แผนรับมือภัยคุกคามทางไซเบอร์

Cybersecurity Incident Response Plan

ประวัติการแก้ไขเอกสาร

เวอร์ชัน	รายละเอียดการแก้ไข	วันที่จัดทำ
01	เอกสารเวอร์ชันตั้งต้น	16 กุมภาพันธ์ 2567

การอนุมัติเอกสาร

ผู้จัดทำเอกสาร	
ชื่อ นายวีรเดช เพ็งกระจ่าง ตำแหน่ง ผู้อำนวยการฝ่าย โครงสร้างพื้นฐานเทคโนโลยีสารสนเทศ วันที่ 12 มีนาคม 2567	ลงชื่อ ..... (นายวีรเดช เพ็งกระจ่าง)
ผู้ตรวจทานเอกสาร	
ชื่อ นายรุ่งโรจน์ กิตติถาวรกุล ตำแหน่ง ผู้อำนวยการ สำนักบริหารเทคโนโลยีสารสนเทศ วันที่ 12 มีนาคม 2567	ลงชื่อ ..... (นายรุ่งโรจน์ กิตติถาวรกุล)
ผู้อนุมัติเอกสาร	
ชื่อ ศาสตราจารย์ดร.บุญไชย สถิตมั่นในธรรม ตำแหน่ง ผู้บริหาร ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ วันที่ 12 มีนาคม 2567	ลงชื่อ ..... (ศาสตราจารย์ดร.บุญไชย สถิตมั่นในธรรม)

1. หลักการและเหตุผล

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

(1) แผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจประเมินผู้ตรวจสอบภายใน หรือผู้ตรวจสอบอิสระจากภายนอก อย่างน้อยปีละหนึ่งครั้ง

(2) แผนการรับมือภัยคุกคามทางไซเบอร์

เพื่อดำเนินการตาม พรบ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ 2562 มาตรา 44 จุฬาลงกรณ์มหาวิทยาลัยจึงได้จัดทำแผนรับมือภัยคุกคามทางไซเบอร์ขึ้นเพื่อรับมือกับภัยคุกคามทางไซเบอร์ในปัจจุบันและอนาคต โดยให้ครอบคลุมถึงการดำเนินมาตรการการป้องกัน (Protect) การตรวจจับ (Detect). การตอบสนอง (Respond) และการคืนสภาพ (Recover)

2. วัตถุประสงค์

(1) เพื่อใช้เป็นแผนในการรับมือเหตุภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัย
(2) เพื่อกำหนดกระบวนการในการเฝ้าระวัง ตรวจสอบ ติดตาม และแก้ไขปัญหาที่เกิดจากภัยคุกคามทางไซเบอร์
(3) เพื่อกำหนดขั้นตอนการรับมือเหตุภัยคุกคามทางไซเบอร์ และการรายงานเหตุภัยคุกคามทางไซเบอร์ไปยังหน่วยงานที่เกี่ยวข้อง

3. ขอบเขต

แผนรับมือฯ ฉบับนี้ ใช้รับมือเหตุภัยคุกคามทางไซเบอร์ที่เกิดขึ้นต่อระบบสารสนเทศ และข้อมูลดิจิทัลของจุฬาลงกรณ์มหาวิทยาลัย รวมถึงบุคคลหรืออุปกรณ์ใด ๆ ซึ่งเข้าถึงระบบสารสนเทศ และข้อมูลดิจิทัลดังกล่าว

4. หน้าที่การทบทวนแผน

สำนักบริหารเทคโนโลยีสารสนเทศ มีหน้าที่ทบทวนและขออนุมัติแผนรับมือฯ ฉบับนี้ถึง ผู้บริหารสูงสุดหรือผู้ที่รับมอบอำนาจหน่วยงานของท่าน

