	แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan Procedure)	รหัสเอกสาร	MLH-MOPH-IR Plan -01
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ ชั้นความลับของ เอกสาร	5 ม.ค 2569 ใช้ภายในเท่านั้น


การอนุมัติเอกสาร

ลงนาม	ผู้เรียบเรียง/จัดทำโดย	ผู้ตรวจทาน/ผู้ทบทวน	ผู้อนุมัติ
ลายเซ็น			
ชื่อ-สกุล	นายสุทธิชัย เสาวสิงห์	นายพรศักดิ์ ตามวงศ์	นพ.สุชัย เจริญแสวงตระกูล
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


เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของโรงพยาบาลแม่ลาว ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตโรงพยาบาลแม่ลาว เอกสารกระดาษนี้ ถือเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

	แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan Procedure)	รหัสเอกสาร	MLH-MOPH-IR Plan -01
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ ชั้นความลับของ เอกสาร	5 ม.ค 2569 ใช้ภายในเท่านั้น

สารบัญ


	หน้า
แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan Procedure : CIRP)	4
1. หลักการและเหตุผล	4
2. วัตถุประสงค์	4
3. ขอบเขต	5
4. คำจำกัดความ/นิยามศัพท์เฉพาะ	5
5. ขั้นตอนการรับมือภัยคุกคามทางไซเบอร์	5
6. โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: BAG - CSIRT) 19	
6.1 โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์	19
6.2 โครงสร้างที่สนับสนุนการดำเนินการรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (ทีมสนับสนุน)	20
6.3 โครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure)	21
7. แผนรับมือเหตุการณ์ทางไซเบอร์	21
7.1 การโจมตีเว็บไซต์เพื่อเปลี่ยนแปลงข้อมูลเผยแพร่หน้าเว็บ (Web Defacement)	21
7.2 การถูกโจมตีจากโปรแกรมประสงค์ร้ายเข้ารหัสข้อมูลเรียกค่าไถ่ (Ransomware) / การโจมตียึด ครองเครื่องแม่ข่าย (Server compromise injection attack) / การบุกรุกโดยการโจมตี (Malicious Logic)	23
7.3 การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)	25

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของโรงพยาบาลแม่ลาว ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตโรงพยาบาลแม่ลาว เอกสารกระดาษนี้ ถือเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

	<p style="text-align: center;">แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan Procedure)</p>	รหัสเอกสาร	MLH-MOPH-IR Plan -01
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ ชั้นความลับของ เอกสาร	5 ม.ค 2569 ใช้ภายในเท่านั้น

8. การติดตาม ควบคุม และทบทวน.....	26
ภาคผนวก.....	27
ภาคผนวก ก	27
ภาคผนวก ข	28
ภาคผนวก ค	30

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของโรงพยาบาลแม่ลาว ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตโรงพยาบาลแม่ลาว เอกสารกระดาษนี้ ถือเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

	แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan Procedure)	รหัสเอกสาร	MLH-MOPH-IR Plan -01
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ ชั้นความลับของ เอกสาร	5 ม.ค 2569 ใช้ภายในเท่านั้น

แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan Procedure : CIRP)

อ้างอิง : พรบ ไซเบอร์ (ม. 43, ม. 44, ม. 45, ม. 56, ม. 57, ม. 58) , ประมวลและกรอบ [ข้อ 24.1.1]

1. หลักการและเหตุผล

แผนรับมือภัยคุกคามทางไซเบอร์ของโรงพยาบาลแม่ลาวฉบับนี้ จัดทำขึ้นเพื่อให้เป็นไปตามมาตรา ๔๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ ที่กำหนดให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ และเพื่อให้เป็นไปตามนโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ กระทรวงสาธารณสุข โดยที่แผนรับมือภัยคุกคามทางไซเบอร์ฉบับนี้จะใช้เป็นแนวทางในการเตรียมความพร้อมเพื่อป้องกัน รับมือ ปรามปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ โดยจะระบุขั้นตอนที่จำเป็นในการตอบสนองต่อภัยคุกคามทางไซเบอร์เพื่อให้หน่วยงานสามารถนำไปประยุกต์ใช้ได้ อย่างมีประสิทธิภาพ โดยจะมีการทบทวนแผนฉบับนี้อย่างน้อยปีละหนึ่งครั้ง


2. วัตถุประสงค์

2.1 เพื่อใช้เป็นแผนรับมือภัยคุกคามทางไซเบอร์ของโรงพยาบาลแม่ลาว ให้เกิดการดำเนินการอย่างเป็นระบบ มีเอกภาพ มีประสิทธิภาพ และทันต่อเหตุการณ์

2.2 เพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ตามประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ให้มีการดำเนินการตรวจสอบข้อมูลที่เกี่ยวข้องของข้อมูลคอมพิวเตอร์ และระบบคอมพิวเตอร์ของหน่วยงาน รวมถึงพฤติการณ์แวดล้อม เพื่อประเมินว่ามีภัยคุกคามทางไซเบอร์

2.3 เพื่อให้เกิดความร่วมมือระหว่าง หน่วยงานอื่น ๆ ในการรับมือกับภัยคุกคามทางไซเบอร์ รวมทั้งบริหารสถานการณ์ต่าง ๆ ที่เกิดขึ้น เพื่อลดผลกระทบที่อาจเกิดขึ้นต่อการดำเนินงานของโรงพยาบาลแม่ลาว

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของโรงพยาบาลแม่ลาว ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตโรงพยาบาลแม่ลาว เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

	แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan Procedure)	รหัสเอกสาร	MLH-MOPH-IR Plan -01
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ ชั้นความลับของ เอกสาร	5 ม.ค 2569 ใช้ภายในเท่านั้น

3. ขอบเขต

แผนรับมือฯ ฉบับนี้ ใช้รับมือภัยคุกคามทางไซเบอร์ที่เกิดขึ้นต่อระบบสารสนเทศ และข้อมูลดิจิทัลของโรงพยาบาลแม่ลาว รวมถึงบุคคลหรืออุปกรณ์ใดๆ ซึ่งเข้าถึงระบบสารสนเทศ และข้อมูลดิจิทัลดังกล่าว


4. คำจำกัดความ/นิยามศัพท์เฉพาะ

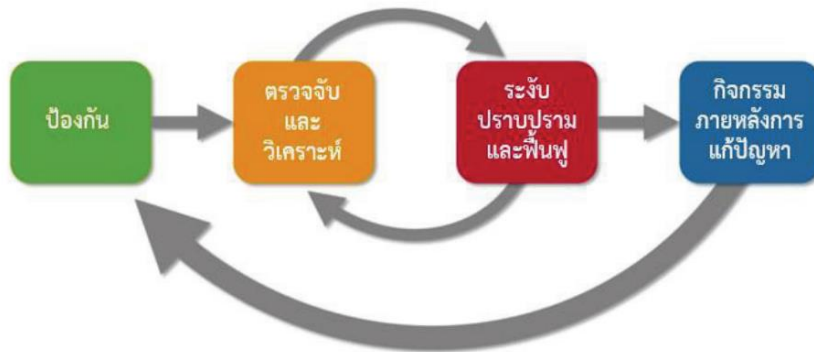
ลำดับ	คำศัพท์	คำจำกัดความ
1	การระงับภัยคุกคามทางไซเบอร์	การดำเนินการเพื่อจำกัดความเสียหายจากภัยคุกคามทางไซเบอร์ที่กำลังเกิดขึ้น กักกันภัยคุกคามไม่ให้แพร่กระจาย และป้องกันไม่ให้ความเสียหายเพิ่มมากขึ้น โดยผู้เผชิญเหตุภัยคุกคามทางไซเบอร์ต้องระมัดระวังไม่ให้หลักฐานทางนิติวิทยาศาสตร์ ถูกทำลายในการดำเนินการดังกล่าว
2	การปราบปรามภัยคุกคามทางไซเบอร์	การดำเนินการกำจัดภัยคุกคาม ผู้เผชิญเหตุภัยคุกคามทางไซเบอร์จะต้องลบโปรแกรมหรือสิ่งที่ไม่พึงประสงค์ (Malicious Object) ออกให้หมด และตรวจสอบระบบที่ได้รับผลกระทบทั้งระบบเพื่อให้มั่นใจถึงความปลอดภัยด้านไซเบอร์ โดยพยายาม ให้ความเสียหายต่อข้อมูลน้อยที่สุด
3	การฟื้นฟูระบบงานที่ได้รับผลกระทบ	การดำเนินการเพื่อนำระบบให้กลับมาอยู่ในสถานะปกติที่มั่นใจว่าปราศจากการโจมตีที่เป็นภัยคุกคาม ทางไซเบอร์ โดยรวมถึงการเฝ้าระวังและตรวจสอบระบบที่ถูกกู้คืนในระยะแรกของการนำกลับมาใช้งาน เพื่อป้องกันการโจมตีซ้ำ

5. ขั้นตอนการรับมือภัยคุกคามทางไซเบอร์

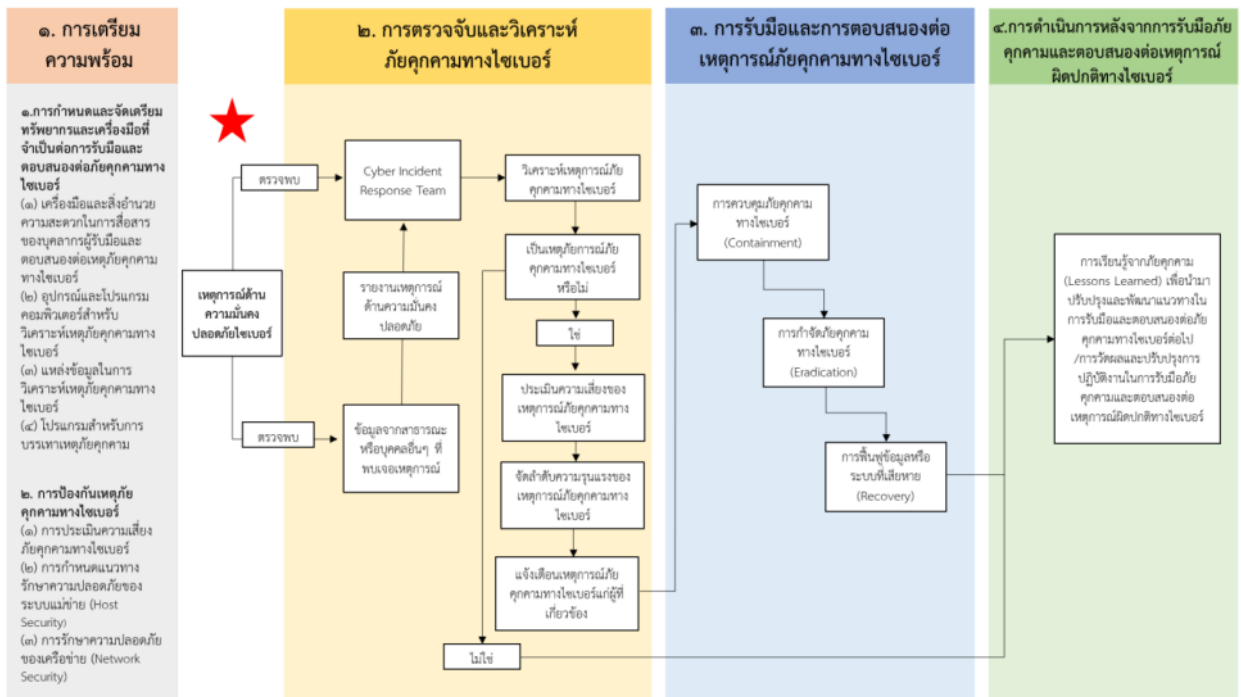
มาตรการป้องกัน รับมือ ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับนั้น มีการดำเนินมาตรการที่เกี่ยวข้องเพื่อจัดการภัยคุกคามทางไซเบอร์ (incident handling) โดยสามารถแบ่งขั้นตอนการดำเนินการออกได้เป็น 4 ขั้นตอนหลัก เพื่อให้สอดคล้องกับมาตรฐานหรือแนวทางปฏิบัติสากลที่เกี่ยวข้องกับการจัดการภัยคุกคามทางไซเบอร์ตามภาพที่ 1 และภาพที่ 2 ดังนี้

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของโรงพยาบาลแม่ลาว ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตโรงพยาบาลแม่ลาว เอกสารกระดาษนี้ ถือเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

	<h1>แผนการรับมือภัยคุกคามทางไซเบอร์</h1> <h2>(Cybersecurity Incident Response Plan Procedure)</h2>	รหัสเอกสาร	MLH-MOPH-IR Plan -01
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ ชั้นความลับของเอกสาร	5 ม.ค 2569 ใช้ภายในเท่านั้น




ภาพที่ 1 แสดงขั้นตอนการดำเนินการมาตรการที่เกี่ยวข้องเพื่อจัดการภัยคุกคามทางไซเบอร์ (Incident Handling Cycle)



ภาพที่ 2 แสดงรายละเอียดขั้นตอนการดำเนินการรับมือภัยคุกคามทางไซเบอร์

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของโรงพยาบาลแม่ลาว ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตโรงพยาบาลแม่ลาว เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

	แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan Procedure)	รหัสเอกสาร	MLH-MOPH-IR Plan -01
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ ชั้นความลับของ เอกสาร	5 ม.ค 2569 ใช้ภายในเท่านั้น

ขั้นตอนที่ 1 : การเตรียมการและป้องกันการเกิดภัยคุกคามทางไซเบอร์

การดำเนินการมาตรการเพื่อเตรียมการและป้องกันการเกิดภัยคุกคามทางไซเบอร์ (Preparation) เป็นสิ่งที่จะต้องทำในระยะเริ่มต้น เพื่อเตรียมความพร้อมเมื่อต้องเผชิญเหตุ ได้แก่ การจัดเตรียมข้อมูลให้พร้อม การจัดตั้งและฝึกอบรมบุคลากรหรือทีมงาน การจัดหาเครื่องมือและทรัพยากรต่าง ๆ ที่จำเป็น การตั้งค่าระบบต่าง ๆ ให้ปลอดภัย การจัดทำนโยบาย แผนงาน และกระบวนการที่เกี่ยวข้อง รวมถึงการสร้างเครือข่ายความร่วมมือ โดยพิจารณาดำเนินการตามรายละเอียดที่ระบุในตารางที่ 2.1


ขั้นตอนที่ 2 : การตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์

แม้ว่าหน่วยงานจะจัดให้มีมาตรการต่าง ๆ เพื่อป้องกันหรือควบคุมไม่ให้เกิดภัยคุกคามทางไซเบอร์ ขึ้นแล้วก็ตาม แต่หน่วยงานก็ยังคงต้องเตรียมความพร้อมอยู่เสมอเพื่อรับมือกับสถานการณ์ภัยคุกคามทางไซเบอร์ที่ไม่อาจหลีกเลี่ยงได้ การดำเนินการมาตรการในการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (Detection and Analysis) จึงเป็นสิ่งจำเป็นที่จะช่วยให้หน่วยงานสามารถบรรเทาความเสี่ยงที่ยังคงเหลืออยู่ และสามารถแจ้งเตือนได้อย่างทันท่วงทีเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น โดยพิจารณาดำเนินการตามรายละเอียดที่ระบุในตารางที่ 2.2

ขั้นตอนที่ 3 : การระงับภัยคุกคามทางไซเบอร์ ปรามปรามภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ

เมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้นหรือเมื่อหน่วยงานได้รับแจ้งเตือนการเกิดภัยคุกคามทางไซเบอร์ หน่วยงานควรกำหนดแนวทางการดำเนินการเพื่อระงับภัยคุกคามทางไซเบอร์การปรามปรามภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ (Containment, Eradication, and Recovery) โดยการดำเนินการดังกล่าว ควรกำหนดให้สอดคล้องกับความรุนแรงและระดับของภัยคุกคามทางไซเบอร์แต่ละระดับ จนกระทั่งสามารถกู้คืนทรัพย์สินสำคัญทางสารสนเทศให้กลับมาดำเนินงานหรือให้บริการได้ตามปกติ โดยพิจารณาดำเนินการตามรายละเอียดที่ระบุในตารางที่ 2.3 ซึ่งการดำเนินการในขั้นตอนนี้จะต้องกระทำควบคู่ไปกับการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ที่อาจมีการลุกลามหรือทวีความรุนแรงมากขึ้นเพื่อให้การระงับและการปรามปรามภัยคุกคามทางไซเบอร์ ตลอดจนการฟื้นฟูระบบงานที่ได้รับผลกระทบจากการเกิดภัยคุกคามทางไซเบอร์สอดคล้องกับสถานการณ์ที่เปลี่ยนแปลงไป

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของโรงพยาบาลแม่ลาว ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตโรงพยาบาลแม่ลาว เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

	แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan Procedure)	รหัสเอกสาร	MLH-MOPH-IR Plan -01
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ ชั้นความลับของ เอกสาร	5 ม.ค 2569 ใช้ภายในเท่านั้น


องค์ประกอบด้วยการดำเนินการ

- 1) จำกัดขอบเขต (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ โดยอาจพิจารณาความเหมาะสมตามภาคผนวก ค
- 2) เรียกใช้งานกระบวนการกู้คืน (Recovery Process) โดยอาจพิจารณาความเหมาะสมตามภาคผนวก ค
- 3) ดำเนินการสอบสวน (Investigate) สาเหตุและผลกระทบของเหตุการณ์ โดยอาจพิจารณาความเหมาะสมตามภาคผนวก ค
- 4) เก็บรักษาหลักฐาน (Preservation of Evidence) ก่อนเริ่มกระบวนการกู้คืนซึ่งรวมถึงการได้มาของบันทึกการยึดหลักฐานคอมพิวเตอร์ที่ได้มา หรืออุปกรณ์อื่น ๆ เพื่อสนับสนุนการสอบสวน ตามโดยอาจพิจารณาความเหมาะสมตามภาคผนวก ค
- 5) ดำเนินการตามระเบียบวิธีการมีส่วนร่วม (Engagement Protocols) กับบุคคลภายนอก หรือแนวปฏิบัติการบริหารจัดการบุคคลภายนอก ซึ่งรวมถึงรายละเอียดการติดต่อ ตัวอย่างเช่น ผู้ขายสำหรับบริการด้านนิติวิทยาศาสตร์/การกู้คืนและการบังคับใช้กฎหมายเพื่อดำเนินคดี โดยอาจพิจารณาความเหมาะสมตามภาคผนวก ค
- 6) ดำเนินการตามเอกสารแนบท้าย 2 ตารางที่ 2.3 ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมินปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. 2564

ขั้นตอนที่ 4 : การดำเนินการภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์

การดำเนินกิจกรรมที่เกี่ยวข้องภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ (Post-Incident Activity) นั้น หน่วยงานควรกำหนดขั้นตอนวิธีปฏิบัติหรือกำหนดนโยบายภายในที่เกี่ยวข้องเพื่อให้มีแนวทางที่ชัดเจน โดยพิจารณาดำเนินมาตรการตามรายละเอียดที่ระบุในตารางที่ 2.4 ซึ่งการปฏิบัติตามมาตรการดังกล่าวจะช่วยให้หน่วยงานสามารถเรียนรู้จากเหตุภัยคุกคามทางไซเบอร์ที่ผ่านมา และสามารถหาแนวทางเพื่อแก้ไข จุดบกพร่อง และพัฒนาแนวทางรับมือกับภัยคุกคามทางไซเบอร์ต่อไปในอนาคต นอกจากนี้หน่วยงานต้องเก็บ รักษาข้อมูลและพยานหลักฐานที่จำเป็น เพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์ หรือใช้ในกรณี ที่ต้องการร้องทุกข์หรือดำเนินคดีเนื่องจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้นนั้น อาจเข้าลักษณะเป็นความผิดตาม ประมวลกฎหมายอาญา

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของโรงพยาบาลแม่ลาว ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตโรงพยาบาลแม่ลาว เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระงับในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

	แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan Procedure)	รหัสเอกสาร	MLH-MOPH-IR Plan -01
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ ชั้นความลับของ เอกสาร	5 ม.ค 2569 ใช้ภายในเท่านั้น

หรือพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 และที่แก้ไขเพิ่มเติม (ถ้ามี) หรือกฎหมายอื่น ๆ ที่เกี่ยวข้อง (โดยการเก็บข้อมูลบางประเภทนั้นอาจจำเป็นต้องดำเนินการตั้งแต่เมื่อมีการตรวจพบว่าภัยคุกคามทางไซเบอร์เกิดขึ้น เนื่องจากข้อมูลดังกล่าวอาจสูญหายไป ในระหว่างที่ต้องระงับเหตุภัยคุกคามทางไซเบอร์นั้น หรืออาจถูกลบหรือทำลายโดยผู้โจมตี)

เมื่อมีการเก็บรวบรวมข้อมูลและหลักฐานที่จำเป็นตามวรรคหนึ่งแล้ว นำข้อมูลและหลักฐานที่รวบรวมได้มาใช้ในการจัดทำบันทึกข้อมูลสถิติภัยคุกคามทางไซเบอร์ โดยอาจจัดทำเป็น รายสัปดาห์หรือรายเดือน เพื่อเสนอต่อผู้ที่มีหน้าที่ดูแลและรับผิดชอบภายในหน่วยงาน และกำหนดขั้นตอน ที่หน่วยงานควรดำเนินการ เพื่อป้องกันไม่ให้เกิดภัยคุกคามทางไซเบอร์ในลักษณะดังกล่าวขึ้นอีกในอนาคต

ตารางที่ 2.1 การดำเนินมาตรการเพื่อเตรียมการและป้องกันการเกิดภัยคุกคามทางไซเบอร์ (Preparation)

ระดับ	แนวปฏิบัติพื้นฐาน (Security Control Baselines)
- กรณีบริการระบบหรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง	1. จัดเตรียมข้อมูลและอุปกรณ์การติดต่อสื่อสารที่จำเป็น เช่น ข้อมูลการติดต่อของบุคคลหรือองค์กรต่าง ๆ คู่มือการปฏิบัติงานเพื่อรับมือกับภัยคุกคามทางไซเบอร์ และกลไกอื่นใดที่ช่วยสนับสนุนการรายงานเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น เป็นต้น
- กรณีบริการระบบหรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับร้ายแรง	2. จัดเตรียมอุปกรณ์หรือทรัพยากรสนับสนุนที่จำเป็นสำหรับการรับมือกับภัยคุกคามทางไซเบอร์
- กรณีบริการระบบหรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับวิกฤติ	3. ดำเนินการให้มีการจัดหมวดหมู่ข้อมูลและระบบสารสนเทศให้สอดคล้องกับ แนวทางของกฎหมาย กฎเกณฑ์ หรือนโยบายต่าง ๆ ที่เกี่ยวข้อง เพื่อธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) ตลอดจนสภาพพร้อมใช้งาน (availability) ของข้อมูลและระบบสารสนเทศดังกล่าว
	4. จัดเตรียมข้อมูลสนับสนุนที่จำเป็นสำหรับการวิเคราะห์เหตุภัยคุกคามทางไซเบอร์ เช่น รายการทรัพย์สินสำคัญทางสารสนเทศ และแผนผังโครงสร้างเครือข่าย (Network diagrams) เป็นต้น

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของโรงพยาบาลแม่ลาว ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตโรงพยาบาลแม่ลาว เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ




แผนการรับมือภัยคุกคามทางไซเบอร์

(Cybersecurity Incident Response Plan Procedure)

รหัสเอกสาร	MLH-MOPH-IR Plan -01
แก้ไขครั้งที่	00
วันที่บังคับใช้ ชั้นความลับของ เอกสาร	5 ม.ค 2569 ใช้ภายในเท่านั้น

ระดับ	แนวปฏิบัติพื้นฐาน (Security Control Baselines)
	<p>5. พิจารณาช่องบริการหรือระบบที่ผู้โจมตีสามารถค้นพบในเครือข่ายได้ง่าย โดยไม่ต้องใช้ความพยายามเจาะระบบ เช่น การค้นหาผ่านกลไกการสืบค้น (discovery protocol) เป็นต้น</p> <p>6. ดำเนินการควบคุมการเปลี่ยนแปลงการตั้งค่าของอุปกรณ์ต่าง ๆ (configuration change control) และจัดทำแผนการบริหารจัดการการตั้งค่า หรือ การเปลี่ยนแปลงค่าของอุปกรณ์ (configuration management plan)</p> <p>7. กำหนดตัวบุคคลหรือมอบหมายให้เจ้าหน้าที่ที่มีความชำนาญเป็นผู้ดำเนินการ ที่เกี่ยวข้องกับการเปลี่ยนแปลงการตั้งค่าของอุปกรณ์ต่าง ๆ รวมถึงการทำหน้าที่ในการประสานงานหรือหารือกับผู้ที่เกี่ยวข้อง</p> <p>8. จัดให้มีกระบวนการในการพิสูจน์ตัวตนผู้ใช้งานก่อนทางการเปลี่ยนแปลงการตั้งค่าของอุปกรณ์ใด ๆ เช่น การเข้ารหัสข้อมูลและการบริหารจัดการคีย์ สำหรับการเข้าถึงระบบต่าง ๆ (cryptography / key managements) เป็นต้น</p> <p>9. ตรวจสอบแอปพลิเคชันที่ให้บริการโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้มีความปลอดภัยเพียงพอ โดยมีการคัดกรองนักพัฒนา (developer screening) ที่ได้รับมอบหมายให้ดำเนินการใด ๆ กับเครือข่ายแอปพลิเคชัน หรือระบบงาน ต่าง ๆ</p> <p>10. ดำเนินการให้มีการทดสอบความสามารถในการตอบสนองต่อภัยคุกคามทางไซเบอร์ (Incident Respond Capability Testing)</p> <p>11. รวบรวมข่าวกรองเกี่ยวกับภัยคุกคามทางไซเบอร์ (threat Intelligence)</p> <p>12. กำหนดแนวทางและระยะเวลาการเก็บรักษาหลักฐานเกี่ยวกับการก่อภัยคุกคามทางไซเบอร์</p> <p>13. ดำเนินการควบคุมการเปลี่ยนแปลงการตั้งค่าของอุปกรณ์ต่าง ๆ (configuration change control) และจัดทำแผนการบริหารจัดการการตั้งค่า หรือ การเปลี่ยนแปลง ค่าของอุปกรณ์ (configuration management plan) โดยจะต้องจัดให้มีกลไกที่สามารถบันทึกประวัติการเปลี่ยนแปลงการตั้งค่า</p>

