ตัวชี้วัด 4.21 : ระดับความสำเร็จของมาตรการขับเคลื่อนการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

4. Output ผลผลิต

4.1 มีผลผลิตตรงตามเป้าหมายที่กำหนด

ระดับความสำเร็จของมาตรการขับเคลื่อนการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ 5 ขั้นตอน (รอบที่ 1 : 5 เดือนแรก)

คะแนน	ขั้นตอน	มาตรการขับเคลื่อน
0.2	ขั้นตอนที่ 1	จัดทำแผนบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ กรมอนามัย
0.4	ขั้นตอนที่ 2	จัดทำระบบเฝ้าระวังและแจ้งภัยคุกคามภัยทางไซเบอร์
0.6	ขั้นตอนที่ 3	จัดตั้งคณะประสานงานการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของกรมอนามัย (Anamai CIRT)
0.8	ขั้นตอนที่ 4	สร้างความตระหนักด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ให้กับเจ้าหน้าที่ของกรมอนามัย
1.0	ขั้นตอนที่ 5	สรุปผลการดำเนินงานตามมาตรการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

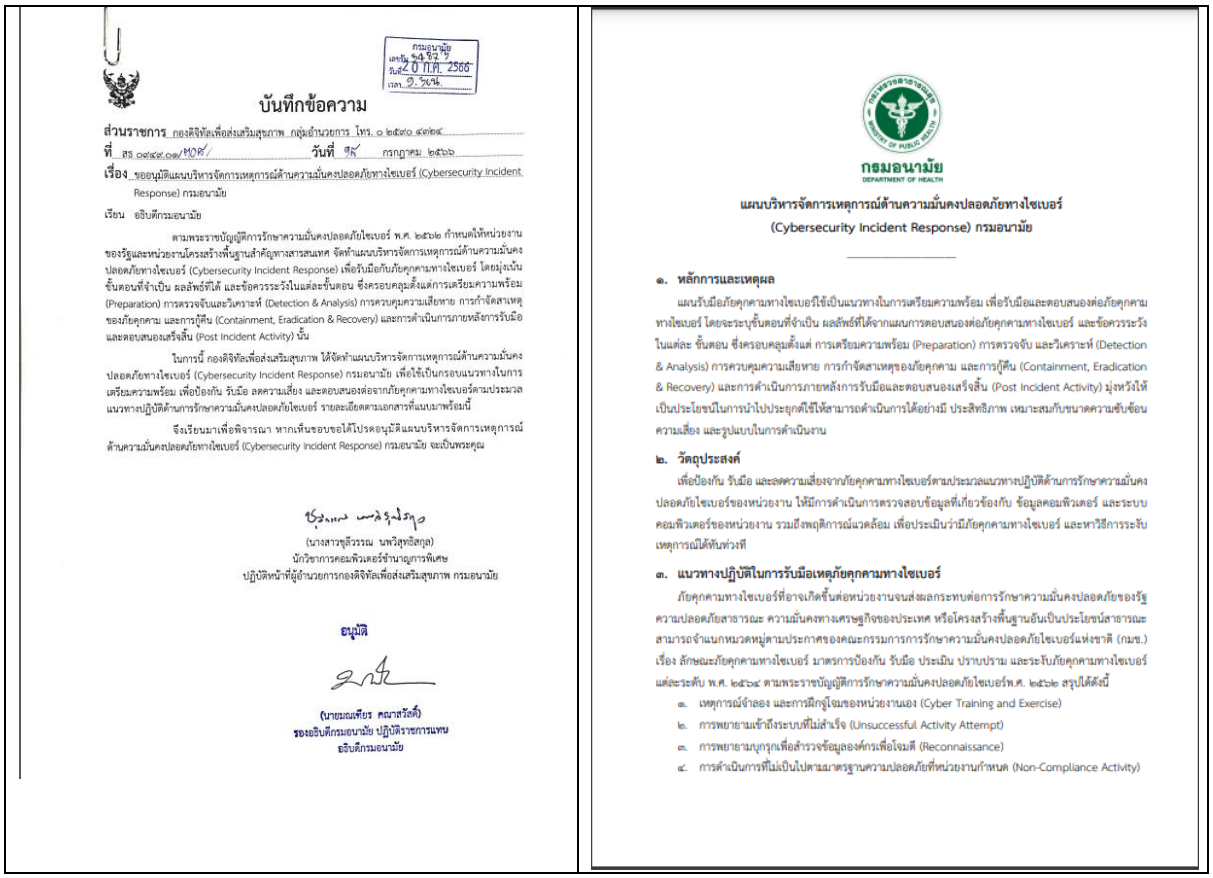
แผนการขับเคลื่อนและกำกับติดตามการดำเนินงานตัวชี้วัดตามคำรับรองการปฏิบัติราชการประจำปีงบประมาณ พ.ศ.2567 (รอบ 5 เดือนแรก)

