18.1(ข), ข้อ 18.1(ค), ข้อ 18.2, ข้อ 18.2(ข), ข้อ 18.3, ข้อ 18.4, ข้อ 21.1.4, ข้อ 21.2.1, ข้อ 21.2.2, ข้อ 21.3.1]

1. วัตถุประสงค์ (Objective)

วัตถุประสงค์ของนโยบายนี้คือเพื่อกำหนดกรอบการทำงานสำหรับการระบุ ประเมิน และบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อให้แน่ใจว่าหน่วยงานที่มีโครงสร้างพื้นฐานและบริการที่สำคัญได้รับการปกป้องจากภัยคุกคามไซเบอร์ นโยบายนี้สอดคล้องกับนโยบายความมั่นคงปลอดภัยทางไซเบอร์ของประเทศไทย โดยเฉพาะ **พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562** และ **นโยบายความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 - 2570)**

2. ขอบเขต (Scope)

นโยบายนี้ครอบคลุมถึงหน่วยงาน แผนก และพันธมิตรภายนอกทั้งหมดที่เกี่ยวข้องกับการบริหารความมั่นคงปลอดภัยไซเบอร์ขององค์กร ซึ่งรวมถึง ...

- โครงสร้างพื้นฐานสำคัญด้านสารสนเทศ
- ข้อมูลและเครือข่ายที่สำคัญ
- ผู้ให้บริการและผู้จำหน่ายภายนอก

3. หลักการบริหารความเสี่ยง (Risk Management Principle)

องค์กรจะใช้หลักการดังต่อไปนี้ในการบริหารความเสี่ยงอย่างมีประสิทธิภาพ

- **การระบุความเสี่ยงเชิงรุก**: การระบุความเสี่ยงด้านไซเบอร์ผ่านการประเมินอย่างสม่ำเสมอและการวิเคราะห์ข้อมูลภัยคุกคาม
- **การประเมินความเสี่ยง**: การประเมินผลกระทบและความเป็นไปได้ของความเสี่ยงที่ระบุ โดยเน้นที่ภัยคุกคามที่อาจส่งผลกระทบต่อโครงสร้างพื้นฐานหรือข้อมูลสำคัญ
- **การลดความเสี่ยง**: ดำเนินการลดหรือขจัดความเสี่ยง โดยจัดลำดับความสำคัญของภัยคุกคาม
- **การติดตามและทบทวนความเสี่ยงอย่างต่อเนื่อง**: การติดตามและทบทวนความเสี่ยงด้านไซเบอร์มีการกระทำอย่างต่อเนื่อง หรืออย่างน้อย ปีละ 1 ครั้ง โดยผ่านระบบอัตโนมัติและการตรวจสอบด้วยตนเองอย่างสม่ำเสมอ

4. ความสอดคล้องกับนโยบายความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 - 2570)

นโยบายนี้จะสอดคล้องกับนโยบายความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 - 2570)

- **พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562**: ปฏิบัติตามข้อกำหนดในการปกป้องโครงสร้างพื้นฐานสำคัญและการรายงานเหตุการณ์
- **นโยบายความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 - 2570)**: เป็นการพัฒนาความมั่นคงปลอดภัยทางทางไซเบอร์ในภาพรวมที่ครอบคลุมในทุกมิติและเพื่อใช้เป็นกรอบแนวทางการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในประเทศ

5. บทบาทและความรับผิดชอบ (Roles and Responsibilities)

- **ทีมงานด้านความมั่นคงปลอดภัยไซเบอร์**: รับผิดชอบในการดำเนินการประเมินความเสี่ยง ดำเนินมาตรการแก้ไข และติดตามความเสี่ยงอย่างต่อเนื่อง
- **ฝ่ายบริหาร**: ต้องมั่นใจว่าการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ถูกรวมเข้ากับกรอบการบริหารจัดการทั่วไปและรายงานความสอดคล้องกับหน่วยงานที่เกี่ยวข้อง

