2568

# (CYBERSECURITY INCIDENT RESPONSE PLAN)

จัดทำโดย....ฝ่ายสารสนเทศ องค์การตลาด
กระทรวงมหาดไทย

# สารบัญ

# แผนการรับมือเหตุภัยคุกคามทางไซเบอร์(Cybersecurity Incident Response Plan)

## ๑. หลักการและเหตุผล

แผนรับมือเหตุภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan) ขององค์การตลาด ฉบับนี้ จัดทำขึ้นเพื่อให้เป็นไปตามมาตรา ๔๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ที่กำหนดให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งประมวลแนวทางปฏิบัติดังกล่าว กำหนดให้อย่างน้อยต้องมีการจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan : CIRP)

องค์การตลาดเป็นหน่วยงานของรัฐ ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ จึงได้จัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ขึ้น เพื่อใช้เป็นแนวทางในการเตรียมความพร้อมรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์ โดยแผนการรับมือฯ ครอบคลุมตั้งแต่การกำหนดโครงสร้างอำนาจหน้าที่ของทีมรับมือเหตุการณ์ (Cyber Incident Response Team: CIRT) การกำหนดประเภทของเหตุภัยคุกคามทางไซเบอร์ การกำหนดความสัมพันธ์กับนโยบายและแนวปฏิบัติที่เกี่ยวข้อง การรายงานเหตุภัยคุกคามทางไซเบอร์ และขั้นตอนการรับมือเหตุภัยคุกคามทางไซเบอร์ รวมไปถึงการสื่อสารไปยังผู้มีส่วนได้ส่วนเสีย เพื่อลดผลกระทบที่อาจเกิดขึ้นต่อการดำเนินงานขององค์การตลาด

## ๒. วัตถุประสงค์

เพื่อให้มีแผนการรับมือภัยคุกคามทางไซเบอร์ ที่ใช้เป็นแนวทางในการเตรียมความพร้อมรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์ สอดคล้องกับประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

## ๓. ขอบเขต

แผนรับมือภัยคุกคามทางไซเบอร์ฉบับนี้ ใช้รับมือเหตุภัยคุกคามทางไซเบอร์ที่เกิดขึ้นต่อระบบสารสนเทศและข้อมูลด้านดิจิทัล รวมถึงบุคคลหรืออุปกรณ์ใดๆ ซึ่งเข้าถึงระบบสารสนเทศ และข้อมูลดิจิทัล

## ๔. หน้าที่การทบทวนแผน

ฝ่ายสารสนเทศ มีหน้าที่ทบทวนและขออนุมัติแผนรับมือภัยคุกคามทางไซเบอร์ฉบับนี้ถึงผู้อำนวยการองค์การตลาด

**๕. หน้าที่ในการดำเนินการตามแผน**

ผู้บริหารความมั่นคงปลอดภัยสารสนเทศ/ไซเบอร์ (Chief Information Security Officer: CISO) ฝ่ายสารสนทศ ผู้ที่ได้รับมอบหมายและผู้ที่เกี่ยวข้อง มีหน้าที่เป็นผู้รับผิดชอบหลักในการดำเนินการตามแผนรับมือเหตุภัยคุกคามทางไซเบอร์ฉบับนี้

**๖. ความเกี่ยวข้องกับเอกสารอื่น**

๖.๑ แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขององค์การตลาด

๖.๒ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

๖.๓ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

**๗. นิยาม**

**ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (DCIO)** หมายถึง ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer) เป็นตำแหน่งที่มีอำนาจหน้าที่ดูแลรับผิดชอบด้านเทคโนโลยีสารสนเทศและดิจิทัลในองค์กร ซึ่งหมายรวมถึงการดูแลเกี่ยวกับมาตรฐาน กฎเกณฑ์ โครงสร้าง งบประมาณ กระบวนการให้ความรู้ บุคลากรของหน่วยงานสารสนเทศ โดย DCIO เป็นผู้ให้คำแนะนำแก่ผู้บริหารสูงสุดขององค์กร (Chief Executive Officer: CEO) เกี่ยวกับการพัฒนาและนำเทคโนโลยีสารสนเทศและดิจิทัลมาใช้ให้การบริหารองค์กรให้ประสบความสำเร็จตามวิสัยทัศน์ และเป้าหมายรวมของหน่วยงานที่กำหนดไว้

**ผู้บริหารความมั่นคงปลอดภัยสารสนเทศ/ไซเบอร์ (CISO)** หมายถึง ผู้บริหารความมั่นคงปลอดภัยสารสนเทศ (Chief Information Security Officer) เป็นตำแหน่งผู้บริหารระดับสูงทางด้านการรักษาความปลอดภัยให้กับโครงสร้าง เครือข่ายและความปลอดภัยของข้อมูลสารสนเทศ เป็นผู้ที่เข้าใจในระบบธุรกิจขององค์กรและการจัดการกับความเสี่ยงที่มีโอกาสเกิดขึ้น เพื่อไม่ให้ปัญหาด้านความความปลอดภัยดังกล่าวส่งผลกระทบกับธุรกิจขององค์กรทั้งทางตรงและทางอ้อม รวมถึงสามารถกำหนดเป้าหมาย นโยบายด้านการรักษาความมั่นคงปลอดภัยที่สอดคล้องกับแผนยุทธศาสตร์ขององค์กร พัฒนานโยบายด้านการรักษาความปลอดภัยของข้อมูล มาตรฐาน ขั้นตอนและแนวปฏิบัติเพื่อให้องค์กรได้มาซึ่งการรักษาความลับของข้อมูล (Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity) และเสถียรภาพความมั่นคงของระบบ (Availability)

**เหตุการณ์ (Event)** หมายถึง การเกิดขึ้นที่สังเกตได้ (Observable Occurrence) ในระบบเครือข่าย สภาพแวดล้อม กระบวนการลำดับการดำเนินการ หรือบุคลากร เหตุการณ์อาจมีหรือไม่มีลักษณะที่ส่งผลเชิงลบก็ได้

**เหตุภัยคุกคามทางไซเบอร์ (Cyber incident)** หมายถึง เหตุการณ์ที่มีผลเชิงลบที่เกิดจากการกระทำหรือการดำเนินการใด ๆ โดยมิชอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์ โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องและเป็นอันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ระบบคอมพิวเตอร์หรือข้อมูลอื่นที่เกี่ยวข้อง

**ภัยคุกคามทางไซเบอร์ (Cyber threat)** หมายถึง การกระทำหรือการดำเนินการใดๆ โดยมิชอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

**เหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญ** หมายถึง เหตุภัยคุกคามทางไซเบอร์ที่ปรากฏต่อระบบสารสนเทศ และเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามมาตรา ๔๙ ซึ่งคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติได้กำหนดลักษณะของภัยคุกคามทางไซเบอร์ไว้ตามมาตรา ๖๐ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

**แพตช์** หมายถึง โปรแกรมที่ใช้ในการปรับปรุงแก้ไขซอฟต์แวร์ โดยส่วนใหญ่จะอยู่ในลักษณะของไฟล์และใช้เพื่อแก้ไขช่องโหว่เรื่องความมั่นคงปลอดภัย หรือเพื่อเพิ่มความสามารถของซอฟต์แวร์ ผู้พัฒนาซอฟต์แวร์เผยแพร่แพตช์ออกมาเป็นระยะ เช่น บริษัท Microsoft จะเผยแพร่แพตช์ที่แก้ไขช่องโหว่ของซอฟต์แวร์ผ่านระบบ Windows Update

- **Recovery Time Objective (RTO)** หมายถึง ระยะเวลาในการกู้คืนระบบ

- **Recovery Point Objective (RPO)** หมายถึง ระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย

- **Maximum Tolerance Period of Disruption (MTPD)** หมายถึง ระยะเวลาสูงสุดที่ยอมให้ธุรกิจหยุดชะงัก เพื่อรองรับการดำเนินธุรกิจอย่างต่อเนื่องของหน่วยงานของรัฐ และหน่วยงาน โครงสร้างพื้นฐานสำคัญทางสารสนเทศและรองรับการเกิดเหตุการณ์ผิดปกติต่าง ๆ ที่อาจส่งผลให้เกิดการหยุดชะงักหรือเกิดความเสียหายต่อระบบ เช่น ภัยคุกคามการท างานได้ตามปกติให้เร็วที่สุด

**รูปแบบภัยคุกคามไซเบอร์** หมายถึง รูปแบบของการกระทำหรือการดำเนินการใด ๆ โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลของบุคคลหรือหน่วยงาน แบ่งเป็น

- **ซอฟต์แวร์ประสงค์ร้าย (Malicious Software)** หรือที่เรียกโดยทั่วไปว่ามัลแวร์ (Malware) เป็นโปรแกรมที่มีการทำงานที่มุ่งประสงค์ร้ายต่อคอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์

