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 และการฝึกจู่โจมของหน่วยงานเอง (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)

๑๐. เหตุการณ์ผิดปกติที่ได้รับการวิเคราะห์แล้วว่าไม่ใช่เหตุการณ์ภัยคุกคาม (Explained Anomaly)

๓.๑ แนวทางการปฏิบัติ

แนวทางปฏิบัติเพื่อให้มีความเข้าใจขั้นตอนการปฏิบัติต่าง ๆ และมีความพร้อมในการปฏิบัติงานในหน้าที่ความรับผิดชอบจึงแบ่งขั้นตอนการปฏิบัติออกเป็น ๔ ขั้น ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ สรุปได้ดังนี้

กระบวนการที่ ๑ : การเตรียมการและป้องกันการเกิดเหตุการณ์ภัยคุกคามทางไซเบอร์ (Preparation)

๑. การจัดเตรียมทรัพยากรและเครื่องมือและสิ่งอำนวยความสะดวกในการสื่อสารของบุคลากรผู้ทำหน้าที่รับมือและตอบสนองภัยคุกคามทางไซเบอร์ ได้แก่

- รายชื่อและช่องทางการติดต่อของผู้ที่เกี่ยวข้องและประสานงานในการรับมือและตอบสนองภัยคุกคามทางไซเบอร์
- ช่องทางการรายงานเหตุการณ์ ให้ผู้ได้รับผลกระทบหรือพบเห็นเหตุการณ์ แจ้งมายังกองดิจิทัลกรมอนามัย
- ช่องทางรายงานและติดตามข้อมูลสถานการณ์ดำเนินการของเหตุการณ์ที่ได้รับแจ้ง
- ห้องประชุม (War Room)
- สถานที่จัดเก็บหลักฐานทางอิเล็กทรอนิกส์ ข้อมูลและอุปกรณ์ ที่มีความมั่นคงปลอดภัย (Secure Storage)

๒. จัดเตรียมอุปกรณ์และซอฟต์แวร์สำหรับวิเคราะห์ภัยคุกคามทางไซเบอร์ ใช้อุปกรณ์ เช่น Firewall, SIEM

๓. มีการจัดตั้งและฝึกอบรมบุคลากรหรือทีมงานในการรับมือเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์

๔. ตั้งค่าระบบต่าง ๆ ให้ปลอดภัย เป็นการตั้งค่าอุปกรณ์เครือข่ายที่จำเป็น เช่น Router, Firewall, IPS การกำหนดแนวทางการรักษาความมั่นคงปลอดภัยของห้องแม่ข่าย มีการปิดช่องโหว่และทำการแพตช์ ระบบมีการกำหนดสิทธิ์ของผู้ใช้งานโดยให้สิทธิเท่าที่จำเป็นต่อการปฏิบัติงานที่ได้รับอนุญาตเท่านั้น การ Update Security Patch เป็นประจำ การมี Software ในการป้องกันและตรวจจับความผิดปกติในระบบ เช่น Malware Prevention

๕. การจัดทำนโยบาย แผนงาน และกระบวนการที่เกี่ยวข้อง รวมถึง การสร้างเครือข่ายความร่วมมือ แนวทางป้องกันและการเตรียมการเบื้องต้น

๖. มีการแต่งตั้ง และกำหนดหน้าที่รับผิดชอบในการรับมือ และประสานงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดย กรมอนามัยได้มีการประกาศแต่งตั้ง อ้างอิง **“คำสั่งกรมอนามัย เรื่อง แต่งตั้งเจ้าหน้าที่ประสานงานการรักษาความมั่นคงปลอดภัยไซเบอร์”**

กระบวนการที่ ๒ : การตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (Cyber Detection and Analysis)

แม้ว่าหน่วยงานจะจัดให้มีมาตรการต่าง ๆ เพื่อป้องกันหรือควบคุมมิให้เกิดภัยคุกคามทางไซเบอร์ขึ้น แต่หน่วยงานก็ยังคงเตรียมความพร้อมอยู่เสมอเพื่อรับมือกับสถานการณ์ภัยคุกคามทางไซเบอร์ที่ไม่อาจหลีกเลี่ยงได้ การดำเนินมาตรการในการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (Detection and Analysis) จึงเป็นสิ่งจำเป็นที่จะช่วยให้หน่วยงานสามารถบรรเทาความเสี่ยงที่ยังคงเหลืออยู่ และสามารถแจ้งเตือนได้อย่างทันทวงทีเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น

๒.๑ การกำหนดวิธีการในการตรวจจับเหตุการณ์ภัยคุกคามทางไซเบอร์

การตรวจจับเหตุการณ์ภัยคุกคามทางไซเบอร์ จะขึ้นอยู่กับระบบงานที่หน่วยงานใช้อยู่ รูปแบบของการพยายามโจมตีและกลไกในการปกป้องระบบ เพราะระบบการป้องกันจะแจ้งเตือน (Alert) หรือเก็บบันทึกข้อมูล (Log) เพื่อใช้ในการวิเคราะห์ หาความผิดปกติและมีการปรับ Fine Tune เพื่อให้มีความเหมาะสมกับสภาพการใช้งานของระบบ

ลักษณะของข้อมูลแจ้งเตือนที่ใช้ในการตรวจจับสามารถแบ่งได้ ๒ ประเภท ดังนี้

- Precursor: เป็นข้อมูลที่บ่งบอกว่า Incident จะเกิดขึ้นในอนาคต
- Indicator: เป็นข้อมูลที่บ่งบอกว่า Incident ได้เคยเกิดขึ้นหรือกำลังเกิดขึ้นอยู่

อุปกรณ์ที่ใช้เพื่อการป้องกันและตรวจจับต้องพิจารณาตามความเหมาะสมกับระบบที่ต้องการ ป้องกัน และต้องทำการปรับ Fine Tune เพื่อให้มีความเหมาะสมกับสภาพการใช้งานของระบบนั้น ๆ ซึ่งข้อมูลการ แจ้งเตือนเพื่อตรวจจับการบุกรุกระบบคอมพิวเตอร์และเครือข่ายมีดังนี้

๑. ประเภท Alert

- IPS และ Web Application Firewall ระบบที่ทำหน้าที่ตรวจจับและป้องกันการโจมตีในระบบเครือข่าย มีการแจ้งเตือน เมื่อพบสิ่งที่ตรงกับวิธีการโจมตีที่ระบบรู้จัก
- Anti-Malware ทำหน้าที่ตรวจจับโปรแกรมประสงค์ร้าย ทำงานทั้งในระดับเครือข่าย และ Host การตรวจเจอ Malware ในระบบเป็นข้อบ่งชี้ได้ทั้งที่กำลังพยายามโจมตีและการโจมตีได้สำเร็จแล้ว
- Third-Party บริการสอดส่องดูแลความผิดปกติที่เกิดขึ้นกับระบบ หรือระบบของหน่วยงาน ถูกนำไปโจมตีระบบอื่น ๆ ภายนอกองค์กรซึ่งบ่งบอกได้ว่าระบบภายในหน่วยงานได้ถูกยึดครองโดยผู้ไม่ประสงค์ดี และนำไปใช้สร้างความเสียหาย

๒. ประเภท Log มีดังนี้

- Operating System and Application Log ข้อมูลจาก Log ของ OS และ Application ที่ประกอบไปด้วยการบันทึกเหตุการณ์หลายประเภท สามารถถูกใช้ในการตรวจจับภัยคุกคามบางอย่างได้ขึ้นอยู่กับ ประเภทของ Log และ Rule set ที่ใช้ในการวิเคราะห์
- Network Device Log อุปกรณ์เครือข่ายที่มีการบันทึกข้อมูลที่ผ่านเข้าออกเครือข่าย สามารถถูกใช้ในการตรวจจับเหตุการณ์ภัยคุกคามบางอย่างได้ขึ้นอยู่กับประเภทของ Log และ Rule set ที่ใช้ในการ วิเคราะห์

๒.๒ การวิเคราะห์เหตุภัยคุกคามหรือความผิดปกติ

การวิเคราะห์ภัยคุกคามเพื่อให้การดำเนินการต่อไปสามารถทำได้เร็วและถูกต้อง ใช้การวิเคราะห์ ความผิดปกติเมื่อได้รับแจ้งดังนี้

