ตัวชี้วัด 4.19 : ระดับความสำเร็จของการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมอนามัย (รอบ 5 เดือนหลัง) ของกองแผนงาน

ระดับที่ 1 Assessment: ศึกษาและวิเคราะห์ข้อมูลการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมอนามัย

1. มีการทบทวนบทวิเคราะห์สถานการณ์ของตัวชี้วัด

1.1 ผลการวิเคราะห์สถานการณ์ของตัวชี้วัด (0.5)

ด้วยกรมอนามัยมีภารกิจหลักในการส่งเสริมให้ประชาชนมีสุขภาพดี มีการศึกษาวิเคราะห์ วิจัย พัฒนาและถ่ายทอดองค์ความรู้และเทคโนโลยีด้านการสร้างเสริมสุขภาพและและอนามัยสิ่งแวดล้อม 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	- การวิเคราะห์เปรียบเทียบรูปแบบมาตรการขับเคลื่อนการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับป้องกันหรือรับมือภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงที แสดงให้เห็นว่าการเตรียมความพร้อมบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ คือ ปัจจัยสู่ความสำเร็จในการยกระดับความมั่นคงปลอดภัยทางไซเบอร์ได้อย่างมีประสิทธิภาพและเห็นผลอย่างเป็นรูปธรรม สามารถสรุปการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ของแต่ละหน่วยงาน ดังนี้ • **หน่วยงานที่ 1 : สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)** เป็นหน่วยงานรับผิดชอบงานตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และประสานการปฏิบัติงาน

ผลผลิต/ผลลัพธ์ระดับ	รายละเอียด
	ร่วมกันทั้งภาครัฐและเอกชน ไม่ว่าในสถานการณ์ทั่วไปหรือสถานการณ์ที่เป็นภัยต่อความมั่นคงอย่างร้ายแรง อันจะทำให้การป้องกันและการรับมือกับภัยคุกคามทางไซเบอร์เป็นไปอย่างมีประสิทธิภาพ • **หน่วยงานที่ 2 : กระทรวงสาธารณสุข** เป็นหน่วยงานควบคุมหรือกำกับดูแล (Regulator) รับแจ้งเหตุภัยคุกคามทางไซเบอร์ และร่วมกับ Sectoral CERT รวบรวมข้อมูลตรวจสอบ ช่วยเหลือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ดังนั้นเพื่อเป็นการขับเคลื่อนการดำเนินงานการรักษาความมั่นคงปลอดภัยไซเบอร์ด้านสาธารณสุข มีการจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยไซเบอร์ด้านสาธารณสุข (Health CIRT) เพื่อทำหน้าหน้าที่ประสานงาน เฝ้าระวัง รับมือ และแก้ไขภัยคุกคามทางไซเบอร์ด้านสาธารณสุข
ผลผลิต/ ผลลัพธ์ ระดับ T (Trends) แนวโน้ม	- การมีมาตรการขับเคลื่อนการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ช่วยให้องค์กรสามารถวางแนวทางการยืนยันตัวตน ปกป้อง ตรวจสอบ และตอบสนองต่อภัยคุกคามและฟื้นฟูระบบหลังจากได้รับผลกระทบไว้ได้อย่างดี พร้อมทั้งกำหนดบทบาทหน้าที่ให้สามารถนำมาใช้ได้ทันที
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 เพื่อให้องค์กรสามารถดำเนินได้อย่างต่อเนื่อง และฟื้นฟูระบบให้กลับคืนมาเหมือนเดิม (Recovery) - ผลการดำเนินการในปัจจุบันมีการดำเนินงาน ดังนี้

