กรมปศุสัตว์

Department of Livestock Development

แผนรับมือภัยคุกคามทางไซเบอร์

Cybersecurity Incident Response Plan

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กรมปศุสัตว์

มีนาคม 2569

ประวัติการแก้ไขเอกสาร

เวอร์ชัน	รายละเอียดการแก้ไข	วันที่จัดทำ
01	เอกสารเวอร์ชันตั้งต้น	มิถุนายน 2567
02	แก้ไขเนื้อหาให้ครอบคลุมตามแนวทางการจัดทำแผนรับมือเหตุภัยคุกคามทางไซเบอร์ของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ	สิงหาคม 2568
03	ปรับปรุงเนื้อหาตามข้อเสนอแนะของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ	มีนาคม 2569

การอนุมัติเอกสาร

ผู้จัดทำเอกสาร

ชื่อ นางสาวมณีนุช เปลี่ยนศรี
ตำแหน่ง นักวิชาการคอมพิวเตอร์ชำนาญการ
วันที่

ลงชื่อ
(นางสาวมณีนุช เปลี่ยนศรี)

ชื่อ นางสาวภาณุตา บุนนาค
ตำแหน่ง นักวิชาการคอมพิวเตอร์ชำนาญการ
วันที่

ลงชื่อ
(นางสาวภาณุตา บุนนาค)

ผู้ตรวจทานเอกสาร

ชื่อ นายกิติกรณ์ เจนไพบูลย์
ตำแหน่ง ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
วันที่

ลงชื่อ
(นายกิติกรณ์ เจนไพบูลย์)

ผู้อนุมัติเอกสาร

ชื่อ นายพงษ์พันธ์ ธรรมมา
ตำแหน่ง รองอธิบดีกรมปศุสัตว์
วันที่

ลงชื่อ
(นายพงษ์พันธ์ ธรรมมา)

สารบัญ

แผนรับมือภัยคุกคามทางไซเบอร์
กรมปศุสัตว์

1. หลักการและเหตุผล

ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มาตรา 44 กำหนดให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำประมวลแนวทางปฏิบัติ และกรอบมาตรฐานของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยเร็ว ซึ่งประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างน้อยต้องประกอบด้วยเรื่องดังต่อไปนี้

1.1 แผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจประเมิน ผู้ตรวจสอบภายใน หรือผู้ตรวจสอบอิสระจากภายนอก อย่างน้อยปีละหนึ่งครั้ง

1.2 แผนรับมือภัยคุกคามทางไซเบอร์ เพื่อดำเนินการตาม พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มาตรา 44 กรมปศุสัตว์ จึงได้จัดทำแผนรับมือภัยคุกคามทางไซเบอร์ขึ้นเพื่อรับมือกับภัยคุกคามทางไซเบอร์ ที่มาในรูปแบบไวรัสคอมพิวเตอร์ และการโจมตีระบบเครือข่ายคอมพิวเตอร์กลางของกรมปศุสัตว์ โดยการดำเนินงานตามแผนจะมุ่งเน้นในการตรวจสอบ ควบคุม ป้องกัน และแก้ไขปัญหาที่เกิดจากภัยคุกคามทางไซเบอร์ รวมถึงการกู้คืนระบบเครือข่ายคอมพิวเตอร์กลางให้สามารถใช้งานได้

2. วัตถุประสงค์

2.1 เพื่อกำหนดวิธีการในการตรวจสอบ ควบคุม ป้องกัน และแก้ไขปัญหาที่เกิดจากภัยคุกคามทางไซเบอร์ เพื่อป้องกัน และลดความเสียหายที่เกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ

2.2 เพื่อกำหนดวิธีการกู้คืนระบบเครือข่ายคอมพิวเตอร์กลางของกรมปศุสัตว์ ให้สามารถใช้งานได้

2.3 เพื่อเตรียมความพร้อมด้านบุคลากรของกรมปศุสัตว์ ในการรับมือกับปัญหาภัยคุกคามทางไซเบอร์

2.4 เพื่อให้การปฏิบัติงานเป็นไปอย่างมีระบบ และต่อเนื่องสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที

3. ขอบเขต

แผนรับมือฯ ฉบับนี้ ใช้สำหรับรับมือเหตุภัยคุกคามทางไซเบอร์ที่เกิดขึ้นต่อระบบสารสนเทศ และข้อมูลดิจิทัลของกรมปศุสัตว์ รวมถึงบุคคลหรืออุปกรณ์ใดๆ ซึ่งเข้าถึงระบบสารสนเทศ และข้อมูลดิจิทัลดังกล่าว

4. หน้าที่การทบทวนแผน

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กรมปศุสัตว์ มีหน้าที่ทบทวนและขออนุมัติแผนรับมือฯ ฉบับนี้ภายใต้การกำกับตรวจสอบของผู้บริหารสูงสุดหรือผู้ที่รับมอบอำนาจหน่วยงานของท่าน โดยทำการทบทวนปีละ 1 ครั้ง

5. หน้าที่ในการดำเนินการตามแผน

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กรมปศุสัตว์ มีหน้าที่เป็นผู้รับผิดชอบหลักในการดำเนินการตามแผนรับมือฯ นี้

6.เอกสารและกรอบมาตรฐานที่เกี่ยวข้อง

6.1 นโยบายและประมวลแนวปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของกรมปศุสัตว์ พ.ศ.2566

6.2 นโยบายคุ้มครองข้อมูลส่วนบุคคล

6.3 นโยบายด้านความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ของกรมปศุสัตว์

6.4 นโยบายด้านความมั่นคงปลอดภัยไซเบอร์

7. นิยาม

เหตุการณ์ (Event) หมายความว่า เหตุการณ์ที่เกิดขึ้นจากการเฝ้าระวังสังเกตการณ์ (Observable occurrence) ในระบบ เครือข่าย สภาพแวดล้อม กระบวนการ ลำดับการดำเนินการ หรือบุคลากร เหตุการณ์อาจมีหรือไม่มีลักษณะที่ส่งผลเชิงลบก็ได้

เหตุภัยคุกคามทางไซเบอร์ (Cyber incident) หมายความว่า เหตุการณ์ที่มีผลเชิงลบที่เกิดจากการ กระทำหรือการดำเนินการใด ๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

ภัยคุกคามทางไซเบอร์ (Cyber threat) หมายความว่า การกระทำหรือการดำเนินการใด ๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์ โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึง ที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

เหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญ[1] หมายความว่า เหตุภัยคุกคามทางไซเบอร์ที่ปรากฏต่อระบบสารสนเทศ และเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามมาตรา 49 ซึ่งคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติได้กำหนดลักษณะของภัยคุกคามทางไซเบอร์ไว้ตามมาตรา 60 แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562

8. รูปแบบภัยคุกคามไซเบอร์

8.1 ซอฟต์แวร์ประสงค์ร้าย (Malicious Software) หรือมัลแวร์ (Malware) ซึ่งเป็นโปรแกรมที่มีการทำงานที่มุ่งประสงค์ร้ายต่อคอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์

8.2 ไวรัสคอมพิวเตอร์ (Computer Virus) เป็นมัลแวร์ชนิดหนึ่ง ที่สามารถคัดลอกตัวเองติดตั้งตัวเองในเครื่องคอมพิวเตอร์อื่น โดยที่เจ้าของเครื่องคอมพิวเตอร์ไม่อนุญาต ซึ่งไวรัสคอมพิวเตอร์จะแพร่กระจายตัวเองไปสู่เครื่องคอมพิวเตอร์เครื่องอื่นๆ โดยใช้พาหะ เช่น แฟลชไดรว์ติดไวรัส หรือไฟล์คอมพิวเตอร์ติดไวรัส เป็นต้น

[1] เหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญ มีนิยามตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ.2566

8.3 หนอนคอมพิวเตอร์ (Computer Worm) เป็นมัลแวร์ชนิดหนึ่ง สามารถคัดลอกตัวเองติดตั้งตัวเองในเครื่องคอมพิวเตอร์อื่นๆ โดยที่เจ้าของเครื่องคอมพิวเตอร์ไม่อนุญาต โดยหนอนคอมพิวเตอร์จะต่างกับไวรัสตรงที่ไวรัสจะแพร่กระจายตัวเองไปสู่คอมพิวเตอร์เครื่องอื่นๆ โดยอาศัยพาหะ แต่หนอนคอมพิวเตอร์จะใช้วิธีสแกนเครื่องคอมพิวเตอร์ที่อยู่ในระบบเครือข่ายและตรวจหาช่องโหว่ของระบบปฏิบัติการหรือช่องโหว่ของแอพพลิเคชั่น จากนั้นจึงทำการคัดลอกตัวเองเข้าไปฝังตัวโดยใช้ช่องโหว่ดังกล่าว

8.4 ม้าโทรจัน (Trojan Horse) เป็นมัลแวร์ชนิดหนึ่ง ที่มีจุดประสงค์เพื่อบุกรุก เข้าถึง และควบคุมเครื่องคอมพิวเตอร์จากระยะไกล ดำเนินการเปลี่ยนแปลง ทำลายไฟล์ข้อมูลสำคัญ หรือทำการคัดลอกข้อมูลดังกล่าวส่งให้แก่ผู้คุกคามผ่านระบบเครือข่ายอินเทอร์เน็ต ซึ่งข้อมูลสำคัญที่ผู้คุกคามต้องการอาจเป็นชื่อผู้ใช้รหัสผ่าน เลขที่บัญชีธนาคาร และข้อมูลส่วนบุคคลอื่นๆ ลักษณะของการติดตั้งม้าโทรจันจะเหมือนกับไวรัสคอมพิวเตอร์คืออาศัยพาหะ ซึ่งอาจมาจากแฟลชไดรว์ หรือทางอีเมล

8.5 สปายแวร์ (Spyware) เป็นมัลแวร์ชนิดหนึ่งที่มีวัตถุประสงค์เพื่อบันทึกการกระทำของผู้ใช้บนเครื่องคอมพิวเตอร์และส่งผ่านอินเทอร์เน็ตโดยที่ผู้ใช้ไม่ได้รับทราบ โปรแกรมแอบดักข้อมูลนั้นสามารถรวบรวมข้อมูล สถิติการใช้งานจากผู้ใช้ได้หลายอย่างขึ้นอยู่กับการออกแบบของโปรแกรม

8.6 ซอฟต์แวร์เรียกค่าไถ่ (Ransomware) เป็นมัลแวร์ชนิดหนึ่งที่มีพฤติกรรมเข้ารหัสไฟล์ต่างๆ ที่อยู่บนเครื่องคอมพิวเตอร์ไม่ว่าจะเป็นไฟล์เอกสาร รูปภาพ วิดีโอ ผู้ใช้งานจะไม่สามารถเปิดไฟล์ใดๆ ได้เลยหากไฟล์เหล่านั้นถูกเข้ารหัส ซึ่งการถูกเข้ารหัสก็หมายความว่าจะต้องใช้คีย์ในการปลดล็อคเพื่อกู้ข้อมูลคืนมาผู้ใช้งานจะต้องทำการจ่ายเงินตามข้อความ "เรียกค่าไถ่" ที่ปรากฏ

8.7 ประตูหลัง (Backdoor) เป็นช่องทางพิเศษที่ใช้เข้าถึงระบบงานคอมพิวเตอร์โดยที่ไม่ต้องผ่านการพิสูจน์ทราบตัวตน ซึ่งส่วนใหญ่เมื่อผู้บุกรุกสามารถเจาะเข้าระบบได้แล้ว ก็จะสร้างประตูหลังเอาไว้เพื่อใช้ในการบุกรุกเข้าสู่ระบบงานคอมพิวเตอร์ในภายหลัง

8.8 Rootkit เป็นโปรแกรมที่ถูกพัฒนาขึ้นมาเพื่อควบคุมระบบหรือขโมยข้อมูลที่อยู่ในระบบคอมพิวเตอร์ ทั้งนี้นอกจากใช้สำหรับบุกรุกเข้าสู่ระบบงานแล้ว Rootkit ยังอาจใช้เพื่อดูแลหรือตรวจสอบระบบคอมพิวเตอร์ได้ด้วย

8.9 การโจมตีแบบ DoS/DDoS มีจุดประสงค์เพื่อทำให้เครื่องคอมพิวเตอร์แม่ข่าย (Server) หยุดทำงาน หากเครื่องคอมพิวเตอร์ที่โจมตีมีเครื่องเดียว เรียกว่าการโจมตีแบบ Denial of Service (DoS) แต่หากมีเครื่องคอมพิวเตอร์ที่โจมตีมีมากกว่า 1 เครื่องและกระทำพร้อมๆ กัน ไม่ว่าจะโดยตั้งใจหรือไม่ตั้งใจ จะเรียกว่าการโจมตีแบบ Distributed Denial of Service (DDoS)

8.10 Botnet เป็นกลุ่มของอุปกรณ์ที่ติดมัลแวร์และถูกเปลี่ยนเป็น Bot (ย่อมาจาก Robot) ไม่ว่าจะเป็นอุปกรณ์คอมพิวเตอร์ เว็บแคม เราท์เตอร์ หรืออุปกรณ์ IoT อื่นๆ เพื่อรอรับคำสั่งจากผู้บุกรุก (Hacker) โดยผู้บุกรุก (Hacker) จะนำ Botnet ที่มีไปใช้ในการโจมตีขนาดใหญ่เช่นการทำ DDoS เป็นต้น

8.11 Spam Mail หรืออีเมลขยะ เป็นขยะออนไลน์ที่ส่งตรงถึงผู้รับโดยที่ผู้รับสารนั้นไม่ต้องการ และ สร้างความเดือดร้อนรำคาญให้กับผู้รับได้ในลักษณะของการโฆษณาสินค้าหรือบริการการชักชวนเข้าไปยังเว็บไซต์

ต่างๆ ซึ่งอาจมีภัยคุกคามชนิด phishing แฝงเข้ามาด้วย ด้วยเหตุนี้จึงควรติดตั้งระบบ Anti-Spam หรือหากใช้ฟรีอีเมลก็จะมีโปรแกรมคัดกรองอีเมลขยะในชั้นหนึ่งแล้ว

8.12 Phishing คือการหลอกลวงทางอินเทอร์เน็ต เพื่อขอข้อมูลที่สำคัญเช่น รหัสผ่าน หรือหมายเลขบัตรเครดิต โดยการส่งข้อความผ่านทางอีเมลหรือเมสเซนเจอร์ ตัวอย่างของการฟิชชิง เช่น การบอกแก่ผู้รับปลายทางว่าเป็นธนาคารหรือบริษัทที่น่าเชื่อถือ และแจ้งว่ามีสาเหตุทำให้คุณต้องเข้าสู่ระบบ และใส่ข้อมูลที่สำคัญใหม่ โดยเว็บไซต์ที่ลิงก์ไปนั้น จะมีหน้าตาคล้ายคลึงกับเว็บที่กล่าวถึง Phishing

8.13 Sniffing เป็นการดักข้อมูลที่ส่งจากคอมพิวเตอร์เครื่องหนึ่ง ไปยังอีกเครื่องหนึ่ง หรือจากเครือข่ายหนึ่งไปยังอีกเครือข่ายหนึ่งเป็นวิธีการหนึ่งที่ผู้บุกรุกระบบนิยมใช้

8.14 Hacking เป็นการเจาะระบบเครือข่ายคอมพิวเตอร์ไม่ว่าจะกระทำด้วยมนุษย์หรืออาศัยโปรแกรมด้วยวัตถุประสงค์ต่างๆ กัน ทั้งนี้โดยทั่วไปแล้วการ Hacking เป็นสิ่งที่ผิดกฎหมาย แต่อย่างไรก็ตามหากได้รับอนุญาตก็ไม่ใช่สิ่งผิดกฎหมาย โดยตัวอย่างของการ Hacking อย่างถูกกฎหมาย เช่น การเจาะระบบเพื่อประเมินความเสี่ยงของระบบคอมพิวเตอร์ และทดสอบระบบการรักษาความปลอดภัยเครือข่ายขององค์กร

8.15 ผู้บุกรุก (Hacker) หมายถึง ผู้ที่ไม่ได้รับอนุญาตในการใช้งานระบบ แต่พยายามลักลอบเข้ามาใช้งานด้วยวัตถุประสงค์ต่างๆ ไม่ว่าจะเพื่อโจรกรรมข้อมูล ผลกำไร หรือความพอใจส่วนบุคคลก็ตาม ความเสียหายจากผู้บุกรุกเป็นภัยคุกตามที่หนัก

9. การเตรียมความพร้อมในการรับมือปัญหาภัยคุกคามทางไซเบอร์

เพื่อให้กรมปศุสัตว์ มีความพร้อมในการรับมือปัญหาภัยคุกคามทางไซเบอร์ตามที่ระบุในข้อ 8 กรมปศุสัตว์ จะดำเนินการเตรียมความพร้อมในด้านต่างๆ ดังนี้