- log Retention Policy คือ การใช้ Log จากอุปกรณ์ต่าง ๆ เช่น IPS, Network Devices ในการวิเคราะห์หาสาเหตุการโจมตี และบันทึกเหตุการณ์เก็บไว้เพื่อหลักฐาน ทางกฎหมายหรือเรียกดูในอนาคต
- Clock Synchronization
- Sniff and Analyze Network Data คือ การดักจับข้อมูลทางเครือข่ายเพื่อนำมาวิเคราะห์ ข้อมูล
- Seek Assistance เมื่อทีมตอบสนองไม่สามารถดำเนินการวิเคราะห์ incident เพื่อหาสาเหตุ ที่แท้จริงได้เพื่อกำจัดผู้บุกรุกออกจากระบบ จึงเรียกใช้บริการให้คำแนะนำจากที่ปรึกษาจากภายนอก

<u>ตัวอย่างการวิเคราะห์ภัยคุกคาม</u>

ประเภท IT & Cyber Security Incident	ตัวอย่างเหตุการณ์
พบเนื้อหาที่เป็นภัยคุกคาม (Abusive Content) ภัยคุกคามที่เกิดจากการใช้ / เผยแพร่ข้อมูลที่ไม่เป็นจริงหรือไม่ เหมาะสม และส่งผลให้เกิดความเสียหายต่อภาพลักษณ์ขององค์กร	ตรวจพบการกระจายข้อมูลเท็จของกรม ซึ่งส่งผลเสียหายต่อภาพลักษณ์ของกรมอนามัย
<u>พบการละเมิดนโยบาย หรือมาตรการป้องกัน</u> ภัยคุกคามที่เกิดจากบุคคลภายใน มีความไม่เข้าใจถึงแนวทางการปฏิบัติที่ถูกต้อง หรือมีการหลบเลี่ยงไม่ปฏิบัติตามแนวทางการปฏิบัติขององค์กร	๑. พบการละเลยไม่ปฏิบัติตามมาตรการรักษาความมั่นคงปลอดภัยของสำนักงาน ๒. ตรวจพบการละเมิดมาตรการป้องกันของสำนักงาน เช่น ดัดแปลง แก้ไข ซอฟต์แวร์ของสำนักงาน
<u>มีการบุกรุก หรือเจาะระบบได้สำเร็จ (Intrusion)</u> ภัยคุกคามที่เกิดกับระบบที่ถูกบุกรุก / เจาะเข้าระบบได้สำเร็จ (Intrusions)และระบบถูกครอบครองโดยผู้ที่ไม่ได้อนุญาต	๑. ตรวจพบการโจมตีระบบคอมพิวเตอร์ หรือเข้าถึงข้อมูลในระบบ สารสนเทศได้ ๒. บัญชีผู้ใช้งาน หรือรหัสผ่านของผู้ใช้งานถูกล่วงละเมิด ๓. พนักงานเข้าถึงระบบสารสนเทศโดยได้สิทธิ์ที่ไม่ถูกต้อง

๒.๓ การบันทึกเหตุการณ์ภัยคุกคาม

ต้องทำการบันทึกข้อมูลเหตุการณ์ภัยคุกคามเพื่อช่วยในการรับมือและตอบสนองภัยคุกคามอย่างมีประสิทธิภาพ และเป็นระบบ

๒.๔ การวิเคราะห์ผลกระทบและการจัดลำดับความสำคัญ

กองดิจิทัล กรมอนามัยมีการวิเคราะห์ระดับผลกระทบ ทั้ง 3 ด้านดังนี้

ระดับผลกระทบ	คำอธิบาย		
	ผลกระทบด้านชื่อเสียง	ผลกระทบด้านการให้บริการ	ผลกระทบการปฏิบัติตามข้อกำหนด
High	กระทบต่อชื่อเสียงขององค์กร และมีความร้ายแรง	ไม่สามารถให้บริการระบบงานนั้นๆ กับผู้ใดได้เป็นการหยุดชะงักโดยสมบูรณ์	เป็นการละเมิดกฎหมายที่สำคัญ และกรมอนามัย อาจถูกฟ้องร้อง
Medium	มีแนวโน้มที่จะกระทบต่อชื่อเสียงขององค์กร	ไม่สามารถบริการระบบงานได้กับ ผู้ใช้บริการบางกลุ่มหรือบางหน่วยงานทั้งภายใน และภายนอก	เป็นการละเมิดข้อกำหนดฉบับรอง ที่ไม่มีบทลงโทษต่อกรมอนามัย
Low	ไม่กระทบต่อชื่อเสียงขององค์กร หรือกระทบน้อยมาก	ไม่มีผลกระทบต่อการให้บริการ	ไม่พบการละเมิดข้อกฎหมายหรือข้อกำหนดใด ๆ

๒.๕ การติดต่อประสานงานและแจ้งข้อมูล

ทีมรับมือ และตอบสนองต่อภัยคุกคามทางไซเบอร์มีหน้าที่รับผิดชอบในการแจ้งข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ ให้กับผู้ที่เกี่ยวข้องทั้งภายใน และภายนอกองค์กร เพื่อให้ทุกคนสามารถดำเนินการตามหน้าที่รับผิดชอบของตนเองตามกำหนดไว้ โดยมีรายละเอียด ดังนี้

ลำดับ	ผู้ที่เกี่ยวข้อง	หน้าที่รับผิดชอบ
๑	ผู้แจ้งเหตุ หรือผู้ได้รับผลกระทบ	แจ้งเหตุการณ์หรือรายงานเหตุการณ์ภัยคุกคามที่พบ หรือต้องสงสัยว่าอาจจะเกิดเหตุการณ์
๒	ผู้รับแจ้งเหตุการณ์ (กองดิจิทัลเพื่อส่งเสริมสุขภาพ)	รับแจ้งเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์
๓	ทีมรับมือ และเฝ้าระวัง (กองดิจิทัลเพื่อส่งเสริมสุขภาพ) (เจ้าหน้าที่ประสานงานการรักษาความมั่นคงปลอดภัยไซเบอร์)	๑. วิเคราะห์เหตุการณ์ภัยคุกคาม ๒. รับมือและตอบสนองต่อเหตุการณ์ภัยคุกคาม ๓. ให้คำปรึกษาในการป้องกัน และข้อควรระวังต่าง ๆ เกี่ยวกับเหตุการณ์ภัยคุกคาม

		๔. เฝ้าระวังและวิเคราะห์การแจ้งเตือนจากอุปกรณ์ตรวจจับ ๕. ติดต่อหน่วยงานภายนอกในกรณีที่ไม่สามารถดำเนินการระงับเหตุการณ์ได้
๔	ผู้บริหาร	รับผิดชอบกำหนดนโยบาย แนวปฏิบัติ ให้ข้อเสนอแนะและสนับสนุนงบประมาณในด้านต่าง ๆ เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์

กระบวนการที่ ๓ การระงับเหตุการณ์ภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบที่ได้รับผลกระทบ

เมื่อหน่วยงานได้รับแจ้งเตือนการเกิดภัยคุกคามทางไซเบอร์ หน่วยงานมีการกำหนดแนวทางการดำเนินมาตรการเพื่อระงับภัยคุกคามทางไซเบอร์และการฟื้นฟูระบบ ที่ได้รับผลกระทบ (Containment, Eradication, and Recovery) โดยกำหนดให้สอดคลองกับความรุนแรง และระดับของภัยคุกคามทางไซเบอร์ โดย กรมอนามัยได้มีการกำหนด แนวทางการระงับเหตุการณ์เบื้องต้น ดังนี้

รูปแบบการระงับเหตุ	ขั้นตอนการดำเนินการ
การระงับการเชื่อมต่อระบบเครือข่าย	● ตรวจสอบ MAC Address หรือUser AD หรือ User Authentication ของเครื่องที่เกิดปัญหาโดยเทียบกับฐานข้อมูลทรัพย์สิน ● Quarantine IP Address ออกจากระบบเครือข่าย
การระงับการให้บริการระบบงานหรือการเข้าถึงระบบงานจากภายนอก	● ตรวจสอบ IP Server ● แจ้งหน่วยงานเจ้าของระบบ (Line, Email) ● ปิดการเข้าถึงระบบจากภายนอก
การระงับสิทธิ์การเข้าใช้งานระบบ Application หรือเครื่องคอมพิวเตอร์แม่ข่าย	● ดำเนินการ Verify กับทาง User ทันที ● ทำการตัด Session การเข้าใช้งานทั้งหมดของ User ออกจากระบบ ● ทำการ Reset Password ของผู้ใช้งาน
กำหนดหน้าเว็บไซต์ชั่วคราว	● ตรวจสอบชื่อ Domain name ● ตรวจสอบ IP Address ● ชี้ Domain name มายังระบบบริการเว็บไซต์ชั่วคราว

