แผนรับมือเหตุภัยคุกคามทางไซเบอร์
มหาวิทยาลัยราชภัฏสกลนคร
Cybersecurity Incident Response Plan

แผนรับมือเหตุภัยคุกคามทางไซเบอร์ มหาวิทยาลัยราชภัฏสกลนคร

1. หลักการและเหตุผล

แผนรับมือเหตุภัยคุกคามทางไซเบอร์ของมหาวิทยาลัยราชภัฏสกลนคร ฉบับนี้ จัดทำขึ้นเพื่อให้เป็นไปตามมาตรา 44 แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ที่กำหนดให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศดำเนินการจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเร็ว ซึ่งอย่างน้อยต้องประกอบด้วยเรื่อง (1) แผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยผู้ตรวจประเมินผู้ตรวจสอบภายใน หรือผู้ตรวจสอบอิสระจากภายนอก ซึ่งต้องดำเนินการอย่างน้อยปีละหนึ่งครั้ง และ (2) แผนการรับมือภัยคุกคามทางไซเบอร์ รวมทั้งเพื่อให้เป็นไปตามนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มหาวิทยาลัยราชภัฏสกลนคร ด้วย

2. วัตถุประสงค์

2.1 เพื่อใช้เป็นแผนในการรับมือเหตุภัยคุกคามทางไซเบอร์ที่เกิดขึ้นในมหาวิทยาลัยราชภัฏสกลนคร

2.2 เพื่อกำหนดหน้าที่และความรับผิดชอบให้กับหน่วยงานต่างๆ ภายใต้มหาวิทยาลัยราชภัฏสกลนคร

2.3 เพื่อกำหนดประเภทของเหตุภัยคุกคามทางไซเบอร์ กำหนดความสัมพันธ์กับนโยบายและแนวปฏิบัติที่เกี่ยวข้อง การรายงานเหตุภัยคุกคามทางไซเบอร์ และขั้นตอนการรับมือเหตุภัยคุกคามทางไซเบอร์ ตามขอบเขตของระบบสารสนเทศที่กำหนดไว้ รวมไปถึงการสื่อสารไปยังผู้มีส่วนได้ส่วนเสีย

2.4 เพื่อลดผลกระทบที่อาจเกิดขึ้นต่อการดำเนินงานของมหาวิทยาลัยราชภัฏสกลนคร

3. ขอบเขต

แผนรับมือเหตุภัยคุกคามทางไซเบอร์ มหาวิทยาลัยราชภัฏสกลนคร ฉบับนี้ ใช้รับมือเหตุภัยคุกคามทางไซเบอร์ที่เกิดขึ้นต่อระบบสารสนเทศ และข้อมูลดิจิทัลของมหาวิทยาลัยราชภัฏสกลนคร รวมถึงบุคคลหรืออุปกรณ์ใดๆ ซึ่งเข้าถึงระบบสารสนเทศและข้อมูลดิจิทัลดังกล่าว

4. หน้าที่การทบทวนแผน

คณะกรรมการจัดทำแผนรับมือภัยคุกคามทางไซเบอร์ ของมหาวิทยาลัยราชภัฏสกลนคร มีหน้าที่ทบทวนและขออนุมัติแผนรับมือเหตุภัยคุกคามทางไซเบอร์ มหาวิทยาลัยราชภัฏสกลนคร ฉบับนี้

5. หน้าที่ในการดำเนินการตามแผน

สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มีหน้าที่เป็นผู้รับผิดชอบหลักในการดำเนินการ ตามแผนรับมือเหตุภัยคุกคามทางไซเบอร์ มหาวิทยาลัยราชภัฏสกลนคร ฉบับนี้ โดยมีหน่วยงานสนับสนุนประกอบด้วย งานพัฒนาเทคโนโลยีเครือข่ายและโครงสร้างพื้นฐาน งานพัฒนาระบบสารสนเทศ รวมถึงสำนักงานอธิการบดี และสำนักส่งเสริมวิชาการและงานทะเบียน

6. รายละเอียดการบังคับใช้เอกสาร

แผนรับมือเหตุภัยคุกคามทางไซเบอร์ มหาวิทยาลัยราชภัฏสกลนคร มีรายละเอียดที่เกี่ยวข้องกับเอกสารดังต่อไปนี้

6.1. รายละเอียดของเอกสาร (Document control and review)

รายละเอียดของเอกสาร (Document control)	
ผู้จัดทำเอกสาร (Author)	คณะกรรมการจัดทำแผนรับมือเหตุภัยคุกคามทางไซเบอร์ ของมหาวิทยาลัยราชภัฏสกลนคร
ผู้ดำเนินการตามเอกสาร (Owner)	สำนักวิทยบริการและเทคโนโลยีสารสนเทศ
วันที่จัดทำเอกสาร (Date created)	13 มกราคม 2568
ผู้ตรวจสอบความถูกต้องของเอกสาร (Last reviewed by)	คณะกรรมการจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงด้านสารสนเทศ ของมหาวิทยาลัยราชภัฏสกลนคร
วันที่ตรวจสอบความถูกต้องของเอกสาร (Last date reviewed)	21 มกราคม 2568
ผู้อนุมัติเอกสาร และวันที่อนุมัติเอกสาร (Endorsed by and date)	อธิการบดีมหาวิทยาลัยราชภัฏสกลนคร
วันที่จะต้องมีการตรวจสอบเอกสารครั้งถัดไป (Next review due date)	21 มกราคม 2569

6.2. การเปลี่ยนแปลงเอกสาร (Version control)

รุ่น (Version)	**วันที่อนุมัติ (Date of Approval)**	**ผู้อนุมัติ (Approved by)**	**สถานะ (Description of change)**
1.0	21 มกราคม 2568	อธิการบดีมหาวิทยาลัยราชภัฏสกลนคร	อนุมัติ

7. เอกสารและกรอบมาตรฐานที่เกี่ยวข้อง

7.1 นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มหาวิทยาลัยราชภัฏสกลนคร

7.2 นโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) มหาวิทยาลัยราชภัฏสกลนคร

7.3 พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

8. นิยาม

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

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

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

เหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญ[1] หมายความว่า เหตุภัยคุกคามทางไซเบอร์ที่ปรากฏต่อระบบสารสนเทศ และเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามมาตรา ๔๙ ซึ่งคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติได้กำหนดลักษณะของภัยคุกคามทางไซเบอร์ไว้ตามมาตรา ๖๐ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒

9. บทบาทหน้าที่และโครงสร้างทีมรับมือเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์

9.1 ผู้รับแจ้งเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ภายในหน่วยงาน

มหาวิทยาลัยราชภัฏสกลนคร มีผู้รับแจ้งเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ภายในหน่วยงาน กรณีเมื่อมีการตรวจพบ หรือมีการรายงานเหตุการณ์เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ คลอบคลุมตลอดระยะเวลา 24 ชั่วโมง / 7 วัน จำนวน 2 คน ได้แก่

ลำดับ	ชื่อ – นามสกุล	ระยะเวลาในการปฏิบัติงาน	ช่องทางการติดต่อสื่อสาร	หน้าที่	ความรับผิดชอบ
1	นายอรรณพ อรังศรี	24 ชั่วโมง / 7 วัน	09-0970-5950 Email: annop@snru.ac.th	ผู้รับรายงานเหตุหลัก	รับรายงานเหตุการณ์เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์
2	นายดนุชา บัวพินธุ	24 ชั่วโมง / 7 วัน	08-687-6422 email : danucha@snru.ac.th	ผู้รับรายงานเหตุรอง	รับรายงานเหตุการณ์เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

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

9.2. โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber incident Response Team : CIRT)

มหาวิทยาลัยราชภัฏสกลนครใช้โมเดลโครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ในลักษณะ แบบรวมศูนย์ (Centralize) ประกอบด้วยสมาชิก ดังนี้

ลำดับ	ชื่อ - นามสกุล	ช่องทางการติดต่อสื่อสาร	หน้าที่	ความรับผิดชอบ
1	ผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ	04-297-0039 Email: arit.snru@snru.ac.th	หัวหน้าทีมรับมือฯ (Team manager)	ทำหน้าที่สื่อสารกับผู้บริหารของหน่วยงาน
2	หัวหน้างานพัฒนาเทคโนโลยีเครือข่ายและโครงสร้างพื้นฐาน (นายจยุตย์ พูลเพิ่ม)	08-3353-4753 Email: promaster@snru.ac.th	รองหัวหน้าทีมรับมือฯ (Deputy team manager)	ทำหน้าที่แทนกรณีหัวหน้าทีมรับมือฯ ไม่อยู่/ไม่สามารถปฏิบัติงานได้
3	หัวหน้างานพัฒนาระบบสารสนเทศ (นายกิตติภูมิ คำศรี)	08-3406-9279 Email: kittipum@snru.ac.th	รองหัวหน้าทีมรับมือฯ (Deputy team manager)	ทำหน้าที่แทนกรณีหัวหน้าทีมรับมือฯ ไม่อยู่/ไม่สามารถปฏิบัติงานได้
4	นายดนุชา บัวพินธุ	08-687-6422 Email: danucha@snru.ac.th	เจ้าหน้าที่รับมือฯ (Incident leader)	ทำหน้าที่ช่วยเหลือ (ชื่อหน่วยงานเจ้าของระบบภายใต้หน่วยงานของท่าน) ให้สามารถควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์ได้
5	นายอรรณพ อรังศรี	09-0970-5950 Email: annop@snru.ac.th	เจ้าหน้าที่เทคนิคฯ (Technical lead)	ทำหน้าที่ให้ความเห็นเกี่ยวกับแนวทางที่เหมาะสมในการควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์