- **ไวรัสคอมพิวเตอร์ (Computer Virus)** เป็นมัลแวร์ชนิดหนึ่งที่สามารถคัดลอกตัวเอง ติดตั้งตัวเองในเครื่องคอมพิวเตอร์อื่นๆ โดยที่เจ้าของเครื่องคอมพิวเตอร์ไม่อนุญาต ไวรัส คอมพิวเตอร์สามารถแพร่กระจายตัวเองไปสู่เครื่องคอมพิวเตอร์เครื่องอื่นๆ โดยใช้พาหะ เช่น แฟลชไดรว์ติดไวรัส หรือไฟล์คอมพิวเตอร์ติดไวรัส เป็นต้น

- **หนอนคอมพิวเตอร์ (Computer worm)** เป็นมัลแวร์ชนิดหนึ่งที่สามารถคัดลอกตัวเอง ติดตั้งตัวเองในเครื่องคอมพิวเตอร์อื่น ๆ โดยที่เจ้าของเครื่องคอมพิวเตอร์ไม่อนุญาต หนอนคอมพิวเตอร์จะต่างกับไวรัสตรงที่ไวรัสจะแพร่กระจายตัวเองไปสู่คอมพิวเตอร์เครื่องอื่น ๆ โดยอาศัยพาหะ แต่หนอนคอมพิวเตอร์จะใช้วิธีสแกนเครื่องคอมพิวเตอร์ที่อยู่ในระบบเครือข่าย และตรวจหาช่องโหว่ของระบบปฏิบัติการหรือช่องโหว่ของแอปพลิเคชันจากนั้นจึงทำการคัดลอกตัวเองเข้าไปฝังโดยใช้ช่องโหว่ดังกล่าว

- **ม้าโทรจัน (Trojan horse)** เป็นมัลแวร์ชนิดหนึ่งที่มีจุดประสงค์เพื่อบุกรุก เข้าถึงและควบคุม เครื่องคอมพิวเตอร์จากระยะไกล ดำเนินการเปลี่ยนแปลง ทำลายไฟล์ข้อมูลสำคัญ หรือทำการคัดลอกข้อมูลดังกล่าวส่งให้แก่ผู้คุกคามผ่านระบบเครือข่ายอินเทอร์เน็ต ซึ่งข้อมูลสำคัญที่ผู้คุกคามต้องการอาจเป็น ชื่อผู้ใช้ รหัสผ่าน เลขที่บัญชีธนาคาร และข้อมูลส่วนบุคคลอื่น ๆลักษณะของการติดตั้งม้าโทรจันจะเหมือนกับไวรัสคอมพิวเตอร์คืออาศัยพาหะซึ่งอาจมาจากแฟลชไดร์หรือทางอีเมล์

- **สปายแวร์ (Spyware)** เป็นมัลแวร์ชนิดหนึ่งที่มีวัตถุประสงค์เพื่อบันทึกการกระทำของผู้ใช้บนเครื่องคอมพิวเตอร์และส่งผ่านอินเทอร์เน็ตโดยที่ผู้ใช้ไม่ได้รับทราบ โปรแกรมแอบดักข้อมูลนั้นสามารถรวบรวมข้อมูลสถิติการใช้งานจากผู้ใช้ได้หลายอย่างขึ้นอยู่กับการออกแบบของโปรแกรม

- **ซอฟต์แวร์เรียกค่าไถ่ (Ransomware)** เป็นมัลแวร์ชนิดหนึ่งที่มีพฤติกรรมเข้ารหัสไฟล์ต่าง ๆ ที่อยู่บนเครื่องคอมพิวเตอร์ไม่ว่าจะเป็นไฟล์เอกสาร รูปภาพ วิดีโอ ผู้ใช้งานจะไม่สามารถเปิดไฟล์ใดๆ ได้เลยหากไฟล์เหล่านั้นถูกเข้ารหัส ซึ่งการถูกเข้ารหัสก็หมายความว่าจะต้องใช้คีย์ในการปลอดล็อคเพื่อกู้ข้อมูลคืนมาโดยผู้ใช้งานจะต้องทำการจ่ายเงินตามข้อความ “เรียกค่าไถ่”

- **Backdoor** เป็นช่องทางพิเศษที่ใช้เข้าถึงระบบหรือเครื่องคอมพิวเตอร์โดยที่ไม่ต้องผ่านการพิสูจน์ตัวตน ซึ่งส่วนใหญ่เมื่อผู้บุกรุกสามารถเจาะเข้าระบบได้แล้ว ก็จะสร้างประตูหลังเอาไว้เพื่อใช้ในการบุกรุกเข้าสู่ระบบหรือเครื่องคอมพิวเตอร์ในภายหลัง

- **Rootkit** เป็นโปรแกรมที่ถูกพัฒนาขึ้นมาเพื่อควบคุมระบบหรือขโมยข้อมูลที่อยู่ในระบบคอมพิวเตอร์ ทั้งนี้ นอกจากใช้สำหรับบุกรุกเข้าสู่ระบบงานแล้ว Rootkit ยังอาจใช้เพื่อดูแลหรือตรวจสอบระบบคอมพิวเตอร์ได้ด้วย

- **การโจมตีแบบ DoS/DDoS** มีจุดประสงค์เพื่อทำให้เครื่องคอมพิวเตอร์แม่ข่าย (Server) หยุดทำงาน หากเครื่องคอมพิวเตอร์ที่โจมตีมีเครื่องเดียว เรียกว่าการโจมตีแบบ Denial of Service (DoS) แต่หากมีเครื่องคอมพิวเตอร์ที่โจมตีมากกว่า 1 เครื่องและทำการโจมตีพร้อมๆกัน ไม่ว่าจะโดยตั้งใจหรือไม่ตั้งใจก็ตาม จะเรียกว่าการโจมตีแบบ Distributed Denial of Service (DDoS)

- **Botnet** เป็นกลุ่มของอุปกรณ์ที่ติดมัลแวร์และถูกเปลี่ยนเป็น Bot (ย่อมาจาก Robot) ไม่ว่าจะเป็นอุปกรณ์คอมพิวเตอร์ เว็บแคม เราท์เตอร์ หรืออุปกรณ์อื่นๆ เพื่อรอรับสั่งจาก ผู้บุกรุกโดยผู้บุกรุกจะนำ Botnet ที่มีไปใช้ในการโจมตีขนาดใหญ่ เช่นการทำ DDoS เป็นต้น

- **Spam Mail** หรืออีเมล์ขยะ เป็นขยะออนไลน์ที่ส่งตรงถึงผู้รับ โดยที่ผู้รับนั้นไม่ต้องการและสร้างความเดือดร้อนรำคาญให้กับผู้รับได้ในลักษณะของการโฆษณาสินค้าหรือบริการการชักชวนเข้าไปยังเว็บไซต์ต่าง ๆ ซึ่งอาจมีภัยคุกคามชนิด Phishing แฝงเข้ามาด้วย ด้วยเหตุนี้จึงควรติดตั้งระบบ Anti Spam หรือหากใช้ฟรีอีเมล์ก็ควรมีโปรแกรมคัดกรองอีเมล์ขยะในชั้นหนึ่งแล้ว

- **Phishing** คือการหลอกลวงทางอินเทอร์เน็ตเพื่อขอข้อมูลที่สำคัญ เช่น รหัสผ่าน หรือหมายเลขบัตรเครดิต โดยการส่งข้อความผ่านทางอีเมล์หรือเมสเซนเจอร์ ตัวอย่างของการ Phishing เช่น การบอกแก่ผู้รับปลายทางว่าเป็นธนาคารหรือบริษัทที่น่าเชื่อถือ และแจ้งว่ามีสาเหตุทำให้คุณต้องเข้าสู่ระบบและใส่ข้อมูลที่สำคัญใหม่ โดยเว็บไซต์ที่ลิงก์ไปนั้นจะมีหน้าตาคล้ายคลึงกับเว็บที่กล่าวถึง Phishing

- **Sniffing** เป็นการดักข้อมูลที่ส่งจากคอมพิวเตอร์เครื่องหนึ่งไปยังอีกเครื่องหนึ่ง หรือจากเครือข่ายหนึ่งไปยังอีกเครือข่ายหนึ่ง เป็นวิธีการหนึ่งที่ผู้บุกรุกนิยมใช้

- **Hacking** เป็นการเจาะระบบเครือข่ายคอมพิวเตอร์ไม่ว่าจะกระทำด้วยมนุษย์หรืออาศัยโปรแกรมด้วยวัตถุประสงค์ต่าง ๆ กัน โดยทั่วไปแล้วการ Hacking เป็นสิ่งผิดกฎหมาย เว้นแต่หากได้รับอนุญาตจากเจ้าของเครื่องคอมพิวเตอร์หรือระบบ โดยตัวอย่างของการ Hacking อย่างถูกกฎหมาย เช่น การเจาะระบบ เพื่อประเมินความเสี่ยงของระบบคอมพิวเตอร์ และทดสอบระบบการรักษาความปลอดภัยเครือข่ายขององค์กร