รูปแบบการระงับเหตุ	ขั้นตอนการดำเนินการ
การนำ Cache ออกจาก Google หรือ Search Engine	• ตรวจสอบ link หรือ Path ที่พบปัญหา • ลบ Cache โดยใช้ Tools ของ Search Engine นั้น ๆ • นำ Path หรือ link ที่มีปัญหาแจ้งในระบบ • ตรวจสอบ Update Cache ของ Search Engine
Block BOT ของ Search Engine	• ตรวจสอบ link หรือ Path ที่พบปัญหา • แทรกคำสั่ง Deny Bot ที่ link หรือ Path ที่มีปัญหา

๓.๑ แนวทางการจัดเก็บและดูแลรักษาหลักฐานทางดิจิทัล

วัตถุประสงค์หลักของการจัดเก็บหลักฐาน คือ เพื่อให้การแก้ไข Incident ส่งผลกระทบต่อธุรกิจให้น้อยที่สุด (Minimizing impact to the business) นอกจากนี้หลักฐานอาจมีความจำเป็นที่จะต้องใช้ในการดำเนินงานตามขั้นตอนทางกฎหมาย โดยรายละเอียดเกี่ยวกับหลักฐาน ควรประกอบด้วยข้อมูลอย่างน้อย ดังนี้

๑. ข้อมูลเฉพาะ เช่น Location, Serial Number, Model Number, Hostname, Media Access Control (MAC), และ Address
๒. ชื่อ ตำแหน่ง และช่องทางติดต่อผู้จัดเก็บและรักษาหลักฐานระหว่างมือ Incident
๓. สถานที่จัดเก็บหลักฐาน

๓.๒ การกำจัดสาเหตุและการกู้คืนระบบให้กลับมาทำงานปกติ

เมื่อมีการควบคุมความเสียหาย และมีการเก็บหลักฐานข้อมูลเพิ่มเติมเรียบร้อยแล้วข้อมูลทั้งหมด จะต้องนำกลับมาวิเคราะห์ตามหลักการที่ได้กล่าวไว้ใน “ขั้นตอนที่ 2 เรื่องการตรวจจับและวิเคราะห์ (Detection & Analysis)” จนกว่าจะสามารถกำจัดสาเหตุที่ทำให้เกิด Incident และช่องทางที่ผู้บุกรุกได้สร้างไว้เพื่อเข้ามา ในระบบทั้งหมดได้เรียบร้อย ซึ่งการกำจัดสาเหตุที่ทำให้เกิด Incident และผลกระทบ ได้แก่

- การปิดช่องโหว่ของระบบ
- การยกเลิกการใช้งานระบบ
- การยกเลิก User Account ที่ผู้บุกรุกใช้เข้าสู่ระบบ
- การแจ้งให้ผู้ใช้งานเปลี่ยนรหัสผ่าน หรือการ Reset รหัสผ่านผ่านทั้งหมด
- การลบโปรแกรมประเภท Backdoor ออกจากระบบ
- การใช้ข้อมูล Indicator of Compromise (Ioc) ในการสแกนหา Malware หรือร่องรอยอื่น ๆ ในระบบที่ยังหลงเหลือของผู้บุกรุกเพื่อดำเนินการกำจัดให้ออกจากระบบทั้งหมด
- การ Update Version Software ให้เป็นปัจจุบัน
- อบรมความรู้ให้ความรู้และสร้างตระหนักแก่เจ้าหน้าที่กรมอนามัยและผู้เกี่ยวข้อง

หลังจากดำเนินการควบคุมความเสียหาย กำจัดสาเหตุของภัยคุกคามเสร็จเรียบร้อยแล้ว จะเข้าสู่กระบวนการฟื้นฟูระบบให้เข้าสู่สภาวะการทำงานปกติโดยในขั้นตอนนี้สิ่งที่มีความสำคัญเป็นอย่างยิ่ง และควรเตรียมการล่วงหน้าในเรื่องดังต่อไปนี้

- การ Restore Operating System หรือ Application Software ต่าง ๆ จาก Master Image ที่ปลอดภัย
- การ Restore ข้อมูลกลับเข้าระบบจาก Back Up Storage

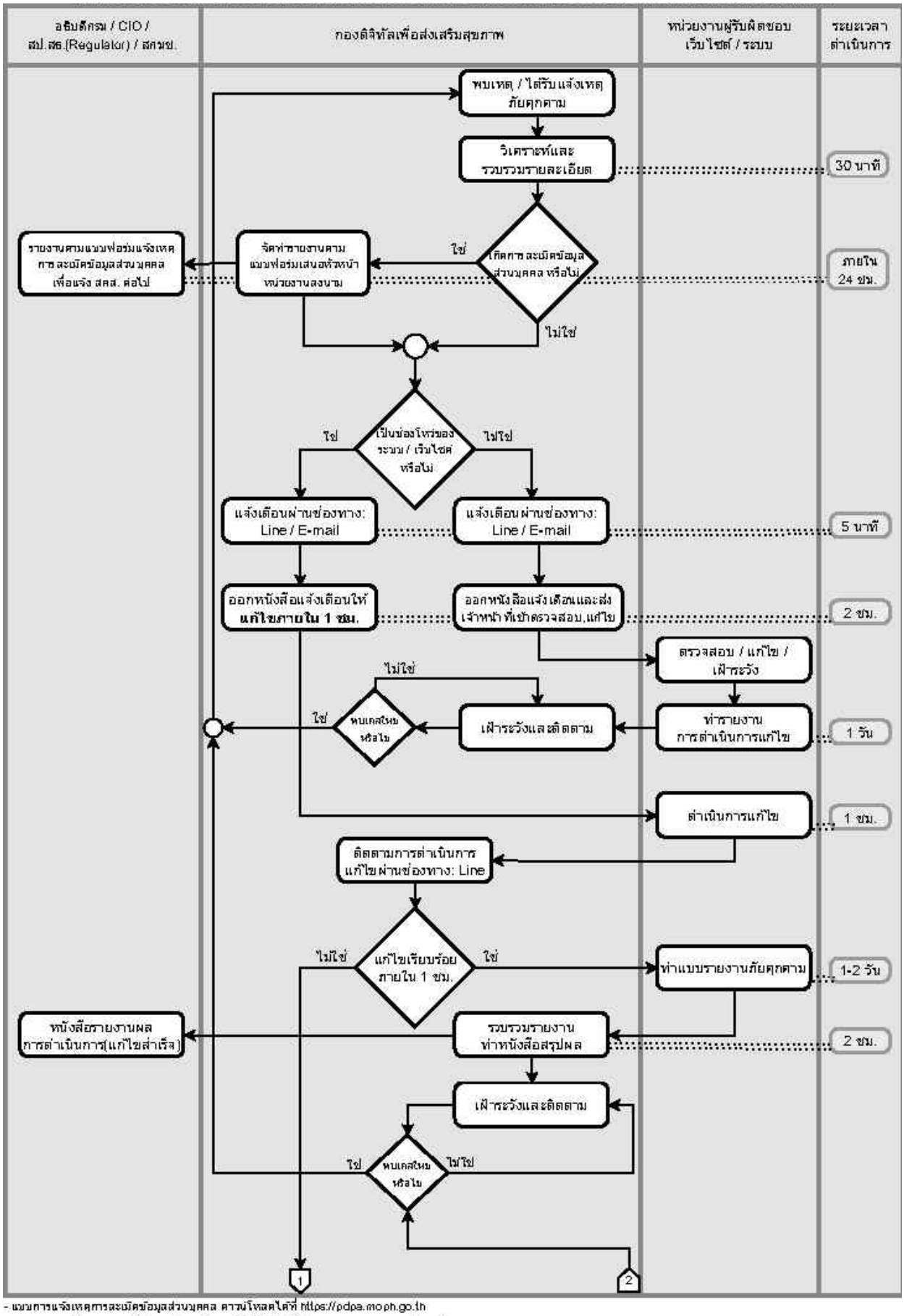
ขั้นตอนที่ ๔ การดำเนินการภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ (Post Incident Activity)

การเรียนรู้เพื่อปรับปรุงการดำเนินการ หลังจากการรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์เสร็จสิ้น (Post-Incident Activity) ทีมรับมือและผู้ที่เกี่ยวข้องทั้งหมดควรมีการประชุมหารือเพื่อแลกเปลี่ยนข้อมูลความคิดเห็น ในการนำไปพัฒนาและปรับปรุงแนวทางในการรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์ รวมทั้งการใช้ข้อมูลจาก Issue Tracking System เพื่อประกอบการพิจารณาปรับปรุงและพัฒนา