9.1 การเตรียมพร้อมด้านอุปกรณ์ เพื่อให้ระบบเครือข่ายคอมพิวเตอร์กลางของกรมปศุสัตว์ สามารถรับมือกับภัยคุกคามทางไซเบอร์ได้ กรมปศุสัตว์จึงควรจัดหาอุปกรณ์และซอฟต์แวร์ที่จำเป็นดังนี้

9.1.1 อุปกรณ์ป้องกันระบบเครือข่าย (Next Generation Firewall) ใช้สำหรับป้องกันภัยคุกคามทางไซเบอร์ประเภท DoS/DDoS, Botnet, Phishing, Sniffing, Hacker ทั้งนี้อุปกรณ์ป้องกันระบบเครือข่ายที่จัดหานอกจากความสามารถในการเป็น Firewall แล้วยังต้องมีความสามารถอื่นๆ เพิ่มเติม ซึ่งได้แก่ความสามารถในด้านการตรวจจับการบุกรุก (IPS) ความสามารถในการคัดกรองเว็บไซต์อันตราย (Web Filtering) และ การควบคุมการใช้งานซอฟต์แวร์(Application Control) เป็นอย่างน้อย

9.1.2 ซอฟต์แวร์ตรวจสอบประสิทธิภาพระบบเครือข่าย (Network Monitoring Software) ใช้สำหรับตรวจจับความผิดปกติที่เกิดขึ้นกับระบบเครือข่ายคอมพิวเตอร์กลางของกรมปศุสัตว์

9.1.3 อุปกรณ์ Web App Firewall ใช้สำหรับป้องกันภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับระบบงานคอมพิวเตอร์ของกรมปศุสัตว์ ที่พัฒนาขึ้นมาให้บริการผ่าน Web Browser ได้แก่ การคุกคามทาง ไซเบอร์ประเภท Hacker โดยสามารถป้องกันเทคนิคการบุกรุกเช่น Cross-Site Scripting และ SQL Injection ได้ เป็นอย่างน้อย

9.1.4 ซอฟต์แวร์สำรองข้อมูล ใช้สำหรับกระบวนการสำรองข้อมูล และการกู้ข้อมูลของระบบเครือข่ายคอมพิวเตอร์ของกรมปศุสัตว์

9.1.5 ระบบคลาวด์กลางภาครัฐ GDCC Cloud ใช้ในระดับกรม (Agency Cloud) เพื่อเป็นโครงสร้างพื้นฐานด้านดิจิทัลรองรับหน่วยงานรัฐให้เข้าถึงทรัพยากรด้านคลาวด์ด้วยมาตรฐานสากลระดับ Tier 4 พร้อม SLA 99.99% ซึ่งเป็นไปตามเป้าหมายของกระทรวงดิจิทัลฯ ในการพัฒนาคลังข้อมูลดิจิทัลภาครัฐ และใช้ประโยชน์ Big Data จากคลังข้อมูล ให้สามารถการบูรณาการข้อมูลข้ามหน่วยงานกันได้อย่างเป็นระบบ เพื่อนำสู่การปรับปรุงเพิ่มประสิทธิภาพบริการดิจิทัลให้แก่ประชาชนและเป็นข้อมูลในการพัฒนาประเทศในทุกมิติ

9.1.6 ระบบงานคอมพิวเตอร์สำรอง ใช้ในกรณีที่ไม่สามารถกู้ระบบงานคอมพิวเตอร์ขึ้นมาได้

9.1.7 อุปกรณ์จัดเก็บ Log File ใช้สำหรับจัดเก็บข้อมูลจราจรคอมพิวเตอร์ ที่เกิดขึ้นจากการใช้งานเครือข่ายคอมพิวเตอร์กลางของกรมปศุสัตว์

9.1.8 อุปกรณ์วิเคราะห์ Log File ใช้สำหรับวิเคราะห์ข้อมูลจราจรคอมพิวเตอร์ ที่เกิดขึ้นจากการใช้งานเครือข่ายคอมพิวเตอร์กลางของกรมปศุสัตว์ ซึ่งข้อมูลที่ถูกวิเคราะห์ดังกล่าวจะช่วยระบุถึง หมายเลข IP Address ของผู้โจมตี และลักษณะภัยคุกคามไซเบอร์ที่โจมตีระบบเครือข่ายคอมพิวเตอร์กลางของกรมปศุสัตว์ และใช้ประกอบการทำรายงานให้แก่คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์

9.1.9 ซอฟต์แวร์ป้องกันไวรัสคอมพิวเตอร์แบบคอร์ปอเรต (Corporate Antivirus Software) ใช้สำหรับติดตั้งบนเครื่องคอมพิวเตอร์ (PC) เครื่องคอมพิวเตอร์พกพา (Notebook) และเครื่องคอมพิวเตอร์ แม่ข่ายของกรมปศุสัตว์ ซึ่งสามารถป้องกันภัยคุกคามไซเบอร์ประเภท Malware, Computer Virus, Computer Worm, Trojan, Spyware, Ransomware, Botnet, Spam Mail

9.2แผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้ระบบเครือข่ายคอมพิวเตอร์กลางของกรมปศุสัตว์ สามารถรับมือกับภัยคุกคามทางไซเบอร์ที่มีการพัฒนาขึ้นตลอดเวลา กรมปศุสัตว์จะพิจารณาจ้างบริษัทผู้เชี่ยวชาญในการประเมินความเสี่ยงการรักษาความมั่นคงปลอดภัยไซเบอร์มาตรวจสอบ โดยจะมีจำนวนครั้งในการตรวจสอบอย่างน้อยปีละ 1 ครั้ง ซึ่งในการตรวจสอบและประเมินความเสี่ยงนี้อาจสามารถค้นหาภัยคุกคามไซเบอร์ประเภท Backdoor ที่ถูกซ่อนเอาไว้จากขั้นตอนการพัฒนาระบบงานคอมพิวเตอร์ได้

9.3 การเตรียมพร้อมด้านบุคลากร

9.3.1 การให้ความรู้ เพื่อให้บุคลากรของกรมปศุสัตว์มีความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ กรมปศุสัตว์ จะพิจารณาจ้างบริษัทผู้เชี่ยวชาญในการประเมินความสี่ยงการรักษาความมั่นคงปลอดภัยไซเบอร์ดำเนินการจัดฝึกอบรมให้ความรู้แก่บุคลากรของกรมปศุสัตว์

9.3.2 การแจ้งรายชื่อเจ้าหน้าที่ สำหรับประสานงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามพ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มาตราที่ 46 กำหนดให้หน่วยงานภาครัฐแจ้งรายชื่อเจ้าหน้าที่ระดับบริหารและระดับปฏิบัติการ เพื่อประสานงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ไปยังสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยกรมปศุสัตว์จะกำหนดระดับภัยคุกคามทางไซเบอร์ตามพ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มาตราที่ 60 และจะแจ้งรายชื่อผู้เจ้าหน้าที่เพื่อประสานงานด้านการรักษาความปลอดภัยไซเบอร์ในระดับต่างๆ

9.3.3 มีผู้ดูแลด้านการรักษาความมั่นคงปลอดภัยเครือข่าย และผู้ดูแลระบบเครือข่ายคอมพิวเตอร์กลางของกรมปศุสัตว์

9.4 การเตรียมพร้อมด้านการสำรองข้อมูลและระบบคอมพิวเตอร์สำรอง ในกรณีที่ภัยคุกคามทางไซเบอร์ก่อให้เกิดความเสียหายแก่ระบบเครือข่ายคอมพิวเตอร์กลางของกรมปศุสัตว์อย่างมากจนไม่สามารถทำงานได้เป็นเวลานาน กรมปศุสัตว์จะพิจารณาทางเลือกในการแก้ไขปัญหาโดยวิธีการกู้คืนข้อมูลที่เสียหาย หรือเปิดใช้ระบบคอมพิวเตอร์สำรอง โดยมีเป้าหมายเพื่อให้ระบบเครือข่ายคอมพิวเตอร์กลางของกรมปศุสัตว์ สามารถกลับมาใช้งานได้อย่างรวดเร็วที่สุด ทั้งนี้แนวทางในการกู้คืนข้อมูล และการใช้ระบบคอมพิวเตอร์สำรองจะกำหนดอยู่ในเอกสารแผนสำรองและกู้คืนระบบของกรมปศุสัตว์

10. บทบาทหน้าที่และโครงสร้างทีมรับมือเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์

10.1. ผู้รับแจ้งเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ภายในหน่วยงาน

10.1.1 ผู้รับแจ้งเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์

ลำดับ	ชื่อ นามสกุล	รายละเอียดการติดต่อ	หน้าที่	ความรับผิดชอบ
1	กลุ่มคอมพิวเตอร์และระบบเครือข่าย	0 2653 4444 ต่อ 2342 callcenter_ict @dld.go.th	รับแจ้งเหตุหรือรับรายงานด้านความมั่นคงปลอดภัยไซเบอร์	ประสานงานหน่วยงานภายในและภายนอกกรมปศุสัตว์

10.2 โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber incident Response Team : CIRT)

กรมปศุสัตว์ใช้โมเดลโครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ในลักษณะแบบรวมศูนย์ (Centralize) โดยมีรายชื่อของบุคลากรที่มีความเกี่ยวข้องกับการรับมือเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ พร้อมทั้งโครงสร้างทีมรับมือฯ ดังนี้

ลำดับ	ชื่อ นามสกุล	รายละเอียดการติดต่อ	หน้าที่	ความรับผิดชอบ
1	ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	0 2653 4444 ต่อ 2311 director.ict@dld.go.th	หัวหน้าทีมรับมือฯ (Team manager)	ทำหน้าที่สื่อสารกับผู้บริหารของหน่วยงาน

ลำดับ	ชื่อ นามสกุล	รายละเอียดการติดต่อ	หน้าที่	ความรับผิดชอบ
2	หัวหน้ากลุ่มคอมพิวเตอร์และระบบเครือข่าย (ภาณุตา บุนนาค)	0 2653 4444 ต่อ 2342 08 2022 2422 panuta.b@dld.go.th	รองหัวหน้าทีมรับมือฯ (Deputy team manager)	ทำหน้าที่แทนกรณีหัวหน้าทีมรับมือฯ ไม่อยู่/ไม่สามารถปฏิบัติงานได้
3	เจ้าหน้าที่กลุ่มคอมพิวเตอร์และระบบเครือข่าย (มณีนุช เปลี่ยนศรี)	0 2653 4444 ต่อ 2342 maneenut.p@dld.go.th	เจ้าหน้าที่รับมือฯ (Incident leader)	ทำหน้าที่ช่วยเหลือเจ้าของระบบให้สามารถควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์ได้
4	เจ้าหน้าที่กลุ่มคอมพิวเตอร์และระบบเครือข่าย (วัชรพงศ์ ชื่นพิมลชาญกิจ)	0 2653 4444 ต่อ 2342 watcharaphong.c@dld.go.th	เจ้าหน้าที่เทคนิค (Technical leader)	ทำหน้าที่ให้ความเห็นเกี่ยวกับแนวทางที่เหมาะสมในการควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์ได้
5	เจ้าหน้าที่กลุ่มพัฒนาระบบเทคโนโลยีสารสนเทศ	0 2653 4444 ต่อ 2331	เจ้าหน้าที่ดูแลระบบงานสารสนเทศของกรม	ทำหน้าที่ดูแลระบบให้สามารถทำงานได้

10.3 รายชื่อผู้ประสานงานหน่วยงานในสังกัดกรมปศุสัตว์ (IT Coordinator)

ลำดับ	ชื่อ - นามสกุล	ตำแหน่ง	หน่วยงาน	เบอร์ติดต่อ	e-Mail
1	ณัฐกาญ อารีเอื้อ	เจ้าหน้าที่ระบบงานคอมพิวเตอร์	กองคลัง	1648	finance2@dld.go.th
2	ปัญญา เพชรดีคาย	เจ้าหน้าที่ระบบงานคอมพิวเตอร์	กองคลัง	0 2653 4444 - 1648	finance2@dld.go.th
3	จิรัฐติกร ปารี	เจ้าหน้าที่ระบบงานคอมพิวเตอร์	สำนักกฎหมาย	06 4561 4499	jirattikornnight@gmail.com
4	สิทธิชัย รักษาทรัพย์	เจ้าพนักงานธุรการ	กลุ่มพัฒนาวิชาการปศุสัตว์	1113	Expert@dld.go.th

ลำดับ	ชื่อ - นามสกุล	ตำแหน่ง	หน่วยงาน	เบอร์ติดต่อ	e-Mail
5	คุณานนต์ วงศ์เทศ	นักวิชาการสัตวบาลปฏิบัติการ	สำนักพัฒนาพันธุ์สัตว์ (สพพ.)	06 1924 6650	puresampran@gmail.com
6	นางสาวอัญชลี เจือหอม	นักวิชาการสัตวบาลชำนาญการ	สพพ. (ระบบฐานข้อมูลการปรับปรุงพันธ์สัตว์)	08 7655 9191	Aunchalee.j@dld.go.th
7	นางสาวสิริรัตน์ ถิ่นขนอน	นักวิชาการสัตวบาล		09 1724 1188	Siriratt@dld.go.th
8	นางวโรชา จำปารัตน์	นักวิชาการสัตวบาลชำนาญการพิเศษ	สพพ. (ระบบฐานข้อมูลจีโนมโคไทยบราห์มัน	08 3934 6716	Cwarocha@gmail.com
9	นายกุลภัทร์ โพธิกนิษฐ	นักวิชาการสัตวบาลชำนาญการพิเศษ	สพพ. (ระบบฐานข้อมูลกระบือ (NBIC))	08 9846 2275	buffxlp11@gmail.com
10	ณัฐพงศ์ ผลาชิต	นักวิเคราะห์นโยบายและแผน	กลุ่มพัฒนาวิชาการปศุสัตว์	1131	papond.2527@gmail.com
11	คชากร เครือสามสุม	นักวิชาการคอมพิวเตอร์	กองสวัสดิภาพสัตว์และสัตวแพทย์บริการ	08 7542 4552	kkhachagon@gmail.com
12	อินทิรา น้อยแสง	เจ้าหน้าที่ระบบงานคอมพิวเตอร์	สำนักงานปศุสัตว์เขต 1	08 6988 8372	r1.strategy@dld.go.th
13	ฮัสนะ ประสานวงษ์	นักวิเคราะห์นโยบายและแผน	สำนักควบคุม ป้องกันและบำบัดโรคสัตว์	08 6321 4258	dcontrol@dld.go.th
14	สราวุฒิ สร้อยสังวาลย์	เจ้าพนักงานธุรการชำนาญงาน	กลุ่มพัฒนาระบบบริหาร	09 1976 5596	manage@dld.go.th
15	พัฒนพงศ์ วรวิชญาวิวัฒน์	เจ้าพนักงานธุรการ	กองส่งเสริมและพัฒนาการปศุสัตว์	06 5543 6614 (เบอร์ภายใน 3316)	pathanapong1975@gmail.com
16	กิติศักดิ์ กลิ่นทอง	นักวิชาการสัตวบาลชำนาญการ	กองควบคุมอาหารและยาสัตว์	08 9487 8884	kitisak.k@dld.go.th
17	รัฐสินธุ์ วัฒโนภาสศิริ	นักวิเคราะห์นโยบายและแผน	กองแผนงาน	09 4485 5586	Planning_mtr@dld.go.th
18	มนฤทัย แสงศิริ	นักวิเคราะห์นโยบายและแผน	กองแผนงาน	08 6933 8956	s.monruthai27@gmail.com
19	พีรภัทร ธานีรัตน์	นักจัดการงานทั่วไป	สำนักงานเลขานุการกรม	08 9761 7524	perapatt1995@gmail.com