- **ผู้บุกรุก (Hacker)** หมายถึง ผู้ที่ไม่ได้รับอนุญาตในการใช้งานระบบหรือเครื่องคอมพิวเตอร์ แต่พยายามลักลอกเข้ามาใช้งานด้วยวัตถุประสงค์ต่าง ๆ เช่น การโจรกรรมข้อมูล แสวงหาผลกำไร หรือเพื่อความสนุกส่วนตัว

- **Social Engineering** หมายถึง การหลอกลวง ล่อหลอกผู้อื่น โดยใช้หลักการพื้นฐานทางจิตวิทยาให้เหยื่อเปิดเผยข้อมูลเพื่อให้ได้ผลประโยชน์ตามที่แฮกเกอร์ต้องการ โดยอาศัยจุดอ่อน ความรู้เท่าไม่ถึงการณ์ ความไม่รู้ ความประมาทของผู้ใช้งานระบบคอมพิวเตอร์

- **Password Attack** หมายถึง การโจมตีที่ผู้บุกรุกพยายามคาดเดา หรือทำให้ได้มาซึ่งรหัสผ่านของผู้ใช้คนใดคนหนึ่ง สำหรับนำไปโจมตีระบบคอมพิวเตอร์

- **Insider Treats** หมายถึง ภัยคุกคามทางไซเบอร์ที่เกิดจากบุคคลภายในองค์กรแบ่งออกเป็น ๓ ประเภท คือ ภัยที่เกิดจากการประมาทโดยไม่ได้ตั้งใจของบุคลากร ภัยที่เกิดจากการขโมยตัวตนหรือข้อมูลบุคลากรที่ทำให้แฮกเกอร์สามารถเจาะเข้าระบบได้ และภัยจากตัวบุคลากรเองที่ต้องการจะบ่อนทำลายองค์กรจากภายใน

- **SQL Injection** หมายถึง การโจมตีที่ระบบฐานข้อมูลของระบบผ่านช่องโหว่ของ SQL ส่งผลให้ระบบฐานข้อมูลถูกขโมย หรือถูกทำลาย หรือแก้ไขให้เกิดความเสียหายได้

- **Form Jacking** หมายถึง ภัยคุกคามทางไซเบอร์ที่เกิดจากผู้ไม่ประสงค์ดีสร้างโค้ด แปลกปลอมไว้บนเว็บไซต์ต่าง ๆ เพื่อหลอกลวงเป้าหมาย โดยมจุดประสงค์ในการเข้าถึงระบบสารสนเทศและข้อมูลเพื่อก่ออาชญากรรม

**๘. บทบาทหน้าที่และโครงสร้างทีมรับมือเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์**

**- ผู้รับแจ้งเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ภายในหน่วยงาน**

| ที่ | ชื่อ-นามสกุล | หน้าที่ | ความรับผิดชอบ | ช่องทางการติดต่อสื่อสาร |
|---|---|---|---|---|
| ๑ | นายวิทยา ทรัพย์เย็น | หัวหน้าทีมรับมือฯ (Team manager) | เป็นผู้รับแจ้งเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ | โทร. ๐๘๑ ๘๓๒๑๔๙๙ ๐๘๙ ๔๙๙๐๘๘๘ |
| ๒ | นางสาวปาริชาติ เยพิทักษ์ | เจ้าหน้าที่รับมือฯ (Incident lead) | เป็นผู้รับแจ้งเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ | โทร. ๐๙๖ ๙๔๙๙๓๙๘ |
| ๓ | นายธนพล จั่นลา | เจ้าหน้าที่รับมือฯ (Incident lead) | เป็นผู้รับแจ้งเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ | โทร. ๐๘๓ ๖๖๒๖๙๙๕ |
| ๔ | นางสาวศศิกานต์ ทายิดา | เจ้าหน้าที่รับมือฯ (Incident lead) | เป็นผู้รับแจ้งเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ | โทร. ๐๙๗ ๐๙๗๔๐๙๑ |

- **โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT)**

| ที่ | ชื่อ-นามสกุล | หน้าที่ | ความรับผิดชอบ |
|---|---|---|---|
| ๑ | นายวิทยา ทรัพย์เย็น<br>DCIO และ CISO ขององค์การตลาด | หัวหน้าทีมรับมือฯ<br>(Team manager) | ทำหน้าที่เป็นหัวหน้าผู้บริหารเทคโนโลยีสารสนเทศ และผู้บริหารระดับสูงที่ดูแลด้านความปลอดภัยของข้อมูล ระบบไซเบอร์ และเทคโนโลยีขององค์กร |
| ๒ | นางสาวปาริชาติ เยพิทักษ์ | เจ้าหน้าที่รับมือฯ<br>(Incident lead) | ทำหน้าที่ประสานงานกับผู้แจ้งเหตุ /เจ้าของทรัพย์สิน เพื่อให้การรับมือและควบคุมผลกระทบที่เกิดจากภัยคุกคามทางไซเบอร์มีประสิทธิภาพและประสานระหว่างทีมรับมือและหน่วยงานอื่นและรับมือเหตุภัยคุกคามทางไซเบอร์ |
| ๓ | นายธนพล จันลา | เจ้าหน้าที่รับมือฯ<br>(Incident lead) | ทำหน้าที่นผู้ประสานระหว่างทีมรับมือและหน่วยงานอื่นรับมือเหตุภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับระบบเครื่องคอมพิวเตอร์แม่ข่ายและระบบคอมพิวเตอร์ และให้ความช่วยเหลือหน่วยงานให้สามารถรับมือและควบคุมผลกระทบที่เกิดจากภัยคุกคามทางไซเบอร์ |
| ๔ | นางสาวศศิกานต์ ทายิดา | เจ้าหน้าที่รับมือฯ<br>(Incident lead) | ทำหน้าที่เป็นผู้ประสานระหว่างทีมรับมือและหน่วยงานอื่นและรับมือเหตุภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับระบบเว็บไซต์ และรับมือภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับฐานข้อมูลกลาง |

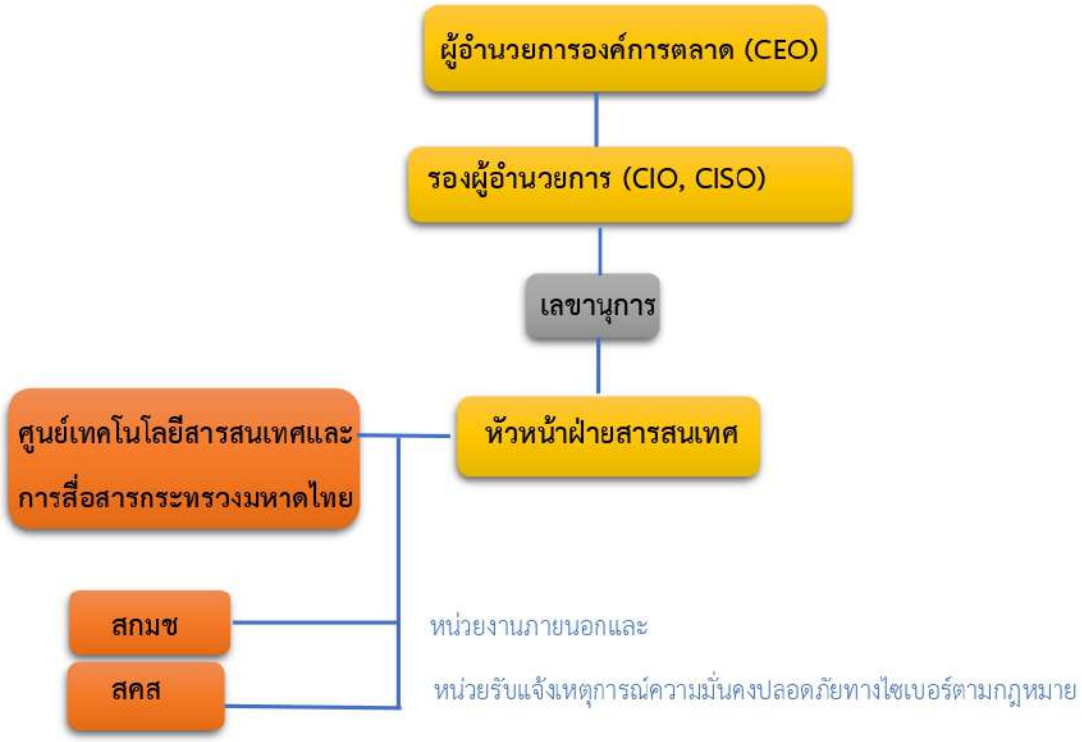
**-หน่วยงานภายนอกที่เกี่ยวข้อง**

| ที่ | ชื่อ-นามสกุล<br>ช่องทางการติดต่อ | หน่วยงาน | ความรับผิดชอบ | ความเกี่ยวข้อง |
|---|---|---|---|---|
| ๑ | ศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ<br>โทร. ๐๒ ๑๑๔ ๓๕๓๑<br>thaicert@ncsa.or.th | สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) | หน่วยงานกำหนดนโยบาย มาตรการ แนวทางการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานภาครัฐและภาคเอกชน ในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ภายในประเทศ | หน่วยงานกำกับดูแล |
| ๒ | ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ | ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ | หน่วยงานเฝ้าระวังความเสี่ยงในการเกิดภัยคุกคามทางไซเบอร์ติดตาม วิเคราะห์และ | หน่วยงานกำกับดูแล |