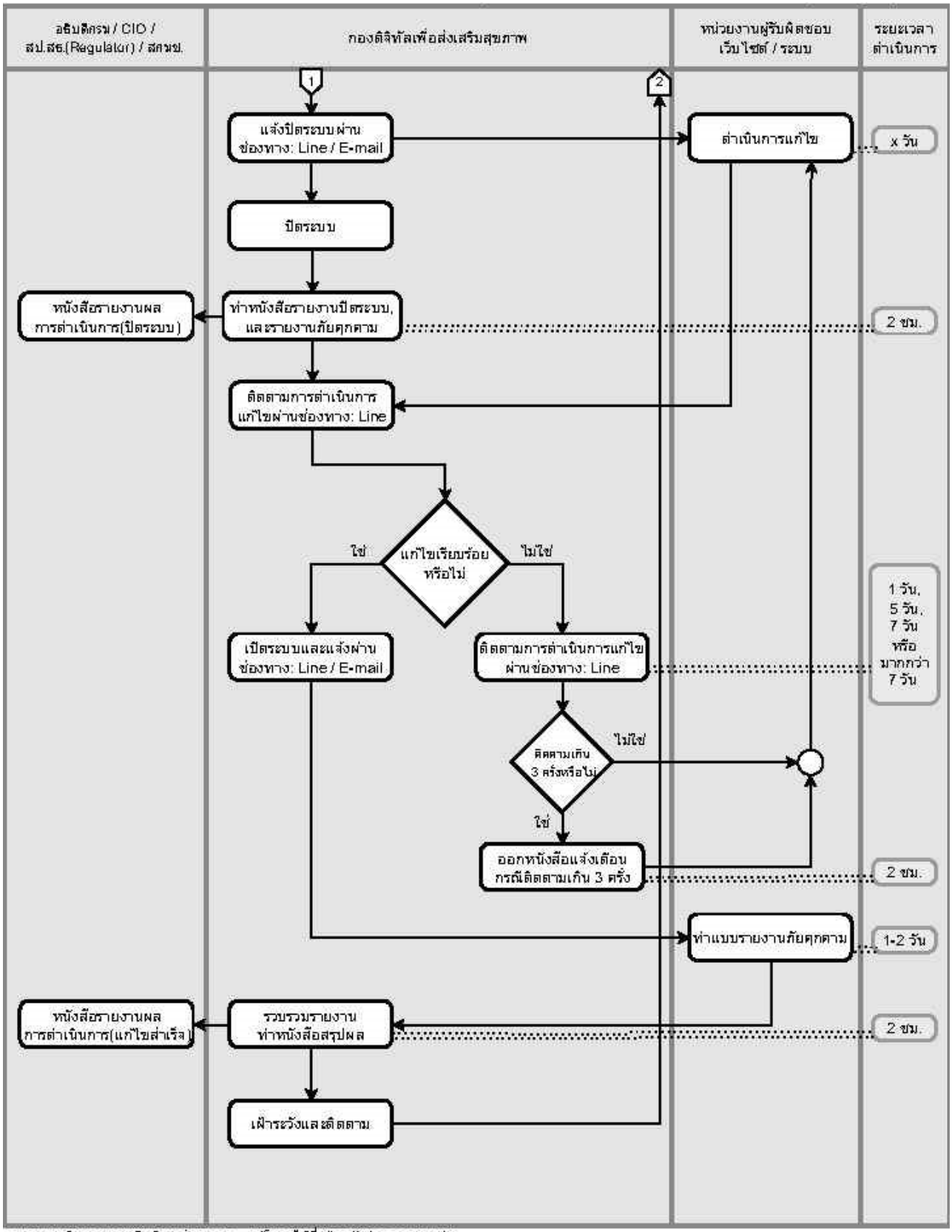
หัวข้อในการพิจารณาเพื่อปรับปรุงกระบวนการ ควรพิจารณาประเด็นดังตัวอย่างต่อไปนี้

- การดำเนินงานเสร็จสิ้นตามระยะเวลาที่กำหนด
- ขั้นตอนการรับมือภัยคุกคามทางไซเบอร์ มีความถูกต้องตามที่ระบุ
- การใช้งานทรัพยากรเพื่อรับมือและตอบสนองเป็นไปตามที่วางแผนไว้
- ข้อมูลที่ใช้ในการทดสอบมีความล่าช้า
- อุปสรรคในการติดต่อสื่อสารภายใน และภายนอก
- เหตุการณ์ภัยคุกคามที่เกิดขึ้นนี้ มีแนวทางการป้องกันไม่ให้เกิดขึ้นในอนาคต

แผนภาพขั้นตอนการจัดการและตอบสนองต่อภัยคุกคามทางไซเบอร์



- แบบการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล ดาวน์โหลดได้ที่ https://pdpa.moph.go.th
- แบบรายงานภัยคุกคามทางไซเบอร์ ดาวน์โหลดได้ที่ https://cybersec.anamai.moph.go.th



- แบบการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล ดาวน์โหลดได้ที่ https://pdpa.moph.go.th
- แบบรายงานภัยคุกคามทางไซเบอร์ ดาวน์โหลดได้ที่ https://cybersec.anamai.moph.go.th

แก้ไขล่าสุด 13 ก.ค. 2566

ภาคผนวก

สำเนาคู่ฉบับ

คำสั่งกรมอนามัย
ที่๑๐๘๗/๒๕๖๗
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 ปฏิรพ	นักวิเคราะห์นโยบายและแผนชำนาญการพิเศษ กองแผนงาน	รองประธาน
๑.๔ นายธนพล สวารักษ์	นักวิชาการคอมพิวเตอร์ปฏิบัติการ กองแผนงาน	คณะทำงาน
๑.๕ นายนันทวัฒน์ จองคำ	นักวิชาการคอมพิวเตอร์ปฏิบัติการ กองการเจ้าหน้าที่	คณะทำงาน
๑.๖ นางสาวศิรินารถ แซ่มโชติ	นักทรัพยากรบุคคล กองการเจ้าหน้าที่	คณะทำงาน

๑.๗ นายศราวุธ...

๑.๗ นายศราวุธ ธรรมชาติ	เจ้าพนักงานการเงินและบัญชี ชำนาญงาน กองคลัง	คณะทำงาน
๑.๘ นายปริมาณ อาภาอมร	พนักงานพิมพ์ ระดับ ส๓ กองคลัง	คณะทำงาน
๑.๙ นางสาวจุฬาลักษณ์ เก่งการช่าง	นักวิเคราะห์นโยบายและแผน ปฏิบัติการ กลุ่มพัฒนาระบบบริหาร	คณะทำงาน
๑.๑๐ นายพีรพัฒน์ เกิดศิริ	นักวิเคราะห์นโยบายและแผน กลุ่มพัฒนาระบบบริหาร	คณะทำงาน
๑.๑๑ นางสาวพิชชากร จิวเลิศสกุล	นักวิชาการตรวจสอบภายใน กลุ่มตรวจสอบภายใน	คณะทำงาน
๑.๑๒ นางสาวนิรชา คะหาญ	เจ้าพนักงานธุรการ กลุ่มตรวจสอบภายใน	คณะทำงาน
๑.๑๓ นายอธิชาติ สนธิรักษ์	เจ้าพนักงานเผยแพร่ประชาสัมพันธ์ สำนักงานเลขานุการกรม	คณะทำงาน
๑.๑๔ นายอาณัตชัย จันทร์ต่าย	เจ้าหน้าที่คอมพิวเตอร์ สำนักงานเลขานุการกรม	คณะทำงาน
๑.๑๕ นายปรัชญา ด่านกลาง	นักวิชาการคอมพิวเตอร์ชำนาญการ สำนักคณะกรรมการผู้ทรงคุณวุฒิ	คณะทำงาน
๑.๑๖ นางสาวจิราภรณ์ สุ่มตื๊บ	นักวิชาการคอมพิวเตอร์ ศูนย์ความร่วมมือระหว่างประเทศ	คณะทำงาน
๑.๑๗ นางสาวเปรมรัตนา วัชโรทัย	นักวิเทศสัมพันธ์ ศูนย์ความร่วมมือระหว่างประเทศ	คณะทำงาน
๑.๑๘ นายพิพัฒน์ นาคนิกร	นักวิชาการคอมพิวเตอร์ปฏิบัติการ สำนักส่งเสริมสุขภาพ	คณะทำงาน
๑.๑๙ นางสาวณัฏฐ์พัชร์ กุญแจทอง	นักวิชาการคอมพิวเตอร์ปฏิบัติการ สำนักส่งเสริมสุขภาพ	คณะทำงาน
๑.๒๐ นายพูลพฤกษ์ โสภารัตน์	ทันตแพทย์ชำนาญการพิเศษ สำนักทันตสาธารณสุข	คณะทำงาน
๑.๒๑ นายณภัทร พ่อบุตรดี	นักเทคโนโลยีสารสนเทศ สำนักทันตสาธารณสุข	คณะทำงาน
๑.๒๒ นางสาววริษา วงศ์วาณิชวัฒนา	นักวิชาการคอมพิวเตอร์ปฏิบัติการ สำนักโภชนาการ	คณะทำงาน
๑.๒๓ นายจักรพันธุ์ บุญชู	นักวิชาการคอมพิวเตอร์ปฏิบัติการ สำนักโภชนาการ	คณะทำงาน
๑.๒๔ นางสาวลดาวัลย์ จิตขาว	นักวิชาการคอมพิวเตอร์ปฏิบัติการ สำนักอนามัยการเจริญพันธุ์	คณะทำงาน

๑.๒๕ นางสาวอารีรัตน์...

