ตัวชี้วัด 4.19 : ระดับความสำเร็จของการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมอนามัย

ระดับ 1 : Assessment

ศึกษาและการวิเคราะห์สถานการณ์ของการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมอนามัย

1.1 ผลการวิเคราะห์สถานการณ์ของตัวชี้วัด (0.5)

ด้วยกรมอนามัยมีภารกิจหลักในการส่งเสริมให้ประชาชนมีสุขภาพดี มีการศึกษาวิเคราะห์ วิจัย พัฒนาและถ่ายทอดองค์ความรู้และเทคโนโลยีด้านการสร้างเสริมสุขภาพและและอนามัยสิ่งแวดล้อม เพื่อให้สามารถป้องกันหรือรับมือกับภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงที ภารกิจหรือบริการด้านสาธารณสุขซึ่งเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ จะต้องมีการป้องกัน มีมาตรการรับมือและบริหารจัดการความเสี่ยงจากภัยคุกคามทางไซเบอร์ มิให้เกิดผลกระทบต่อความมั่นคงปลอดภัยทางด้านสาธารณสุขของประเทศ ซึ่งกรมอนามัย ได้ดำเนินการตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ให้มีการรักษาความมั่นคงปลอดภัยทางไซเบอร์อย่างมีประสิทธิภาพ โดยมีการสรุปผลการวิเคราะห์สถานการณ์ของตัวชี้วัด และความรู้ที่นำมาใช้ประกอบการวิเคราะห์ ดังนี้

1) ผลผลิต/ ผลลัพธ์ระดับ C (Comparisons) การเปรียบเทียบ

การวิเคราะห์เปรียบเทียบรูปแบบมาตรการขับเคลื่อนการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับป้องกันหรือรับมือภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงที แสดงให้เห็นว่าการเตรียมความพร้อมบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ คือ ปัจจัยสู่ความสำเร็จในการยกระดับความมั่นคงปลอดภัยทางไซเบอร์ได้อย่างมีประสิทธิภาพและเห็นผลอย่างเป็นรูปธรรม สามารถสรุปการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ของแต่ละหน่วยงาน ดังนี้

• **หน่วยงานที่ 1 : สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)** เป็นหน่วยงานรับผิดชอบงานตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และประสานการปฏิบัติงานร่วมกันทั้งภาครัฐและเอกชน ทั้งในสถานการณ์ ทั่วไปหรือสถานการณ์ที่เป็นภัยต่อความมั่นคงอย่างร้ายแรง อันจะทำให้การป้องกันและการรับมือกับภัยคุกคามทางไซเบอร์เป็นไปอย่างมีประสิทธิภาพ

• **หน่วยงานที่ 2 : กระทรวงสาธารณสุข** เป็นหน่วยงานควบคุมหรือกำกับดูแล (Regulator) รับแจ้งเหตุภัยคุกคามทางไซเบอร์ และร่วมกับ Sectoral CERT รวบรวมข้อมูล ตรวจสอบ ช่วยเหลือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ดังนั้นเพื่อเป็นการขับเคลื่อนการดำเนินงานการรักษาความมั่นคงปลอดภัยไซเบอร์ด้านสาธารณสุข มีการจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยไซเบอร์ด้านสาธารณสุข (Health CIRT) เพื่อทำหน้าหน้าที่ประสานงาน เฝ้าระวัง รับมือ และแก้ไขภัยคุกคามทางไซเบอร์ด้านสาธารณสุข

2) ผลผลิต/ ผลลัพธ์ ระดับ T (Trends) แนวโน้ม

การมีมาตรการขับเคลื่อนการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ช่วยให้องค์กรสามารถวางแนวทางการยืนยันตัวตน ปกป้อง ตรวจสอบ และตอบสนองต่อภัยคุกคาม และฟื้นฟูระบบหลังจากได้รับผลกระทบไว้ได้อย่างดี พร้อมทั้งกำหนดบทบาทหน้าที่ให้สามารถนำมาใช้ได้ทันที