ลำดับ	ชื่อ - นามสกุล	ตำแหน่ง	หน่วยงาน	เบอร์ติดต่อ	e-Mail
20	วสุวัฒน์ คงเมือง	นักวิชาการคอมพิวเตอร์	สถาบันสุขภาพสัตว์แห่งชาติ	08 9772 9221	wasuwat2007@gmail.com
21	ยุทธพิชัย นิจประพันธ์	เจ้าหน้าที่ระบบงานคอมพิวเตอร์	กองการเจ้าหน้าที่	0 2653 4444 ต่อ 2113	person@dld.go.th
22	สิริพงศ์ สุขถาวรเจริญพร	นายสัตวแพทย์ชำนาญการพิเศษ	สำนักตรวจสอบคุณภาพสินค้าปศุสัตว์	08 6674 7899	sirisuk2522@gmail.com
23	พิตตินันท์ ปัญญาศิริ	นักจัดการงานทั่วไป	กองความร่วมมือด้านการปศุสัตว์ระหว่างประเทศ	1353	khunman12@gmail.com
24	ชัยรัตน์ เอียดเมือง	วิศวกร	สำนักพัฒนาระบบและรับรองมาตรฐานสินค้าปศุสัตว์	0 2653 4444 ต่อ 3114	blsccertify@gmail.com
25	ณัฐธวิทย์ วงษ์ทน	นักจัดการงานทั่วไป	กองผลิตภัณฑ์ปศุสัตว์	09 6305 3482	Samutchaparty@gmail.com
26	วรพจน์ แก้วเจริญ	นักวิชาการตรวจสอบภายในปฏิบัติการ	กลุ่มตรวจสอบภายใน	0 2653 4444 ต่อ 1212-1213	tarn.tantoktok@gmail.com
27	อานุภาพ เส็งสาย	ผู้เชี่ยวชาญด้านอาหารสัตว์กระเพาะเดี่ยว	สำนักพัฒนาอาหารสัตว์	08 1456 2561	nuphab@gmail.com
28	ปาลินี ผลประเสริฐ	พนักงานผู้ช่วยสัตวบาล	กองงานพระราชดำริและกิจกรรมพิเศษ	06 2598 6618	drasa1@dld.go.th
29	บัณฑิต มีโชคสม	เจ้าหน้าที่ระบบงานคอมพิวเตอร์	สำนักเทคโนโลยีชีวภัณฑ์สัตว์	08 6726 4295	biologic@dld.go.th
30	ปรีดา บุญประถัมภ์	นักจัดการงานทั่วไป	กองสารวัตรและกักกัน	08 6331 7386	aqidata@dld.go.th
31	ไชยันต์ เดือนขาว	เจ้าพนักงานสัตวบาล	สำนักเทคโนโลยีชีวภาพการผลิตปศุสัตว์	09 9075 3203	chaiyunpooh6@gmail.com
32	กล้าณรงค์ แท่งทอง	นักวิชาการคอมพิวเตอร์	สำนักเทคโนโลยีชีวภาพการผลิตปศุสัตว์	08 6986 6861	klanarong.t@dld.go.th

10.4 หน่วยงานภายนอกที่เกี่ยวข้อง

ข้อมูลติดต่อสื่อสารของหน่วยงานภายนอกที่เกี่ยวข้อง เช่น สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.), สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.), THAI-CERT และผู้ให้บริการภายนอกของหน่วยงาน

ลำดับ	หน่วยงาน	ชื่อผู้ประสานงาน	เบอร์ติดต่อ	e-Mail	ความเกี่ยวข้อง
1	สำนักงาน คณะกรรมการ การรักษาความ มั่นคงปลอดภัย ไซเบอร์แห่งชาติ (สกมช.)		0 2114 3531	thaicert@ncsa.or.th	แจ้งเหตุภัย คุกคาม ไซเบอร์
2	สำนักงาน คณะกรรมการ คุ้มครองข้อมูล ส่วนบุคคล (สคส.)		0 2111 8800	saraban@pdpc.or.th	แจ้งเหตุการ ละเมิดข้อมูลส่วน บุคคล
3	ศูนย์ประสานการ รักษาความมั่นคง ปลอดภัยระบบ คอมพิวเตอร์แห่งชาติ THAICERT)		0 2142 6888	thaicert@ncsa.or.th	แจ้งเหตุภัย คุกคาม ไซเบอร์
4	บริษัท โทรคมนาคม แห่งชาติ จำกัด (มหาชน)		NT Contact Center 1888	1888@ntplc.co.th	บริษัทคู่สัญญา ให้บริการ เครือข่าย อินเทอร์เน็ต
5	บริษัท โทรคมนาคม แห่งชาติ จำกัด (มหาชน) (NT Data Center NTDC))	1.นายปพิชญ์ภูมิ สุขเกษม 2.นางสาวอรพรรณ มงคลเกิด 3.นายกิตติพงศ์ พรรคพล	08 6326 7176 09 7264 2941 09 5480 8996 0 2104 3039 0 2104 4013	papitpoom.s@ntplc.co.th oraphan.m@innovationssolution.com kittipong.p@innovationssolution.com government_	บริษัทคู่สัญญา ให้บริการดูแล ระบบ Data Center

ลำดับ	หน่วยงาน	ชื่อผู้ประสานงาน	เบอร์ติดต่อ	e-Mail	ความเกี่ยวข้อง
				cust@ntplc.co.th	
6	บริษัท เอ็นพีร่า จำกัด	นางสาวสิรีทร อึ้งรัตนกล้าแข็ง	0 2977 9500 09 3596 8224	sireethorn@npera.co.th	บริษัทคู่สัญญาให้บริการดูแลระบบเครือข่าย กรมปศุสัตว์พญาไท
7	บริษัท เน็กซ์เทค เอเชีย จำกัด	คุณหทัยรัตน์ สอนซุน	0 2150 2740 08 9323 4567	support@nextech-asia.com	บริษัทคู่สัญญาให้บริการดูแลระบบเครือข่าย กรมปศุสัตว์ ปทุมธานี
8	บริษัท โกลบอล เทคโนโลยีอินทิเกรเทด จำกัด	นายณัฐพงศ์ วานิชชินชัย	08 2441 4641	nuttapong.v@outlook.com	บริษัทคู่สัญญาให้บริการดูแลระบบ e - Operation
9	บริษัท จันวาณิชย์ จำกัด	คุณคุณลสิดา ต่ายเพ็ชร์	06 1031 2155	helpdeskcwn.bu8@chanwanich.digital Line : @405pyvwc LINE : Pattorowadee.p May	บริษัทคู่สัญญาให้บริการดูแลระบบ Televet
10	บริษัท มาสเตอ เมกเคอ จำกัด	คุณพิทยา ดวงผล คุณปุริม นิลพรหม	08 3115 7524 (Hw) 08 7316 9810 (Sw) 08 7769 2522 08 4701 4321	service@mastermakerth.com pitthaya.d@zealtechinter.com purim.n@zealtechinter.com	บริษัทคู่สัญญาให้บริการดูแลระบบงานต่างๆ ภายในกรม
11	บริษัท ไอแมกซ์ โซลูชั่นส์ จำกัด	นายชาญศักดิ์ เจริญจารุวงศ์	0 2794 3106 09 8989 7255	chansak@imaxxsol.com	บริษัทคู่สัญญาให้บริการดูแลระบบ e-Breeding
12	บริษัท คนดีไซน์ ซอฟท์เทค โซลูชั่นส์ จำกัด	นายผาสุข เลิศบัวบาน	08 3934 6716	kondesign.team@gmail.com	บริษัทคู่สัญญาให้บริการดูแลระบบ

ลำดับ	หน่วยงาน	ชื่อผู้ประสานงาน	เบอร์ติดต่อ	e-Mail	ความเกี่ยวข้อง
					ฐานข้อมูลจีโนมโคไทยบราห์มัน
13	บริษัท เอ็นวาย โค้ดดิ้ง จำกัด	นายภาณุวัฒน์ สุขทัศน์	08 6504 9717	panuwat.std@gmail.com	บริษัทคู่สัญญาให้บริการดูแลระบบฐานข้อมูลกระบือ (NBIC)
14	บริษัท เอ็กซ์เซลลิ้งค์ จำกัด	นางสาววรัญชน์พร ศิริพัชรมนต์	09 5569 4414	warunporn@excelink .co.th	บริษัทคู่สัญญาให้บริการดูแลระบบ
15	บริษัท พายซอฟท์ จำกัด	คุณเยาวภา นาคใหม่	06 1225 4599 0 2123 8900		บริษัทคู่สัญญาให้บริการดูแลระบบ

10.5 โครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure)

เพื่อให้การดำเนินการรับมือเหตุภัยคุกคามทางไซเบอร์ สามารถนำไปปฏิบัติได้อย่างมีประสิทธิภาพ จะต้องกำหนดโครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ โดยแต่ละตำแหน่งจะต้องร่วมมือติดตาม ปฏิบัติงาน ตามบทบาทที่กำหนดไว้

ภาพที่ 1 แสดงโครงสร้างการรายงานเหตุภัยคุกคามทางไซเบอร์

*CISO เป็นผู้บริหารระดับสูงที่ดูแลด้านความปลอดภัยของข้อมูล ระบบไซเบอร์และเทคโนโลยีของกรม

ลำดับขั้นตอนการรายงานเหตุการณ์

ลำดับ	ผู้รับบทบาท	สิ่งที่ต้องทำ
1. ผู้พบเหตุ	พนักงาน/เจ้าหน้าที่ประสานงานคอมพิวเตอร์ของหน่วยงาน	หยุดการแพร่กระจาย: ถอดสายแลน/ปิด Wi-Fi ของเครื่องที่สงสัย และแจ้ง IT ทันที
2. ด่านหน้า	เจ้าหน้าที่กลุ่มคอมพิวเตอร์ Technical Lead	คัดกรอง: ยืนยันว่าเป็นภัยคุกคามจริงหรือไม่ (False Positive check) และบันทึกเวลาที่เกิด
3. ทีมเทคนิค	เจ้าหน้าที่กลุ่มคอมพิวเตอร์ฯ Incident Leader	วิเคราะห์: ประเมินความรุนแรง แยกแยะประเภท (เช่น Ransomware, Phishing, Data Leak)
4. ผู้บริหาร	CISO/Team manager /Deputy Team	ตัดสินใจ: ประเมินผลกระทบต่อธุรกิจ และพิจารณาประกาศภาวะฉุกเฉิน
5. หน่วยงานภายนอก	ThaiCERT/ สกมช./สคส.	รายงานตามกฎหมาย: แจ้งเหตุต่อหน่วยงานกำกับดูแล (หากเข้าเงื่อนไขตาม พ.ร.บ. ไซเบอร์ฯ)

11. ขั้นตอนการรับมือ

แผนรับมือฯ ฉบับนี้ ประกอบด้วยขั้นตอนการรับมือเหตุภัยคุกคามทางไซเบอร์ตามข้อ 19.1 ในประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ.2564, ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. 2564 และประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ.2566 รวมถึง นโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของกรมปศุสัตว์ ดังนี้

11.1 ขั้นตอนการเตรียมการ (Preparation)

กรมปศุสัตว์ดำเนินมาตรการเพื่อเตรียมการและป้องกันการเกิดภัยคุกคามทางไซเบอร์ (Preparation) เพื่อเตรียมความพร้อมเมื่อต้องเผชิญเหตุ ได้แก่ การจัดเตรียมข้อมูลให้พร้อม การจัดตั้งและฝึกอบรมบุคลากรหรือทีมงาน การจัดหาเครื่องมือและทรัพยากรต่าง ๆ ที่จำเป็น การตั้งค่าระบบต่าง ๆ ให้ปลอดภัย การจัดทำนโยบายแผนงาน และกระบวนการที่เกี่ยวข้อง รวมถึง การสร้างเครือข่ายความร่วมมือ โดยดำเนินการดังต่อไปนี้

(1) กำหนดโครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT) รายละเอียดปรากฏตามข้อ 10.2

(2) กำหนดโครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure) รายละเอียดปรากฏตามข้อ 10.4

(3) กำหนดเกณฑ์และขั้นตอนในการเรียกใช้งาน (Activate) การตอบสนองต่อเหตุการณ์ และการติดต่อไปยังหน่วยงาน CIRT ต่าง ๆ

(4) จัดเตรียมข้อมูลและอุปกรณ์ รวมถึงช่องทางในการติดต่อสื่อสารที่จำเป็น เช่น ข้อมูลการติดต่อและอุปกรณ์ติดต่อสื่อสารของบุคลากร, กลไกรายงานเหตุการณ์, ห้องประชุม War room เป็นต้น

(5) จัดเตรียมอุปกรณ์, ซอฟต์แวร์ และแหล่งข้อมูลสำหรับวิเคราะห์เหตุภัยคุกคามทางไซเบอร์

(6) จัดให้มีการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน (Risk Assessment)

(7) จัดทำแผนผังโครงสร้างขั้นตอนการรับมือฯ ของหน่วยงาน โดยหน่วยงานอาจดูตัวอย่างการจัดทำแผนผังโครงสร้างขั้นตอนการรับมือฯ ได้ (รายละเอียดปรากฏตามภาคผนวก 1)

นอกจากนี้ กรมปศุสัตว์ได้พิจารณาดำเนินการตามเอกสารแนบท้าย 2 ตารางที่ 2.1 ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. 2564 เพิ่มเติม

11.2 ขั้นตอนการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (Detection and Analysis)

กรมปศุสัตว์ดำเนินการในการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ ซึ่งเป็นสิ่งจำเป็นที่ช่วยบรรเทาความเสี่ยงที่ยังคงเหลืออยู่ และสามารถแจ้งเตือนได้อย่างทันท่วงทีเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น โดยดำเนินการดังต่อไปนี้

(1) ดำเนินการจัดเตรียมแนวทางรับมือเมื่อเกิดการโจมตีรูปแบบทั่วไปที่เคยเกิดขึ้น หรืออาจเกิดขึ้นกับหน่วยงาน โดยรูปแบบการโจมตีที่ควรจัดเตรียมแนวทางรับมือไว้นั้น อาจพิจารณาได้จาก Attack Vector ที่หน่วยงานมี เช่น มีการอนุญาตให้ใช้งานอุปกรณ์แบบถอดได้ (External/Removable Media) ซึ่งมีความเสี่ยงต่อการเผยแพร่มัลแวร์ หรือมีการให้บริการเว็บไซต์ที่เสี่ยงต่อการโจมตีแบบ Cross-site scripting เป็นต้น

(2) ดำเนินการจัดให้มีกลไกที่สามารถตรวจจับสิ่งบ่งชี้หรือลักษณะเบื้องต้นของการเกิดภัยคุกคามทางไซเบอร์ได้ในเวลาอันเหมาะสม โดยอาจอาศัยข้อมูลจากแหล่งข้อมูลต่าง ๆ เช่น ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เป็นต้น

(3) ดำเนินการจัดให้มีแนวทางในการวิเคราะห์ผลกระทบและระดับของภัยคุกคามทางไซเบอร์ (Incident Prioritization) เพื่อรับมือกับภัยคุกคามทางไซเบอร์ให้ทันท่วงที โดยพิจารณาปัจจัยต่าง ๆ ที่เกี่ยวข้องเช่น ผลกระทบต่อการทำงานของระบบ (Functional impact) ผลกระทบต่อข้อมูล (Information impact) และความสามารถในการกู้คืน (Recoverability effort)[2] เป็นต้น

[2] หน่วยงานอาจพิจารณากำหนดระดับความรุนแรงภัยคุกคามออกเป็น 3 ประเภท โดยศึกษาเพิ่มเติมได้ที่ NIST SP 800-61r2 ข้อที่ 3.2.6 หน้าที่ 32

ตารางที่ 1 ตัวอย่างเกณฑ์การประเมินระดับของภัยคุกคามของหน่วยงาน

ความรุนแรง	คำอธิบาย	การตอบสนองต่อเหตุการณ์
ต่ำ (Low)	ส่งผลกระทบต่อหน่วยงานในวงจำกัด เช่น เกิดการหยุดชะงักของการให้บริการเล็กน้อย หรือกระทบแค่หน่วยงานเดียว สามารถกู้คืนโดยใช้ทรัพยากรที่มีได้ ความเสียหายทางการเงินต่ำ ไม่ส่งผลกระทบต่อชื่อเสียงหรือความเชื่อมั่นของสาธารณะ หรือไม่เกี่ยวข้องกับการรายงานต่อหน่วยงานด้านกฎหมายหรือหน่วยงานกำกับดูแล	แก้ไขภายใน 72 ชั่วโมง
ปานกลาง (Medium)	ส่งผลกระทบต่อหน่วยงานในระดับปานกลาง เช่น เกิดการหยุดชะงักของการให้บริการที่ยาวนานขึ้น กระทบหลายหน่วยงาน สามารถกู้คืนได้แต่ต้องมีการจัดหาทรัพยากรเพิ่ม มีความเสียหายทางการเงินมากขึ้น เริ่มส่งผลกระทบต่อชื่อเสียงและความเชื่อมั่นของสาธารณะ หรือเกี่ยวข้องกับการรายงานต่อหน่วยงานด้านกฎหมายหรือหน่วยงานกำกับดูแลในระดับไม่ร้ายแรง	แก้ไขภายใน 48 ชั่วโมง
สูง (High)	ส่งผลกระทบอย่างมากต่อหน่วยงาน เช่น ระบบสารสนเทศบางส่วนถูกทำลาย การดำเนินงานหยุดชะงักอย่างมากในช่วงเวลาหนึ่ง เวลาในการกู้คืนไม่สามารถคาดการณ์ได้ ต้องใช้ทรัพยากรและความช่วยเหลือจากภายนอก ข้อมูลสำคัญจำนวนมากสูญหาย ความเสียหายทางการเงินสูง ส่งผลกระทบอย่างมากต่อชื่อเสียงและความเชื่อมั่นของสาธารณะ หรือเกี่ยวข้องกับการรายงานต่อหน่วยงานด้านกฎหมายหรือหน่วยงานกำกับดูแลในระดับร้ายแรง	แก้ไขภายใน 24 ชั่วโมง
สูงมาก (Extreme)	ส่งผลกระทบอย่างร้ายแรงต่อหน่วยงาน เช่น มีภัยคุกคามต่อชีวิต ระบบสารสนเทศหลักถูกทำลาย การดำเนินงานทั้งหมดหยุดชะงักจนต้องปิดการให้บริการ ไม่สามารถทำการกู้คืนได้ ข้อมูลสำคัญจำนวนมากสูญหายและถูกนำไปเผยแพร่ต่อสาธารณะ ความเสียหายทางการเงินสูงมาก ส่งผลกระทบอย่างรุนแรงต่อชื่อเสียงและความเชื่อมั่นของสาธารณะ หรือเกี่ยวข้องกับการรายงานต่อหน่วยงานด้านกฎหมายหรือหน่วยงานกำกับดูแลในระดับวิกฤติ	แก้ไขภายใน 4 ชั่วโมง

