ตัวชี้วัด 4.19 : ระดับความสำเร็จของการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมอนามัย

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

แผนการขับเคลื่อนและกำกับติดตามการดำเนินงานตัวชี้วัดตามคำรับรองการปฏิบัติราชการ ประจำปีงบประมาณ พ.ศ.2568 (รอบ 5 เดือนแรก)

ที่	กิจกรรม/ขั้นตอน	เป้าหมาย (จำนวน)	หน่วยนับ	วันที่เริ่มกิจกรรม	วันที่สิ้นสุด	ผลการดำเนินงาน	
						อยู่ระหว่างดำเนินการ	ดำเนินการครบถ้วน
1	จัดทำแผนบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ กรมอนามัย	1	ครั้ง	1 ต.ค.67	31 ธ.ค.67		✓
2	จัดทำระบบเฝ้าระวังและแจ้งภัยคุกคามทางไซเบอร์	1	ครั้ง	1 พ.ย.67	31 ม.ค.68		✓
3	จัดตั้งคณะประสานงานการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของกรมอนามัย (Anamai CIRT)	1	ครั้ง	1 ธ.ค.67	31 ม.ค.68		✓
4	สร้างความตระหนักด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ให้กับเจ้าหน้าที่ของกรมอนามัย	1	ครั้ง	1 ธ.ค.67	31 ม.ค.68		✓
5	สรุปผลการดำเนินงานตามมาตรการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	1	ครั้ง	1 ก.พ.67	28 ก.พ.68		✓

ดำเนินงานตามมาตรการขับเคลื่อนการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ 5 ขั้นตอน ดังต่อไปนี้

ขั้นตอนที่ 1 : จัดทำแผนบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ กรมอนามัย

การจัดทำแผนบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity Incident Response) กรมอนามัย ใช้เป็นแนวทางในการเตรียมความพร้อม 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 โดยมีรายละเอียด ดังนี้

กรมอนามัย
DEPARTMENT OF HEALTH

แผนบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์
(Cybersecurity Incident Response) กรมอนามัย ประจำปี ๒๕๖๘

---

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 และการฝึกซ้อมของหน่วยงานเอง (Cyber Training and Exercise)
๒. การพยายามเข้าถึงระบบที่ไม่สำเร็จ (Unsuccessful Activity Attempt)
๓. การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance)
๔. การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยที่หน่วยงานกำหนด (Non-Compliance Activity)
๕. การบุกรุกโดยการใช้มัลแวร์ (Malicious Logic)
๖. การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion)
๗. การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion)
๘. การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)
๙. เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating)

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

   1.1 อุปกรณ์ป้องกันความปลอดภัยด้านเครือข่าย เช่น

   - อุปกรณ์ป้องกันเครือข่าย (Firewall)
   - อุปกรณ์ป้องกันและตรวจจับการบุกรุก (Intrusion Prevention System : IPS)
   - อุปกรณ์ตรวจจับและป้องกันการโจมตีระบบเครือข่ายแบบ (DDoS)
   - อุปกรณ์ป้องกันการบุกรุกเว็บไซต์ (Web Application Firewall)
   - ระบบป้องกันไวรัส (Kaspersky Antivirus Security System)
   - อุปกรณ์จัดเก็บ Log File ระบบเครือข่าย

   1.2 การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ โดยการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น

   - เทคโนโลยีการเข้ารหัสข้อมูล (Secure Socket Layer : SSL) โดยการเข้ารหัสข้อมูล เพื่อเพิ่มความปลอดภัยในการสื่อสารหรือส่งข้อมูลบนเครือข่ายอินเทอร์เน็ต ระหว่างเครื่องเซิร์ฟเวอร์กับเว็บเบราว์เซอร์
   - เครือข่ายส่วนตัวเสมือน (Virtual Private Network : VPN) โดยสร้างการเชื่อมต่อเครือข่ายส่วนตัวระหว่างอุปกรณ์ต่างๆ ผ่านอินเทอร์เน็ต

