แผนรับมือเหตุภัยคุกคามทางไซเบอร์ มหาวิทยาลัยราชภัฏอุบลราชธานี

(Cybersecurity Incident Response Plan)

ประวัติการแก้ไขเอกสาร (Version Control)

รุ่น (Version)	วันที่อนุมัติ (Date of Approval)	ผู้อนุมัติ (Approved by)	สถานะ (Description of change)
1.0A	10 กันยายน 2567	รศ.ธรรมรักษ์ ละอองนวล อธิการบดี	ไม่ใช้งาน
2.0A	15 มกราคม 2569	รศ.ธรรมรักษ์ ละอองนวล อธิการบดี	ใช้งาน

รายละเอียดของเอกสาร (Document control and review)

ผู้จัดทำเอกสาร	
ชื่อ นายเอกภพ บุตรศรี ตำแหน่ง หัวหน้างานพัฒนาระบบคอมพิวเตอร์และเครือข่าย วันที่ 15 มกราคม 2569	ลงชื่อ ..... (นายเอกภพ บุตรศรี)
ผู้ตรวจทานเอกสาร	
ชื่อ นายภุชงค์ พรหมลาศ ตำแหน่ง รักษาการในตำแหน่งผู้อำนวยการศูนย์คอมพิวเตอร์ วันที่ 15 มกราคม 2569	ลงชื่อ ..... (นายภุชงค์ พรหมลาศ)
ผู้เห็นชอบเอกสาร	
ชื่อ นางเสาวลักษณ์ ภูสมสาย ตำแหน่ง ผู้อำนวยการสำนักงานอธิการบดี วันที่ 15 มกราคม 2569	ลงชื่อ ..... (นางเสาวลักษณ์ ภูสมสาย)
ผู้เห็นชอบเอกสาร	
ชื่อ ผู้ช่วยศาสตราจารย์กชกร เจตินัย ตำแหน่ง รองอธิการบดี วันที่ 15 มกราคม 2569	ลงชื่อ ..... (ผู้ช่วยศาสตราจารย์กชกร เจตินัย)
ผู้อนุมัติเอกสาร	
ชื่อ รองศาสตราจารย์ธรรมรักษ์ ละอองนวล ตำแหน่ง อธิการบดี วันที่ 15 มกราคม 2569	ลงชื่อ ..... (รองศาสตราจารย์ธรรมรักษ์ ละอองนวล)

1. หลักการและเหตุผล

ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 มาตรา 44 กำหนดให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเร็ว ซึ่งประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างน้อยต้องประกอบด้วยเรื่องต่อไปนี้

(1) แผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยผู้ตรวจประเมิน ผู้ตรวจสอบภายใน หรือผู้ตรวจสอบอิสระจากภายนอก อย่างน้อยปีละหนึ่งครั้งและ

(2) แผนการรับมือภัยคุกคามทางไซเบอร์

เพื่อดำเนินการตาม พรบ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 มาตรา 44 มหาวิทยาลัยราชภัฏอุบลราชธานี จึงได้จัดทำแผนรับมือเหตุภัยคุกคามทางไซเบอร์ขึ้น เพื่อรับมือกับภัยคุกคามทางไซเบอร์ในปัจจุบันและอนาคต โดยให้ครอบคลุมถึง การดำเนินมาตรการการป้องกัน (Protect) การตรวจจับ (Detect) การตอบสนอง (Respond) และการคืนสภาพ (Recover)

2. วัตถุประสงค์

2.1 เพื่อใช้เป็นแผนในการรับมือเหตุภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัย

2.2 เพื่อกำหนดกระบวนการในการเฝ้าระวัง ตรวจสอบ ติดตาม และแก้ไขปัญหาที่เกิดขึ้นจากภัยคุกคามทางไซเบอร์

2.3 เพื่อกำหนดขั้นตอนการรับมือภัยคุกคามทางไซเบอร์ และการรายงานเหตุภัยคุกคามทางไซเบอร์ไปยังหน่วยงานที่เกี่ยวข้อง

3. ขอบเขต

แผนรับมือฯ ฉบับนี้ ใช้รับมือเหตุภัยคุกคามทางไซเบอร์ที่เกิดขึ้นต่อระบบสารสนเทศ และข้อมูลดิจิทัลของมหาวิทยาลัยราชภัฏอุบลราชธานี รวมถึงบุคคลหรืออุปกรณ์ใดๆ ซึ่งเข้าถึงระบบสารสนเทศ และข้อมูลดิจิทัลดังกล่าว

4. หน้าที่การทบทวนแผน

ศูนย์คอมพิวเตอร์ สำนักงานอธิการบดี มหาวิทยาลัยราชภัฏอุบลราชธานี มีหน้าที่ทบทวนและขออนุมัติแผนรับมือฯ ฉบับนี้ถึงผู้บริหารสูงสุดหรือผู้ที่รับมอบอำนาจหน่วยงาน

5. หน้าที่ในการดำเนินการตามแผน

ศูนย์คอมพิวเตอร์ สำนักงานอธิการบดี มหาวิทยาลัยราชภัฏอุบลราชธานี มีหน้าที่เป็นผู้รับผิดชอบหลักในการดำเนินการตามแผนรับมือฯ ฉบับนี้ โดยมีหน่วยงานสนับสนุนประกอบด้วย สำนักงานตรวจสอบภายใน งานวินัยและนิติการ และงานประชาสัมพันธ์ กองเลขานุการ สำนักงานอธิการบดี

6. เอกสารและกรอบมาตรฐานที่เกี่ยวข้อง

6.1 นโยบายและแนวปฏิบัติด้านการปกป้องข้อมูลส่วนบุคคลที่เกี่ยวข้อง

6.1.1 ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่องมาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล พ.ศ.2563

6.2 กฎหมายที่เกี่ยวข้อง

6.2.1 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 และที่แก้ไขเพิ่มเติม

6.2.2 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

6.2.3 พระราชบัญญัติการรักษาด้านความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562

- ประกาศ กกม. เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ.2564
- ประกาศ กมช. เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ
- ประกาศ กกม. เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ. 2566
- ประกาศ กมช. เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ.2566
- ประกาศ กมช. เรื่อง มาตรฐานขั้นต่ำของข้อมูลหรือระบบสารสนเทศ พ.ศ. 2566
- ประกาศ สกมช. เรื่อง แนวทางการจัดทำแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2567

7. นิยาม

เหตุการณ์ (Event) หมายความว่า เหตุการณ์ที่เกิดขึ้นจากการเฝ้าระวังสังเกตการณ์ (observable occurrence) ในระบบเครือข่าย สภาพแวดล้อม กระบวนการ ลำดับการดำเนินการ หรือบุคลากรเหตุการณ์อาจมีหรือไม่มีลักษณะที่ส่งผลเชิงลบก็ได้

เหตุภัยคุกคามทางไซเบอร์ (Cyber incident) หมายความว่า เหตุการณ์ที่มีผลเชิงลบที่เกิดจากการกระทำหรือการดำเนินการใดๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

ภัยคุกคามทางไซเบอร์ (Cyber threat) หมายความว่า การกระทำหรือการดำเนินการใดๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะ ก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

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

8. บทบาทหน้าที่และโครงสร้างทีมรับมือเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์

8.1. ผู้รับแจ้งเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ภายในหน่วยงาน

หน่วยงานมีการระบุข้อมูลการติดต่อของผู้รับแจ้งเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ภายในหน่วยงาน กรณีเมื่อมีการตรวจพบ หรือมีการรายงานเหตุการณ์เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ โดยควรมีผู้รับแจ้งเหตุฯ หลัก รวมถึงช่องทางหลักในการติดต่อ และเตรียมผู้รับแจ้งเหตุฯ สำรองพร้อมช่องทางสำหรับกรณีที่ไม่สามารถติดต่อผู้รับแจ้งเหตุคนแรกได้ โดยหน่วยงานควรจะกำหนดให้มีผู้ทำหน้าที่รับแจ้งเหตุฯ ครอบคลุมตลอดระยะเวลา 24 ชั่วโมง/7 วัน

ลำดับ	ชื่อ – นามสกุล	ระยะเวลาในการปฏิบัติงาน	ช่องทางการติดต่อสื่อสาร	หน้าที่	ความรับผิดชอบ
1	นายเอกภพ บุตรศรี	08.00-17.00 น.	akapop@ubru.ac.th 084 584 3423	รับแจ้งเหตุ	แจ้งเหตุ/ระงับเหตุ
2	นายวันเฉลิม พรจันทร์	08.00-17.00 น.	wanchaleam.p@ubru.ac.th 091 467 1791	รับแจ้งเหตุ	แจ้งเหตุ/ระงับเหตุ
3	นายพิษณุ อุตราศรี	08.00-17.00 น.	pitsanu.u@ubru.ac.th 061 029 2013	รับแจ้งเหตุ	แจ้งเหตุ/ระงับเหตุ
4	นายศรัณย์ ศรีทานันท์	08.00-17.00 น.	sarun.s@ubru.ac.th 083 931 1369	รับแจ้งเหตุ	แจ้งเหตุ/ระงับเหตุ

8.2. โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber incident Response Team : CIRT)

มหาวิทยาลัยราชภัฏอุบลราชธานีใช้โมเดลโครงสร้างทีมรับมือเหตุการณ์เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ในลักษณะแบบรวมศูนย์ (Centralize) โดยหน่วยงานระบุรายชื่อของบุคลากรที่มีความเกี่ยวข้องกับการรับมือเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ พร้อมทั้งโครงสร้างทีมรับมือฯ ดังนี้

ลำดับ	ชื่อ - นามสกุล	ช่องทางการติดต่อสื่อสาร	หน้าที่	ความรับผิดชอบ
1	ผศ.กชกร เจตินัย รองอธิการบดี	045-352000-29 ต่อ 5154 082 782 8226 kotchakorn.j@ubru.ac.th	*หัวหน้าทีมรับมือฯ (Team manager)*	*-ทำหน้าที่สื่อสารกับผู้บริหารของหน่วยงาน*