ที่	กิจกรรม/ขั้นตอน	เป้าหมาย (จำนวน)	หน่วยนับ	วันที่เริ่มกิจกรรม	วันที่สิ้นสุด	ผลการดำเนินงาน		
						ไม่ได้ดำเนินการ	อยู่ระหว่างดำเนินการ	ดำเนินการครบถ้วน
1	จัดทำแผนบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ กรมอนามัย	1	ครั้ง	1 ต.ค.66	31 ธ.ค. 66			✓
2	จัดทำระบบเฝ้าระวังและแจ้งภัยคุกคามทางไซเบอร์	1	ครั้ง	1 พ.ย.66	31 ม.ค. 67			✓
3	จัดตั้งคณะประสานงานการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของกรมอนามัย (Anamai CIRT)	1	ครั้ง	1 ธ.ค.66	31 ม.ค. 67			✓
4	สร้างความตระหนักด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ให้กับเจ้าหน้าที่ของกรมอนามัย	1	ครั้ง	1 ธ.ค. 66	31 ม.ค. 67			✓
5	สรุปผลการดำเนินงานตามมาตรการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	1	ครั้ง	1 ก.พ. 66	29 ก.พ. 67			✓

ดำเนินงานตามมาตรการขับเคลื่อนการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ 5 ขั้นตอน ดังต่อไปนี้

ขั้นตอนที่ 1 : จัดทำแผนบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ กรมอนามัย

การจัดทำแผนบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity Incident Response) กรมอนามัย ใช้เป็นแนวทางในการเตรียมความพร้อม เพื่อรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์ โดยจะระบุขั้นตอนที่จำเป็น ผลลัพธ์ที่ได้จากแผนการตอบสนองต่อภัยคุกคามทางไซเบอร์ และข้อควรระวังในแต่ละ ขั้นตอน ซึ่งครอบคลุมตั้งแต่ การเตรียมความพร้อม (Preparation) การตรวจจับและวิเคราะห์ (Detection & Analysis) การควบคุมความเสียหาย การกำจัดสาเหตุของภัยคุกคาม และการกู้คืน (Containment, Eradication & Recovery) และการดำเนินการภายหลังการรับมือและตอบสนองเสร็จสิ้น (Post Incident Activity) มุ่งหวังให้เป็นประโยชน์ในการนำไปประยุกต์ใช้ให้สามารถดำเนินการได้อย่างมีประสิทธิภาพ เหมาะสมกับขนาดความซับซ้อน ความเสี่ยง และรูปแบบในการดำเนินงาน โดยมีรายละเอียดดังนี้



กรมอนามัย
เลขรับ 34827
วันที่ 20 ก.ค. 2566
เวลา 9.30 น.