   1.3 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

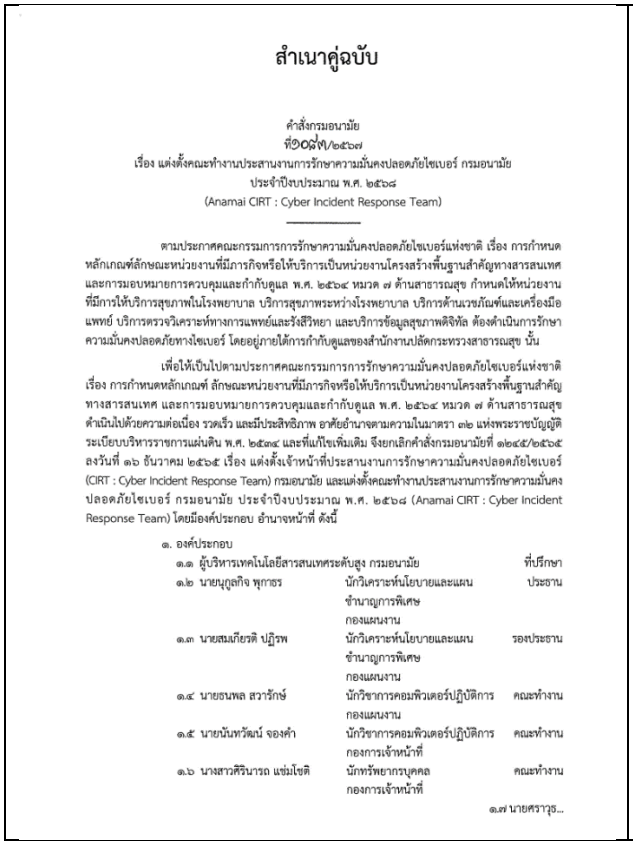
ลำดับ	ผู้ที่เกี่ยวข้อง	หน้าที่รับผิดชอบ
1	ผู้แจ้งเหตุ หรือผู้ได้รับผลกระทบ	แจ้งเหตุการณ์หรือรายงานเหตุการณ์ภัยคุกคามที่พบหรือต้องสงสัยว่าอาจจะเกิดเหตุการณ์
2	ผู้รับแจ้งเหตุการณ์ (กองแผนงาน)	รับแจ้งเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์
3	ทีมรับมือ และเฝ้าระวัง (กองแผนงาน) (เจ้าหน้าที่ประสานงานการรักษาความมั่นคงปลอดภัยไซเบอร์)	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 โดยอยู่ภายใต้การกำกับดูแลของสำนักงานปลัดกระทรวงสาธารณสุข นั้น และ**แต่งตั้งคณะทำงานประสานงานการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมอนามัย ประจำปีงบประมาณ พ.ศ. 2568** (Anamai CIRT : Cyber Incident Response Team) โดยมีรายละเอียด ดังนี้



สำเนาคู่ฉบับ

คำสั่งกรมอนามัย
ที่๒๐๘๗/๒๕๖๗
เรื่อง แต่งตั้งคณะทำงานประสานงานการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมอนามัย
ประจำปีงบประมาณ พ.ศ. ๒๕๖๘
(Anamai CIRT : Cyber Incident Response Team)

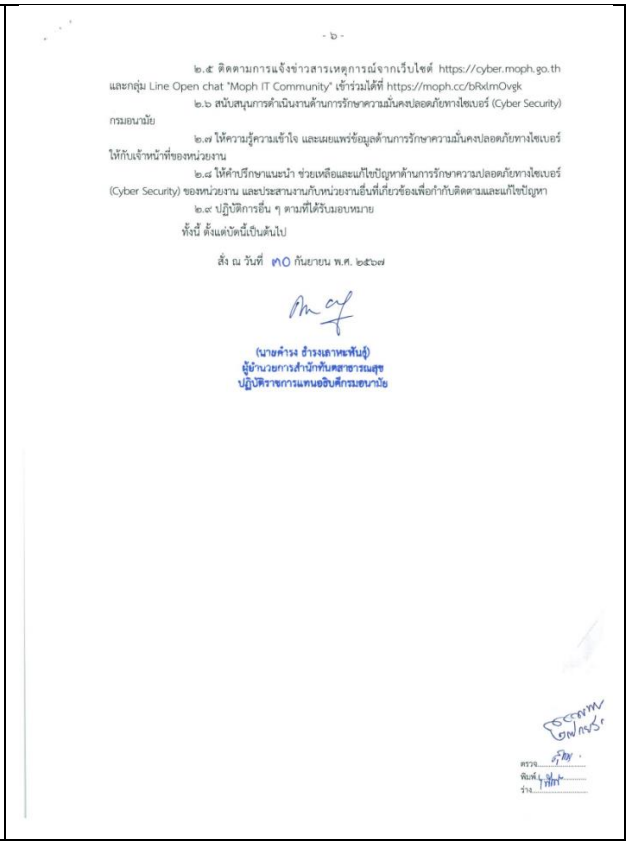
ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง การกำหนดหลักเกณฑ์ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและการมอบหมายการควบคุมและกำกับดูแล พ.ศ. ๒๕๖๔ หมวด ๗ ด้านสาธารณสุข กำหนดให้หน่วยงานที่มีการให้บริการสุขภาพในโรงพยาบาล บริการสุขภาพระหว่างโรงพยาบาล บริการด้านเวชภัณฑ์และเครื่องมือแพทย์ บริการตรวจวิเคราะห์ทางการแพทย์และรังสีวิทยา และบริการข้อมูลสุขภาพดิจิทัล ต้องดำเนินการรักษาความมั่นคงปลอดภัยทางไซเบอร์ โดยอยู่ภายใต้การกำกับดูแลของสำนักงานปลัดกระทรวงสาธารณสุข นั้น