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของโรงพยาบาลแม่ลาว ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตโรงพยาบาลแม่ลาว เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ


	แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan Procedure)	รหัสเอกสาร	MLH-MOPH-IR Plan -01
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ ชั้นความลับของ เอกสาร	5 ม.ค 2569 ใช้ภายในเท่านั้น

ระดับ	แนวปฏิบัติพื้นฐาน (Security Control Baselines)
	<p>ของอุปกรณ์ที่เป็นลายลักษณ์อักษร การแจ้งเตือนเมื่อมีการเปลี่ยนแปลงค่าของอุปกรณ์ที่ตั้งไว้ และให้พิจารณาจัดให้มีกลไกที่สามารถป้องกันการเปลี่ยนแปลงค่าของอุปกรณ์ต่าง ๆ โดยอัตโนมัติ (ถ้าหน่วยงานมีความพร้อม)</p> <p>14. จัดให้มีการฝึกร่วมเพื่อเตรียมพร้อมรับมือกับสถานการณ์ฉุกเฉินเมื่อมีภัย คุกคามทางไซเบอร์เกิดขึ้น (simulated events) เพื่อให้ผู้ปฏิบัติรับทราบบทบาทและความรับผิดชอบของตนเมื่อต้องรับมือกับสถานการณ์ดังกล่าว</p> <p>15. สร้างเครือข่ายความร่วมมือเพื่อแบ่งปันข้อมูลและประสานงานเกี่ยวกับการจัดการภัยคุกคามทางไซเบอร์</p>

ตารางที่ 2.2 การดำเนินมาตรการในการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (Detection and Analysis)

ระดับ	แนวปฏิบัติพื้นฐาน (Security Control Baselines)
- กรณีบริการ ระบบ หรือ อุปกรณ์ มีแนวโน้มที่จะ เกิดผลกระทบเป็น ภัยคุกคามทางไซเบอร์ ในระดับไม่ ร้ายแรง กรณีบริการ ระบบ หรือ อุปกรณ์ มีแนวโน้มที่ จะเกิด ผลกระทบเป็นภัยคุกคาม ทางไซเบอร์ในระดับร้ายแรง	<ol style="list-style-type: none"> 1. จัดให้มีกลไกที่สามารถตรวจจับสิ่งบ่งชี้หรือลักษณะเบื้องต้นของการเกิดภัยคุกคามทางไซเบอร์ได้ในเวลาอันเหมาะสม โดยอาจอาศัยข้อมูลจากแหล่งข้อมูล ต่าง ๆ เช่น ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เป็นต้น 2. จัดให้มีกลไกที่สามารถรับการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์ 3. จัดให้มีข้อพึงปฏิบัติพื้นฐานเกี่ยวกับการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Logs) ข้อความการแจ้งข้อผิดพลาด หรือข้อความเตือนภัยจากเครื่องมือรักษา ความปลอดภัยด้านไซเบอร์ และการตรวจสอบระบบงานที่มีความสำคัญ (Critical Systems) โดยจะต้องจัดให้มีข้อพึงปฏิบัติที่สูงขึ้นสำหรับทุกระบบงาน ที่มีความสำคัญมากขึ้น

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของโรงพยาบาลแม่ลาว ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตโรงพยาบาลแม่ลาว เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

	แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan Procedure)	รหัสเอกสาร	MLH-MOPH-IR Plan -01
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ ชั้นความลับของ เอกสาร	5 ม.ค 2569 ใช้ภายในเท่านั้น

ระดับ	แนวปฏิบัติพื้นฐาน (Security Control Baselines)
	<p>4. วิเคราะห์ข้อมูลและประวัติการใช้งานต่าง ๆ เช่น ลักษณะการใช้งานเครือข่าย และระบบงาน (Profile Networks and Systems) เป็นต้น เพื่อทำความเข้าใจ พฤติกรรมการใช้งานในช่วงเวลาปกติ (Normal Behaviours) ทางการศึกษา วิจัยและค้นหาความสัมพันธ์ของข้อมูลในระบบกับสถานการณ์ต่าง ๆ (Event Correlation)</p> <p>5. ทันทันที่พบว่า มี หรืออาจมีภัยคุกคามทางไซเบอร์เกิดขึ้น ให้ดำเนินการสืบหาและ รวบรวมข้อมูลทั้งหมด เช่น ลักษณะภัยคุกคามทางไซเบอร์, ช่องโหว่ที่อาจถูกใช้ ในการโจมตี, สถานการณ์ของการโจมตี (อาทิ กำลังเกิดเหตุหรือสถานการณ์ได้ สิ้นสุดแล้ว การโจมตีเป็นผลสำเร็จหรือไม่สำเร็จ ฯลฯ) จำนวนระบบหรือบริการ ที่ได้รับผลกระทบ, โฮสต์เนม ตำแหน่งหรือสถานที่ของระบบหรือบริการที่ได้รับ ผลกระทบ ข้อมูลผู้ใช้ เวลาประทับ ข้อมูล payload ข้อมูลแจ้งเตือนจาก IDS (ถ้ามี) และ ข้อมูลจราจรทางคอมพิวเตอร์ (log) เป็นต้น โดยหน่วยงานจะต้อง เก็บรักษาข้อมูลดังกล่าว (safeguard incident data) ให้มีความปลอดภัย เพื่อใช้ ในกระบวนการทางนิติวิทยาศาสตร์และใช้ เป็นพยานหลักฐานในการดำเนินคดี รวมถึงการจัดทำรายงานที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์</p> <p>6. ระบุหมวดหมู่ของภัยคุกคามทางไซเบอร์ตามสถานการณ์ที่เกิดขึ้น และติดตาม เพื่อระบุหมวดหมู่ของภัยคุกคามทางไซเบอร์ที่เปลี่ยนแปลงไปจนกว่าสถานการณ์ ดังกล่าวจะสิ้นสุด โดยอาจพิจารณาจากข้อมูลตามที่ระบุในข้อ 2 ของภาคผนวก ข แนบท้ายนี้</p> <p>7. จัดลำดับความสำคัญของการดำเนินการเพื่อรับมือกับภัยคุกคามทางไซเบอร์ให้ ทันท่วงที โดยพิจารณาปัจจัยต่าง ๆ ที่เกี่ยวข้อง เช่น ผลกระทบต่อการทำงาน ของระบบ (functional impact) ผลกระทบต่อข้อมูล (information impact) และ ความสามารถในการกู้คืน (recoverability effort) เป็นต้น</p>

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของโรงพยาบาลแม่ลาว ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตโรงพยาบาลแม่ลาว เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ




แผนการรับมือภัยคุกคามทางไซเบอร์

(Cybersecurity Incident Response Plan Procedure)

รหัสเอกสาร	MLH-MOPH-IR Plan -01
แก้ไขครั้งที่	00
วันที่บังคับใช้ ชั้นความลับของ เอกสาร	5 ม.ค 2569 ใช้ภายในเท่านั้น

ระดับ	แนวปฏิบัติพื้นฐาน (Security Control Baselines)
	<p>8. ศึกษาวิธีและลักษณะการโจมตี พร้อมทั้งระบุสาเหตุที่แท้จริงของภัยคุกคามทาง ไซเบอร์รวมถึงจุดอ่อนของระบบที่ถูกโจมตี</p> <p>9. ดำเนินการแจ้งไปยังผู้ที่รับผิดชอบในการเผชิญเหตุหรือผู้ที่เกี่ยวข้องผ่านช่องทาง ที่มีความปลอดภัย โดยคำนึงถึงระดับชั้นความลับและความสำคัญของข้อมูล เพื่อให้บุคคลดังกล่าวสามารถปฏิบัติหน้าที่ในการรับมือกับภัยคุกคามทางไซเบอร์ ที่เกิดขึ้น</p> <p>10. รายงานภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับบริการของโครงสร้างพื้นฐานสำคัญ ทางสารสนเทศอย่างมีนัยสำคัญให้ผู้ที่เกี่ยวข้องทราบภายในระยะเวลาที่ หน่วยงานควบคุมหรือกำกับดูแลกำหนด (โดยหน่วยงานควบคุมหรือกำกับดูแล อาจจะนำข้อปฏิบัติตามแผนการกู้คืนของหน่วยงานมาประกอบการ พิจารณาด้วยก็ได้) หรืออาจเทียบเคียงจากตัวอย่างตามที่ระบุในข้อ 3 ของ ภาคผนวก ข แนบท้ายนี้ แล้วแต่กรณี</p>
- กรณีบริการ ระบบ หรือ อุปกรณ์ มีแนวโน้มที่จะเกิด ผลกระทบเป็น ภัยคุกคาม ทางไซเบอร์ในระดับวิกฤติ	<p>ให้ดำเนินการตามข้อ 1 ถึงข้อ 2 และดำเนินการมาตรการเพิ่มเติม ดังนี้</p> <ol style="list-style-type: none"> 1. จัดให้มีกลไกที่สามารถแจ้งเตือนได้ทันที (real-time alerts) เมื่อพบว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้น 2. จัดให้มีกลไกหรือระบบงานที่สามารถติดตามเหตุการณ์ และสามารถจัดเก็บและ วิเคราะห์ข้อมูลต่าง ๆ เพื่อตรวจจับการเกิดภัยคุกคามทางไซเบอร์ได้โดยอัตโนมัติ (ถ้าหน่วยงานมีความพร้อม) 3. จัดให้มีการแจ้งเตือนเกี่ยวกับความผิดปกติของการใช้ทรัพยากรของระบบงาน เช่น แจ้งเตือนเมื่อหน่วยความจำที่ใช้ในการจัดเก็บข้อมูลจากรางคอมพิวเตอร์ เหลือน้อย (storage capacity warning) เมื่อมีการใช้หน่วยประมวลผลกลาง (CPU) หรือมีการใช้หน่วยความจำหลัก (RAM) ของอุปกรณ์เครือข่ายหรือระบบ งานหลักที่สูงผิดปกติ หรือเมื่อมีการส่งข้อมูลออกนอกเครือข่ายมากผิดปกติ เป็นต้น

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของโรงพยาบาลแม่ลาว ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตโรงพยาบาลแม่ลาว เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

	แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan Procedure)	รหัสเอกสาร	MLH-MOPH-IR Plan -01
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ ชั้นความลับของ เอกสาร	5 ม.ค 2569 ใช้ภายในเท่านั้น

ระดับ	แนวปฏิบัติพื้นฐาน (Security Control Baselines)
	4. วิเคราะห์ข้อมูลและค้นหาความสัมพันธ์ของข้อมูลกับเหตุการณ์ต่าง ๆ (information correlation) โดยอาจรับข้อมูลจากแหล่งข้อมูลอื่น ๆ นอกเหนือจากข้อมูล ในระบบ เพื่อเพิ่มความสามารถในการรับรู้และดำเนินการตรวจจับและวิเคราะห์ ภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ

ตารางที่ 2.3 การดำเนินการมาตรการเพื่อระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคามทาง ไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ (Containment, Eradication and Recovery)

ระดับ	แนวปฏิบัติพื้นฐาน (Security Control Baselines)
- กรณีบริการระบบ หรือ อุปกรณ์ มีแนวโน้มที่จะเกิดผลกระทบ เป็นภัยคุกคามทางไซเบอร์ใน ระดับ ไม่ร้ายแรง	<ol style="list-style-type: none"> ดำเนินการตามแนวทางหรือวิธีการในการจำกัดขอบเขตและระงับ ภัยคุกคาม ทางไซเบอร์ โดยที่แนวทางหรือวิธีการดังกล่าวจะต้องมี หลักเกณฑ์ที่ชัดเจนเพื่อใช้ ประกอบการตัดสินใจในการดำเนินการ ทั้งนี้ แนวทางดังกล่าวรวมถึง <ol style="list-style-type: none"> 1.1 การดำเนินการเชิงเทคนิค เช่น การลบมัลแวร์ การปิดการใช้งานบัญชี ของผู้ใช้งานที่ถูกละเมิด การปิดระบบหรือตัดการเชื่อมต่อของ ระบบ จากเครือข่ายภายหลังการเก็บหลักฐานหรือข้อมูลที่จำเป็นเพื่อใช้ใน กระบวนการทางนิติวิทยาศาสตร์และใช้เป็นพยานหลักฐานในการ ดำเนิน คดีแล้ว เป็นต้น 1.2 การดำเนินการเชิงบริหาร เช่น กำหนดแนวทางดำเนินการหรือ การตัดสินใจของฝ่ายบริหารของหน่วยงาน การสื่อสารทั้งภายในและ ภายนอกหน่วยงาน เป็นต้น 1.3 การเตรียมการเพื่อดำเนินการทางกฎหมายกับผู้กระทำความผิด 2. ดำเนินการตามแนวปฏิบัติที่เกี่ยวข้องเพื่อเก็บรวบรวมและจัดการ หลักฐานต่าง ๆ ที่เกี่ยวข้องกับการก่อกำเนิดภัยคุกคามทางไซเบอร์โดยทันที หลังจากที่ได้รับพบ เช่น การจัดการกับข้อมูลที่บันทึกอยู่ในหน่วยความจำ