บันทึกข้อความ

ส่วนราชการ กองดิจิทัลเพื่อส่งเสริมสุขภาพ กลุ่มอำนวยการ โทร. ๐ ๒๕๙๐ ๔๗๒๔
ที่ สธ ๐๙๔๙.๐๓/พิเศษ **วันที่** ๑๙ กรกฎาคม ๒๕๖๖
เรื่อง ขออนุมัติแผนบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity Incident Response) กรมอนามัย

เรียน อธิบดีกรมอนามัย

ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดให้หน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ จัดทำแผนบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity Incident Response) เพื่อรับมือกับภัยคุกคามทางไซเบอร์ โดยมุ่งเน้นขั้นตอนที่จำเป็น ผลลัพธ์ที่ได้ และข้อควรระวังในแต่ละขั้นตอน ซึ่งครอบคลุมตั้งแต่การเตรียมความพร้อม (Preparation) การตรวจจับและวิเคราะห์ (Detection & Analysis) การควบคุมความเสียหาย การกำจัดสาเหตุของภัยคุกคาม และการกู้คืน (Containment, Eradication & Recovery) และการดำเนินการภายหลังการรับมือและตอบสนองเสร็จสิ้น (Post Incident Activity) นั้น

ในการนี้ กองดิจิทัลเพื่อส่งเสริมสุขภาพ ได้จัดทำแผนบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity Incident Response) กรมอนามัย เพื่อใช้เป็นกรอบแนวทางในการเตรียมความพร้อม เพื่อป้องกัน รับมือ ลดความเสี่ยง และตอบสนองต่อจากภัยคุกคามทางไซเบอร์ตามประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ รายละเอียดตามเอกสารที่แนบมาพร้อมนี้

จึงเรียนมาเพื่อพิจารณา หากเห็นชอบขอได้โปรดอนุมัติแผนบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity Incident Response) กรมอนามัย จะเป็นพระคุณ

(นางสาวชุลีวรรณ นพวิสุทธิสกุล)
นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ
ปฏิบัติหน้าที่ผู้อำนวยการกองดิจิทัลเพื่อส่งเสริมสุขภาพ กรมอนามัย

อนุมัติ

(นายมณเฑียร คณาสวัสดิ์)
รองอธิบดีกรมอนามัย ปฏิบัติราชการแทน
อธิบดีกรมอนามัย

กรมอนามัย
DEPARTMENT OF HEALTH

แผนบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์
(Cybersecurity Incident Response) กรมอนามัย

๑. หลักการและเหตุผล

แผนรับมือภัยคุกคามทางไซเบอร์ใช้เป็นแนวทางในการเตรียมความพร้อม เพื่อรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์ โดยจะระบุขั้นตอนที่จำเป็น ผลลัพธ์ที่ได้จากแผนการตอบสนองต่อภัยคุกคามทางไซเบอร์ และข้อควรระวังในแต่ละ ขั้นตอน ซึ่งครอบคลุมตั้งแต่ การเตรียมความพร้อม (Preparation) การตรวจจับ และวิเคราะห์ (Detection & Analysis) การควบคุมความเสียหาย การกำจัดสาเหตุของภัยคุกคาม และการกู้คืน (Containment, Eradication & Recovery) และการดำเนินการภายหลังการรับมือและตอบสนองเสร็จสิ้น (Post Incident Activity) มุ่งหวังให้เป็นประโยชน์ในการนำไปประยุกต์ใช้ให้สามารถดำเนินการได้อย่างมี ประสิทธิภาพ เหมาะสมกับขนาดความซับซ้อน ความเสี่ยง และรูปแบบในการดำเนินงาน

๒. วัตถุประสงค์

เพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ตามประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน ให้มีการดำเนินการตรวจสอบข้อมูลที่เกี่ยวข้องกับ ข้อมูลคอมพิวเตอร์ และระบบคอมพิวเตอร์ของหน่วยงาน รวมถึงพฤติการณ์แวดล้อม เพื่อประเมินว่ามีภัยคุกคามทางไซเบอร์ และหาวิธีการระงับเหตุการณ์ได้ทันท่วงที

๓. แนวทางปฏิบัติในการรับมือเหตุภัยคุกคามทางไซเบอร์

ภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นต่อหน่วยงานจนส่งผลกระทบต่อการรักษาความมั่นคงปลอดภัยของรัฐ ความปลอดภัยสาธารณะ ความมั่นคงทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ สามารถจำแนกหมวดหมู่ตามประกาศของคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์พ.ศ. ๒๕๖๒ สรุปได้ดังนี้

