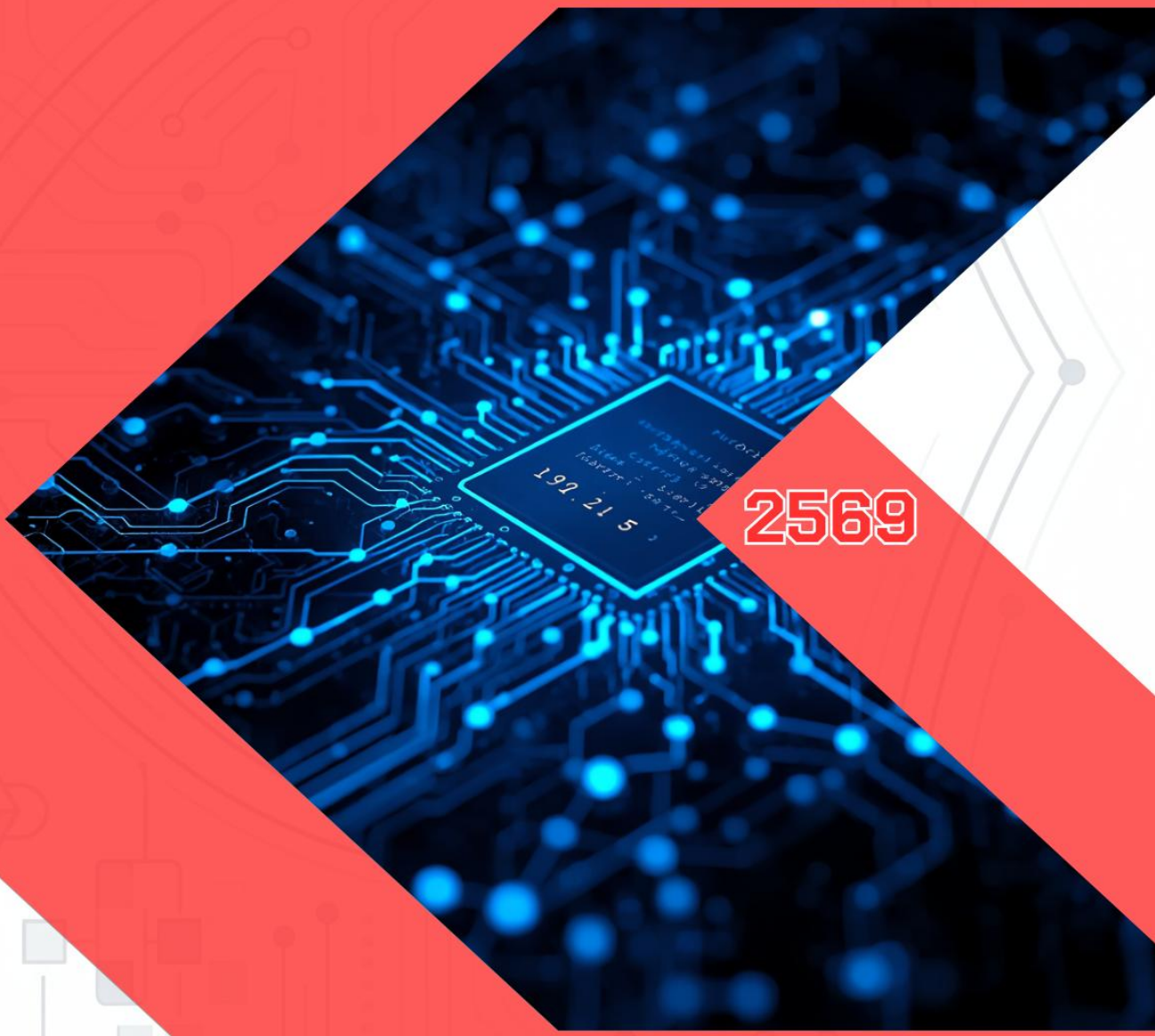
แผนรับมือเหตุภัยคุกคามทางไซเบอร์
CYBERSECURITY INCIDENT RESPONSE PLAN



2569

กรมพัฒนาสังคมและสวัสดิการ
กระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์

คำนำ

ในยุคดิจิทัลปัจจุบัน ระบบสารสนเทศและข้อมูลมีความสำคัญอย่างยิ่งต่อการขับเคลื่อนภารกิจขององค์กร กรมพัฒนาสังคมและสวัสดิการ ได้ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยทางไซเบอร์ จึงได้จัดทำ “แผนรับมือเหตุภัยคุกคามทางไซเบอร์” ของกรมพัฒนาสังคมและสวัสดิการฉบับนี้ขึ้น เพื่อให้สอดคล้องกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. 2563 โดยมีวัตถุประสงค์เพื่อกำหนดบทบาทหน้าที่ ขั้นตอนการรับมือ การรายงานเหตุการณ์ และการสื่อสารอย่างเป็นระบบ เพื่อลดผลกระทบต่อการดำเนินงานของกรมฯ ให้เหลือน้อยที่สุด อย่างไรก็ตาม รูปแบบของภัยคุกคามทางไซเบอร์ในปัจจุบันได้พัฒนาและเปลี่ยนแปลงไปอย่างรวดเร็ว การปรับปรุงแผนรับมือฉบับนี้ให้ทันต่อยุคสมัยจึงเป็นสิ่งจำเป็นอย่างยิ่ง โดยเฉพาะอย่างยิ่งจากสาเหตุสำคัญของ “เทคโนโลยีอุบัติใหม่” ที่มีความล้ำสมัย รวมถึงขีดความสามารถที่ก้าวข้ามขีดความสามารถในการป้องกันความปลอดภัยทางไซเบอร์เดิมอย่างเทียบไม่ได้ จึงควรมีแนวทางและมาตรการที่สอดรับกับการเปลี่ยนแปลงดังกล่าวอย่างทันท่วงที

กองยุทธศาสตร์และแผนงาน จึงหวังเป็นอย่างยิ่งว่า แผนรับมือเหตุภัยคุกคามทางไซเบอร์ของกรมพัฒนาสังคมและสวัสดิการฉบับนี้ จะเป็นเครื่องมือสำคัญที่ช่วยให้ผู้บริหารและบุคลากรทุกระดับมีความพร้อมในการเฝ้าระวัง ป้องกัน และตอบสนองต่อเหตุการณ์ฉุกเฉินทางไซเบอร์ได้อย่างมีประสิทธิภาพทันท่วงที และช่วยสร้างความมั่นคงปลอดภัยให้กับระบบสารสนเทศขององค์กรได้อย่างยั่งยืนต่อไป

กองยุทธศาสตร์และแผนงาน
กรมพัฒนาสังคมและสวัสดิการ

สารบัญ

แผนรับมือเหตุภัยคุกคามทางไซเบอร์ กรมพัฒนาสังคมและสวัสดิการ

1. หลักการและเหตุผล

แผนรับมือเหตุภัยคุกคามทางไซเบอร์ของกรมพัฒนาสังคมและสวัสดิการ ฉบับนี้ จัดทำขึ้นเพื่อให้เป็นไป ตามมาตรา 44 แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ที่กำหนดให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเร็ว ซึ่งอย่างน้อยต้องประกอบด้วย เรื่อง (1) แผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยผู้ตรวจประเมินผู้ตรวจสอบภายใน หรือผู้ตรวจสอบอิสระจากภายนอกอย่างน้อยปีละหนึ่งครั้งและ (2) แผนการรับมือภัยคุกคามทางไซเบอร์ รวมทั้งเพื่อให้เป็นไปตาม นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. 2563 ด้วย