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของโรงพยาบาลแม่ลาว ห้ามแจกจ่ายไปยัง บุคคลภายนอกโดยไม่ได้รับอนุญาตโรงพยาบาลแม่ลาว เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ



แผนการรับมือภัยคุกคามทางไซเบอร์

(Cybersecurity Incident Response Plan Procedure)

รหัสเอกสาร	MLH-MOPH-IR Plan -01
แก้ไขครั้งที่	00
วันที่บังคับใช้ ชั้นความลับของ เอกสาร	5 ม.ค 2569 ใช้ภายในเท่านั้น

ระดับ	แนวปฏิบัติพื้นฐาน (Security Control Baselines)
	<p>ประเภทที่สามารถสูญหายได้ เมื่อปิดอุปกรณ์ (volatile data) การเก็บข้อมูลจราจรทางคอมพิวเตอร์ (logs) ข้อมูลเกี่ยวกับมัลแวร์ ข้อมูลสถานะของระบบ (system snapshot) หรือ ข้อมูลอื่น ๆ ที่จำเป็นให้เพียงพอสำหรับใช้วิเคราะห์ในเชิงเทคนิค และ เพื่อทางนิติวิทยาศาสตร์และใช้เป็นพยานหลักฐานในการดำเนินคดี</p> <p>3. ดำเนินการเพื่อให้มีการระบุแหล่งที่มาของการโจมตี (attacking host) เช่น การระบุหมายเลขประจำเครื่อง (IP address) การระบุช่องทางที่ผู้โจมตีใช้ การค้นหาและวิจัยที่มาของการโจมตีจากแหล่งข้อมูลต่าง ๆ เช่น ฐานข้อมูล ภัยคุกคามทางไซเบอร์ที่รวบรวมข้อมูลจากหลายแหล่ง เป็นต้น</p> <p>4. ประสานงานเพื่อแจ้งหรือรายงานสถานการณ์การรับมือภัยคุกคามทางไซเบอร์ และความคืบหน้าในการตอบสนองไปยังบุคคลหรือหน่วยงานที่เกี่ยวข้อง ตลอดจนผู้ที่อาจได้รับผลกระทบ อย่างทันทั่วถึง โดยอาจขอความช่วยเหลือไปยัง บุคคลหรือหน่วยงานต่าง ๆ โดยเฉพาะการเกิดภัยคุกคามทางไซเบอร์ที่จัดอยู่ใน หมวดหมู่ที่ 1, 2, 4, 5 และ 7 ตามที่ระบุในข้อ 1 ของภาคผนวก ข แนบท้ายนี้ ทั้งนี้ ในการแจ้งหรือรายงานสถานการณ์นั้น หน่วยงานควรเลือกใช้ช่องทางที่มีความเหมาะสมและปลอดภัยและดำเนินการแจ้งหรือรายงานเหตุภายในระยะเวลาที่หน่วยงานควบคุมหรือกำกับดูแลกำหนด หรืออาจเทียบเคียงจากตัวอย่างตามที่ระบุในข้อ 3 ของภาคผนวก ข แนบท้ายนี้ แล้วแต่กรณี</p> <p>5. ดำเนินการจัดการกับช่องโหว่ทั้งหมดที่ได้รับผลกระทบจากภัยคุกคามทางไซเบอร์ และดำเนินการตามวิธีการป้องกันระบบจากความเสียหายที่อาจเกิดขึ้นเพิ่มเติม เช่น การปรับเปลี่ยนการควบคุมการเข้าถึงเครือข่าย (อาทิ ไฟร์วอลล์) การติดตั้ง ลายเซ็นของ Anti-Virus หรือ IDS / IPS ใหม่ หรือการเปลี่ยนแปลงทางกายภาพ ในโครงสร้างพื้นฐาน และ</p>

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของโรงพยาบาลแม่ลาว ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตโรงพยาบาลแม่ลาว เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ




แผนการรับมือภัยคุกคามทางไซเบอร์

(Cybersecurity Incident Response Plan Procedure)

รหัสเอกสาร	MLH-MOPH-IR Plan -01
แก้ไขครั้งที่	00
วันที่บังคับใช้ ชั้นความลับของ เอกสาร	5 ม.ค 2569 ใช้ภายในเท่านั้น

ระดับ	แนวปฏิบัติพื้นฐาน (Security Control Baselines)
	<p>ดำเนินการระงับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นโดย ทันทีหลังจากที่ตรวจพบ เป็นต้น</p> <p>6. ดำเนินการที่เกี่ยวข้องเพื่อให้มั่นใจว่าระบบงานต่าง ๆ ยังคงสามารถใช้งานได้ ตามปกติภายในกรอบระยะเวลาที่กำหนด (Restore within time period) เช่น การกู้คืนระบบให้กลับมาดำเนินการได้ตามปกติ (Integrity restoration) การสร้างระบบงานขึ้นใหม่ (Rebuild) การแทนที่ไฟล์ที่ได้รับผลกระทบ (replace) การติดตั้งโปรแกรมคอมพิวเตอร์ (install) การเปลี่ยนแปลงรหัสผ่าน และการรักษาความปลอดภัยทางเครือข่าย (securing network) เป็นต้น</p> <p>7. สร้างมาตรการป้องกันทั้งเชิงรุกและเชิงรับ เพื่อป้องกันไม่ให้เกิดภัยคุกคามทาง ไซเบอร์ที่มีลักษณะคล้ายคลึงกันเกิดขึ้นอีกในอนาคต เช่น การเพิ่มมาตรการ ฝ้าระวังสัญญาณเตือนและเหตุการณ์ต่าง ๆ ที่มีความเกี่ยวข้องกับภัยคุกคาม ทางไซเบอร์ที่เกิดขึ้นแล้ว เป็นต้น</p> <p>8. สร้างมาตรการป้องกันทั้งเชิงรุกและเชิงรับเพื่อป้องกันไม่ให้เกิดภัยคุกคามทางไซเบอร์ที่มีลักษณะคล้ายคลึงกันเกิดขึ้นอีกในอนาคต เช่น การเพิ่มมาตรการ ฝ้าระวังสัญญาณเตือนและเหตุการณ์ต่าง ๆ ที่มีความเกี่ยวข้องกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นแล้ว เป็นต้น</p>
- กรณีบริการระบบ หรือ อุปกรณ์ มีแนวโน้มที่จะเกิด ผลกระทบ เป็นภัยคุกคามทางไซเบอร์ในระดับ ร้ายแรง	<p>ให้หน่วยงานดำเนินการตามข้อ 1 และดำเนินการเพิ่มเติม ดังนี้</p> <p>1. หากมีความจำเป็น ให้หน่วยงานดำเนินการใช้ระบบงานสำรอง สำหรับการประมวลผล (Alternate Processing) การจัดเก็บข้อมูล (Storage Site) และกู้คืนข้อมูลที่เกี่ยวข้องกับการทำรายการหรือการดำเนินธุรกรรมต่าง ๆ (Transaction Recovery)</p> <p>2. ส่งคำแจ้งเตือนเพื่อขอรับการสนับสนุน ความช่วยเหลือ หรือประสานความร่วมมือไปยังหน่วยงานที่เกี่ยวข้อง (Supply Chain Coordination) รวมถึงแจ้งไปยังศูนย์ ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ</p>


เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของโรงพยาบาลแม่ลาว ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตโรงพยาบาลแม่ลาว เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

	แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan Procedure)	รหัสเอกสาร	MLH-MOPH-IR Plan -01
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ ชั้นความลับของ เอกสาร	5 ม.ค 2569 ใช้ภายในเท่านั้น

ระดับ	แนวปฏิบัติพื้นฐาน (Security Control Baselines)
	<p>3. ดำเนินการตามนโยบายการรายงานเกี่ยวกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นภายในหน่วยงานซึ่งครอบคลุมถึงรูปแบบ ระดับความลับ และเนื้อหาที่ต้องรายงาน ลำดับชั้นการรายงาน กำหนดเวลา เครื่องมือที่ใช้รายงาน (โดยอาจพิจารณาใช้เครื่องมือที่สามารถช่วยรายงานภัยคุกคามโดยอัตโนมัติ (ถ้าหน่วยงาน มีความพร้อม)</p> <p>4. ให้การช่วยเหลือ สนับสนุน หรือปฏิบัติงานร่วมกับสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ หน่วยงานควบคุมหรือกำกับดูแล พนักงานเจ้าหน้าที่ หรือบุคคลอื่นใดที่ปฏิบัติหน้าที่หรือได้รับมอบหมายให้ปฏิบัติ หน้าที่ตามกฎหมาย</p> <p>5. พิจารณาจัดให้มีกลไกที่สามารถทำงานได้โดยอัตโนมัติ ในการรับมือหรือสนับสนุนการรับมือเมื่อเกิดภัยคุกคามทางไซเบอร์ (Automated Incident Handling Processes) (ถ้าหน่วยงานมีความพร้อม)</p>
- กรณีบริการระบบ หรือ อุปกรณ์ มีแนวโน้มที่จะเกิด ผลกระทบ เป็นภัยคุกคามทางไซเบอร์ในระดับวิกฤติ	<p>ให้หน่วยงานดำเนินการตามข้อ 1 ถึงข้อ 2 และดำเนินการมาตรการเพิ่มเติม ดังนี้</p> <p>1. ดำเนินการตามแผนการทำงานในการกู้คืนระบบงานต่าง ๆ เพื่อให้ระบบสามารถ ให้บริการได้ภายในกรอบระยะเวลาที่กำหนด Restore within Time Period) โดยอาศัยความรู้จากทีมผู้เชี่ยวชาญด้านต่าง ๆ เพื่อให้การกู้คืนระบบและ เครือข่ายของหน่วยงานทำได้อย่างรวดเร็ว</p>

หมายเหตุ: ในกรณีที่ภัยคุกคามทางไซเบอร์เกิดขึ้นแล้ว แต่หน่วยงานยังไม่สามารถระบุระดับของภัยคุกคามทางไซเบอร์ได้ ซึ่งอาจเกิดจากการที่หน่วยงานยังไม่สามารถรวบรวมรายละเอียดหรือข้อมูลที่จำเป็นเพื่อใช้ในการวิเคราะห์ได้ในช่วงแรก หรือไม่ว่าด้วยเหตุอื่นใดก็ตาม ให้หน่วยงานดำเนินการประเมินผลกระทบเบื้องต้น โดยพิจารณาจากตัวอย่างตาม ที่ระบุในข้อ 1 ของภาคผนวก ข แนบท้ายนี้ จนกว่าจะมีข้อมูลหรือปรากฏหลักฐานที่เพียงพอต่อการวิเคราะห์ เพื่อระบุระดับของภัยคุกคามทางไซเบอร์


เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของโรงพยาบาลแม่ลาว ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตโรงพยาบาลแม่ลาว เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

	แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan Procedure)	รหัสเอกสาร	MLH-MOPH-IR Plan -01
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ ชั้นความลับของ เอกสาร	5 ม.ค 2569 ใช้ภายในเท่านั้น

ตารางที่ 2.4 การดำเนินกิจกรรมที่เกี่ยวข้องภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ (Post-incident Activity)