ตารางเปรียบเทียบระดับความรุนแรงของภัยคุกคามที่หน่วยงานกำหนด กับลักษณะของภัยคุกคามทางไซเบอร์ตามมาตรา 60 แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

หน่วยงานกำหนด		**ตามมาตรา 60**		**การตอบสนองต่อเหตุการณ์**
ความรุนแรง	**คำอธิบาย**	**ลักษณะ**	**คำอธิบาย**	
ต่ำ (Low)	ส่งผลกระทบต่อหน่วยงานในวงจำกัด เช่น เกิดการหยุดชะงักของการให้บริการเล็กน้อย หรือกระทบแค่หน่วยงานเดียว สามารถกู้คืนโดยใช้ทรัพยากรที่มีได้ ความเสียหายทางการเงินต่ำ ไม่ส่งผลกระทบต่อชื่อเสียงหรือความเชื่อมั่นของสาธารณะ หรือไม่เกี่ยวข้องกับการรายงานต่อหน่วยงานด้านกฎหมายหรือหน่วยงานกำกับดูแล	ไม่ร้ายแรง	ภัยคุกคามทางไซเบอร์ที่มีความเสี่ยงอย่างมีนัยสำคัญถึงระดับที่ทำให้ระบบคอมพิวเตอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศหรือการให้บริการของรัฐด้อยประสิทธิภาพลง	แก้ไขภายใน 72 ชั่วโมง
ปานกลาง (Medium)	ส่งผลกระทบต่อหน่วยงานในระดับปานกลาง เช่น เกิดการหยุดชะงักของการให้บริการที่ยาวนานขึ้น กระทบหลายหน่วยงาน สามารถกู้คืนได้แต่ต้องมีการจัดหาทรัพยากรเพิ่ม มีความเสียหายทางการเงินมากขึ้น เริ่มส่งผลกระทบต่อชื่อเสียงและความเชื่อมั่นของสาธารณะ หรือเกี่ยวข้องกับการรายงานต่อหน่วยงานด้านกฎหมายหรือหน่วยงานกำกับดูแลในระดับไม่ร้ายแรง			แก้ไขภายใน 48 ชั่วโมง
สูง (High)	ส่งผลกระทบอย่างมากต่อหน่วยงาน เช่น ระบบสารสนเทศบางส่วนถูกทำลาย การดำเนินงานหยุดชะงักอย่างมากในช่วงเวลาหนึ่ง เวลาในการกู้คืนไม่สามารถคาดการณ์ได้ ต้องใช้ทรัพยากรและความช่วยเหลือจากภายนอก ข้อมูลสำคัญจำนวนมากสูญหาย ความเสียหายทางการเงินสูง ส่งผลกระทบอย่างมากต่อชื่อเสียง	ร้ายแรง	ภัยคุกคามที่มีลักษณะการเพิ่มขึ้นอย่างมีนัยสำคัญของการโจมตีระบบคอมพิวเตอร์ คอมพิวเตอร์ หรือข้อมูลคอมพิวเตอร์ โดยมุ่งหมายเพื่อโจมตีโครงสร้างพื้นฐานสำคัญของประเทศและการโจมตีดังกล่าวมีผลทำให้ระบบคอมพิวเตอร์หรือโครงสร้างสำคัญทางสารสนเทศที่เกี่ยวข้องกับการให้บริการของ	แก้ไขภายใน 24 ชั่วโมง

หน่วยงานกำหนด		ตามมาตรา 60		การตอบสนองต่อเหตุการณ์
ความรุนแรง	คำอธิบาย	ลักษณะ	คำอธิบาย	
	และความเชื่อมั่นของสาธารณะ หรือเกี่ยวข้องกับการรายงานต่อหน่วยงานด้านกฎหมายหรือหน่วยงานกำกับดูแลในระดับร้ายแรง		โครงสร้างพื้นฐานสำคัญของประเทศ ความมั่นคงของรัฐ ความสัมพันธ์ระหว่างประเทศ การป้องกันประเทศ เศรษฐกิจ การสาธารณสุข	
สูงมาก (Extreme)	ส่งผลกระทบอย่างร้ายแรงต่อหน่วยงาน เช่น มีภัยคุกคามต่อชีวิต ระบบสารสนเทศหลักถูกทำลาย การดำเนินงานทั้งหมดหยุดชะงักจนต้องปิดการให้บริการ ไม่สามารถทำการกู้คืนได้ ข้อมูลสำคัญจำนวนมากสูญหายและถูกนำไปเผยแพร่ต่อสาธารณะ ความเสียหายทางการเงินสูงมาก ส่งผลกระทบอย่างรุนแรงต่อชื่อเสียงและความเชื่อมั่นของสาธารณะ หรือเกี่ยวข้องกับการรายงานต่อหน่วยงานด้านกฎหมายหรือหน่วยงานกำกับดูแลในระดับวิกฤติ	วิกฤติ	- เป็นภัยคุกคามทางไซเบอร์ที่เกิดจากการโจมตีระบบคอมพิวเตอร์ คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ในระดับที่สูงขึ้นกว่าภัยคุกคามทางไซเบอร์ในระดับร้ายแรง โดยส่งผลกระทบรุนแรง ต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศในลักษณะที่เป็นวงกว้าง จนทำให้การทำงานของหน่วยงานรัฐหรือการให้บริการของโครงสร้างพื้นฐานสำคัญของประเทศที่ให้กับประชาชนล้มเหลวทั้งระบบจนรัฐไม่สามารถควบคุมการทำงานส่วนกลางของระบบคอมพิวเตอร์ของรัฐได้ หรือการใช้มาตรการเยียวยาตามปกติในการแก้ไขปัญหาภัยคุกคามไม่สามารถแก้ไขปัญหาได้ และมีความเสี่ยงที่จะลุกลามไปยังโครงสร้างพื้นฐานสำคัญอื่น ๆ ของประเทศ ซึ่งอาจมีผลทำให้บุคคลจำนวนมากเสียชีวิตหรือระบบคอมพิวเตอร์ คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์จำนวนมากถูกทำลายเป็นวงกว้างในระดับประเทศ - เป็นภัยคุกคามทางไซเบอร์อันกระทบหรืออาจกระทบต่อความสงบเรียบร้อยของประชาชนหรือ	แก้ไขภายใน 4 ชั่วโมง

หน่วยงานกำหนด		ตามมาตรา 60		การตอบสนองต่อเหตุการณ์
ความรุนแรง	คำอธิบาย	ลักษณะ	คำอธิบาย	
			เป็นภัยต่อความมั่นคงของรัฐหรืออาจทำให้ประเทศหรือส่วนใดส่วนหนึ่งของประเทศตกอยู่ในภาวะคับขันหรือมีการกระทำความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา การรบหรือการสงคราม ซึ่งจำเป็นต้องมีมาตรการเร่งด่วนเพื่อรักษาไว้ซึ่งการปกครองระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุขตามรัฐธรรมนูญแห่งราชอาณาจักรไทย เอกราชและบูรณภาพแห่งอาณาเขตผลประโยชน์ของชาติ การปฏิบัติตามกฎหมาย ความปลอดภัยของประชาชน การดำรงชีวิตโดยปกติสุขของประชาชน การคุ้มครองสิทธิเสรีภาพ ความสงบเรียบร้อยหรือประโยชน์ส่วนรวม หรือการป้องปัดหรือแก้ไขเยียวยาความเสียหายจากภัยพิบัติสาธารณะอันมีมาอย่างฉุกเฉินและร้ายแรง	

(4) ดำเนินการจัดให้มีบันทึกรายงานสถานการณ์เหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ โดยอาจกำหนดให้มีรายละเอียดตามแบบฟอร์มตัวอย่าง (รายละเอียดปรากฏตามภาคผนวก 2)

(5) จัดให้มีการจัดทำบันทึกข้อมูลกิจกรรมเหตุการณ์ความปลอดภัยทางไซเบอร์ (Incident Documentation) โดยหน่วยงานควรบันทึกข้อมูลเกี่ยวกับเหตุการณ์ความปลอดภัยทางไซเบอร์ทุกขั้นตอน ตั้งแต่ตรวจพบเหตุการณ์จนถึงกระบวนการสุดท้าย และข้อมูลดังกล่าวควรระบุรายละเอียดพร้อมเวลาที่เกิดเหตุ ตลอดถึงระยะเวลาที่ใช้ระงับเหตุด้วย ทั้งนี้ ควรบันทึกข้อมูลดังกล่าวที่เกี่ยวข้องกับเหตุการณ์ โดยระบุวันที่และลงนามโดยผู้มีหน้าที่จัดการรับมือเหตุการณ์นั้น ๆ เพื่อให้มั่นใจได้ว่าเหตุการณ์ความปลอดภัยทางไซเบอร์ที่เกิดขึ้นจะได้รับการจัดการแก้ไขภายในระยะเวลาที่เหมาะสม โดยอาจกำหนดให้มีรายละเอียดตามแบบฟอร์มตัวอย่าง (รายละเอียดปรากฏตามภาคผนวก 3)

(6) จัดให้มีการรายงานภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับบริการของโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้ผู้ที่เกี่ยวข้องทราบตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ.2566 ดังนี้

(ก) กรณีมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นกับหน่วยงานรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศตาม ข้อ 4 แห่งประกาศฯ ฉบับดังกล่าว ให้ใช้เอกสาร ก1 โดยใช้แบบฟอร์มการแจ้งตามกฎหมาย หรือนำส่งข้อมูลที่มีรายละเอียดเทียบเท่ากับเอกสาร ก1 (รายละเอียดปรากฏตามภาคผนวก 4) การส่งข้อมูลจะต้องส่งผ่านช่องทางที่มีความมั่นคงปลอดภัย มีการเข้ารหัสของข้อมูลที่เหมาะสม และส่งผ่านช่องทางที่สำนักงานกำหนด

(ข) กรณีมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญต่อระบบของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศกับหน่วยงานรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศตาม ข้อ 5 แห่งประกาศฯ ฉบับดังกล่าว ให้ใช้เอกสาร ก2 รายงานไปยัง สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ภายในระยะเวลา 24 ชั่วโมง โดยใช้แบบฟอร์มการรายงานตามกฎหมาย (รายละเอียดปรากฏตามภาคผนวก 4) การส่งข้อมูลจะต้องส่งผ่านช่องทางที่มีความมั่นคงปลอดภัย มีการเข้ารหัสของข้อมูลที่เหมาะสม และส่งผ่านช่องทางที่สำนักงานกำหนด

(ค) หน่วยงานของรัฐหรือหน่วยงานควบคุมหรือกำกับดูแล จะต้องจัดทำและส่งรายงานสรุปจำนวนเหตุภัยคุกคามทางไซเบอร์ทั้งหมดที่ได้เกิดขึ้นกับข้อมูลหรือระบบสารสนเทศของหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ภายใต้การควบคุมหรือกำกับดูแลของตนในแต่ละปี ภายในวันที่ 31 มกราคม ของปีถัดไป ให้แก่สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ โดยให้แยกสถิติหมวดหมู่ตามแบบที่กำหนดในเอกสาร ก3 โดยใช้แบบฟอร์มการรายงานตามกฎหมาย (รายละเอียดปรากฏตามภาคผนวก 4) การส่งข้อมูลจะต้องส่งผ่านช่องทางที่มีความมั่นคงปลอดภัย มีการเข้ารหัสของข้อมูลที่เหมาะสม และส่งผ่านช่องทางที่สำนักงานกำหนด

นอกจากนี้ กรมปศุสัตว์ได้พิจารณาดำเนินการตามเอกสารแนบท้าย 2 ตารางที่ 2.2 ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. 2564 เพิ่มเติม

11.3 ขั้นตอนการระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ (containment, eradication, and recovery)

กรมปศุสัตว์ได้ดำเนินการเพื่อระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคาม ทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ โดยควรกำหนดให้สอดคล้องกับความรุนแรงและระดับของภัยคุกคามทางไซ

เบอร์แต่ละระดับจนกระทั่งสามารถกู้คืนทรัพย์สินสำคัญทางสารสนเทศให้กลับมาดำเนินงานหรือให้บริการได้ตามปกติ ซึ่งการดำเนินการในขั้นตอนนี้อาจจะต้องกระทำควบคู่ไปกับการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ที่ อาจมีการลุกลามหรือทวีความรุนแรงมากขึ้นเพื่อให้การระงับและการปราบปรามภัยคุกคามทางไซเบอร์ ตลอดจนการฟื้นฟูระบบงานที่ได้รับผลกระทบจากการเกิดภัยคุกคามทางไซเบอร์ สอดคล้องกับสถานการณ์ที่เปลี่ยนแปลงไป โดยดำเนินการดังต่อไปนี้

(1) จำกัดขอบเขต (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

(2) เรียกใช้งานกระบวนการกู้คืน (Recovery Process)

(3) ดำเนินการสอบสวน (Investigate) สาเหตุและผลกระทบของเหตุการณ์

(4) เก็บรักษาหลักฐาน (Preservation of Evidence) ก่อนเริ่มกระบวนการกู้คืนซึ่งรวมถึงการได้มาของบันทึกการยึดหลักฐานคอมพิวเตอร์ที่ได้มา หรืออุปกรณ์อื่น ๆ เพื่อสนับสนุนการสอบสวน

(5) ดำเนินการตามระเบียบวิธีการมีส่วนร่วม (Engagement Protocols) กับบุคคลภายนอก หรือแนวปฏิบัติการบริหารจัดการบุคคลภายนอก ซึ่งรวมถึงรายละเอียดการติดต่อ ตัวอย่างเช่น ผู้ให้บริการด้านนิติวิทยาศาสตร์/การกู้คืนและการบังคับใช้กฎหมายเพื่อดำเนินคดี

นอกจากนี้ หน่วยงานควรพิจารณาดำเนินการตามเอกสารแนบท้าย 2 ตารางที่ 2.3 ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. 2564 เพิ่มเติม

<u>11.4 ขั้นตอนการดำเนินการภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ (Post-Incident activity)</u>

กรมปศุสัตว์มีการกำหนดขั้นตอน วิธี ปฏิบัติ หรือกำหนดนโยบายภายในที่เกี่ยวข้องเพื่อให้มีแนวทางที่ชัดเจน ซึ่งการปฏิบัติตามมาตรการดังกล่าว จะช่วยให้หน่วยงานสามารถเรียนรู้จากเหตุภัยคุกคามทางไซเบอร์ที่ผ่านมา และสามารถหาแนวทางเพื่อแก้ไข จุดบกพร่องและพัฒนาแนวทางรับมือกับภัยคุกคามทางไซเบอร์ต่อไปในอนาคต นอกจากนี้หน่วยงานต้องเก็บ รักษาข้อมูลและพยานหลักฐานที่จำเป็น เพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์ หรือใช้ในกรณีที่ต้องการร้องทุกข์หรือดำเนินคดี เนื่องจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้นนั้น อาจเข้าลักษณะเป็นความผิดตามประมวล กฎหมายอาญา หรือพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2560 และที่แก้ไข เพิ่มเติม (ถ้ามี) หรือกฎหมายอื่น ๆ ที่เกี่ยวข้อง ประกอบด้วยการดำเนินการทบทวนหลังการดำเนินการ (After-Action Review Process) เพื่อระบุและแนะนำให้ปรับปรุงการดำเนินการเพื่อป้องกันการเกิดซ้ำ