2. วัตถุประสงค์

เพื่อใช้เป็นแผนในการรับมือเหตุภัยคุกคามทางไซเบอร์ที่เกิดขึ้นในกรมพัฒนาสังคมและสวัสดิการ โดยจะเป็นการกำหนดหน้าที่และความรับผิดชอบให้กับหน่วยงานต่าง ๆ ภายใต้กรมพัฒนาสังคมและสวัสดิการ การกำหนดประเภทของเหตุภัยคุกคามทางไซเบอร์ การกำหนดความสัมพันธ์กับนโยบายและแนวปฏิบัติที่เกี่ยวข้อง การรายงานเหตุภัยคุกคามทางไซเบอร์ และขั้นตอนการรับมือเหตุภัยคุกคามทางไซเบอร์ตามขอบเขตของระบบสารสนเทศที่กำหนดไว้ รวมไปถึงการสื่อสารไปยังผู้มีส่วนได้ส่วนเสีย เพื่อลดผลกระทบที่อาจเกิดขึ้นต่อการดำเนินงานของกรมพัฒนาสังคมและสวัสดิการ

3. ขอบเขต

แผนรับมือเหตุภัยคุกคามทางไซเบอร์ฉบับนี้ ใช้รับมือเหตุภัยคุกคามทางไซเบอร์ที่เกิดขึ้นต่อระบบสารสนเทศและข้อมูลดิจิทัลของกรมพัฒนาสังคมและสวัสดิการ รวมถึงบุคคลหรืออุปกรณ์ใด ๆ ซึ่งเข้าถึงระบบสารสนเทศและข้อมูลดิจิทัลดังกล่าว รวมถึงระบบคลาวด์ บริการซอฟต์แวร์ผ่านอินเทอร์เน็ต และการเชื่อมต่อข้อมูลผ่านระบบเครือข่ายหรือ API กับหน่วยงานภายนอกที่อยู่ภายใต้การใช้งานหรือการกำกับดูแลของกรมพัฒนาสังคมและสวัสดิการ

4. หน้าที่การทบทวนแผน

กลุ่มเทคโนโลยีสารสนเทศ กองยุทธศาสตร์และแผนงาน มีหน้าที่ทบทวนและขออนุมัติแผนรับมือเหตุภัยคุกคามทางไซเบอร์ฉบับนี้ถึงผู้บริหารสูงสุดหรือผู้ที่รับมอบอำนาจจากกรมพัฒนาสังคมและสวัสดิการ

5. หน้าที่ในการดำเนินการตามแผน

กลุ่มเทคโนโลยีสารสนเทศ กองยุทธศาสตร์และแผนงาน มีหน้าที่เป็นผู้รับผิดชอบหลักในการดำเนินการตามแผนรับมือเหตุภัยคุกคามทางไซเบอร์ฉบับนี้ โดยมีกรมพัฒนาสังคมและสวัสดิการสนับสนุนประกอบด้วย

5.1 กลุ่มงานผู้เชี่ยวชาญ (กชช.)

5.2 สำนักงานเลขานุการกรม (สลก.)

5.3 กองยุทธศาสตร์และแผนงาน (กยผ.)

5.4 สำนักงานคณะกรรมการส่งเสริมการจัดสวัสดิการสังคมแห่งชาติ (ก.ส.ค.)

5.5 กองกิจการอาสาสมัครและภาคประชาสังคม (กอส.)

5.6 กองคุ้มครองสวัสดิภาพและเสริมสร้างคุณภาพชีวิต (กคส.)

5.7 กองพัฒนาสังคมกลุ่มเป้าหมายพิเศษ (กพพ.)

5.8 กลุ่มพัฒนาระบบบริหาร (กพร.)

5.9 กลุ่มตรวจสอบภายใน (กตส.)

5.10 ศูนย์ส่งเสริมจริยธรรมและต่อต้านการทุจริตกรมพัฒนาสังคมและสวัสดิการ (ศจท.)

6. รายละเอียดการบังคับใช้เอกสาร

กรมพัฒนาสังคมและสวัสดิการกำหนดรายละเอียดที่เกี่ยวข้องกับเอกสาร ดังต่อไปนี้

6.1 รายละเอียดของเอกสาร (Document control and review)

รายละเอียดของเอกสาร (Document control)	
ผู้จัดทำเอกสาร (Author)	กลุ่มเทคโนโลยีสารสนเทศ กองยุทธศาสตร์และแผนงาน
ผู้ดำเนินการตามเอกสาร (Owner)	กลุ่มเทคโนโลยีสารสนเทศ กองยุทธศาสตร์และแผนงาน
วันที่จัดทำเอกสาร (Date created)	วันที่ 7 พฤษภาคม 2569
ผู้ตรวจสอบความถูกต้องของเอกสาร (Last reviewed by)	หัวหน้ากลุ่มเทคโนโลยีสารสนเทศ กองยุทธศาสตร์และแผนงาน
วันที่ตรวจสอบความถูกต้องของเอกสาร (Last date reviewed)	วันที่ 7 พฤษภาคม 2569
ผู้อนุมัติเอกสาร และวันที่อนุมัติเอกสาร (Endorsed by and date)	ผู้อำนวยการกองยุทธศาสตร์และแผนงาน วันที่ 7 พฤษภาคม 2569
วันที่จะต้องมีการตรวจสอบเอกสารครั้งถัดไป (Next review due date)	วันที่ 7 พฤษภาคม 2570

6.2 การเปลี่ยนแปลงเอกสาร (Version control)

รุ่น (Version)	วันที่อนุมัติ (Date of Approval)	ผู้อนุมัติ (Approved by)	สถานะ (Description of change)
1	วันที่ 14 กุมภาพันธ์ 2567	ผู้อำนวยการกองยุทธศาสตร์และแผนงาน	อนุมัติ
2	วันที่ 7 พฤษภาคม 2569	ผู้อำนวยการกองยุทธศาสตร์และแผนงาน	อนุมัติ

7. เอกสารและกรอบมาตรฐานที่เกี่ยวข้อง

7.1 นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. 2563

7.2 นโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy policy) ของกรมพัฒนาสังคมและสวัสดิการ

8. นิยาม

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

เหตุภัยคุกคามทางไซเบอร์ (Cyber incident) หมายความว่า เหตุการณ์ที่มีผลเชิงลบที่เกิดจากการกระทำหรือการดำเนินการใด ๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึง ๆ ประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

ภัยคุกคามทางไซเบอร์ (Cyber threat) หมายความว่า การกระทำหรือการดำเนินการใด ๆ โดยมีชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

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

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

ภัยคุกคามที่ขับเคลื่อนด้วยปัญญาประดิษฐ์ (AI) หมายความว่า ภัยคุกคามไซเบอร์ที่มีการประยุกต์ใช้เทคโนโลยีปัญญาประดิษฐ์ (AI) หรือ Machine Learning เพื่อเพิ่มประสิทธิภาพในการโจมตี เช่น การสร้างอีเมลหลอกลวงที่แนบเนียน การปลอมแปลงตัวตนด้วยเสียงหรือภาพ (Deepfake) หรือการสแกนหาช่องโหว่ของระบบแบบอัตโนมัติขั้นสูง

9. บทบาทหน้าที่และโครงสร้างทีมรับมือเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์