ทั้งนี้ นอกจากทีมรับมือฯ ดังกล่าวข้างต้น ให้มีบุคคลดังต่อไปนี้ทำหน้าที่สนับสนุนการดำเนินการของแผนรับมือฯ ฉบับนี้ ดังนี้

ลำดับ	ชื่อ - นามสกุล	ช่องทางการติดต่อสื่อสาร	หน้าที่	ความรับผิดชอบ
1	ผู้แทนจากสำนักงานอธิการบดี	โทรศัพท์ : 042-970021 email: saraban@snru.ac.th	งานบริหารทั่วไป กองกลาง สำนักงานอธิการบดี	ทำหน้าที่ควบคุมผลกระทบจากภัยคุกคาม
2	ผู้แทนจากสำนักส่งเสริมวิชาการและงานทะเบียน	โทรศัพท์ : 042-970025 email: academic@snru.ac.th	สำนักส่งเสริมวิชาการและงานทะเบียน	ทำหน้าที่ควบคุมผลกระทบจากภัยคุกคาม

ลำดับ	ชื่อ - นามสกุล	ช่องทางการติดต่อสื่อสาร	หน้าที่	ความรับผิดชอบ
3	ผู้แทนจากหน่วยวินัยและนิติการ	โทรศัพท์ : 042-970112 email: lps@snru.ac.th	เจ้าหน้าที่ด้านการปฏิบัติตามกฎหมาย (Compliance)	ทำหน้าที่ดูแลด้านกฎระเบียบของมหาวิทยาลัย และกฎหมายที่เกี่ยวข้อง
4	นายอรรณพ อรังศรี	โทรศัพท์ : 09-0970-5950 email: annop@snru.ac.th	ผู้ทดสอบเจาะระบบ	ทำหน้าที่ทดสอบความมั่นคงปลอดภัยของระบบ
5	นายอัครชัย ใจตรง	โทรศัพท์ : 09-0970-5950 email: akarachai@snru.ac.th	ผู้ทดสอบเจาะระบบ	ทำหน้าที่ทดสอบความมั่นคงปลอดภัยของระบบ
6	ผู้แทนจากงานตรวจสอบภายใน	โทรศัพท์ : 042-970112 email: lps@snru.ac.th	ผู้บริหารจัดการความเสี่ยง	ทำหน้าที่ตรวจสอบผลกระทบจากภัยคุกคามที่เกิดขึ้น
7	ผู้แทนจากกองนโยบายและแผน สำนักงานอธิการบดี	โทรศัพท์ : 042-970047 Email: plan@snru.ac.th	ผู้บริหารจัดการความเสี่ยง	ทำหน้าที่ตรวจสอบผลกระทบจากภัยคุกคามที่เกิดขึ้น
8	ผู้แทนจากกองกลาง สำนักงานอธิการบดี	โทรศัพท์ : 042-970022 Email: saraban@snru.ac.th	ผู้บริหารจัดการความเสี่ยง	ทำหน้าที่ตรวจสอบผลกระทบจากภัยคุกคามที่เกิดขึ้น
9	ผู้แทนจากกองพัฒนานักศึกษา สำนักงานอธิการบดี	โทรศัพท์ : 042-970161 Facebook: www.facebook.com/sdd.snru	ผู้บริหารจัดการความเสี่ยง	ทำหน้าที่ตรวจสอบผลกระทบจากภัยคุกคามที่เกิดขึ้น
10	ผู้แทนจากบัณฑิตวิทยาลัย	โทรศัพท์ : 042-970229 Email: -	ผู้บริหารจัดการความเสี่ยง	ทำหน้าที่ตรวจสอบผลกระทบจากภัยคุกคามที่เกิดขึ้น
11	ผู้แทนจากงานประชาสัมพันธ์และโสตทัศนูปกรณ์สำนักงานอธิการบดี	โทรศัพท์ : 042-970021 email: pr@snru.ac.th	ผู้รับผิดชอบด้านสื่อสารองค์กร	ทำหน้าที่สื่อสารประชาสัมพันธ์ระหว่าง และหลังจากเกิดภัยคุกคาม

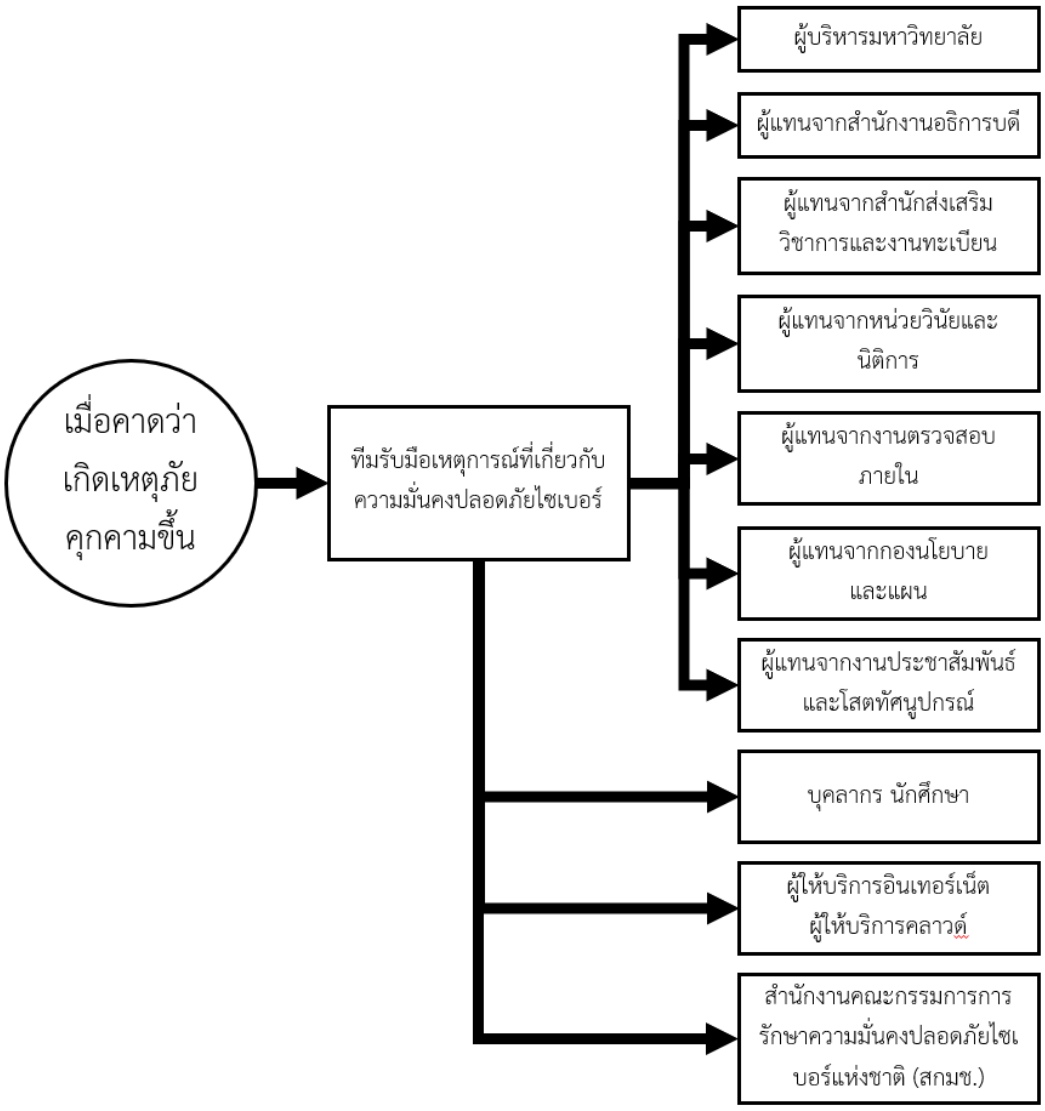
9.3 หน่วยงานภายนอกที่เกี่ยวข้อง

มหาวิทยาลัยราชภัฏสกลนคร กำหนดข้อมูลติดต่อสื่อสารของหน่วยงานภายนอกที่เกี่ยวข้อง ได้แก่ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.), หน่วยงานกำกับดูแล (Regulator), THAI – CERT และผู้ให้บริการภายนอกของหน่วยงาน ผู้ให้บริการด้านการตรวจสอบพิสูจน์หลักฐานทางดิจิทัล (Digital Forensic Investigator) และกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม ซึ่งเป็นหน่วยงานกำกับดูแล

ลำดับ	ชื่อ - นามสกุล	ช่องทางการติดต่อสื่อสาร	หน่วยงาน	ความเกี่ยวข้อง
1	ผู้แทนจาก สกมช.	เบอร์โทรศัพท์มือถือ : 02 142 6888 Email: saraban@ncsa.or.th ที่อยู่สำนักงาน :	*สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)*	ให้คำปรึกษากับหน่วยงานรัฐด้านภัยคุกคามทางไซเบอร์
2	ผู้แทนจาก กระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัย และนวัตกรรม	คุณสุพัชรพงษ์ บัวนาค 086 9868875 Email:	*กระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม*	*หน่วยงานกำกับดูแล*
3	ผู้แทนจาก Thai-cert	thaicert@ncsa.or.th 02 142 6888	*THAI – CERT*	ดูแลด้านความภัยคุกคามไซเบอร์ระดับประเทศ