5. หน้าที่ในการดำเนินการตามแผน

หน่วยงานภายใต้จุฬาลงกรณ์มหาวิทยาลัย อาทิ คณะ สถาบัน วิทยาลัย และหน่วยงานต่าง ๆ มีหน้าที่เป็นผู้รับผิดชอบหลักในการดำเนินการ ตามแผนรับมือฯ ฉบับนี้ โดยมีหน่วยงานสนับสนุนประกอบด้วย สำนักบริหารเทคโนโลยีสารสนเทศ รวมถึงศูนย์คอมพิวเตอร์หรือหน่วยงานที่ทำหน้าที่กำกับดูแลระบบเทคโนโลยีสารสนเทศหรือข้อมูลประจำหน่วยงาน

6.เอกสารและกรอบมาตรฐานที่เกี่ยวข้อง

6.1 นโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้อง

- แนวทางปฏิบัติเรื่องความมั่นคงปลอดภัยสารสนเทศ (Cyber Security Guideline)
- นโยบายการรักษาความมั่นคงความปลอดภัยด้านสารสนเทศ (CU IT Security Policy)

6.2 นโยบายและแนวปฏิบัติด้านการปกป้องข้อมูลส่วนบุคคลที่เกี่ยวข้อง

- ข้อบังคับจุฬาลงกรณ์มหาวิทยาลัย ว่าด้วย การคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2563
- ประกาศจุฬาลงกรณ์มหาวิทยาลัย เรื่อง การคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2565
- ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล พ.ศ. 2563

6.3 กฎหมายที่เกี่ยวข้อง

ที่	กฎหมายที่เกี่ยวข้อง
1.	**พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม**
	ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. ๒๕๖๔
2.	**พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒**
	ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการจัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลสำหรับผู้ประมวลผลข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕
	ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕
	ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕
	ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลที่เป็นหน่วยงานของรัฐซึ่งต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๖
3.	**พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒**
	ประกาศ กกม. เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔
	ประกาศ กมช. เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ
	ประกาศ กกม. เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ. ๒๕๖๖
	ประกาศ กมช. เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. ๒๕๖๖
	ประกาศ กมช. เรื่อง มาตรฐานขั้นต่ำของข้อมูลหรือระบบสารสนเทศ พ.ศ. ๒๕๖๖
	ประกาศ สกมช. เรื่อง แนวทางการจัดทำแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๗

7. นิยาม

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

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

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

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

8. บทบาทหน้าที่และโครงสร้างทีมรับมือเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์

8.1 ผู้รับแจ้งเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ภายในหน่วยงาน

ลำดับ	ชื่อ – นามสกุล	ระยะเวลาในการปฏิบัติงาน	ช่องทางการติดต่อสื่อสาร	หน้าที่	ความรับผิดชอบ
1	ฝ่ายบริการเทคโนโลยีสารสนเทศ	8.00-17.00น.	02-218-3314	รับแจ้งเหตุ	หน่วยงานภายในจุฬาฯ
2	เจ้าหน้าที่กลุ่มงานด้านความมั่นคงปลอดภัย ฯ	8.00-17.00น.	02-218-3413	รับแจ้งเหตุ	หน่วยงานภายในจุฬาฯ และหน่วยงานภายนอก

8.2 โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber incident Response Team : CIRT)

จุฬาลงกรณ์มหาวิทยาลัยใช้โมเดลโครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ในลักษณะแบบกระจาย (Distributed) และแบบให้คำปรึกษา (Coordinating) โดยแต่ละหน่วยงานภายใต้จุฬาลงกรณ์มหาวิทยาลัยจะต้องมีการระบุรายชื่อของบุคลากรที่มีความเกี่ยวข้องกับการรับมือเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน พร้อมทั้งโครงสร้างทีมรับมือฯ ดังนี้

ลำดับ	ชื่อ - นามสกุล	ช่องทางการติดต่อสื่อสาร	หน้าที่	ความรับผิดชอบ
1.	ผู้อำนวยการสำนักบริหารเทคโนโลยีสารสนเทศ	เบอร์โทรศัพท์ภายใน : 02-218-3414 Email: rungroj.k@chula.ac.th	หัวหน้าทีมรับมือฯ (Team manager)	ทำหน้าที่สื่อสารกับผู้บริหารของหน่วยงาน