ระดับ	แนวปฏิบัติพื้นฐาน (Security Control Baselines)
- กรณีบริการ ระบบ หรือ อุปกรณ์ มีแนวโน้มที่จะเกิด ผลกระทบ เป็น ภัยคุกคามทาง ไซเบอร์ใน ระดับไม่ร้ายแรง	<p>ภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ ให้หน่วยงานพิจารณา ดำเนินการดังนี้</p> <ol style="list-style-type: none"> นำเหตุการณ์ที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นและมีลักษณะเป็น ภัยคุกคามทางไซเบอร์ที่มีนัยสำคัญมาเป็นกรณีศึกษา เช่น การพิจารณาถึง จุดอ่อนของโครงสร้างพื้นฐานของบริการ นโยบายและ กระบวนการ การฝึก บุคลากร การระงับผู้มีอำนาจดำเนินงาน และเครื่องมือ ที่ใช้ เป็นต้น และหา แนวทางเพื่อเตรียมการรับมือและป้องกันการเกิดภัย คุกคามทางไซเบอร์ที่มี ลักษณะดังกล่าวร่วมกับบุคคลหรือหน่วยงาน ที่เกี่ยวข้อง รวบรวมข้อมูลการดำเนินงานที่เกี่ยวข้องกับการรับมือภัยคุกคามทาง ไซเบอร์ (โดยอาจดำเนินการเป็นรายสัปดาห์หรือรายเดือน) เช่น จำนวนของ ภัยคุกคาม ทางไซเบอร์ที่เกิดขึ้น เวลาที่ใช้ในการจัดการกับภัยคุกคาม ทางไซเบอร์ประเภท ต่าง ๆ และวัตถุประสงค์ของการโจมตี เป็นต้น เพื่อ เสนอต่อผู้ที่มีหน้าที่ดูแล และรับผิดชอบภายในหน่วยงาน ปรับปรุงมาตรการเตรียมการและป้องกัน รับมือ ปราบปราม และ ระงับภัย คุกคามทางไซเบอร์แต่ละระดับให้มีความเหมาะสม และเป็น ปัจจุบัน เก็บรักษาข้อมูลและหลักฐานที่จำเป็น เพื่อใช้ในกระบวนการทางนิติ วิทยาศาสตร์ หรือใช้ในกรณีที่ต้องการร้องทุกข์หรือดำเนินคดี ตามแนวทาง และระยะเวลาการ เก็บรักษาหลักฐานเกี่ยวกับการก่อภัยคุกคามทางไซเบอร์ ที่หน่วยงานได้กำหนด
- กรณีบริการ ระบบ หรือ อุปกรณ์ มีแนวโน้มที่จะเกิด ผลกระทบ เป็น ภัยคุกคามทาง ไซเบอร์ใน ระดับร้ายแรง	
- กรณีบริการ ระบบ หรือ อุปกรณ์ มีแนวโน้มที่จะเกิด ผลกระทบ เป็น ภัยคุกคามทาง ไซเบอร์ใน ระดับวิกฤต	

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของโรงพยาบาลแม่ลาว ห้ามแจกจ่ายไปยัง บุคคลภายนอกโดยไม่ได้รับอนุญาตโรงพยาบาลแม่ลาว เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

	แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan Procedure)	รหัสเอกสาร	MLH-MOPH-IR Plan -01
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ ชั้นความลับของ เอกสาร	5 ม.ค 2569 ใช้ภายในเท่านั้น


อนึ่งแนวปฏิบัติพื้นฐาน (Security Control Baselines) ตามรายละเอียดที่กำหนดไว้ในตารางที่ 2.1 – ตารางที่ 2.4 นี้ เป็นเพียงแนวทางมาตรการเตรียมการและป้องกัน รับมือปราบปราม และ ระวังภัยคุกคามทางไซเบอร์แต่ละระดับได้อย่างมีประสิทธิภาพ

6. โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: BAG - CSIRT)

6.1 โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

ลำดับที่	ชื่อ นามสกุล รายละเอียดการติดต่อ	หน้าที่	ความรับผิดชอบ
1	นายแพทย์สุขชัย เจริญเศวตตระกูล ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ และการสื่อสาร โทร. 053 603100 ต่อ 2136	หัวหน้าทีมรับมือฯ (Team manager)	ทำหน้าที่สื่อสารกับ ผู้บริหารของหน่วยงาน
2	ทต.เสกสรร คูดิษฐาเลิศ รองผู้อำนวยการศูนย์เทคโนโลยี สารสนเทศและการสื่อสาร โทร. 053 603100 ต่อ 3116	รองหัวหน้าทีมรับมือฯ (Deputy team manager)	ทำหน้าที่แทนกรณีหัวหน้า ทีมรับมือฯ ไม่อยู่/ไม่ สามารถปฏิบัติงานได้
3	พันจ่าเอกพรชัย บุญเพียร โทร. 053 603100 ต่อ 2136	หัวหน้าเจ้าหน้าที่ รับมือฯ (Incident lead)	ทำหน้าที่ช่วยเหลือ หน่วยงานเจ้าของระบบ ภายใต้หน่วยงานของท่าน ให้สามารถควบคุม ผลกระทบจากภัยคุกคาม ทางไซเบอร์ได้
4	นายพรศักดิ์ ตามวงศ์ หัวหน้ากลุ่มสุขภาพดิจิทัล โทร 081-4733415	หัวหน้าเจ้าหน้าที่ เทคนิค (Technical lead)	ทำหน้าที่ให้ความเห็น เกี่ยวกับแนวทางที่ เหมาะสมในการควบคุม

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของโรงพยาบาลแม่ลาว ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตโรงพยาบาลแม่ลาว เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ


	แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan Procedure)	รหัสเอกสาร	MLH-MOPH-IR Plan -01
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ ชั้นความลับของ เอกสาร	5 ม.ค 2569 ใช้ภายในเท่านั้น

ลำดับที่	ชื่อ นามสกุล รายละเอียดการติดต่อ	หน้าที่	ความรับผิดชอบ
			ผลกระทบจากภัยคุกคามทางไซเบอร์

6.2 โครงสร้างทีมสนับสนุนการดำเนินการรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (ทีมสนับสนุน)

ลำดับที่	ชื่อ นามสกุล รายละเอียดการติดต่อ	หน้าที่	ความรับผิดชอบ
1	นายพรศักดิ์ ตามวงศ์ หัวหน้ากลุ่มสุขภาพดิจิทัล โทร 053 603100 ต่อ 3163	เจ้าหน้าที่ควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์	ทำหน้าที่ควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์
2	นางอรุณี ไชยเมือง หัวหน้ากลุ่มผู้ป่วยใน โทร 053 603100 ต่อ 3102	เจ้าหน้าที่ด้านการปฏิบัติตามกฎหมาย (Compliance)	ทำหน้าที่ตามนโยบาย หรือ คำสั่งที่เกี่ยวข้อง
3	นางสาวรำไพ ยารวง เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล โทร 053 603100 ต่อ 1104	เจ้าหน้าที่ด้านการปฏิบัติตามกฎหมาย (Compliance)	ทำหน้าที่ตามนโยบาย หรือ คำสั่งที่เกี่ยวข้อง
4	นางสาวมันทนา บุศเมือง โทร 053 603114 ต่อ	ผู้รับผิดชอบด้านสื่อสารองค์กร	ทำหน้าที่ตามนโยบาย หรือ คำสั่งที่เกี่ยวข้อง
5	นายศราวุธ ชัยรัตน์ โทร 053 603100 ต่อ 3144	ผู้รับผิดชอบด้านสื่อสารองค์กร	ทำหน้าที่ตามนโยบาย หรือ คำสั่งที่เกี่ยวข้อง
6	นายสุทธิชัย เสาวสิงห์ โทร 053 603100 ต่อ 3163	เจ้าหน้าที่เทคนิค	ทำหน้าที่ตามนโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
7	ภก.ปชชน อนุพงศานุกุล โทร 053 603100 ต่อ 3115	ผู้บริหารจัดการความเสี่ยง	ทำหน้าที่ตามนโยบาย หรือ คำสั่งที่เกี่ยวข้อง
8	ทต.ญ บงกช บัณฑิตศตฤกุล โทร 0 2590 1169	ผู้บริหารจัดการความเสี่ยง	ทำหน้าที่ตามนโยบาย หรือ คำสั่งที่เกี่ยวข้อง

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของโรงพยาบาลแม่ลาว ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตโรงพยาบาลแม่ลาว เอกสารกระดาษนี้ ถือเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

	แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan Procedure)	รหัสเอกสาร	MLH-MOPH-IR Plan -01
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ ชั้นความลับของ เอกสาร	5 ม.ค 2569 ใช้ภายในเท่านั้น

6.3 โครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure)

โครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure) ตามแผนฉบับนี้ เป็นการกำหนดตามประมวลและแนวทางปฏิบัติฯ ว่าหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจะปฏิบัติตามภาระหน้าที่ในการรายงานภายใต้พระราชบัญญัติ และกฎหมายย่อยใด ๆ ที่ทำขึ้นภายใต้กฎหมายดังกล่าว ตลอดจนภาระหน้าที่ในการรายงานภายใต้กฎหมาย และข้อกำหนดด้านกฎระเบียบที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยมีโครงสร้างการรายงานและ Flow การรายงาน ตามภาคผนวก ก

7. แผนรับมือเหตุการณ์ทางไซเบอร์

7.1 การโจมตีเว็บไซต์เพื่อเปลี่ยนแปลงข้อมูลเผยแพร่หน้าเว็บ (Web Defacement)

ข้อ	รายละเอียดขั้นตอน/กิจกรรม/กระบวนการปฏิบัติ	ผู้รับผิดชอบ
1	ติดต่อประสานงานผู้ที่เกี่ยวข้อง ทีมสนับสนุนดำเนินการแจ้งเหตุการณ์ถูกโจมตีเว็บไซต์เพื่อเปลี่ยนแปลงข้อมูลเผยแพร่หน้าเว็บ (Web Defacement) ไปยังทีมบริหาร เพื่อแนะนำและพิจารณาอนุมัติดำเนินการตามแผนรับมือเหตุการณ์ทางไซเบอร์ และติดต่อประสานไปผู้ที่เกี่ยวข้อง	ทีมแม่ลาว CSIRT
2	ทีมบริหารให้คำแนะนำและอนุมัติดำเนินการตามแผนรับมือเหตุการณ์ทางไซเบอร์	ทีมบริหาร
3	ดำเนินการตัดการเชื่อมต่อของระบบ	ทีมแม่ลาว CSIRT
4	ทีมสนับสนุนเก็บรวบรวมและจัดการหลักฐานต่าง ๆ ที่เกี่ยวข้องกับการก่อกำเนิดภัยคุกคามทางไซเบอร์ เช่น - การจัดการกับข้อมูลที่บ้านที่อยู่ในหน่วยความจำประเภทที่สามารถสูญหายได้เมื่อทำการปิดอุปกรณ์ (Volatile data) - การเก็บข้อมูลจราจรทางคอมพิวเตอร์ (logs) - ข้อมูลสถานะของระบบ (system snapshot)	ทีมแม่ลาว CSIRT

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของโรงพยาบาลแม่ลาว ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตโรงพยาบาลแม่ลาว เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ




แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan Procedure)

รหัสเอกสาร	MLH-MOPH-IR Plan -01
แก้ไขครั้งที่	00
วันที่บังคับใช้ ชั้นความลับของ เอกสาร	5 ม.ค 2569 ใช้ภายในเท่านั้น

ข้อ	รายละเอียดขั้นตอน/กิจกรรม/กระบวนการปฏิบัติ	ผู้รับผิดชอบ
	- ข้อมูลอื่น ๆ ที่จำเป็นให้เพียงพอสำหรับใช้วิเคราะห์ในเชิงเทคนิค และ เพื่อทางนิติวิทยาศาสตร์และใช้เป็นพยานหลักฐานในการดำเนินคดี	
5	ทีมสนับสนุนดำเนินการวิเคราะห์ ดังนี้ - เพื่อระบุแหล่งที่มาของการโจมตี (attacking host) เช่น การระบุหมายเลขประจำเครื่อง (IP address) การระบุช่องทางที่ผู้โจมตีใช้การค้นหาและวิจัยที่มาของการโจมตีจากแหล่งข้อมูลต่าง ๆ เช่น ฐานข้อมูลภัยคุกคามทางไซเบอร์ที่รวบรวมข้อมูลจากหลายแหล่ง - ตรวจสอบช่องโหว่ที่ทำให้เกิดเหตุการณ์ถูกโจมตีเว็บไซต์เพื่อเปลี่ยนแปลงข้อมูลเผยแพร่หน้าเว็บ (Web Defacement)	ทีมสนับสนุน
6	ทีมสนับสนุนดำเนินการตั้งค่าระบบให้มีความมั่นคงปลอดภัย ดังนี้ - การปรับเปลี่ยนการควบคุมการเข้าถึงเครือข่ายจากเซก อุปกรณ์ Firewall อุปกรณ์เครือข่าย เป็นต้น - การติดตั้งหรือ Update Anti-Virus หรือ IDS/IPS - การเปลี่ยนแปลงทางกายภาพโครงสร้างพื้นฐาน - ดำเนินการระงับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นโดยทันทีหลังจากที่ตรวจพบ	ทีมสนับสนุน
7	ทีมสนับสนุนดำเนินการกู้คืนระบบโดยพิจารณา วิธีการตามความเหมาะสมได้ ดังนี้ - การกู้คืนระบบให้กลับมาดำเนินการได้ตามปกติ (integrity restoration) - การสร้างระบบงานขึ้นใหม่ (rebuild) - การแทนที่ไฟล์ที่ได้รับผลกระทบ (replace) - การติดตั้งโปรแกรมคอมพิวเตอร์ (install) - การเปลี่ยนแปลงรหัสผ่านของเครื่อง Web Server - การปรับปรุงหรือ Update ระบบปฏิบัติการ (OS)	ทีมสนับสนุน
8	ทีมสนับสนุนกำหนดการเฝ้าระวังในการถูกโจมตีซ้ำ	ทีมสนับสนุน
9	ทีมสนับสนุนตรวจสอบข้อมูลและการใช้งานของระบบ เพื่อกลับมาใช้งานได้อย่างปกติ	ทีมสนับสนุน

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของโรงพยาบาลแม่ลาว ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตโรงพยาบาลแม่ลาว เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

	แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan Procedure)	รหัสเอกสาร	MLH-MOPH-IR Plan -01
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ ชั้นความลับของ เอกสาร	5 ม.ค 2569 ใช้ภายในเท่านั้น

ข้อ	รายละเอียดขั้นตอน/กิจกรรม/กระบวนการปฏิบัติ	ผู้รับผิดชอบ
10	ติดต่อประสานงานผู้ที่เกี่ยวข้อง ทีมสนับสนุนแจ้งผลการดำเนินการตามแผนรับมือเหตุการณ์ทางไซเบอร์ไปยังทีมบริหารและ ผู้ที่เกี่ยวข้องรับทราบ Web Site กลับมาใช้งานได้อย่างปกติ	ทีมสนับสนุน

7.2 การถูกโจมตีจากโปรแกรมประสงค์ร้ายเข้ารหัสข้อมูลเรียกค่าไถ่ (Ransomware) / การโจมตียึด
 เครื่องแม่ข่าย (Server compromise injection attack) / การบุกรุกโดยการไข่มัลแวร์
 (Malicious Logic)

ข้อ	รายละเอียดขั้นตอน/กิจกรรม/กระบวนการปฏิบัติ	ผู้รับผิดชอบ
1	ติดต่อประสานงานผู้ที่เกี่ยวข้อง ทีมสนับสนุนดำเนินการแจ้งเหตุการณ์ถูกโจมตีจากโปรแกรมประสงค์ร้ายเข้ารหัสข้อมูลเรียก ค่าไถ่ (Ransomware) ไปยังทีมบริหาร เพื่อแนะนำและพิจารณาอนุมัติดำเนินการตามแผน รับมือเหตุการณ์ทางไซเบอร์ และติดต่อประสานไปผู้ที่เกี่ยวข้อง	ทีมแม่ลาว CSIRT
2	ทีมบริหารให้คำแนะนำและอนุมัติดำเนินการตามแผนรับมือเหตุการณ์ทางไซเบอร์	ทีมบริหาร
3	ดำเนินการตัดการเชื่อมต่อของระบบ	ทีมสนับสนุน
4	ทีมสนับสนุนเก็บรวบรวมและจัดการหลักฐานต่าง ๆ ที่เกี่ยวข้องกับการก่อกำเนิดภัยคุกคาม ทางไซเบอร์ เช่น <ul style="list-style-type: none"> - การจัดการกับข้อมูลที่บันทึกอยู่ในหน่วยความจำประเภทที่สามารถสูญหายได้เมื่อทำ การปิดอุปกรณ์ (Volatile data) - การเก็บข้อมูลจราจรทางคอมพิวเตอร์ (logs) - ข้อมูลสถานะของระบบ (system snapshot) - ข้อมูลอื่น ๆ ที่จำเป็นให้เพียงพอสำหรับใช้วิเคราะห์ในเชิงเทคนิค และ เพื่อทางนิติ วิทยาศาสตร์และใช้เป็นพยานหลักฐานในการดำเนินคดี 	ทีมสนับสนุน

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น
 กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของโรงพยาบาลแม่ลาว ห้ามแจกจ่ายไปยัง
 บุคคลภายนอกโดยไม่ได้รับอนุญาตโรงพยาบาลแม่ลาว เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้
 ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ




แผนการรับมือภัยคุกคามทางไซเบอร์

(Cybersecurity Incident Response Plan Procedure)

รหัสเอกสาร	MLH-MOPH-IR Plan -01
แก้ไขครั้งที่	00
วันที่บังคับใช้ ชั้นความลับของเอกสาร	5 ม.ค 2569 ใช้ภายในเท่านั้น

ข้อ	รายละเอียดขั้นตอน/กิจกรรม/กระบวนการปฏิบัติ	ผู้รับผิดชอบ
5	ทีมสนับสนุนดำเนินการวิเคราะห์ ดังนี้ <ul style="list-style-type: none"> - เพื่อระบุแหล่งที่มาของการโจมตี (attacking host) เช่น การระบุหมายเลขประจำเครื่อง (IP address) การระบุช่องทางที่ผู้โจมตีใช้การค้นหาและวิจัยที่มาของการโจมตีจากแหล่งข้อมูลต่าง ๆ เช่น - ฐานข้อมูลภัยคุกคามทางไซเบอร์ที่รวบรวมข้อมูลจากหลายแหล่ง - ตรวจสอบช่องโหว่ที่ทำให้เกิดเหตุการณ์ถูกโจมตี 	ทีมสนับสนุน
6	ทีมสนับสนุนดำเนินการตั้งค่าระบบให้มีความมั่นคงปลอดภัย ดังนี้ <ul style="list-style-type: none"> - การปรับเปลี่ยนการควบคุมการเข้าถึงเครือข่ายจากเซ่น อุปกรณ์ Firewall อุปกรณ์เครือข่าย เป็นต้น - การติดตั้งหรือ Update Anti-Virus หรือ IDS/IPS - การเปลี่ยนแปลงทางกายภาพโครงสร้างพื้นฐาน - ดำเนินการระงับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นโดยทันทีหลังจากที่ตรวจพบ 	ทีมสนับสนุน
7	ทีมสนับสนุนดำเนินการกู้คืนระบบโดยพิจารณา วิธีการตามความเหมาะสมได้ ดังนี้ <ul style="list-style-type: none"> - การกู้คืนระบบให้กลับมาดำเนินการได้ตามปกติ (integrity restoration) - การสร้างระบบงานขึ้นใหม่ (rebuild) - การแทนที่ไฟล์ที่ได้รับผลกระทบ (replace) - การติดตั้งโปรแกรมคอมพิวเตอร์ (install) - การเปลี่ยนแปลงรหัสผ่านของเครื่องแม่ข่าย - การปรับปรุงหรือ Update ระบบปฏิบัติการ (OS) 	ทีมสนับสนุน
8	ทีมสนับสนุนกำหนดการเฝ้าระวังในการถูกโจมตีซ้ำ	ทีมสนับสนุน
9	ทีมสนับสนุนตรวจสอบข้อมูลและการใช้งานของระบบ เพื่อกลับมาใช้งานได้ปกติ	ทีมสนับสนุน
10	ติดต่อประสานงานผู้ที่เกี่ยวข้อง ทีมสนับสนุนแจ้งผลการดำเนินการตามแผนรับมือเหตุการณ์ทางไซเบอร์ไปยังทีมบริหารและผู้ที่ส่วนเกี่ยวข้องรับทราบว่าจะระบบกลับมาใช้งานได้ปกติ	ทีมสนับสนุน


เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของโรงพยาบาลแม่ลาว ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตโรงพยาบาลแม่ลาว เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา "สำเนาควบคุม" เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

	แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan Procedure)	รหัสเอกสาร	MLH-MOPH-IR Plan -01
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ ชั้นความลับของ เอกสาร	5 ม.ค 2569 ใช้ภายในเท่านั้น

7.3 การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)

ข้อ	รายละเอียดขั้นตอน/กิจกรรม/กระบวนการปฏิบัติ	ผู้รับผิดชอบ
1	ติดต่อประสานงานผู้ที่เกี่ยวข้อง ทีมสนับสนุนดำเนินการแจ้งเหตุการณ์การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service) ไปยังทีมบริหาร เพื่อแนะนำและพิจารณาอนุมัติดำเนินการตามแผนรับมือเหตุการณ์ทางไซเบอร์ และติดต่อประสานไปผู้ที่เกี่ยวข้อง	ทีมสนับสนุน
2	ทีมบริหารให้คำแนะนำและอนุมัติดำเนินการตามแผนรับมือเหตุการณ์ทางไซเบอร์	ทีมบริหาร
3	ทีมสนับสนุนประสานผู้ให้บริการภายนอกเพื่อปิดกั้นการบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)	ทีมสนับสนุน
4	ทีมสนับสนุนเก็บรวบรวมและจัดการหลักฐานต่าง ๆ ที่เกี่ยวข้องกับการก่อกำเนิดภัยคุกคามทางไซเบอร์ เช่น <ul style="list-style-type: none"> - การจัดการกับข้อมูลที่บันทึกอยู่ในหน่วยความจำประเภทที่สามารถสูญหายได้เมื่อทำการปิดอุปกรณ์ (Volatile data) - การเก็บข้อมูลจราจรทางคอมพิวเตอร์ (logs) - ข้อมูลสถานะของระบบ (system snapshot) - ข้อมูลอื่น ๆ ที่จำเป็นให้เพียงพอสำหรับใช้วิเคราะห์ในเชิงเทคนิค และ เพื่อทางนิติวิทยาศาสตร์และใช้เป็นพยานหลักฐานในการดำเนินคดี 	ทีมสนับสนุน
5	ทีมสนับสนุนดำเนินการวิเคราะห์ ดังนี้ <ul style="list-style-type: none"> - เพื่อระบุแหล่งที่มาของการโจมตี (attacking host) เช่น การระบุหมายเลขประจำเครื่อง (IP address) การระบุช่องทางที่ผู้โจมตีใช้การค้นหาและวิจัยที่มาของการโจมตีจากแหล่งข้อมูลต่าง ๆ เช่น ฐานข้อมูลภัยคุกคามทางไซเบอร์ที่รวบรวมข้อมูลจากหลายแหล่ง - ตรวจสอบช่องโหว่ที่ทำให้เกิดเหตุการณ์การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service) 	ทีมสนับสนุน

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของโรงพยาบาลแม่ลาว ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตโรงพยาบาลแม่ลาว เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

	แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan Procedure)	รหัสเอกสาร	MLH-MOPH-IR Plan -01
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ ชั้นความลับของ เอกสาร	5 ม.ค 2569 ใช้ภายในเท่านั้น


ข้อ	รายละเอียดขั้นตอน/กิจกรรม/กระบวนการปฏิบัติ	ผู้รับผิดชอบ
6	ทีมสนับสนุนดำเนินการตั้งค่าระบบให้มีความมั่นคงปลอดภัย ดังนี้ - การปรับเปลี่ยนการควบคุมการเข้าถึงเครือข่ายจากเซ่น อุปกรณ์ Firewall อุปกรณ์เครือข่าย เป็นต้น - การติดตั้งหรือ Update Anti-Virus หรือ IDS/IPS - การเปลี่ยนแปลงทางกายภาพโครงสร้างพื้นฐาน - ดำเนินการระงับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นโดยทันทีหลังจากที่ตรวจพบ	ทีมสนับสนุน
7	ทีมสนับสนุนกำหนดการเฝ้าระวังในการถูกโจมตีซ้ำ	ทีมสนับสนุน
8	ทีมสนับสนุนตรวจสอบข้อมูลและการใช้งานของระบบ เพื่อกลับมาใช้งานได้อย่างปกติ	ทีมสนับสนุน
9	ติดต่อประสานงานผู้ที่เกี่ยวข้อง ทีมสนับสนุนแจ้งผลการดำเนินการตามแผนรับมือเหตุการณ์ทางไซเบอร์ไปยังทีมบริหารและ ผู้ที่เกี่ยวข้องรับทราบว่าจะระบบในการให้บริการกลับมาใช้งานได้ปกติ	ทีมสนับสนุน

8. การติดตาม ควบคุม และทบทวน

แผนการรับมือภัยคุกคามฉบับนี้ จะต้องมีการติดตาม ควบคุม และทบทวน ดังนี้

- 1) ต้องติดตามและควบคุมให้แผนการรับมือภัยคุกคามทางไซเบอร์ฉบับนี้ได้มีการสื่อสารไปยังบุคลากรที่เกี่ยวข้องทั้งหมดอย่างมีประสิทธิภาพ เพื่อสนับสนุนบริการสำคัญของโรงพยาบาลแม่ลาว
- 2) ทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ฉบับนี้ อย่างน้อยปีละ 1 ครั้ง โดยนับแต่วันที่แผนได้รับการอนุมัติ
- 3) ทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ฉบับนี้ เมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญในสภาพแวดล้อมการปฏิบัติการทางไซเบอร์ของบริการที่สำคัญของโรงพยาบาลแม่ลาว หรือข้อกำหนดในการตอบสนองต่อเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์