เพื่อให้เป็นไปตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง การกำหนดหลักเกณฑ์ ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการมอบหมายการควบคุมและกำกับดูแล พ.ศ. ๒๕๖๔ หมวด ๗ ด้านสาธารณสุข ดำเนินไปด้วยความต่อเนื่อง รวดเร็ว และมีประสิทธิภาพ อาศัยอำนาจตามความในมาตรา ๓๒ แห่งพระราชบัญญัติระเบียบบริหารราชการแผ่นดิน พ.ศ. ๒๕๓๔ และที่แก้ไขเพิ่มเติม จึงยกเลิกคำสั่งกรมอนามัยที่ ๑๒๔๕/๒๕๖๕ ลงวันที่ ๑๖ ธันวาคม ๒๕๖๕ เรื่อง แต่งตั้งเจ้าหน้าที่ประสานงานการรักษาความมั่นคงปลอดภัยไซเบอร์ (CIRT : Cyber Incident Response Team) กรมอนามัย และแต่งตั้งคณะทำงานประสานงานการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมอนามัย ประจำปีงบประมาณ พ.ศ. ๒๕๖๘ (Anamai CIRT : Cyber Incident Response Team) โดยมีองค์ประกอบ อำนาจหน้าที่ ดังนี้

๑. องค์ประกอบ

๑.๑ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง กรมอนามัย		ที่ปรึกษา
๑.๒ นายนุกูลกิจ พุกาธร	นักวิเคราะห์นโยบายและแผนชำนาญการพิเศษ กองแผนงาน	ประธาน
๑.๓ นายสมเกียรติ ปฏิรูพ	นักวิเคราะห์นโยบายและแผนชำนาญการพิเศษ กองแผนงาน	รองประธาน
๑.๔ นายธนพล สวารักษ์	นักวิชาการคอมพิวเตอร์ปฏิบัติการ กองแผนงาน	คณะทำงาน
๑.๕ นายนันทวัฒน์ จองคำ	นักวิชาการคอมพิวเตอร์ปฏิบัติการ กองการเจ้าหน้าที่	คณะทำงาน
๑.๖ นางสาวศิรินารถ แข่มโชติ	นักทรัพยากรบุคคล กองการเจ้าหน้าที่	คณะทำงาน

๑.๗ นายศราวุธ...



- ๖ -

๒.๕ ติดตามการแจ้งข่าวสารเหตุการณ์จากเว็บไซต์ https://cyber.moph.go.th และกลุ่ม Line Open chat "Moph IT Community" เข้าร่วมได้ที่ https://moph.cc/bRxlmOvgk

๒.๖ สนับสนุนการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security) กรมอนามัย

๒.๗ ให้ความรู้ความเข้าใจ และเผยแพร่ข้อมูลด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ให้กับเจ้าหน้าที่ของหน่วยงาน

๒.๘ ให้คำปรึกษาแนะนำ ช่วยเหลือและแก้ไขปัญหาด้านการรักษาความปลอดภัยทางไซเบอร์ (Cyber Security) ของหน่วยงาน และประสานงานกับหน่วยงานอื่นที่เกี่ยวข้องเพื่อกำกับติดตามและแก้ไขปัญหา