ลำดับ	ชื่อ - นามสกุล	ช่องทางการติดต่อสื่อสาร	หน้าที่	ความรับผิดชอบ
2	นายภุชงค์ พรหมลาศ รักษาการใน ตำแหน่ง ผอ.ศูนย์คอมพิวเตอร์	045-352000-29 ต่อ 3203 087 448 1822 puchong.p@ubru.ac.th	*รองหัวหน้าทีมรับมือฯ (Deputy team manager)*	*-ทำหน้าที่แทนกรณีหัวหน้าทีมรับมือฯ ไม่อยู่/ไม่สามารถปฏิบัติงานได้* *-ทำหน้าที่ควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์*
3	นายเอกภพ บุตรศรี	045-352000-29 ต่อ 3210 084 584 3423 akapop@ubru.ac.th	*เจ้าหน้าที่รับมือฯ (Incident leader)*	*-ทำหน้าที่ช่วยเหลือหน่วยงานภายใต้ มรภ.อุบลราชธานีให้สามารถควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์ได้* *-ทำหน้าที่ควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์*
4	นายวันเฉลิม พรจันทร์	045-352000-29 ต่อ 3209 091 467 1791 wanchaleam@ubru.ac.th	*เจ้าหน้าที่รับมือฯ (Incident leader)*	*-ทำหน้าที่ช่วยเหลือหน่วยงานภายใต้ มรภ.อุบลราชธานีให้สามารถควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์ได้* *-ทำหน้าที่ควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์*
5	นายพิษณุ อุตราศรี	045-352000-29 ต่อ 3202 088 031 0125 pitsanu.u@ubru.ac.th	*เจ้าหน้าที่รับมือฯ (Incident leader)*	*-ทำหน้าที่ช่วยเหลือหน่วยงานภายใต้ มรภ.อุบลราชธานีให้สามารถควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์ได้* *-ทำหน้าที่ควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์*
6	นายจักรพงศ์ หอมเย็น	045-352000-29 ต่อ 3203 096 093 3209 chakkapong.h@ubru.ac.th	*เจ้าหน้าที่รับมือฯ (Incident leader)*	*-ทำหน้าที่ช่วยเหลือหน่วยงานภายใต้ มรภ.อุบลราชธานีให้สามารถควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์ได้* *-ทำหน้าที่ควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์*

ลำดับ	ชื่อ - นามสกุล	ช่องทางการติดต่อสื่อสาร	หน้าที่	ความรับผิดชอบ
7	นายศรัณย์ ศรีทานันท์	045-352000-29 ต่อ 3211 083 931 1369 sarun.s@ubru.ac.th	*เจ้าหน้าที่รับมือฯ* *(Incident leader)*	*-ทำหน้าที่ช่วยเหลือหน่วยงานภายใต้ มรภ.อุบลราชธานีให้สามารถควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์ได้* *-ทำหน้าที่ควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์*
8	นายทิวัตถ์ บุตรศรี	045-352000-29 ต่อ 3208 085 303 1886 thiwat.B@Ubru.ac.th	*เจ้าหน้าที่รับมือฯ* *(Incident leader)*	*-ทำหน้าที่ช่วยเหลือหน่วยงานภายใต้ มรภ.อุบลราชธานีให้สามารถควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์ได้* *-ทำหน้าที่ควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์*
9	น.ส.มะลิวรรณ นาคำมูล	045-352000-29 ต่อ 3200 087 870 9609 maliwan.n@ubru.ac.th	*เจ้าหน้าที่รับมือฯ* *(Incident leader)*	*-ทำหน้าที่ประสานงานหน่วยงานภายใต้มหาวิทยาลัยราชภัฏอุบลราชธานี และจัดทำหนังสือราชการแจ้งเหตุรวมถึงรายงานผลการรับมือเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ต่อหน่วยงานที่เกี่ยวข้องและสกมช.*
10	น.ส.อรอนงค์ อารีกุล	045-352000-29 ต่อ 3212 094 514 9938 onanong.a@ubru.ac.th	*เจ้าหน้าที่รับมือฯ* *(Incident leader)*	*-ทำหน้าที่ประสานงานหน่วยงานภายใต้มหาวิทยาลัยราชภัฏอุบลราชธานี และจัดทำหนังสือราชการแจ้งเหตุรวมถึงรายงานผลการรับมือเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ต่อหน่วยงานที่เกี่ยวข้องและสกมช.*

ลำดับ	ชื่อ - นามสกุล	ช่องทางการติดต่อสื่อสาร	หน้าที่	ความรับผิดชอบ
11	นางมาลัย อุ่นศรี	045-352000-29 ต่อ 3208 080 545 5495 malai.s@ubru.ac.th	*เจ้าหน้าที่รับมือฯ (Incident leader)*	*-ทำหน้าที่ประสานงานหน่วยงานภายใต้มหาวิทยาลัยราชภัฏอุบลราชธานี และจัดทำหนังสือราชการแจ้งเหตุรวมถึงรายงานผลการรับมือเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ต่อหน่วยงานที่เกี่ยวข้องและสกมช.*

ทั้งนี้ นอกจากทีมรับมือฯ ดังกล่าวข้างต้น ให้มีบุคคลดังต่อไปนี้ทำหน้าที่สนับสนุนการดำเนินการของแผนรับมือฯ ฉบับนี้ ดังนี้

ลำดับ	ชื่อ - นามสกุล	ช่องทางการติดต่อสื่อสาร	หน้าที่	ความรับผิดชอบ
1	ผู้แทนจากสำนักงานตรวจสอบภายใน	เบอร์โทรศัพท์ภายใน : 5155, 1175	*เจ้าหน้าที่ด้านการปฏิบัติตามกฎหมาย (Compliance)*	*ทำหน้าที่ควบคุมผลกระทบจากภัยคุกคาม*
2	ผู้แทนจากงานวินัยและนิติการ กองเลขานุการ สำนักงานอธิการบดี	เบอร์โทรศัพท์ภายใน : 2407/5126	*ผู้เชี่ยวชาญด้านกฎหมาย*	*ทำหน้าที่รายงานเหตุภัยคุกคามทางไซเบอร์*
3	ผู้แทนจาก งานประชาสัมพันธ์ กองเลขานุการ สำนักงานอธิการบดี	เบอร์โทรศัพท์ภายใน : 1007	*ผู้รับผิดชอบด้านสื่อสารองค์กร*	*ประชาสัมพันธ์ไปยังผู้มีส่วนได้ส่วนเสียเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์*

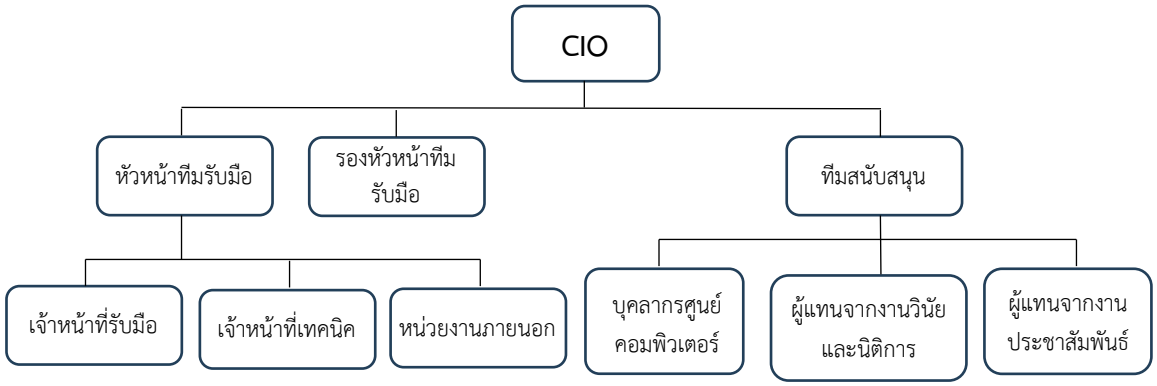
8.3. หน่วยงานภายนอกที่เกี่ยวข้อง

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

ลำดับ	ชื่อ - นามสกุล	ช่องทางการติดต่อสื่อสาร	หน่วยงาน	ความเกี่ยวข้อง
1	National Cyber Security Agency (NCSA)	02 142 6888 saraban@ncsa.or.th 120 หมู่ 3 อาคารรัฐประศาสนภักดี (อาคาร B) ชั้น 7 ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ 10210	สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)	แจ้งเหตุภัยคุกคามไซเบอร์
2	สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล	02 142 1033 02 141 6993 saraban@pdpc.or.th 120 หมู่ 3 อาคารรัฐประศาสนภักดี (อาคาร B) ชั้น 7 ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ 10210	สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.)	แจ้งเหตุการละเมิดข้อมูลส่วนบุคคล
3	กระทรวงการอุดมศึกษาวิทยาศาสตร์ วิจัยและนวัตกรรม	02 610 5200 เลขที่ 328 ถนนศรีอยุธยา แขวงทุ่งพญาไท เขตราชเทวี กรุงเทพมหานคร	กระทรวงการอุดมศึกษาวิทยาศาสตร์ วิจัยและนวัตกรรม	หน่วยงานกำกับดูแล
4	THAICERT	02 142 6888 thaicert@ncsa.or.th 120 หมู่ 3 อาคารรัฐประศาสนภักดี (อาคาร B) ชั้น 7 ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ 10210	ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ	
5	ผู้ประสานงาน Uninet	02 232 4000 noc@uni.net.th 328 ถ.ศรีอยุธยา แขวง ทุ่งพญาไท เขต ราชเทวี กรุงเทพฯ 10400	สำนักงานบริหารเทคโนโลยีสารสนเทศเพื่อพัฒนาการศึกษา	ผู้ให้บริการระบบ Internet
6	ผู้ประสานงาน AIS	เบอร์โทร 1175 Kamron Promsonthi kamronp@ais.co.th 081 955 3334	บริษัท แอดวานซ์ ไวร์เลส เน็ทเวิร์อค จำกัด	ให้บริการระบบ Internet

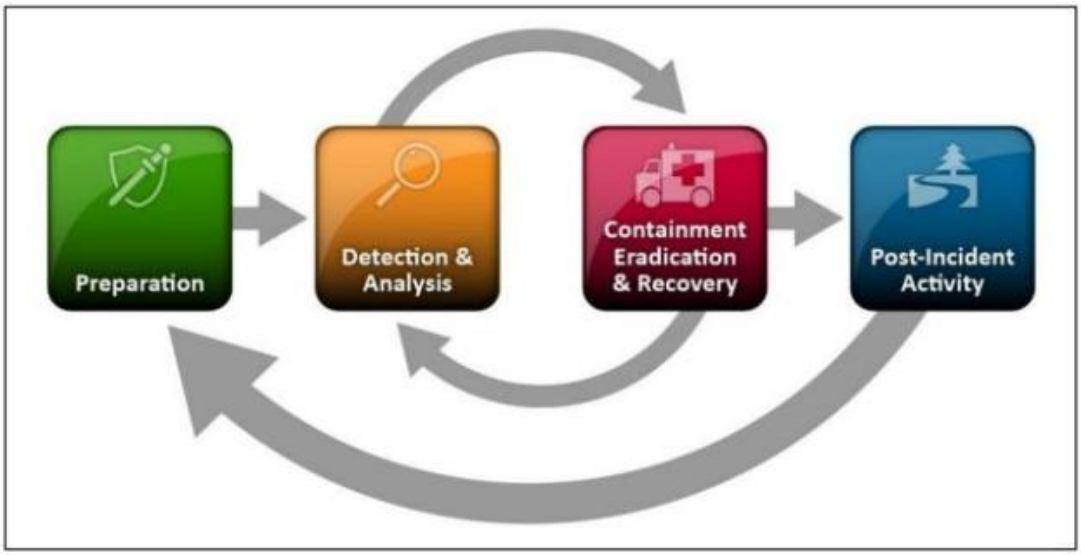
8.4. โครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure)