๑. เหตุการณ์จำลอง และการฝึกรู้โจมของหน่วยงานเอง (Cyber Training and Exercise)
๒. การพยายามเข้าถึงระบบที่ไม่สำเร็จ (Unsuccessful Activity Attempt)
๓. การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance)
๔. การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยที่หน่วยงานกำหนด (Non-Compliance Activity)

ขั้นตอนที่ 2 : จัดทำระบบเฝ้าระวังและแจ้งภัยคุกคามทางไซเบอร์

การจัดทำระบบเฝ้าระวังและแจ้งภัยคุกคามภัยทางไซเบอร์ 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 โดยมีรายละเอียด ดังนี้

1. จัดเตรียมระบบ/อุปกรณ์สำหรับป้องกัน ตรวจจับ และเฝ้าระวังการบุกรุกระบบคอมพิวเตอร์และเครือข่าย จากภัยคุกคามทางไซเบอร์ ดังนี้
   - อุปกรณ์ป้องกันความปลอดภัยด้านเครือข่าย เช่น
     - อุปกรณ์ป้องกันเครือข่าย (Firewall)
     - อุปกรณ์ป้องกันและตรวจจับการบุกรุก (Intrusion Prevention System : IPS)
     - อุปกรณ์ตรวจจับและป้องกันการโจมตีระบบเครือข่ายแบบ (DDoS)
     - อุปกรณ์ป้องกันการบุกรุกเว็บไซต์ (Web Application Firewall)
     - ระบบป้องกันไวรัส (Kaspersky Antivirus Security System)
     - อุปกรณ์จัดเก็บ Log File ระบบเครือข่าย
   - การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ โดยการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น
     - เทคโนโลยีการเข้ารหัสข้อมูล (Secure Socket Layer : SSL) โดยการเข้ารหัสข้อมูล เพื่อเพิ่มความปลอดภัยในการสื่อสารหรือส่งข้อมูลบนเครือข่ายอินเทอร์เน็ต ระหว่างเครื่องเซิร์ฟเวอร์กับเว็บเบราว์เซอร์
     - เครือข่ายส่วนตัวเสมือน (Virtual Private Network : VPN) โดยสร้างการเชื่อมต่อเครือข่ายส่วนตัวระหว่างอุปกรณ์ต่างๆ ผ่านอินเทอร์เน็ต
   - ซอฟต์แวร์เฝ้าระวังภัยคุกคามทางไซเบอร์ เช่น PRTG Network Monitor เป็นต้น
     - ระบบตรวจสอบสถานะเครือข่าย (PRTG Network Monitoring) โดยมีโปรโตคอลสำหรับมอนิเตอร์อุปกรณ์ (SNMP) และคำสั่งตรวจสอบสถานะการทำงาน UP/Down (Ping)
2. จัดเตรียมบุคลากร เพื่อทำหน้าที่ประสานงาน เฝ้าระวัง รับมือและแก้ไขภัยคุกคามทางไซเบอร์
   - ทีมรับมือ และตอบสนองต่อภัยคุกคามทางไซเบอร์มีหน้าที่รับผิดชอบในการแจ้งข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ ให้กับผู้ที่เกี่ยวข้องทั้งภายใน และภายนอกองค์กร เพื่อให้ทุกคนสามารถดำเนินการตามหน้าที่รับผิดชอบของตนเองตามกำหนดไว้ โดยมีรายละเอียด ดังนี้

