



แผนรองรับสถานการณ์ฉุกเฉินเทคโนโลยีสารสนเทศและความมั่นคงทางไซเบอร์
หน่วยงาน มหาวิทยาลัยราชภัฏนครราชสีมา ประจำปี 2568

1. หลักการและเหตุผล

แผนรองรับสถานการณ์ฉุกเฉินเทคโนโลยีสารสนเทศและความมั่นคงทางไซเบอร์ ของ มหาวิทยาลัยราชภัฏนครราชสีมา ฉบับนี้ จัดทำขึ้นเพื่อให้เป็นไป ตามมาตรา 44 แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 ที่กำหนดให้หน่วยงาน ของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเร็ว ซึ่งอย่างน้อยต้องประกอบด้วยเรื่อง (1) แผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยผู้ตรวจประเมิน ผู้ตรวจสอบภายใน หรือผู้ตรวจสอบอิสระจากภายนอก อย่างน้อยปีละหนึ่งครั้งและ (2) แผนการรับมือภัยคุกคามทางไซเบอร์ รวมทั้งเพื่อให้เป็นไปตาม นโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของมหาวิทยาลัยราชภัฏนครราชสีมา ด้วย

2. วัตถุประสงค์

เพื่อใช้เป็นแผนรองรับสถานการณ์ฉุกเฉินเทคโนโลยีสารสนเทศและความมั่นคงทางไซเบอร์ ที่เกิดขึ้นใน มหาวิทยาลัยราชภัฏนครราชสีมา โดยจะเป็นการกำหนดหน้าที่และความรับผิดชอบให้กับหน่วยงานต่างๆ ภายใต้ มหาวิทยาลัยราชภัฏนครราชสีมา การกำหนดประเภทของเหตุภัยคุกคามทาง ไซเบอร์ การกำหนดความสัมพันธ์กับ นโยบายและแนวปฏิบัติที่เกี่ยวข้อง การรายงานเหตุภัยคุกคามทางไซเบอร์ และขั้นตอนการรับมือเหตุภัยคุกคามทางไซเบอร์ ตามขอบเขตของระบบสารสนเทศที่กำหนดไว้ รวมไปถึงการสื่อสารไปยังผู้มีส่วนได้ส่วนเสีย เพื่อลดผลกระทบที่อาจเกิดขึ้นต่อการดำเนินงานของ มหาวิทยาลัยราชภัฏนครราชสีมา

3. ขอบเขต

แผนรับมือฯ ฉบับนี้ ใช้รับมือเหตุภัยคุกคามทางไซเบอร์ที่เกิดขึ้นต่อระบบสารสนเทศ และข้อมูลดิจิทัลของ มหาวิทยาลัยราชภัฏนครราชสีมา รวมถึงบุคคลหรืออุปกรณ์ใดๆ ซึ่งเข้าถึงระบบสารสนเทศ และข้อมูลดิจิทัลดังกล่าว

4. หน้าที่การทบทวนแผน

สำนักคอมพิวเตอร์ มีหน้าที่ทบทวนและขออนุมัติแผนรับมือฯ ฉบับนี้ถึง ผู้บริหารสูงสุดหรือผู้ที่รับมอบอำนาจ หน่วยงานของท่าน

5. หน้าที่ในการดำเนินการตามแผน

สำนักคอมพิวเตอร์ มีหน้าที่เป็นผู้รับผิดชอบหลักในการดำเนินการ ตามแผนรับมือฯ ฉบับนี้ โดยมีหน่วยงาน สนับสนุนประกอบด้วย สำนักวิทยบริการและเทคโนโลยีสารสนเทศ รวมถึง สำนักส่งเสริมวิชาการและงานทะเบียน และ กองบริหารงานบุคคล และหน่วยงานภายในมหาวิทยาลัย

6. รายละเอียดการบังคับใช้เอกสาร

หน่วยงานจะต้องระบุรายละเอียดที่เกี่ยวข้องกับเอกสาร ดังต่อไปนี้

6.1. รายละเอียดของเอกสาร (Document control and review)

รายละเอียดของเอกสาร (Document control)	
ผู้จัดทำเอกสาร (Author)	ผศ.ดร.สายสุนีย์ จีบโจร
ผู้ดำเนินการตามเอกสาร (Owner)	นายอนุพงษ์ โพธิ์
วันที่จัดทำเอกสาร (Date created)	23 กุมภาพันธ์ 2568
ผู้ตรวจสอบความถูกต้องของเอกสาร (Last reviewed by)	นายอนุพงษ์ โพธิ์
วันที่ตรวจสอบความถูกต้องของเอกสาร (Last date reviewed)	23 กุมภาพันธ์ 2568
ผู้อนุมัติเอกสาร และวันที่อนุมัติเอกสาร (Endorsed by and date)	รศ.ดร.อดิศร เนาวนนท์ 23 กุมภาพันธ์ 2568
วันที่จะต้องมีการตรวจสอบเอกสารครั้ง ถัดไป (Next review due date)	23 กุมภาพันธ์ 2569

6.2. การเปลี่ยนแปลงเอกสาร (Version control)

รุ่น (Version)	วันที่อนุมัติ (Date of Approval)	ผู้อนุมัติ (Approved by)	สถานะ (Description of change)
2.0a	23 กุมภาพันธ์ 2568	รศ.ดร.อดิศร เนาวนนท์	Active