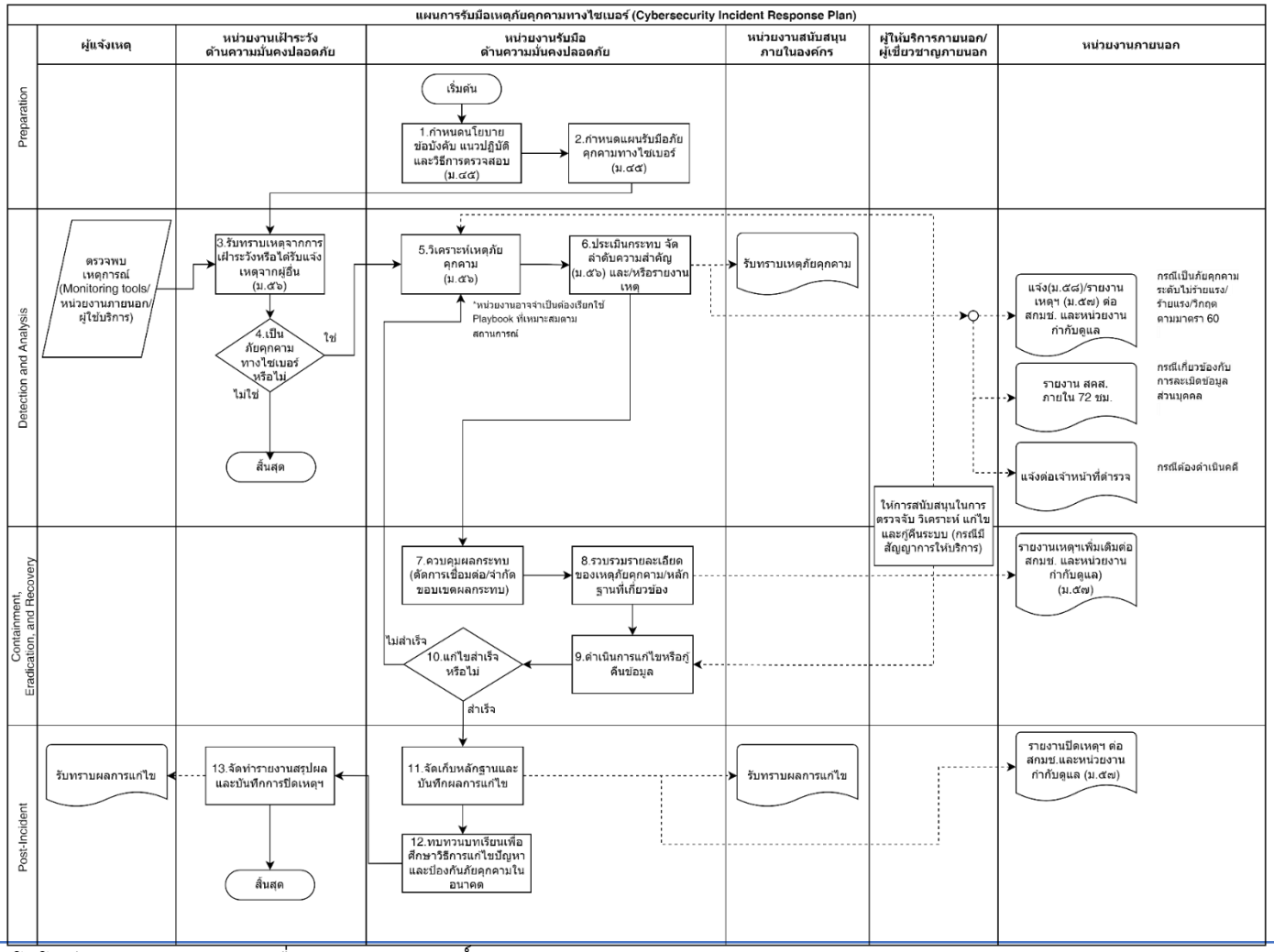
นอกจากนี้ กรมปศุสัตว์ได้พิจารณาดำเนินการตามเอกสารแนบท้าย 2 ตารางที่ 2.4 ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. 2564 เพิ่มเติม

11.5. การจัดทำรายการตรวจสอบการจัดการเหตุการณ์ (Incident Handling Checklist)

กรมปศุสัตว์จัดทำรายการตรวจสอบการจัดการเหตุการณ์ (Incident Handling Checklist) ซึ่งจะช่วยให้แนวทางแก่หน่วยงานเกี่ยวกับขั้นตอนสำคัญที่ควรดำเนินการ โดยหน่วยงานสามารถใช้ข้อมูลเพื่อประกอบการพิจารณาความเหมาะสมในการจัดทำรายการตรวจสอบของตนเองได้ (รายละเอียดปรากฏตามภาคผนวก 5)

ภาคผนวก 1 แผนการรับมือเหตุภัยคุกคามทางไซเบอร์และขั้นตอนการรับมือภัยคุกคามแต่ละประเภท

1. แผนการรับมือเหตุภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)



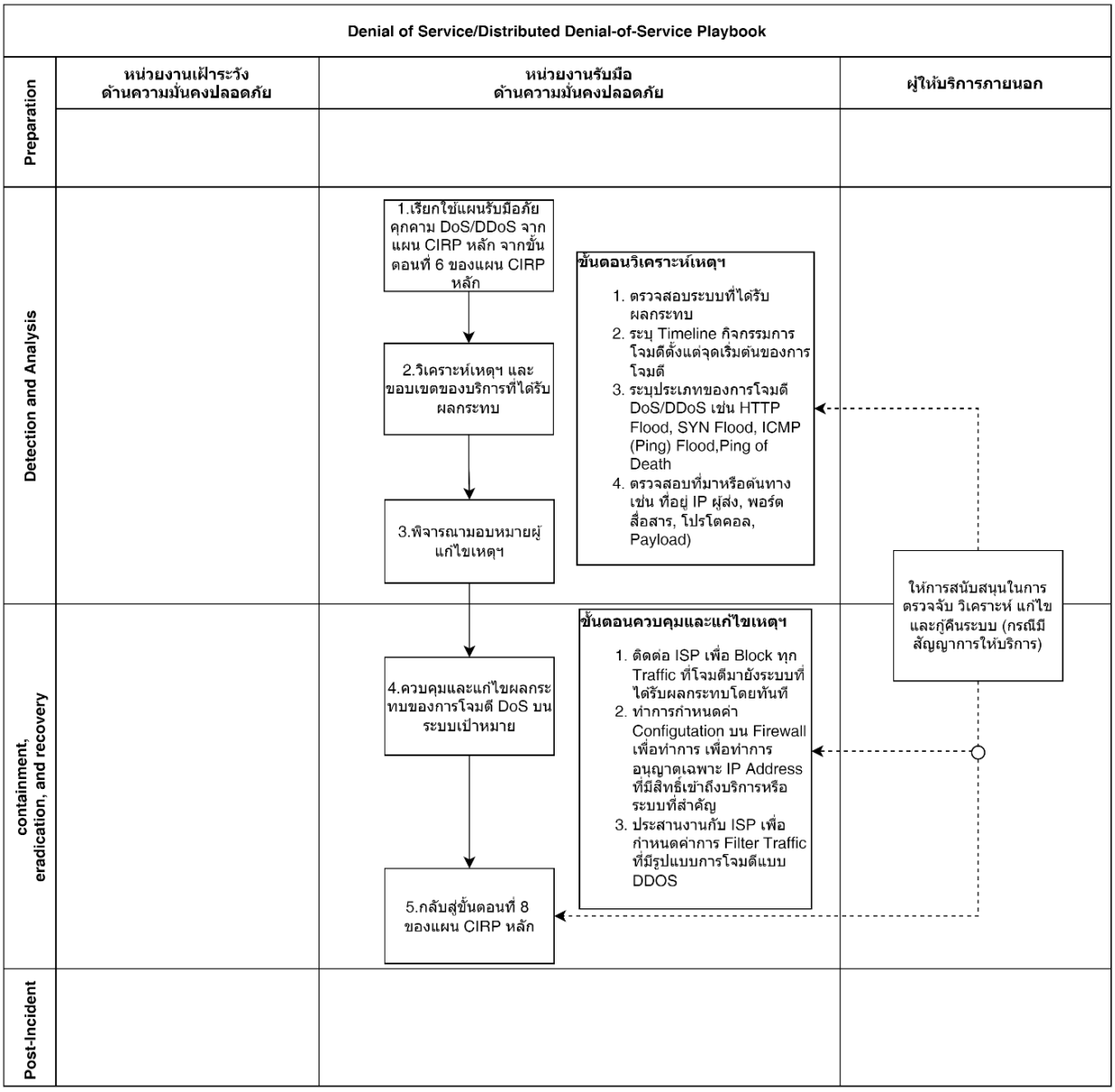
คำอธิบายแผนการรับมือเหตุภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)

ลำดับ	หัวข้อ	คำอธิบาย
ขั้นตอนการเตรียมการ (preparation)		
1	กำหนดนโยบาย ข้อบังคับ แนวปฏิบัติ และวิธีการตรวจสอบ (ม.45)	หน่วยงานรับมือด้านความมั่นคงปลอดภัย ร่วมกับผู้บริหารของหน่วยงานกำหนดนโยบาย ข้อบังคับ แนวปฏิบัติ และวิธีการตรวจสอบด้านความมั่นคงปลอดภัย โดยสอดคล้องตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (ตามมาตรา 13 วรรคหนึ่ง (4))
2	กำหนดแผนรับมือภัยคุกคามทางไซเบอร์ (ม.45)	หน่วยงานรับมือด้านความมั่นคงปลอดภัย กำหนดแผนรับมือภัยคุกคามทางไซเบอร์ โดยระบุภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นกับหน่วยงาน กำหนดขั้นตอนและวิธีการในการรับมือกับเหตุการณ์ภัยคุกคามทางไซเบอร์ กำหนดผู้รับผิดชอบในแต่ละขั้นตอน และกำหนดให้มีการทดสอบแผนรับมือภัยคุกคามทางไซเบอร์อย่างสม่ำเสมอ
ขั้นตอนการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (detection and analysis)		
3	รับทราบเหตุจากการเฝ้าระวังหรือได้รับแจ้งเหตุจากผู้อื่น (ม.56)	หน่วยงานเฝ้าระวังด้านความมั่นคงปลอดภัย ได้รับทราบเหตุจากการเฝ้าระวัง (Monitoring tools) หรือได้รับแจ้งเหตุจากผู้อื่นที่ตรวจพบเหตุการณ์ เช่น หน่วยงานภายนอก หรือผู้ใช้บริการ
4	เป็นภัยคุกคามทางไซเบอร์หรือไม่	หน่วยงานเฝ้าระวังด้านความมั่นคงปลอดภัย พิจารณาเหตุการณ์ว่าเป็นภัยคุกคามทางไซเบอร์หรือไม่
5	วิเคราะห์เหตุภัยคุกคาม	หน่วยงานเฝ้าระวังด้านความมั่นคงปลอดภัย พิจารณาประเภทของภัยคุกคาม หมวดหมู่ของภัยคุกคาม รายละเอียดแหล่งที่มาหรือต้นเหตุของเหตุภัยคุกคาม ข้อมูล จำนวนระบบ บริการหรือสินทรัพย์ที่ได้รับผลกระทบ
6	ประเมินกระทบ และจัดลำดับความสำคัญ (ม.56)	1. หน่วยงานเฝ้าระวังด้านความมั่นคงปลอดภัย ดำเนินการประเมินกระทบ และจัดลำดับความสำคัญของเหตุภัยคุกคาม รวมถึงเลือกแนวทางในการรับมือกับเหตุภัยคุกคามทางไซเบอร์ หมายเหตุ: หน่วยงานอาจจำเป็นต้องเรียกใช้ Playbook ที่เหมาะสมตามสถานการณ์

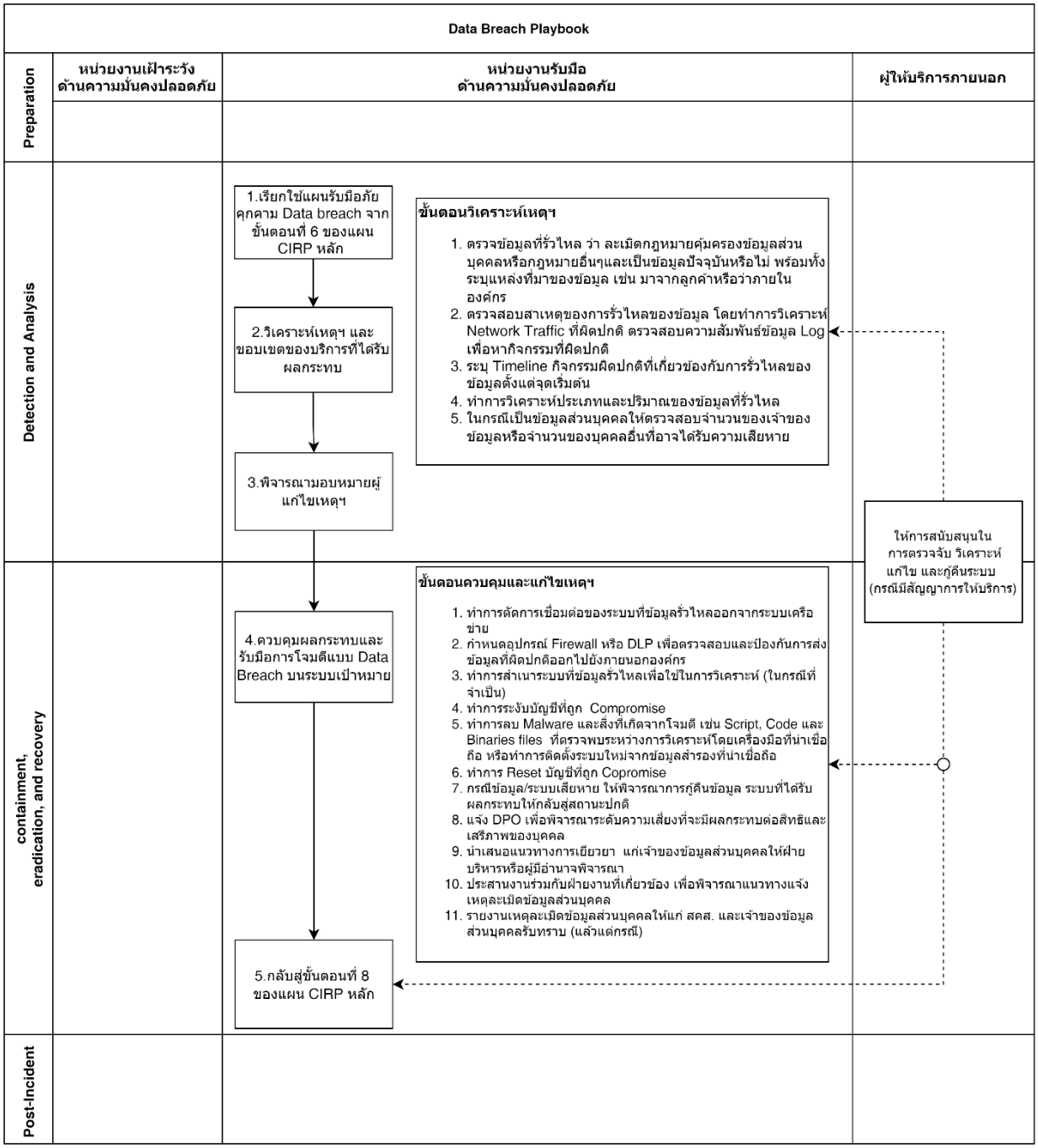
ลำดับ	หัวข้อ	คำอธิบาย
		2. หน่วยงานเฝ้าระวังด้านความมั่นคงปลอดภัย รายงานเหตุภัยคุกคามทางไซเบอร์ต่อหน่วยงานต่าง ๆ ● กรณีเป็นภัยคุกคามระดับไม่ร้ายแรง/ร้ายแรง/วิกฤต ตามมาตรา 60 หน่วยงานต้องแจ้งเหตุภัยคุกคาม (มาตรา 58) (เอกสาร ก.1 หรือมีข้อมูลเทียบเท่า) และ/หรือรายงานเหตุภัยคุกคาม (มาตรา 57) (เอกสาร ก.2) ต่อ สกมช. และหน่วยงานกำกับดูแล ● กรณีเกี่ยวข้องกับการละเมิดข้อมูลส่วนบุคคล หน่วยงานอาจต้องแจ้งไปยัง สคส. ● กรณีมีความจำเป็นต้องดำเนินคดีเนื่องจากเหตุนั้นเหตุนั้นเข้าลักษณะเป็นความผิดตามประมวล กฎหมายอาญา หรือพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2560 และที่แก้ไข เพิ่มเติม (ถ้ามี) หรือกฎหมายอื่น ๆ ที่เกี่ยวข้อง หน่วยงานอาจต้องแจ้งไปยังเจ้าหน้าที่ตำรวจเกี่ยวกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นนั้น
ขั้นตอนการระงับภัยคุกคาม ปราบปราม และฟื้นฟูระบบงานที่ได้รับผลกระทบ (containment, eradication, and recovery)		
7	ควบคุมผลกระทบ (ตัดการเชื่อมต่อ/จำกัดขอบเขตผลกระทบ)	หน่วยงานเฝ้าระวังด้านความมั่นคงปลอดภัย ควรจำกัดขอบเขต (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ ทำการกำจัดสาเหตุ (Eradicate the incident) กำจัด หรือลบมัลแวร์ และสาเหตุภัยคุกคามอื่น ๆ
8	รวบรวมรายละเอียดของเหตุภัยคุกคาม/หลักฐานที่เกี่ยวข้อง	1. หน่วยงานเฝ้าระวังด้านความมั่นคงปลอดภัย บันทึกเหตุการณ์ และดำเนินการจัดเก็บรักษาหลักฐานเกี่ยวกับเหตุการณ์ทั้งหมดก่อนเริ่มกระบวนการกู้คืน ซึ่งรวมถึงการได้มาของบันทึกการยึดหลักฐานคอมพิวเตอร์ที่ได้มา หรืออุปกรณ์อื่น ๆ เพื่อสนับสนุนการสอบสวน 2. หน่วยงานเฝ้าระวังด้านความมั่นคงปลอดภัย รายงานเหตุการณ์เพิ่มเติมต่อ สกมช. และหน่วยงานกำกับดูแล