เพื่อให้การดำเนินการรับมือเหตุภัยคุกคามทางไซเบอร์ สามารถนำไปปฏิบัติได้อย่างมีประสิทธิภาพจะต้องกำหนดโครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ โดยแต่ละตำแหน่งจะต้องร่วมมือ ติดตาม ปฏิบัติงานตาม บทบาทหน้าที่ที่กำหนดไว้



9. 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 ดังนี้



วัฏจักรของการตอบสนองต่อเหตุการณ์

9.1 <u>ขั้นการเตรียมการ (preparation)</u>

เป็นการดำเนินมาตรการเพื่อเตรียมการและป้องกันการเกิดภัยคุกคามทางไซเบอร์เป็นสิ่งที่จะต้องทำในระยะเริ่มต้น เพื่อเตรียมความพร้อมเมื่อต้องเผชิญเหตุ ได้แก่ การจัดเตรียมข้อมูลให้พร้อม การจัดตั้งและฝึกอบรมบุคลากรหรือทีมงาน การจัดหาเครื่องมือและทรัพยากรต่างๆ ที่จำเป็น การตั้งค่าระบบต่างๆ ให้ปลอดภัย การจัดทำนโยบาย แผนงาน และกระบวนการที่เกี่ยวข้อง รวมถึงการสร้างเครือข่ายความร่วมมือ โดยดำเนินการดังต่อไปนี้

(1) กำหนดโครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT) รายละเอียดปรากฏตามข้อ 8.2

(2) กำหนดโครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure) รายละเอียดปรากฏตามข้อ 8.4

(3) กำหนดเกณฑ์และขั้นตอนในการเรียกใช้งาน (Activate) การตอบสนองต่อเหตุการณ์และ CIRT

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

(5) จัดเตรียมอุปกรณ์, ซอฟต์แวร์ และแหล่งข้อมูลสำหรับวิเคราะห์เหตุภัยคุกคามทางไซเบอร์

(6) จัดให้มีการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน (Risk Assessment)

(7) จัดทำแผนผังโครงสร้างขั้นตอนการรับมือฯ ของหน่วยงาน โดยหน่วยงานอาจดูตัวอย่างการจัดทำแผนผังโครงสร้างขั้นตอนการรับมือฯ ได้ (รายละเอียดปรากฏตามภาคผนวก 1)

(8) พิจารณาดำเนินการตามเอกสารแนบท้าย 2 ตารางที่ 2.1 ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ.2564

<u>9.2 ขั้นการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์</u>

เป็นการดำเนินการในการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (Detection and Analysis) ซึ่งเป็นสิ่งจำเป็นที่จะช่วยให้หน่วยงานสามารถบรรเทาความเสี่ยงที่ยังคงเหลืออยู่ และสามารถแจ้งเตือนได้อย่างทันท่วงทีเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น โดยดำเนินการดังต่อไปนี้

9.2.1 วิธีการที่ใช้ในการตรวจจับภัยคุกคาม

1) อุปกรณ์เฝ้าระวังเหตุการณ์ด้านความมั่นคงปลอดภัย

เครื่องมือและอุปกรณ์เฝ้าระวังเหตุการณ์ด้านความมั่นคงปลอดภัย

- Firewall ระบบรักษาความปลอดภัยของเครือข่ายคอมพิวเตอร์ที่สามารถควบคุม คัดกรองข้อมูลที่รับและส่งผ่านเครือข่ายได้
- IPS ระบบที่ทำหน้าที่ตรวจจับและป้องกันการโจมตีโดยเฉพาะที่เกิดขึ้นในระบบเครือข่าย โดยระบบประเภทนี้จะตรวจจับได้เฉพาะสิ่งที่ตรงกับวิธีการโจมตีที่ระบบรู้จัก
- Centralized Log Management ระบบจัดเก็บและบริหารจัดการข้อมูล Log File แบบศูนย์กลาง

2) แหล่งข่าวสารภัยคุกคามจากภายนอก (Threat Intelligence)

Chanel Types	**URL**
Cybersecurity news sites	
	https://webboard-nsoc.ncsa.or.th/category/12/cyber-security-news
	https://www.thaicert.or.th/category/cybernews/
	https://www.blognone.com/
	https://www.techtalkthai.com/category/security/
	https://thehackernews.com/
Community Facebook Pages	
	https://www.facebook.com/NCSA.Thailand/
	https://www.facebook.com/thaicert/
	https://www.facebook.com/pdpc.th/
	https://www.facebook.com/TBCERT.Official/
	https://www.facebook.com/2600Thailand/
	https://www.facebook.com/owaspbangkok/
	https://www.facebook.com/InfoSecThaiGirl/
	https://www.facebook.com/thaicysec/
	https://www.facebook.com/hackandsecbook/
	https://www.facebook.com/isecure.mssp/
Cyber Threat Intelligence Tools	
	https://attack.mitre.org/
	https://www.talosintelligence.com/
Cyber Threat Intelligence Tools	https://www.virustotal.com/gui/
	https://otx.alienvault.com/browse/
	https://urlscan.io/
	https://www.opencve.io/cve
	https://www.cvedetails.com/
	https://www.filescan.io/scan
	https://dnsdumpster.com/

9.2.2 ประเภทภัยคุกคามของหน่วยงาน

1) การจำแนกประเภทภัยคุกคามของหน่วยงาน

ประเภท	ความหมาย
Malicious Code (โปรแกรมไม่พึงประสงค์)	มัลแวร์ (Malware), Virus, Worm, Trojan, Ransomware, และ Spyware ต่าง ๆ ซึ่งเป็นโปรแกรมที่มีการทำงานที่มุ่งประสงค์ร้ายต่อคอมพิวเตอร์ หรือระบบเครือข่ายคอมพิวเตอร์
Intrusion Attempts Intrusions (ความพยายามบุกรุกเข้าระบบ)	Login Attempt, Connection Attempt, Brute-force เป็นการ ดำเนินการเพื่อจะควบคุมหรือทำให้เกิดความขัดข้องกับบริการของระบบ
Availability (ความพร้อมใช้ของระบบ)	การถูกโจมตีความพร้อมใช้งานของระบบ เช่น DDoS (Denial of Service), Open DNS Resolver, Flood ทำให้เกิดความล่าช้าในการบริการ จนถึงทำให้ระบบไม่สามารถทำงานได้
Phishing (การหลอกลวงโดยใช้อีเมลหรือหน้าเว็บไซต์ปลอมเพื่อให้ได้มาซึ่งข้อมูล)	การถูกสร้างหน้าเว็บไซต์ปลอม (Web Phishing) หรือหลอกลวงเพื่อให้ได้ ข้อมูลผ่านทางอีเมล
Web Defacement	การถูกปรับเปลี่ยนหน้าเว็บไซต์
SEO attack	เว็บไซต์ถูกโจมตี ด้วยการฝังสคริปต์โฆษณาเว็บไซต์การพนันออนไลน์
Vulnerability	ช่องโหว่ของระบบหรือจุดอ่อนของระบบบริหารจัดการเว็บไซต์
Abuse	การละเมิดการใช้งานเครือข่าย เช่น Spam, Copyright

2) การจำแนกประเภทภัยคุกคามตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์ พ.ศ. 2564

หมวดหมู่ คำอธิบาย	หมวดหมู่ คำอธิบาย
0	เหตุการณ์จำลอง และ การฝึกจู่โจม ของหน่วยงานเอง (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)

หมวดหมู่ คำอธิบาย	หมวดหมู่ คำอธิบาย
6	การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion)
7	การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)
8	เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating)
9	เหตุการณ์ผิดปกติที่ได้รับการวิเคราะห์แล้วว่าไม่ใช่เหตุการณ์ที่เป็นภัยคุกคาม (Explained Anomaly)

9.2.3 การวิเคราะห์ผลกระทบและระดับของภัยคุกคามทางไซเบอร์ (Incident Prioritization)

เพื่อรับมือภัยคุกคามทางไซเบอร์ให้ทันท่วงที โดยพิจารณาปัจจัยต่างๆ ที่เกี่ยวข้อง เช่น ผลกระทบต่อการทำงานของระบบ (functional impact) ผลกระทบต่อข้อมูล (information impact) และความสามารถในการกู้คืน (recoverability effort) เป็นต้น

ระดับผลกระทบต่อการดำเนินงาน (การเรียนการสอน การวิจัย การบริการวิชาการ)

ระดับผลกระทบ	หลักเกณฑ์การพิจารณาระดับของผลกระทบ
None	ไม่มีผลกระทบต่อการดำเนินงาน
Low	ส่งผลให้การปฏิบัติงานตามภารกิจหลักมีความล่าช้า แต่ยังสามารถดำเนินงานต่อได้
Medium	ส่งผลให้งานตามภารกิจหลักไม่สามารถดำเนินการได้บางส่วน
High	ส่งผลให้งานตามภารกิจหลักหยุดชะงัก

ระดับผลกระทบต่อข้อมูล

ระดับผลกระทบ	หลักเกณฑ์การพิจารณาระดับของผลกระทบ
None	ไม่มีข้อมูลรั่วไหล ถูกเปลี่ยนแปลง ทำลาย หรือเข้าถึง โดยที่ไม่ได้รับอนุญาต
Confidentiality Breach	การละเมิดความลับของข้อมูลส่วนบุคคลซึ่งมีการเข้าถึง หรือเปิดเผยข้อมูลส่วนบุคค
Integrity Breach	การละเมิดความถูกต้องครบถ้วนของข้อมูลส่วนบุคคลซึ่งมีการเปลี่ยนแปลงแก้ไขข้อมูลส่วนบุคคลให้ไม่ถูกต้อง ไม่สมบูรณ์ หรือไม่ครบถ้วน
Availability Breach	การละเมิดความพร้อมใช้งานของข้อมูลส่วนบุคคล ซึ่งทำให้ไม่สามารถเข้าถึงข้อมูลส่วนบุคคลได้ หรือมีการทำลายข้อมูลส่วนบุคคล ทำให้ข้อมูลส่วนบุคคลไม่อยู่ในสภาพที่พร้อมใช้งานได้ตามปกติ