9.4 โครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure)

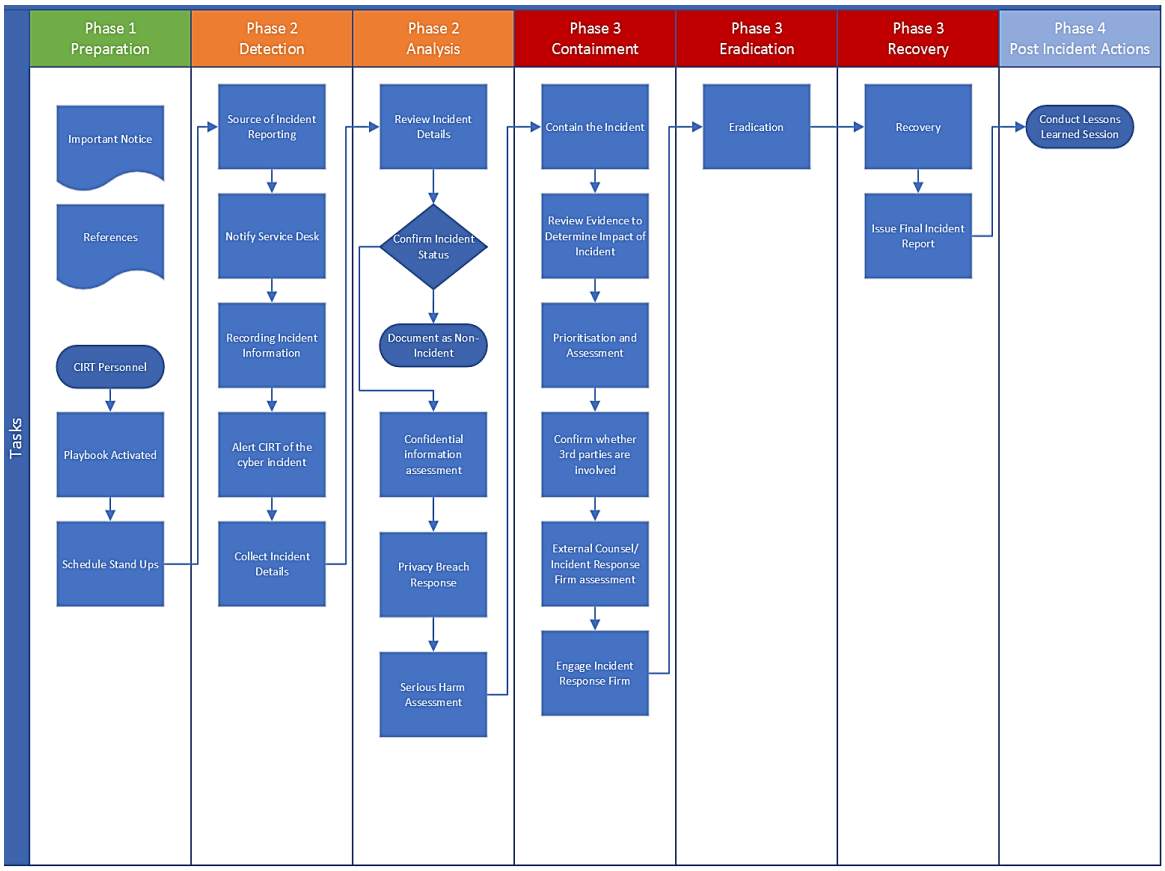
มหาวิทยาลัยราชภัฏสกลนคร และหน่วยงานสำคัญที่เกี่ยวข้องด้านโครงสร้างพื้นฐานทางสารสนเทศ ปฏิบัติตามภาระหน้าที่ในการรายงานภายใต้พระราชบัญญัติ และกฎหมายย่อยใด ๆ ที่ทำขึ้นภายใต้กฎหมายดังกล่าว ตลอดจนภาระหน้าที่ในการรายงานภายใต้กฎหมาย และข้อกำหนดด้านกฎระเบียบที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยมหาวิทยาลัยมีโครงสร้างการรายงานเหตุการณ์ ดังแผนภาพที่ 1



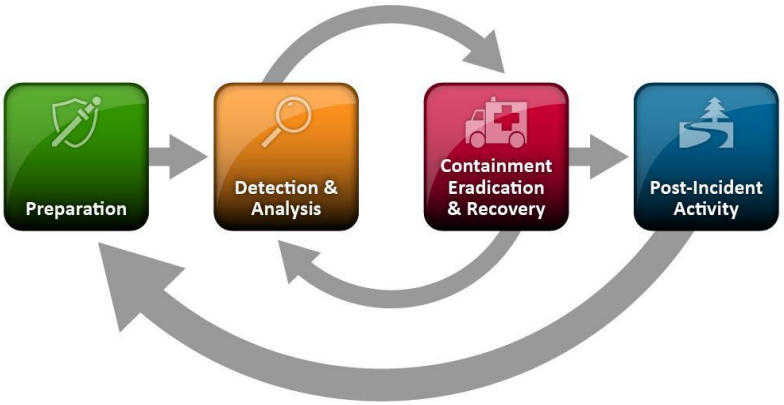
แผนภาพ 1 โครงสร้างการรายงานเหตุการณ์

10. ขั้นตอนการรับมือ

แผนรับมือรับมือเหตุภัยคุกคามทางไซเบอร์ ฉบับนี้ ประกอบด้วยขั้นตอนการรับมือเหตุภัยคุกคามทางไซเบอร์ ตามข้อ 19.1 ในประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564 ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. 2564 และประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ. 2566 รวมถึง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มหาวิทยาลัยราชภัฏสกลนคร ดังนี้



แผนภาพที่ ๒ แผนผังโครงสร้างขั้นตอนการรับมือเหตุภัยคุกคามทางไซเบอร์



แผนภาพที่ ๓ ขั้นเตรียมการและป้องกันการเกิดภัยคุกคามทางไซเบอร์

10.1 ขั้นการเตรียมการ (preparation)

มหาวิทยาลัยราชภัฏสกลนคร มีมาตรการเพื่อเตรียมการและป้องกันการเกิดภัยคุกคามทางไซเบอร์ (preparation) เป็นสิ่งที่จะต้องทำในระยะเริ่มต้น เพื่อเตรียมความพร้อมเมื่อต้องเผชิญเหตุ ได้แก่ การจัดเตรียมข้อมูลให้พร้อม การจัดตั้งและฝึกอบรมบุคลากรหรือทีมงาน การจัดหาเครื่องมือและทรัพยากรต่าง ๆ ที่จำเป็น การตั้งค่าระบบต่าง ๆ ให้ปลอดภัย การจัดทำนโยบาย แผนงาน และกระบวนการที่เกี่ยวข้อง รวมถึง การสร้างเครือข่ายความร่วมมือ โดยดำเนินการดังต่อไปนี้

(1) กำหนดโครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT) รายละเอียดปรากฏตามข้อ 9.2
(2) กำหนดโครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure) รายละเอียดปรากฏตามข้อ 9.4
(3) หลักเกณฑ์และขั้นตอนในการเรียกใช้งาน (Activate) การตอบสนองต่อเหตุการณ์ และ CIRT
(4) จัดเตรียมข้อมูลและอุปกรณ์ รวมถึงช่องทางในการติดต่อสื่อสารที่จำเป็น เช่น ข้อมูลการติดต่อและอุปกรณ์ติดต่อสื่อสารของบุคลากร, กลไกรายงานเหตุการณ์, ห้องประชุม War room เป็นต้น
(5) จัดเตรียมอุปกรณ์, ซอฟต์แวร์ และแหล่งข้อมูลสำหรับวิเคราะห์เหตุภัยคุกคามทางไซเบอร์
(6) ประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน (Risk Assessment)
(7) แผนผังโครงสร้างขั้นตอนการรับมือเหตุภัยคุกคามทางไซเบอร์ (แผนภาพที่ 2)

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

10.2 ขั้นการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (Detection and Analysis)

มหาวิทยาลัยมีการดำเนินการในการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ ซึ่งเป็นสิ่งจำเป็นที่จะช่วยให้สามารถบรรเทาความเสี่ยงที่ยังคงเหลืออยู่ และสามารถแจ้งเตือนได้อย่างทันท่วงทีเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น โดยดำเนินการดังต่อไปนี้

(1) มหาวิทยาลัยดำเนินการจัดเตรียมแนวทางรับมือเมื่อเกิดการโจมตีรูปแบบทั่วไปที่เคยเกิดขึ้นหรืออาจเกิดขึ้นกับหน่วยงาน (Common Attack Vectors/ Common Threat Vectors) โดยการโจมตีรูปแบบทั่วไปที่อาจเกิดขึ้น มีตัวอย่าง ดังนี้

