

ตัวชี้วัด 4.21 : ระดับความสำเร็จของมาตรการขับเคลื่อนการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

มาตรการขับเคลื่อนการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมอนามัย ขั้นตอนที่ 5 : สรุปผลการดำเนินงานตามมาตรการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

สรุปผลการดำเนินงานตามมาตรการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ดังนี้

1. ทบทวนการจัดทำแผนบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ กรมอนามัย โดยจัดทำแผนบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity Incident Response) กรมอนามัย ใช้เป็นแนวทางในการเตรียมความพร้อม เพื่อรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์ โดยจะระบุขั้นตอนที่จำเป็น ผลลัพธ์ที่ได้จากแผนการตอบสนองต่อภัยคุกคามทางไซเบอร์ และข้อควรระวังในแต่ละ ขั้นตอน โดยมีรายละเอียด ดังนี้

- 1.1 ปรับปรุงเนื้อหาในส่วน (Playbook)
- 1.2 ปรับปรุงระดับความรุนแรง (Severity Level)
- 1.3 ทบทวนช่องทางการสื่อสารของการรับมือภัยคุกคาม (Communication Protocols)
- 1.4 ปรับปรุงระดับความรุนแรงที่เหมาะสมในการติดต่อกับหน่วยงาน (Outside Parties list)

2. ทบทวนการจัดทำระบบเฝ้าระวังและแจ้งภัยคุกคามทางไซเบอร์ โดยดำเนินการจัดทำระบบตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ เพื่อตอบสนองและยังยึดต่อภัยคุกคามทางไซเบอร์ โดยมีการจัดเตรียมระบบ/อุปกรณ์ บุคลากร และช่องทางการสื่อสารแจ้งภัยคุกคามทางไซเบอร์ของกรมอนามัย สำหรับป้องกัน ตรวจจับ และเฝ้าระวังการบุกรุกระบบคอมพิวเตอร์และเครือข่าย รวมทั้งหน่วยงานภาครัฐที่กำหนดนโยบาย มาตรการ แนวทางการรักษาความมั่นคงปลอดภัยไซเบอร์ เช่น สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เป็นหน่วยงานทำหน้าที่ประสานการปฏิบัติงานร่วมกันทั้งภาครัฐและเอกชน ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562, กระทรวงสาธารณสุข โดยศูนย์ประสานการรักษาความมั่นคงปลอดภัยไซเบอร์ด้านสาธารณสุข (Health CERT) เป็นหน่วยงานทำหน้าที่ประสานงาน เฝ้าระวัง รับมือและแก้ไขภัยคุกคามทางไซเบอร์ด้านสาธารณสุข และคณะประสานงานการรักษาความมั่นคงปลอดภัยไซเบอร์ (Anamai CIRT) ของกรมอนามัย เป็นต้น โดยมีรายละเอียด ดังนี้

- 2.1 จัดเตรียมระบบ/อุปกรณ์สำหรับป้องกัน ตรวจจับ และเฝ้าระวังการบุกรุกระบบคอมพิวเตอร์และเครือข่ายจากภัยคุกคามทางไซเบอร์ เช่น อุปกรณ์ป้องกันความปลอดภัยด้านเครือข่าย, ซอฟต์แวร์เฝ้าระวังภัยคุกคามทางไซเบอร์ และเทคนิคเข้ารหัสการรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ เป็นต้น
- 2.2 จัดเตรียมบุคลากร เพื่อทำหน้าที่ประสานงาน เฝ้าระวัง รับมือและแก้ไขภัยคุกคามทางไซเบอร์ โดยมีหน้าที่รับผิดชอบในการแจ้งข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ ให้กับผู้ที่เกี่ยวข้องทั้งภายใน และภายนอกองค์กร เพื่อให้ทุกคนสามารถดำเนินการตามหน้าที่รับผิดชอบของตนเองตามกำหนดไว้

2.3 กำหนดช่องทางการสื่อสารแจ้งภัยคุกคามทางไซเบอร์ของกรมอนามัย เพื่อเป็นช่องทางการรายงานเหตุการณ์ ให้ผู้ได้รับผลกระทบหรือพบเห็นเหตุการณ์ เช่น จดหมายอิเล็กทรอนิกส์, กลุ่มไลน์, เบอร์ติดต่อ และเว็บไซต์เผยแพร่ข่าวสาร เป็นต้น

3. ทบทวนการจัดตั้งคณะประสานงานการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของกรมอนามัย (Anamai CIRT)

โดยดำเนินการจัดตั้งคณะประสานงานการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของกรมอนามัย (Anamai CIRT : Cyber Incident Response Team) ประจำปีงบประมาณ พ.ศ. 2567 ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง การกำหนดหลักเกณฑ์ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและการมอบหมายการควบคุมและกำกับดูแล พ.ศ. 2564 หมวด 7 ด้านสาธารณสุข กำหนดให้หน่วยงานที่มีภารกิจให้บริการสุขภาพในโรงพยาบาล บริการสุขภาพระหว่างโรงพยาบาล บริการด้านเวชภัณฑ์และเครื่องมือแพทย์ บริการตรวจวิเคราะห์ทางการแพทย์และรังสีวิทยา และบริการข้อมูลสุขภาพดิจิทัล ต้องดำเนินการรักษาความมั่นคงปลอดภัยทางไซเบอร์ โดยอยู่ภายใต้การกำกับดูแลของสำนักงานปลัดกระทรวงสาธารณสุข

4. สร้างความตระหนักด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ให้กับเจ้าหน้าที่ของกรมอนามัย
การจัดประชุมส่งเสริมและสนับสนุนทักษะความเข้าใจและใช้เทคโนโลยีดิจิทัลของกรมอนามัย (Digital Literacy) เรื่อง การสร้างความตระหนักด้านความมั่นคงทางไซเบอร์ (Cybersecurity Awareness) เพื่อให้เจ้าหน้าที่กรมอนามัยตระหนักถึงภัยคุกคามทางไซเบอร์ และเสริมสร้างความรู้ความเข้าใจเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ ตามพระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มีรายละเอียด ดังนี้

- 4.1 สร้างความเข้าใจเกี่ยวกับอันตรายจากการโจมตีทางไซเบอร์
- 4.2 การเข้าใจเกี่ยวกับมาตรการป้องกันการโจมตีทางไซเบอร์
- 4.3 สร้างทักษะในการระมัดระวังต่อการละเมิดความปลอดภัย
- 4.4 ส่งเสริมพฤติกรรมที่ปลอดภัยที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์
- 4.5 สนับสนุนและการกำกับดูแลผู้ใช้งานในการปฏิบัติตามนโยบายและมาตรการ
- 4.6 เผยแพร่ความรู้และข้อมูลเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์