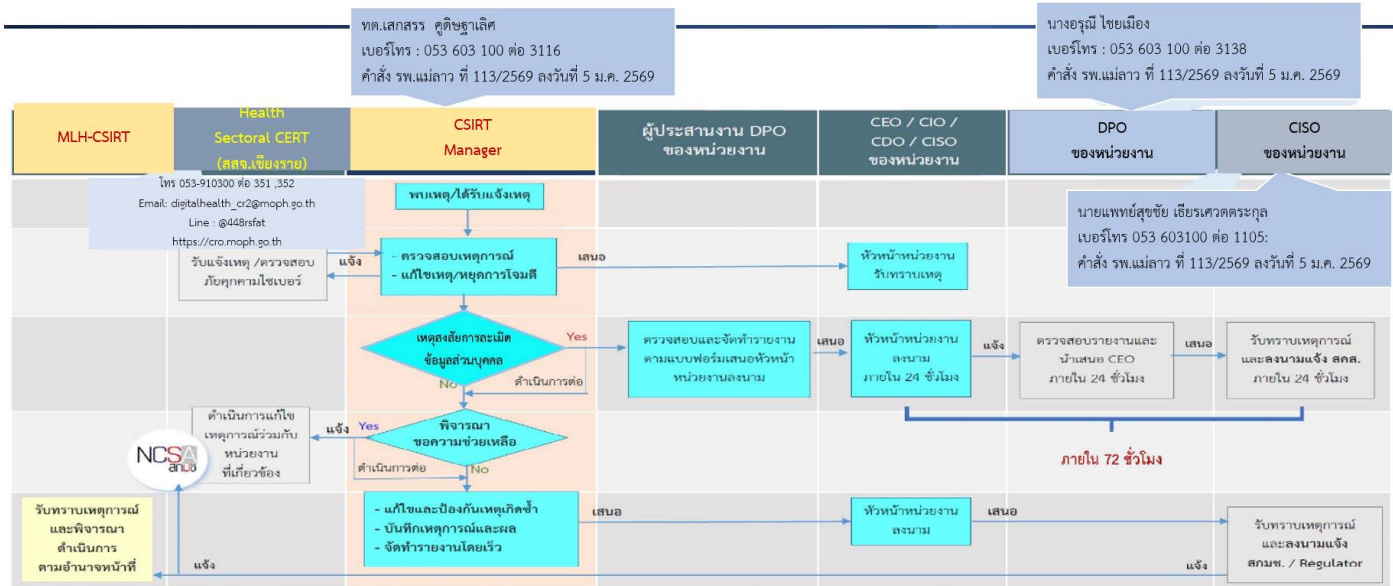
เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของโรงพยาบาลแม่ลาว ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตโรงพยาบาลแม่ลาว เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

	แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan Procedure)	รหัสเอกสาร	MLH-MOPH-IR Plan -01
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ ชั้นความลับของ เอกสาร	5 ม.ค 2569 ใช้ภายในเท่านั้น


ภาคผนวก

ภาคผนวก ก

โครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure) และ Flow การรายงาน



เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของโรงพยาบาลแม่ลาว ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตโรงพยาบาลแม่ลาว เอกสารกระดาษนี้ ถือเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

	แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan Procedure)	รหัสเอกสาร	MLH-MOPH-IR Plan -01
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ ชั้นความลับของ เอกสาร	5 ม.ค 2569 ใช้ภายในเท่านั้น

ภาคผนวก ข


ข้อ 1 การจำแนกหมวดหมู่ของภัยคุกคามทางไซเบอร์

หมวดหมู่	คำอธิบาย
0	เหตุการณ์จำลองและการฝึกซ้อมของหน่วยงานเอง (Training and Exercises)
1	การพยายามเข้าถึงระบบที่ไม่สำเร็จ (Unsuccessful Activity Attempt)
2	การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance)
3	การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยที่หน่วยงานกำหนด (Non-Compliance Activity)
4	การบุกรุกโดยการใช้มัลแวร์ (Malicious Logic)
5	การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion)
6	การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion)
7	การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)
8	เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating)
9	เหตุการณ์ผิดปกติที่ได้รับการวิเคราะห์แล้วว่าไม่ใช่เหตุการณ์ที่เป็นภัยคุกคาม (Explained Anomaly)

ข้อ 2 ตัวอย่างลักษณะภัยคุกคามทางไซเบอร์แยกตามระดับต่าง ๆ

ประเภทอุปกรณ์เครือข่าย	หมวดหมู่ภัยคุกคาม						
	1	2	3	4	5	6	7
Backbone	ไม่ ร้ายแรง	ไม่ ร้ายแรง	ไม่ ร้ายแรง	ไม่ ร้ายแรง	วิกฤต	วิกฤต	วิกฤต
เราเตอร์	ไม่ ร้ายแรง	ไม่ ร้ายแรง	ร้ายแรง	ไม่ ร้ายแรง	วิกฤต	วิกฤต	วิกฤต
เครื่องแม่ข่ายสำหรับการจัดการ เครือข่าย หรือ ดูแลความปลอดภัย	ไม่ ร้ายแรง	ไม่ ร้ายแรง	ร้ายแรง	ร้ายแรง	วิกฤต	วิกฤต	วิกฤต

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของโรงพยาบาลแม่ลาว ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตโรงพยาบาลแม่ลาว เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

	แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan Procedure)	รหัสเอกสาร	MLH-MOPH-IR Plan -01
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ ชั้นความลับของ เอกสาร	5 ม.ค 2569 ใช้ภายในเท่านั้น


ประเภทอุปกรณ์เครือข่าย	หมวดหมู่ภัยคุกคาม						
	1	2	3	4	5	6	7
เครื่องแม่ข่ายที่ไม่ได้ให้บริการกับ สาธารณะ	ไม่ ร้ายแรง	ไม่ ร้ายแรง	ร้ายแรง	ร้ายแรง	วิกฤต	ร้ายแรง	ร้ายแรง
เครื่องแม่ข่ายที่เปิดให้บริการกับ สาธารณะ	ไม่ ร้ายแรง	ไม่ ร้ายแรง	ไม่ ร้ายแรง	ร้ายแรง	ไม่ ร้ายแรง	ไม่ ร้ายแรง	ร้ายแรง
เครื่องเวิร์กสเตชัน	ไม่ ร้ายแรง	ไม่ ร้ายแรง	ไม่ ร้ายแรง	ร้ายแรง	ไม่ ร้ายแรง	ไม่ ร้ายแรง	ร้ายแรง

ข้อ 3 ตัวอย่างกำหนดระยะเวลาในการแจ้งและรายงานภัยคุกคามทางไซเบอร์

การแจ้งหรือรายงานภัยคุกคามตามหมวดนี้เกิดขึ้นเมื่อผู้เผชิญเหตุยังไม่ทราบรายละเอียดภัยคุกคาม และกำลังดำเนินการวิเคราะห์เหตุการณ์ (เช่น อาจอยู่ในช่วงแรก ๆ ที่พบการกระทำผิด) โดยหากทราบผลของการสอบสวนแล้ว ผู้รายงานควรเปลี่ยนเป็นหมวดอื่นให้ถูกต้อง และ ในรายงานสรุปปิดเหตุการณ์ ไม่ควรมีภัยคุกคามที่อยู่ในหมวดนี้ เนื่องจากการวิเคราะห์สอบสวนเสร็จสิ้นแล้ว)

หมวดหมู่ภัย คุกคามทาง ไซเบอร์	ระดับภัยคุกคาม ทางไซเบอร์	การแจ้งเบื้องต้นตาม ช่องทางที่กำหนด (ภายในเวลา)	การส่งรายงานให้ หน่วยงานควบคุมหรือ กำกับดูแล (ภายในเวลา)	การส่งรายงานให้ สำนักงานสาธารณสุข จังหวัดเชียงราย (ภายในเวลา)
1	ทุกเหตุการณ์	30 นาที	2 ชั่วโมง	4 ชั่วโมง
2	ทุกเหตุการณ์	ตามหน่วยงานกำหนด	ตามหน่วยงานกำหนด	ตามหน่วยงานกำหนด
3	ทุกเหตุการณ์	30 นาที	2 ชั่วโมง	8 ชั่วโมง
4	วิกฤต	10 นาที	30 นาที	1 ชั่วโมง
	ร้ายแรง	20 นาที	1 ชั่วโมง	2 ชั่วโมง
	ไม่ร้ายแรง	ตามหน่วยงานกำหนด	ตามหน่วยงานกำหนด	ตามหน่วยงานกำหนด
5	วิกฤต	10 นาที	30 นาที	1 ชั่วโมง
	ร้ายแรง	20 นาที	1 ชั่วโมง	2 ชั่วโมง
	ไม่ร้ายแรง	30 นาที	2 ชั่วโมง	4 ชั่วโมง

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของโรงพยาบาลแม่ลาว ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตโรงพยาบาลแม่ลาว เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

	แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan Procedure)	รหัสเอกสาร	MLH-MOPH-IR Plan -01
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ ชั้นความลับของ เอกสาร	5 ม.ค 2569 ใช้ภายในเท่านั้น


หมวดหมู่ภัย คุกคามทาง ไซเบอร์	ระดับภัยคุกคาม ทางไซเบอร์	การแจ้งเบื้องต้นตาม ช่องทางที่กำหนด (ภายในเวลา)	การส่งรายงานให้ หน่วยงานควบคุมหรือ กำกับดูแล (ภายในเวลา)	การส่งรายงานให้ สำนักงานสาธารณสุข จังหวัดเชียงราย (ภายในเวลา)
6	วิกฤต	10 นาที	30 นาที	1 ชั่วโมง
	ร้ายแรง	20 นาที	1 ชั่วโมง	2 ชั่วโมง
	ไม่ร้ายแรง	30 นาที	2 ชั่วโมง	4 ชั่วโมง
7	วิกฤต	10 นาที	30 นาที	1 ชั่วโมง
	ร้ายแรง	30 นาที	1 ชั่วโมง	1 ชั่วโมง
	ไม่ร้ายแรง	ตามหน่วยงานกำหนด	ตามหน่วยงานกำหนด	ตามหน่วยงานกำหนด
8	-	20 นาที	ตามเวลาที่ต้องใช้ในการ การสืบสวน	4 ชั่วโมง
9	-	-	4 ชั่วโมง	12 ชั่วโมง

ภาคผนวก ค

ข้อ 1 วิธีการ/ขั้นตอนจำกัดขอบเขตหรือควบคุมความเสียหาย (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ โดยพิจารณาเลือกใช้ที่เหมาะสม ดังนี้

- 1) ตัดการเชื่อมต่อทางเครือข่ายทั้งหมด (Network disconnection) ทั้งนี้ อาจมียกเว้นการเชื่อมต่อสำหรับ Endpoint Detection & Response Agent (กระบวนการตรวจสอบและตรวจจับกิจกรรมหรือเหตุการณ์ที่น่าสงสัยใด ๆ ที่เกิดขึ้นที่ปลายทางแบบเรียลไทม์)
- 2) แยกระบบที่ได้รับผลกระทบออกจากเครือข่ายหลักเพื่อป้องกันการแพร่กระจายไปยังระบบอื่น
- 3) หยุดการทำงานของฟังก์ชันที่เกี่ยวข้อง (Disabling Certain Functions)
- 4) Redirect Network Traffic และ/หรือความสนใจของผู้บุกรุกไปยัง Black hole/ Sandbox/ Honeypot
- 5) ประเมินความเสียหายและระบุว่ามีระบบใดที่เกี่ยวข้อง

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของโรงพยาบาลแม่ลาว ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตโรงพยาบาลแม่ลาว เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ


	แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan Procedure)	รหัสเอกสาร	MLH-MOPH-IR Plan -01
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ ชั้นความลับของ เอกสาร	5 ม.ค 2569 ใช้ภายในเท่านั้น

- 6) ดำเนินการแก้ไขเบื้องต้น เช่น การปิดพอร์ตที่ถูกโจมตีหรือการบล็อก IP ที่มีพฤติกรรมไม่พึงประสงค์
- 7) เก็บข้อมูลสำคัญจากระบบที่ได้รับผลกระทบเพื่อใช้ในกระบวนการสอบสวน
 ทั้งนี้ การตัดสินใจเลือกใช้วิธีการ/ขั้นตอนใดที่จะจำกัดขอบเขตหรือควบคุมความเสียหาย ขึ้นอยู่กับลักษณะสถานการณ์ที่กำลังเผชิญประเภทของภัยคุกคาม ระบบงานหรือบริการที่ได้รับผลกระทบ ระยะเวลาและทรัพยากรที่จำเป็นต่อการควบคุมความเสียหาย

ข้อ 2 การจัดเก็บและดูแลรักษาหลักฐาน (Preservation of Evidence) ก่อนเริ่มกระบวนการกู้คืนซึ่งรวมถึงการได้มาของบันทึกการยึดหลักฐานคอมพิวเตอร์ที่ได้มา หรืออุปกรณ์อื่น ๆ เพื่อสนับสนุนการสอบสวน
 วัตถุประสงค์หลักของการจัดเก็บหลักฐาน คือ เพื่อให้การแก้ไข Incident ส่งผลกระทบต่อธุรกิจให้น้อยที่สุด (Minimizing impact to the business) นอกจากนี้ หลักฐานอาจมีความจำเป็นที่จะต้องใช้ในการดำเนินการตามขั้นตอนทางกฎหมาย ดังนั้น การดำเนินการจัดเก็บหลักฐานทางดิจิทัลสามารถดำเนินการโดยพิจารณาตามหลักการ/ขั้นตอน ที่เหมาะสม ดังนี้