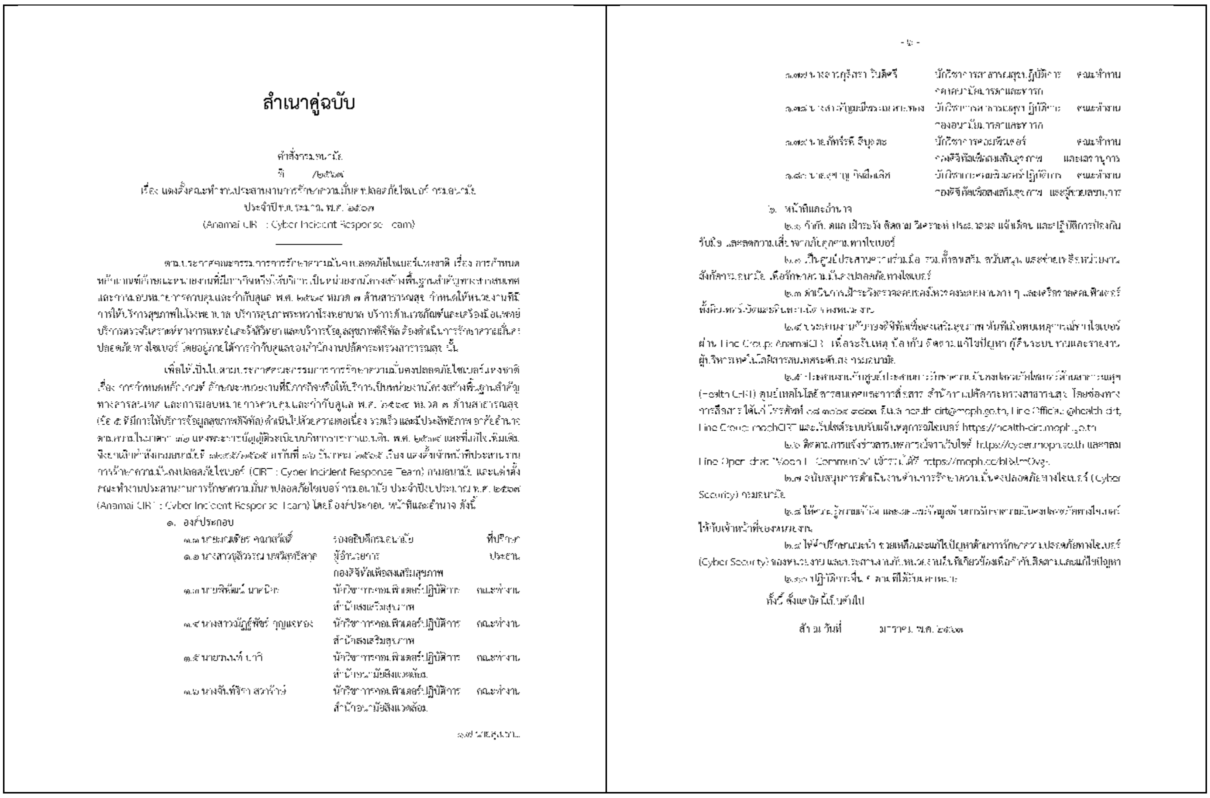
ลำดับ	ผู้ที่เกี่ยวข้อง	หน้าที่รับผิดชอบ
1	ผู้แจ้งเหตุ หรือผู้ได้รับผลกระทบ	แจ้งเหตุการณ์หรือรายงานเหตุการณ์ภัยคุกคามที่พบหรือต้องสงสัยว่าอาจจะเกิดเหตุการณ์
2	ผู้รับแจ้งเหตุการณ์ (กองดิจิทัลเพื่อส่งเสริมสุขภาพ)	รับแจ้งเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์
3	ทีมรับมือ และเฝ้าระวัง (กองดิจิทัลเพื่อส่งเสริมสุขภาพ) (เจ้าหน้าที่ประสานงานการรักษาความมั่นคงปลอดภัยไซเบอร์)	1. วิเคราะห์เหตุการณ์ภัยคุกคาม 2. รับมือและตอบสนองต่อเหตุการณ์ภัยคุกคาม 3. ให้คำปรึกษาในการป้องกัน และข้อควรระวังต่าง ๆ เกี่ยวกับเหตุการณ์ภัยคุกคาม 4. เฝ้าระวังและวิเคราะห์การแจ้งเตือนจากอุปกรณ์ตรวจจับ 5. ติดต่อหน่วยงานภายนอกในกรณีที่ไม่สามารถดำเนินการระงับเหตุการณ์ได้
4	ผู้บริหาร	รับผิดชอบกำหนดนโยบาย แนวปฏิบัติ ให้ข้อเสนอแนะ และสนับสนุนงบประมาณในด้านต่าง ๆ เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์