7. เอกสารและกรอบมาตรฐานที่เกี่ยวข้อง

- 7.1 นโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของมหาวิทยาลัยราชภัฏนครราชสีมา
- 7.2 นโยบายและแนวปฏิบัติด้านการปกป้องข้อมูลส่วนบุคคลของของมหาวิทยาลัยราชภัฏนครราชสีมา
- 7.3 ประกาศ เรื่องวิธีปฏิบัติการใช้งานระบบคอมพิวเตอร์และเครือข่ายของมหาวิทยาลัยราชภัฏนครราชสีมา

8. นิยาม

เหตุการณ์ (Event) หมายความว่า เหตุการณ์ที่เกิดขึ้นจากการเฝ้าระวังสังเกตการณ์ (observable occurrence) ในระบบ เครือข่าย สภาพแวดล้อม กระบวนการ ลำดับการดำเนินการ หรือบุคลากร เหตุการณ์อาจมีหรือไม่ มีลักษณะที่ส่งผลเชิงลบก็ได้

เหตุภัยคุกคามทางไซเบอร์ (Cyber incident) หมายความว่า เหตุการณ์ที่มีผลเชิงลบที่เกิดจากการ กระทำ หรือการดำเนินการใด ๆ โดยมีขอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นอันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

ภัยคุกคามทางไซเบอร์ (Cyber threat) หมายความว่า การกระทำหรือการดำเนินการใด ๆ โดยมี ขอบโดยใช้ คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นอันตรายที่ใกล้จะถึงที่จะ ก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

เหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญ¹ หมายความว่า เหตุภัยคุกคามทางไซเบอร์ที่ปรากฏต่อระบบสารสนเทศ และเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามมาตรา 49 ซึ่งคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติได้กำหนดลักษณะของภัยคุกคามทางไซเบอร์ไว้ตามมาตรา 60 แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562

9. บทบาทหน้าที่และโครงสร้างที่รับมือเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์

9.1. ผู้รับแจ้งเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ภายในหน่วยงาน

หน่วยงานควรระบุข้อมูลการติดต่อของผู้รับแจ้งเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ภายในหน่วยงาน กรณีเมื่อมีการตรวจพบ หรือมีการรายงานเหตุการณ์เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ โดยควรมีผู้รับแจ้งเหตุฯ หลัก รวมถึงช่องทางหลักในการติดต่อ และเตรียมผู้รับแจ้งเหตุฯ คนที่สอง รวมถึงช่องทางสำรองสำหรับกรณีที่ไม่สามารถติดต่อผู้รับแจ้งเหตุคนแรกได้ โดยหน่วยงานควรจะกำหนดให้มีผู้ทำหน้าที่รับแจ้งเหตุฯ คลอบคลุมตลอดระยะเวลา 24 ชั่วโมง/ 7 วัน

ลำดับ	ชื่อ – นามสกุล	ระยะเวลาในการปฏิบัติงาน	ช่องทางการติดต่อสื่อสาร	หน้าที่	ความรับผิดชอบ
1	นายอนุพงษ์ โพธิ์	8.30-16.30	083-4611434	หัวหน้าผู้รับแจ้งเหตุ	รับแจ้งเหตุการโจมตี
2	นายอภิเชฐ แผลสันเทียะ	8.30-16.30	083-4611434	ผู้รับแจ้งเหตุ	รับแจ้งเหตุการโจมตี

¹ เหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญ มีนิยามตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ.2566

9.2. โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber incident Response Team : CIRT)

โปรดระบุว่าหน่วยงานใช้โมเดลโครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ในลักษณะแบบใด เช่น แบบรวมศูนย์ (Centralize), แบบกระจาย (Distributed), แบบให้คำปรึกษา (Coordinating) หรือ แบบอื่นๆ ตามบริบทของหน่วยงาน² โดยหน่วยงานจะต้องระบุรายชื่อของบุคลากรที่มีความเกี่ยวข้องกับการรับมือเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ พร้อมทั้งโครงสร้างทีมรับมือฯ ดังนี้

ลำดับ	ชื่อ - นามสกุล	ช่องทางการติดต่อสื่อสาร	หน้าที่	ความรับผิดชอบ
1	ผศ.ดร.สายสุนีย์ จับโจร	เบอร์โทรศัพท์มือถือ : 096-138-7904 Email : saisunee@nrru.ac.th	หัวหน้าทีมรับมือฯ (Team manager)	ทำหน้าที่สื่อสารกับ ผู้บริหารของหน่วยงาน
2	นายอนุพงษ์ โพธิ์	เบอร์โทรศัพท์ภายใน : 2733 เบอร์โทรศัพท์มือถือ : 096-44632490 Email : apichet.p@nrru.ac.th	รองหัวหน้าทีมรับมือ ฯ (Deputy team manager)	ทำหน้าที่แทนกรณี หัวหน้าทีมรับมือฯ ไม่อยู่/ ไม่สามารถปฏิบัติงานได้
3	นายอภิเชษฐ์ แผลสันเทียะ	เบอร์โทรศัพท์ภายใน : 2733 เบอร์โทรศัพท์มือถือ : 096-44632490 Email : apichet.p@nrru.ac.th	เจ้าหน้าที่รับมือฯ (Incident leader)	ทำหน้าที่ช่วยเหลือ (ชื่อ หน่วยงานเจ้าของระบบ ภายใต้หน่วยงานของ ท่าน) ให้สามารถควบคุม ผลกระทบจากภัยคุกคาม ทางไซเบอร์ได้
4	นายอภิเชษฐ์ แผลสันเทียะ	เบอร์โทรศัพท์ภายใน : 2733 เบอร์โทรศัพท์มือถือ : 096-44632490 Email : apichet.p@nrru.ac.th	เจ้าหน้าที่เทคนิคฯ (Technical lead)	ทำหน้าที่ให้ความเห็น เกี่ยวกับแนวทางที่ เหมาะสมในการควบคุม ผลกระทบจากภัยคุกคาม ทางไซเบอร์