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

(2) มหาวิทยาลัยดำเนินการจัดให้มีกลไกที่สามารถตรวจจับสิ่งบ่งชี้หรือลักษณะเบื้องต้นของการเกิดภัยคุกคามทางไซเบอร์ได้ในเวลาอันเหมาะสม โดยอาจอาศัยข้อมูลจากแหล่งข้อมูลต่าง ๆ เช่น ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เป็นต้น

(3) มหาวิทยาลัยดำเนินการจัดให้มีแนวทางในการวิเคราะห์ผลกระทบและระดับของภัยคุกคามทางไซเบอร์ (Incident Prioritization) เพื่อรับมือกับภัยคุกคามทางไซเบอร์ให้ทันท่วงที โดยพิจารณาปัจจัยต่าง ๆ ที่เกี่ยวข้องเช่น ผลกระทบต่อการทำงานของระบบ (functional impact) ผลกระทบต่อข้อมูล (information impact) และความสามารถในการกู้คืน (recoverability effort[2]) เป็นต้น

(4) มหาวิทยาลัยดำเนินการจัดให้มีบันทึกรายงานสถานการณ์เหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ โดยกำหนดให้มีรายละเอียดตามแบบฟอร์มตัวอย่าง (รายละเอียดปรากฏตามภาคผนวก 2)

(5) มหาวิทยาลัยจัดให้มีการจัดทำบันทึกข้อมูลกิจกรรมเหตุการณ์ความปลอดภัยทางไซเบอร์ (Incident Documentation) โดยหน่วยงานควรบันทึกข้อมูลเกี่ยวกับเหตุการณ์ความปลอดภัยทางไซเบอร์ ทุกขั้นตอนตั้งแต่ตรวจพบเหตุการณ์จนถึงกระบวนการสุดท้าย และข้อมูลดังกล่าวควรระบุรายละเอียดพร้อมเวลาที่เกิดเหตุและระยะเวลาที่ใช้ด้วย บันทึกข้อมูลดังกล่าวที่เกี่ยวข้องกับเหตุการณ์ควรลงวันที่และลงนาม โดยผู้มีหน้าที่จัดการรับมือเหตุการณ์นั้นๆ เพื่อให้มั่นใจได้ว่าเหตุการณ์ความปลอดภัยทางไซเบอร์ที่เกิดขึ้นจะได้รับการจัดการแก้ไขภายในระยะเวลาที่เหมาะสมโดยอาจกำหนดให้มีรายละเอียดตามแบบฟอร์มตัวอย่าง (รายละเอียดปรากฏตามภาคผนวก 3)

(6) มหาวิทยาลัยราชภัฏสกลนคร และหน่วยงานสำคัญที่เกี่ยวข้องด้านโครงสร้างพื้นฐานทางสารสนเทศจะต้องมีการรายงานภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับบริการของโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ให้ผู้ที่เกี่ยวข้องทราบตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ.2566 ดังนี้

(ก) กรณีมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นกับมหาวิทยาลัยและหน่วยงานสำคัญที่เกี่ยวข้องด้านโครงสร้างพื้นฐานทางสารสนเทศ ตาม ข้อ 4 แห่งประกาศฯ ฉบับดังกล่าว ให้ใช้แบบฟอร์ม ก 1 โดยใช้แบบฟอร์มการรายงานตามกฎหมาย (รายละเอียดปรากฏตามภาคผนวก 4)

(ข) กรณีมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญต่อระบบของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ กับมหาวิทยาลัยและหน่วยงานสำคัญที่เกี่ยวข้องด้านโครงสร้างพื้นฐานทางสารสนเทศ ตาม ข้อ 5 แห่งประกาศฯ ฉบับดังกล่าว ให้ใช้แบบฟอร์ม ก 2 รายงานไปยังสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ภายในระยะเวลา 24 ชั่วโมง โดยใช้แบบฟอร์มการรายงานตามกฎหมาย (รายละเอียดปรากฏตามภาคผนวก 4)

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

(ค) มหาวิทยาลัยกำกับดูแล จัดทำและส่งรายงานสรุปจำนวนเหตุภัยคุกคามทางไซเบอร์ทั้งหมดที่ได้เกิดขึ้นกับข้อมูลหรือระบบสารสนเทศของหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ภายใต้การควบคุมหรือกำกับดูแลในแต่ละปี ภายในวันที่ ๓๑ มกราคม ของปีถัดไป ให้แก่สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ โดยให้แยกสถิติหมวดหมู่ตามแบบที่กำหนดในเอกสาร ก ๓ โดยใช้แบบฟอร์มการรายงานตามกฎหมาย (รายละเอียดปรากฏตามภาคผนวก ๔)

นอกจากนี้ มหาวิทยาลัยจะดำเนินการตามเอกสารแนบท้าย ๒ ตารางที่ ๒.๒ ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ เพิ่มเติม

10.3 การกำหนดวิธีการที่จะใช้ในการตรวจจับ incident

การตรวจจับ incident จะขึ้นอยู่กับระบบงานที่ใช้อยู่ รูปแบบของความพยายามโจมตี และกลไกในการปกป้องระบบ เพราะระบบการป้องกันจะแจ้งเตือน (Alert) หรือเก็บบันทึกข้อมูล (Log) เพื่อใช้ในการวิเคราะห์ หาความผิดปกติและมีการปรับ Fine Tune เพื่อให้มีความเหมาะสมกับสภาพการใช้งานของระบบ ลักษณะของข้อมูลแจ้งเตือนที่ใช้ในการตรวจจับแบ่งได้เป็น 2 ประเภท

- Precursor เป็นข้อมูลบ่งบอกว่า incident จะเกิดขึ้นในอนาคต
- Indicator เป็นข้อมูลบ่งบอกว่า incident ได้เคยเกิดขึ้นหรือกำลังเกิดขึ้นอยู่

อุปกรณ์ที่ใช้เพื่อการป้องกันและตรวจจับต้องพิจารณาตามความเหมาะสมกับระบบที่ต้องการป้องกัน และต้องทำการปรับ Fine Tune เพื่อให้มีความเหมาะสมกับสภาพการใช้งานของระบบนั้น ๆ ซึ่งข้อมูลการ แจ้งเตือนเพื่อตรวจจับการบุกรุกระบบคอมพิวเตอร์และเครือข่ายมีดังนี้

10.3.1 ประเภท Alert

1) IPS ระบบที่ทำหน้าที่ตรวจจับและป้องกันการโจมตีในระบบเครือข่าย มีการแจ้งเตือน เมื่อพบสิ่งที่ตรงกับวิธีการโจมตีที่ระบบรู้จัก

2) SIEM ระบบตรวจจับความผิดปกติโดยใช้ข้อมูล Log จากระบบอื่น ๆ เพื่อนำมาวิเคราะห์ โดยต้องตั้งค่า Rule set โดยผู้เชี่ยวชาญ และเหมาะสมกับสภาพแวดล้อมที่เชื่อมต่ออยู่กับ SIEM (จะจัดหาในปีงบประมาณ 2571)

3) Anti-Malware ทำหน้าที่ตรวจจับโปรแกรมประสงค์ร้าย ทำงานทั้งในระดับเครือข่าย และ Host การตรวจเจอ Malware ในระบบเป็นข้อบ่งชี้ได้ทั้งที่กำลังพยายามโจมตีและการโจมตีได้สำเร็จแล้ว

4) Third-Party บริการสอดส่องดูแลความผิดปกติที่เกิดขึ้นกับระบบ หรือระบบของหน่วยงานถูกนำไปโจมตีระบบอื่น ๆ ภายนอกองค์กรซึ่งบ่งบอกได้ว่าระบบภายในหน่วยงานได้ถูกยึดครองโดยผู้ไม่ประสงค์ดีและนำไปใช้สร้างความเสียหาย

10.3.2 ประเภท Log

1) Operating System and Application Log ข้อมูลจาก Log ของ OS และ Application ที่ประกอบไปด้วยการบันทึกเหตุการณ์หลายประเภท สามารถถูกใช้ในการตรวจจับภัยคุกคามบางอย่างได้ขึ้นอยู่กับ ประเภทของ Log และ Rule set ที่ใช้ในการวิเคราะห์

2) Network Device Log อุปกรณ์เครือข่ายที่มีการบันทึกข้อมูลที่ผ่านเข้าออกเครือข่าย สามารถถูกใช้ในการตรวจจับเหตุการณ์ภัยคุกคามบางอย่างได้ขึ้นอยู่กับประเภทของ Log และ Rule set ที่ใช้ในการ วิเคราะห์

10.3.3 ข้อมูลจากแหล่งสาธารณะข้อมูลช่องโหว่และวิธีการโจมตีระบบรูปแบบใหม่สามารถถูกใช้เป็น ข้อบ่งชี้ภัยคุกคามได้

10.3.4 บุคคลที่ทำหน้าที่แจ้งเตือนบุคคลภายในองค์กร บุคลากรทุกตำแหน่งสามารถเข้ารับการฝึกฝน เพื่อช่วยสอดส่องดูแล

10.4 การวิเคราะห์เหตุภัยคุกคามหรือความผิดปกติเมื่อได้รับแจ้ง

การวิเคราะห์ภัยคุกคามเพื่อให้การดำเนินการต่อไปสามารถทำได้เร็วและถูกต้อง ใช้การวิเคราะห์ความผิดปกติเมื่อได้รับแจ้งดังนี้