3. ช่องทางการสื่อสารแจ้งภัยคุกคามทางไซเบอร์ของกรมอนามัย เพื่อเป็นช่องทางการรายงานเหตุการณ์ ให้ผู้ได้รับผลกระทบหรือพบเห็นเหตุการณ์ ดังนี้

- จดหมายอิเล็กทรอนิกส์ : cybersec@anamai.mail.go.th
- กลุ่มไลน์ : AnamaiCIRT
- เบอร์ติดต่อ : 0 2590 4310
  เว็บไซต์เผยแพร่ข่าวสาร : https://cybersec.anamai.moph.go.th

ขั้นตอนที่ 3 : จัดตั้งคณะประสานงานการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของกรมอนามัย (Anamai CIRT)

การจัดตั้งคณะประสานงานการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของกรมอนามัย (Anamai CIRT) โดยดำเนินการตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง การกำหนดหลักเกณฑ์ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและการมอบหมายการควบคุมและกำกับดูแล พ.ศ. ๒๕๖๔ หมวด ๗ ด้านสาธารณสุข กำหนดให้หน่วยงานที่มีการให้บริการสุขภาพในโรงพยาบาล บริการสุขภาพระหว่างโรงพยาบาล บริการด้านเวชภัณฑ์และเครื่องมือแพทย์ บริการตรวจวิเคราะห์ทางการแพทย์และรังสีวิทยา และบริการข้อมูลสุขภาพดิจิทัล ต้องดำเนินการรักษาความมั่นคงปลอดภัยทางไซเบอร์ โดยอยู่ภายใต้การกำกับดูแลของสำนักงานปลัดกระทรวงสาธารณสุขนั้น และแต่งตั้งคณะทำงานประสานงานการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมอนามัย ประจำปีงบประมาณ พ.ศ. ๒๕๖๗ (Anamai CIRT : Cyber Incident Response Team) โดยมีรายละเอียด ดังนี้


สำเนาคู่ฉบับ

ขั้นตอนที่ 4 : สร้างความตระหนักด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ให้กับเจ้าหน้าที่ของกรมอนามัย

การจัดประชุมส่งเสริมและสนับสนุนทักษะความเข้าใจและใช้เทคโนโลยีดิจิทัลของกรมอนามัย (Digital Literacy) เรื่อง การสร้างความตระหนักด้านความมั่นคงทางไซเบอร์ (Cybersecurity Awareness) เพื่อให้เจ้าหน้าที่กรมอนามัยตระหนักถึงภัยคุกคามทางไซเบอร์ และเสริมสร้างความรู้ความเข้าใจเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มีรายละเอียด ดังนี้

1. สร้างความเข้าใจเกี่ยวกับอันตรายจากการโจมตีทางไซเบอร์ สามารถเกิดขึ้นได้ทุกเมื่อและมีผลกระทบที่หลากหลาย
2. การเข้าใจเกี่ยวกับมาตรการป้องกัน โดยอธิบายหรือแสดงให้เห็นถึงมาตรการที่สามารถใช้ป้องกันการโจมตีทางไซเบอร์ เช่น การใช้รหัสผ่านที่ปลอดภัย การป้องกันมัลแวร์ และการอัพเดตซอฟต์แวร์ เป็นต้น
3. สร้างทักษะในการระมัดระวัง โดยแนะนำหรือสอนทักษะเกี่ยวกับการระมัดระวังต่อการละเมิดความปลอดภัยที่อาจเกิดขึ้น เช่น การระวังการส่งอีเมล์แฝง การตรวจสอบลิงก์ก่อนคลิก และการระวังการใช้ข้อมูลส่วนตัว เป็นต้น
4. ส่งเสริมพฤติกรรมที่ปลอดภัย ที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์ เช่น การสำรวจและรายงานข้อผิดพลาด การส่งรายงานการบุกรุกทางไซเบอร์ และการรายงานการโจมตีที่สำเร็จ เป็นต้น
5. สนับสนุนและการกำกับดูแลผู้ใช้งาน ในการปฏิบัติตามนโยบายและมาตรการที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์
6. เผยแพร่ความรู้และข้อมูลเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์อย่างต่อเนื่อง ผ่านช่องทางต่าง ๆ เช่น สื่อสังคมออนไลน์ อีเมล์ และการประชาสัมพันธ์ เป็นต้น