๒.๙ ปฏิบัติการอื่น ๆ ตามที่ได้รับมอบหมาย

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

สั่ง ณ วันที่ ๓๐ กันยายน พ.ศ. ๒๕๖๗

(นายคำรน อำรงเสาหะพันธุ์)
ผู้อำนวยการสำนักทันตสาธารณสุข
ปฏิบัติราชการแทนอธิบดีกรมอนามัย

ขั้นตอนที่ 4 : สร้างความตระหนักด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ให้กับเจ้าหน้าที่ของกรมอนามัย

การจัดประชุมเชิงปฏิบัติการขับเคลื่อนการดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศของกรมอนามัย เพื่อให้เจ้าหน้าที่กรมอนามัยตระหนักถึงภัยคุกคามทางไซเบอร์ และเสริมสร้างความรู้ความเข้าใจเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 มีรายละเอียดดังนี้

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

ด่วนที่สุด **บันทึกข้อความ**

ส่วนราชการ กองแผนงาน กลุ่มสื่อสัขัดส่งเสริมสุขภาพ โทร. ๐ ๒๔๑๐ ๔๓๓๐
ที่ สธ ๐๗๐๕.๐๑/๒๔๖๔ **วันที่** ธันวาคม ๒๕๖๗
เรื่อง ขอเชิญเข้าร่วมประชุมเชิงปฏิบัติการขับเคลื่อนการดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศของกรมอนามัย

เรียน ประธานคณะกรรมการผู้ทรงคุณวุฒิ
ผู้อำนวยการสำนัก/กอง/กลุ่ม/สถาบัน ในสังกัดกรมอนามัย
เลขานุการกรม

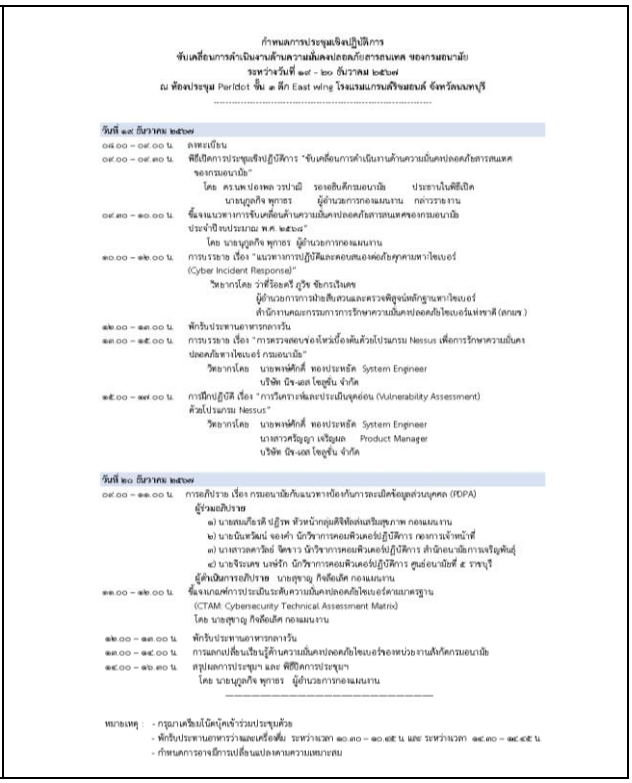
ตามที่กรมอนามัย ได้อนุมัติให้กองแผนงานจัดประชุมเชิงปฏิบัติการขับเคลื่อนการดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศของกรมอนามัย ระหว่างวันที่ ๑๙ – ๒๐ ธันวาคม ๒๕๖๗ ณ โรงแรมแกรนด์ริชมอนด์ จังหวัดนนทบุรี เพื่อสร้างความรู้ ความเข้าใจ ทักษะที่จำเป็นแก่บุคลากรของกรมอนามัย ในการเตรียมความพร้อมเพื่อรับมือจากภัยคุกคามทางไซเบอร์ นั้น