ระดับความสามารถในการกู้คืน

ระดับผลกระทบ	หลักเกณฑ์การพิจารณาระดับของผลกระทบ
Regular	เวลาในการกู้คืนสามารถคาดการณ์ได้ โดยใช้ทรัพยากรที่มี
Supplemented	เวลาในการกู้คืนสามารถคาดการณ์ได้ แต่ต้องมีการจัดหาทรัพยากรเพิ่ม
Extended	เวลาในการกู้คืนไม่สามารถคาดการณ์ได้ ต้องใช้ทรัพยากรและความช่วยเหลือจากภายนอก
Not Recoverable	การกู้คืนไม่สามารถทำได้ ใช้กับสถานการณ์ที่ข้อมูลได้รั่วไหลสู่สาธารณะแล้ว ให้ใช้วิธีการติดตามและจำกัดการแพร่กระจายรวมถึงการเยียวยาผลกระทบ

9.2.4 การบันทึกภัยคุกคาม

ต้องทำการบันทึกข้อมูลเหตุการณ์ภัยคุกคามเพื่อช่วยในการรับมือและตอบสนองภัยคุกคามอย่างมีประสิทธิภาพ และเป็นระบบ โดยทำการบันทึกตั้งแต่การตรวจพบจนถึงสิ้นสุดของเหตุการณ์ภัยคุกคามตามแบบฟอร์มการบันทึกข้อมูลเหตุการณ์ภัยคุกคาม (รายละเอียดตามภาคผนวก 2)

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

เมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้นหรือเมื่อหน่วยงานได้รับแจ้งเตือนการเกิดภัยคุกคามทางไซเบอร์ หน่วยงานต้องมีการกำหนดแนวทางการดำเนินมาตรการเพื่อระงับภัยคุกคามทางไซเบอร์และการฟื้นฟูระบบที่ได้รับผลกระทบ โดยกำหนดให้สอดคล้องกับความรุนแรง และระดับของภัยคุกคามทางไซเบอร์แต่ละระดับ จนกระทั่งสามารถกู้คืนทรัพย์สินสำคัญทางสารสนเทศให้กลับมาดำเนินงานหรือให้บริการได้ตามปกติ

9.3.1 วิธีการควบคุมความเสียหาย คือ การตัดสินใจเลือกใช้วิธีที่เหมาะสมดังนี้

1) ดำเนินการสอบสวน (Investigate) สาเหตุและผลกระทบของเหตุการณ์

2) ปิดระบบ (Shut Down)

3) ตัดการเชื่อมต่อทางเครือข่ายทั้งหมด (Network disconnection) ทั้งนี้ อาจมียกเว้นการเชื่อมต่อสำหรับ Endpoint Detection & Response Agent (กระบวนการตรวจสอบและตรวจจับกิจกรรมหรือเหตุการณ์ ที่น่าสงสัยใดๆ ที่เกิดขึ้นที่ปลายทางแบบเรียลไทม์)

4) หยุดการทำงานของฟังก์ชันที่เกี่ยวข้อง (Disabling Certain Functions)

5) Redirect Network Traffic และ/หรือความสนใจของผู้บุกรุกไปยัง Blackhole/ Sandbox/ Honeypot

ทั้งนี้ การตัดสินใจเลือกใช้วิธีการควบคุมความเสียหายจะขึ้นอยู่กับลักษณะสถานการณ์ที่กำลังเผชิญ ประเภทของภัยคุกคาม ระบบงานหรือบริการที่ได้รับผลกระทบ ระยะเวลาและทรัพยากรที่จำเป็นต่อการควบคุม ความเสียหาย

9.3.2 การจัดเก็บและดูแลรักษาหลักฐานทางดิจิทัล

วัตถุประสงค์หลักของการจัดเก็บหลักฐาน คือเพื่อให้การแก้ไข Incident ส่งผลกระทบต่อมหาวิทยาลัยให้น้อยที่สุด (Minimizing impact to the university) นอกจากนี้ หลักฐานอาจมีความจำเป็นที่จะต้องใช้ในการดำเนินการตามขั้นตอนทางกฎหมาย การดำเนินการจัดเก็บหลักฐานทางดิจิทัลสามารถดำเนินการโดยพิจารณาตามหลักการดังต่อไปนี้

1) เป็นไปตามขั้นตอนที่กำหนดไว้ในกฎหมายข้อบังคับที่เกี่ยวกับหลักฐานดิจิทัล เพื่อให้สามารถนำไปใช้ ได้ในชั้นศาล

2) หลักฐานมีบันทึกการเข้าถึงและการกระทำการใดๆ ต่อหลักฐานตลอดเวลาอย่างรัดกุม

3) การเปลี่ยนตัวผู้ดูแลจำเป็นต้องมีการจัดทำบันทึกห่วงโซ่หลักฐาน (Chain of Custody) รายละเอียดเกี่ยวกับหลักฐาน ควรประกอบด้วยข้อมูลอย่างน้อยดังต่อไปนี้

3.1) ข้อมูลเฉพาะ เช่น Location, Serial Number, Model Number, Hostname, Media Access Control (MAC) Address เป็นต้น

3.2) ชื่อ ตำแหน่ง และช่องทางการติดต่อผู้จัดเก็บและรักษาหลักฐานระหว่างการรับมือ Incident

3.3) สถานที่จัดเก็บหลักฐาน

9.3.3 การกำจัดสาเหตุและการกู้คืนระบบให้กลับมาทำงานปกติ

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

1) การปิดช่องโหว่ของระบบ- การยกเลิก User Account ที่ผู้บุกรุกใช้เข้าสู่ระบบ

2) การแจ้งให้ผู้ใช้งานเปลี่ยนรหัสผ่าน

3) การลบโปรแกรมประเภท Backdoor ออกจากระบบ

4) การใช้ข้อมูล Indicator of Compromise (IOC) ในการสแกนหา Malware หรือร่องรอยอื่นๆ ในระบบที่ยังหลงเหลือของผู้บุกรุกเพื่อดำเนินการกำจัดให้ออกจากระบบทั้งหมด

หลังจากดำเนินการควบคุมความเสียหาย กำจัดสาเหตุของภัยคุกคามเสร็จเรียบร้อยแล้ว จะเข้าสู่กระบวนการฟื้นฟูระบบให้เข้าสู่สภาวะการทำงานปกติโดยในขั้นตอนนี้สิ่งที่มีความสำคัญเป็นอย่างยิ่ง และควร เตรียมการล่วงหน้าในเรื่องดังต่อไปนี้

1) การ Restore Operating System หรือ Application Software ต่างๆ จาก Master Image ที่ปลอดภัย

2) การ Restore ข้อมูลกลับเข้าระบบจาก Back Up Storage

<u>9.4 ขั้นการดำเนินการภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์</u>

การดำเนินกิจกรรมที่เกี่ยวของภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ (Post-incident Activity) นั้น ให้จัดทำข้อกำหนดขั้นตอน วิธีปฏิบัติ ที่เกี่ยวของเพื่อให้มีแนวทางที่ชัดเจน ซึ่งการปฏิบัติตามมาตรการดังกล่าว เพื่อให้สามารถเรียนรู้จากเหตุภัยคุกคามทางไซเบอร์ที่ผ่านมา และสามารถหาแนวทางเพื่อแก้ไขจุดบกพร่อง และพัฒนาแนวทางรับมือกับภัยคุกคามทางไซเบอร์ต่อไปในอนาคต โดยให้มีการประชุมหารือเพื่อแลกเปลี่ยนข้อมูล ความคิดเห็นในการนำไปพัฒนาและปรับปรุงแนวทางในการรับมือและตอบสนองภัยคุกคามทางไซเบอร์ รวมทั้งการ ใช้ข้อมูลเพื่อประกอบการพิจารณาปรับปรุง

นอกจากนี้ต้องเก็บรักษาข้อมูลและพยานหลักฐานที่จำเป็น เพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์ หรือใช้ในกรณีที่ต้องการร้องทุกข์หรือดำเนินคดี เนื่องจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้นนั้นอาจเข้าลักษณะเป็น 12 ความผิดตามประมวลกฎหมายอาญา หรือพระราชบัญญัติว่าด้วยการกระทำ

ความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 และที่แก้ไขเพิ่มเติม หรือกฎหมายอื่นๆ ที่เกี่ยวข้อง โดยการเก็บข้อมูลบางประเภทนั้นอาจจำเป็นต้อง ดำเนินการตั้งแต่เมื่อมีการตรวจพบว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้น เนื่องจากข้อมูลดังกล่าวอาจสูญหายไปใน ระหว่างที่ต้องระงับเหตุภัยคุกคามทางไซเบอร์นั้น หรืออาจถูกลบหรือทำลายโดยผู้โจมตีเมื่อมีการเก็บรวบรวมข้อมูล และหลักฐานที่จำเป็นแล้ว ให้นำข้อมูลและหลักฐานที่รวบรวมได้มาใช้ในการจัดทำบันทึกข้อมูลสถิติภัยคุกคาม ทางไซเบอร์โดยอาจจัดทำเป็นรายสัปดาห์หรือรายเดือน เพื่อเสนอต่อผู้ที่มีหน้าที่ดูแลและรับผิดชอบภายใน หน่วยงาน และกำหนดขั้นตอนที่หน่วยงานควรดำเนินการ เพื่อป้องกันไม่ให้เกิดภัยคุกคามทางไซเบอร์ในลักษณะ ดังกล่าวขึ้นอีกในอนาคต
หลักการดูแลรักษาหลักฐานทางดิจิทัลที่สำคัญมีดังนี้

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

Chain of custody หรือ “ห่วงโซ่การคุ้มครองพยานหลักฐาน” คือ เอกสารแสดงลำดับการเกิดเหตุการณ์ หรือเอกสารแสดงทุกขั้นตอน ตั้งแต่การยึดเครื่องคอมพิวเตอร์ การดูแลรักษา การควบคุม การวิเคราะห์ และการ จัดเก็บหลักฐานทางอิเล็กทรอนิกส์ เนื่องจากหลักฐานที่พบสามารถนำไปใช้ในยืนยันได้ในชั้นศาล หลักฐานเหล่านี้จึง จะต้องได้รับการจัดการอย่างระมัดระวัง และรอบคอบเพื่อหลีกเลี่ยงข้อกล่าวหาว่าเป็นหลักฐานที่ปลอมหรือทำ ขึ้นมา

9.5 การจัดทำรายการตรวจสอบการจัดการเหตุการณ์ (incident Handing Checklist)

หน่วยงานจะต้องจัดทำรายการตรวจสอบการจัดการเหตุการณ์ ซึ่งจะช่วยให้แนวทางแก่หน่วยงานเกี่ยวกับขั้นตอนสำคัญที่ควรดำเนินการ โดยหน่วยงานสามารถใช้ข้อมูลเพื่อประกอบการพิจารณาความเหมาะสมในการจัดทำรายการตรวจสอบของตนเองได้ (รายละเอียดตามภาคผนวก 3)

ภาคผนวก 1

1. ขั้นตอนการทำงานและรับมือเหตุภัยคุกคามทางไซเบอร์ที่กระทบต่อบริการที่สำคัญของหน่วยงาน

ตรวจสอบเหตุการณ์ด้านความมั่นคงปลอดภัยจากระบบเฝ้าระวัง หรือเมื่อได้รับแจ้งเหตุและหากพบเหตุการณ์ที่เกิดขึ้นกระทบต่อบริการที่สำคัญของหน่วยงานให้เริ่มดำเนินการตามประบวนการทำงาน ดังนี้

1.1 มีการเฝ้าระวังและตรวจสอบเหตุการณ์ด้านความมั่นคงปลอดภัย (Detection)

1.2 ดำเนินการตรวจสอบข้อมูลภัยคุกคามทางไซเบอร์ (Analysis) และประเมินระดับภัยคุกคามตามที่กำหนดใน พรบ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 มาตรา 60

1.3 พิจารณารายงานแจ้งเหตุละเมิดไปยังหน่วยงานที่เกี่ยวข้อง เช่น สกมช. สคส.