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

2.	ผู้อำนวยการฝ่ายโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศ	เบอร์โทรศัพท์ภายใน : 02-218-3435 Email: weeradach.p@chula.ac.th	รองหัวหน้าทีมรับมือฯ (Deputy team manager)	ทำหน้าที่แทนกรณีหัวหน้าทีมรับมือฯ ไม่อยู่/ไม่สามารถปฏิบัติงานได้
3.	ฝ่ายโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศ	เบอร์โทรศัพท์ภายใน : 02-218-3246, 02-218-3413 Email: nw-dept@it.chula.ac.th, csirt@chula.ac.th	เจ้าหน้าที่รับมือฯ (Incident leader)	ทำหน้าที่ช่วยเหลือหน่วยงานภายใต้จุฬาลงกรณ์มหาวิทยาลัยให้สามารถควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์ได้
4.	ฝ่ายโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศ	เบอร์โทรศัพท์ภายใน : 02-218-3246, 02-218-3413 Email: nw-dept@it.chula.ac.th, csirt@chula.ac.th	เจ้าหน้าที่เทคนิคฯ (Technical lead)	ทำหน้าที่ให้ความเห็นเกี่ยวกับแนวทางที่เหมาะสมในการควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์

ทั้งนี้ นอกจากทีมรับมือฯ ดังกล่าวข้างต้น ให้มีบุคคลดังต่อไปนี้ทำหน้าที่สนับสนุนการดำเนินการของแผนรับมือฯ ฉบับนี้ ดังนี้

ลำดับ	ชื่อ - นามสกุล	ช่องทางการติดต่อสื่อสาร	หน้าที่	ความรับผิดชอบ
1.	สำนักบริหารเทคโนโลยีสารสนเทศ จุฬาลงกรณ์มหาวิทยาลัย	เบอร์โทรศัพท์ภายใน : 02-218-3314	ควบคุมผลกระทบจากภัยคุกคาม	ทำหน้าที่ควบคุมผลกระทบจากภัยคุกคาม
2.	สำนักตรวจสอบ จุฬาลงกรณ์มหาวิทยาลัย	เบอร์โทรศัพท์ภายใน : 02-218-3343	เจ้าหน้าที่ด้านการปฏิบัติตามกฎหมาย (Compliance)	Internal Audit
3.	ผู้ให้บริการภายนอก	-	ผู้ทดสอบเจาะระบบ	
4.	ศูนย์กฎหมายและนิติการ จุฬาลงกรณ์มหาวิทยาลัย	เบอร์โทรศัพท์ภายใน : 02-218-0146, 02-218-0190	ผู้เชี่ยวชาญด้านกฎหมาย	
5.	ศูนย์บริหารความเสี่ยง จุฬาลงกรณ์มหาวิทยาลัย	เบอร์โทรศัพท์ภายใน: 02-218-2000	ผู้บริหารจัดการความเสี่ยง	
6.	ศูนย์สื่อสารองค์กร จุฬาลงกรณ์มหาวิทยาลัย	เบอร์โทรศัพท์ภายใน : 02-218-3364, 02-218-3365	ผู้รับผิดชอบด้านสื่อสารองค์กร	