ในการนี้ กองแผนงาน ขอเชิญบุคลากรที่รับผิดชองงานเทคโนโลยีสารสนเทศ จำนวน ๑ คน เข้าร่วมประชุมเชิงปฏิบัติการขับเคลื่อนการดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศของกรมอนามัย ระหว่างวันที่ ๑๙ – ๒๐ ธันวาคม ๒๕๖๗ ณ โรงแรมแกรนด์ริชมอนด์ จังหวัดนนทบุรี ทั้งนี้ ขอให้ลงทะเบียนเข้าร่วมประชุมผ่าน QR Code ภายในวันที่ ๑๖ ธันวาคม ๒๕๖๗ รายละเอียดตามเอกสารที่แนบมาพร้อมนี้

จึงเรียนมาเพื่อโปรดพิจารณามอบหมายเจ้าหน้าที่ผู้เกี่ยวข้องเข้าร่วมประชุมเชิงปฏิบัติการฯ ตามวัน เวลา และสถานที่ดังกล่าว จะเป็นพระคุณ

(นายนฤดลกิจ พุกาธร)
ผู้อำนวยการกองแผนงาน กรมอนามัย

ลงทะเบียนเข้าร่วมการประชุม
เอกสารประกอบการประชุม



กำหนดการประชุมเชิงปฏิบัติการ
ขับเคลื่อนการดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศ ของกรมอนามัย
ระหว่างวันที่ ๑๙ - ๒๐ ธันวาคม ๒๕๖๗
ณ ห้องประชุม Peridot ชั้น ๑ ตึก East wing โรงแรมแกรนด์ริชมอนด์ จังหวัดนนทบุรี

วันที่ ๑๙ ธันวาคม ๒๕๖๗

๐๘.๐๐ – ๐๙.๐๐ น. ลงทะเบียน
๐๙.๐๐ – ๐๙.๓๐ น. พิธีเปิดการประชุมเชิงปฏิบัติการ "ขับเคลื่อนการดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศของกรมอนามัย"
โดย ดร.นพ.ปองพล รวยปาณี รองอธิบดีกรมอนามัย ประธานในพิธีเปิด
นายนฤดลกิจ พุกาธร ผู้อำนวยการกองแผนงาน กล่าวรายงาน
๐๙.๓๐ – ๑๐.๐๐ น. ชี้แจงแนวทางการขับเคลื่อนด้านความมั่นคงปลอดภัยสารสนเทศของกรมอนามัย ประจำปีงบประมาณ พ.ศ. ๒๕๖๘"
โดย นายนฤดลกิจ พุกาธร ผู้อำนวยการกองแผนงาน
๑๐.๐๐ – ๑๒.๐๐ น. การบรรยาย เรื่อง "แนวทางการปฏิบัติและตอบสนองต่อภัยคุกคามทางไซเบอร์ (Cyber Incident Response)"
วิทยากรโดย ว่าที่ร้อยตรี ภูวิช ชิตกรเจิดศร
ผู้อำนวยการกองการฝึกอบรมและตรวจพิสูจน์หลักฐานทางไซเบอร์
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)
๑๒.๐๐ – ๑๓.๐๐ น. พักรับประทานอาหารกลางวัน
๑๓.๐๐ – ๑๔.๐๐ น. การบรรยาย เรื่อง "การตรวจสอบช่องโหว่เบื้องต้นด้วยโปรแกรม Nessus เพื่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์ กรมอนามัย"
วิทยากรโดย นายพงษ์ศักดิ์ ทองประหยัด System Engineer
บริษัท นิช-เอส โซลูชั่น จำกัด
๑๔.๐๐ – ๑๗.๐๐ น. การฝึกปฏิบัติ เรื่อง "การวิเคราะห์และประเมินจุดอ่อน (Vulnerability Assessment) ด้วยโปรแกรม Nessus"
วิทยากรโดย นายพงษ์ศักดิ์ ทองประหยัด System Engineer
นางสาวศรัญญา เจริญผล Product Manager
บริษัท นิช-เอส โซลูชั่น จำกัด