10.4.2 Clock Synchronization ดำเนินการให้อุปกรณ์ทุกชิ้นบนเครือข่ายได้รับการปรับเทียบเวลา (Synchronize) ให้ตรงกันอยู่เสมอ เพื่อให้การเชื่อมโยงเหตุการณ์ (Event Correlation) สามารถทำได้อย่างมีประสิทธิภาพ

10.4.3 Sniff and Analyze Network Data ดำเนินการดักจับและวิเคราะห์ข้อมูลทางเครือข่ายเพื่อตรวจหาความผิดปกติหรือภัยคุกคาม

10.4.4 Seek Assistance ในกรณีที่ทีมตอบสนองไม่สามารถดำเนินการวิเคราะห์เหตุการณ์ (Incident) เพื่อหาสาเหตุที่แท้จริงหรือกำจัดผู้บุกรุกออกจากระบบได้ มหาวิทยาลัยจะพิจารณาขอคำแนะนำหรือความช่วยเหลือจากหน่วยงานภายนอกที่มีความเชี่ยวชาญ เช่น ทีมตอบสนองต่อเหตุการณ์ฉุกเฉินทางคอมพิวเตอร์ (Computer Emergency Response Team: CERT) ต่าง ๆ

10.4.5 การวิเคราะห์ผลกระทบและการจัดลำดับความสำคัญของ Incident

การวิเคราะห์ผลกระทบและความรุนแรง เพื่อจัดลำดับความสำคัญของ Incident และช่วยในการตัดสินใจ เชิงกลยุทธ์เพื่อดำเนินการรับมือและตอบสนองต่อภัยคุกคามที่เกิดขึ้นได้อย่างเหมาะสมภายใต้ทรัพยากรที่มีอยู่ อย่างจำกัด และลดผลกระทบทางธุรกิจให้น้อยลงที่สุด การกำหนดแนวทางในการวิเคราะห์ผลกระทบและการจัดลำดับความสำคัญของ Incident โดยอย่างน้อยควรครอบคลุมในด้านผลกระทบต่อการให้บริการ (Functional Impact) ผลกระทบต่อข้อมูล (Information Impact) และความสามารถในการฟื้นฟูระบบ (Recoverability)

ก) ผลกระทบต่อการให้บริการ (Functional Impact) ผลกระทบต่อการให้บริการ และการ ดำเนินงานของหน่วยงานที่เกิดภัยคุกคาม พิจารณาผลกระทบที่เกิดขึ้นทั้งในปัจจุบัน และผลกระทบที่มีโอกาสเกิดขึ้นหากเหตุการณ์ภัยคุกคามยังไม่ถูกควบคุมโดยทันทีซึ่งรวมถึงผลกระทบทางด้านการปฏิบัติงานของระบบการให้บริการต่าง ๆ ซึ่งส่งผลโดยตรงต่อการดำเนินธุรกิจ (Impact to Business) ที่ทำให้เกิดความขัดข้องหรือเสียหาย ต่อธุรกิจ ซึ่งหากไม่ได้รับการแก้ไขโดยเร็วอาจจะมีผลเสียมากยิ่งขึ้น โดยระดับของ Severity level มีดังนี้

Severity level

- Low ไม่มีผลกระทบในการให้บริการหรือดำเนินงานตามปกติ
- Medium มีผลน้อยมากต่อกระบวนการทำงานหลัก ทำให้ช้าลงบ้างแต่ผลที่ได้ยังครบถ้วนสมบูรณ์
- High ไม่สามารถให้บริการที่ครบถ้วนสมบูรณ์กับผู้ใช้งานบางกลุ่ม ทั้งภายใน และภายนอก
- Critical/Extreme ไม่สามารถให้บริการกับผู้ใดได้อีกต่อไป เป็นการหยุดชะงักโดยสมบูรณ์

ข) ผลกระทบต่อข้อมูล (Information Impact) ผลกระทบต่อข้อมูล ควรพิจารณา ๓ ด้าน ได้แก่ ด้านการรักษาความลับ (Confidentiality) ด้านการรักษาความครบถ้วน (Integrity) และด้านการรักษาสภาพพร้อม ใช้ (Availability) รวมทั้งควรพิจารณาว่าเหตุการณ์ภัยคุกคามส่งผลต่อการดำเนินงานโดยรวมที่จะส่งผลต่อข้อมูล สำคัญ (Sensitive Information)อย่างไร เช่น ข้อมูลถูกทำลาย หรือสูญหาย หรือรั่วไหล หรือการแก้ไขโดยไม่ได้รับ อนุญาตเป็นต้น โดยระดับของ Functional Impact มีดังนี้

- None ไม่มีข้อมูลรั่วไหล ถูกเปลี่ยนแปลง ทำลาย หรือเข้าถึง โดยที่ไม่ได้รับอนุญาต
- Privacy Breach ข้อมูลที่ใช้ระบุตัวบุคคล (Personal Identifiable Information; PII) รั่วไหลหรือถูกเข้าถึงโดยไม่ได้รับอนุญาต
- Proprietary Breach ข้อมูลความลับที่ใช้ในการดำเนินธุรกิจ รั่วไหล หรือถูกเข้าถึงโดยไม่ได้ รับอนุญาต
- Integrity Loss ข้อมูลที่เป็น Privacy และ Propriety ถูกเปลี่ยนแปลง หรือทำลายโดยไม่ได้ รับอนุญาต

ค) ความสามารถในการฟื้นฟูระบบ (Recoverability) ความสามารถในการฟื้นฟูระบบควรพิจารณาจากระยะเวลาและทรัพยากรที่ต้องใช้ในการฟื้นฟูระบบจากเหตุภัยคุกคาม ซึ่งความรุนแรงของเหตุภัยคุกคามและประเภทของทรัพย์สินสารสนเทศเช่น ระบบ และข้อมูล เป็นต้น ที่ได้รับผลกระทบจะเป็นส่วนสำคัญในการพิจารณาความสามารถ หรือความยากง่ายในการฟื้นฟูระบบ รวมทั้งทรัพยากรที่จำเป็นต้องใช้โดยระดับของ Recoverability Effort มีดังนี้

- Regular เวลาในการกู้คืนสามารถคาดการณ์ได้ โดยใช้ทรัพยากรที่มี
- Supplemented เวลาในการกู้คืนสามารถคาดการณ์ได้ แต่ต้องมีการจัดหาทรัพยากรเพิ่ม
- Extended เวลาในการกู้คืนไม่สามารถคาดการณ์ได้ ต้องใช้ทรัพยากรและความช่วยเหลือ จากภายนอก ๙
- Not Recoverable การกู้คืนไม่สามารถทำได้ ใช้กับสถานการณ์ที่ข้อมูลได้รั่วไหลสู่สาธารณะ แล้ว เป็นต้น ให้ใช้วิธีการติดตามและจำกัดการแพร่กระจายรวมถึงการเยียวยาผลกระทบ

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

มหาวิทยาลัยจะดำเนินการเพื่อระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคาม ทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ โดยพิจารณาตามระดับความรุนแรงของภัยคุกคามทางไซเบอร์ จนกระทั่งสามารถกู้คืนทรัพย์สินสำคัญทางสารสนเทศให้กลับมาดำเนินงานหรือให้บริการได้ตามปกติ ซึ่งการดำเนินการในขั้นตอนนี้อาจจะต้องกระทำควบคู่ไปกับการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ ที่อาจมีการลุกลามหรือทวีความรุนแรงมากขึ้นเพื่อให้การระงับและการปราบปรามภัยคุกคามทางไซเบอร์ ตลอดจนการฟื้นฟูระบบงานที่ได้รับผลกระทบจากการเกิดภัยคุกคามทางไซเบอร์ สอดคล้องกับสถานการณ์ที่เปลี่ยนแปลงไป โดยดำเนินการดังต่อไปนี้

(1) จำกัดขอบเขต (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

(2) ดำเนินการเรียกใช้งานกระบวนการกู้คืน (Recovery Process)

(3) ดำเนินการสอบสวน (Investigate) ถึงสาเหตุและผลกระทบของเหตุการณ์ที่เกิดขึ้น

(4) เก็บรักษาหลักฐาน (Preservation of Evidence) โดยดำเนินการก่อนเริ่มกระบวนการกู้คืน ซึ่งรวมถึงการได้มาของบันทึกการยึดหลักฐานคอมพิวเตอร์ที่ได้มา หรืออุปกรณ์อื่น ๆ ที่เกี่ยวข้องเพื่อสนับสนุนการสอบสวนต่อไป

(5) ดำเนินการตามระเบียบวิธีการมีส่วนร่วม (Engagement Protocols) กับบุคคลภายนอก หรือแนวปฏิบัติการบริหารจัดการบุคคลภายนอก โดยมีรายละเอียดการติดต่อที่จำเป็น อาทิ ผู้ให้บริการด้านนิติวิทยาศาสตร์/การกู้คืนและการบังคับใช้กฎหมายเพื่อดำเนินคดี