ผลผลิต/ผลลัพธ์ระดับ	รายละเอียด
	• การให้ความรู้และทำความเข้าใจกับบุคลากร โดยมีการจัดอบรมให้ความรู้ด้านความปลอดภัยไซเบอร์ตามมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ และการสแกนช่องโหว่บนเครือข่าย และตรวจสอบเฝ้าระวังสถานะเครื่องแม่ข่าย - สรุปผลผลการดำเนินการในปัจจุบันมีการดำเนินงาน ดังนี้ 1. จัดทำแผนบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ กรมอนามัย โดยจัดทำแผนบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity Incident Response) กรมอนามัย ใช้เป็นแนวทางในการเตรียมความพร้อม เพื่อรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์ โดยจะระบุขั้นตอนที่จำเป็นผลลัพธ์ที่ได้จากแผนการตอบสนองต่อภัยคุกคามทางไซเบอร์ 2. จัดทำระบบเฝ้าระวังและแจ้งภัยคุกคามภัยทางไซเบอร์ โดยดำเนินการจัดทำระบบตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ เพื่อตอบสนองและยังยั้งต่อภัยคุกคามทางไซเบอร์ โดยมีการจัดเตรียมระบบ/อุปกรณ์ บุคลากร และช่องทางการสื่อสารแจ้งภัยคุกคามทางไซเบอร์ของกรมอนามัย สำหรับป้องกัน ตรวจจับ และเฝ้าระวังการบุกรุกระบบคอมพิวเตอร์และเครือข่าย รวมทั้งหน่วยงานภาครัฐที่กำหนดนโยบาย มาตรการ แนวทางการรักษาความมั่นคงปลอดภัยไซเบอร์ เช่น สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เป็นหน่วยงานทำหน้าที่ประสานการปฏิบัติงานร่วมกันทั้งภาครัฐและเอกชน ตามพระราช บัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562, กระทรวงสาธารณสุข โดยศูนย์ประสานการรักษาความมั่นคงปลอดภัยไซเบอร์ด้านสาธารณสุข (Health CERT) เป็นหน่วยงานทำหน้าที่ประสานงาน เฝ้าระวัง รับมือและแก้ไขภัยคุกคามทางไซเบอร์ด้านสาธารณสุข และคณะประสานงานการรักษาความมั่นคงปลอดภัยไซเบอร์ (Anamai CIRT) ของกรมอนามัย เป็นต้น 3. จัดตั้งคณะประสานงานการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของกรมอนามัย (Anamai CIRT) โดยดำเนินการจัดตั้งคณะประสานงานการรักษาความมั่นคงปลอดภัยทางไซเบอร์

ผลผลิต/ผลลัพธ์ระดับ	รายละเอียด
	ของกรมอนามัย (Anamai CIRT : Cyber Incident Response Team) ประจำปีงบประมาณ พ.ศ. 2568 ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง การกำหนดหลักเกณฑ์ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและการมอบหมายการควบคุมและกำกับดูแล พ.ศ. 2564 หมวด 7 ด้านสาธารณสุข กำหนดให้หน่วยงานที่มีการให้บริการสุขภาพในโรงพยาบาล บริการสุขภาพระหว่างโรงพยาบาล บริการด้านเวชภัณฑ์และเครื่องมือแพทย์ บริการตรวจวิเคราะห์ทางการแพทย์และรังสีวิทยา และบริการข้อมูลสุขภาพดิจิทัล ต้องดำเนินการรักษาความมั่นคงปลอดภัยทางไซเบอร์ โดยอยู่ภายใต้การกำกับดูแลของสำนักงานปลัดกระทรวงสาธารณสุข 4. สร้างความตระหนักด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ให้กับเจ้าหน้าที่ของกรมอนามัย • การประชุมเชิงปฏิบัติการขับเคลื่อนการดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศของกรมอนามัย เพื่อให้เจ้าหน้าที่กรมอนามัยตระหนักถึงภัยคุกคามทางไซเบอร์และเสริมสร้างความรู้ความเข้าใจเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 5. ผลลัพธ์ของตัวชี้วัดร้อยละการรายงานภัยคุกคามทางไซเบอร์ (Outcome) มีผลลัพธ์ตรงเป้าหมายเป็นสัดส่วนตามระยะเวลา ระหว่างเดือนตุลาคม 2567 – กุมภาพันธ์ 2568 ดังนี้ 5.1 จำนวนการละเมิดความปลอดภัยทางไซเบอร์ (Security Breaches) ของกรมอนามัยลดลงจาก 32 ครั้ง/ปี เหลือไม่เกิน 25 ครั้ง/ปี พบว่า ผลลัพธ์ของจำนวนการละเมิดความปลอดภัยทางไซเบอร์ (Security Breaches) ของกรมอนามัย จำนวน 6 ครั้ง ซึ่งลดลงจาก 12 ครั้งในรอบ 5 เดือนแรก

ผลผลิต/ผลลัพธ์ระดับ	รายละเอียด
	5.2 ร้อยละความสำเร็จในการกู้คืนระบบงานกองแผนงานให้พร้อมใช้งานภายใน 24 ชั่วโมง หลังจากตรวจพบการถูกละเมิดความปลอดภัยทางไซเบอร์ (Security Breaches) ผลลัพธ์ คือ กองแผนงานไม่มีระบบงานที่ต้องดำเนินการกู้คืนให้พร้อมใช้งานภายใน 24 ชม. ระบบมีความพร้อมในการป้องกันการถูกละเมิดความปลอดภัยทางไซเบอร์ในรอบ 5 เดือนแรก จึงไม่มีข้อมูลที่ถูกละเมิดและแก้ไขปัญหาได้ทันที

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	ความปลอดภัยของข้อมูลส่วนตัวที่ภาครัฐเก็บไว้ต้องมีการรักษาความมั่นคงปลอดภัยไซเบอร์

1.2.2 กลุ่มผู้มีส่วนได้ส่วนเสีย

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