ตัวชี้วัด ๔.๒๐ : ระดับความสำเร็จของการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมอนามัย (รอบ ๕ เดือนแรก)

ระดับที่ ๕ Outcome ผลลัพธ์ของตัวชี้วัด

๕.๑ ร้อยละความสำเร็จในการกู้คืนระบบงานกองแผนงานให้พร้อมใช้งานภายใน ๒๔ ชั่วโมง หลังจากตรวจพบการถูกละเมิดความปลอดภัยทางไซเบอร์ (Security Breaches) จากจำนวนระบบทั้งหมด ๑๒ ระบบ

๕.๑.๑ แนวทางการประเมิน

๑) เกณฑ์คะแนน

คะแนน	เป้าหมาย (ร้อยละ)
๐.๒	<=๘๐
๐.๔	๘๐-๘๔.๙๙
๐.๖	๘๕-๘๙.๙๙
๐.๘	๙๐-๙๔.๙๙
๑.๐	>=๙๕ ขึ้นไป

๒) สูตรคำนวณการดำเนินงานตามตัวชี้วัด

$$\text{ร้อยละความสำเร็จในการกู้คืนระบบงานกองแผนงาน} = \frac{(\text{จำนวนครั้งที่กู้คืนระบบสำเร็จภายใน } 24 \text{ ชม.})}{(\text{จำนวนครั้งที่ถูกละเมิดความปลอดภัยทางไซเบอร์})} \times ๑๐๐$$

Outcome ผลลัพธ์ในรอบ ๕ เดือนแรก (ตุลาคม ๒๕๖๘ – กุมภาพันธ์ ๒๕๖๙) ตามตัวชี้วัดที่ ๔.๒๐ ระดับความสำเร็จของการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมอนามัย กองแผนงานตรวจพบเหตุการณ์การถูกละเมิดความปลอดภัยทางไซเบอร์จำนวน ๖ ครั้ง โดยทุกกรณีไม่ส่งผลกระทบต่อระบบงานหลัก ไม่พบการรั่วไหลของข้อมูล และสามารถควบคุมสถานการณ์ได้ภายใน ๒๔ ชั่วโมง ทั้งนี้ **ไม่ปรากฏระบบงานใดที่ต้องดำเนินการกู้คืนให้กลับมาใช้งานภายในระยะเวลาดังกล่าว**

จากผลการดำเนินงานข้างต้น สะท้อนให้เห็นถึงประสิทธิภาพของมาตรการเฝ้าระวัง ป้องกัน และตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน ตามเกณฑ์การประเมินที่กำหนดไว้ เนื่องจากไม่มีกรณีที่ต้องดำเนินการกู้คืนระบบภายใน ๒๔ ชั่วโมง จึงได้รับผลการประเมิน **๑ คะแนน** ทั้งนี้ภาพรวมแสดงถึงความพร้อมและความสามารถในการบริหารจัดการเหตุการณ์ไซเบอร์ได้อย่างมีประสิทธิภาพ และไม่เกิดความเสียหายต่อภารกิจของหน่วยงาน

สรุปผลการดำเนินงานตามมาตรการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

สรุปผลการดำเนินงานตามมาตรการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ดังนี้

๑. การจัดทำแผนบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ กรมอนามัย โดยจัดทำแผนบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity Incident Response) กรมอนามัย ใช้เป็นแนวทางในการเตรียมความพร้อม เพื่อรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์ โดยจะระบุขั้นตอนที่จำเป็น ผลลัพธ์ที่ได้จากแผนการตอบสนองต่อภัยคุกคามทางไซเบอร์ และข้อควรระวังในแต่ละขั้นตอน มีรายละเอียด ดังนี้

๑.๑ การเตรียมความพร้อม (Preparation)

๑.๒ การตรวจจับและวิเคราะห์ (Detection & Analysis)

๑.๓ การควบคุมความเสียหาย การกำจัดสาเหตุของภัยคุกคาม และการกู้คืน (Containment, Eradication & Recovery)

๑.๔ การดำเนินการภายหลังการรับมือและตอบสนองเสร็จสิ้น (Post Incident Activity)