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

10.5.1 วิธีการควบคุมความเสียหาย คือการตัดสินใจเลือกใช้วิธีการที่เหมาะสม ดังนี้

- ปิดระบบ (Shut Down)
- ตัดการเชื่อมต่อทางเครือข่ายทั้งหมด (Network disconnection) โดยอาจพิจารณายกเว้นการเชื่อมต่อสำหรับ Endpoint Detection & Response Agent (กระบวนการตรวจสอบและตรวจจับกิจกรรมหรือเหตุการณ์ ที่น่าสงสัยใด ๆ ที่เกิดขึ้นที่ปลายทางแบบเรียลไทม์)
- หยุดการทำงานของฟังก์ชันที่เกี่ยวข้อง (Disabling Certain Functions)
- ดำเนินการ Redirect Network Traffic และ/หรือความสนใจของผู้บุกรุกไปยัง Blackhole/ Sandbox/ Honeypot

ทั้งนี้ การตัดสินใจเลือกใช้วิธีการควบคุมความเสียหายจะขึ้นอยู่กับลักษณะสถานการณ์ที่กำลังเผชิญ ประเภทของภัยคุกคาม ระบบงานหรือบริการที่ได้รับผลกระทบ ระยะเวลาและทรัพยากรที่จำเป็นต่อการควบคุม ความเสียหาย

10.5.2 การจัดเก็บและดูแลรักษาหลักฐานทางดิจิทัล

วัตถุประสงค์หลักของการจัดเก็บหลักฐาน คือเพื่อให้การแก้ไข Incident ส่งผลกระทบต่อการดำเนินงานของมหาวิทยาลัยให้น้อย ที่สุด (Minimizing impact to the business) นอกจากนี้ หลักฐานอาจมีความจำเป็นที่จะต้องใช้ในการดำเนินการ ตามขั้นตอนทางกฎหมาย โดยการดำเนินการจัดเก็บหลักฐานทางดิจิทัลสามารถดำเนินการโดยพิจารณา ตามหลักการดังต่อไปนี้

- ดำเนินการเป็นไปตามขั้นตอนที่กำหนดไว้ในกฎหมายข้อบังคับที่เกี่ยวกับหลักฐานดิจิทัล เพื่อให้สามารถนำไปใช้ ได้ในชั้นศาล
- หลักฐานมีบันทึกการเข้าถึงและการกระทำการใด ๆ ต่อหลักฐานตลอดเวลาอย่างรัดกุม
- การเปลี่ยนตัวผู้ดูแลจำเป็นต้องมีการจัดทำบันทึกห่วงโซ่หลักฐาน (Chain of Custody) (ภาคผนวก) รายละเอียดเกี่ยวกับหลักฐาน ควรประกอบด้วยข้อมูลอย่างน้อยดังต่อไปนี้

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

2) ชื่อ ตำแหน่ง และช่องทางการติดต่อผู้จัดเก็บและรักษาหลักฐานระหว่างการรับมือ Incident

3) สถานที่จัดเก็บหลักฐาน

10.6 การกำจัดสาเหตุและการกู้คืนระบบให้กลับมาทำงานปกติ

เมื่อมีการควบคุมความเสียหาย และมีการดำเนินการจัดเก็บหลักฐานข้อมูลเพิ่มเติมเรียบร้อยแล้ว จะต้องนำข้อมูลทั้งหมดมาวิเคราะห์ตามหลักการที่ได้กล่าวไว้ใน “ขั้นตอนที่ 2 เรื่องการตรวจจับและวิเคราะห์ (Detection & Analysis)” จนกว่าจะสามารถกำจัดสาเหตุที่ทำให้เกิด Incident และช่องทางที่ผู้บุกรุกได้สร้างไว้เพื่อเข้ามา ในระบบทั้งหมดได้อย่างครบถ้วน ~~ซึ่ง~~โดยการกำจัดสาเหตุที่ทำให้เกิด Incident และผลกระทบ มีแนวทางดังต่อไปนี้

- การปิดช่องโหว่ของระบบ- การยกเลิก User Account ที่ผู้บุกรุกใช้เข้าสู่ระบบ
- การแจ้งให้ผู้ใช้งานเปลี่ยนรหัสผ่าน
- การลบโปรแกรมประเภท Backdoor ออกจากระบบ
- การใช้ข้อมูล Indicator of Compromise (Ioc) ในการสแกนหา Malware หรือร่องรอยอื่น ๆ ในระบบที่ยังหลงเหลือของผู้บุกรุกเพื่อดำเนินการกำจัดให้ออกจากระบบทั้งหมด

ทั้งนี้ หลังจากดำเนินการควบคุมความเสียหาย และกำจัดสาเหตุของภัยคุกคามเสร็จเรียบร้อยแล้ว จะเข้าสู่กระบวนการฟื้นฟูระบบให้เข้าสู่สภาวะการทำงานปกติโดยในขั้นตอนนี้สิ่งที่มีความสำคัญเป็นอย่างยิ่ง และควรเตรียมการล่วงหน้าในเรื่องดังต่อไปนี้

- การ Restore Operating System หรือ Application Software ต่าง ๆ จาก Master Image ที่ปลอดภัย
- การ Restore ข้อมูลกลับเข้าระบบจาก Back Up Storage

การดำเนินการตามขั้นตอนข้างต้นจะช่วยให้ระบบสามารถกลับมาทำงานได้ตามปกติ และมีความปลอดภัยจากภัยคุกคามที่เคยเกิดขึ้น

10.7 ขั้นการดำเนินการภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ (post-incident activity)

มหาวิทยาลัยกำหนดขั้นตอน วิธี ปฏิบัติ และกำหนดนโยบายภายในที่เกี่ยวข้องเพื่อให้มีแนวทางที่ชัดเจน ซึ่งโดยการปฏิบัติตามมาตรการดังกล่าว จะช่วยให้หน่วยงานสามารถเรียนรู้จากเหตุภัยคุกคามทางไซเบอร์ที่ผ่านมา และสามารถหาแนวทางเพื่อแก้ไข จุดบกพร่องและพัฒนาแนวทางรับมือกับภัยคุกคามทางไซเบอร์ต่อไป ในอนาคต นอกจากนี้หน่วยงานต้องเก็บ รักษาข้อมูลและพยานหลักฐานที่จำเป็น เพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์ หรือใช้ในกรณีที่ต้องการร้องทุกข์หรือดำเนินคดี เนื่องจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้นนั้น อาจเข้าลักษณะเป็นความผิดตามประมวล กฎหมายอาญา หรือพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2560 และที่แก้ไข เพิ่มเติม (ถ้ามี) หรือกฎหมายอื่น ๆ ที่เกี่ยวข้อง โดยประกอบด้วยการดำเนินการในเรื่องดังต่อไปนี้

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

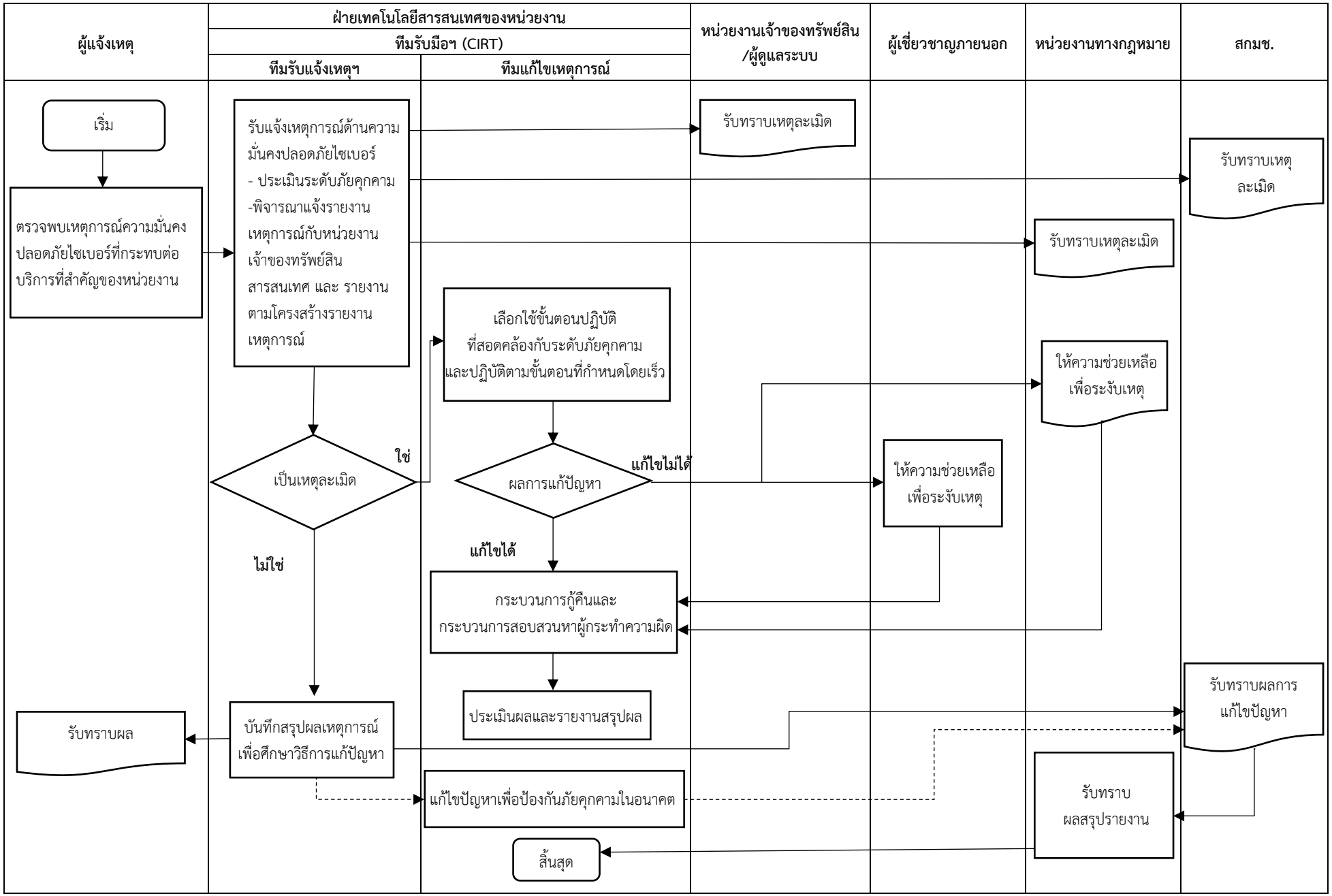
นอกจากนี้ หน่วยงานควรพิจารณาดำเนินการตามเอกสารแนบท้าย 2 ตารางที่ 2.4 ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. 2564 เพิ่มเติม

