**ตัวชี้วัด 4.21 : ระดับความสำเร็จของมาตรการขับเคลื่อนการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (รอบ 5 เดือนหลัง)**

Assessment

**1. มีการทบทวนบทวิเคราะห์สถานการณ์ของตัวชี้วัด**

**1.1 ผลการวิเคราะห์สถานการณ์ของตัวชี้วัด (0.5)**

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

- ผลผลิต/ ผลลัพธ์ระดับ C (Comparisons) การเปรียบเทียบ
- ผลผลิต/ ผลลัพธ์ ระดับ T (Trends) แนวโน้ม
- ผลผลิต/ ผลลัพธ์ระดับ Le (Level) ของผลการดำเนินการในปัจจุบัน

**ตาราง** แสดงข้อมูลรายละเอียดผลผลิต/ผลลัพธ์ ได้แก่ ระดับ C (Comparisons) การเปรียบเทียบ, T (Trends) แนวโน้ม และ Le (Level) ของผลการดำเนินการในปัจจุบัน

| ผลผลิต/ผลลัพธ์ระดับ | รายละเอียด |
|---|---|
| **ผลผลิต/ ผลลัพธ์ระดับ C (Comparisons) การเปรียบเทียบ** | - การวิเคราะห์เปรียบเทียบรูปแบบมาตรการขับเคลื่อนการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับป้องกันหรือรับมือภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงที แสดงให้เห็นว่าการเตรียมความพร้อมบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ คือปัจจัยสู่ความสำเร็จในการยกระดับความมั่นคงปลอดภัยทางไซเบอร์ได้อย่างมีประสิทธิภาพและเห็นผลอย่างเป็นรูปธรรม สามารถสรุปการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ของแต่ละหน่วยงาน ดังนี้<br>● **หน่วยงานที่ 1 : สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)** เป็นหน่วยงานรับผิดชอบงานตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และประสานการปฏิบัติงานร่วมกันทั้งภาครัฐและเอกชน ไม่ว่าในสถานการณ์ทั่วไปหรือสถานการณ์ที่เป็นภัยต่อความมั่นคงอย่างร้ายแรง อันจะทำให้การป้องกันและการรับมือกับภัยคุกคามทางไซเบอร์เป็นไปอย่างมีประสิทธิภาพ |

| ผลผลิต/ผลลัพธ์ระดับ | รายละเอียด |
|---|---|
| | ● **หน่วยงานที่ 2 : กระทรวงสาธารณสุข** เป็นหน่วยงานควบคุมหรือกำกับดูแล (Regulator) รับแจ้งเหตุภัยคุกคามทางไซเบอร์ และร่วมกับ Sectoral CERT รวบรวมข้อมูล ตรวจสอบ ช่วยเหลือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ดังนั้นเพื่อเป็นการขับเคลื่อนการดำเนินงานการรักษาความมั่นคงปลอดภัยไซเบอร์ด้านสาธารณสุข มีการจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยไซเบอร์ด้านสาธารณสุข (Health CIRT) เพื่อทำหน้าหน้าที่ประสานงาน เฝ้าระวัง รับมือ และแก้ไขภัยคุกคามทางไซเบอร์ด้านสาธารณสุข |
| **ผลผลิต/ ผลลัพธ์ ระดับ T (Trends) แนวโน้ม** | - การมีมาตรการขับเคลื่อนการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ช่วยให้องค์กรสามารถวางแนวทางการยืนยันตัวตน ปกป้อง ตรวจสอบ และตอบสนองต่อภัยคุกคาม และฟื้นฟูระบบหลังจากได้รับผลกระทบไว้ได้อย่างดี พร้อมทั้งกำหนดบทบาทหน้าที่ให้สามารถนำมาใช้ได้ทันที |
| **ผลผลิต/ ผลลัพธ์ระดับ Le (Level) ของผลการดำเนินการในปัจจุบัน** | - การทำงานด้านความมั่นคงปลอดภัยไซเบอร์ ซึ่งแต่ละขั้นตอนจะช่วยให้องค์กรสามารถวางแผนป้องกัน ตรวจจับ และตอบสนองต่อภัยคุกคามได้อย่างรวดเร็วและเป็นระบบ โดยแบ่งออกเป็น 5 ขั้นตอนสำคัญ ดังนี้<br>● การบริหารจัดการความเสี่ยง (Identity)<br>● การวางมาตรฐานควบคุมเพื่อปกป้องระบบองค์กร (Protect)<br>● การกำหนดขั้นตอนและกระบวนการต่าง ๆ เพื่อตรวจจับสถานการณ์ที่ผิดปกติ (Detect)<br>● การกำหนดขั้นตอนและกระบวนการต่าง ๆ เพื่อรับมือกับสถานการณ์ผิดปกติที่เกิดขึ้น (Respone)<br>● การกำหนดขั้นตอนและกระบวนการต่าง ๆ เพื่อให้องค์กรสามารถดำเนินได้อย่างต่อเนื่อง และฟื้นฟูระบบให้กลับคืนมาเหมือนเดิม (Recovery)<br>- ผลการดำเนินการในปัจจุบันมีการดำเนินงาน ดังนี้<br>● การให้ความรู้และทำความเข้าใจกับบุคลากร โดยมีการประชุมแนวทางดำเนินงานด้านความปลอดภัยไซเบอร์ตามมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ และการสแกนช่องโหว่บนเครือข่าย และตรวจสอบเฝ้าระวังสถานะเครื่องแม่ข่าย |