3) ผลผลิต/ ผลลัพธ์ระดับ Le (Level) ของผลการดำเนินการในปัจจุบัน

การทำงานด้านความมั่นคงปลอดภัยไซเบอร์ ซึ่งแต่ละขั้นตอนจะช่วยให้องค์กรสามารถวางแผนป้องกัน ตรวจจับ และตอบสนองต่อภัยคุกคามได้อย่างรวดเร็วและเป็นระบบ โดยแบ่งออกเป็น 5 ขั้นตอนสำคัญ ดังนี้

- การบริหารจัดการความเสี่ยง (Identity)
- การวางมาตรฐานควบคุมเพื่อปกป้องระบบองค์กร (Protect)
- การกำหนดขั้นตอนและกระบวนการต่าง ๆ เพื่อตรวจจับสถานการณ์ที่ผิดปกติ (Detect)
- การกำหนดขั้นตอนและกระบวนการต่าง ๆ เพื่อรับมือกับสถานการณ์ผิดปกติที่เกิดขึ้น (Response)
- การกำหนดขั้นตอนและกระบวนการต่าง ๆ เพื่อให้องค์กรสามารถดำเนินได้อย่างต่อเนื่องและฟื้นฟูระบบให้กลับคืนมาเหมือนเดิม (Recovery)

<u>ผลการดำเนินการในปัจจุบันมีการดำเนินงานในปีงบประมาณ พ.ศ. 2567</u> ดังนี้

1. ดำเนินการแผนบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ กรมอนามัย โดยจัดทำแผนบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity Incident Response) กรมอนามัย ใช้เป็นแนวทางในการเตรียมความพร้อม เพื่อรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์

2. ดำเนินการจัดทำระบบเฝ้าระวังและแจ้งภัยคุกคามภัยทางไซเบอร์ โดยดำเนินการจัดทำระบบตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ เพื่อตอบสนองและยังยั้งต่อภัยคุกคามทางไซเบอร์ โดยมีการจัดเตรียมระบบ/อุปกรณ์ บุคลากร และช่องทางการสื่อสารแจ้งภัยคุกคามทางไซเบอร์ของกรมอนามัย สำหรับป้องกัน ตรวจจับ และเฝ้าระวังการบุกรุกระบบคอมพิวเตอร์และเครือข่าย รวมทั้งหน่วยงานภาครัฐที่กำหนดนโยบาย มาตรการ แนวทางการรักษาความมั่นคงปลอดภัยไซเบอร์

3. ดำเนินการจัดตั้งคณะประสานงานการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของกรมอนามัย (Anamai CIRT : Cyber Incident Response Team) ประจำปีงบประมาณ พ.ศ. 2567 ตามประกาศคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง การกำหนดหลักเกณฑ์ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและการมอบหมายการควบคุมและกำกับดูแล พ.ศ. 2564 หมวด 7

4. จัดประชุมส่งเสริมและสนับสนุนทักษะความเข้าใจและใช้เทคโนโลยีดิจิทัลของกรมอนามัย (Digital Literacy) เรื่อง การสร้างความตระหนักด้านความมั่นคงทางไซเบอร์ (Cybersecurity Awareness) เพื่อให้เจ้าหน้าที่กรมอนามัยตระหนักถึงภัยคุกคามทางไซเบอร์ และเสริมสร้างความรู้ความเข้าใจเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562

1.2 ผลการวิเคราะห์ผู้รับบริการและผู้มีส่วนได้ส่วนเสียเพื่อขับเคลื่อนตัวชี้วัด (0.5)

ผลการวิเคราะห์ผู้รับบริการและผู้มีส่วนได้ส่วนเสียเพื่อขับเคลื่อน ได้แก่ กลุ่มผู้รับบริการ และผู้มีส่วนได้ส่วนเสีย โดยมีการสรุปผล ดังนี้

