มีการฝึกซ้อม และทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ (INCIDENT RESPONSE PLAN) อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ

โรงพยาบาลแม่ลาว

****

หลักการและเหตุผล

แผนรับมือภัยคุกคามทางไซเบอร์ของโรงพยาบาลแม่ลาวฉบับนี้จัดทำขึ้นเพื่อให้เป็นไปตามมาตรา ๔๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ ที่กำหนดให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์และเพื่อให้เป็นไปตามนโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศกระทรวงสาธารณสุข โดยที่แผนรับมือภัยคุกคามทางไซเบอร์ฉบับนี้จะใช้เป็นแนวทางในการเตรียมความพร้อมเพื่อป้องกัน รับมือ ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ โดยจะระบุขั้นตอนที่จำเป็นในการตอบสนองต่อภัยคุกคามทางไซเบอร์เพื่อให้หน่วยงานสามารถนำไปประยุกต์ใช้ได้อย่างมีประสิทธิภาพ โดยจะมีการทบทวนแผนฉบับนี้อย่างน้อยปีละหนึ่งครั้ง

วัตถุประสงค์

เพื่อใช้เป็นแผนรับมือภัยคุกคามทางไซเบอร์ของโรงพยาบาลแม่ลาว ให้เกิดการดำเนินการอย่างเป็นระบบ มีเอกภาพ มีประสิทธิภาพ และทันต่อเหตุการณ์

เพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ตามประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ให้มีการดำเนินการตรวจสอบข้อมูลที่เกี่ยวของข้อมูลคอมพิวเตอร์และระบบคอมพิวเตอร์ของหน่วยงาน รวมถึงพฤติการณ์แวดล้อม เพื่อประเมินว่ามีภัยคุกคามทางไซเบอร์

เพื่อให้เกิดความร่วมมือระหว่าง หน่วยงานอื่นๆ ในการรับมือกับภัยคุกคามทางไซเบอร์ รวมทั้งบริหารสถานการณ์ต่างๆ ที่เกิดขึ้น เพื่อลดผลกระทบที่อาจเกิดขึ้นต่อการดำเนินงานของโรงพยาบาลแม่ลาว

ขอบเขตการฝึกซ้อม

- ระบบ HIS ใช้งานไม่ได้
- ข้อมูลผู้ป่วยรั่วไหล
- ระบบเครือข่ายใช้งานไม่ได้ล่ม
- เหตุภัยพิบัติกระทบต่อการบริการ
- โดน Ransomware

จัดทีมร่วมการฝึกซ้อม

1	**หัวหน้าทีมฝึกซ้อม**	กำหนดทิศทางและเป้าหมายของการฝึกซ้อม รวมถึงประสานงานกับคณะกรรมการที่เกี่ยวข้อง
2	**ผู้เชี่ยวชาญด้านความปลอดภัยไซเบอร์**	จัดทำและออกแบบสถานการณ์จำลองภัยคุกคาม รวมถึงให้คำแนะนำด้านเทคนิค
3	**ผู้จัดการการสื่อสาร**	จัดการการสื่อสารกับพนักงานและทีมงานทั้งหมดที่มีส่วนเกี่ยวข้องในการฝึกซ้อม
4	**ผู้จัดการด้าน IT**	รับผิดชอบในการจัดการและตรวจสอบระบบเทคโนโลยีสารสนเทศที่เกี่ยวข้องในสถานการณ์จำลอง

ขั้นตอนการฝึกซ้อม

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

การประเมินผลฝึกซ้อม

ประเมินผลการฝึกซ้อมแผน เพื่อวิเคราะห์จุดแข็งและจุดอ่อนที่ต้องปรับปรุงใน การฟื้นฟูความเสียหายจากภัยคุกคามทางไซเบอร์ และต้องมีการจัดทำรายงานผลการฝึกซ้อมที่สรุปผลการดำเนินงาน พร้อมข้อเสนอแนะการปรับปรุงแผน เพื่อเพิ่มประสิทธิภาพในการ ฟื้นฟูความเสียหายในอนาคต

กำหนดการฝึกซ้อม

ดำเนินการฝึกซ้อมแผน อย่างน้อยปีละ 1 ครั้ง