| ผลผลิต/ผลลัพธ์ระดับ | รายละเอียด |
| --- | --- |
| | - สรุปผลผลการดำเนินการในปัจจุบันมีการดำเนินงาน ดังนี้<br>1. จัดทำแผนบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ กรมอนามัย โดยจัดทำแผนบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity Incident Response) กรมอนามัย ใช้เป็นแนวทางในการเตรียมความพร้อม เพื่อรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์ โดยจะระบุขั้นตอนที่จำเป็น ผลลัพธ์ที่ได้จากแผนการตอบสนองต่อภัยคุกคามทางไซเบอร์<br>2. จัดทำระบบเฝ้าระวังและแจ้งภัยคุกคามภัยทางไซเบอร์ โดยดำเนินการจัดทำระบบตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ เพื่อตอบสนองและยังยั้งต่อภัยคุกคามทางไซเบอร์ 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<br>3. จัดตั้งคณะประสานงานการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของกรมอนามัย (Anamai CIRT) โดยดำเนินการจัดตั้งคณะประสานงานการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของกรมอนามัย (Anamai CIRT : Cyber Incident Response Team) ประจำปีงบประมาณ พ.ศ. 2567 ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง การกำหนดหลักเกณฑ์ลักษณะหน่วยงานที่มีภารกิจ หรือให้บริการเป็น |

| ผลผลิต/ผลลัพธ์ระดับ | รายละเอียด |
| --- | --- |
| | หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและการมอบหมายการควบคุมและกำกับดูแล พ.ศ. 2564 หมวด 7 ด้านสาธารณสุข กำหนดให้หน่วยงานที่มีการให้บริการสุขภาพในโรงพยาบาล บริการสุขภาพระหว่างโรงพยาบาล บริการด้านเวชภัณฑ์และเครื่องมือแพทย์ บริการตรวจวิเคราะห์ทางการแพทย์และรังสีวิทยา และบริการข้อมูลสุขภาพดิจิทัล ต้องดำเนินการรักษาความมั่นคงปลอดภัยทางไซเบอร์ โดยอยู่ภายใต้การกำกับดูแลของสำนักงานปลัดกระทรวงสาธารณสุข<br>4. สร้างความตระหนักด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ให้กับเจ้าหน้าที่ของกรมอนามัย การจัดประชุมส่งเสริมและสนับสนุนทักษะความเข้าใจและใช้เทคโนโลยีดิจิทัลของกรมอนามัย (Digital Literacy) เรื่องการสร้างความตระหนักด้านความมั่นคงทางไซเบอร์ (Cybersecurity Awareness) เพื่อให้เจ้าหน้าที่กรมอนามัยตระหนักถึงภัยคุกคามทางไซเบอร์ และเสริมสร้างความรู้ความเข้าใจเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562<br>5. ผลลัพธ์ของตัวชี้วัดร้อยละการรายงานภัยคุกคามทางไซเบอร์ (Outcome) มีผลลัพธ์ตรงเป้าหมายเป็นสัดส่วนตามระยะเวลา ระหว่างเดือนตุลาคม 2566 – กุมภาพันธ์ 2567 ดังนี้<br>5.1 ร้อยละการสรุปรายงานผลภัยคุกคามทางไซเบอร์เสนอต่อผู้บริหาร (ร้อยละ 100) คือ สามารถดำเนินการได้ ร้อยละ 100 ซึ่งดำเนินการได้ครบทุกรายงานผลภัยคุกคามทางไซเบอร์เสนอต่อผู้บริหาร<br>5.2 ร้อยละของการช่วยเหลือให้หน่วยงานในสังกัดกรมอนามัย ตามมาตรการขับเคลื่อนการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมอนามัย (ร้อยละ 80) คือ เท่ากับเกณฑ์เป้าหมาย (ร้อยละ) คือ > 80 ขึ้นไป โดยสามารถดำเนินการได้ ร้อยละ 100 ซึ่งดำเนินการได้ครบทุกหน่วยงานในสังกัดกรมอนามัยที่เกิดภัยคุกคามทางไซเบอร์ |