วันที่ ๒๐ ธันวาคม ๒๕๖๗

๐๙.๐๐ – ๑๑.๐๐ น. การอภิปราย เรื่อง กรมอนามัยกับแนวทางป้องกันการละเมิดข้อมูลส่วนบุคคล (PDPA)
ผู้ร่วมอภิปราย
๑) นายสมเกียรติ ปฏิโพ หัวหน้ากลุ่มสื่อสัขัดส่งเสริมสุขภาพ กองแผนงาน
๒) นายนันทวัฒน์ จองคำ นักวิชาการคอมพิวเตอร์ปฏิบัติการ กองการเจ้าหน้าที่
๓) นางสาวลดาวัลย์ วัฒชาว นักวิชาการคอมพิวเตอร์ปฏิบัติการ สำนักอนามัยการเจริญพันธุ์
๔) นายจิรเดช นพจักร นักวิชาการคอมพิวเตอร์ปฏิบัติการ ศูนย์อนามัยที่ ๕ ราชบุรี
ผู้ดำเนินการอภิปราย นายสุชาญ กิจอ่อนศิล กองแผนงาน
๑๑.๐๐ – ๑๒.๐๐ น. ชี้แจงเกณฑ์การประเมินระดับความมั่นคงปลอดภัยไซเบอร์ตามมาตรฐาน (CTAM: Cybersecurity Technical Assessment Matrix)
โดย นายสุชาญ กิจอ่อนศิล กองแผนงาน
๑๒.๐๐ – ๑๓.๐๐ น. พักรับประทานอาหารกลางวัน
๑๓.๐๐ – ๑๔.๐๐ น. การแลกเปลี่ยนเรียนรู้ด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานสังกัดกรมอนามัย
๑๔.๐๐ – ๑๖.๓๐ น. สรุปผลการประชุมฯ และ พิธีปิดการประชุมฯ
โดย นายนฤดลกิจ พุกาธร ผู้อำนวยการกองแผนงาน

หมายเหตุ : - กรุณาเตรียมไมค์ผู้เข้าร่วมประชุมด้วย
- พักรับประทานอาหารว่างและเครื่องดื่ม ระหว่างเวลา ๑๐.๓๐ – ๑๐.๔๕ น. และ ระหว่างเวลา ๑๔.๓๐ – ๑๔.๔๕ น.
- กำหนดการอาจมีการเปลี่ยนแปลงตามความเหมาะสม

การประชุมเชิงปฏิบัติการขับเคลื่อนการดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศของกรมอนามัย

- ดร.นพ. ปองพล วรปาณิ รองอธิบดีกรมอนามัย เป็นประธานเปิดการประชุมเชิงปฏิบัติการ "ขับเคลื่อนการดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศของกรมอนามัย" ณ โรงแรมแกรนด์ริชมอนด์ จ.นนทบุรี เพื่อชี้แจงมาตรการและแนวทางด้าน Cyber Security ของกรมอนามัย ให้ผู้ปฏิบัติ ทุกหน่วยงานได้รับทราบและถือปฏิบัติ
- กองแผนงานจัดทำเกณฑ์การประเมินระดับความมั่นคงปลอดภัยไซเบอร์ตามมาตรฐาน (CTAM) ของกรมอนามัย เพื่อยกระดับการป้องกันภัยคุกคามด้านไซเบอร์ของกรมอนามัยทั้งส่วนกลาง และส่วนภูมิภาค
- วิทยากรจากสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ให้มาเกียรติบรรยายและแลกเปลี่ยนเรียนรู้เกี่ยวกับการตอบโต้ภัยคุกคามทางไซเบอร์ และบริษัท นิช-เอส โซลูชั่น จำกัด ให้มาเกียรติบรรยายและฝึกปฏิบัติการตรวจสอบช่องโหว่เบื้องต้นด้วยโปรแกรม Nessus

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 และเทคนิคเข้ารหัสการรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ เป็นต้น

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. 2568 ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง การกำหนดหลักเกณฑ์ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและการมอบหมายการควบคุมและกำกับดูแล พ.ศ. 2564 หมวด 7 ด้านสาธารณสุข กำหนดให้หน่วยงานที่มีการให้บริการสุขภาพในโรงพยาบาล บริการสุขภาพระหว่างโรงพยาบาล บริการด้านเวชภัณฑ์และเครื่องมือแพทย์ บริการตรวจวิเคราะห์ทางการแพทย์และรังสีวิทยา และบริการข้อมูลสุขภาพดิจิทัล ต้องดำเนินการรักษาความมั่นคงปลอดภัยทางไซเบอร์ โดยอยู่ภายใต้การกำกับดูแลของสำนักงานปลัดกระทรวงสาธารณสุข

4. สร้างความตระหนักด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ให้กับเจ้าหน้าที่ของกรมอนามัย

การจัดประชุมเชิงปฏิบัติการขับเคลื่อนการดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศของกรมอนามัย 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