๑.๒๕ นางสาวอารีรัตน์ จันทร์ลำภู	นักวิชาการคอมพิวเตอร์ปฏิบัติการ สำนักอนามัยการเจริญพันธุ์	คณะทำงาน
๑.๒๖ นายสันสนะ ณรงค์อินทร์	นักวิชาการคอมพิวเตอร์ปฏิบัติการ กองกิจกรรมทางกายเพื่อสุขภาพ	คณะทำงาน
๑.๒๗ นายทรงพล คำนึงเกียรติวงศ์	นักวิชาการสาธารณสุขชำนาญการ สำนักอนามัยผู้สูงอายุ	คณะทำงาน
๑.๒๘ ว่าที่ร้อยตรีกรวิชญ์ คล้ายเพ็ง	ผู้ดูแลระบบฐานข้อมูล สำนักอนามัยผู้สูงอายุ	คณะทำงาน
๑.๒๙ นางสาวประภาพรรณ ปะพุธสะโร	นักวิชาการคอมพิวเตอร์ปฏิบัติการ กองส่งเสริมความรอบรู้ และสื่อสารสุขภาพ	คณะทำงาน
๑.๓๐ นายณัฐวิทย์ ญาดี	นักวิชาการคอมพิวเตอร์ กองส่งเสริมความรอบรู้ และสื่อสารสุขภาพ	คณะทำงาน
๑.๓๑ นายวนนท์ บากี	นักวิชาการคอมพิวเตอร์ปฏิบัติการ สำนักอนามัยสิ่งแวดล้อม	คณะทำงาน
๑.๓๒ นางจันท์จิรา สวารักษ์	นักวิชาการคอมพิวเตอร์ปฏิบัติการ สำนักอนามัยสิ่งแวดล้อม	คณะทำงาน
๑.๓๓ นายสุเมธา บุญประเสริฐ	นักวิชาการคอมพิวเตอร์ปฏิบัติการ สำนักสุขาภิบาลอาหารและน้ำ	คณะทำงาน
๑.๓๔ นายประยูร ภักดีพัฒนาทร	นักวิเคราะห์นโยบายและแผน ปฏิบัติการ กองประเมินผลกระทบต่อสุขภาพ	คณะทำงาน
๑.๓๕ นายชาลี วุฒิสรรค์	พนักงานธุรการ ระดับ ส๓ กองห้องปฏิบัติการสาธารณสุขกรมอนามัย	คณะทำงาน
๑.๓๖ นายพงษวัฒน์ มูลเงิน	นักวิชาการคอมพิวเตอร์ กองห้องปฏิบัติการสาธารณสุขกรมอนามัย	คณะทำงาน
๑.๓๗ นายไอลวิล ชันธสนธิ์	นักวิชาการคอมพิวเตอร์ กองกฎหมาย	คณะทำงาน
๑.๓๘ นางชุติมา แก้วช่วย	นักวิชาการสาธารณสุขชำนาญการ กองอนามัยฉุกเฉิน	คณะทำงาน
๑.๓๙ นางสาวฐิติพร ผาสอน	นักวิชาการสาธารณสุขปฏิบัติการ กองอนามัยฉุกเฉิน	คณะทำงาน
๑.๔๐ นายสาธิต อยู่ศรี	นักวิชาการคอมพิวเตอร์ชำนาญการ ศูนย์อนามัยที่ ๑ เชียงใหม่	คณะทำงาน
๑.๔๑ นายปรัชญา ชมพล	นักวิชาการคอมพิวเตอร์ชำนาญการ ศูนย์อนามัยที่ ๑ เชียงใหม่	คณะทำงาน
๑.๔๒ นายเอกมล อ่อนทอง	นักวิชาการคอมพิวเตอร์ปฏิบัติการ ศูนย์อนามัยที่ ๒ พิษณุโลก	คณะทำงาน

๑.๔๓ นายอนุวัตน์...

๑.๔๓ นายอนุวัตน์ พัฒสงคราม	นักวิชาการคอมพิวเตอร์ปฏิบัติการ ศูนย์อนามัยที่ ๒ พิษณุโลก	คณะทำงาน
๑.๔๔ นายเอกลักษณ์ ชินคำ	นักวิชาการคอมพิวเตอร์ปฏิบัติการ ศูนย์อนามัยที่ ๓ นครสวรรค์	คณะทำงาน
๑.๔๕ นางสาวสายฝน สร้อยสด	นักวิชาการคอมพิวเตอร์ปฏิบัติการ ศูนย์อนามัยที่ ๓ นครสวรรค์	คณะทำงาน
๑.๔๖ นายอนุพงศ์ กันธิมา	นักวิชาการคอมพิวเตอร์ปฏิบัติการ ศูนย์อนามัยที่ ๔ สระบุรี	คณะทำงาน
๑.๔๗ นายเอกพจน์ ผดุงศักดิ์	เจ้าหน้าที่คอมพิวเตอร์ ศูนย์อนามัยที่ ๔ สระบุรี	คณะทำงาน
๑.๔๘ นายประดิภาส สุขเสาร์เกิด	นักวิชาการคอมพิวเตอร์ปฏิบัติการ ศูนย์อนามัยที่ ๕ ราชบุรี	คณะทำงาน
๑.๔๙ นายจิระเดช นงษ์รัก	นักวิชาการคอมพิวเตอร์ปฏิบัติการ ศูนย์อนามัยที่ ๕ ราชบุรี	คณะทำงาน
๑.๕๐ นายนิธิศ วีระธิติศ	นักวิชาการคอมพิวเตอร์ปฏิบัติการ ศูนย์อนามัยที่ ๖ ชลบุรี	คณะทำงาน
๑.๕๑ นายณัฐวุฒิ การุณเกียรติกุล	นักวิชาการคอมพิวเตอร์ปฏิบัติการ ศูนย์อนามัยที่ ๖ ชลบุรี	คณะทำงาน
๑.๕๒ นายจักรพันธ์ สุกใส	นักวิชาการคอมพิวเตอร์ปฏิบัติการ ศูนย์อนามัยที่ ๗ ขอนแก่น	คณะทำงาน
๑.๕๓ นายอลงกรณ์ สุกใส	เจ้าพนักงานคอมพิวเตอร์ ศูนย์อนามัยที่ ๗ ขอนแก่น	คณะทำงาน
๑.๕๔ นายสุทัศน์ บุราณ	นักวิชาการคอมพิวเตอร์ปฏิบัติการ ศูนย์อนามัยที่ ๘ อุดรธานี	คณะทำงาน
๑.๕๕ นางสาวรุ้งลาวัลย์ ตรงกะพงศ์	นักวิชาการคอมพิวเตอร์ปฏิบัติการ ศูนย์อนามัยที่ ๘ อุดรธานี	คณะทำงาน
๑.๕๖ นายเกรียงศักดิ์ แสนไชย	นักวิชาการคอมพิวเตอร์ปฏิบัติการ ศูนย์อนามัยที่ ๙ นครราชสีมา	คณะทำงาน
๑.๕๗ นายสันติพล พรมทิ	เจ้าพนักงานเครื่องคอมพิวเตอร์ ศูนย์อนามัยที่ ๙ นครราชสีมา	คณะทำงาน
๑.๕๘ นายวรวุฒิ สมดี	นักวิชาการคอมพิวเตอร์ปฏิบัติการ ศูนย์อนามัยที่ ๑๐ อุบลราชธานี	คณะทำงาน
๑.๕๙ นายเอกภพ ทะวาเงิน	นักวิชาการคอมพิวเตอร์ปฏิบัติการ ศูนย์อนามัยที่ ๑๐ อุบลราชธานี	คณะทำงาน
๑.๖๐ นายชยกร พิมพานนท์	นักจัดการงานทั่วไป ศูนย์อนามัยที่ ๑๐ อุบลราชธานี	คณะทำงาน
๑.๖๑ นางสาวลัลน์ณภัทร ดีดาษ	นักวิชาการคอมพิวเตอร์ปฏิบัติการ ศูนย์อนามัยที่ ๑๑ นครศรีธรรมราช	คณะทำงาน

๑.๖๒ นายสุทธินนท์...