10.8 การจัดทำรายการตรวจสอบการจัดการเหตุการณ์ (Incident Handling Checklist)

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

การจัดทำรายการตรวจสอบนี้จะช่วยให้การจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์เป็นไปอย่างมีประสิทธิภาพและเป็นระบบ

ภาคผนวก 1 แผนผังโครงสร้างขั้นตอนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response)



ภาคผนวก 2

บันทึกรายงานสถานการณ์เหตุการณ์ความมั่นคงปลอดภัยไซเบอร์

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

ภาคผนวก 3

บันทึกข้อมูลกิจกรรมเหตุการณ์ความปลอดภัยทางไซเบอร์ (Incident Documentation)

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

ภาคผนวก 4

เอกสาร ก 1 ข้อมูลที่ต้องแจ้ง

ข้อมูลการประสานงานและผลการตรวจสอบภัยคุกคามเบื้องต้น

1. ข้อมูลการประสานงาน

ชื่อหน่วยงานที่รับผิดชอบติดตามเหตุภัยคุกคาม

วันที่และเวลาที่แจ้ง

2. ด้านภารกิจหรือบริการของหน่วยงาน และ ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม

ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม

ที่อยู่ของหน่วยงานหรือหน่วยงานย่อยที่เกิดเหตุภัยคุกคาม

3. ข้อมูลการติดต่อสำหรับการประสานงานเหตุภัยคุกคาม

ชื่อ-นามสกุล ตำแหน่งงาน

ชื่อหน่วยงาน อีเมล

โทรศัพท์ (ที่ทำงาน / มือถือ)

4. ความต่อเนื่องของเหตุภัยคุกคาม

☐ เหตุภัยคุกคามใหม่ ☐ การรายงานข้อมูลต่อเนื่องจากเหตุภัยคุกคามเดิม

5. ลักษณะภัยคุกคามทางไซเบอร์

ระบบที่ได้รับผลกระทบมีความสำคัญต่อพันธกิจหลักของหน่วยงานหรือไม่

เหตุการณ์ที่เกิดขึ้นเกิดจากภัยคุกคามทางไซเบอร์[3] ในระดับใด (มาตรา 60)

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

☐ ยังไม่สามารถระบุได้

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)

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

เอกสาร ก 2 แบบรายงานภัยคุกคามทางไซเบอร์

ส่วนที่ 1
หมวด ก. ข้อมูลการประสานงานและผลการตรวจสอบภัยคุกคามเบื้องต้น
หมายเลขอ้างอิง (สำหรับเจ้าหน้าที่ สกมช.): โปรดระบุ **หน่วยงานที่รับผิดชอบติดตามเหตุภัยคุกคาม (ถ้ามี):** โปรดระบุ **วันที่:** เลือกวันที่ **เวลา:** โปรดระบุ
ก 1. ด้านภารกิจหรือบริการของหน่วยงาน และ ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม: โปรดระบุ ที่อยู่ของหน่วยงานหรือหน่วยงานย่อยที่เกิดเหตุภัยคุกคาม: โปรดระบุ
ก 2. ข้อมูลการติดต่อสำหรับการประสานงานเหตุภัยคุกคาม ชื่อ-นามสกุล: โปรดระบุ ตำแหน่งงาน: โปรดระบุ ชื่อหน่วยงาน: โปรดระบุ อีเมล: โปรดระบุ โทรศัพท์ (ที่ทำงาน / มือถือ) : โปรดระบุ
ก 3. ความต่อเนื่องของเหตุภัยคุกคาม ☐ เหตุภัยคุกคามใหม่ ☐ การรายงานข้อมูลต่อเนื่องจากเหตุภัยคุกคามเดิม
ก 4. ลักษณะภัยคุกคามทางไซเบอร์ ระบบที่ได้รับผลกระทบมีความสำคัญต่อพันธกิจหลักของหน่วยงาน ☐ ใช่ ☐ ไม่ใช่ เหตุการณ์ที่เกิดขึ้นเกิดจากภัยคุกคามทางไซเบอร์[4] ในระดับใด (มาตรา 60) ☐ ไม่ร้ายแรง ☐ ร้ายแรง ☐ วิกฤต (ก) ☐ วิกฤต (ข) ☐ ยังไม่สามารถระบุได้

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

หมวด ข. ข้อมูลการตรวจพบภัยคุกคามไซเบอร์

ข 1. วัน เวลา ที่เกิดเหตุภัยคุกคาม

วันที่ : เลือกวันที่ เวลา : โปรดระบุ

วัน เวลา ที่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศทราบเหตุภัยคุกคาม

วันที่ : เลือกวันที่ เวลา : โปรดระบุ

ข 2. วัน เวลา ที่แจ้งเหตุภัยคุกคามให้หน่วยงานควบคุมหรือกำกับดูแลทราบ

☐ ยังไม่ได้แจ้ง ☐ แจ้งแล้ว _____

ข 3. หมวดหมู่ของภัยคุกคาม (เลือกได้มากกว่า 1 รายการ)

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

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

ข 4. 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
ค 1. สถานการณ์หรือการแก้ไขเหตุภัยคุกคาม (เลือกได้มากกว่า 1 รายการ) ☐ เพิ่งพบเหตุการณ์ ☐ อยู่ในขั้นตอนการขอความช่วยเหลือ ☐ อยู่ในขั้นตอนการสอบสวน ☐ กำลังลุกลาม ☐ อยู่ในขั้นตอนการระงับภัย ☐ สามารถระงับภัยได้แล้ว ☐ รายงานปิดเหตุการณ์ภัยคุกคามแล้ว ☐ อื่น ๆ: โปรดระบุ
ค 2. สิ่งที่ได้ดำเนินการหรือได้แก้ไขไปแล้ว ☐ ยังไม่ได้ดำเนินการแก้ไขใด ๆ ☐ ยกเลิกการเชื่อมต่อระบบออกจากเครือข่ายแล้ว ☐ ตรวจสอบข้อมูลจราจร (Log) แล้ว ☐ ตรวจสอบโปรแกรม (แฟ้ม binaries/.exe) แล้ว ☐ กู้คืนกลับมาด้วยระบบหรือข้อมูลสำรองที่ตรวจสอบความถูกต้องแล้ว ☐ รายละเอียดการแก้ไขภัยคุกคามที่เกิดขึ้นเพิ่มเติม: โปรดระบุ
ค 3. รายละเอียดการรับมือภัยคุกคามอื่น ๆ (ถ้ามี) โปรดระบุ

ส่วนที่ 2

หมวด ง : รายละเอียดภัยคุกคาม

ง 1. ข้อมูลการตรวจจับและการวิเคราะห์

ง 1.1 <u>วัน เวลา ที่ผู้โจมตีได้เริ่มต้นเข้าถึงระบบ</u> (System Access)

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

ง 1.2 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

ง 1.3 รายละเอียดผลกระทบจากเหตุภัยคุกคาม (ระบุผลกระทบที่มีเกิดขึ้นต่อ ระบบ คน หรือข้อมูล)

จำนวนระบบ บริการ หรือสินทรัพย์ที่เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่ได้รับผลกระทบ (โดยประมาณ): โปรดระบุ

ทรัพย์สินที่สำคัญอื่น ๆ ที่อาจได้รับผลกระทบ: โปรดระบุ

จำนวนผู้ได้รับผลกระทบ (โดยประมาณ): โปรดระบุ

มูลค่าความเสียหาย (โดยประมาณ): โปรดระบุ

ในกรณีที่ข้อมูลที่ระบุตัวบุคคลได้รั่วไหล (หรือถูกขโมย):

จำนวนบุคคลที่เป็นเจ้าของข้อมูล : โปรดระบุ

ชนิดของข้อมูล (เลือกทุกข้อที่ใช่):

☐ ข้อมูลไบโอเมตริกซ์ ☐ ข้อมูลการติดต่อ

☐ ข้อมูลการเงิน ☐ ข้อมูลบุคลากรของรัฐ

☐ หมายเลขบัตรประชาชน ☐ ข้อมูลการติดต่อกับหน่วยงานต่าง ๆ

☐ ข้อมูลทางการแพทย์

☐ อื่น ๆ : โปรดระบุ

จำนวนข้อมูล (Record) ที่ได้รับผลกระทบ: โปรดระบุ

ผลกระทบอื่น ๆ ที่เกิดขึ้น: โปรดระบุ

ง 1.4 <u>รายละเอียดของระบบ หรือข้อมูลที่ได้รับผลกระทบ (Information of Affected System)</u>