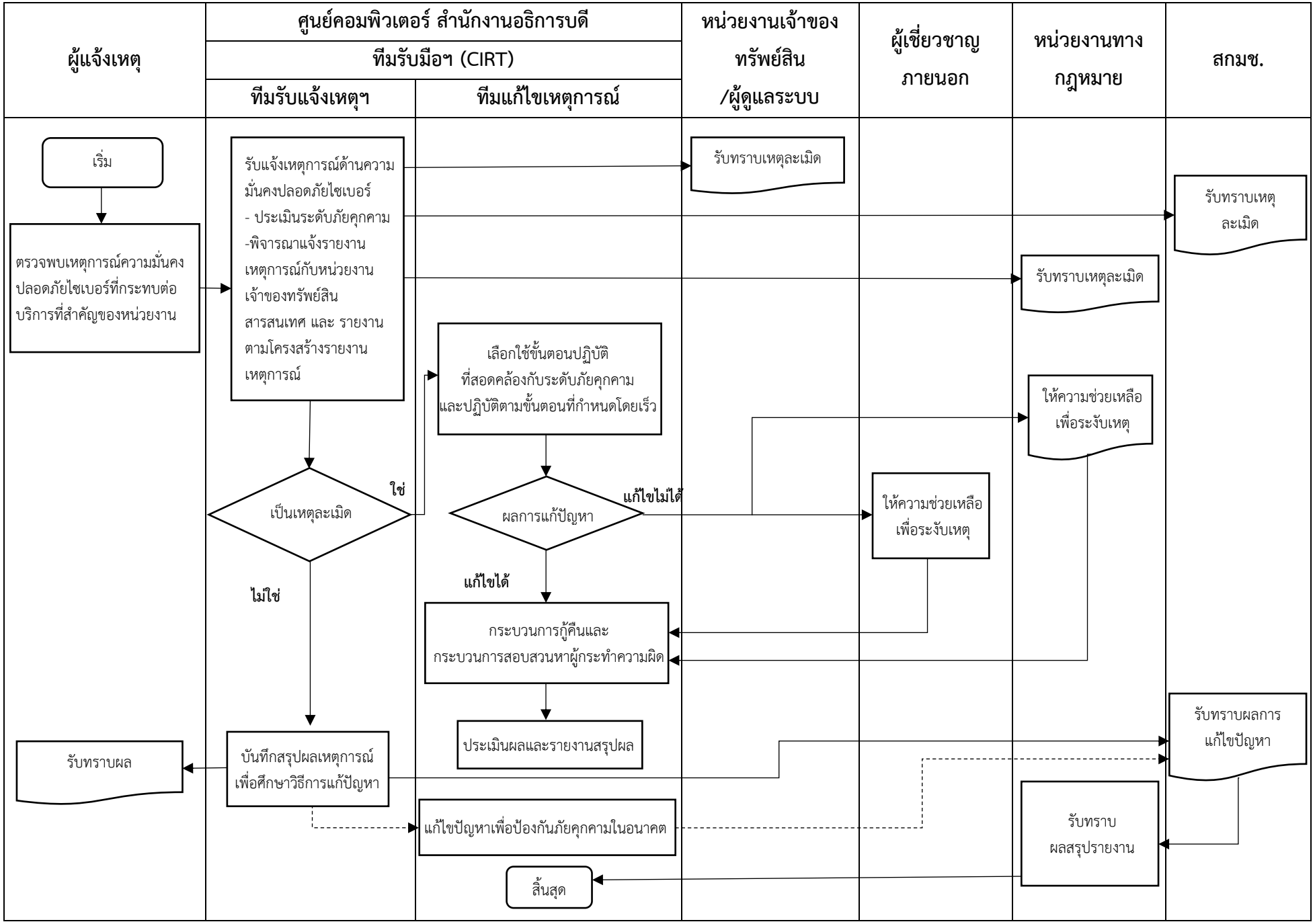
1.4 ดำเนินการควบคุมภัยคุกคามทางไซเบอร์ (Containment) เพื่อให้ส่งผลกระทบน้อยที่สุดและเพื่อป้องกันไม่ให้เกิดการแพร่กระจายไปยังส่วนอื่นๆ ซึ่งหากเป็นกรณีที่เร่งด่วนและเป็นภัยคุกคามทางไซเบอร์ในระดับร้ายแรงมหาวิทยาลัยจะดำเนินการปิดกั้น หรือ ตัดการเชื่อมต่อระบบคอมพิวเตอร์เป็นการชั่วคราว

1.5 ดำเนินการแก้ไข (Eradication) กู้คืนระบบ และในกรณีที่ไม่สามารถแก้ไขปัญหาได้จะดำเนินการติดต่อประสานงานไปยังศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) หรือผู้เชี่ยวชาญภายนอกเพื่อขอคำแนะนำหรือขอความช่วยเหลือ

1.6 ติดตามผลการแก้ไขและสถานการณ์ทำงานของระบบ หากพบว่าเหตุการณ์ยังไม่สิ้นสุดให้ดำเนินการควบคุม แก้ไข และติดตามสถานการณ์ต่อไปจนกว่าระบบที่ได้รับผลกระทบกลับมาทำงานได้ตามปกติ

1.7 ประเมินผลและจัดทำรายงานสรุปผลการดำเนินการรับมือภัยคุกคามทางไซเบอร์ที่เกิดขึ้น

แผนผังโครงสร้างขั้นตอนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response)



2. ขั้นตอนการทำงานการเฝ้าระวังเหตุการณ์ด้านความมั่นคงปลอดภัยจากหน่วยงานภายใน/ภายนอกมหาวิทยาลัย (ไม่กระทบต่อบริการที่สำคัญ)

ตรวจสอบเหตุการณ์ด้านความมั่นคงปลอดภัยจากระบบเฝ้าระวังฯ หากพบเหตุการณ์ด้านความมั่นคงปลอดภัยที่ผิดปกติ หรือได้รับการแจ้งเตือนพบเหตุการณ์ที่ผิดปกติจากหน่วยงานภายนอกมหาวิทยาลัยให้เริ่มดำเนินการตามกระบวนการทำงาน ดังนี้

1) บันทึกข้อมูลเหตุการณ์ด้านความมั่นคงปลอดภัยที่ผิดปกติที่ได้ตรวจสอบพบ หรือได้รับการแจ้งเตือนลงในแบบรายงานฯ

2) รวบรวมข้อมูลต่างๆ ที่เกี่ยวข้องกับภัยคุกคามที่ตรวจสอบพบ หรือได้รับการแจ้งเตือนจากหน่วยงานภายนอก จากอุปกรณ์ด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

3) วิเคราะห์ข้อมูลภัยคุกคามที่ตรวจสอบพบเป็นการโจมตีประเภทใด

4) บันทึกข้อมูลลงในแบบรายงาน

5) จัดระดับความเร่งด่วนในการแก้ไขปัญหาภัยคุกคาม รายละเอียด ดังนี้

(1) เร่งด่วน : มีความเสี่ยงส่งผลกระทบในวงกว้างทั่วทั้งมหาวิทยาลัย

(2) มาก : มีความเสี่ยงส่งผลกระทบต่อคณะ ส่วนงาน ตั้งแต่ 2 แห่งขึ้นไป

(3) ปานกลาง : มีความเสี่ยงส่งผลกระทบต่อคณะ ส่วนงาน หน่วยงาน ที่โดนโจมตีเท่านั้น

(4) ปกติ : ยังไม่มีผลกระทบที่เกิดขึ้น แต่หากไม่ดำเนินการจะส่งผลกระทบในอนาคต

6) บันทึกข้อมูลลงในแบบรายงานฯ

7) เตรียมแนวทางการแก้ไขปัญหา หากมีข้อมูลเดิมที่ได้จัดทำไว้แล้วให้นำข้อมูลดังกล่าวนำส่งต่อไป หากยังไม่มีแนวทางการแก้ไขปัญหา ต้องค้นคว้าหาข้อมูลแนวทางแก้ไขปัญหาเพิ่มเติม

8) ตรวจสอบข้อมูลเหตุการณ์ด้านความมั่นคงปลอดภัยที่ตรวจสอบพบนั้น เป็นของหน่วยงานใดหรือผู้ใช้งานใด

9) แจ้งปัญหาพร้อมทั้งแนะนำแนวทางแก้ไขปัญหาไปยังหน่วยงานที่เกี่ยวข้อง ตามระดับความเร่งด่วน รายละเอียด ดังนี้