9.1 ผู้รับแจ้งเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ภายในกรมพัฒนาสังคมและสวัสดิการ

กรมพัฒนาสังคมและสวัสดิการได้กำหนดข้อมูลการติดต่อของผู้รับแจ้งเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ภายในกรมพัฒนาสังคมและสวัสดิการ กรณีเมื่อมีการตรวจพบ หรือมีการรายงานเหตุการณ์เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์โดยควรมีผู้รับแจ้งเหตุฯ หลัก รวมถึงช่องทางหลักในการติดต่อ และเตรียมผู้รับแจ้งเหตุฯ คนที่สอง รวมถึงช่องทางสำรองสำหรับกรณีที่ไม่สามารถติดต่อผู้รับแจ้งเหตุคนแรกได้ โดยกรมพัฒนาสังคมและสวัสดิการกำหนดให้มีผู้ทำหน้าที่รับแจ้งเหตุฯ คลอบคลุมตลอดระยะเวลา 24 ชั่วโมง / 7 วัน

ลำดับ	ชื่อ – นามสกุล	ระยะเวลาในการปฏิบัติงาน	ช่องทางการติดต่อสื่อสาร	หน้าที่	ความรับผิดชอบ
1	(หลัก) นางสาวอังศุวรรณ คุ้มปรีดี (สำรอง) นางสาวภัคจิรา พูลสมบัติ	06.00 – 14.00 น.	เบอร์โทรศัพท์ติดต่อ : 0 2659 6229 เบอร์โทรศัพท์ติดต่อ : 0 2659 6363	- เฝ้าระวังดูแลระบบ - รับเรื่องแจ้งเหตุ - ประสานผู้ที่เกี่ยวข้อง	ทำหน้าที่ควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์ และรายงานผล
2	(หลัก) นายเมธา โตสวัสดิ์ (สำรอง) นายวงศ์เทพ ศิริรัตน์	14 .00 – 22.00 น.	เบอร์โทรศัพท์ติดต่อ : 0 2659 6229 เบอร์โทรศัพท์ติดต่อ : 0 2659 6363	- เฝ้าระวังดูแลระบบ - รับเรื่องแจ้งเหตุ - ประสานผู้ที่เกี่ยวข้อง	ทำหน้าที่ควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์ และรายงานผล
3	(หลัก) นายจิรภัทร จันทรรัตนะ (สำรอง) นางสาวสุจรรยา กสิกิจ	22.00 – 06.00 น.	เบอร์โทรศัพท์ติดต่อ : 0 2659 6229 เบอร์โทรศัพท์ติดต่อ : 0 2659 6363	- เฝ้าระวังดูแลระบบ - รับเรื่องแจ้งเหตุ - ประสานผู้ที่เกี่ยวข้อง	ทำหน้าที่ควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์ และรายงานผล

9.2 โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team : CIRT)

กรมพัฒนาสังคมและสวัสดิการใช้โมเดลโครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ เช่น แบบรวมศูนย์ (Centralize), แบบกระจาย (Distributed), แบบให้คำปรึกษา (Coordinating) หรือแบบอื่นตามบริบทของหน่วยงาน[2] โดยกรมพัฒนาสังคมและสวัสดิการได้กำหนดรายชื่อของบุคลากรที่มีความเกี่ยวข้องกับการรับมือเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ พร้อมทั้งโครงสร้างทีมรับมือฯ ดังนี้

ลำดับ	ชื่อ - นามสกุล	ช่องทางการติดต่อสื่อสาร	หน้าที่	ความรับผิดชอบ
1	นางนภารัตน์ เจริญรัตน์	เบอร์โทรศัพท์ติดต่อ : 0 2659 6226	หัวหน้าทีมรับมือฯ (Team manager)	ทำหน้าที่สื่อสารกับผู้บริหารของกรมพัฒนาสังคมและสวัสดิการ
2	นายศุภศิษฎ์ วิสิฐสรัลพร	เบอร์โทรศัพท์ติดต่อ : 0 2659 6227	รองหัวหน้าทีมรับมือฯ (Deputy team manager)	ทำหน้าที่แทนกรณีหัวหน้าทีมรับมือฯ ไม่อยู่/ไม่สามารถปฏิบัติงานได้
3	นางสาวอังศุวรรณ คุ้มปรีดี	เบอร์โทรศัพท์ติดต่อ : 0 2659 6229	เจ้าหน้าที่รับมือฯ (Incident leader)	ทำหน้าที่ช่วยเหลือให้สามารถควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์ได้
4	1. นางสาวภัคจิรา พูลสมบัติ 2. นายจิรภัทร จันทรรัตนะ	เบอร์โทรศัพท์ติดต่อ : 0 2659 6229	เจ้าหน้าที่เทคนิคฯ (Technical lead)	ทำหน้าที่ให้ความเห็นเกี่ยวกับแนวทางที่เหมาะสมในการควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์

[2] หน่วยงานอาจเลือกใช้โมเดลโครงสร้างทีมรับมือฯ แบบรวมศูนย์ (Centralize) แบบกระจาย (Distributed) แบบให้คำปรึกษา (Coordinating) หรือแบบอื่นๆ ตามบริบทของหน่วยงานที่อาจแตกต่างกัน ทั้งนี้ ท่านสามารถศึกษาเพิ่มเติมได้ที่ NIST SP 800-61r2 ข้อที่ 2.4 หน้าที่ 13

ทั้งนี้ นอกจากทีมรับมือฯ ดังกล่าวข้างต้น ให้มีบุคคลดังต่อไปนี้ทำหน้าที่สนับสนุนการดำเนินการของแผนรับมือฯ ฉบับนี้ ดังนี้

ลำดับ	ชื่อ - นามสกุล	ช่องทางการติดต่อสื่อสาร	หน้าที่	ความรับผิดชอบ
1	หัวหน้ากลุ่ม กฎหมาย	เบอร์โทรศัพท์ติดต่อ : 0 2659 6297	ผู้เชี่ยวชาญด้านกฎหมาย	ทำหน้าที่ควบคุม ดูแล และดำเนินการเกี่ยวกับคดี/ฟ้องร้องที่เกิดขึ้นกับกรมพัฒนาสังคมและสวัสดิการให้ถูกต้องตามกฎหมาย (พรบ. PDPA และ พรบ. Cyber)
2	เจ้าหน้าที่กลุ่ม กฎหมาย	เบอร์โทรศัพท์ติดต่อ : 0 2659 6229	เจ้าหน้าที่ด้านการปฏิบัติตามกฎหมาย (Compliance)	ดำเนินการจัดทำข้อมูล/ชี้แจงรายละเอียดข้อเท็จจริงตามเหตุละเมิด พรบ. PDPA และ พรบ. Cyber
3	หัวหน้า กพร.	เบอร์โทรศัพท์ติดต่อ : 0 2659 6243	ผู้บริหารจัดการความเสี่ยง	ทำหน้าที่ดูแลการบริหารจัดการความเสี่ยงให้สอดรับตามนโยบายความมั่นคงปลอดภัยสารสนเทศทางไซเบอร์
4	หัวหน้ากลุ่ม ประชาสัมพันธ์	เบอร์โทรศัพท์ติดต่อ : 0 2659 6245	ผู้รับผิดชอบด้านสื่อสารองค์กร	ทำหน้าที่เป็นช่องทางในการประชาสัมพันธ์การดำเนินงานตามแผน
4	นางสาวอังศุ วรรณ คุ้มปรีดี	เบอร์โทรศัพท์ติดต่อ : 0 2659 6229	เจ้าหน้าที่ประสานงาน	ทำหน้าที่ควบคุมผลกระทบจากภัยคุกคาม
6	บริษัท กู๊ดเซอร์วิส คอมพิวเตอร์ จำกัด	เบอร์โทรศัพท์ติดต่อ : 08 1354 2253	ผู้ทดสอบเจาะระบบ	ทำหน้าที่ทดสอบ หาช่องโหว่และแนวทางป้องกัน