| | | | | |
|---|---|---|---|---|
| | โทร. ๐๒ ๑๑๔ ๓๕๓๑<br>thaicert@ncsa.or.th | Thailand Computer Emergency Response Team (ThaiCERT) | ประมวลผลข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ และการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์ | |
| ๓ | ศูนย์เฝ้าระวังการละเมิดข้อมูลส่วนบุคคล - PDPC Eagle Eye<br>โทรศัพท์ ๐๒๑๔๒๐๐๓๓<br>saraban@pdpc.or.th | สำนักงานคุ้มครองข้อมูลส่วนบุคคล (สคส.) | หน่วยงานเฝ้าระวังความเสี่ยงในการเกิดภัยคุกคามการละเมิดข้อมูลส่วนบุคคล | หน่วยงานกำกับดูแล |
| ๔ | ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารกระทรวงมหาดไทย<br>โทร. ๐๒ ๒๘๒ ๖๕๖๐ | ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารกระทรวงมหาดไทย | หน่วยงานเฝ้าระวังความเสี่ยงในการเกิดภัยคุกคามทางไซเบอร์ติดตามวิเคราะห์และประมวลผล<br>ข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ และการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์ | ผู้ดูแลระบบเครือข่าย |

**-โครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure)**

โครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure) ของบุคลากรภายในทีมรับมือฯ ตามกฎหมาย และหน่วยงานภายนอก



**๙. ขั้นตอนการรับมือในการเรียกใช้งาน (Activate) การตอบสนองต่อเหตุการณ์และ CIRT**

แผนรับมือเหตุภัยคุกคามทางไซเบอร์ฉบับนี้ ประกอบด้วยขั้นตอนการรับมือเหตุภัยคุกคามทางไซเบอร์ตามข้อ ๑๙.๑ ในประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ.๒๕๖๔ ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์ แต่ละระดับ พ.ศ.๒๕๖๔ และประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ.๒๕๖๖ รวมถึง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขององค์การตลาด

๙.๑ การเตรียมการ (preparation) มีมาตรการเพื่อเตรียมการและป้องกันการเกิดภัยคุกคามทางไซเบอร์ (preparation) เป็นการเตรียมความพร้อมเมื่อต้องเผชิญเหตุ ได้แก่ การจัดเตรียมข้อมูลให้พร้อม การจัดตั้งและฝึกอบรม บุคลากรหรือทีมงาน การจัดหาเครื่องมือและทรัพยากรต่าง ๆ ที่จำเป็น การตั้งค่าระบบต่าง ๆ ให้ปลอดภัย การจัดทำนโยบาย แผนงาน และกระบวนการที่เกี่ยวข้อง รวมถึง การสร้างเครือข่ายความร่วมมือ โดยดำเนินการดังต่อไปนี้

(๑) กำหนดโครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT)

(๒) กำหนดโครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure)

(๓) กำหนดเกณฑ์และขั้นตอนในการเรียกใช้งาน (Activate)การตอบสนองต่อเหตุการณ์ และ CIRT

(๔) จัดเตรียมข้อมูลและอุปกรณ์ รวมถึงช่องทางในการติดต่อสื่อสารที่จำเป็น ดังนี้

– รายชื่อและช่องทางการติดต่อของผู้ที่เกี่ยวข้องและประสานงานในการรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์

- ช่องทางการรายงานและติดตามข้อมูลสถานการณ์ของเหตุการณ์ที่ได้รับแจ้งกับผู้ที่เกี่ยวข้องและหน่วยงานสนับสนุนจากภายนอก

(๕) จัดเตรียมอุปกรณ์ ซอฟต์แวร์ และแหล่งข้อมูลสำหรับวิเคราะห์เหตุภัยคุกคามทางไซเบอร์

- อุปกรณ์ป้องกันเครือข่าย (Next Generation Firewall)

- อุปกรณ์ป้องกันภัยคุกคามแบบ (DDoS )

- อุปกรณ์ป้องกันการบุกรุกโจมตีเว็บไซต์ (WAF)

- ระบบรักษาความปลอดภัยสำหรับใช้งานอินเทอร์เน็ต (Secure Web Gateway)

- ระบบจัดเก็บ LOG

- ระบบวิเคราะห์ข้อมูลความปลอดภัย (SIEM)

- ระบบตรวจสอบการโจมตีและตอบสนองภัยคุกคาม (XDR)

(๖) มีการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน (Risk Assessment) ปีละ ๑ ครั้ง

(๗) จัดทำแผนผังโครงสร้างขั้นตอนการรับมือฯ

๙.๒ การตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (Detection and Analysis) ดำเนินการในการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ เพื่อบรรเทาความเสี่ยง ที่ยังคงเหลืออยู่ และแจ้งเตือนได้อย่างทันท่วงทีเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น โดยดำเนินการดังต่อไปนี้

(๑) ดำเนินการจัดเตรียมแนวทางรับมือเมื่อเกิดการโจมตีรูปแบบทั่วไปที่เคยเกิดขึ้นหรืออาจเกิดขึ้น (Common Attack Vectors/ Common Threat Vectors) โดยการโจมตีรูปแบบทั่วไปที่อาจเกิดขึ้น มีตัวอย่าง ดังนี้

| ประเภท | อธิบาย | วิธีการรับมือ |
|---|---|---|
| Weak or compromised access credentials | ผู้โจมตีขโมยชื่อผู้ใช้งานและรหัสผ่าน เพื่อใช้ในการเข้าถึงระบบและข้อมูล | มีนโยบายเปลี่ยนรหัสผ่านทุกๆ ๖เดือน และกำหนดรูปแบบของรหัสผ่านให้มีความยากในการคาดเดา รวมถึงมีการยืนยันตัวตน และเมื่อมีสถานการณ์อยู่ในช่ายน่าสงสัยที่จะถูกภัยคุกคามให้ทำการเปลี่ยนรหัสผ่านทันที |
| Unpatched software | ผู้โจมตีใช้ช่องโหว่ของระบบปฏิบัติการ / ซอฟต์แวร์อื่นๆ ทำให้สามารถเข้าถึงและควบคุมเครื่องคอมพิวเตอร์แม่ข่ายและลูกข่าย | ดำเนินการปรับปรุงเวอร์ชั่นของระบบปฏิบัติการ / ซอฟต์แวร์อื่นๆ อย่างสม่ำเสมอเพื่อปิดช่องโหว่ที่ผู้โจมตีจะสามารถเข้าถึงเครื่องได้ |
| Malware | เครื่องคอมพิวเตอร์ติดโปรแกรมไวรัสซึ่งอาจทำให้เครื่องคอมพิวเตอร์และข้อมูลที่อยู่ภายในเครื่องไม่สามารถใช้งานได้ | ติดตั้งระบบป้องกันไวรัสคอมพิวเตอร์หรือระบบตรวจสอบการโจมตีและตอบสนองภัยคุกคาม (EDR/XDR) ที่เครื่องคอมพิวเตอร์ |

(๒) มีกลไกเพื่อตรวจจับสิ่งบ่งชี้หรือลักษณะเบื้องต้นของการเกิดภัยคุกคามทางไซเบอร์ เพื่อตอบสนองต่อภัยคุกคามได้อย่างเหมาะสมและทันท่วงที รายละเอียดดังนี้

- ผู้ให้บริการเฝ้าระวังภัยคุกคามทางไซเบอร์

- ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (สกมช.)