(1) เร่งด่วน : โทรแจ้งทันที พร้อมทั้งแจ้งอีเมล

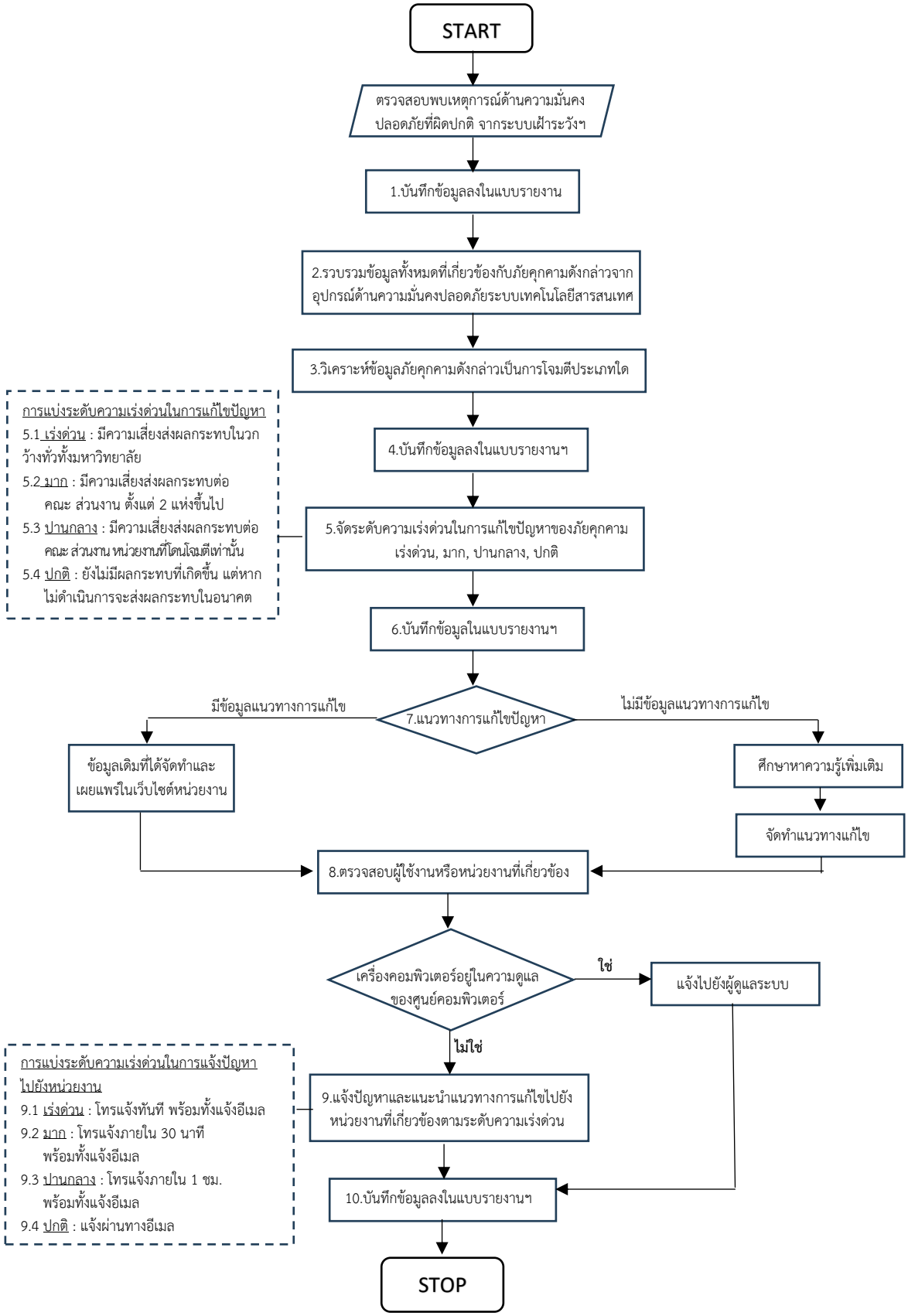
(2) มาก : โทรแจ้งภายใน 30 นาที พร้อมทั้งแจ้งอีเมล

(3) ปานกลาง : โทรแจ้งภายใน 1 ชั่วโมง พร้อมทั้งแจ้งอีเมล

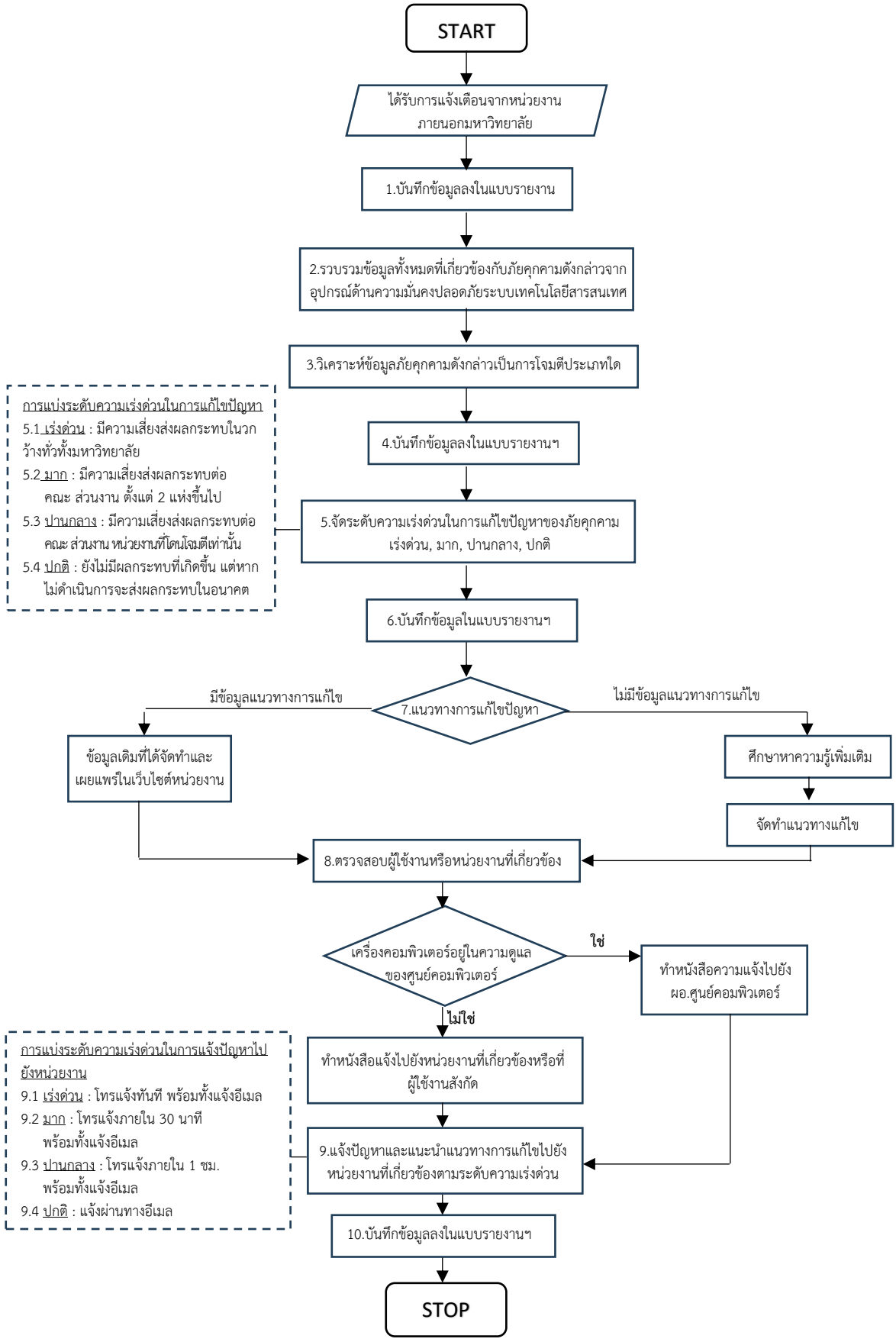
(4) ปกติ : แจ้งผ่านทางอีเมล

10) บันทึกข้อมูลลงในแบบรายงานฯ

กระบวนการทำงาน
เฝ้าระวังเหตุการณ์ด้านความมั่นคงปลอดภัยจากหน่วยงานภายในมหาวิทยาลัยราชภัฏอุบลราชธานี



กระบวนการทำงาน
เฝ้าระวังเหตุการณ์ด้านความมั่นคงปลอดภัยจากหน่วยงานภายนอกมหาวิทยาลัยราชภัฏอุบลราชธานี



3. ขั้นตอนการทำงานการประสานงานติดตามเหตุการณ์ด้านความมั่นคงปลอดภัย มหาวิทยาลัยราชภัฏอุบลราชธานี

3.1 ติดตาม Ticket ในแบบรายงาน

3.2 ตรวจสอบตามระดับความเร่งด่วนในการแก้ไข รายละเอียด ดังนี้

3.2.1 เร่งด่วน : มีความเสี่ยงส่งผลกระทบในวงกว้างทั่วทั้งมหาวิทยาลัย

3.2.2 มาก : มีความเสี่ยงส่งผลกระทบต่อคณะ ส่วนงาน ตั้งแต่ 2 แห่งขึ้นไป

3.2.3 ปานกลาง : มีความเสี่ยงส่งผลกระทบต่อคณะ ส่วนงาน หน่วยงาน ที่โดนโจมตีเท่านั้น

3.2.4 ปกติ : ยังไม่มีผลกระทบที่เกิดขึ้น แต่หากไม่ดำเนินการจะส่งผลกระทบในอนาคต

3.3 แบ่งประเภทของการประสานงาน

3.3.1 กรณีประสานภายนอกมหาวิทยาลัย

1) ตรวจสอบการแก้ไขปัญหาจากระบบหากพบว่าแก้ไขสำเร็จทำการบันทึกข้อมูลลงในระบบรายงาน

2) ตรวจสอบการแก้ไขปัญหาจากระบบหากพบว่าแก้ไขไม่สำเร็จ ให้ติดต่อไปยังหน่วยงานถึงปัญหาที่ยังคงอยู่อีกครั้ง