- 1) ดำเนินการให้เป็นไปตามขั้นตอนที่กำหนดไว้ในกฎหมายข้อบังคับที่เกี่ยวข้องกับหลักฐานดิจิทัล เพื่อให้สามารถนำไปใช้ได้ในพื้นที่ศาล
 - 2) บันทึกการเข้าถึงและการกระทำการใด ๆ ต่อหลักฐานตลอดเวลาอย่างรัดกุม
 - 3) บันทึกรายละเอียดเกี่ยวกับหลักฐาน ควรประกอบด้วยข้อมูลอย่างน้อยดังต่อไปนี้
 - 3.1) ข้อมูลเฉพาะ เช่น Location, Serial Number, Model Number, Hostname, Media Access Control (MAC) และ Address เป็นต้น
 - 3.2) ชื่อ ตำแหน่ง และช่องทางการติดต่อผู้จัดเก็บและรักษาหลักฐานระหว่างการรับมือ Incident
 - 3.3) สถานที่จัดเก็บหลักฐาน
 - 4) บันทึกข้อมูลจากระบบที่ได้รับผลกระทบ เช่น ล็อกไฟล์ การจับภาพหน้าจอ และอุปกรณ์เครือข่ายที่เกี่ยวข้อง
 - 5) จัดเก็บอุปกรณ์ที่มีหลักฐานไว้ในที่ปลอดภัยเพื่อป้องกันการดัดแปลง เช่น จัดเก็บในตู้ที่มีการล็อก และการควบคุมการเข้าถึง
 - 6) ทำรายการหลักฐานทั้งหมดที่ถูกเก็บรวบรวม พร้อมระบุวันที่และเวลาที่รับหลักฐาน
- ทั้งนี้ให้พิจารณาดูแลรักษาหลักฐานทางดิจิทัลที่สำคัญตามขั้นตอน ดังนี้

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งหมดฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของโรงพยาบาลแม่ลาว ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตโรงพยาบาลแม่ลาว เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

	แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan Procedure)	รหัสเอกสาร	MLH-MOPH-IR Plan -01
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ ชั้นความลับของ เอกสาร	5 ม.ค 2569 ใช้ภายในเท่านั้น


1. Assessment	การประเมินเพื่อหาจุดที่ต้องดำเนินการจัดเก็บหลักฐานของ incident ที่กำลังรับมือ และตอบสนอง เช่น Hard Disk, RAM, External Hard Disk, Mobile Device เป็นต้น
2. Acquisition	ดำเนินการจัดเก็บหลักฐานด้วยการทำสำเนา (Duplication/Bit-for-bit Acquisition) ด้วยเครื่องมือที่เหมาะสม โดยมีข้อควรระวังในเรื่องดังต่อไปนี้ 1. ต้องป้องกันการเปลี่ยนแปลงของหลักฐานด้วยการใช้งาน Hardware Write Blocker 2. ต้องคำนึงถึง Volatility หรือความอ่อนไหวต่อการสูญเสียกระแสไฟฟ้าของหลักฐาน เช่น ข้อมูลที่เสี่ยงต่อการสูญหายหากไม่มีกระแสไฟคอยเลี้ยง เช่น RAM ต้องได้รับการเก็บรักษาเป็นอันดับแรก เป็นต้น 3. ต้องบันทึกรายละเอียดการดำเนินงานทุกขั้นตอนที่ลงมือปฏิบัติอย่างละเอียด 4. ต้องทำการบันทึกหลักฐาน (Chain of Custody)
3. Authentication	ทำการตรวจสอบความถูกต้องของหลักฐานที่ Duplicate และเปรียบเทียบกับต้นฉบับ ด้วยวิธี Cryptographic Hash เช่น MD5, SHA1, SHA256
4. Analysis & Report	วิเคราะห์หาข้อมูลจากชุดหลักฐานที่ดำเนินการจัดเก็บเพื่อพิสูจน์ข้อเท็จจริง หรือเพื่อ ค้นหาสาเหตุของการเกิด Incident
5. Archive	จัดเก็บหลักฐานไว้ในที่ที่เหมาะสม ปลอดภัย และบันทึก Chain of Custody Form ทุกครั้งที่มีการเคลื่อนย้ายหลักฐาน พร้อมทั้งระบุเหตุผลของการเคลื่อนย้าย

ข้อ 3 การจัดการสาเหตุ

เมื่อมีการจำกัดขอบเขต/การควบคุมความเสียหาย และมีการเก็บหลักฐานข้อมูลเรียบร้อยแล้วข้อมูลทั้งหมดจะต้องนำกลับมาวิเคราะห์ตามหลักการในขั้นตอนที่ 2 การตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ จนกว่าจะสามารถจัดการสาเหตุที่ทำให้เกิด Incident และจัดการช่องทางที่ผู้บุกรุกได้สร้างไว้เพื่อเข้ามาในโจมตีระบบทั้งหมดได้เรียบร้อยแล้ว ซึ่งการจัดการสาเหตุที่ทำให้เกิด Incident และผลกระทบ พิจารณาดำเนินการ ดังนี้

- 1) ปิดช่องโหว่ของระบบ
- 2) ยกเลิก User Account ที่ผู้บุกรุกใช้เข้าสู่ระบบ

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของโรงพยาบาลแม่ลาว ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตโรงพยาบาลแม่ลาว เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

	แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan Procedure)	รหัสเอกสาร	MLH-MOPH-IR Plan -01
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ ชั้นความลับของ เอกสาร	5 ม.ค 2569 ใช้ภายในเท่านั้น

- 3) แจ้งให้ผู้ใช้งานเปลี่ยนรหัสผ่าน
- 4) ลบโปรแกรมประเภท Backdoor ออกจากระบบ
- 5) ใช้ข้อมูล Indicator of Compromise (IoC) ในการสแกนหา Malware หรือร่องรอยอื่น ๆ ในระบบที่ยังหลงเหลือของผู้บุกรุกเพื่อดำเนินการจัดการให้ออกจากระบบทั้งหมด

ข้อ 4 การสอบสวน (Investigation)


- 1) เก็บหลักฐานทางดิจิทัลจากระบบที่ได้รับผลกระทบ เช่น ไฟล์ล็อก การจับภาพหน้าจอ การตรวจสอบ ข้อมูลเครือข่าย
- 2) วิเคราะห์สาเหตุของเหตุการณ์ เช่น ตรวจสอบวิธีการที่ผู้โจมตีใช้ในการเข้าถึงระบบ
- 3) ระบุผู้ที่อาจรับผิดชอบต่อเหตุการณ์ เช่น การระบุที่อยู่ IP หรือการตรวจสอบพฤติกรรมที่ผิดปกติ
- 4) จัดทำรายงานการสอบสวนและเสนอแนวทางการป้องกันเพื่อไม่ให้เกิดเหตุการณ์ซ้ำในอนาคต

ข้อ 5 การกู้คืนระบบให้กลับมาทำงานปกติ

หลังจากจำกัดขอบเขต/การควบคุมความเสียหาย จัดการสาเหตุของภัยคุกคามเสร็จเรียบร้อยแล้ว จะเข้าสู่กระบวนการกู้คืนระบบ/การฟื้นฟูระบบให้เข้าสู่สภาวะการทำงานปกติ ซึ่งจะต้องจัดเตรียมข้อมูลสำหรับกู้คืนระบบไว้ก่อน โดยพิจารณาดำเนินการ ดังนี้

- 1) ตรวจสอบและซ่อมแซมระบบที่ได้รับผลกระทบเพื่อให้แน่ใจว่าไม่มีช่องโหว่ที่ยังไม่ได้รับการแก้ไข
- 2) ฟื้นฟูระบบโดยการกู้คืนข้อมูลจากระบบสำรองล่าสุด (Backup)
- 3) Restore Operating System หรือ Application Software ต่าง ๆ จาก Master Image ที่ปลอดภัย
- 4) Restore ข้อมูลกลับเข้าสู่ระบบจาก Back Up Storage
- 5) ทดสอบระบบทั้งหมดเพื่อยืนยันว่าระบบปลอดภัยและสามารถทำงานได้ปกติ
- 6) ตรวจสอบการทำงานของระบบสำรองเพื่อให้แน่ใจว่าข้อมูลที่กู้คืนครบถ้วน

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของโรงพยาบาลแม่ลาว ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตโรงพยาบาลแม่ลาว เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

	แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan Procedure)	รหัสเอกสาร	MLH-MOPH-IR Plan -01
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ ชั้นความลับของ เอกสาร	5 ม.ค 2569 ใช้ภายในเท่านั้น

ข้อ 6 การมีส่วนร่วม (Engagement Protocols) กับบุคคลภายนอก หรือแนวปฏิบัติการบริหารจัดการบุคคลภายนอก

การมีส่วนร่วมกับหน่วยงานภายนอกองค์กร (Information Sharing) ควรกำหนดขั้นตอนการสื่อสารและประเภทข้อมูล ที่สามารถนำไปแบ่งปันได้กับบุคคลภายนอก ทั้งหน่วยงานบังคับใช้กฎหมาย หน่วยงานกำกับดูแลองค์กรอื่น หรือการติดต่อเพื่อขอความช่วยเหลือจากผู้เชี่ยวชาญจากภายนอกองค์กรที่เกี่ยวข้องกับเหตุการณ์ความมั่นคงปลอดภัยทางไซเบอร์ อาทิ Thai CERT หรือ CERT ของ Sector อื่น ๆ เป็นต้น เพื่อแบ่งปันข้อมูลข่าวสารด้านภัยคุกคามทางไซเบอร์เพื่อช่วยให้การป้องกันและตอบสนองต่อภัยคุกคามได้เร็วยิ่งขึ้น โดยพิจารณาดำเนินการ ดังนี้

- 1) ติดต่อบุคคลภายนอกตามความจำเป็น
- 2) ประสานงานกับหน่วยงานบังคับใช้กฎหมาย หากมีความจำเป็นในการดำเนินคดี
- 3) ส่งมอบหลักฐานที่เกี่ยวข้องให้กับผู้เชี่ยวชาญภายนอก พร้อมรายการหลักฐานทั้งหมดเพื่อใช้ในการตรวจสอบ


ข้อ 7 กระบวนการทบทวนหลังการดำเนินการ (After-Action Review Process)

- 1) ประเมินผลการดำเนินการ เช่น ความเร็วในการตอบสนอง การกู้คืนระบบ และการจำกัดขอบเขตเหตุการณ์
- 2) ระบุข้อบกพร่องและข้อเสนอแนะสำหรับการปรับปรุงกระบวนการตอบสนอง
- 3) เสนอมาตรการปรับปรุงแผนรับมือภัยคุกคาม เพื่อให้มีประสิทธิภาพมากขึ้นในการป้องกันเหตุการณ์ในอนาคต

ข้อ 8 การสื่อสารและการทบทวนแผน (Communication and Plan Review)

- 1) สื่อสารแผนการรับมือภัยคุกคามทางไซเบอร์ให้กับบุคลากรที่เกี่ยวข้องทั้งหมดผ่านการอบรมและเอกสารที่เกี่ยวข้อง
- 2) จัดอบรมพนักงานอย่างสม่ำเสมอเกี่ยวกับการตอบสนองต่อเหตุการณ์ฉุกเฉิน
- 3) ทบทวนแผนการรับมือภัยคุกคามทุกปี หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญในสภาพแวดล้อมทางไซเบอร์

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือว่าเป็นสมบัติของโรงพยาบาลแม่ลาว ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตโรงพยาบาลแม่ลาว เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ

	<p style="text-align: center;">แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan Procedure)</p>	รหัสเอกสาร	MLH-MOPH-IR Plan -01
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ ชั้นความลับของ เอกสาร	5 ม.ค 2569 ใช้ภายในเท่านั้น

4) ปรับปรุงแผนตามผลการทบทวนและการฝึกซ้อมแผนรับมือภัยคุกคาม

การทบทวนแผนการรับมือภัยคุกคาม

แผนการรับมือภัยคุกคาม นี้จะได้รับการทบทวนเป็นประจำทุกปีหรือตามความจำเป็นเพื่อให้มั่นใจในประสิทธิภาพและและถ้ามีการเปลี่ยนแปลงนโยบายนี้จะต้องมีการสื่อสารไปยังทุกฝ่ายที่ได้รับผลกระทบหรือทุกฝ่ายที่เกี่ยวข้องทราบ

เอกสารอ้างอิง

1. โครงสร้างทีมรับมือภัยคุกคามทางไซเบอร์
2. รายงานสรุปเหตุการณ์
3. แผนการรับมือภัยคุกคามทางไซเบอร์

เอกสารนี้ ฉบับทางการจะอยู่ในรูปไฟล์อิเล็กทรอนิกส์ ซึ่งอยู่ในระบบเครือข่ายเท่านั้น หากปรากฏเอกสารนี้ส่วนหนึ่งส่วนใดหรือทั้งฉบับในรูปแบบสื่อเอกสาร เช่น กระดาษ ให้ตรวจสอบเอกสารกับฉบับทางการบนระบบเครือข่ายก่อนใช้เพื่ออ้างอิง เอกสารนี้ถือเป็นสมบัติของโรงพยาบาลแม่ลาว ห้ามแจกจ่ายไปยังบุคคลภายนอกโดยไม่ได้รับอนุญาตโรงพยาบาลแม่ลาว เอกสารกระดาษนี้ ถือว่าเป็นเอกสารไม่ควบคุม เว้นแต่มีการประทับตรา “สำเนาควบคุม” เท่านั้น ซึ่งผู้ครอบครองจะถูกระบุในบัญชีแจกจ่ายเอกสารที่เป็นสื่อกระดาษ