ทั้งนี้ นอกจากทีมรับมือฯ ดังกล่าวข้างต้น ให้มีบุคคลดังต่อไปนี้ทำหน้าที่สนับสนุนการดำเนินการของแผนรับมือฯ ฉบับนี้ ดังนี้

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

ลำดับ	ชื่อ - นามสกุล	ช่องทางการติดต่อสื่อสาร	หน้าที่	ความรับผิดชอบ
1	นายอนุพงษ์ โพธิ์	เบอร์โทรศัพท์ภายใน : 2733 เบอร์โทรศัพท์มือถือ : 083-4611434 Email : anupong.p@nrru.ac.th	สำนักคอมพิวเตอร์ (ชื่อหน่วยงาน เจ้าของระบบ ภายใต้ หน่วยงานหลัก)	ทำหน้าที่ ควบคุม ผลกระทบจาก ภัยคุกคาม
2	นายสุชานนท์ โนนยะโส	เบอร์โทรศัพท์มือถือ : 098-6657477 Email : suchanon.n@nrru.ac.th	เจ้าหน้าที่ด้าน การปฏิบัติตาม กฎหมาย (Compliance)	ทำหน้าที่ทำ ตามข้อบังคับ หรือกฎหมาย เกี่ยวกับเรื่อง ใด
3	บริษัท Snagfor Technologies Company (Thailand)	เบอร์โทรศัพท์มือถือ: 092-8874446 Email :winyou.adisaktragoon@sangfor.com	ผู้ทดสอบเจาะ ระบบ	ทำหน้าที่ ทดสอบการ เจาะระบบ
4	นายสุชานนท์ โนนยะโส	เบอร์โทรศัพท์มือถือ : 098-6657477 Email : suchanon.n@nrru.ac.th	กองกฎหมาย มหาวิทยาลัย ราชภัฏ นครราชสีมา	ทำหน้าที่ร่าง เอกสารในการ ฟ้องร้องตาม กฎหมาย
5	ดร.ยुทธกร ฤทธิไธสง	เบอร์โทรศัพท์มือถือ : 081-9558029 Email : yuttakorn.r@nrru.ac.th	ประธาน กรรมการบริหาร ความเสี่ยง มหาวิทยาลัย	ทำหน้าที่ บริหารจัดการ เรื่องความ เสี่ยงต่อการ ถูกโจมตี
6	นางสาวภัทรวดี ปรีชา ประเสริฐ	เบอร์โทรศัพท์มือถือ : 090-5982246 Email : pattarawadee.p@nrru.ac.th	ประชาสัมพันธ์ งานระบบ เครือข่าย	ทำหน้าที่ ประชาสัมพันธ์ และสื่อสารส ถานการณ์ การถูกโจมตี

9.3. หน่วยงานภายนอกที่เกี่ยวข้อง

หน่วยงานจะต้องจัดให้มีข้อมูลติดต่อสื่อสารของหน่วยงานภายนอกที่เกี่ยวข้อง เช่น สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.), หน่วยงานกำกับดูแล (Regulator), THAI – CERT และผู้ให้บริการภายนอกของหน่วยงาน เช่น หน่วยงานผู้ให้บริการด้านการตรวจสอบพิสูจน์หลักฐานทางดิจิทัล (Digital Forensic Investigator) เป็นต้น

ลำดับ	ชื่อ - นามสกุล	ช่องทางการติดต่อสื่อสาร	หน่วยงาน	ความเกี่ยวข้อง
1	ผู้ประสานงาน จาก สกมช.	เบอร์โทรศัพท์มือถือ : Email : ที่อยู่สำนักงาน :	สำนักงานคณะกรรมการ การรักษาความมั่นคง ปลอดภัยไซเบอร์แห่งชาติ (สกมช.)	
2	ผู้ประสานงานจาก กระทรวงฯ	เบอร์โทรศัพท์ : 02 333 3700 Call Center : 1313 Email : mcs@mhesi.go.th ที่อยู่สำนักงาน : 75/47 ถนนพระราม 6 แขวงทุ่งพญาไท เขตราช เทวี กรุงเทพฯ 10400	กระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและ นวัตกรรม	หน่วยงานกำกับดูแล
3	ผู้ประสานงานจาก THAI – CERT	เบอร์โทรศัพท์ : 02 142 6888 ที่อยู่สำนักงาน : 120 หมู่ 3 อาคารรัฐ ประศาสนภักดี (อาคารบี) ชั้น 7 ศูนย์ราชการเฉลิมพระ เกียรติ 80 พรรษา 5 ธันวาคม 2550 ถนนแจ้ง วัฒนะ แขวงทุ่งสองห้อง เขต หลักสี่ กรุงเทพฯ 10210 Email : thaicert@ncsa.or.th	ศูนย์ประสานการรักษา ความมั่นคงปลอดภัย ระบบคอมพิวเตอร์ แห่งชาติ (THAI – CERT)	
4	โครงการ เครือข่าย สารสนเทศ	เบอร์โทรศัพท์ : 02 232 4000 ที่อยู่สำนักงาน :	Uninet	

	เพื่อพัฒนา การศึกษา (Uninet)	328 ถ.ศรีอยุธยา แขวง พญาไท เขตราชเทวี กรุงเทพฯ 10400 Email : staff@uni.net.th noc@uni.net.th		
--	------------------------------------	--	--	--

9.4. โครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure)

หน่วยงานควรจัดทำแผนผังโครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure) ของบุคลากรภายในทีมรับมือฯ ผู้บริหารหน่วยงาน หน่วยงานกำกับดูแล หน่วยงานรับแจ้งเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ตามกฎหมาย และหน่วยงานภายนอก เป็นต้น รวมถึงกำหนดว่า หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจะปฏิบัติตามภาระหน้าที่ในการรายงานภายใต้พระราชบัญญัติ และกฎหมายย่อยใด ๆ ที่ทำขึ้นภายใต้กฎหมายดังกล่าว ตลอดจนภาระหน้าที่ในการรายงานภายใต้กฎหมาย และข้อกำหนดด้านกฎระเบียบที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

10. ขั้นตอนการรับมือ

แผนรับมือฯ ฉบับนี้ ประกอบด้วยขั้นตอนการรับมือเหตุภัยคุกคามทางไซเบอร์ตามข้อ 19.1 ในประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564, ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์มาตรการป้องกัน รับมือ ประเมิน ปรามปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ.2564 และประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ. 2566 รวมถึง (นโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน) ดังนี้

10.1 ขั้นการเตรียมการ (preparation)

หน่วยงานจะต้องดำเนินการมาตรการเพื่อเตรียมการและป้องกันการเกิดภัยคุกคามทางไซเบอร์ (preparation) เป็นสิ่งที่ต้องทำในระยะเริ่มต้น 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

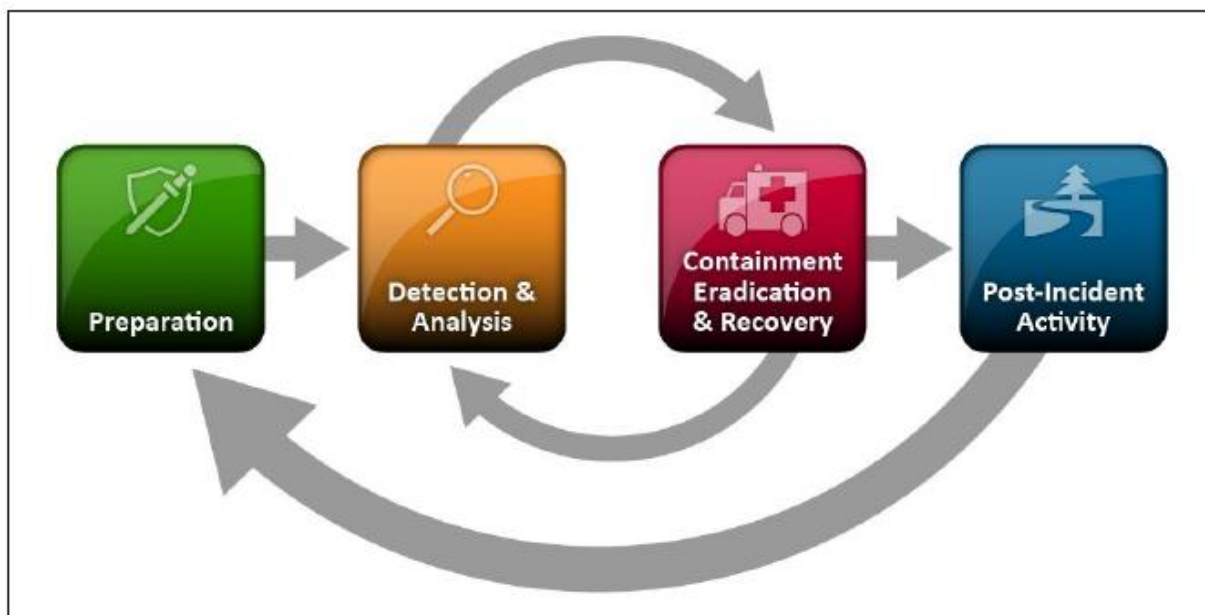
- (4) จัดเตรียมข้อมูลและอุปกรณ์ รวมถึงช่องทางในการติดต่อสื่อสารที่จำเป็น เช่น ข้อมูลการติดต่อและอุปกรณ์ติดต่อสื่อสารของบุคลากร, กลไกรายงานเหตุการณ์ เป็นต้น
- (5) จัดเตรียมอุปกรณ์, ซอฟต์แวร์ และแหล่งข้อมูลสำหรับวิเคราะห์เหตุการณ์ภัยคุกคามทางไซเบอร์
- (6) จัดให้มีการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน (Risk Assessment)
- (7) จัดทำแผนผังโครงสร้างขั้นตอนการรับมือฯ ของหน่วยงาน โดยหน่วยงานอาจดูตัวอย่างการจัดทำแผนผังโครงสร้างขั้นตอนการรับมือฯ ได้ (รายละเอียดปรากฏตามภาคผนวก 1)

นอกจากนี้ หน่วยงานควรพิจารณาดำเนินการตามเอกสารแนบท้าย 2 ตารางที่ 2.1 ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมินปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. 2564 เพิ่มเติม



10.2 ขั้นการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (Detection and Analysis)

หน่วยงานจะต้องดำเนินการในการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ ซึ่งเป็นสิ่งจำเป็นที่จะช่วยให้หน่วยงานสามารถบรรเทาความเสี่ยงที่ยังคงเหลืออยู่ และสามารถแจ้งเตือนได้อย่างทันท่วงทีเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น โดยดำเนินการดังต่อไปนี้



- (1) หน่วยงานจะต้องดำเนินการจัดเตรียมแนวทางรับมือเมื่อเกิดการโจมตีรูปแบบทั่วไปที่เคยเกิดขึ้นหรืออาจเกิดขึ้นกับหน่วยงาน (Common Attack Vectors/ Common Threat Vectors) โดยการโจมตีรูปแบบทั่วไปที่อาจเกิดขึ้น มีตัวอย่าง ดังนี้