ลำดับ	หัวข้อ	คำอธิบาย
		(ม.57) (เอกสาร ก.2)
9	ดำเนินการแก้ไขหรือกู้คืนข้อมูล	หน่วยงานเฝ้าระวังด้านความมั่นคงปลอดภัย เรียกใช้งานกระบวนการกู้คืน (Recovery Process)
10	แก้ไขสำเร็จหรือไม่	หน่วยงานเฝ้าระวังด้านความมั่นคงปลอดภัย พิจารณาว่าระบบที่ได้รับผลกระทบจากภัยคุกคามกลับสู่สถานะพร้อมใช้งานแล้วหรือไม่ หากยืนยันว่าระบบที่ได้รับผลกระทบกลับมาทำงานได้ตามปกติ ให้ดำเนินการต่อที่ขั้นตอนที่ 11 หากยังไม่สามารถแก้ไขได้ ให้ดำเนินการขั้นตอนที่ 5 ซ้ำเพื่อวิเคราะห์ภัยคุกคามทางไซเบอร์อีกครั้ง
ขั้นตอนการดำเนินการภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ (Post-Incident Activity)		
11	จัดเก็บหลักฐานและบันทึกผลการแก้ไข	1. หน่วยงานเฝ้าระวังด้านความมั่นคงปลอดภัย เก็บรักษาข้อมูลและพยานหลักฐานที่จำเป็น เพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์ หรือใช้ในกรณีที่ต้องการร้องทุกข์หรือดำเนินคดี 2. บันทึกผลการแก้ไขเหตุภัยคุกคามและวิธีการแก้ไขเพื่อจัดเก็บเป็นบทเรียน 3. รายงานปิดเหตุการณ์ต่อ สกมช. และหน่วยงานกำกับดูแล (ม.57) (เอกสาร ก.2)
12	ทบทวนบทเรียนเพื่อศึกษาวิธีการแก้ไขปัญหา และป้องกันภัยคุกคามในอนาคต	หน่วยงานเฝ้าระวังด้านความมั่นคงปลอดภัย จัดการประชุมทบทวนบทเรียนที่เกิดจากเหตุการณ์ดังกล่าว และกำหนดแนวทางในการป้องกันการเกิดเหตุซ้ำ หรือป้องกันภัยคุกคามอื่น ๆ ที่มีลักษณะคล้ายคลึงกันในอนาคต
13	จัดทำรายงานสรุปผลและบันทึกการปิดเหตุฯ	หน่วยงานเฝ้าระวังด้านความมั่นคงปลอดภัย จัดทำรายงานสรุปผลและบันทึกการปิดเหตุการณ์ รวมถึงแจ้งผลการแก้ไขไปยังผู้เกี่ยวข้องให้รับทราบ

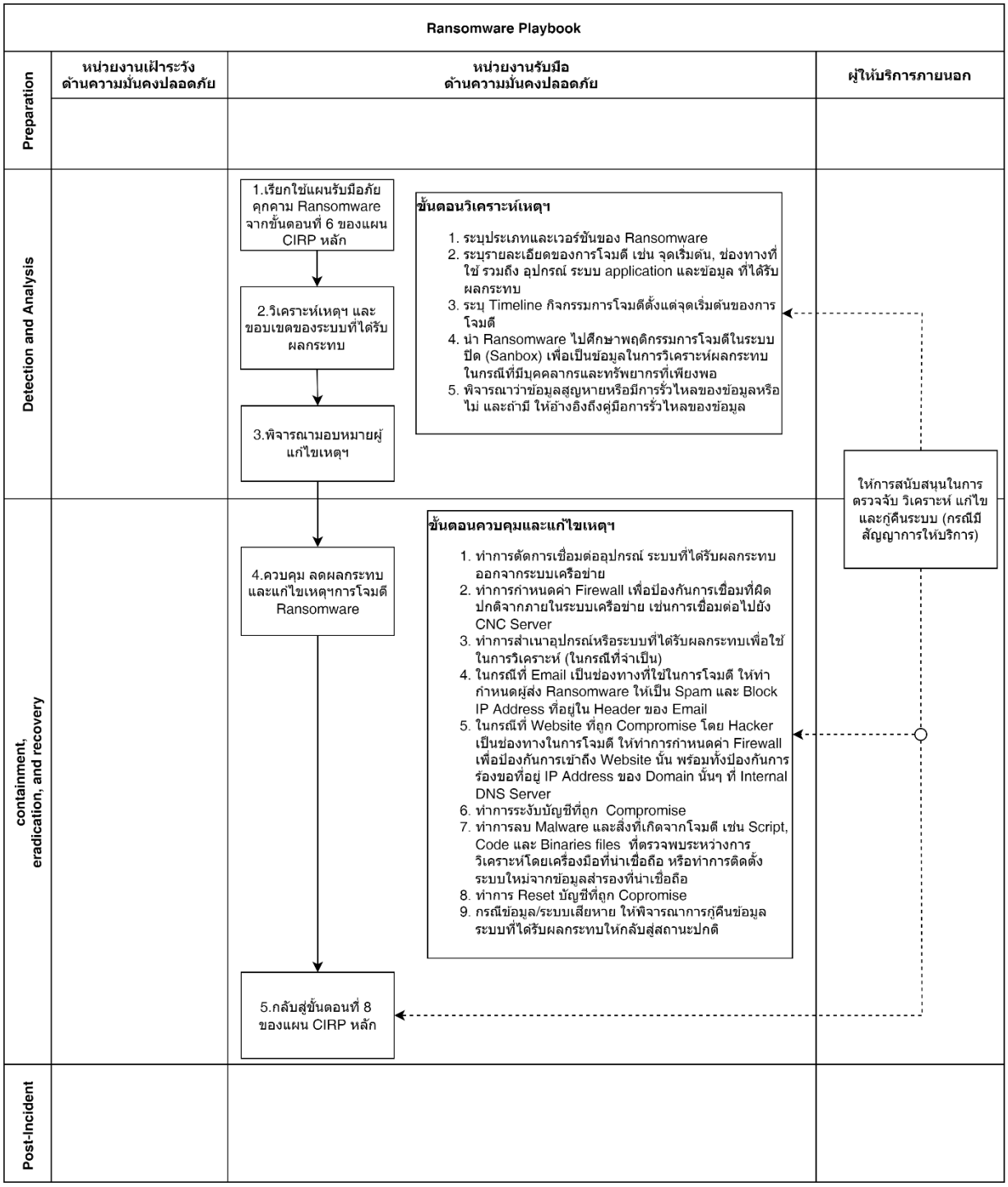
2. ขั้นตอนการรับมือภัยคุกคามแบบ Denial of Service/Distributed Denial-of-Service (DoS/DDoS Playbook)



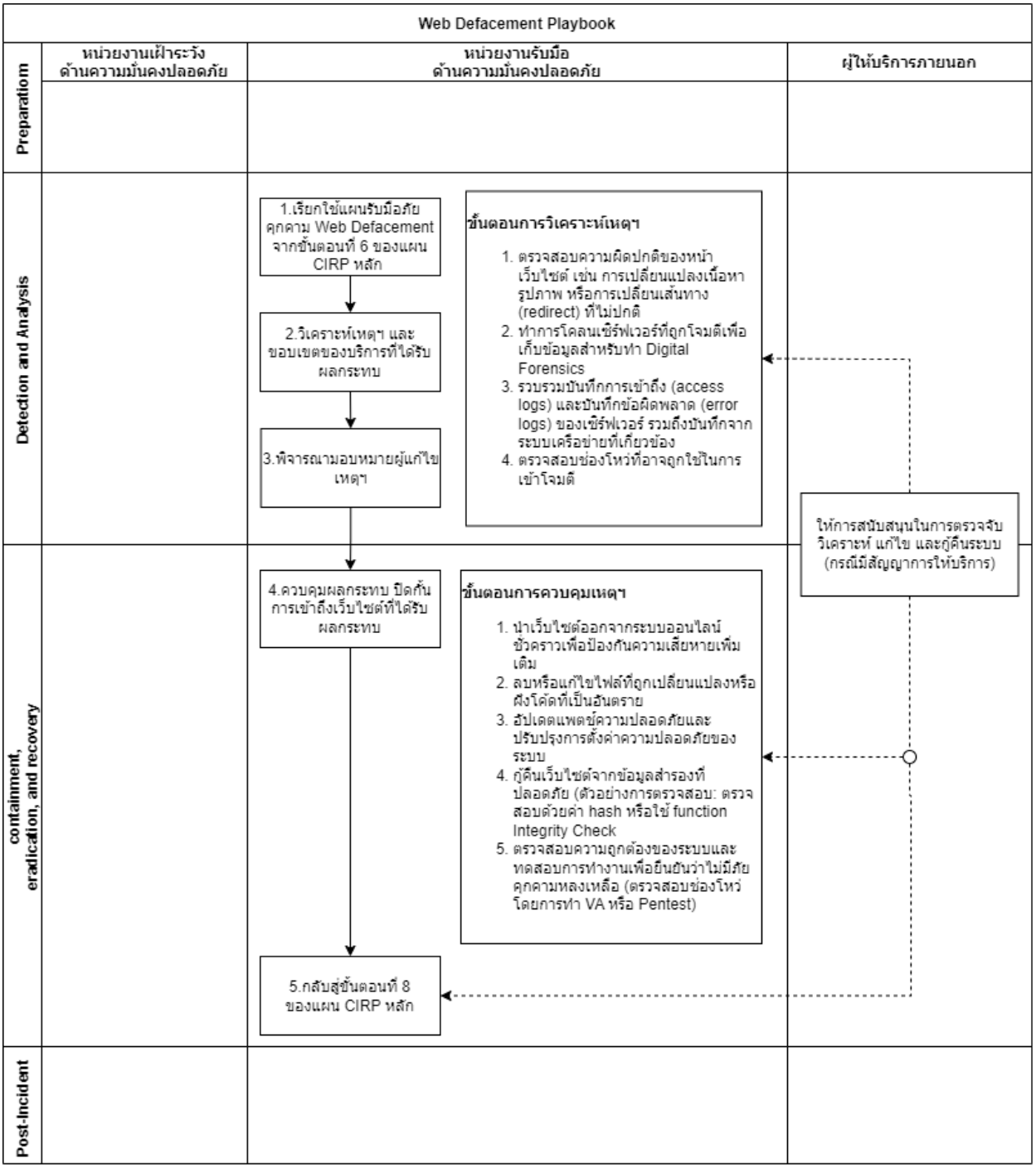
3. ขั้นตอนการรับมือภัยคุกคามแบบ Data Breach (Data Breach Playbook)



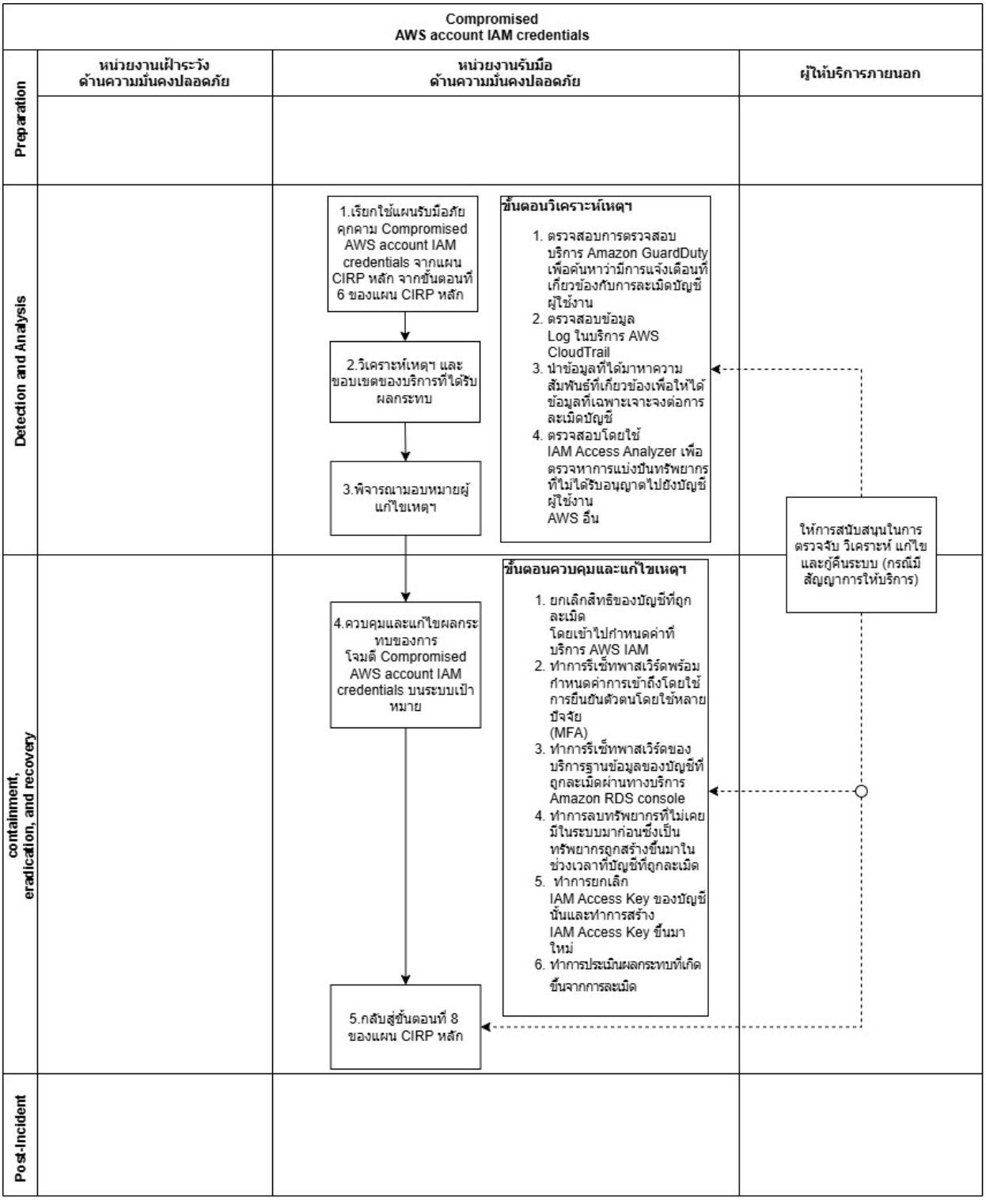
4. ขั้นตอนการรับมือภัยคุกคามแบบ Ransomware (Ransomware Playbook)