8.3 หน่วยงานภายนอกที่เกี่ยวข้อง

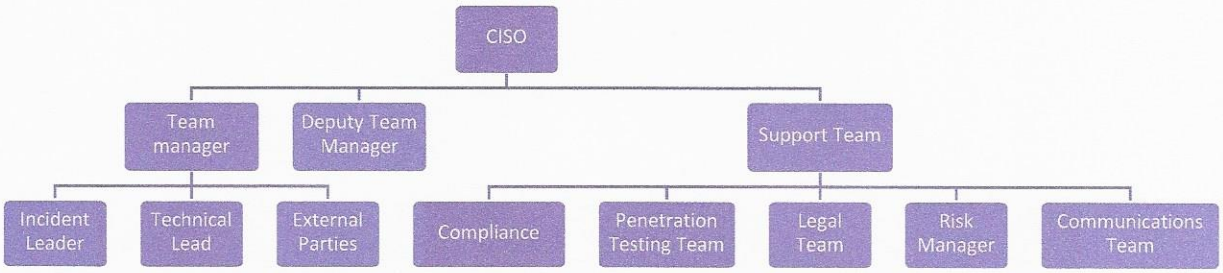
ข้อมูลติดต่อสื่อสารของหน่วยงานภายนอกที่เกี่ยวข้อง เช่น สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.), หน่วยงานกำกับดูแล (Regulator), THAI – CERT และผู้ให้บริการภายนอกของหน่วยงาน เช่น หน่วยงานผู้ให้บริการด้านการตรวจสอบพิสูจน์หลักฐานทางดิจิทัล (Digital Forensic Investigator) เป็นต้น

ลำดับ	ชื่อ - นามสกุล	ช่องทางการติดต่อสื่อสาร	หน่วยงาน	ความเกี่ยวข้อง
1.	National Cyber Security Agency	เบอร์โทรศัพท์: 02-142-6888 Email: saraban@ncsa.or.th ที่อยู่สำนักงาน: 120 หมู่ 3 อาคารรัฐประศาสนภักดี (อาคารบี) ชั้น 7 ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ 10210	สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)	แจ้งเหตุภัยคุกคามไซเบอร์
2.	สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล	เบอร์โทรศัพท์: 02-142-1033, 02-141-6993 Email: saraban@pdpc.or.th ที่อยู่สำนักงาน: เลขที่ 120 หมู่ 3 ศูนย์ราชการเฉลิมพระเกียรติ 80 พรรษาฯ อาคารรัฐประศาสนภักดี (อาคารบี) ชั้น 7 ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ 10210	สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.)	แจ้งเหตุการละเมิดข้อมูลส่วนบุคคล
3.	กระทรวงการอุดมศึกษาวิทยาศาสตร์ วิจัยและนวัตกรรม	เบอร์โทรศัพท์: 1313 ที่อยู่สำนักงาน: เลขที่ 75/47 ถนนโยธี และเลขที่ 328 ถนนศรีอยุธยา แขวงทุ่งพญาไท เขตราชเทวี กรุงเทพฯ	กระทรวงการอุดมศึกษาวิทยาศาสตร์ วิจัยและนวัตกรรม	หน่วยงานกำกับดูแล
4.	THAICERT	เบอร์โทรศัพท์: 02-142-6888 Email: thaicert@ncsa.or.th ที่อยู่สำนักงาน: 120 หมู่ 3 อาคารรัฐประศาสนภักดี(อาคารบี) ชั้น 7 ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ 10210	ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ	
5.	Uninet	เบอร์โทรศัพท์: 02-232-4000 Email: noc@uni.net.th ที่อยู่สำนักงาน: 328 ถ.ศรีอยุธยา แขวง ทุ่งพญาไท เขต ราชเทวี กรุงเทพฯ 10400		
6.	บริษัทคู่สัญญา ดูแลระบบ Network	-	บริษัทผู้ให้บริการภายนอก (บริษัท Data Pro)	ดูแลระบบ Network

7.	บริษัทคู่สัญญา ดูแลระบบ VM	-	บริษัทผู้ให้บริการภายนอก (บริษัท Data Pro)	ดูแลระบบ VM
8.	บริษัทคู่สัญญา ดูแลระบบ Backup	-	บริษัทผู้ให้บริการภายนอก (บริษัท G-able)	ดูแลระบบ Backup
9.	บริษัทคู่สัญญา ดูแลระบบ Data Center	-	บริษัทผู้ให้บริการภายนอก (บริษัท FirstOne)	ดูแลระบบ Data Center
10.	บริษัทคู่สัญญา ดูแลระบบ storage	-	บริษัทผู้ให้บริการภายนอก (บริษัท Yip In Tsoi)	ดูแลระบบ Storage
11.	บริษัทคู่สัญญา ดูแลระบบป้องกันมัลแวร์	-	บริษัทผู้ให้บริการภายนอก (บริษัท (Zenith)	ดูแลระบบป้องกันมัลแวร์