ประเภท	อธิบาย	วิธีการรับมือ
อุปกรณ์แบบถอดได้ (External/Removable Media)	การโจมตีที่ดำเนินการจากอุปกรณ์แบบถอดได้หรืออุปกรณ์ต่อพ่วง ตัวอย่างเช่น โค้ดที่เป็นอันตรายแพร่กระจายไปยังระบบจากแฟลชไดรฟ์ที่ติดไวรัส	ดำเนินการถอนการติดตั้งอุปกรณ์แบบถอดได้ที่เป็นสาเหตุของภัยคุกคามออกจากอุปกรณ์และระบบเครือข่ายของหน่วยงาน และตรวจสอบสาเหตุและประเภทของภัยคุกคามว่าเป็นภัยคุกคามประเภทใด

- (2) หน่วยงานจะต้องดำเนินการจัดให้มีกลไกที่สามารถตรวจจับสิ่งบ่งชี้หรือลักษณะเบื้องต้นของการเกิดภัยคุกคามทางไซเบอร์ได้ในเวลาอันเหมาะสม โดยอาจอาศัยข้อมูลจากแหล่งข้อมูลต่าง ๆ เช่น ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เป็นต้น

- (3) หน่วยงานจะต้องดำเนินการจัดให้มีแนวทางในการวิเคราะห์ผลกระทบและระดับของภัยคุกคามทางไซเบอร์ (Incident Prioritization) เพื่อรับมือกับภัยคุกคามทางไซเบอร์ให้ทัน่วงที โดยพิจารณาปัจจัยต่าง ๆ ที่เกี่ยวข้อง เช่น ผลกระทบต่อการทำงานของระบบ (functional impact) ผลกระทบต่อข้อมูล (information impact) และความสามารถในการกู้คืน (recoverability effort³) เป็นต้น

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

(4) หน่วยงานจะต้องดำเนินการจัดให้มีบันทึกรายงานสถานการณ์เหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ โดยอาจกำหนดให้มีรายละเอียดตามแบบฟอร์มตัวอย่าง (รายละเอียดปรากฏตามภาคผนวก 2)

(5) หน่วยงานจะต้องจัดให้มีการจัดทำบันทึกข้อมูลกิจกรรมเหตุการณ์ความปลอดภัยทางไซเบอร์ (Incident Documentation) โดยหน่วยงานควรบันทึกข้อมูลเกี่ยวกับเหตุการณ์ความปลอดภัยทางไซเบอร์ ทุกขั้นตอนตั้งแต่ตรวจพบเหตุการณ์จนถึงกระบวนการสุดท้าย และข้อมูลดังกล่าวควรระบุรายละเอียดพร้อมเวลาที่เกิดเหตุและระยะเวลาที่ใช้ด้วย บันทึกข้อมูลดังกล่าวที่เกี่ยวข้องกับเหตุการณ์ควรลงวันที่และลงนามโดยผู้มีหน้าที่จัดการรับมือเหตุการณ์นั้นๆ เพื่อให้มั่นใจได้ว่าเหตุการณ์ความปลอดภัยทางไซเบอร์ที่เกิดขึ้นจะได้รับการจัดการแก้ไขภายในระยะเวลาที่เหมาะสมโดยอาจกำหนดให้มีรายละเอียดตามแบบฟอร์มตัวอย่าง (รายละเอียดปรากฏตามภาคผนวก 3)

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

(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 จะต้องจัดทำและส่งรายงานสรุปจำนวนเหตุภัยคุกคามทางไซเบอร์ทั้งหมดที่เกิดขึ้นกับข้อมูลหรือระบบสารสนเทศของหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ภายใต้การควบคุมหรือกำกับดูแลของตนในแต่ละปี ภายในวันที่ 31 มกราคม ของปีถัดไป ให้แก่สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ โดยให้แยกสถิติหมวดหมู่ตามแบบที่กำหนดในเอกสาร ก3 โดยใช้แบบฟอร์มการรายงานตามกฎหมาย (รายละเอียดปรากฏตามภาคผนวก 4)

นอกจากนี้ หน่วยงานควรพิจารณาดำเนินการตามเอกสารแนบท้าย 2 ตารางที่ 2.2 ในประกาศคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมินปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. 2564 เพิ่มเติม

10.3 ขั้นการระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ (containment, eradication, and recovery)

ระดับความรุนแรงของผลกระทบ

ระดับความรุนแรง	คำอธิบาย
0 (ต่ำ)	เหตุการณ์ที่มีผลกระทบน้อยที่สุด ตัวอย่างอาจเป็นอีเมลสแปม การติดไวรัส ที่แยกได้ ฯลฯ
1(กลาง)	เหตุการณ์ที่มีผลกระทบอย่างมีนัยสำคัญ ตัวอย่างอาจเป็นความล่าช้าหรือความสามารถในการให้บริการที่จำกัด ตรงตาม [มหาวิทยาลัยราชภัฏนครราชสีมา] การกิจ การส่งจดหมายอิเล็กทรอนิกส์ที่สำคัญหรือการถ่ายโอนข้อมูลล่าช้า เป็นต้น
2(สูง)	เหตุการณ์ที่มีผลกระทบรุนแรง ตัวอย่างอาจเป็นการหยุดชะงักในการให้บริการและ/หรือการปฏิบัติหน้าที่ภารกิจ ของเรา ข้อมูลที่เป็นกรรมสิทธิ์หรือเป็นความลับ ของ [มหาวิทยาลัยราชภัฏนครราชสีมา] ถูกบุกรุก ไวรัสหรือเวิร์ม แพร่กระจายในวงกว้าง และส่งผลกระทบต่อพนักงานมากกว่า 1 เปอร์เซนต์ ระบบความปลอดภัย สาธารณะไม่พร้อมใช้งาน หรือ [มหาวิทยาลัยราชภัฏนครราชสีมา] แจ้งผู้บริหารระดับสูงแล้ว
3(สุดขีด)	เหตุการณ์ที่มีผลกระทบเป็นหายนะ ตัวอย่างอาจเป็นการปิดบริการเครือข่ายของ [มหาวิทยาลัยราชภัฏนครราชสีมา] ทั้งหมด ข้อมูลที่เป็นกรรมสิทธิ์หรือเป็นความลับของ [มหาวิทยาลัยราชภัฏนครราชสีมา] ถูกบุกรุกและเผยแพร่ใน/บน สถานที่หรือไซต์สาธารณะ ระบบความปลอดภัยสาธารณะ ใช้งานไม่ได้ฝ่ายบริหารจะต้องแถลงต่อสาธารณะ