9.3 หน่วยงานภายนอกที่เกี่ยวข้อง

กรมพัฒนาสังคมและสวัสดิการมีข้อมูลติดต่อสื่อสารของหน่วยงานภายนอกที่เกี่ยวข้อง เช่น สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.), หน่วยงานกำกับดูแล (Regulator), THAI – CERT และผู้ให้บริการภายนอกของกรมพัฒนาสังคมและสวัสดิการ เช่น หน่วยงานผู้ให้บริการด้านการตรวจสอบพิสูจน์หลักฐานทางดิจิทัล (Digital forensic investigator) เป็นต้น

ลำดับ	ชื่อ - นามสกุล	ช่องทางการติดต่อสื่อสาร	หน่วยงาน	ความเกี่ยวข้อง
1	บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) (NT : National Telecom Public Company Limited)	เบอร์โทรศัพท์ติดต่อ : 08 9762 7488 Email : paksangsila@gmail.com ที่อยู่สำนักงาน : บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) 99 ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ 10210	บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) (NT : National Telecom Public Company Limited)	ผู้ดูแลโครงสร้างและระบบเครือข่ายภายในกรมพัฒนาสังคมและสวัสดิการ
2	บริษัท กู๊ดเซอร์วิส คอมพิวเตอร์ จำกัด (Good Service Computer Co., Ltd.)	เบอร์โทรศัพท์ติดต่อ : 08 1354 2253 Email : support@goodservicecomputer.com ที่อยู่สำนักงาน : บริษัท กู๊ดเซอร์วิส คอมพิวเตอร์ จำกัด 68/869 หมู่ที่ 8 ซอยรัตนาธิเบศร์ 28 ถนนรัตนาธิบศร์ ตำบลบางกระสอ อำเภอเมือง จังหวัดนนทบุรี 11000	บริษัท กู๊ดเซอร์วิส คอมพิวเตอร์ จำกัด (Good Service Computer Co., Ltd.)	ผู้พัฒนาระบบสารสนเทศร่วมกับกรมพัฒนาสังคมและสวัสดิการ
3	บริษัท จิ๊กซอว์ อินโนเวชั่น จำกัด (Jigsaw Innovation Co., Ltd.)	เบอร์โทรศัพท์ติดต่อ : 08 6586 2599 Email : jigsawinnovation@gmail.com ที่อยู่สำนักงาน : 1569 อาคารภูฟ้า เพลส เลขที่ 177/1 ถนนคลองชลประทาน หมู่ 1 ตำบลช้างเผือก อำเภอเมือง เชียงใหม่ เชียงใหม่ 50300	บริษัท จิ๊กซอว์ อินโนเวชั่น จำกัด (Jigsaw Innovation Co., Ltd.)	ผู้พัฒนาระบบสารสนเทศร่วมกับกรมพัฒนาสังคมและสวัสดิการ

4	สำนักงาน คณะกรรมการ การรักษาความ มั่นคงปลอดภัย ไซเบอร์แห่งชาติ (สกมช.)	เบอร์โทรศัพท์ติดต่อ : 0 2142 6888 thaicert@ncsa.or.th ที่อยู่สำนักงาน : 120 หมู่ 3 อาคารรัฐประศาสน ภักดี (อาคารบี) ชั้น 7 ศูนย์ราชการ เฉลิมพระเกียรติ 80 พรรษา 5 ธันวาคม 2550 ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ 10210	สำนักงาน คณะกรรมการการ รักษาความมั่นคง ปลอดภัยไซเบอร์ แห่งชาติ (สกมช.)	ตามหน้าที่และ อำนาจของ สำนักงาน คณะกรรมการ การรักษาความ มั่นคงปลอดภัย ไซเบอร์แห่งชาติ (สกมช.)
5	เคมิท กรุ๊ป จำกัด	เบอร์โทรศัพท์ติดต่อ : 0 2049 1740 www.kmit-group.com ที่อยู่สำนักงาน :บริษัท เคเมิท กรุ๊ป จำกัด 89 อาคารคอสโม ออฟฟิศ พาร์ค ชั้น 5 ยูนิต ไอ ถนนป๊อปปู ล่า ตำบลบ้านใหม่ อำเภอปากเกร็ด จังหวัดนนทบุรี 11120	บริษัท เคเมิท กรุ๊ป จำกัด	ผู้รักษาความ มั่นคงปลอดภัย ด้านเทคโนโลยี สารสนเทศ ทั้ง ตรวจสอบ และ ซ่อมแซม อุปกรณ์ คอมพิวเตอร์
6	โอดีโอ โซลูชั่น จำกัด	บริษัท โอดีโอ โซลูชั่น จำกัด (สำนักงานใหญ่) 89/397 หมู่ 10 ถนนรัตนาธิเบศร์ ต.บางรักใหญ่ อ.บางบัวทอง จ. นนทบุรี 11110 โทร. 02-0130458 เลขประจำตัว ผู้เสียภาษีอากร 0125556027373	บริษัท โอดีโอ โซลูชั่น จำกัด	ผู้ให้บริการและ ดูแลระบบ กลุ่มเป้าหมาย ราษฎรบนพื้นที่ สูง

9.4 โครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure)

กรมพัฒนาสังคมและสวัสดิการจัดทำแผนผังโครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure) ของบุคลากรภายในทีมรับมือฯ ผู้บริหารหน่วยงาน หน่วยงานกำกับดูแล หน่วยงานรับแจ้งเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ตามกฎหมาย และหน่วยงานภายนอก เป็นต้น รวมถึงกำหนดว่าหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจะปฏิบัติตามภาระหน้าที่ในการรายงานภายใต้พระราชบัญญัติ และกฎหมายย่อยใด ๆ ที่ทำขึ้นภายใต้กฎหมายดังกล่าว ตลอดจนภาระหน้าที่ในการรายงานภายใต้กฎหมาย และข้อกำหนดด้านกฎระเบียบที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (ตามภาคผนวก 1)

10. 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 นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. 2563 ดังนี้

10.1 ขั้นการเตรียมการ (Preparation)

กรมพัฒนาสังคมและสวัสดิการดำเนินมาตรการเพื่อเตรียมการและป้องกันการเกิดภัยคุกคามทางไซเบอร์ (Preparation) เป็นสิ่งที่จะต้องทำในระยะเริ่มต้น เพื่อเตรียมความพร้อมเมื่อต้องเผชิญเหตุ ได้แก่ การจัดเตรียมข้อมูลให้พร้อม การจัดตั้งและฝึกอบรมบุคลากรหรือทีมงาน การจัดหาเครื่องมือและทรัพยากรต่าง ๆ ที่จำเป็น การตั้งค่าระบบต่าง ๆ ให้ปลอดภัย การจัดทำนโยบาย แผนงาน และกระบวนการที่เกี่ยวข้อง รวมถึง การสร้างเครือข่ายความร่วมมือ โดยดำเนินการดังต่อไปนี้