3.3.2 กรณีประสานภายในมหาวิทยาลัย

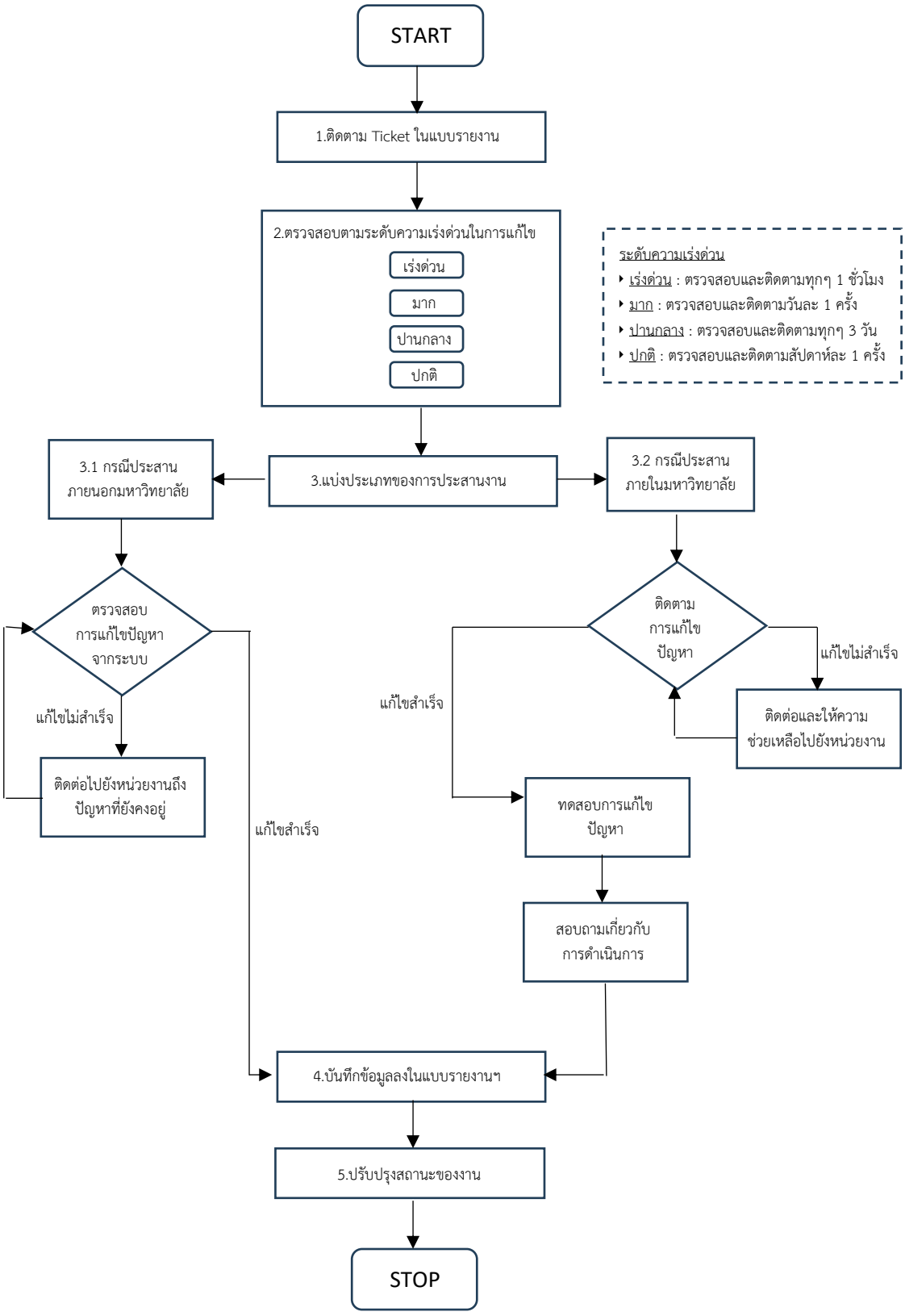
1) ติดตามการแก้ไขปัญหากรณีหน่วยงานแก้ไขสำเร็จ ทำการทดสอบการแก้ไขปัญหาดังกล่าว พร้อมทั้งสอบถามเกี่ยวกับการดำเนินการ

2) ติดตามการแก้ไขปัญหากรณีหน่วยงานแก้ไขไม่สำเร็จ ให้ทำการติดต่อและให้ความช่วยเหลือไปยังหน่วยงาน กรณีที่หน่วยงานมีการร้องขอ

3.4 บันทึกลงในระบบรายงาน

3.5 ปรับปรุงสถานะของงาน

กระบวนการทำงาน
การประสานงานติดตามเหตุการณ์ด้านความมั่นคงปลอดภัยมหาวิทยาลัยราชภัฏอุบลราชธานี



ภาคผนวก 2

แบบรายงานภัยคุกคามทางไซเบอร์

<table>
<tr><td>วันที่ :</td><td>เวลา :</td><td>ผู้บันทึกรายงาน :
ติดต่อ :</td></tr>
<tr><td colspan="3">ข้อมูลทั่วไป (General Information)</td></tr>
<tr><td colspan="3">ชื่อหน่วยงาน .....
ชื่อระบบงาน / โครงการ .....</td></tr>
<tr><td colspan="2">ชื่อผู้ประสานงานของหน่วยงาน.....
โทรศัพท์ .....
E-mail .....</td><td>ระบบปฏิบัติการ .....
IP Address .....
Mac Address .....</td></tr>
<tr><td colspan="2">ข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์</td><td></td></tr>
<tr><td>วันและเวลาที่เกิดเหตุการณ์ :</td><td colspan="2"></td></tr>
<tr><td>สถานะเหตุการณ์ปัจจุบัน :</td><td colspan="2">☐ เพิ่งพบเหตุการณ์ ☐ อยู่ในขั้นตอนการขอความช่วยเหลือ ☐ อยู่ในขั้นตอนการสอบสวน
☐ กำลังลุกลาม ☐ อยู่ในขั้นตอนการระงับภัย ☐ สามารถระงับภัยได้แล้ว
☐ รายงานปิดเหตุการณ์ภัยคุกคามแล้ว ☐ อื่นๆ .....</td></tr>
<tr><td>ประเภทเหตุการณ์ :</td><td colspan="2">
<table>
<tr><th>หมวดหมู่</th><th>คำอธิบาย</th></tr>
<tr><td>☐ 0</td><td>เหตการณ์จำลองและการฝึกจู่โจมของหน่วยงาน (Training and Exercises)</td></tr>
<tr><td>☐ 1</td><td>การพยายามเข้าถึงระบบที่ไม่สำเร็จ (Unsuccessful Activity Attempt)</td></tr>
<tr><td>☐ 2</td><td>การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance)</td></tr>
<tr><td>☐ 3</td><td>การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยที่หน่วยงานกำหนด (Non-Compliance Activity)</td></tr>
<tr><td>☐ 4</td><td>การบุกรุกโดยใช้มัลแวร์ (Malicious Logic)</td></tr>
<tr><td>☐ 5</td><td>การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion)</td></tr>
<tr><td>☐ 6</td><td>การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion)</td></tr>
<tr><td>☐ 7</td><td>การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)</td></tr>
<tr><td>☐ 8</td><td>เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating)</td></tr>
<tr><td>☐ 9</td><td>เหตุการณ์ผิดปกติที่ได้รับการวิเคราะห์แล้วว่าไม่ใช่เหตุการณ์ที่เป็นภัยคุกคาม (Explained Anomaly)</td></tr>
</table>
(ทั้งนี้ ภัยคุกคามหมวดหมู่ 0 1 และ 9 ไม่เข้าข่ายเป็นภัยคุกคามทางไซเบอร์ที่ต้องรายงาน)
</td></tr>
<tr><td>ระดับความรุนแรง
และผลกระทบที่เกิดขึ้น:</td><td colspan="2">ระบบที่ได้รับผลกระทบมีความสำคัญต่อพันธกิจหลักของหน่วยงานหรือไม่
☐ ใช่ ☐ ไม่ใช่
เหตุการณ์ที่เกิดขึ้นเกิดจากภัยคุกคามทางไซเบอร์มนระดับใด (มาตรา 60)
☐ ไม่ร้ายแรง ☐ ร้ายแรง ☐ วิกฤต (ก) ☐ วิกฤต (ข) ☐ ยังไม่สามารถระบุได้</td></tr>
<tr><td>รายละเอียดเหตุการณ์ :</td><td colspan="2"></td></tr>
<tr><td>ความเสียหายที่เกิดขึ้น :</td><td colspan="2"></td></tr>
<tr><td colspan="3">ข้อมูลการรับมือภัยคุกคาม</td></tr>
<tr><td>การสำรองข้อมูล (Backup)</td><td colspan="2">☐ มี ☐ ไม่มี</td></tr>
<tr><td>การดำเนินการตอบสนองต่อเหตุการณ์ :</td><td colspan="2">☐ ยังไม่ได้ดำเนินการแก้ไขใดๆ ☐ ยกเลิกการเชื่อมต่อระบบออกจากเครือข่ายแล้ว
☐ ตรวจสอบข้อมูลจราจร (Log) แล้ว ☐ ตรวจสอบโปรแกรม (แฟ้ม binaries/.exe) แล้ว
☐ กู้คืนกลับมาด้วยระบบหรือข้อมูลสำรองที่ตรวจสอบความถูกต้องแล้ว
☐ รายละเอียดการแก้ไขภัยคุกคามที่เกิดขึ้นเพิ่มเติม .....</td></tr>
<tr><td>รายละเอียดการรับมือภัยคุกคามอื่นๆ :</td><td colspan="2"></td></tr>
</table>

คำอธิบาย มาตรา 60

มาตรา ๖๐ การพิจารณาเพื่อใช้อำนาจในการป้องกันภัยคุกคามทางไซเบอร์ คณะกรรมการจะกำหนดลักษณะของภัยคุกคามทางไซเบอร์ โดยแบ่งออกเป็นสามระดับ ดังต่อไปนี้

(๑) ภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง หมายถึง ภัยคุกคามทางไซเบอร์ที่มีความเสี่ยงอย่างมีนัยสำคัญถึงระดับที่ทำให้ระบบคอมพิวเตอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศหรือการให้บริการของรัฐด้อยประสิทธิภาพลง

(๒) ภัยคุกคามทางไซเบอร์ในระดับร้ายแรง หมายถึง ภัยคุกคามที่มีลักษณะการเพิ่มขึ้น อย่างมีนัยสำคัญของการโจมตีระบบคอมพิวเตอร์ คอมพิวเตอร์ หรือข้อมูลคอมพิวเตอร์ โดยมุ่งหมาย เพื่อโจมตีโครงสร้างพื้นฐานสำคัญของประเทศและการโจมตีดังกล่าวมีผลทำให้ระบบคอมพิวเตอร์หรือ โครงสร้างสำคัญทางสารสนเทศที่เกี่ยวข้องกับการให้บริการของโครงสร้างพื้นฐานสำคัญของประเทศ ความมั่นคงของรัฐ ความสัมพันธ์ระหว่างประเทศ การป้องกันประเทศ เศรษฐกิจ การสาธารณสุข ความปลอดภัยสาธารณะหรือความสงบเรียบร้อยของประชาชนเสียหาย จนไม่สามารถทำงานหรือให้บริการได้

(๓) ภัยคุกคามทางไซเบอร์ในระดับวิกฤติ หมายถึง ภัยคุกคามทางไซเบอร์ในระดับวิกฤติ ที่มีลักษณะ ดังต่อไปนี้