หน่วยงานจะต้องดำเนินการเพื่อระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคาม ทางไซเบอร์ 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 หน่วยงานควรพิจารณาดำเนินการตามเอกสารแนบท้าย 2 ตารางที่ 2.3 ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมินปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. 2564 เพิ่มเติม

10.4. ขั้นตอนการดำเนินการภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ (Post-Incident activity)

หน่วยงานควรกำหนดขั้นตอน วิธี ปฏิบัติ หรือกำหนดนโยบายภายในที่เกี่ยวข้องเพื่อให้มีแนวทางที่ชัดเจน ซึ่งการปฏิบัติตามมาตรการดังกล่าว จะช่วยให้หน่วยงานสามารถเรียนรู้จากเหตุภัยคุกคามทางไซเบอร์ที่ผ่านมา และสามารถหาแนวทางเพื่อแก้ไข จุดบกพร่องและพัฒนาแนวทางรับมือกับภัยคุกคามทางไซเบอร์ต่อไปในอนาคต นอกจากนี้หน่วยงานต้องเก็บ รักษาข้อมูลและพยานหลักฐานที่จำเป็น เพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์ หรือใช้ในกรณีที่ต้องการร้องทุกข์หรือดำเนินคดี เนื่องจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้นนั้น อาจเข้าลักษณะเป็นความผิดตามประมวล กฎหมายอาญา หรือพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2560 และที่แก้ไข เพิ่มเติม (ถ้ามี) หรือกฎหมายอื่น ๆ ที่เกี่ยวข้อง ประกอบด้วยการดำเนินการในเรื่องดังต่อไปนี้

(1) ทบทวนหลังการดำเนินการ (After-Action Review Process) เพื่อระบุและแนะนำให้ปรับปรุงการดำเนินการเพื่อป้องกันการเกิดซ้ำ

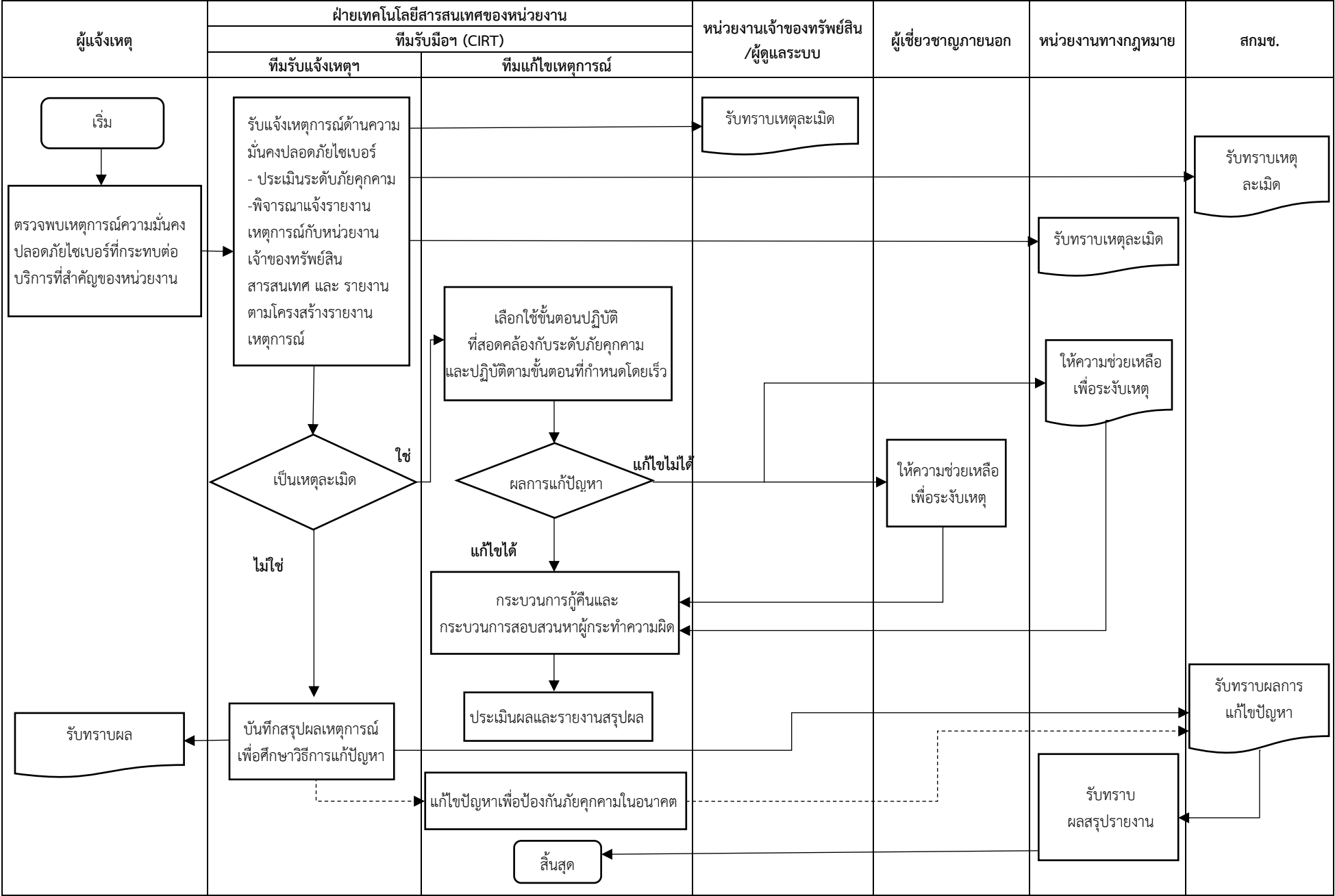
นอกจากนี้ หน่วยงานควรพิจารณาดำเนินการตามเอกสารแนบท้าย 2 ตารางที่ 2.4 ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมินปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. 2564 เพิ่มเติม