- **เจ้าหน้าที่กำกับดูแล**: รับผิดชอบในการตรวจสอบและให้แน่ใจว่าปฏิบัติตามกฎหมายและระเบียบข้อบังคับตามที่ระบุใน **พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562**

6. กระบวนการระบุและประเมินความเสี่ยง (Risk Identification and Risk Assessment)

- **ทะเบียนความเสี่ยง**: จะมีการบันทึกความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ทั้งหมดในทะเบียนความเสี่ยง โดยจะมีการประเมินแต่ละความเสี่ยง เช่น
  - **ความเป็นไปได้**: ความน่าจะเป็นที่ความเสี่ยงจะเกิดขึ้น
  - **ผลกระทบ**: ความเสียหายหรือการรบกวนที่อาจเกิดขึ้นจากความเสี่ยง
  - **มาตรการควบคุม**: ขั้นตอนที่มีอยู่ในปัจจุบัน สามารถเพื่อบรรเทาความเสี่ยงนั้นๆ
- **การจัดประเภทความเสี่ยง**: ความเสี่ยงจะถูกจัดหมวดหมู่ตามระดับ เช่น สูง กลาง ต่ำ ตามความรุนแรงที่ประเมิน

7. การจัดการความเสี่ยง (Risk Treatment)

- **การหลีกเลี่ยง**: ความเสี่ยงที่สามารถหลีกเลี่ยงได้จะถูกขจัดออกโดยการเปลี่ยนแปลงระบบหรือกระบวนการในการปฏิบัติ
- **การลดความเสี่ยง**: ลดความเสี่ยงโดยการดำเนินมาตรการควบคุมเพิ่มเติม เช่น การเข้ารหัสไฟล์ วางไฟร์วอลล์ และฝึกอบรมพนักงาน
- **การยอมรับ**: มีการกำหนดความเสี่ยงในระดับต่ำที่ยอมรับได้ โดยไม่ต้องมีมาตรการเพิ่มเติม
- **การโอนความเสี่ยง**: โอนความเสี่ยงให้หน่วยงานหรือองค์กรภายนอก โดยการทำสัญญาหรือประกันภัยในกรณีที่เหมาะสม

8. การตอบสนองและรายงานเหตุการณ์ (Response and Incident Reporting)

- ทุกเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์จะต้องรายงานต่อทีมรับมือเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ทันที

- เหตุการณ์ที่รุนแรงที่ส่งผลต่อโครงสร้างพื้นฐานสำคัญจะถูกส่งต่อไปยังผู้บริหารระดับสูงและหน่วยงานควบคุมหรือกำกับดูแล ตาม **พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562**

9. การปรับปรุงอย่างต่อเนื่อง (Continuously Improvement)

- จะมีการตรวจสอบและประเมินผลนโยบายฯอย่างสม่ำเสมอ เพื่อให้แน่ใจว่ากรอบการบริหารความเสี่ยงนั้นยังคงมีประสิทธิภาพ
- นโยบายฯนี้จะได้รับการปรับปรุงเพื่อให้ทันกับการเปลี่ยนแปลงของภัยคุกคามทางไซเบอร์

10. การปฏิบัติตามและการกำกับดูแล (Operate and Governance)

นโยบายฯนี้จะได้รับการตรวจสอบอย่างต่อเนื่องเพื่อให้สอดคล้องกับยุทธศาสตร์ไซเบอร์แห่งชาติหรือนโยบายความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 - 2570) รวมถึงข้อกำหนดของ **สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)** การไม่ปฏิบัติตามนโยบายนี้จะมีบทลงโทษตามข้อกำหนดขององค์กร

การทบทวนนโยบาย (Policy Review)

นโยบายนี้จะได้รับการทบทวนเป็นประจำทุกปีหรือตามความจำเป็นเพื่อให้มั่นใจในประสิทธิภาพและและถ้ามีการเปลี่ยนแปลงนโยบายนี้จะต้องมีการสื่อสารไปยังทุกฝ่ายที่ได้รับผลกระทบหรือทุกฝ่ายที่เกี่ยวข้องทราบ