บันทึกข้อความ

ส่วนราชการ กองดิจิทัลเพื่อส่งเสริมสุขภาพ กลุ่มงานบริการ โทร. ๐ ๒๕๙๐ ๔๑๒๔

ที่ สธ ๐๙๔๕.๐๗/- **วันที่** ๑๕ ธันวาคม ๒๕๖๖

เรื่อง ขอส่งสรุปรายงานการประชุมส่งเสริม และสนับสนุนทักษะความเข้าใจและใช้เทคโนโลยีดิจิทัลของกรมอนามัย (Digital Literacy) ครั้งที่ ๒/๒๕๖๖

เรียน ผู้อำนวยการกองดิจิทัลเพื่อส่งเสริมสุขภาพ

ตามที่กรมอนามัย ได้อนุมัติให้กองดิจิทัลเพื่อส่งเสริมสุขภาพดำเนินการจัดทำโครงการพัฒนาด้านเทคโนโลยีดิจิทัลและการสร้างความมั่นคงปลอดภัยของระบบสารสนเทศกรมอนามัย เพื่อยกระดับศักยภาพขององค์กรในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ กรมอนามัย ให้มีเสถียรภาพสามารถทำงานได้อย่างมีประสิทธิภาพ และพัฒนาทักษะการทำงานของเจ้าหน้าที่ผู้ดูแลระบบเทคโนโลยีสารสนเทศ และได้ดำเนินการจัดการประชุมส่งเสริม และสนับสนุนทักษะความเข้าใจและใช้เทคโนโลยีดิจิทัลของกรมอนามัย (Digital Literacy) ครั้งที่ ๒/๒๕๖๖ เรื่อง การสร้างความตระหนักด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity Awareness) วันที่ ๒๗ พฤศจิกายน ๒๕๖๖ ณ ห้องประชุมกองแผนงาน อาคาร ๕ ชั้น ๔ กรมอนามัย เรียบร้อยแล้ว นั้น

ในการนี้ เพื่อกองดิจิทัลเพื่อส่งเสริมสุขภาพ ได้ดำเนินการสรุปผลการดำเนินงานการประชุมส่งเสริม และสนับสนุนทักษะความเข้าใจและใช้เทคโนโลยีดิจิทัลของกรมอนามัย (Digital Literacy) ครั้งที่ ๒/๒๕๖๖ รายละเอียดตามเอกสารโครงการฯ ที่แนบมาพร้อมนี้

จึงเรียนมาเพื่อโปรดทราบ จะเป็นพระคุณ

(นายกิตติบันทึ สายแวส)
นักวิชาการคอมพิวเตอร์ปฏิบัติการ

๑๖ ธ.ค. ๖๖

วาระการประชุมส่งเสริม และสนับสนุนทักษะความเข้าใจและใช้เทคโนโลยีดิจิทัล
ของกรมอนามัย (Digital Literacy)
ในวันที่ ๒๗ พฤศจิกายน ๒๕๖๖ เวลา ๐๙.๓๐ - ๑๖.๓๐ น.
ณ ห้องประชุมอเนกประสงค์ อาคาร ๒ ชั้น ๒ กรมอนามัย