10.5. การจัดทำรายการตรวจสอบการจัดการเหตุการณ์ (Incident Handling Checklist)

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

ภาคผนวก 1

แผนผังโครงสร้างขั้นตอนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response)



ภาคผนวก 2

ตัวอย่าง : บันทึกรายงานสถานการณ์เหตุการณ์ความมั่นคงปลอดภัยไซเบอร์

วันที่ :	เวลา :	ผู้บันทึกรายงาน : ติดต่อ :
วันและเวลาที่เกิดเหตุการณ์ :		
สถานะเหตุการณ์ปัจจุบัน :		
ประเภทเหตุการณ์ :		
ระดับความรุนแรง :		
รายละเอียดเหตุการณ์ :		
ผลกระทบที่เกิดขึ้น :		
ความเสียหายที่เกิดขึ้น :		
การรายงานเหตุการณ์ :		
หน่วยงานที่ขอความช่วยเหลือ :		
การดำเนินการตอบสนองต่อ เหตุการณ์ :		
รายละเอียดเพิ่มเติม :		
ผู้จัดการรับมือฯ เหตุการณ์ :		
ข้อมูลติดต่อผู้จัดการรับมือฯ เหตุการณ์ :		
วันและเวลาที่มีรายงานความคืบหน้า ครั้งถัดไป :		

ภาคผนวก 3

บันทึกข้อมูลกิจกรรมเหตุการณ์ความปลอดภัยทางไซเบอร์ (Incident Documentation)

[illegible]

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 ☐ วิฤต (ก) ☐ วิฤต (ข) ☐ ยังไม่สามารถระบุได้																	
6. หมวดหมู่ของภัยคุกคาม (แจ้งได้มากกว่า 1 รายการ) <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 20%;">หมวดหมู่*</th> <th>คำอธิบาย</th> </tr> </thead> <tbody> <tr> <td>หมวดหมู่ที่ 2</td> <td>การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance)</td> </tr> <tr> <td>หมวดหมู่ที่ 3</td> <td>การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยของหน่วยงาน (Non-Compliance Activity)</td> </tr> <tr> <td>หมวดหมู่ที่ 4</td> <td>การบุกรุกโดยการใช้มัลแวร์ (Malicious Logic)</td> </tr> <tr> <td>หมวดหมู่ที่ 5</td> <td>การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion)</td> </tr> <tr> <td>หมวดหมู่ที่ 6</td> <td>การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion)</td> </tr> <tr> <td>หมวดหมู่ที่ 7</td> <td>การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)</td> </tr> <tr> <td>หมวดหมู่ที่ 8</td> <td>เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating)</td> </tr> </tbody> </table>		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)
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 ปรามปราม และระงับภัยคุกคามทางไซเบอร์แต่ละ ระดับ พ.ศ. 2564 (ทั้งนี้ ภัยคุกคามทางไซเบอร์หมวดหมู่ที่ 0 หมวดหมู่ที่ 1 และหมวดหมู่ที่ 9 ไม่เข้าข่ายเป็นภัยคุกคาม ทางไซเบอร์ที่ต้องรายงาน)																	

⁴ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 กำหนดความหมายของ “ภัยคุกคามทางไซเบอร์” ดังนี้ การกระทำหรือการดำเนินการใด ๆ โดยมีขอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภัยอันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ 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 ☐ วิฤต (ก) ☐ วิฤต (ข) ☐ ยังไม่สามารถระบุได้