๑.๖๒ นายสุทธินนท์ ศัลยคุปต์	นักวิชาการคอมพิวเตอร์ปฏิบัติการ ศูนย์อนามัยที่ ๑๑ นครศรีธรรมราช	คณะทำงาน
๑.๖๓ นายอิมรอน บินอาแว	นักวิชาการคอมพิวเตอร์ปฏิบัติการ ศูนย์อนามัยที่ ๑๒ ยะลา	คณะทำงาน
๑.๖๔ นายคอบอรี ตีมุง	นักวิชาการคอมพิวเตอร์ปฏิบัติการ ศูนย์อนามัยที่ ๑๒ ยะลา	คณะทำงาน
๑.๖๕ นายวิทยุทธ์ นิลรัตน์	นักวิชาการคอมพิวเตอร์ปฏิบัติการ สถาบันพัฒนาสุขภาวะเขตเมือง	คณะทำงาน
๑.๖๖ นายเทวพงศ์ วงค์เขื่อนแก้ว	นักวิชาการคอมพิวเตอร์ปฏิบัติการ สถาบันพัฒนาสุขภาวะเขตเมือง	คณะทำงาน
๑.๖๗ นายสุเมธ ศรีโสดา	นักวิชาการคอมพิวเตอร์ปฏิบัติการ ศูนย์อนามัยกลุ่มชาติพันธุ์ ชายขอบ และแรงงานข้ามชาติ	คณะทำงาน
๑.๖๘ นายสุรสีห์ ฉันทกุล	นักวิชาการคอมพิวเตอร์ปฏิบัติการ ศูนย์อนามัยกลุ่มชาติพันธุ์ ชายขอบ และแรงงานข้ามชาติ	คณะทำงาน
๑.๖๙ นายธวัชชัย สุธาชัย	นักวิชาการคอมพิวเตอร์ปฏิบัติการ ศูนย์ทันตสาธารณสุขระหว่างประเทศ	คณะทำงาน
๑.๗๐ นายพรสรรค์ ภู่ทอง	นักเทคโนโลยีสารสนเทศ ศูนย์ทันตสาธารณสุขระหว่างประเทศ	คณะทำงาน
๑.๗๑ นายสุชาญ กิจลือเลิศ	นักวิชาการคอมพิวเตอร์ปฏิบัติการ กองแผนงาน	คณะทำงาน และเลขานุการ
๑.๗๒ นางสาวมัณฑนา ควรพินิจ	นักวิชาการคอมพิวเตอร์ปฏิบัติการ กองแผนงาน	คณะทำงาน และผู้ช่วยเลขานุการ
๑.๗๓ นางสาวพันทวี แข่งขัน	นักวิเคราะห์นโยบายและแผน กองแผนงาน	คณะทำงาน และผู้ช่วยเลขานุการ

๒. อำนาจหน้าที่

๒.๑ กำกับ ดูแล เฝ้าระวัง ติดตาม วิเคราะห์ ประมวลผล แจ้งเตือน และปฏิบัติการป้องกัน รับมือ แก้ไข และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

๒.๒ เป็นศูนย์ประสานความร่วมมือ รวมทั้งส่งเสริม สนับสนุน และช่วยเหลือหน่วยงานสังกัดกรมอนามัย เพื่อรักษาความมั่นคงปลอดภัยทางไซเบอร์

๒.๓ ดำเนินการเฝ้าระวังตรวจสอบช่องโหว่ของระบบงานต่าง ๆ และเครือข่ายคอมพิวเตอร์ทั้งอินเทอร์เน็ตและอินทราเน็ต ของหน่วยงาน

๒.๔ ประสานงานกับกองแผนงาน ทันทีเมื่อพบเหตุการณ์ทางไซเบอร์ ผ่าน Line Group: AnamaiCIRT เพื่อระงับเหตุ ป้องกัน ติดตามแก้ไขปัญหา กู้คืนระบบงานและรายงานผู้บริหารเทคโนโลยีสารสนเทศระดับสูง กรมอนามัย

๒.๕ ติดตาม...

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

(นายคำรง ธำรงเลาหะพันธุ์)
ผู้อำนวยการสำนักทันตสาธารณสุข
ปฏิบัติราชการแทนอธิบดีกรมอนามัย

ตรวจ.....
พิมพ์.....
ร่าง.....

เอกสารแนบท้ายประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์เรื่อง
หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ. ๒๕๖๘
ว่าด้วยข้อมูลที่ต้องแจ้งและแบบการรายงานภัยคุกคามทางไซเบอร์

บทนำ

ตามที่พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ได้กำหนดลักษณะของภัยคุกคามทางไซเบอร์ โดยแบ่งออกเป็น ๓ ระดับ ได้แก่ ภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรงภัยคุกคามทางไซเบอร์ในระดับร้ายแรง และภัยคุกคามทางไซเบอร์ในระดับวิกฤติ และให้หน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศแจ้งในกรณีที่เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ต่อระบบสารสนเทศซึ่งอยู่ในความดูแลรับผิดชอบของหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำรายงานเมื่อมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญต่อระบบของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ นั้น

เพื่อให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ มีแนวทางปฏิบัติที่ชัดเจนในการรายงานการดำเนินมาตรการตามที่กำหนดในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติว่าด้วยลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ จึงกำหนดให้หน่วยงานดังกล่าวจัดทำรายงานเหตุภัยคุกคามทางไซเบอร์ที่เกิดขึ้นอย่างมีนัยสำคัญต่อระบบของหน่วยงานตามรายการที่กำหนดไว้ในแนบท้ายนี้ ผ่านการส่งทางอีเมล โทรสารหรือด้วยวิธีการทางอิเล็กทรอนิกส์อื่นใดที่มีความปลอดภัย เช่น การส่งรายงานที่เข้ารหัสด้วย PGP มาทางอีเมล (เป็นอย่างน้อย)

เนื่องด้วยการส่งรายงานของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้ทันการณ์เป็นเรื่องที่สำคัญ[๑,๒] ในกรณีหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศยังไม่สามารถแจ้งข้อมูลตามแบบรายงานได้อย่างครบถ้วนภายในระยะเวลา ๒๔ ชั่วโมง ให้หน่วยงานดังกล่าวจัดส่งรายงานด้วยข้อมูลเท่าที่มีและเมื่อมีความคืบหน้าหรือมีข้อมูลเพิ่มเติมในการดำเนินการรับมือ ให้แจ้งต่อสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเป็นระยะ และรีบจัดทำและส่งรายงานที่สมบูรณ์ให้แก่สำนักงานโดยเร็ว ทั้งนี้ ให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศพิจารณาส่งข้อมูลสำคัญที่จำเป็นต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ และสอดคล้องกับนโยบายการรักษาความลับของหน่วยงาน

ในกรณีที่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศไม่สามารถดำเนินการจัดเตรียมข้อมูลในรายงานได้ด้วยเหตุผลบางประการ ให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศแจ้งหน่วยงานควบคุมหรือกำกับดูแลของตนและสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติให้ทราบโดยเร็ว

ทั้งนี้ เพื่อให้หน่วยงานของรัฐ มีแนวทางปฏิบัติที่ชัดเจนในการรายงานเหตุภัยคุกคามทางไซเบอร์ กรณีมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญต่อระบบสารสนเทศของหน่วยงานของรัฐ จึงให้นำหลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศดังกล่าวข้างต้น มาบังคับใช้แก่หน่วยงานของรัฐโดยอนุโลม

---

[๑] การรายงานภัยคุกคามทางไซเบอร์ที่เกิดขึ้นอย่างมีนัยสำคัญต้องรายงานภายในระยะเวลาที่หน่วยงานควบคุมหรือกำกับดูแลกำหนด (โดยหน่วยงานควบคุมหรือกำกับดูแลอาจกำหนดให้นำข้อปฏิบัติตามแผนการกู้คืนของหน่วยงานมาประกอบการพิจารณาด้วยก็ได้) หรืออาจเทียบเคียงจากตัวอย่างตามที่ระบุในข้อ ๓ ของภาคผนวกแนบท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔

[๒] มาตรา ๗๓ กำหนดให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่ไม่รายงานเหตุภัยคุกคามทางไซเบอร์ โดยไม่มีเหตุอันสมควร ต้องระวางโทษปรับไม่เกิน ๒๐๐,๐๐๐ บาท