(๓) มีแนวทางในการวิเคราะห์ผลกระทบและระดับของภัยคุกคามทางไซเบอร์ เพื่อรับมือกับภัยคุกคามทางไซเบอร์ให้ทันท่วงที โดยพิจารณาปัจจัยต่าง ๆ ที่เกี่ยวข้อง เช่น ผลกระทบต่อการทำงานของระบบ (functional impact) และความสามารถในการกู้คืน (recoverability effort) เป็นต้น

| ประเภท/รูปแบบเหตุการณ์ (Incident Categories) | ระดับความรุนแรง (Severity Level) | เวลาในการตอบสนอง (Threat Response SLA) | ระยะเวลาในการกู้คืน (Recovery Time) |
|---|---|---|---|
| เป็น Incident ที่เกิดขึ้นและยังไม่ส่งผลกระทบต่อบริการขององค์กร เช่น e-mail Spam, การติดไวรัสคอมพิวเตอร์ที่ไม่อันตราย | Low | ๑๒ ชั่วโมง | ๔ ชั่วโมง |

| ประเภท/รูปแบบเหตุการณ์ (Incident Categories) | ระดับความรุนแรง (Severity Level) | เวลาในการตอบสนอง (Threat Response SLA) | ระยะเวลาในการกู้คืน (Recovery Time) |
|---|---|---|---|
| เป็น Incident ที่เกิดขึ้นและส่งผลกระทบต่อบริการขององค์กรให้เกิดความล่าช้า ใช้งานได้ไม่เต็มประสิทธิภาพ เช่น การถูกโจมตีแบบ DDoS | Medium | ๒ ชั่วโมง | ๔ ชั่วโมง |
| เป็น Incident ที่เกิดขึ้นและส่งผลกระทบต่อบริการบางส่วนขององค์กรไม่สามารถให้บริการได้ เช่น การโดนโจมตีจากช่องโหว่ของระบบและวางโปรแกรมประสงค์ร้ายไว้ในเครื่อง, Key Logger ในเครื่องระดับ Admin | High | ๑ ชั่วโมง | ๔ ชั่วโมง |
| เป็น Incident ที่เกิดขึ้นและส่งผลกระทบต่อบริการทั้งหมดขององค์กรไม่สามารถให้บริการได้ เช่นการโดนโจมตีจากไวรัส Ransomware | Critical | ๐.๕ ชั่วโมง | ๔ ชั่วโมง |

(๔) มีบันทึกรายงานสถานการณ์เหตุการณ์ความมั่นคงปลอดภัยไซเบอร์

(๕) กรณีเกิดเหตุต้องมีการจัดทำบันทึกข้อมูลกิจกรรมเหตุการณ์ความปลอดภัยทางไซเบอร์ (Incident Documentation) โดยบันทึกข้อมูลเกี่ยวกับเหตุการณ์ความปลอดภัยทางไซเบอร์ ทุกขั้นตอนตั้งแต่ตรวจพบเหตุการณ์จนถึงกระบวนการสุดท้าย

(๖) มีการรายงานภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับบริการของโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้ผู้ที่เกี่ยวข้องทราบตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ.๒๕๖๖ ดังนี้

(ก) กรณีมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้น ตามข้อ ๔ แห่งประกาศฯ ฉบับดังกล่าว ใช้แบบฟอร์มรายงานตามที่กฎหมายกำหนด

(ข) กรณีมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญ ตาม ข้อ ๕ แห่งประกาศฯ ฉบับดังกล่าว รายงานไปยังสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ภายในระยะเวลา ๒๔ ชั่วโมง ตามกฎหมาย

(ค) จัดทำและส่งรายงานสรุปจำนวนเหตุภัยคุกคามทางไซเบอร์ทั้งหมดที่เกิดขึ้นกับข้อมูล หรือระบบ ภายในวันที่ ๓๑ มกราคม ของปีถัดไป ให้แก่สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ แห่งชาติ รายงานตามกฎหมายกำหนด

๙.๓ การระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคามทางไซเบอร์ และการฟื้นฟู ระบบงานที่ได้รับผลกระทบ (containment, eradication, and recovery) ให้ดำเนินการระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคามทางไซเบอร์ และการฟื้นฟู ระบบงานที่ได้รับผลกระทบ โดยกำหนดให้สอดคล้องกับความรุนแรงและระดับของภัยคุกคามทางไซเบอร์ แต่ละระดับจนกระทั่งสามารถกู้คืนทรัพย์สินสำคัญทางสารสนเทศให้กลับมาดำเนินงานหรือให้บริการ ได้ตามปกติโดยมีรายละเอียดดังต่อไปนี้

(๑) จำกัดขอบเขต (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

- ตัดการเชื่อมต่อทางเครือข่ายทั้งหมด (Network disconnection)

- หยุดการทำงานของฟังก์ชันที่เกี่ยวข้อง (Disabling Certain Functions) - Redirect Network Traffic และ/หรือเบี่ยงเบนความสนใจของผู้บุกรุกไปยัง Blackhole/ Sandbox Honeypot ทั้งนี้ การตัดสินใจเลือกใช้วิธีการควบคุมความเสียหายจะขึ้นอยู่กับลักษณะสถานการณ์ที่กำลัง เผชิญประเภทของภัยคุกคาม ระบบงานหรือบริการที่ได้รับผลกระทบ ระยะเวลาและทรัพยากร ที่จำเป็นต่อการควบคุมความเสียหาย

(๒) เรียกใช้งานกระบวนการกู้คืน (Recovery Process) - การ Restore Operating System หรือ Application Software ต่าง ๆ จาก Master Image ที่ปลอดภัย - การ Restore ข้อมูลกลับเข้าระบบจาก Backup Storage

(๓) ดำเนินการสอบสวน (Investigate) สาเหตุและผลกระทบของเหตุการณ์.

- รวบรวมข้อมูลจราจรทางคอมพิวเตอร์ (Log) จากเครื่องคอมพิวเตอร์ อุปกรณ์เครือข่าย อุปกรณ์ด้านการรักษาความมั่นคงปลอดภัย มาตรวจสอบหาความเชื่อมโยงของเหตุการณ์ที่ผิดปกติ

- นำข้อมูลที่ได้จากการตรวจสอบเบื้องต้นตั้งสมมุติฐานถึงสาเหตุและหาผลกระทบจากเหตุการณ์ที่เกิดขึ้น

- ตรวจสอบและดำเนินการปิดกั้นในส่วนที่อาจได้รับผลกระทบจากเหตุการณ์

- แจ้งหน่วยงานที่เกี่ยวข้องตามกฎหมาย ร่วมสอบสวนเหตุการณ์ที่เกิดขึ้น

(๔) เก็บรักษาหลักฐาน (Preservation of Evidence) ก่อนเริ่มกระบวนการกู้คืนเป็นการคงสภาพของหลักฐานเพื่อสนับสนุนการสอบสวนและการดำเนินการตามขั้นตอนทางกฎหมายต่อไป

- จัดเก็บหลักฐานให้เป็นไปตามขั้นตอนที่กำหนดไว้ในกฎหมายข้อบังคับที่เกี่ยวกับหลักฐานดิจิทัล

- มีบันทึกการเข้าถึงและการกระทำการใด ๆ ต่อหลักฐานตลอดเวลาอย่างรัดกุม

- จัดหาสถานที่จัดเก็บที่มีความมั่นคงปลอดภัยเพื่อใช้ในการเก็บหลักฐานข้อมูลและพยานวัตถุอื่นๆ ที่สำคัญ

(๕) ดำเนินการตามระเบียบวิธีการมีส่วนร่วม (Engagement Protocols) กับบุคคลภายนอกตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๙.๔. การดำเนินการภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ (Post-Incident activity) มีการกำหนดขั้นนตอน วิธีปฏิบัติ และกำหนดนโยบายภายในที่เกี่ยวข้องเพื่อให้มีแนวทางที่ชัดเจน ซึ่งการปฏิบัติตามมาตรการดังกล่าว จะช่วยให้หน่วยงานสามารถเรียนรู้จากเหตุภัยคุกคามทางไซเบอร์ที่ผ่านมา และสามารถหาแนวทางเพื่อแก้ไขจุดบกพร่องและพัฒนาแนวทางรับมือกับภัยคุกคามทางไซเบอร์ต่อไป โดยมีแนวทางดังต่อไปนี้

(๑) ต้องทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ อย่างน้อยปีละ ๑ ครั้ง

(๒) การฝึกฝนและการทดสอบแผน มีการอบรมฝึกฝนและทดสอบการรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์ เพื่อให้ทุกคนตระหนักและเข้าใจถึงหน้าที่ความรับผิดชอบ และเป้าหมายตามแผนที่กำหนด รวมทั้งเป็นการพัฒนา ทักษะเพื่อให้สามารถดำเนินงานตามแผนได้อย่างมีประสิทธิภาพ อย่างน้อยปีละ ๑ ครั้ง

(๓) เผยแพร่ประชาสัมพันธ์และฝึกอบรม ให้เจ้าหน้าที่รับทราบ เข้าใจและไม่กระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และตระหนักรู้ตามพระราชบัญญัติการรักษาความ