(1) กำหนดโครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT) รายละเอียดปรากฏตามข้อ 9.2

(2) กำหนดโครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure) รายละเอียดปรากฏตามข้อ 9.4

(3) กำหนดเกณฑ์และขั้นตอนในการเรียกใช้งาน (Activate) การตอบสนองต่อเหตุการณ์ และ CIRT (ตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. 2563)

(4) จัดเตรียมข้อมูลและอุปกรณ์ รวมถึงช่องทางในการติดต่อสื่อสารที่จำเป็น เช่น ข้อมูลการติดต่อและอุปรกรณ์ติดต่อสื่อสารของบุคลากร, กลไกรายงานเหตุการณ์ เป็นต้น

(5) จัดเตรียมอุปกรณ์, ซอฟต์แวร์ และแหล่งข้อมูลสำหรับวิเคราะห์เหตุภัยคุกคามทางไซเบอร์

(6) จัดให้มีการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของกรมพัฒนาสังคมและสวัสดิการ (Risk assessment)

(7) จัดเตรียมและส่งเสริมการนำเทคโนโลยีปัญญาประดิษฐ์ (AI) และกระบวนการทำงานแบบอัตโนมัติ (Automation) มาประยุกต์ใช้เพื่อเพิ่มประสิทธิภาพในการเฝ้าระวัง ป้องกัน และวิเคราะห์ความเสี่ยงล่วงหน้า ตลอดจนจัดให้มีการสร้างความตระหนักรู้และอบรมบุคลากรให้รู้เท่าทันรูปแบบการโจมตีทางไซเบอร์ขั้นสูงที่อาศัย AI เป็นเครื่องมือ (เช่น การสร้างเนื้อหาหลอกลวงที่แนบเนียนด้วย AI หรือการปลอมแปลงตัวตนด้วยเทคนิค Deepfake)

(8) จัดให้มีการติดตามและประเมินความเสี่ยงจากเทคโนโลยีอุบัติใหม่ โดยเฉพาะการก้าวกระโดดของคอมพิวเตอร์ควอนตัม (Quantum Computing) ที่อาจส่งผลกระทบต่อมาตรฐานการเข้ารหัสข้อมูลแบบดั้งเดิม พร้อมทั้งเตรียมความพร้อมในการศึกษาและยกระดับระบบโครงสร้างพื้นฐานเพื่อรองรับมาตรฐานการเข้ารหัสลับหลังยุคควอนตัม (Post-Quantum Cryptography : PQC) เพื่อปกป้องข้อมูลสำคัญและข้อมูลส่วนบุคคลของหน่วยงานในระยะยาว

(9) จัดให้มีการซักซ้อมแผนรับมือเหตุภัยคุกคามทางไซเบอร์ หรือการทดสอบจำลองสถานการณ์ร่วมกับผู้บริหารและทีมงานที่เกี่ยวข้อง เพื่อประเมินความพร้อม ทดสอบความเข้าใจและปรับปรุงขั้นตอนการปฏิบัติงานให้มีประสิทธิภาพอยู่เสมอ

(10) จัดทำกระบวนการบริหารจัดการช่องโหว่ (Vulnerability Management) โดยกำหนดให้มีการสแกนหาช่องโหว่ของระบบ (Vulnerability Assessment) และการทดสอบเจาะระบบ (Penetration Testing) เพื่อระบุและแก้ไขจุดอ่อนก่อนที่จะถูกผู้ไม่หวังดีนำไปใช้ประโยชน์

(11) กำหนดมาตรการประเมินความเสี่ยงและตรวจสอบการรักษาความมั่นคงปลอดภัยของบุคคลที่สาม เช่น ผู้ให้บริการภายนอก (Outsource) บริษัทคู่ค้า หรือผู้พัฒนาระบบ เพื่อป้องกันภัยคุกคามทางไซเบอร์ที่อาจเกิดจากการเชื่อมต่อหรือห่วงโซ่อุปทาน

(12) จัดเตรียมและทดสอบการกู้คืนระบบสำรองข้อมูล โดยใช้หลักการจัดเก็บข้อมูลสำรองที่ปลอดภัยจากการถูกดัดแปลงหรือเข้ารหัส (เช่น Immutable Backup หรือ Offline Backup) เพื่อให้มั่นใจว่ากรมพัฒนาสังคมและสวัสดิการจะสามารถกู้คืนข้อมูลสำคัญและกลับมาให้บริการได้ทันทีหากเผชิญกับการโจมตีของโปรแกรมเรียกค่าไถ่

(13) จัดทำแผนผังโครงสร้างขั้นตอนการรับมือภัยคุกคามทางไซเบอร์ของกรมพัฒนาสังคมและสวัสดิการ โดยมีตัวอย่างแผนผังโครงสร้างขั้นตอนการรับมือฯ (รายละเอียดปรากฏตามภาคผนวก 1)

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

10.2 ขั้นการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (Detection and analysis)

กรมพัฒนาสังคมและสวัสดิการดำเนินการในการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ ซึ่งเป็นสิ่งจำเป็นที่จะช่วยให้กรมพัฒนาสังคมและสวัสดิการสามารถบรรเทาความเสี่ยงที่ยังคงเหลืออยู่ และสามารถแจ้งเตือนได้อย่างทันท่วงที เมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น โดยดำเนินการดังต่อไปนี้

(1) กรมพัฒนาสังคมและสวัสดิการดำเนินการจัดเตรียมแนวทางรับมือเมื่อเกิดการโจมตีรูปแบบทั่วไปที่เคยเกิดขึ้นหรืออาจเกิดขึ้นกับกรมพัฒนาสังคมและสวัสดิการ (Common Attack Vectors / Common Threat Vectors) โดยการโจมตีรูปแบบทั่วไปที่อาจเกิดขึ้น ดังนี้

ประเภท	อธิบาย	ระยะเวลาการกู้คืนระบบ (SLA)
ระดับ 0 (ระดับต่ำ)	เหตุการณ์ที่มีผลกระทบน้อยที่สุด ตัวอย่างอาจเป็นอีเมลขยะ การติดไวรัส ฯลฯ	ภายใน 1 ชั่วโมง
ระดับ 1 (ระดับปานกลาง)	เหตุการณ์ที่มีผลกระทบอย่างมีนัยสำคัญ ตัวอย่างอาจเป็นความล่าช้าหรือความสามารถที่จำกัดในการให้บริการ การส่งจดหมายอิเล็กทรอนิกส์หรือการถ่ายโอนข้อมูลที่สำคัญล่าช้า เป็นต้น	ภายในไม่เกิน 4 ชั่วโมง
ระดับ 2 (ระดับสูง)	เหตุการณ์ที่เกิดผลกระทบรุนแรง ตัวอย่างการหยุดชะงักในการให้บริการ การปฏิบัติหน้าที่ ข้อมูลที่เป็นกรรมสิทธิ์หรือข้อมูลที่เป็นความลับของถูกบุกรุกด้วยไวรัสหรือเวิร์มแพร่กระจายอย่างกว้างขวางและส่งผลกระทบต่อพนักงานมากกว่า 1 เปอร์เซ็นต์ ระบบความปลอดภัยสาธารณะไม่พร้อมใช้งาน หรือผู้บริหารระดับสูงได้รับแจ้งแล้ว	มากกว่า 4 ชั่วโมงขึ้นไป
ระดับ 3 (ระดับร้ายแรง)	เหตุการณ์ที่ส่งผลกระทบอย่างร้ายแรง ตัวอย่าง การปิดกั้นบริการเครือข่ายทั้งหมด ข้อมูลที่เป็นกรรมสิทธิ์หรือเป็นความลับถูกบุกรุกและเผยแพร่บนสถานที่หรือไซต์สาธารณะ ระบบความปลอดภัยสาธารณะใช้งานไม่ได้ ฝ่ายบริหารจะต้องแถลงต่อสาธารณะ	มากกว่า 8 ชั่วโมงขึ้นไป