เอกสาร ก๑ ข้อมูลที่ต้องแจ้ง

ข้อมูลการประสานงานและผลการตรวจสอบภัยคุกคามเบื้องต้น

๑. ข้อมูลการประสานงาน

ชื่อหน่วยงานที่รับผิดชอบติดตามเหตุภัยคุกคาม

วันที่และเวลาที่แจ้ง

๒. ด้านภารกิจหรือบริการของหน่วยงาน และ ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม

ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม

ที่อยู่ของหน่วยงานหรือหน่วยงานย่อยที่เกิดเหตุภัยคุกคาม

๓. ข้อมูลการติดต่อสำหรับการประสานงานเหตุภัยคุกคาม

ชื่อ-นามสกุล ตำแหน่งงาน

ชื่อหน่วยงาน อีเมล

โทรศัพท์ (ที่ทำงาน / มือถือ)

๔. ความต่อเนื่องของเหตุภัยคุกคาม

☐ เหตุภัยคุกคามใหม่ ☐ การรายงานข้อมูลต่อเนื่องจากเหตุภัยคุกคามเดิม

๕. ลักษณะภัยคุกคามทางไซเบอร์

ระบบที่ได้รับผลกระทบมีความสำคัญต่อพันธกิจหลักของหน่วยงานหรือไม่

เหตุการณ์ที่เกิดขึ้นเกิดจากภัยคุกคามทางไซเบอร์[๓] ในระดับใด (มาตรา ๖๐)

☐ ไม่ร้ายแรง ☐ ร้ายแรง ☐ วิกฤต (ก) ☐ วิกฤต (ข)

☐ ยังไม่สามารถระบุได้

๖. หมวดหมู่ของภัยคุกคาม (แจ้งได้มากกว่า ๑ รายการ)

หมวดหมู่*	คำอธิบาย
หมวดหมู่ที่ ๒	การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance)
หมวดหมู่ที่ ๓	การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยของหน่วยงาน (Non-Compliance Activity)
หมวดหมู่ที่ ๔	การบุกรุกโดยการใช้มัลแวร์ (Malicious Logic)
หมวดหมู่ที่ ๕	การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion)
หมวดหมู่ที่ ๖	การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion)
หมวดหมู่ที่ ๗	การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)
หมวดหมู่ที่ ๘	เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating)

* อ้างอิงหมวดหมู่ตามภาคผนวกท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ (ทั้งนี้ภัยคุกคามทางไซเบอร์หมวดหมู่ที่ ๐ หมวดหมู่ที่ ๑ และหมวดหมู่ที่ ๙ ไม่เข้าข่ายเป็นภัยคุกคามทางไซเบอร์ที่ต้องรายงาน)

[๓] พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดความหมายของ “ภัยคุกคามทางไซเบอร์” ดังนี้ การกระทำหรือการดำเนินการใด ๆ โดยมิชอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

เอกสาร ก๒ แบบรายงานภัยคุกคามทางไซเบอร์

ส่วนที่ ๑

หมวด ก. ข้อมูลการประสานงานและผลการตรวจสอบภัยคุกคามเบื้องต้น

หมายเลขอ้างอิง (สำหรับเจ้าหน้าที่ สกมช.): โปรดระบุ
หน่วยงานที่รับผิดชอบติดตามเหตุภัยคุกคาม (ถ้ามี): โปรดระบุ
วันที่: เลือกวันที่ **เวลา:** โปรดระบุ

ก๑. ด้านภารกิจหรือบริการของหน่วยงาน และ ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม

ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม: โปรดระบุ
ที่อยู่ของหน่วยงานหรือหน่วยงานย่อยที่เกิดเหตุภัยคุกคาม: โปรดระบุ

ก๒. ข้อมูลการติดต่อสำหรับการประสานงานเหตุภัยคุกคาม

ชื่อ-นามสกุล: โปรดระบุ ตำแหน่งงาน: โปรดระบุ
ชื่อหน่วยงาน: โปรดระบุ อีเมล: โปรดระบุ
โทรศัพท์ (ที่ทำงาน / มือถือ): โปรดระบุ

ก๓. ความต่อเนื่องของเหตุภัยคุกคาม

☐ เหตุภัยคุกคามใหม่ ☐ การรายงานข้อมูลต่อเนื่องจากเหตุภัยคุกคามเดิม

ก๔. ลักษณะภัยคุกคามทางไซเบอร์

ระบบที่ได้รับผลกระทบมีความสำคัญต่อพันธกิจหลักของหน่วยงาน
☐ ใช่ ☐ ไม่ใช่
เหตุการณ์ที่เกิดขึ้นเกิดจากภัยคุกคามทางไซเบอร์[๕] ในระดับใด (มาตรา ๖๐)
☐ ไม่ร้ายแรง ☐ ร้ายแรง ☐ วิกฤต (ก) ☐ วิกฤต (ข)
☐ ยังไม่สามารถระบุได้

[๕] พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดความหมายของ “ภัยคุกคามทางไซเบอร์” ดังนี้ การกระทำหรือการดำเนินการใด ๆ โดยมิชอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

หมวด ข. ข้อมูลการตรวจพบภัยคุกคามไซเบอร์

ข๑. วัน เวลา ที่เกิดเหตุภัยคุกคาม

วันที่ : เลือกวันที่ เวลา : โปรดระบุ

วัน เวลา ที่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศทราบเหตุภัยคุกคาม

วันที่ : เลือกวันที่ เวลา : โปรดระบุ

ข๒. วัน เวลา ที่แจ้งเหตุภัยคุกคามให้หน่วยงานควบคุมหรือกำกับดูแลทราบ

☐ ยังไม่ได้แจ้ง ☐ แจ้งแล้ว _____

ข๓. หมวดหมู่ของภัยคุกคาม (เลือกได้มากกว่า ๑ รายการ)

หมวดหมู่*	คำอธิบาย
☐ หมวดหมู่ที่ ๒	การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance)
☐ หมวดหมู่ที่ ๓	การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยของหน่วยงาน (Non-Compliance Activity)
☐ หมวดหมู่ที่ ๔	การบุกรุกโดยการใช้มัลแวร์ (Malicious Logic)
☐ หมวดหมู่ที่ ๕	การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion)
☐ หมวดหมู่ที่ ๖	การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion)
☐ หมวดหมู่ที่ ๗	การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)
☐ หมวดหมู่ที่ ๘	เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating)
☐ อื่น ๆ	โปรดระบุ

* อ้างอิงหมวดหมู่ตามภาคผนวกท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ (ทั้งนี้ภัยคุกคามหมวดหมู่ที่ ๐ ๑ และ ๙ ไม่เข้าข่ายเป็นภัยคุกคามที่ต้องรายงาน)

ข๔. ข้อมูลเบื้องต้นเกี่ยวกับระบบคอมพิวเตอร์ คอมพิวเตอร์ บริการ หรือข้อมูลที่ได้รับผลกระทบ:

สถานที่ตั้งของเครื่อง ข้อมูล หรือสินทรัพย์ที่ได้รับผลกระทบ (เช่น จังหวัด ตำบล ตึก ห้อง):

โปรดระบุ

ชื่อผู้ให้บริการเครือข่ายที่ให้บริการแก่ระบบ บริการ หรือข้อมูลที่ได้รับผลกระทบ :

โปรดระบุ

บริการของระบบ ข้อมูล หรือสินทรัพย์ที่ได้รับผลกระทบ (เช่น บริการการโอนเงิน):

โปรดระบุ

ฮาร์ดแวร์ ซอฟต์แวร์ที่ได้รับผลกระทบ (โปรดระบุรายละเอียด เช่น ผู้ผลิตหรือยี่ห้อ รุ่นของเครื่องคอมพิวเตอร์): โปรดระบุรายละเอียด

มีผลกระทบต่อการสื่อสาร (ทางโทรศัพท์ หรือ การใช้งานเครือข่าย): โปรดระบุ

รายละเอียดอื่น ๆ: โปรดระบุ

หมวด ค: ข้อมูลการรับมือภัยคุกคาม

ค๑. สถานการณ์หรือการแก้ไขเหตุภัยคุกคาม (เลือกได้มากกว่า ๑ รายการ)

- ☐ เพิ่งพบเหตุการณ์
- ☐ อยู่ในขั้นตอนการขอความช่วยเหลือ
- ☐ อยู่ในขั้นตอนการสอบสวน
- ☐ กำลังลุกลาม
- ☐ อยู่ในขั้นตอนการระงับภัย
- ☐ สามารถระงับภัยได้แล้ว
- ☐ รายงานปิดเหตุการณ์ภัยคุกคามแล้ว
- ☐ อื่น ๆ: โปรดระบุ