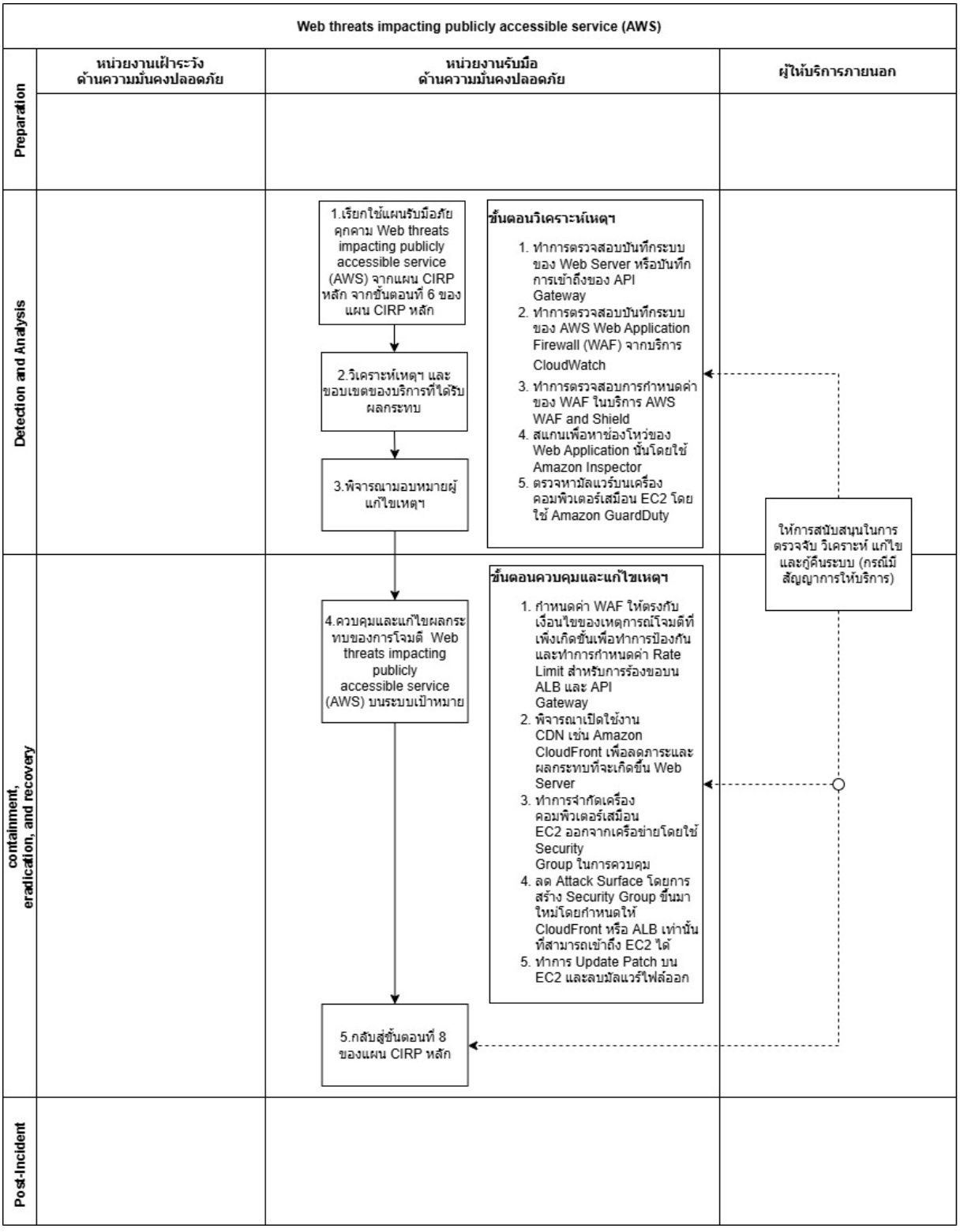
5. ขั้นตอนการรับมือภัยคุกคามแบบ Web Defacement (Web Defacement Playbook)



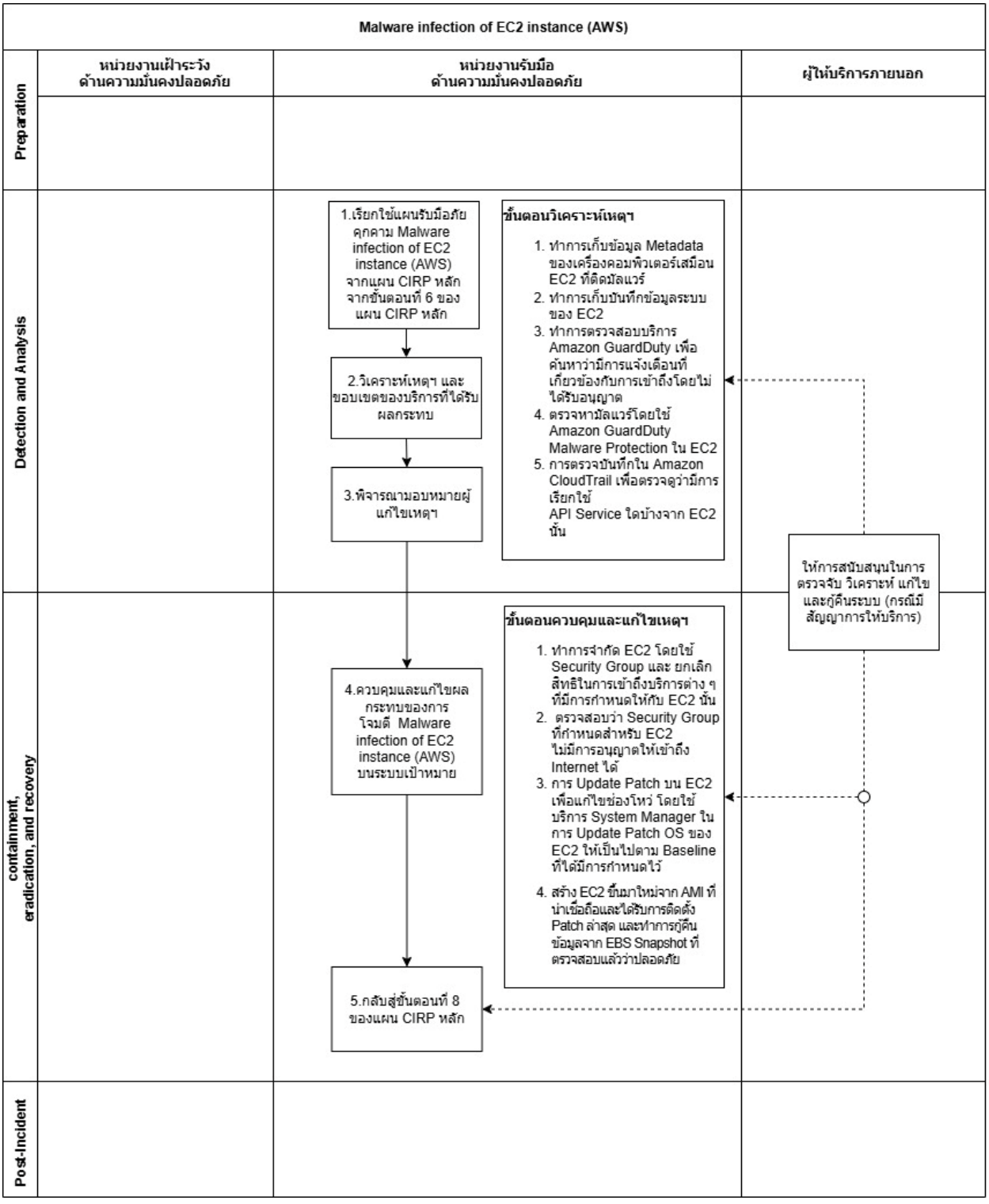
6. ขั้นตอนการรับมือภัยคุกคามการละเมิดบัญชีผู้ใช้งาน AWS IAM (Compromised AWS account IAM credentials)



ขั้นตอนการรับมือภัยคุกคามการโจมตีบริการที่เข้าถึงได้โดยสาธารณะบน AWS (Web threats impacting publicly accessible service (AWS))



7. ขั้นตอนการรับมือภัยคุกคามการติดมัลแวร์บนเครื่องคอมพิวเตอร์เสมือน EC2 บน AWS (Malware infection of EC2 instance (AWS)) กรณีใช้ Amazon web service



ภาคผนวก 2

ตัวอย่าง : บันทึกรายงานสถานการณ์เหตุการณ์ความมั่นคงปลอดภัยไซเบอร์

วันที่ :	เวลา :	ผู้บันทึกรายงาน : ติดต่อ :
วันและเวลาที่เกิดเหตุการณ์ :		
สถานะเหตุการณ์ปัจจุบัน :		
ประเภทเหตุการณ์ :		
ระดับความรุนแรง :		
รายละเอียดเหตุการณ์ :		
ผลกระทบที่เกิดขึ้น :		
ความเสียหายที่เกิดขึ้น :		
การรายงานเหตุการณ์ :		
หน่วยงานที่ขอความช่วยเหลือ :		
การดำเนินการตอบสนองต่อเหตุการณ์ :		
รายละเอียดเพิ่มเติม :		
ผู้จัดการรับมือฯ เหตุการณ์ :		
ข้อมูลติดต่อผู้จัดการรับมือฯ เหตุการณ์ :		
วันและเวลาที่มีรายงานความคืบหน้าครั้งถัดไป :		

ภาคผนวก 3

บันทึกข้อมูลกิจกรรมเหตุการณ์ความปลอดภัยทางไซเบอร์ (Incident Documentation)

วันที่และเวลา	บันทึกกิจกรรมที่เกิดขึ้น (ข้อเท็จจริง, สถานการณ์ที่เกิดขึ้น, การตัดสินใจ, ผลกระทบ)
ตัวอย่าง 12/1/66 – 09.00 น.	*ทีมรับมือฯ ตรวจสอบพบภัยคุกคามลักษณะ Phishing ทำให้เกิด Ransomware เข้าสู่ระบบเครือข่ายภายในหน่วยงาน*

ภาคผนวก 4

เอกสาร ก1 ข้อมูลที่ต้องแจ้ง

ข้อมูลการประสานงานและผลการตรวจสอบภัยคุกคามเบื้องต้น
1. ข้อมูลการประสานงาน ชื่อหน่วยงานที่รับผิดชอบติดตามเหตุภัยคุกคาม วันที่และเวลาที่แจ้ง
2. ด้านภารกิจหรือบริการของหน่วยงาน และ ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม ที่อยู่ของหน่วยงานหรือหน่วยงานย่อยที่เกิดเหตุภัยคุกคาม
3. ข้อมูลการติดต่อสำหรับการประสานงานเหตุภัยคุกคาม ชื่อ-นามสกุล ตำแหน่งงาน ชื่อหน่วยงาน อีเมล โทรศัพท์ (ที่ทำงาน / มือถือ)
4. ความต่อเนื่องของเหตุภัยคุกคาม ☐ เหตุภัยคุกคามใหม่ ☐ การรายงานข้อมูลต่อเนื่องจากเหตุภัยคุกคามเดิม
5. ลักษณะภัยคุกคามทางไซเบอร์ ระบบที่ได้รับผลกระทบมีความสำคัญต่อพันธกิจหลักของหน่วยงานหรือไม่ เหตุการณ์ที่เกิดขึ้นเกิดจากภัยคุกคามทางไซเบอร์[3] ในระดับใด (มาตรา 60) ☐ ไม่ร้ายแรง ☐ ร้ายแรง ☐ วิกฤต (ก) ☐ วิกฤต (ข) ☐ ยังไม่สามารถระบุได้

[3] พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 กำหนดความหมายของ “ภัยคุกคามทางไซเบอร์” ดังนี้ การกระทำหรือการดำเนินการใด ๆ โดยมิชอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

6. หมวดหมู่ของภัยคุกคาม (แจ้งได้มากกว่า 1 รายการ)

หมวดหมู่*	คำอธิบาย
หมวดหมู่ที่ 2	การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance)
หมวดหมู่ที่ 3	การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยของหน่วยงาน (Non-Compliance Activity)
หมวดหมู่ที่ 4	การบุกรุกโดยการใช้มัลแวร์ (Malicious Logic)
หมวดหมู่ที่ 5	การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion)
หมวดหมู่ที่ 6	การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion)
หมวดหมู่ที่ 7	การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)
หมวดหมู่ที่ 8	เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating)

* อ้างอิงหมวดหมู่ตามภาคผนวกท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. 2564 (ทั้งนี้ ภัยคุกคามทางไซเบอร์หมวดหมู่ที่ 0 หมวดหมู่ที่ 1 และหมวดหมู่ที่ 9 ไม่เข้าข่ายเป็นภัยคุกคามทางไซเบอร์ที่ต้องรายงาน)

เอกสาร ก2 แบบรายงานภัยคุกคามทางไซเบอร์

ส่วนที่ 1
หมวด ก. ข้อมูลการประสานงานและผลการตรวจสอบภัยคุกคามเบื้องต้น
หมายเลขอ้างอิง (สำหรับเจ้าหน้าที่ สกมช.): โปรดระบุ **หน่วยงานที่รับผิดชอบติดตามเหตุภัยคุกคาม (ถ้ามี):** โปรดระบุ **วันที่:** เลือกวันที่ **เวลา:** โปรดระบุ
ก1. ด้านภารกิจหรือบริการของหน่วยงาน และ ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม: โปรดระบุ ที่อยู่ของหน่วยงานหรือหน่วยงานย่อยที่เกิดเหตุภัยคุกคาม: โปรดระบุ
ก2. ข้อมูลการติดต่อสำหรับการประสานงานเหตุภัยคุกคาม ชื่อ-นามสกุล: โปรดระบุ ตำแหน่งงาน: โปรดระบุ ชื่อหน่วยงาน: โปรดระบุ อีเมล: โปรดระบุ โทรศัพท์ (ที่ทำงาน / มือถือ) : โปรดระบุ
ก3. ความต่อเนื่องของเหตุภัยคุกคาม ☐ เหตุภัยคุกคามใหม่ ☐ การรายงานข้อมูลต่อเนื่องจากเหตุภัยคุกคามเดิม
ก4. ลักษณะภัยคุกคามทางไซเบอร์ ระบบที่ได้รับผลกระทบมีความสำคัญต่อพันธกิจหลักของหน่วยงาน ☐ ใช่ ☐ ไม่ใช่ เหตุการณ์ที่เกิดขึ้นเกิดจากภัยคุกคามทางไซเบอร์[4] ในระดับใด (มาตรา 60) ☐ ไม่ร้ายแรง ☐ ร้ายแรง ☐ วิกฤต (ก) ☐ วิกฤต (ข) ☐ ยังไม่สามารถระบุได้
หมวด ข. ข้อมูลการตรวจพบภัยคุกคามไซเบอร์
ข1. วัน เวลา ที่เกิดเหตุภัยคุกคาม วันที่ : เลือกวันที่ เวลา : โปรดระบุ **วัน เวลา ที่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศทราบเหตุภัยคุกคาม** วันที่ : เลือกวันที่ เวลา : โปรดระบุ

[4] พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 กำหนดความหมายของ “ภัยคุกคามทางไซเบอร์” ดังนี้ การกระทำ หรือการดำเนินการใด ๆ โดยมิชอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหาย หรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

ข2. วัน เวลา ที่แจ้งเหตุภัยคุกคามให้หน่วยงานควบคุมหรือกำกับดูแลทราบ

☐ ยังไม่ได้แจ้ง ☐ แจ้งแล้ว _____

ข3. หมวดหมู่ของภัยคุกคาม (เลือกได้มากกว่า 1 รายการ)

หมวดหมู่*	คำอธิบาย
☐ หมวดหมู่ที่ 2	การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance)
☐ หมวดหมู่ที่ 3	การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยของหน่วยงาน (Non-Compliance Activity)
☐ หมวดหมู่ที่ 4	การบุกรุกโดยการใช้มัลแวร์ (Malicious Logic)
☐ หมวดหมู่ที่ 5	การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion)
☐ หมวดหมู่ที่ 6	การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion)
☐ หมวดหมู่ที่ 7	การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)
☐ หมวดหมู่ที่ 8	เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating)
☐ อื่น ๆ	โปรดระบุ

* อ้างอิงหมวดหมู่ตามภาคผนวกท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. 2564 (ทั้งนี้ ภัยคุกคามหมวดหมู่ที่ 0 1 และ 9 ไม่เข้าข่ายเป็นภัยคุกคามทางไซเบอร์ที่ต้องรายงาน)