หมายเลข CVE: โปรดระบุ

ช่องโหว่ที่ถูกใช้จู่โจม: โปรดระบุ

การใช้ระบบหรือเครื่องที่ได้รับผลกระทบเป็นฐานเพื่อจู่โจมขยายผลไปยังระบบหรือเครื่องอื่น: โปรดระบุ

อาการหรือสิ่งผิดปกติ (เลือกได้มากกว่า 1 รายการ)

☐ ระบบล่ม ☐ รายการข้อมูลจราจรทางคอมพิวเตอร์ที่ผิดปกติ

☐ บัญชีผู้ใช้ถูกสร้างขึ้นมาใหม่โดยไม่ทราบสาเหตุ หรือ บัญชีผู้ใช้มีความผิดปกติ

☐ การจู่โจมด้วยวิศวกรรมสังคม (Social Engineering) ทั้งที่สำเร็จและไม่สำเร็จ

☐ ประสิทธิภาพของระบบด้อยลง (ทั้งที่รู้ว่าเป็นเพราะเหตุภัยคุกคามและที่ไม่รู้สาเหตุ)

☐ การเปลี่ยนแปลงใน DNS หรือ กฎของ Router หรือกฎไฟร์วอลล์ โดยไม่ทราบสาเหตุ

☐ การยกระดับสิทธิ์การเข้าถึงระบบโดยไม่ทราบสาเหตุ

☐ การตรวจพบการทำงานของโปรแกรมหรืออุปกรณ์ Sniffer เพื่อจับการรับส่งข้อมูลภายในเครือข่าย

☐ การเข้าใช้งานครั้งสุดท้ายของผู้ใช้ที่ไม่สอดคล้องกับการใช้งานครั้งสุดท้ายที่เกิดขึ้นจริง

☐ การแจ้งเตือนจากเครื่องมือตรวจจับการบุกรุก

☐ การเข้ามาลาดตระเวน (Probing) หรือการเรียกดู (Browsing) ที่น่าสงสัย

☐ รูปแบบการใช้งานที่ผิดปกติ ☐ การเปลี่ยนแปลงขนาดไฟล์ไปจากเดิมแบบผิดปกติ

☐ ความพยายามที่จะเขียนไฟล์ของระบบ ☐ การเปลี่ยนแปลงวันที่ของไฟล์ไปจากเดิมแบบผิดปกติ

☐ การแก้ไขหรือลบข้อมูลที่ผิดปกติ ☐ การจู่โจมให้เกิดการปฏิเสธการให้บริการ (DOS, DDOS)

☐ ไฟล์ใหม่ถูกสร้างขึ้นโดยไม่ทราบสาเหตุ ☐ การใช้งานหรือมีกิจกรรมที่เกิดในเวลาที่ผิดปกติ

☐ การแก้ไขหน้าเว็บ ☐ การสร้างแฟ้มข้อมูล setuid หรือ setgid ใหม่ที่ผิดปกติเกิดขึ้น

☐ การเปลี่ยนแปลงในไดเรกทอรีและแฟ้มข้อมูลของระบบปฏิบัติการที่ผิดปกติ

☐ การตรวจพบโปรแกรมเจาะระบบ (Crack utility)

☐ สิ่งที่ผิดปกติไปจากเดิมอื่น ๆ: โปรดระบุ

ง 1.5 รายละเอียดของเหตุภัยคุกคามตามลำดับเวลา ตั้งแต่การจู่โจมครั้งแรก จนถึงปัจจุบัน (เช่น ลำดับของการจู่โจม, Attack vector, เทคนิคหรือเครื่องมือที่ผู้จู่โจมใช้ ฯลฯ)

โปรดระบุ

ง 1.6 รายละเอียดอื่น ๆ ที่พบเกี่ยวข้องกับเหตุภัยคุกคาม: โปรดระบุ

ง 2. ข้อมูลการระงับ ปราบปราม และฟื้นฟู

ง 2.1 รายละเอียดการดำเนินการเพื่อแก้ไขเหตุภัยคุกคาม: โปรดระบุ

ง 2.2 การคาดการณ์ความสามารถฟื้นฟู

โปรดระบุรายละเอียดการฟื้นฟู ทรัพยากรที่ต้องใช้และที่ต้องการเพิ่ม และประมาณระยะเวลาการฟื้นฟู

ง 3. ข้อมูลกิจกรรมภายหลังการแก้ปัญหา (ถ้ามี)

ง 3.1 วัน เวลา ที่เหตุภัยคุกคามสิ้นสุด วันที่: เลือกวันที่ **เวลา:** โปรดระบุ

ง 3.2 การดำเนินการเพื่อป้องกันเหตุภัยคุกคามที่คล้ายคลึงกัน: โปรดระบุ

ง 3.3 บทเรียนที่ได้จากเหตุภัยคุกคาม: โปรดระบุ

เอกสาร ก 3 แบบรายงานสรุปภัยคุกคามทางไซเบอร์ในหนึ่งรอบปี

ข้อ 1 สถิติรายปีจำแนกตามหมวดหมู่ของภัยคุกคามทางไซเบอร์[5]

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

ข้อ 2 สถิติรายปีจำแนกตามทรัพย์สินที่ได้รับผลกระทบ

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

ข้อ 3 สถิติรายปีจำแนกตามระดับภัยคุกคามทางไซเบอร์[6]

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

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

[6] ระดับภัยคุกคามทางไซเบอร์ตามมาตรา 60 แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562

ภาคผนวก 5

ตัวอย่าง : รายการตรวจสอบการจัดการเหตุการณ์ (Incident Handling Checklist)

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

แหล่งที่มา

- ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ.2564

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

- ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ.2566

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

- ACSC Cyber Incident Response Plan Guidance

ประวัติการแก้ไขเอกสาร

เวอร์ชั่น	รายละเอียดการแก้ไข	วันที่จัดทำ
21-01-68	เอกสารเวอร์ชั่นตั้งต้น	21 มกราคม 2568

การอนุมัติเอกสาร

ผู้จัดทำเอกสาร	
ชื่อ นายกิตติภูมิ คำศรี **ตำแหน่ง** หัวหน้างานพัฒนาระบบสารสนเทศ **วันที่** 13 มกราคม 2568	**ลงชื่อ** ..... **(นายกิตติภูมิ คำศรี)**
ผู้จัดทำเอกสาร	
ชื่อ นายจยุตย์ พูลเพิ่ม **ตำแหน่ง** หัวหน้างานพัฒนาเทคโนโลยีเครือข่ายและโครงสร้างพื้นฐาน **วันที่** 13 มกราคม 2568	**ลงชื่อ** ..... **(นายจยุตย์ พูลเพิ่ม)**
ผู้ตรวจทานเอกสาร	
ชื่อ ดร.ชายแดน มิ่งเมือง **ตำแหน่ง** รองผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีวารสนเทศ **วันที่** 13 มกราคม 2568	**ลงชื่อ** ..... **(ดร.ชายแดน มิ่งเมือง)**
ชื่อ นายกรกช มาตะรัตน์ **ตำแหน่ง** ผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ ผู้บริหารด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ **วันที่** 13 มกราคม 2568	**ลงชื่อ** ..... **(นายกรกช มาตะรัตน์)**
ผู้อนุมัติเอกสาร	
ชื่อ ผู้ช่วยศาสตราจารย์ชาคริต ชาญชิตปรีชา **ตำแหน่ง** อธิการบดีมหาวิทยาลัยราชภัฏสกลนคร **วันที่** 21 มกราคม 2568	**ลงชื่อ** ..... **(ผู้ช่วยศาสตราจารย์ชาคริต ชาญชิตปรีชา)**

แผนรับมือเหตุภัยคุกคามทางไซเบอร์
มหาวิทยาลัยราชภัฏสกลนคร
Cybersecurity Incident Response Plan

ที่ปรึกษา

ผู้ช่วยศาสตราจารย์ชาคริต	ชาญชิตปรีชา	อธิการบดีมหาวิทยาลัยราชภัฏสกลนคร
ศาสตราจารย์ ดร.ทศวรรษ	สีตะวัน	รองอธิการบดีฝ่ายวางแผน
อาจารย์กรกช	มาตะรัตน์	ผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ
อาจารย์ ดร.ชายแดน	มิ่งเมือง	รองผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ
นายเกษม	บุตรดี	ผู้อำนวยการสำนักงานอธิการบดี

คณะทำงาน

คณะกรรมการจัดทำแผนรับมือเหตุภัยคุกคามทางไซเบอร์มหาวิทยาลัยราชภัฏสกลนคร Cybersecurity Incident Response Plan

รวบรวม/วิเคราะห์ข้อมูล/รูปเล่ม

นางสาวอังคณา	ศิริกุล	หัวหน้าสำนักงานผู้อำนวยการ สำนักวิทยบริการและเทคโนโลยีสารสนเทศ
นายกิตติภูมิ	คำศรี	หัวหน้างานพัฒนาระบบสารสนเทศ
นายจยุตย์	พูลเพิ่ม	หัวหน้างานพัฒนาเทคโนโลยีเครือข่ายและโครงสร้างพื้นฐาน

ปีที่พิมพ์

มกราคม 2568