มั่นคงปลอดภัยไซเบอร์ รวมถึงกฎหมายอื่น ๆ ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ รวมถึงมีความรับผิดชอบในการใช้ทรัพยากรทางด้านเทคโนโลยีสารสนเทศอย่างเหมาะสม และต้องมีการเก็บรักษาข้อมูลและพยานหลักฐานที่จำเป็น เพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์ หรือใช้ในกรณีที่ต้องการร้องทุกข์หรือดำเนินคดี เนื่องจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้นนั้น อาจเข้าลักษณะเป็นความผิดตามประมวลกฎหมายอาญา หรือพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ หรือกฎหมายอื่น ๆ ที่เกี่ยวข้องประกอบด้วยการดำเนินการในเรื่องดังต่อไปนี้

| | |
|---|---|
| 1. Assessment | การประเมินเพื่อหาจุดที่ต้องดำเนินการจัดเก็บหลักฐานของ Incident ที่กำลังรับมือและตอบสนอง เช่น Hard Disk, RAM, External Hard Disk, Mobile Device เป็นต้น |
| 2. Acquisition | ดำเนินการจัดเก็บหลักฐานด้วยการทำสำเนา (Duplication/Bit-for-bit Acquisition) ด้วยเครื่องมือที่เหมาะสม โดยมีข้อควรระวังในเรื่องดังต่อไปนี้<br>1. ต้องป้องกันการเปลี่ยนแปลงของหลักฐานด้วยการใช้งาน Hardware Write Blocker<br>2. ต้องคำนึงถึง Volatility หรือความอ่อนไหวต่อการสูญเสียกระแสไฟฟ้าของหลักฐาน เช่น ข้อมูลที่เสี่ยงต่อการสูญหายหากไม่มีกระแสไฟคอยเลี้ยง เช่น RAM ต้องได้รับการเก็บรักษาเป็นอันดับแรก เป็นต้น<br>3. ต้องบันทึกรายละเอียดการดำเนินงานทุกขั้นตอนที่ลงมือปฏิบัติอย่างละเอียด<br>4. ต้องทำการบันทึกหลักฐาน (Chain of Custody) |
| 3. Authentication | ทำการตรวจสอบความถูกต้องของหลักฐานที่ Duplicate และเปรียบเทียบกับ ต้นฉบับด้วยวิธี Cryptographic Hash เช่น MD5, SHA1, SHA256 |
| 4. Analysis & Report | วิเคราะห์หาข้อมูลจากชุดหลักฐานที่ดำเนินการจัดเก็บเพื่อพิสูจน์ข้อเท็จจริง หรือ เพื่อค้นหาสาเหตุของการเกิด Incident |
| 5. Archive | จัดเก็บหลักฐานไว้ในที่เหมาะสม ปลอดภัย และบันทึก Chain of Custody Form ทุกครั้งที่มีการเคลื่อนย้ายหลักฐาน พร้อมทั้งระบุเหตุผลของการเคลื่อนย้าย |

๙.๕. การจัดทำรายการตรวจสอบการจัดการเหตุการณ์ (Incident Handling Checklist) จัดทำรายการตรวจสอบการจัดการเหตุการณ์ (Incident Handling Checklist) เพื่อใช้เป็น แนวทางลำดับขั้นตอนสำคัญที่ควรดำเนินการ

## ๑๐.ขั้นตอนการปฏิบัติเมื่อเกิดภัยคุกคามทางไซเบอร์

| ขั้นตอน | รายละเอียด |
|---|---|
| ตรวจพบภัยคุกคามทางไซเบอร์ | มีการแจ้งเหตุจากผู้ใช้งานหรือตรวจจับภัยคุกคามทางไซเบอร์ได้จากศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยสารสนเทศ |
| ตรวจสอบภัยคุกคามทางไซเบอร์ | ตรวจสอบข้อมูลของภัยคุกคามทางไซเบอร์ และประเมินระดับภัยคุกคามตามที่กำหนดใน พรบ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๖๐ |
| ควบคุมภัยคุกคามทางไซเบอร์ | ดำเนินการควบคุมภัยคุกคามทางไซเบอร์ ให้ส่งผลกระทบน้อยที่สุดและป้องกันไม่ให้เกิดการแพร่กระจายไปยังส่วนอื่น ๆ ซึ่งในกรณีที่เร่งด่วนจะทำการปิดระบบ หรือ ตัดการเชื่อมต่อของระบบคอมพิวเตอร์ชั่วคราว |
| การแก้ไขปัญหา | ดำเนินการแก้ไขหรือกำจัดภัยคุกคามทางไซเบอร์ในเบื้องต้นในทันที |
| ติดต่อประสานสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) | ในกรณีที่ไม่สามารถแก้ไขปัญหาได้จะดำเนินการติดต่อประสานสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เพื่อขอคำแนะนำหรือขอความช่วยเหลือ |
| แก้ไขปัญหาสำเร็จและดำเนินการหาวิธีป้องกันการเกิดภัยคุกคามไซเบอร์ในลักษณะเดิม | หลังจากแก้ไขปัญหาภัยคุกคามไซเบอร์แล้วจะดำเนินการตรวจหาช่องโหว่ โดยอุปกรณ์ตรวจสอบช่องโหว่ระบบเครือข่าย หรือเครื่องมืออื่นๆ และหาวิธีเพื่อป้องกันการเกิดภัยคุกคามไซเบอร์ในลักษณะเดิม |
| การทดสอบระบบ | ตรวจสอบการทำงานของโครงสร้างพื้นฐานสำคัญทางสารสนเทศว่าสามารถทำงานได้สมบูรณ์หรือไม่ ในกรณีที่พบว่าการทำงานไม่สมบูรณ์ หรือข้อมูลสำคัญสูญหายไปจะดำเนินการกู้คืนระบบงาน |
| กู้คืนระบบ | ดำเนินการตามขั้นตอนการกู้คืนข้อมูลตามที่ระบุในแผนการสำรองและกู้คืนระบบ ในกรณีที่กู้คืนระบบไม่ได้จะพิจารณาเปิดใช้ระบบงานคอมพิวเตอร์สำรอง และเร่งกู้ระบบงานคอมพิวเตอร์หลัก |
| ระบบสามารถใช้งานได้ตามปกติ | เมื่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศสามารถ ทำงานได้ตามปกติแล้ว หน่วยงานที่ดูแลรับผิดชอบด้านโครงข่ายระบบสารสนเทศ จะดำเนินการสรุปผลในการดำเนินการรับมือภัยคุกคามไซเบอร์ |
| สรุปผลในการรับมือภัยคุกคามทางไซเบอร์และจัดทำรายงาน | สรุปผลในการรับมือภัยคุกคามทางไซเบอร์ และแจ้งผลการดำเนินงานให้แก่ผู้เกี่ยวข้อง |

**แบบฟอร์ม**

**บันทึกรายงานสถานการณ์เหตุการณ์ความมั่นคงปลอดภัยไซเบอร์**

๑.วันที่/เวลา บันทึกข้อมูล :

๒.วันและเวลาที่เกิดเหตุการณ์ :

๓.สถานะเหตุการณ์ปัจจุบัน :

๔.ประเภทเหตุการณ์ :

๕.ระดับความรุนแรง :

๖.รายละเอียดเหตุการณ์ :

๗.ผลกระทบที่เกิดขึ้น :

๘.ความเสียหายที่เกิดขึ้น :

๙.การรายงานเหตุการณ์ :

๑๐.หน่วยงานที่ขอความช่วยเหลือ :

๑๑.การดำเนินการตอบสนองต่อเหตุการณ์ :

๑๒.รายละเอียดเพิ่มเติม :

๑๓.ผู้จัดการรับมือฯ เหตุการณ์ :

๑๔.ข้อมูลติดต่อผู้จัดการรับมือฯเหตุการณ์ :

๑๕.วันและเวลาที่มีรายงานความคืบหน้าครั้งถัดไป :

ลงชื่อ.....

(ผู้บันทึกรายงาน)

**แบบฟอร์ม**

**แบบตอบรับการดำเนินการตามแนวปฏิบัติขั้นพื้นฐานสำหรับการป้องกัน เฝ้าระวัง และรับมือภัยคุกคามทางไซเบอร์**

ชื่อหน่วยงาน.....

| ลำดับ | หัวข้อ | ป้องกัน/เฝ้าระวัง/รับมือ | รายละเอียด | ดำเนินการเรียบร้อย |
|---|---|---|---|---|
| 1 | Distributed Denial of Service (DDoS) | แนวทางการป้องกัน | ใช้บริการป้องกัน DDoS จากผู้ให้บริการ Cloud หรือ CDN เช่น Cloudflare, Akamai, AWS Shield | ☐ |
| | | | วางระบบ Load Balancer เพื่อกระจายโหลดไปยังหลายเซิร์ฟเวอร์ | ☐ |
| | | | Rate Limiting และ Firewall Rules บน Web Application Firewall (WAF) | ☐ |
| | | แนวทางการเฝ้าระวัง | ติดตั้งระบบ Monitoring เพื่อตรวจสอบทราฟฟิกการใช้งานแบบ Real-time | ☐ |
| | | | กำหนด Threshold การใช้งาน Bandwidth และ Connections เพื่อแจ้งเตือนเมื่อเกินค่าที่กำหนด | ☐ |
| | | | ตรวจสอบ Logs การใช้งานจากอุปกรณ์จต่างๆ เช่น Firewall, Router และ Load Balancer อย่างสม่ำเสมอ | ☐ |
| | | แนวทางการรับมือ | จัดทำ Playbook การตอบสนองฉุกเฉิน (Incident Response Plan) สำหรับ DDoS<br>แจ้งผู้ให้บริการระบบรับทราบ เพื่อบล็อกทราฟฟิกที่โจมตีหากจำเป็น | ☐ |
| 2 | Credential Leak | แนวทางการป้องกัน | ใช้งาน Multi-Factor Authentication (MFA) สำหรับทุกบัญชีที่เข้าถึงระบบ | ☐ |
| | | | บังคับใช้นโยบายรหัสผ่านที่เข้มงวด (เช่น มีความยาวขั้นต่ำ, complexity) | ☐ |
| | | แนวทางการเฝ้าระวัง | ตรวจสอบรหัสผ่านรั่วไหลในฐานข้อมูลสาธารณะ (เช่น HavelBeenPwned) ด้วยเครื่องมืออัตโนมัติ | ☐ |