(ก) เป็นภัยคุกคามทางไซเบอร์ที่เกิดจากการโจมตีระบบคอมพิวเตอร์ คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ในระดับที่สูงขึ้นกว่าภัยคุกคามทางไซเบอร์ในระดับร้ายแรง โดยส่งผลกระทบรุนแรง ต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศในลักษณะที่เป็นวงกว้าง จนทำให้การทำงานของหน่วยงานรัฐหรือการให้บริการของโครงสร้างพื้นฐานสำคัญของประเทศที่ให้กับประชาชนล้มเหลวทั้งระบบจนรัฐไม่สามารถควบคุมการทำงานส่วนกลางของระบบคอมพิวเตอร์ของรัฐได้ หรือการใช้มาตรการเยียวยาตามปกติในการแก้ไขปัญหาภัยคุกคามไม่สามารถแก้ไขปัญหาได้และมีความเสี่ยงที่จะลุกลามไปยังโครงสร้างพื้นฐานสำคัญอื่น ๆ ของประเทศ ซึ่งอาจมีผลทำให้บุคคลจำนวนมากเสียชีวิตหรือระบบคอมพิวเตอร์ คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์จำนวนมากถูกทำลายเป็นวงกว้างในระดับประเทศ

(ข) เป็นภัยคุกคามทางไซเบอร์อันกระทบหรืออาจกระทบต่อความสงบเรียบร้อยของประชาชนหรือเป็นภัยต่อความมั่นคงของรัฐหรืออาจทำให้ประเทศหรือส่วนใดส่วนหนึ่งของประเทศตกอยู่ในภาวะคับขันหรือมีการกระทำความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา การรบหรือการสงคราม ซึ่งจำเป็นต้องมีมาตรการเร่งด่วนเพื่อรักษาไว้ซึ่งการปกครองระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุขตามรัฐธรรมนูญแห่งราชอาณาจักรไทย เอกราชและบูรณภาพแห่งอาณาเขต ผลประโยชน์ของชาติ การปฏิบัติตามกฎหมาย ความปลอดภัยของประชาชน การดำรงชีวิตโดยปกติสุขของประชาชน การคุ้มครองสิทธิเสรีภาพ ความสงบเรียบร้อยหรือประโยชน์ส่วนรวม หรือการป้องปัด หรือแก้ไขเยียวยาความเสียหายจากภัยพิบัติสาธารณะอันมีมาอย่างฉุกเฉินและร้ายแรง

ทั้งนี้ รายละเอียดของลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ ให้คณะกรรมการเป็นผู้ประกาศกำหนด

ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. 2564 เพิ่มเติม (https://www.ratchakitcha.soc.go.th/DATA/PDF/2564/E/303/T_0003.PDF)

ภาคผนวก 3

รายการตรวจสอบการจัดการเหตุการณ์ (Incident Handling Checklist)

รายการตรวจสอบการจัดการเหตุการณ์		บทบาทความรับผิดชอบ	Complete
ขั้นการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (detection and analysis)			
1.	ตรวจสอบว่ามีเหตุการณ์เกิดขึ้นหรือไม่	ทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์	
1.1	วิเคราะห์ตรวจจับสัญญาณเหตุการณ์ความปลอดภัยทางไซเบอร์		
1.2	ค้นหาข้อมูลเพิ่มเติมที่มีความสัมพันธ์กัน		
1.3	ดำเนินการสืบค้นข้อมูล (เช่น search engines, ฐานข้อมูลอื่นๆ เป็นต้น)		
1.4	ทันทีที่ผู้ผู้จัดการรับมือฯ เหตุการณ์เชื่อว่ามีเหตุการณ์เกิดขึ้น ให้เริ่มบันทึกการสอบสวนและรวบรวมหลักฐาน		
2.	จัดลำดับความสำคัญในการจัดการเหตุการณ์ตามระดับความรุนแรงของภัยคุกคามที่เกิดขึ้น		
3.	รายงานเหตุการณ์ดังกล่าวต่อผู้บริหารและหน่วยงานภายนอกที่เกี่ยวข้อง		
ขั้นการระงับภัยคุกคาม ปราบปราม และฟื้นฟูระบบงานที่ได้รับผลกระทบ (containment, eradication, and recovery)			
4.	บันทึกเหตุการณ์, จัดเก็บและดูแลรักษาหลักฐานเกี่ยวกับเหตุการณ์ทั้งหมดก่อนเริ่มกระบวนการกู้คืนซึ่งรวมถึงการได้มาของบันทึกการยึดหลักฐานคอมพิวเตอร์ที่ได้มา หรืออุปกรณ์อื่นๆ เพื่อสนับสนุนการสอบสวน	ทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์	
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	หากจำเป็นให้ดำเนินการติดตามสถานการณ์ต่อไปเพื่อค้นหาเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ที่อาจเกี่ยวข้องในอนาคต		
การดำเนินการภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ (post-incident activity)			
9.	จัดทำรายงานการติดตามผล	ทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์	
10.	จัดการประชุมทบทวนบทเรียนที่เกิดขึ้นจากเหตุการณ์ดังกล่าว		

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 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)

* 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 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

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)
☐ อื่นๆ	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

รายละเอียดอื่นๆ: โปรดระบุ

หมวด ค: ข้อมูลการรับมือภัยคุกคาม
ค1. สถานการณ์หรือการแก้ไขเหตุภัยคุกคาม (เลือกได้มากกว่า 1 รายการ) ☐ เพิ่งพบเหตุการณ์ ☐ อยู่ในขั้นตอนการขอความช่วยเหลือ ☐ อยู่ในขั้นตอนการสอบสวน ☐ กำลังลุกลาม ☐ อยู่ในขั้นตอนการระงับภัย ☐ สามารถระงับภัยได้แล้ว ☐ รายงานปิดเหตุการณ์ภัยคุกคามแล้ว ☐ อื่นๆ: โปรดระบุ
ค2. สิ่งที่ได้ดำเนินการหรือได้แก้ไขไปแล้ว ☐ ยังไม่ได้ดำเนินการแก้ไขใดๆ ☐ ยกเลิกการเชื่อมต่อระบบออกจากเครือข่ายแล้ว ☐ ตรวจสอบข้อมูลจราจร (Log) แล้ว ☐ ตรวจสอบโปรแกรม (แฟ้ม binaries/.exe) แล้ว ☐ กู้คืนกลับมาด้วยระบบหรือข้อมูลสำรองที่ตรวจสอบความถูกต้องแล้ว ☐ รายละเอียดการแก้ไขภัยคุกคามที่เกิดขึ้นเพิ่มเติม: โปรดระบุ
ค3. รายละเอียดการรับมือภัยคุกคามอื่นๆ (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

ทรัพย์สินที่สำคัญอื่นๆ ที่อาจได้รับผลกระทบ: โปรดระบุ

จำนวนผู้ได้รับผลกระทบ (โดยประมาณ): โปรดระบุ

มูลค่าความเสียหาย (โดยประมาณ): โปรดระบุ

ในกรณีที่ข้อมูลที่ระบุตัวบุคคลได้รั่วไหล (หรือถูกขโมย):

จำนวนบุคคลที่เป็นเจ้าของข้อมูล : โปรดระบุ

ชนิดของข้อมูล (เลือกทุกข้อที่ใช่):

☐ ข้อมูลไบโอเมตริกซ์ ☐ ข้อมูลการติดต่อ

☐ ข้อมูลการเงิน ☐ ข้อมูลบุคลากรของรัฐ

☐ หมายเลขบัตรประชาชน ☐ ข้อมูลการติดต่อกับหน่วยงานต่างๆ

☐ ข้อมูลทางการแพทย์

☐ อื่นๆ : โปรดระบุ

จำนวนข้อมูล (Record) ที่ได้รับผลกระทบ: โปรดระบุ

ผลกระทบอื่นๆ 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)
☐ สิ่งที่ผิดปกติไปจากเดิมอื่นๆ: โปรดระบุ

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

ง1.6 รายละเอียดอื่นๆ 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

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)	
อื่นๆ	

ข้อ 3 สถิติรายปีจำแนกตามระดับภัยคุกคามทางไซเบอร์

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

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

ตารางแสดงความสอดคล้องกับประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564

ประกาศ กกม. เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานฯ พ.ศ. 2564	แผนรับมือฯ ฉบับนี้
19.2 ต้องจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan) ที่กำหนดว่าควรตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์อย่างไร โดยแผนการรับมือภัยคุกคามทางไซเบอร์ต้องมีรายละเอียดอย่างน้อย ดังต่อไปนี้	
(ก) โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT) รวมถึงบทบาทและความรับผิดชอบที่กำหนดไว้อย่างชัดเจนของสมาชิกในทีมแต่ละคนและรายละเอียดการติดต่อ	ข้อที่ 8.2
(ข) โครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure) ซึ่งกำหนดว่าหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจะปฏิบัติตามภาระหน้าที่ในการรายงานภายใต้พระราชบัญญัติ และกฎหมายย่อยใด ๆ ที่ทำขึ้นภายใต้กฎหมายดังกล่าว ตลอดจนภาระหน้าที่ในการรายงานภายใต้กฎหมาย และข้อกำหนดด้านกฎระเบียบที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ	ข้อที่ 8.4
(ค) เกณฑ์และขั้นตอนในการเรียกใช้งาน (Activate) การตอบสนองต่อเหตุการณ์และ CIRT	ข้อที่ 9.1 (3)
(ง) ขั้นตอนจำกัดขอบเขต (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์	ข้อที่ 9.3
(จ) การเรียกใช้งานกระบวนการกู้คืน (Recovery Process)	ข้อที่ 9.3.3
(ฉ) ขั้นตอนในการสอบสวน (Investigate) สาเหตุและผลกระทบของเหตุการณ์	ข้อที่ 9.3.1 ภาคผนวก 1
(ช) ขั้นตอนการเก็บรักษาหลักฐาน (Preservation of Evidence) ก่อนเริ่มกระบวนการกู้คืนซึ่งรวมถึงการได้มาของบันทึกการยึดหลักฐานคอมพิวเตอร์ที่ได้มา หรืออุปกรณ์อื่น ๆ เพื่อสนับสนุนการสอบสวน	ข้อที่ 9.3.2
(ซ) ระเบียบวิธีการมีส่วนร่วม (Engagement Protocols) กับบุคคลภายนอก หรือแนวปฏิบัติการบริหารจัดการบุคคลภายนอก ซึ่งรวมถึงรายละเอียดการติดต่อ ตัวอย่างเช่น ผู้ขายสำหรับบริการด้านนิติวิทยาศาสตร์/การกู้คืนและการบังคับใช้กฎหมายเพื่อดำเนินคดี และ	ข้อที่ 8.4
(ฌ) กระบวนการทบทวนหลังการดำเนินการ (After-Action Review Process) เพื่อระบุและแนะนำให้ปรับปรุงการดำเนินการเพื่อป้องกันการเกิดซ้ำ	ข้อที่ 9.4