- กลุ่มผู้รับบริการและผู้มีส่วนได้ส่วนเสีย
- ความต้องการ/ความคาดหวัง
- ความผูกพัน
- ความพึงพอใจ/ความไม่พึงพอใจ
- ข้อเสนอแนะจากผู้รับบริการ

1.2.1 กลุ่มผู้รับบริการ

รายการข้อมูล	รายละเอียด
กลุ่มผู้รับริการ	1. เจ้าหน้าที่สังกัดกรมอนามัย 2. ประชาชน
ความต้องการ	ระบบงานที่มีความมั่นคงปลอดภัย สามารถป้องกันการเข้าถึงข้อมูลได้
ความคาดหวัง	การรักษาความมั่นคงปลอดภัยไซเบอร์ ต้องมีระดับที่สูงขึ้นและการตอบสนองที่รวดเร็วต่อการละเมิดภัยคุกคามทางไซเบอร์
ความผูกพัน	การปฏิบัติตามกฎหมายที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์
ความพึงพอใจ	ระบบการแจ้งเตือนทางไซเบอร์ที่ทำให้ผู้รับบริการมีความตระหนักถึงความเสี่ยงทางด้านความมั่นคงปลอดภัยทางไซเบอร์
ความไม่พึงพอใจ	1. การไม่เข้าใจในกระบวนการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ 2. การใช้ภาษาด้านเทคนิคเข้าใจยาก
ข้อเสนอแนะจากผู้รับบริการ	1. ความปลอดภัยของข้อมูลส่วนตัวที่ภาครัฐเก็บไว้ต้องมีการรักษาความมั่นคงปลอดภัยไซเบอร์ 2. เผยแพร่ความรู้และข้อมูลเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์

1.2.2 กลุ่มผู้มีส่วนได้ส่วนเสีย

รายการข้อมูล	รายละเอียด
กลุ่มผู้มีส่วนได้ส่วนเสียปัจจุบัน	1. ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง กรมอนามัย (CIO) 2. เจ้าหน้าที่ประสานงานการรักษาความมั่นคงปลอดภัยทางไซเบอร์ กรมอนามัย (Anamai-CIRT) 3. ศูนย์ประสานการรักษาความมั่นคงปลอดภัยทางไซเบอร์ด้านสาธารณสุข (Health-CIRT) 4. สำนักคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)
ความต้องการ	การดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่สอดคล้องตามกฎหมาย มาตรฐาน และนโยบายที่เกี่ยวข้อง
ความคาดหวัง	การป้องกันการเข้าถึงข้อมูลที่เป็นความลับ สามารถเข้าได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น
ความผูกพัน	การกำหนดนโยบายและมาตรการที่เข้มงวด เพื่อสนับสนุนความมั่นคงปลอดภัยทางไซเบอร์
ความพึงพอใจ	ระบบการแจ้งเตือนทางไซเบอร์ที่ทำให้ผู้มีส่วนได้ส่วนเสียรับทราบและตระหนักถึงความเสี่ยงอย่างรวดเร็ว
ความไม่พึงพอใจ	การปรับปรุงระบบงานอาจต้องใช้งบประมาณจำนวนมากในการแก้ไขและปิดช่องโหว่ต่าง ๆ
ข้อเสนอแนะจากผู้มีส่วนได้ส่วนเสีย	1. การพัฒนาระบบงานให้เน้นที่ความมั่นคงปลอดภัยและประสิทธิภาพ 2. การพัฒนาทักษะบุคลากรและผู้ที่มีส่วนเกี่ยวข้องให้มีความตระหนักและการระมัดระวังต่อการละเมิดความปลอดภัยทางไซเบอร์ 3. ส่งเสริมและสนับสนุนให้ผู้ปฏิบัติงานมีเข้าใจเกี่ยวกับมาตรการป้องกันการโจมตีทางไซเบอร์