**แบบฟอร์ม**

**แบบตอบรับการดำเนินการตามแนวปฏิบัติขั้นพื้นฐานสำหรับการป้องกัน เฝ้าระวัง และรับมือภัยคุกคามทางไซเบอร์**

ชื่อหน่วยงาน.....

| ลำดับ | หัวข้อ | ป้องกัน/เฝ้าระวัง/รับมือ | รายละเอียด | ดำเนินการเรียบร้อย |
|---|---|---|---|---|
| 1 | Distributed Denial of Service (DDoS) | แนวทางการป้องกัน | ใช้บริการป้องกัน DDoS จากผู้ให้บริการ Cloud หรือ CDN เช่น Cloudflare, Akamai, AWS Shield | ☐ |
| | | | วางระบบ Load Balancer เพื่อกระจายโหลดไปยังหลายเซิร์ฟเวอร์ | ☐ |
| | | | Rate Limiting และ Firewall Rules บน Web Application Firewall (WAF) | ☐ |
| | | แนวทางการเฝ้าระวัง | ติดตั้งระบบ Monitoring เพื่อตรวจสอบทราฟฟิกการใช้งานแบบ Real-time | ☐ |
| | | | กำหนด Threshold การใช้งาน Bandwidth และ Connections เพื่อแจ้งเตือนเมื่อเกินค่าที่กำหนด | ☐ |
| | | | ตรวจสอบ Logs การใช้งานจากอุปกรณ์จต่างๆ เช่น Firewall, Router และ Load Balancer อย่างสม่ำเสมอ | ☐ |
| | | แนวทางการรับมือ | จัดทำ Playbook การตอบสนองฉุกเฉิน (Incident Response Plan) สำหรับ DDoS<br>แจ้งผู้ให้บริการระบบรับทราบ เพื่อบล็อกทราฟฟิกที่โจมตีหากจำเป็น | ☐ |
| 2 | Credential Leak | แนวทางการป้องกัน | ใช้งาน Multi-Factor Authentication (MFA) สำหรับทุกบัญชีที่เข้าถึงระบบ | ☐ |
| | | | บังคับใช้นโยบายรหัสผ่านที่เข้มงวด (เช่น มีความยาวขั้นต่ำ, complexity) | ☐ |
| | | แนวทางการเฝ้าระวัง | ตรวจสอบรหัสผ่านรั่วไหลในฐานข้อมูลสาธารณะ (เช่น HavelBeenPwned) ด้วยเครื่องมืออัตโนมัติ | ☐ |

| ลำดับ | หัวข้อ | ป้องกัน/เฝ้าระวัง/รับมือ | รายละเอียด | ดำเนินการเรียบร้อย |
|---|---|---|---|---|
| | | | ตรวจสอบการเข้าสู่ระบบนอกเวลาทำงานหรือจากอุปกรณ์หรือแหล่งที่ไม่ทราบที่มา | ☐ |
| | | แนวทางการรับมือ | รีเซ็ตรหัสผ่านทันที เมื่อทราบถึงเหตุการณ์รั่วไหลจากบัญชีผู้ใช้ภายในหน่วยงาน แจ้งผู้ใช้และแนะนำการเปลี่ยนรหัสผ่าน | ☐ |
| 3 | Web Defacement | แนวทางการป้องกัน | อัปเดต CMS/Framework และ Plugins เสมอ | ☐ |
| | | | จำกัดสิทธิ์ของผู้ใช้งาน (Principle of Least Privilege) โดยเฉพาะบัญชี Admin | ☐ |
| | | | ใช้ Web Application Firewall (WAF) เพื่อตรวจจับและป้องการโจมตี | ☐ |
| | | แนวทางการเฝ้าระวัง | ใช้ระบบ File Integrity Monitoring (FIM) เพื่อตรวจสอบการเปลี่ยนแปลงของไฟล์ในเว็บเซิร์ฟเวอร์ | ☐ |
| | | | ตั้งระบบตรวจจับการเปลี่ยนแปลงหน้าเว็บแบบอัตโนมัติ (เช่น เครื่องมือ Web page diff checker) | ☐ |
| | | แนวทางการรับมือ | ตรวจสอบช่องโหว่ที่ถูกใช้ และทำการอุดช่องโหว่ทันที | ☐ |
| | | | เก็บหลักฐานการโจมตี (Logs, Snapshot) เพื่อใช้ในการวิเคราะห์และดำเนินคดี | ☐ |
| | | | แจ้งผู้เกี่ยวข้อง เช่น ผู้ให้บริการ Hosting หรือ CERT | ☐ |
| 4 | Data Breach | แนวทางการป้องกัน | การควบคุมสิทธิ์การเข้าถึงข้อมูล (Access Control) โดยใช้หลัก Least Privilege และ Role-Based Access Control (RBAC) จำกัดสิทธิ์ให้ผู้ใช้งานเข้าถึงเฉพาะข้อมูลที่จำเป็นเท่านั้น | ☐ |
| | | | เข้ารหัสข้อมูล (Data Encryption) เข้ารหัสข้อมูลทั้งขณะจัดเก็บและขณะส่งผ่าน โดยใช้มาตรฐานการเข้ารหัสที่ยอมรับได้ เช่น AES-256, TLS 1.3 | ☐ |
| | | | ใช้นโยบายรหัสผ่านและ MFA บังคับใช้รหัสผ่านที่รัดกุมและใช้ Multi-Factor Authentication (MFA) สำหรับการเข้าถึงระบบที่สำคัญ | ☐ |

| ลำดับ | หัวข้อ | ป้องกัน/เฝ้าระวัง/รับมือ | รายละเอียด | ดำเนินการเรียบร้อย |
|---|---|---|---|---|
| | | แนวทางการเฝ้าระวัง | ใช้ระบบ SIEM (Security Information and Event Management) รวม log จากหลายแหล่ง เพื่อตรวจสอบและแจ้งเตือนเหตุการณ์ผิดปกติ เช่น การเข้าถึงข้อมูลจำนวนมากผิดปกติ | ☐ |
| | | | ติดตามพฤติกรรมของผู้ใช้งานไซ้ เพื่อระบุพฤติกรรมผิดปกติที่อาจบ่งชี้ถึงการละเมิดข้อมูล | ☐ |
| | | แนวทางการรับมือ | จัดทำ Incident Response Plan สำหรับ Data Breach โดยเฉพาะ ระบุขั้นตอนการรับมือ การติดต่อภายใน/ภายนอก และการรายงานเหตุการณ์ตามกฎหมาย | ☐ |
| | | | แจ้งเตือนผู้ได้รับผลกระทบ ดำเนินการตามข้อกำหนดด้านกฎหมาย เช่น NCSA, PDPA โดยแจ้งผู้ใช้งานหรือลูกค้าที่ได้รับผลกระทบโดยเร็ว | ☐ |
| | | | มีแผนฟื้นฟูระบบและปรับปรุงมาตรการรักษาความปลอดภัย อัปเดตระบบ, รีเซ็ตรหัสผ่าน, แก้ไขช่องโหว่ และทบทวนมาตรการที่ใช้ | ☐ |

ลงชื่อ .....

(..... .....)

ตำแหน่ง.....

วันที่.....

(หัวหน้าหน่วยงาน หรือผู้รับมอบอำนาจ)

**เอกสาร ก๑ ข้อมูลที่ต้องแจ้ง**

**ข้อมูลการประสานงานและผลการตรวจสอบภัยคุกคามเบื้องต้น**

**๑. ข้อมูลการประสานงาน**

ชื่อหน่วยงานที่รับผิดชอบติดตามเหตุภัยคุกคาม: โปรดระบุ

วันที่และเวลาที่แจ้ง:โปรดระบุ

**๒. ด้านภารกิจหรือบริการของหน่วยงาน และ ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม**

ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม: โปรดระบุ

ที่อยู่ของหน่วยงานหรือหน่วยงานย่อยที่เกิดเหตุภัยคุกคาม: โปรดระบุ

**๓. ข้อมูลการติดต่อสำหรับการประสานงานเหตุภัยคุกคาม**

ชื่อ-นามสกุล: โปรดระบุ ตำแหน่งงาน: โปรดระบุ

ชื่อหน่วยงาน: โปรดระบุ อีเมล: โปรดระบุ

โทรศัพท์ (ที่ทำงาน / มือถือ): โปรดระบุ

**๔. ความต่อเนื่องของเหตุภัยคุกคาม**

☐ เหตุภัยคุกคามใหม่ ☐ การรายงานข้อมูลต่อเนื่องจากเหตุภัยคุกคามเดิม

**๕. ลักษณะภัยคุกคามทางไซเบอร์**

ระบบที่ได้รับผลกระทบมีความสำคัญต่อพันธกิจหลักของหน่วยงานหรือไม่

เหตุการณ์ที่เกิดขึ้นเกิดจากภัยคุกคามทางไซเบอร์[๔] 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 และระงับภัยคุกคาม ทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ (ทั้งนี้ ภัยคุกคามทางไซเบอร์หมวดหมู่ที่ ๐ หมวดหมู่ที่ ๑ และหมวดหมู่ที่ ๙ ไม่เข้าข่ายเป็นภัยคุกคามทางไซเบอร์ที่ต้องรายงาน)