(2) กรมพัฒนาสังคมและสวัสดิการมีทีมรับมือเหตุภัยคุกคามทางไซเบอร์ (CIRT) ที่สามารถตรวจจับสิ่งบ่งชี้หรือลักษณะเบื้องต้นของการเกิดภัยคุกคามทางไซเบอร์ได้ในเวลาอันเหมาะสม โดยอาจอาศัยข้อมูลจากแหล่งข้อมูลต่าง ๆ รวมถึงมีคณะกรรมการธรรมาภิบาลข้อมูลภาครัฐ กรมพัฒนาสังคมและสวัสดิการ ซึ่งมีหน้าที่ กำหนดนโยบาย กรอบแนวทางมาตรฐานข้อมูล และทิศทางการดำเนินงานด้านธรรมาภิบาลข้อมูล ตรวจสอบและกำกับการปฏิบัติงานของผู้ที่เกี่ยวข้อง ประเมินความพร้อมของธรรมาภิบาลข้อมูลภาครัฐ คุณภาพข้อมูล ความมั่นคงปลอดภัยของข้อมูล และการรักษาความเป็นส่วนบุคคล และคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล กรมพัฒนาสังคมและสวัสดิการ ซึ่งมีหน้าที่ จัดทำร่างแผนแม่บทการดำเนินงานด้านการส่งเสริม และการคุ้มครองข้อมูลส่วนบุคคล วิเคราะห์และรับรองความสอดคล้องและความถูกต้องตามมาตรฐาน หรือตามมาตรการหรือกลไกการกำกับดูแลที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล รวมทั้งติดตามความเคลื่อนไหวของสถานการณ์ด้านการคุ้มครองข้อมูลส่วนบุคคล

(3) กรมพัฒนาสังคมและสวัสดิการมีขั้นตอนการรับมือภัยคุกคามทางไซเบอร์ (ภาคผนวก 1) ในการรับแจ้งเหตุและแก้ไขเหตุการณ์ เพื่อไม่ให้เกิดผลกระทบที่รุนแรง เช่น การหยุดชะงักในการให้บริการและ/หรือการปฏิบัติหน้าที่ภารกิจของกรมฯ ข้อมูลที่เป็นกรรมสิทธิ์หรือเป็นความลับถูกบุกรุก ไวรัสหรือเวิร์มแพร่กระจายอย่างกว้างขวางและส่งผลกระทบต่อพนักงานมากกว่า 1 เปอร์เซ็นต์ ระบบความปลอดภัยสาธารณะไม่พร้อมใช้งาน หรือผู้บริหารระดับสูงได้รับแจ้ง จัดให้มีแนวทางในการวิเคราะห์ผลกระทบและระดับของภัยคุกคามทางไซเบอร์ (Incident prioritization) เพื่อรับมือกับภัยคุกคามทางไซเบอร์ให้ทันท่วงที โดยพิจารณาปัจจัยต่าง ๆ ที่เกี่ยวข้อง เช่น ผลกระทบต่อการทำงานของระบบ (Functional impact) ผลกระทบต่อข้อมูล (Information impact) และความสามารถในการกู้คืน (Recoverability effort[3]) เป็นต้น

(4) กรมพัฒนาสังคมและสวัสดิการมีการบันทึกรายงานสถานการณ์เหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ โดยอาจกำหนดให้มีรายละเอียดตามแบบฟอร์มตัวอย่าง (รายละเอียดปรากฏตามภาคผนวก 2)

(5) กรมพัฒนาสังคมและสวัสดิการมีการจัดทำบันทึกข้อมูลกิจกรรมเหตุการณ์ความปลอดภัยทางไซเบอร์ (Incident documentation) โดยกรมพัฒนาสังคมและสวัสดิการบันทึกข้อมูลเกี่ยวกับเหตุการณ์ความปลอดภัยทางไซเบอร์ ทุกขั้นตอนตั้งแต่ตรวจพบเหตุการณ์จนถึงกระบวนการสุดท้าย และข้อมูลเกี่ยวกับเหตุการณ์ความปลอดภัยทางไซเบอร์โดยระบุรายละเอียด พร้อมเวลาที่เกิดเหตุ และระยะเวลาที่ใช้บันทึกข้อมูลที่เกี่ยวข้องกับเหตุการณ์ลงวันที่และลงนาม โดยผู้มีหน้าที่จัดการรับมือเหตุการณ์นั้น ๆ เพื่อให้มั่นใจได้ว่าเหตุการณ์ความปลอดภัยทางไซเบอร์ที่เกิดขึ้น จะได้รับการจัดการแก้ไขภายในระยะเวลาที่เหมาะสม โดยกำหนดให้มีรายละเอียดตามแบบฟอร์ม (รายละเอียดปรากฏตามภาคผนวก 3)

(6) กรมพัฒนาสังคมและสวัสดิการดำเนินการกรณีหน่วยงานรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจะต้องจัดให้มีการรายงานภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับบริการของโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้ผู้ที่เกี่ยวข้องทราบ ตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ. 2566 ดังนี้

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

(ก) กรณีมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นกับหน่วยงานรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศตาม ข้อ 4 แห่งประกาศฯ ฉบับดังกล่าว ให้ใช้แบบฟอร์ม ก1 โดยใช้แบบฟอร์มการรายงานตามกฎหมาย (รายละเอียดปรากฏตามภาคผนวก 4)

(ข) กรณีมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญต่อระบบของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศกับหน่วยงานรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศตาม ข้อ 5 แห่งประกาศฯ ฉบับดังกล่าว ให้ใช้แบบฟอร์ม ก2 รายงานไปยัง สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ภายในระยะเวลา 24 ชั่วโมง โดยใช้แบบฟอร์มการรายงานตามกฎหมาย (รายละเอียดปรากฏตามภาคผนวก 4)

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

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

10.3 ขั้นตอนการระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ (Containment, Eradication, and Recovery)

กรมพัฒนาสังคมและสวัสดิการดำเนินการเพื่อระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ โดยควรกำหนดให้สอดคล้องกับความรุนแรงและระดับของภัยคุกคามทางไซเบอร์แต่ละระดับจนกระทั่งสามารถกู้คืนทรัพย์สินสำคัญทางสารสนเทศให้กลับมาดำเนินงานหรือให้บริการได้ตามปกติ ซึ่ง การดำเนินการในขั้นตอนนี้อาจจะต้องกระทำควบคู่ไปกับการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ที่ 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 กรมพัฒนาสังคมและสวัสดิการพิจารณาได้ดำเนินการตามเอกสารแนบท้าย 2 ตารางที่ 2.3 ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. 2564 เพิ่มเติม

10.4 ขั้นตอนการดำเนินการภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ (Post-Incident activity)