ค๒. สิ่งที่ได้ดำเนินการหรือได้แก้ไขไปแล้ว

- ☐ ยังไม่ได้ดำเนินการแก้ไขใด ๆ
- ☐ ยกเลิกการเชื่อมต่อระบบออกจากเครือข่ายแล้ว
- ☐ ตรวจสอบข้อมูลจราจร (Log) แล้ว
- ☐ ตรวจสอบโปรแกรม (แฟ้ม binaries/.exe) แล้ว
- ☐ กู้คืนกลับมาด้วยระบบหรือข้อมูลสำรองที่ตรวจสอบความถูกต้องแล้ว
- ☐ รายละเอียดการแก้ไขภัยคุกคามที่เกิดขึ้นเพิ่มเติม: โปรดระบุ

ค๓. รายละเอียดการรับมือภัยคุกคามอื่น ๆ (ถ้ามี)

โปรดระบุ

ส่วนที่ ๒

หมวด ง : รายละเอียดภัยคุกคาม

ง๑. ข้อมูลการตรวจจับและการวิเคราะห์

ง๑.๑ <u>วัน เวลา ที่ผู้โจมตีได้เริ่มต้นเข้าถึงระบบ</u> (System Access)

วันที่: เลือกวันที่ เวลา: โปรดระบุ ไม่ทราบ: ☐

ง๑.๒ ข้อมูลการพบเห็นเหตุภัยคุกคามทางไซเบอร์

รายละเอียดแหล่งที่มา หรือต้นเหตุของเหตุภัยคุกคาม (เท่าที่ทราบ เช่น คน, ความผิดพลาดของระบบ, ภัยธรรมชาติ, การจู่โจม, ความผิดพลาดจากคนนอกองค์กร):

โปรดระบุ

บุคคล วิธี หรือเครื่องมือที่ตรวจพบภัยคุกคาม (เช่น ผู้ใช้, ผู้ดูแลระบบ, โปรแกรม Anti-virus, IDS, การวิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์, ไม่ทราบ):

โปรดระบุ

รายละเอียดของปัญหาลักษณะคล้ายกันที่หน่วยงานเคยพบมาก่อน (ถ้ามี โปรดระบุรายละเอียด):

โปรดระบุ

ง๑.๓ รายละเอียดผลกระทบจากเหตุภัยคุกคาม (ระบุผลกระทบที่มีเกิดขึ้นต่อ ระบบ คน หรือข้อมูล)

จำนวนระบบ บริการ หรือสินทรัพย์ที่เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่ได้รับผลกระทบ (โดยประมาณ): โปรดระบุ

ทรัพย์สินที่สำคัญอื่น ๆ ที่อาจได้รับผลกระทบ: โปรดระบุ

จำนวนผู้ได้รับผลกระทบ (โดยประมาณ): โปรดระบุ

มูลค่าความเสียหาย (โดยประมาณ): โปรดระบุ

ในกรณีที่ข้อมูลที่ระบุตัวบุคคลได้รั่วไหล (หรือถูกขโมย):

จำนวนบุคคลที่เป็นเจ้าของข้อมูล : โปรดระบุ

ชนิดของข้อมูล (เลือกทุกข้อที่ใช่):

☐ ข้อมูลไบโอเมตริกซ์ ☐ ข้อมูลการติดต่อ

☐ ข้อมูลการเงิน ☐ ข้อมูลบุคลากรของรัฐ

☐ หมายเลขบัตรประชาชน ☐ ข้อมูลการติดต่อกับหน่วยงานต่าง ๆ

☐ ข้อมูลทางการแพทย์

☐ อื่น ๆ : โปรดระบุ

จำนวนข้อมูล (Record) ที่ได้รับผลกระทบ: โปรดระบุ

ผลกระทบอื่น ๆ ที่เกิดขึ้น: โปรดระบุ

๑.๔ <u>รายละเอียดของระบบ หรือข้อมูลที่ได้รับผลกระทบ (Information of Affected System)</u>

หมายเลข CVE: โปรดระบุ

ช่องโหว่ที่ถูกใช้จู่โจม: โปรดระบุ

การใช้ระบบหรือเครื่องที่ได้รับผลกระทบเป็นฐานเพื่อจู่โจมขยายผลไปยังระบบหรือเครื่องอื่น:
โปรดระบุ

อาการหรือสิ่งผิดปกติ (เลือกได้มากกว่า ๑ รายการ)

☐ ระบบล่ม
☐ รายการข้อมูลจราจรทางคอมพิวเตอร์ที่ผิดปกติ
☐ บัญชีผู้ใช้ถูกสร้างขึ้นมาใหม่โดยไม่ทราบสาเหตุ หรือ บัญชีผู้ใช้มีความผิดปกติ
☐ การจู่โจมด้วยวิศวกรรมสังคม (Social Engineering) ทั้งที่สำเร็จและไม่สำเร็จ
☐ ประสิทธิภาพของระบบด้อยลง (ทั้งที่รู้ว่าเป็นเพราะเหตุภัยคุกคามและที่ไม่รู้สาเหตุ)
☐ การเปลี่ยนแปลงใน DNS หรือ กฎของ Router หรือกฎไฟร์วอลล์ โดยไม่ทราบสาเหตุ
☐ การยกระดับสิทธิ์การเข้าถึงระบบโดยไม่ทราบสาเหตุ
☐ การตรวจพบการทำงานของโปรแกรมหรืออุปกรณ์ Sniffer เพื่อจับการรับส่งข้อมูลภายในเครือข่าย
☐ การเข้าใช้งานครั้งสุดท้ายของผู้ใช้ที่ไม่สอดคล้องกับการใช้งานครั้งสุดท้ายที่เกิดขึ้นจริง
☐ การแจ้งเตือนจากเครื่องมือตรวจจับการบุกรุก
☐ การเข้ามาลาดตระเวน (Probing) หรือการเรียกดู (Browsing) ที่น่าสงสัย
☐ รูปแบบการใช้งานที่ผิดปกติ
☐ การเปลี่ยนแปลงขนาดไฟล์ไปจากเดิมแบบผิดปกติ
☐ ความพยายามที่จะเขียนไฟล์ของระบบ
☐ การเปลี่ยนแปลงวันที่ของไฟล์ไปจากเดิมแบบผิดปกติ
☐ การแก้ไขหรือลบข้อมูลที่ผิดปกติ
☐ การจู่โจมให้เกิดการปฏิเสธการให้บริการ (DOS, DDOS)
☐ ไฟล์ใหม่ถูกสร้างขึ้นโดยไม่ทราบสาเหตุ
☐ การใช้งานหรือมีกิจกรรมที่เกิดในเวลาที่ผิดปกติ
☐ การแก้ไขหน้าเว็บ
☐ การสร้างแฟ้มข้อมูล setuid หรือ setgid ใหม่ที่ผิดปกติเกิดขึ้น
☐ การเปลี่ยนแปลงในไดเรกทอรีและแฟ้มข้อมูลของระบบปฏิบัติการที่ผิดปกติ
☐ การตรวจพบโปรแกรมเจาะระบบ (Crack utility)
☐ สิ่งที่ผิดปกติไปจากเดิมอื่น ๆ: โปรดระบุ

๑.๕ รายละเอียดของเหตุภัยคุกคามตามลำดับเวลา ตั้งแต่การจู่โจมครั้งแรก จนถึงปัจจุบัน (เช่น ลำดับของการจู่โจม, Attack vector, เทคนิคหรือเครื่องมือที่ผู้จู่โจมใช้ ฯลฯ)

โปรดระบุ

๑.๖ รายละเอียดอื่น ๆ ที่พบเกี่ยวข้องกับเหตุภัยคุกคาม: โปรดระบุ

๒. ข้อมูลการระงับ ปราบปราม และฟื้นฟู

๒.๑ รายละเอียดการดำเนินการเพื่อแก้ไขเหตุภัยคุกคาม: โปรดระบุ

๒.๒ การคาดการณ์ความสามารถฟื้นฟู

โปรดระบุรายละเอียดการฟื้นฟู ทรัพยากรที่ต้องใช้และที่ต้องการเพิ่ม และประมาณระยะเวลาการฟื้นฟู

๓. ข้อมูลกิจกรรมภายหลังการแก้ปัญหา (ถ้ามี)

๓.๑ วัน เวลา ที่เหตุภัยคุกคามสิ้นสุด วันที่: เลือกวันที่ เวลา: โปรดระบุ

๓.๒ การดำเนินการเพื่อป้องกันเหตุภัยคุกคามที่คล้ายคลึงกัน: โปรดระบุ

๓.๓ บทเรียนที่ได้จากเหตุภัยคุกคาม: โปรดระบุ