[๔] พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดความหมายของ “ภัยคุกคามทางไซเบอร์” ดังนี้ การกระทำหรือการดำเนินการใด ๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อ ระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบ ต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

**เอกสาร ก๒ แบบรายงานภัยคุกคามทางไซเบอร์**

| **ส่วนที่ ๑** |
|---|
| **หมวด ก. ข้อมูลการประสานงานและผลการตรวจสอบภัยคุกคามเบื้องต้น** |
| หมายเลขอ้างอิง (สำหรับเจ้าหน้าที่ สกมช.): โปรดระบุ<br>หน่วยงานที่รับผิดชอบติดตามเหตุภัยคุกคาม (ถ้ามี): โปรดระบุ<br>วันที่: โปรดระบุ เวลา: โปรดระบุ |
| **ก๑. ด้านภารกิจหรือบริการของหน่วยงาน และ ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม**<br>ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม: โปรดระบุ<br>ที่อยู่ของหน่วยงานหรือหน่วยงานย่อยที่เกิดเหตุภัยคุกคาม: โปรดระบุ |
| **ก๒. ข้อมูลการติดต่อสำหรับการประสานงานเหตุภัยคุกคาม**<br>ชื่อ-นามสกุล: โปรดระบุ ตำแหน่งงาน: โปรดระบุ<br>ชื่อหน่วยงาน: โปรดระบุ อีเมล: โปรดระบุ<br>โทรศัพท์ (ที่ทำงาน / มือถือ): โปรดระบุ |
| **ก๓. ความต่อเนื่องของเหตุภัยคุกคาม**<br>☐ เหตุภัยคุกคามใหม่ ☐ การรายงานข้อมูลต่อเนื่องจากเหตุภัยคุกคามเดิม |
| **ก๔. ลักษณะภัยคุกคามทางไซเบอร์**<br>ระบบที่ได้รับผลกระทบมีความสำคัญต่อพันธกิจหลักของหน่วยงาน<br>☐ ใช่ ☐ ไม่ใช่<br>เหตุการณ์ที่เกิดขึ้นเกิดจากภัยคุกคามทางไซเบอร์[๕] ในระดับใด (มาตรา ๖๐)<br>☐ ไม่ร้ายแรง ☐ ร้ายแรง ☐ วิกฤต (ก) ☐ วิกฤต (ข)<br>☐ ยังไม่สามารถระบุได้ |

[๕] พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดความหมายของ “ภัยคุกคามทางไซเบอร์” ดังนี้ การกระทำ หรือการดำเนินการใด ๆ โดยมิชอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิด การประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหาย หรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

**หมวด ข. ข้อมูลการตรวจพบภัยคุกคามไซเบอร์**

**ข๑. วัน เวลา ที่เกิดเหตุภัยคุกคาม**

วันที่ : โปรดระบุ เวลา : โปรดระบุ

**วัน เวลา ที่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศทราบเหตุภัยคุกคาม**

วันที่ : โปรดระบุ 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 และระงับภัยคุกคามทาง ไซเบอร์แต่ละระดับ 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 รุ่นของเครื่อง คอมพิวเตอร์):

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 วัน เวลา ที่ผู้โจมตีได้เริ่มต้นเข้าถึงระบบ (System Access)**

วันที่: โปรดระบุ เวลา: โปรดระบุ ไม่ทราบ: ☐

**ง๑.๒ ข้อมูลการพบเห็นเหตุภัยคุกคามทางไซเบอร์**

รายละเอียดแหล่งที่มา หรือต้นเหตุของเหตุภัยคุกคาม (เท่าที่ทราบ เช่น คน, ความผิดพลาดของ ระบบ, 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 รายละเอียดของระบบ หรือข้อมูลที่ได้รับผลกระทบ (Information of Affected System)**

หมายเลข CVE: โปรดระบุ

ช่องโหว่ที่ถูกใช้จู่โจม: โปรดระบุ

การใช้ระบบหรือเครื่องที่ได้รับผลกระทบเป็นฐานเพื่อจู่โจมขยายผลไปยังระบบหรือเครื่องอื่น:
โปรดระบุ

อาการหรือสิ่งผิดปกติ (เลือกได้มากกว่า ๑ รายการ)

- ☐ ระบบล่ม
- ☐ รายการข้อมูลจราจรทางคอมพิวเตอร์ที่ผิดปกติ
- ☐ บัญชีผู้ใช้ถูกสร้างขึ้นมาใหม่โดยไม่ทราบสาเหตุ หรือ บัญชีผู้ใช้มีความผิดปกติ
- ☐ การจู่โจมด้วยวิศวกรรมสังคม (Social Engineering) ทั้งที่ลำดับและไม่ลำดับ
- ☐ 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 :** โปรดระบุ

**๒.๑ รายละเอียดการดำเนินการเพื่อแก้ไขเหตุภัยคุกคาม:**

โปรดระบุ

**๒.๒ การคาดการณ์ความสามารถฟื้นฟู**

โปรดระบุรายละเอียดการฟื้นฟู ทรัพยากรที่ต้องใช้และที่ต้องการเพิ่ม และประมาณระยะเวลาการฟื้นฟู

**๓. ข้อมูลกิจกรรมภายหลังการแก้ปัญหา (ถ้ามี)**

**๓.๑ วัน เวลา ที่เหตุภัยคุกคามสิ้นสุด** **วันที่:** โปรดระบุ **เวลา:** โปรดระบุ

**๓.๒ การดำเนินการเพื่อป้องกันเหตุภัยคุกคามที่คล้ายคลึงกัน:** โปรดระบุ

**๓.๓ บทเรียนที่ได้จากเหตุภัยคุกคาม:** โปรดระบุ

**เอกสาร ก๓ แบบรายงานสรุปภัยคุกคามทางไซเบอร์ในหนึ่งรอบปี**

**ข้อ ๑ สถิติรายปีจำแนกตามหมวดหมู่ของภัยคุกคามทางไซเบอร์[๖]**

| หมวดหมู่ | คำอธิบาย | จำนวน |
|---|---|---|
| ๐ | เหตุการณ์จำลองและการฝึกจู่โจมของหน่วยงาน (Training and Exercises) | |
| ๑ | การพยายามเข้าถึงระบบที่ไม่สำเร็จ (Unsuccessful Activity Attempt) | |
| ๒ | การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance) | |
| ๓ | การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยที่หน่วยงานกำหนด (Non-Compliance Activity) | |
| ๔ | การบุกรุกโดยการใช้มัลแวร์ (Malicious Logic) | |
| ๕ | การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion) | |
| ๖ | การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion) | |
| ๗ | การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service) | |
| ๘ | เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating) | |
| ๙ | เหตุการณ์ผิดปกติที่ได้รับการวิเคราะห์แล้วว่าไม่ใช่เหตุการณ์ที่เป็นภัยคุกคาม (Explained Anomaly) | |

**ข้อ ๒ สถิติรายปีจำแนกตามทรัพย์สินที่ได้รับผลกระทบ**

| ทรัพย์สินที่ได้รับผลกระทบ | จำนวน |
|---|---|
| เครื่องแม่ข่าย / แอคทีฟ ไดเรกทอรี (Active Directory) | |
| เครื่องเวิร์กสเตชัน (Workstation) | |
| สวิตช์ (Switch) /เราเตอร์ (Router) | |
| เว็บไซต์ (Website) | |
| อื่น ๆ | |

**ข้อ ๓ สถิติรายปีจำแนกตามระดับภัยคุกคามทางไซเบอร์[๗]**

| ระดับภัยคุกคาม | จำนวน |
|---|---|
| ไม่ร้ายแรง | |
| ร้ายแรง | |
| วิกฤต (ก) | |
| วิกฤต (ข) | |

[๖] หมวดหมู่ตามข้อ ๑ ของภาคผนวกท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคาม ทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์ แต่ละระดับ พ.ศ. ๒๕๖๔

[๗] ระดับภัยคุกคามทางไซเบอร์ตามมาตรา ๖๐ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

ประจำปีงบประมาณ 2568

# แผนการรับมือเหตุภัยคุกคามทางไซเบอร์ (CYBERSECURITY INCIDENT RESPONSE PLAN)

**จัดทำโดย....ฝ่ายสารสนเทศ องค์การตลาดกระทรวงมหาดไทย**