ข4. 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
ค1. สถานการณ์หรือการแก้ไขเหตุภัยคุกคาม (เลือกได้มากกว่า 1 รายการ) ☐ เพิ่งพบเหตุการณ์ ☐ อยู่ในขั้นตอนการขอความช่วยเหลือ ☐ อยู่ในขั้นตอนการสอบสวน ☐ กำลังลุกลาม ☐ อยู่ในขั้นตอนการระงับภัย ☐ สามารถระงับภัยได้แล้ว ☐ รายงานปิดเหตุการณ์ภัยคุกคามแล้ว ☐ อื่น ๆ: โปรดระบุ
ค2. สิ่งที่ได้ดำเนินการหรือได้แก้ไขไปแล้ว ☐ ยังไม่ได้ดำเนินการแก้ไขใด ๆ ☐ ยกเลิกการเชื่อมต่อระบบออกจากเครือข่ายแล้ว ☐ ตรวจสอบข้อมูลจราจร (Log) แล้ว ☐ ตรวจสอบโปรแกรม (แฟ้ม binaries/.exe) แล้ว ☐ กู้คืนกลับมาด้วยระบบหรือข้อมูลสำรองที่ตรวจสอบความถูกต้องแล้ว ☐ รายละเอียดการแก้ไขภัยคุกคามที่เกิดขึ้นเพิ่มเติม: โปรดระบุ
ค3. รายละเอียดการรับมือภัยคุกคามอื่น ๆ (ถ้ามี) โปรดระบุ

ส่วนที่ 2

หมวด ง : รายละเอียดภัยคุกคาม

ง1. ข้อมูลการตรวจจับและการวิเคราะห์

ง1.1 <u>วัน เวลา ที่ผู้โจมตีได้เริ่มต้นเข้าถึงระบบ</u> (System Access)

วันที่: เลือกวันที่ **เวลา:** โปรดระบุ **ไม่ทราบ:** ☐

ง1.2 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

ง1.3 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

ง1.4 <u>รายละเอียดของระบบ หรือข้อมูลที่ได้รับผลกระทบ (Information of Affected System)</u>

หมายเลข CVE: โปรดระบุ
ช่องโหว่ที่ถูกใช้จู่โจม: โปรดระบุ
การใช้ระบบหรือเครื่องที่ได้รับผลกระทบเป็นฐานเพื่อจู่โจมขยายผลไปยังระบบหรือเครื่องอื่น: โปรดระบุ
อาการหรือสิ่งผิดปกติ (เลือกได้มากกว่า 1 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

ง1.5 รายละเอียดของเหตุภัยคุกคามตามลำดับเวลา ตั้งแต่การจู่โจมครั้งแรก จนถึงปัจจุบัน (เช่น ลำดับของการจู่โจม, Attack vector, เทคนิคหรือเครื่องมือที่ผู้จู่โจมใช้ ฯลฯ) โปรดระบุ

ง1.6 รายละเอียดอื่น ๆ ที่พบเกี่ยวข้องกับเหตุภัยคุกคาม: โปรดระบุ

ง2. ข้อมูลการระงับ ปราบปราม และฟื้นฟู

ง2.1 รายละเอียดการดำเนินการเพื่อแก้ไขเหตุภัยคุกคาม: โปรดระบุ

ง2.2 การคาดการณ์ความสามารถฟื้นฟู

โปรดระบุรายละเอียดการฟื้นฟู ทรัพยากรที่ต้องใช้และที่ต้องการเพิ่ม และประมาณระยะเวลาการฟื้นฟู

ง3. ข้อมูลกิจกรรมภายหลังการแก้ปัญหา (ถ้ามี)

ง3.1 วัน เวลา ที่เหตุภัยคุกคามสิ้นสุด วันที่: เลือกวันที่ **เวลา:** โปรดระบุ

ง3.2 การดำเนินการเพื่อป้องกันเหตุภัยคุกคามที่คล้ายคลึงกัน: โปรดระบุ

ง3.3 บทเรียนที่ได้จากเหตุภัยคุกคาม: โปรดระบุ

เอกสาร ก3 แบบรายงานสรุปภัยคุกคามทางไซเบอร์ในหนึ่งรอบปี

ข้อ 1 สถิติรายปีจำแนกตามหมวดหมู่ของภัยคุกคามทางไซเบอร์[5]

หมวดหมู่	คำอธิบาย	จำนวน
0	เหตุการณ์จำลองและการฝึกจู่โจมของหน่วยงาน (Training and Exercises)	
1	การพยายามเข้าถึงระบบที่ไม่สำเร็จ (Unsuccessful Activity Attempt)	
2	การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance)	
3	การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยที่หน่วยงานกำหนด (Non-Compliance Activity)	
4	การบุกรุกโดยการใช้มัลแวร์ (Malicious Logic)	
5	การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion)	
6	การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion)	
7	การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)	
8	เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating)	
9	เหตุการณ์ผิดปกติที่ได้รับการวิเคราะห์แล้วว่าไม่ใช่เหตุการณ์ที่เป็นภัยคุกคาม (Explained Anomaly)	

ข้อ 2 สถิติรายปีจำแนกตามทรัพย์สินที่ได้รับผลกระทบ

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

ข้อ 3 สถิติรายปีจำแนกตามระดับภัยคุกคามทางไซเบอร์[6]

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

[5] หมวดหมู่ตามข้อ 1 ของภาคผนวกท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์ แต่ละระดับ พ.ศ.2564

[6] ระดับภัยคุกคามทางไซเบอร์ตามมาตรา 60 แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562

ภาคผนวก 5

ตัวอย่าง : รายการตรวจสอบการจัดการเหตุการณ์ (Incident Handling Checklist)

รายการตรวจสอบการจัดการเหตุการณ์		Complete
ขั้นตอนการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (detection and analysis)		
1	ตรวจสอบว่ามีเหตุการณ์เกิดขึ้นหรือไม่	
1.1	วิเคราะห์ตรวจจับสัญญาณเหตุการณ์ความปลอดภัยทางไซเบอร์	
1.2	ค้นหาข้อมูลเพิ่มเติมที่มีความสัมพันธ์กัน	
1.3	ดำเนินการสืบค้นข้อมูล (เช่น search engines, ฐานข้อมูลอื่น ๆ เป็นต้น)	
1.4	ทันทีที่ผู้จัดการรับมือฯ เหตุการณ์เชื่อว่ามีเหตุการณ์เกิดขึ้น ให้เริ่มบันทึกการสอบสวนและรวบรวมหลักฐาน	
2	จัดลำดับความสำคัญในการจัดการเหตุการณ์ตามระดับความรุนแรงของภัยคุกคามที่เกิดขึ้น	
3	รายงานเหตุการณ์ดังกล่าวต่อผู้บริหารและหน่วยงานภายนอกที่เกี่ยวข้อง	
ขั้นตอนการระงับภัยคุกคาม ปราบปราม และฟื้นฟูระบบงานที่ได้รับผลกระทบ (containment, eradication, and recovery)		
4	บันทึกเหตุการณ์, จัดเก็บและดูแลรักษาหลักฐานเกี่ยวกับเหตุการณ์ทั้งหมดก่อนเริ่มกระบวนการกู้คืนซึ่งรวมถึงการได้มาของบันทึกการยึดหลักฐานคอมพิวเตอร์ที่ได้มา หรืออุปกรณ์อื่น ๆ เพื่อสนับสนุนการสอบสวน	
5	จำกัดขอบเขต (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์	
6	ดำเนินการสอบสวน (Investigate) สาเหตุและผลกระทบของเหตุการณ์	
7	ทำการกำจัดสาเหตุ (Eradicate the incident)	
7.1	ระบุช่องโหว่ของระบบที่โดนโจมตีและบรรเทาผลกระทบที่เกิดขึ้น	
7.2	กำจัด หรือลบมัลแวร์ และสาเหตุภัยคุกคามอื่น ๆ	
7.3	หากมีการตรวจพบว่ามีระบบใหม่ได้รับผลกระทบ (เช่น การติดมัลแวร์ใหม่) ให้ทำซ้ำขั้นตอนการตรวจจับและการวิเคราะห์ภัยคุกคามทางไซเบอร์ (detection and analysis)	
8	เรียกใช้งานกระบวนการกู้คืน (Recovery Process)	
8.1	ระบบที่ได้รับผลกระทบจากภัยคุกคามกลับสู่สถานะพร้อมใช้งาน	
8.2	ยืนยันว่าระบบที่ได้รับผลกระทบกลับมาทำงานได้ตามปกติ	
8.3	หากจำเป็น ให้ดำเนินการติดตามสถานการณ์ต่อไป เพื่อค้นหาเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ที่อาจเกี่ยวข้องในอนาคต	
ขั้นตอนการดำเนินการภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ (Post-Incident Activity)		
9	จัดทำรายงานการติดตามผล	
10	จัดการประชุมทบทวนบทเรียนที่เกิดจากเหตุการณ์ดังกล่าว	

ภาคผนวก 6

การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise)

การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์คือการจำลองสถานการณ์และทดสอบความพร้อมขององค์กรในการรับมือกับเหตุการณ์ทางไซเบอร์ต่างๆ ที่ผิดปกติและส่งผลกระทบต่อการดำเนินงาน การฝึกซ้อมนี้จะช่วยให้องค์กรสามารถทดสอบผลกระทบ แนวทางการรับมือและการแก้ไขจากเหตุการณ์จำลองในสภาพแวดล้อมที่ควบคุม รวมถึงช่วยให้องค์กรได้ตรวจสอบว่ากระบวนรับมือต่อเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์สามารถใช้ได้จริงหรือไม่ และระบุจุดแข็งหรือสิ่งที่ทำได้ดี และจุดอ่อนที่ควรต้องปรับปรุง

การฝึกซ้อมรับมือภัยคุกคามทางไซเบอร์มีหลายประเภท ขึ้นอยู่กับระดับการจำลองเหตุการณ์ สภาพแวดล้อมทางเทคนิค และเวลาที่ใช้ โดยจำแนกได้ 2 ประเภทหลัก ดังต่อไปนี้

- **Table Top Exercise** เป็นการซ้อมในรูปแบบการหารือร่วมกัน (Discussion-based Exercise) ผู้เข้าร่วมจะฝึกซ้อมตามบทในสถานการณ์จำลอง โดยมุ่งเน้นการทบทวนขั้นตอน แผนปฏิบัติ และบทบาทหน้าที่ของแต่ละฝ่าย โดยไม่มีการปฏิบัติการจริงในระบบ จุดประสงค์หลักคือเพื่อฝึกการตัดสินใจ การสื่อสาร และการประสานงาน ตัวอย่างเช่น การซ้อมการแจ้งเตือนเหตุการณ์ การรายงานไปยังผู้บริหาร และการประสานงานกับหน่วยงานภายนอก การฝึกซ้อมรูปแบบนี้เหมาะสำหรับการซักซ้อมและทบทวนในระดับนโยบายหรือผู้บริหาร ผู้ปฏิบัติการทั่วไป รวมถึงการฝึกอบรมเบื้องต้นให้กับเจ้าหน้าที่ใหม่
- **Functional Exercise** เป็นการซ้อมการปฏิบัติการเชิงเทคนิค ซึ่งทำการยกระดับการฝึกซ้อมให้มีความสมจริงมากกว่า Table Top Exercise การฝึกซ้อมแบบ Functional Exercise นี้จะมีการจำลองระบบหรือเหตุการณ์บางส่วนขึ้นจริง เพื่อให้ผู้เข้าร่วมได้ตอบสนองต่อเหตุการณ์ในลักษณะที่ใกล้เคียงกับสถานการณ์จริง ตัวอย่างเช่น การรับมือกับการติดมัลแวร์ แรนซัมแวร์ การวิเคราะห์ Log การประสานระหว่างทีม SOC และหน่วย CERT เป็นต้น โดยการฝึกซ้อมแบบ Functional Exercise อาจใช้ระบบจำลอง (Simulation Tools) หรือเครือข่ายทดสอบ (Testbed) เพื่อจำลองการโจมตีและการตอบโต้ การฝึกซ้อมรูปแบบนี้เหมาะสำหรับทีมเทคนิค เช่น Blue / Red Team หน่วยงาน SOC หรือหน่วยงาน CSIRT

โดยขั้นตอนในการดำเนินการฝึกซ้อมรับมือเหตุภัยคุกคามทางไซเบอร์มีรายละเอียดดังต่อไปนี้

<u>การเตรียมการ</u>

- **เลือกรูปแบบการฝึกซ้อม** ขึ้นอยู่กับวัตถุประสงค์ ทรัพยากร และระดับความพร้อมขององค์กร การจัดฝึกซ้อมอย่างสม่ำเสมอและครอบคลุมจะช่วยให้องค์กรสามารถรับมือกับเหตุการณ์ทางไซเบอร์ได้อย่างมีประสิทธิภาพมากยิ่งขึ้น ดังนั้นการเตรียมการฝึกซ้อมเป็นกิจกรรมที่สำคัญให้การดำเนินการซ้อมรับมือเหตุภัยคุกคามทางไซเบอร์มีประสิทธิภาพ โดยเริ่มต้นจากการกำหนดเป้าหมายที่ชัดเจน เป้าหมายควรระบุสิ่งที่ต้องการทดสอบอย่าง

เฉพาะเจาะจง เช่น ความเร็วในการรับมือการติดมัลแวร์ โดยเป้าหมายควรเชื่อมโยงกับเกณฑ์ในการประเมินความพร้อมการรับมือเหตุภัยคุกคามทางไซเบอร์ขององค์กร

- **เลือกทีมงาน** รวบรวมบุคลากรที่เกี่ยวข้องจากฝ่ายต่างๆ เช่น ทีม IT ทีมความมั่นคงปลอดภัยไซเบอร์ ผู้บริหาร และผู้มีส่วนได้ส่วนเสียจากแผนกอื่นๆ ที่อาจได้รับผลกระทบ เช่น กฎหมาย การตลาด และทรัพยากรบุคคล การมีส่วนร่วมของบุคลากรข้ามแผนกเป็นสิ่งสำคัญอย่างยิ่งในการส่งเสริมการทำงานร่วมกันและสร้างความเข้าใจในบทบาทของตนเอง

- **ออกแบบสถานการณ์จำลอง** ควรออกแบบสถานการณ์ที่สมจริงและเกี่ยวข้องกับความเสี่ยงเฉพาะที่องค์กรอาจเผชิญ สามารถเลือกจากสถานการณ์ตัวอย่างที่มีอยู่หรือปรับแต่งสถานการณ์ให้เหมาะสมกับบริบทขององค์กร การออกแบบควรคำนึงถึงการปรับระดับความยากและรวมถึงการสร้างสถานการณ์จำลองที่มีความซับซ้อนเพียงพอที่จะท้าทายผู้เข้ารับการฝึกซ้อม

- **ชี้แจง** ก่อนการซ้อมควรมีการชี้แจงผู้เข้าร่วม เกี่ยวกับบทบาทและหน้าที่ของแต่ละคนในการฝึกซ้อมอย่างชัดเจน

- **สำรองข้อมูล** ควรสำรองข้อมูลที่นำมาใช้ในการฝึกซ้อมทั้งหมด

- **ตรวจสอบกฎหมายที่เกี่ยวข้อง** เพื่อให้แน่ใจว่าการฝึกซ้อมไม่ละเมิดข้อกฎหมายหรือข้อกำหนดใดๆ

<u>การดำเนินการฝึกซ้อม</u>

ระหว่างการฝึกซ้อม ทีมงานจะดำเนินงานตามสถานการณ์จำลองที่วางแผนไว้ ในสภาพแวดล้อมที่ได้รับการควบคุมและมีความปลอดภัย เช่น แพลตฟอร์มที่ใช้ในการจำลองและทำให้การโจมตีทางไซเบอร์ โดยจะต้องมีการบันทึก กิจกรรมการตอบสนองของทีมงานอย่างละเอียด ตลอดกระบวนการ เพื่อใช้ในการวิเคราะห์ภายหลัง

<u>การประเมินผลและสรุปบทเรียน</u>

หลังจากการฝึกซ้อมเสร็จ จะต้องทำการจัดประชุมสรุปผลเพื่อวิเคราะห์จุดแข็งและจุดอ่อนที่พบในระหว่างการฝึกซ้อม ในขั้นตอนนี้ จะมีการประเมินผลการฝึกซ้อมโดยเทียบกับเป้าหมายที่ตั้งไว้ ผลลัพธ์จากการประเมินจะถูกนำไปจัดทำเป็นรายงานสรุปและข้อเสนอแนะสำหรับการปรับปรุงการรับมือเหตุภัยคุกคามทางไซเบอร์ขององค์กรทั้งในด้านบุคลากร กระบวนการ และเทคโนโลยี

แหล่งที่มา

- ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564

- ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ.2564

- ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทาง ไซเบอร์ พ.ศ.2566

- NIST SP 800-61r2 Computer Security Incident Handling Guide

- ACSC Cyber Incident Response Plan Guidance

- Cyber Security Agency (CSA) of Singapore, Cloud Incident Response Playbook

- UK National Cyber Security Centre (NCSC), Cyber Incident Exercising: Technical Standard

- Finnish Transport and Communications Agency, Instructions for Organising Cyber Exercises

- Victorian Government, Cyber Exercise Guide

- European Union Agency for Cybersecurity (ENISA), Technical Guideline for the Implementation of Article 4