๒. จัดทำระบบเฝ้าระวังและแจ้งภัยคุกคามภัยทางไซเบอร์ โดยดำเนินการจัดทำระบบตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ เพื่อตอบสนองและยังยั้งต่อภัยคุกคามทางไซเบอร์ โดยมีการจัดเตรียมระบบ/อุปกรณ์ บุคลากร และช่องทางการสื่อสารแจ้งภัยคุกคามทางไซเบอร์ของกรมอนามัย สำหรับป้องกัน ตรวจจับ และเฝ้าระวังการบุกรุกระบบคอมพิวเตอร์และเครือข่าย รวมทั้งหน่วยงานภาครัฐที่กำหนดนโยบาย มาตรการ แนวทางการรักษาความมั่นคงปลอดภัยไซเบอร์ เช่น สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เป็นหน่วยงานทำหน้าที่ประสานการปฏิบัติงานร่วมกันทั้งภาครัฐและเอกชน ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒, กระทรวงสาธารณสุข โดยศูนย์ประสานการรักษาความมั่นคงปลอดภัยไซเบอร์ด้านสาธารณสุข (Health CERT) เป็นหน่วยงานทำหน้าที่ประสานงาน เฝ้าระวัง รับมือและแก้ไขภัยคุกคามทางไซเบอร์ด้านสาธารณสุข และคณะประสานงานการรักษาความมั่นคงปลอดภัยไซเบอร์ (Anamai CIRT) ของกรมอนามัย เป็นต้น โดยมีรายละเอียด ดังนี้

๒.๑ จัดเตรียมระบบ/อุปกรณ์สำหรับป้องกัน ตรวจจับ และเฝ้าระวังการบุกรุกระบบคอมพิวเตอร์และเครือข่ายจากภัยคุกคามทางไซเบอร์ เช่น อุปกรณ์ป้องกันความปลอดภัยด้านเครือข่าย, ซอฟต์แวร์เฝ้าระวังภัยคุกคามทางไซเบอร์ และเทคนิคเข้ารหัสการรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ เป็นต้น

๒.๒ จัดเตรียมบุคลากร เพื่อทำหน้าที่ประสานงาน เฝ้าระวัง รับมือและแก้ไขภัยคุกคามทางไซเบอร์ โดยมีหน้าที่รับผิดชอบในการแจ้งข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ ให้กับผู้ที่เกี่ยวข้องทั้งภายใน และภายนอกองค์กร เพื่อให้ทุกคนสามารถดำเนินการตามหน้าที่รับผิดชอบของตนเองตามกำหนดไว้

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

๓. ทบทวนจัดตั้งคณะประสานงานการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของกรมอนามัย (Anamai CIRT) โดยดำเนินการจัดตั้งคณะประสานงานการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของกรมอนามัย (Anamai CIRT : Cyber Incident Response Team) ประจำปีงบประมาณ พ.ศ. ๒๕๖๙ ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง การกำหนดหลักเกณฑ์ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและการมอบหมายการควบคุมและกำกับดูแล พ.ศ. ๒๕๖๔ หมวด ๗ ด้านสาธารณสุข กำหนดให้หน่วยงานที่มีการให้บริการสุขภาพในโรงพยาบาล บริการสุขภาพระหว่างโรงพยาบาล บริการด้านเวชภัณฑ์และเครื่องมือแพทย์ บริการตรวจวิเคราะห์ทางการแพทย์และรังสีวิทยา และบริการข้อมูลสุขภาพดิจิทัล ต้องดำเนินการรักษาความมั่นคงปลอดภัยทางไซเบอร์ โดยอยู่ภายใต้การกำกับดูแลของสำนักงานปลัดกระทรวงสาธารณสุข

๔. สร้างความตระหนักด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ให้กับเจ้าหน้าที่ของกรมอนามัย เพื่อให้เจ้าหน้าที่กรมอนามัยตระหนักถึงภัยคุกคามทางไซเบอร์ และเสริมสร้างความรู้ความเข้าใจเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ ดังนี้

๔.๑ สร้างความเข้าใจเกี่ยวกับอันตรายจากการโจมตีทางไซเบอร์

๔.๒ การเข้าใจเกี่ยวกับมาตรการป้องกันการโจมตีทางไซเบอร์ และทักษะในการระมัดระวังต่อการละเมิดความปลอดภัย

๔.๓ ส่งเสริมพฤติกรรมที่ปลอดภัยที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์

๔.๔ สนับสนุนและการกำกับดูแลผู้ใช้งานในการปฏิบัติตามนโยบายและมาตรการ

๔.๕ เผยแพร่ความรู้และข้อมูลเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์

กองแผนงาน จัดประชุมเชิงปฏิบัติการ ขับเคลื่อนการดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศ ประจำปีงบประมาณ พ.ศ. ๒๕๖๙ มีวัตถุประสงค์เพื่อเสริมสร้างศักยภาพและความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ของกรมอนามัยให้สอดคล้องกับสถานการณ์ภัยคุกคามที่เปลี่ยนแปลงอย่างรวดเร็ว โดยได้รับเกียรติจากผู้เชี่ยวชาญด้าน Cybersecurity จากสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) และภาคเอกชน ร่วมบรรยายและถ่ายทอดองค์ความรู้