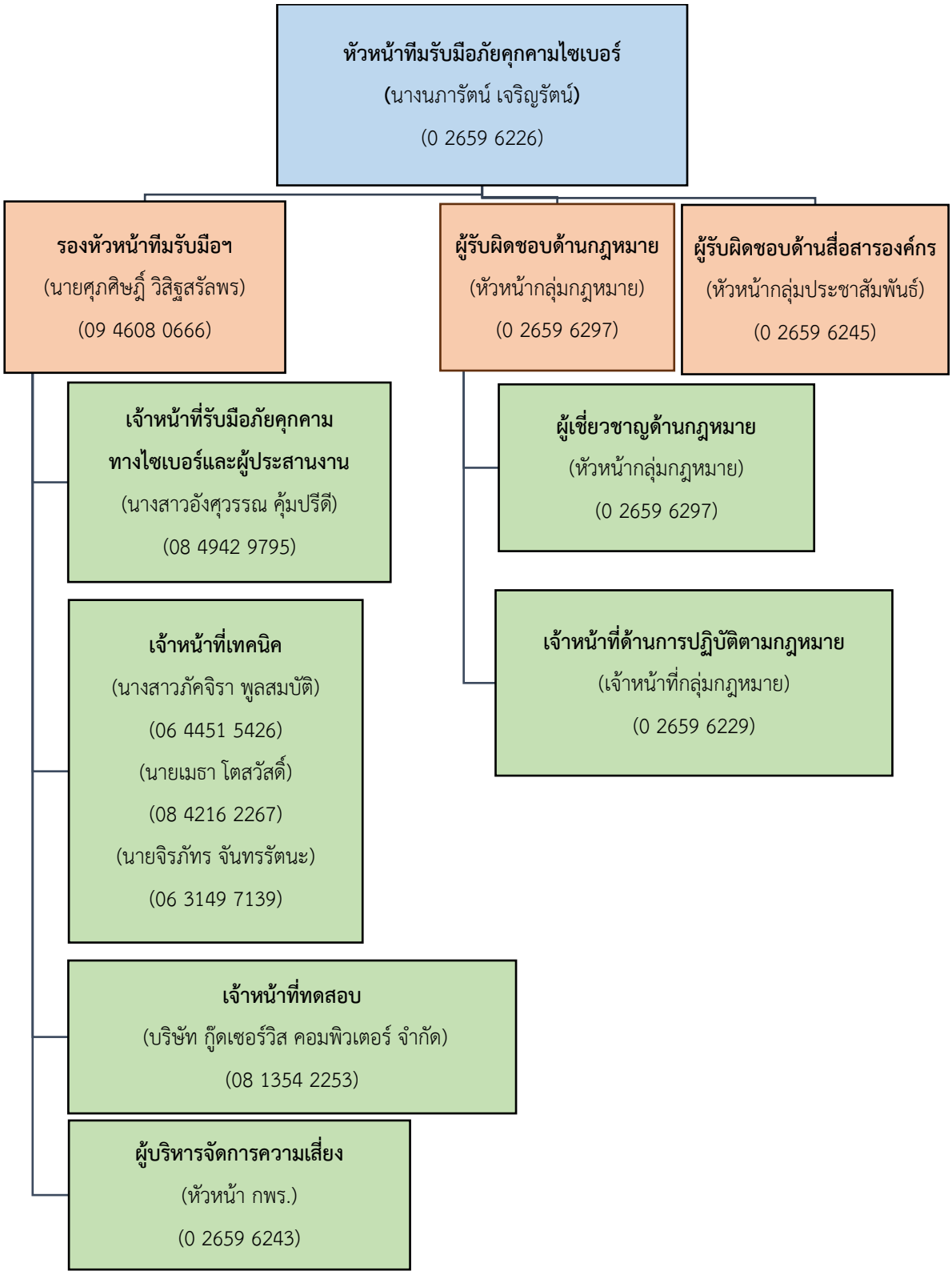
กรมพัฒนาสังคมและสวัสดิการกำหนดขั้นตอน วิธี ปฏิบัติ หรือกำหนดนโยบายภายในที่เกี่ยวข้อง เพื่อให้มีแนวทางที่ชัดเจน ซึ่งการปฏิบัติตามมาตรการดังกล่าว จะช่วยให้กรมพัฒนาสังคมและสวัสดิการสามารถเรียนรู้จากเหตุภัยคุกคามทางไซเบอร์ที่ผ่านมา และสามารถหาแนวทางเพื่อแก้ไข จุดบกพร่องและพัฒนาแนวทางรับมือกับภัยคุกคามทางไซเบอร์ต่อไปในอนาคต นอกจากนี้กรมพัฒนาสังคมและสวัสดิการต้องเก็บ รักษาข้อมูลและพยานหลักฐานที่จำเป็น เพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์ หรือใช้ในกรณีที่ต้องการร้องทุกข์หรือดำเนินคดี เนื่องจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้นนั้น อาจเข้าลักษณะเป็นความผิดตามประมวล กฎหมายอาญา หรือพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 และที่แก้ไข เพิ่มเติม (ถ้ามี) หรือกฎหมายอื่น ๆ ที่เกี่ยวข้อง ประกอบด้วยการทบทวนหลังการดำเนินการ (After-Action Review Process) เพื่อระบุและแนะนำให้ปรับปรุงการดำเนินการเพื่อป้องกันการเกิดซ้ำ นอกจากนี้ควรมีการรวบรวมข้อมูลเชิงลึกด้านภัยคุกคาม รวมถึงเทคนิค รูปแบบ และขั้นตอนการโจมตี (TTPs: Tactics, Techniques, and Procedures) ที่ตรวจพบจากเหตุการณ์ มาปรับปรุงกฎการตรวจจับในระบบรักษาความปลอดภัย และพิจารณาแบ่งปันข้อมูลดังกล่าวให้กับเครือข่ายเฝ้าระวังของหน่วยงานภาครัฐที่เกี่ยวข้องเพื่อป้องกันการโจมตีในอนาคต

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

10.5. การจัดทำรายการตรวจสอบการจัดการเหตุการณ์ (Incident Handling Checklist)