วาระที่ ๑ เรื่องที่ประธานแจ้งให้ทราบ

-

วาระที่ ๒ เรื่องเพื่อทราบ

๒.๑ การสร้างความตระหนักด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์
(Cybersecurity Awareness)
- ความรู้พื้นฐานของความมั่นคงปลอดภัยทางไซเบอร์
- รูปแบบภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นในองค์กร
- วิธีการตรวจสอบและแนวทางป้องกันภัยคุกคามทางไซเบอร์ในชีวิตประจำวัน
เพื่อให้มีความปลอดภัย
โดย ผู้แทนหน่วยงาน จากบริษัท อินฟอร์เมชั่น เซอร์วิส แอนด์ คอนซัลแทนท์ จำกัด
กลุ่มเป้าหมาย : เจ้าหน้าที่ผู้ใช้งานทั่วไป

วาระที่ ๓ เรื่องอื่น ๆ (ถ้ามี)

-

ขั้นตอนที่ 5 : สรุปผลการดำเนินงานตามมาตรการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

สรุปผลการดำเนินงานตามมาตรการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ดังนี้

1. จัดทำแผนบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ กรมอนามัย โดยจัดทำแผนบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity Incident Response) กรมอนามัย ใช้เป็นแนวทางในการเตรียมความพร้อม เพื่อรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์ โดยจะระบุขั้นตอนที่จำเป็น ผลลัพธ์ที่ได้จากแผนการตอบสนองต่อภัยคุกคามทางไซเบอร์ และข้อควรระวังในแต่ละขั้นตอน โดยมีรายละเอียด ดังนี้

1.1 การเตรียมความพร้อม (Preparation)

1.2 การตรวจจับและวิเคราะห์ (Detection & Analysis)

1.3 การควบคุมความเสียหาย การกำจัดสาเหตุของภัยคุกคาม และการกู้คืน (Containment, Eradication & Recovery)

1.4 การดำเนินการภายหลังการรับมือและตอบสนองเสร็จสิ้น (Post Incident Activity)

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 โดยมีรายละเอียด ดังนี้

2.1 จัดเตรียมระบบ/อุปกรณ์สำหรับป้องกัน ตรวจจับ และเฝ้าระวังการบุกรุกระบบคอมพิวเตอร์และเครือข่ายจากภัยคุกคามทางไซเบอร์ เช่น อุปกรณ์ป้องกันความปลอดภัยด้านเครือข่าย, ซอฟต์แวร์เฝ้าระวังภัยคุกคามทางไซเบอร์ และเทคนิคเข้ารหัสการรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะเป็นต้น

2.2 จัดเตรียมบุคลากร เพื่อทำหน้าที่ประสานงาน เฝ้าระวัง รับมือและแก้ไขภัยคุกคามทางไซเบอร์ โดยมีหน้าที่รับผิดชอบในการแจ้งข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ ให้กับผู้ที่เกี่ยวข้องทั้งภายใน และภายนอกองค์กร เพื่อให้ทุกคนสามารถดำเนินการตามหน้าที่รับผิดชอบของตนเองตามกำหนดไว้

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

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

4. สร้างความตระหนักด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ให้กับเจ้าหน้าที่ของกรมอนามัย

การจัดประชุมส่งเสริมและสนับสนุนทักษะความเข้าใจและใช้เทคโนโลยีดิจิทัลของกรมอนามัย (Digital Literacy) เรื่อง การสร้างความตระหนักด้านความมั่นคงทางไซเบอร์ (Cybersecurity Awareness) เพื่อให้เจ้าหน้าที่กรมอนามัยตระหนักถึงภัยคุกคามทางไซเบอร์ และเสริมสร้างความรู้ความเข้าใจเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มีรายละเอียด ดังนี้

4.1 สร้างความเข้าใจเกี่ยวกับอันตรายจากการโจมตีทางไซเบอร์

4.2 การเข้าใจเกี่ยวกับมาตรการป้องกันการโจมตีทางไซเบอร์

4.3 สร้างทักษะในการระมัดระวังต่อการละเมิดความปลอดภัย

4.4 ส่งเสริมพฤติกรรมที่ปลอดภัยที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์

4.5 สนับสนุนและการกำกับดูแลผู้ใช้งานในการปฏิบัติตามนโยบายและมาตรการ

4.6 เผยแพร่ความรู้และข้อมูลเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์