⁵ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 กำหนดความหมายของ “ภัยคุกคามทางไซเบอร์” ดังนี้ การกระทำ หรือการดำเนินการใด ๆ โดยมีขอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นอันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหาย หรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ 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 ปรามปราม 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 วัน เวลา ที่ผู้โจมตีได้เริ่มต้นเข้าถึงระบบ (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 (เลือกทุกข้อที่ใช้): <table><tr><td>☐ ข้อมูลไบโอเมตริกซ์</td><td>☐ ข้อมูลการติดต่อ</td></tr><tr><td>☐ ข้อมูลการเงิน</td><td>☐ ข้อมูลบุคลากรของรัฐ</td></tr><tr><td>☐ หมายเลขบัตรประชาชน</td><td>☐ ข้อมูลการติดต่อกับหน่วยงานต่าง ๆ</td></tr><tr><td>☐ ข้อมูลทางการแพทย์</td><td></td></tr><tr><td>☐ อื่น ๆ : โปรดระบุ</td><td></td></tr></table> จำนวนข้อมูล (Record) ที่ได้รับผลกระทบ: โปรดระบุ ผลกระทบอื่น ๆ ที่เกิดขึ้น: โปรดระบุ	☐ ข้อมูลไบโอเมตริกซ์	☐ ข้อมูลการติดต่อ	☐ ข้อมูลการเงิน	☐ ข้อมูลบุคลากรของรัฐ	☐ หมายเลขบัตรประชาชน	☐ ข้อมูลการติดต่อกับหน่วยงานต่าง ๆ	☐ ข้อมูลทางการแพทย์		☐ อื่น ๆ : โปรดระบุ	
☐ ข้อมูลไบโอเมตริกซ์	☐ ข้อมูลการติดต่อ									
☐ ข้อมูลการเงิน	☐ ข้อมูลบุคลากรของรัฐ									
☐ หมายเลขบัตรประชาชน	☐ ข้อมูลการติดต่อกับหน่วยงานต่าง ๆ									
☐ ข้อมูลทางการแพทย์										
☐ อื่น ๆ : โปรดระบุ										

ง1.4 รายละเอียดของระบบ หรือข้อมูลที่ได้รับผลกระทบ (Information of Affected System)

หมายเลข CVE: โปรดระบุ

ช่องโหว่ที่ถูกใช้โจมตี: โปรดระบุ

การใช้ระบบหรือเครื่องที่ได้รับผลกระทบเป็นฐานเพื่อโจมตีขยายผลไปยังระบบหรือเครื่องอื่น:

โปรดระบุ

อาการหรือสิ่งผิดปกติ (เลือกได้มากกว่า 1 รายการ)

- | | |
|--|---|
| ☐ ระบบล่ม | ☐ รายการข้อมูลจราจรทางคอมพิวเตอร์ที่ผิดปกติ |
| ☐ บัญชีผู้ใช้ถูกสร้างขึ้นใหม่โดยไม่ทราบสาเหตุ หรือ บัญชีผู้ใช้มีความผิดปกติ | |
| ☐ การโจมตีด้วยวิศวกรรมสังคม (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 | ☐ การโจมตีให้เกิดการปฏิเสธการให้บริการ (DOS, DDOS) |
| ☐ ไฟล์ใหม่ถูกสร้างขึ้นโดยไม่ทราบสาเหตุ | ☐ การใช้งานหรือมีกิจกรรมที่เกิดขึ้นในเวลาที่ไม่ปกติ |
| ☐ การแก้ไขหน้าเว็บ | ☐ การสร้างแฟ้มข้อมูล setuid หรือ setgid ใหม่ที่ผิดปกติเกิดขึ้น |
| ☐ การเปลี่ยนแปลงในไดเรกทอรีและแฟ้มข้อมูลของระบบปฏิบัติการที่ผิดปกติ | |
| ☐ การตรวจพบโปรแกรมเจาะระบบ (Crack utility) | |
| ☐ สิ่งผิดปกติไปจากเดิมอื่น ๆ: โปรดระบุ | |

ง1.5 รายละเอียดของเหตุภัยคุกคามตามลำดับเวลา ตั้งแต่การโจมตีครั้งแรก จนถึงปัจจุบัน (เช่น ลำดับของการโจมตี, Attack vector, เทคนิคหรือเครื่องมือที่ผู้โจมตีใช้ ฯลฯ)

โปรดระบุ

ง1.6 รายละเอียดอื่น ๆ ที่พบเกี่ยวข้องกับเหตุภัยคุกคาม: โปรดระบุ

ง2. ข้อมูลการระงับ ปรามปราม 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 สถิติรายปีจำแนกตามหมวดหมู่ของภัยคุกคามทางไซเบอร์⁶

หมวดหมู่	คำอธิบาย	จำนวน
0	เหตุการณ์จำลองและการฝึกซ้อมของหน่วยงาน (Training and Exercises)	
1	การพยายามเข้าถึงระบบที่ไม่สำเร็จ (Unsuccessful Activity Attempt)	
2	การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance)	
3	การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยที่หน่วยงานกำหนด (Non-Compliance Activity)	
4	การบุกรุกโดยใช้มัลแวร์ (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 สถิติรายปีจำแนกตามระดับภัยคุกคามทางไซเบอร์⁷

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

⁶ หมวดหมู่ตามข้อ 1 ของภาคผนวกท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์
มาตรการป้องกัน รับมือ ประเมิน ปรามปราม 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 เหตุการณ์เชื่อว่ามีการเกิดขึ้น ให้เริ่มบันทึกการสอบสวนและรวบรวมหลักฐาน	
2	จัดลำดับความสำคัญในการจัดการเหตุการณ์ตามระดับความรุนแรงของภัยคุกคามที่เกิดขึ้น	
3	รายงานเหตุการณ์ดังกล่าวต่อผู้บริหารและหน่วยงานภายนอกที่เกี่ยวข้อง	
ขั้นการระงับภัยคุกคาม ปรามปราม 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 และสาเหตุภัยคุกคามอื่นๆ	
7.3	หากมีการตรวจพบว่ามีระบบใหม่ได้รับผลกระทบ (เช่น การติดมัลแวร์ใหม่) ให้ทำซ้ำขั้นตอนการตรวจจับและการวิเคราะห์ภัยคุกคามทางไซเบอร์ (detection and analysis)	
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 ปรามปราม 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

ประกาศ ณ วันที่ 22 ตุลาคม พ.ศ 2568



(ผู้ช่วยศาสตราจารย์ ดร. สายสุนีย์ จັบโจร)

ผู้อำนวยการสำนักคอมพิวเตอร์