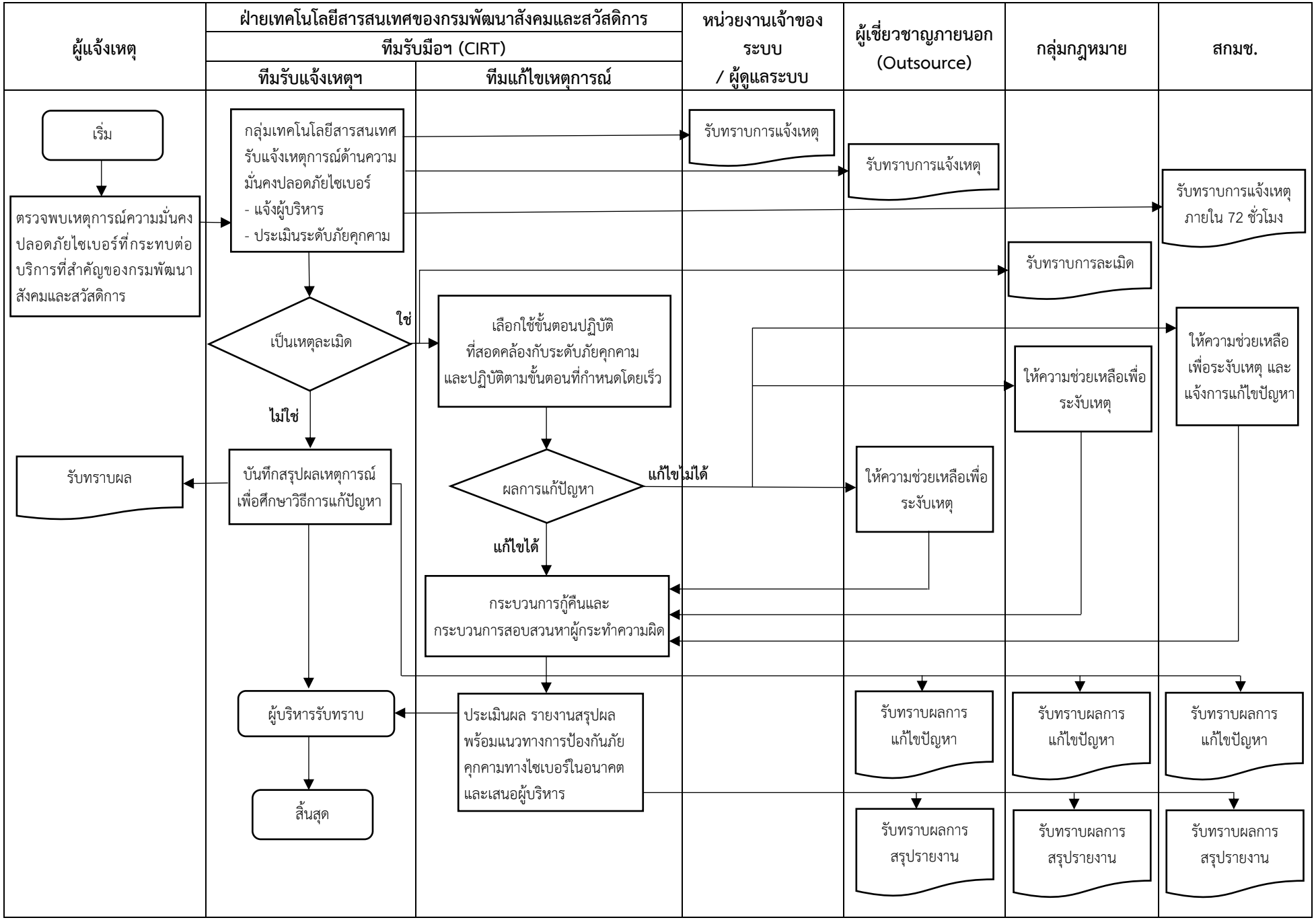
กรมพัฒนาสังคมและสวัสดิการจัดทำรายการตรวจสอบการจัดการเหตุการณ์ (Incident Handling Checklist) ซึ่งจะช่วยให้แนวทางแก่กรมพัฒนาสังคมและสวัสดิการเกี่ยวกับขั้นตอนสำคัญที่ควรดำเนินการโดยกรมพัฒนาสังคมและสวัสดิการสามารถใช้ข้อมูลเพื่อประกอบการพิจารณาความเหมาะสมในการจัดทำรายการตรวจสอบของตนเองได้ (รายละเอียดปรากฏตามภาคผนวก 5)

แผนผังแสดงโครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์
กรมพัฒนาสังคมและสวัสดิการ
(Cyber Incident Response Team : CIRT)



ภาคผนวก 1

แผนผังโครงสร้างขั้นตอนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response) ของกรมพัฒนาสังคมและสวัสดิการ



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[4] ในระดับใด (มาตรา 60)

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

☐ ยังไม่สามารถระบุได้

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)

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

[4] พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 กำหนดความหมายของ “ภัยคุกคามทางไซเบอร์” ดังนี้ การกระทำหรือการดำเนินการใด ๆ โดยมิชอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบ ต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

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[5] ในระดับใด (มาตรา 60) ☐ ไม่ร้ายแรง ☐ ร้ายแรง ☐ วิกฤต (ก) ☐ วิกฤต (ข) ☐ ยังไม่สามารถระบุได้

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

หมวด ข. ข้อมูลการตรวจพบภัยคุกคามไซเบอร์

ข1. วัน เวลา ที่เกิดเหตุภัยคุกคาม

วันที่ : เลือกวันที่ เวลา : โปรดระบุ

วัน เวลา ที่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศทราบเหตุภัยคุกคาม

วันที่ : เลือกวันที่ เวลา : โปรดระบุ

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[6]

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)	
สวิตซ์ (Switch) /เราเตอร์ (Router)	
เว็บไซต์ (Website)	
อื่น ๆ	

ข้อ 3 สถิติรายปีจำแนกตามระดับภัยคุกคามทางไซเบอร์[7]

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

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

[7] ระดับภัยคุกคามทางไซเบอร์ตามมาตรา 60 แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562

ภาคผนวก 5

ตัวอย่าง : รายการตรวจสอบการจัดการเหตุการณ์ (Incident Handling Checklist)

	รายการตรวจสอบการจัดการเหตุการณ์	Complete
	ขั้นการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (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	
	ขั้นการระงับภัยคุกคาม ปราบปราม และฟื้นฟูระบบงานที่ได้รับผลกระทบ (containment, eradication, and recovery)	
4	บันทึกเหตุการณ์, จัดเก็บและดูแลรักษาหลักฐานเกี่ยวกับเหตุการณ์ทั้งหมดก่อนเริ่มกระบวนการกู้คืนซึ่งรวมถึงการได้มาของบันทึกการยึดหลักฐานคอมพิวเตอร์ที่ได้มาหรืออุปกรณ์อื่น ๆ เพื่อสนับสนุนการสอบสวน	
5	จำกัดขอบเขต (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์	
6	ดำเนินการสอบสวน (Investigate) สาเหตุและผลกระทบของเหตุการณ์	
7	ทำการกำจัดสาเหตุ (Eradicate the incident)	
7.1	ระบุช่องโหว่ของระบบที่โดนโจมตีและบรรเทาผลกระทบที่เกิดขึ้น	
7.2	กำจัด หรือลบมัลแวร์ และสาเหตุภัยคุกคามอื่นๆ	
7.3	หากมีการตรวจพบว่ามีระบบใหม่ได้รับผลกระทบ (เช่น การติดมัลแวร์ใหม่) ให้ทำซ้ำขั้นตอนการตรวจจับและการวิเคราะห์ภัยคุกคามทางไซเบอร์ (detection and analysis)	
7.4	ตรวจสอบการลักลอบนำข้อมูลออกนอกระบบเครือข่ายองค์กร (Data Exfiltration) และประเมินความเสี่ยงกรณีข้อมูลส่วนบุคคลรั่วไหล เพื่อเตรียมความพร้อมในการดำเนินการตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล (PDPA)	
8	เรียกใช้งานกระบวนการกู้คืน (Recovery Process)	
8.1	ระบบที่ได้รับผลกระทบจากภัยคุกคามกลับสู่สถานะพร้อมใช้งาน	

8.2	ยืนยันว่าระบบที่ได้รับผลกระทบกลับมาทำงานได้ตามปกติ	
8.3	หากจำเป็น ให้ดำเนินการติดตามสถานการณ์ต่อไป เพื่อค้นหาเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ที่อาจเกี่ยวข้องในอนาคต	
การดำเนินการภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ (Post-Incident Activity)		
9	จัดทำรายงานการติดตามผล	
10	จัดการประชุมทบทวนบทเรียนที่เกิดจากเหตุการณ์ดังกล่าว	

แหล่งที่มา

- ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ.2564
- ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ.2564
- ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ.2566
- NIST SP 800-61r2 Computer Security Incident Handling Guide
- ACSC Cyber Incident Response Plan Guidance