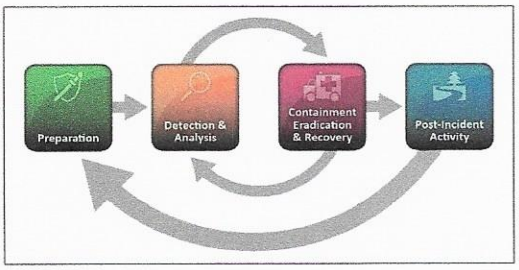
8.4 โครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure)

เพื่อให้การดำเนินการรับมือเหตุภัยคุกคามทางไซเบอร์ สามารถนำไปปฏิบัติได้อย่างมีประสิทธิภาพจะต้องกำหนดโครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ โดยแต่ละตำแหน่งจะต้องร่วมมือ ติดตาม ปฏิบัติงานตามบทบาทหน้าที่กำหนดไว้



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 รวมถึงนโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน ดังนี้



วัฏจักรของการตอบสนองต่อเหตุการณ์

9.1 ขั้นการเตรียมการ (preparation)

เป็นการดำเนินมาตรการเพื่อเตรียมการและป้องกันการเกิดภัยคุกคามทางไซเบอร์ (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 8.2
(2) กำหนดโครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure) รายละเอียดปรากฏตามข้อ 8.4
(3) กำหนดเกณฑ์และขั้นตอนในการเรียกใช้งาน (Activate) การตอบสนองต่อเหตุการณ์ และ CIRT
(4) จัดเตรียมข้อมูลและอุปกรณ์ รวมถึงช่องทางในการติดต่อสื่อสารที่จำเป็น เช่น ข้อมูลการติดต่อและอุปกรณ์ติดต่อสื่อสารของบุคลากร, กลไกรายงานเหตุการณ์, ห้องประชุม เป็นต้น
(5) จัดเตรียมอุปกรณ์, ซอฟต์แวร์ และแหล่งข้อมูลสำหรับวิเคราะห์เหตุภัยคุกคามทางไซเบอร์
(6) จัดให้มีการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน (Risk Assessment)
(7) จัดทำแผนผังโครงสร้างขั้นตอนการรับมือฯ ของหน่วยงาน (รายละเอียดปรากฏตามภาคผนวก 1)
(8) พิจารณาดำเนินการตามเอกสารแนบท้าย 2 ตารางที่ 2.1 ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. 2564

9.2 ขั้นการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์

เป็นการดำเนินการในการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (detection and analysis) ซึ่งเป็นสิ่งจำเป็นที่จะช่วยให้หน่วยงานสามารถบรรเทาความเสี่ยงที่ยังคงเหลืออยู่ และสามารถแจ้งเตือนได้อย่างทันท่วงทีเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น โดยดำเนินการดังต่อไปนี้

9.2.1 วิธีการที่ใช้ในการตรวจจับภัยคุกคาม

- อุปกรณ์เฝ้าระวังเหตุการณ์ด้านความมั่นคงปลอดภัย

เครื่องมือและอุปกรณ์เฝ้าระวังเหตุการณ์ด้านความมั่นคงปลอดภัย

- Firewall ระบบรักษาความปลอดภัยของเครือข่ายคอมพิวเตอร์ ที่สามารถควบคุม คัดกรองข้อมูลที่รับและส่งผ่านเครือข่ายได้
- IPS ระบบที่ทำหน้าที่ตรวจจับและป้องกันการโจมตีโดยเฉพาะที่เกิดขึ้นในระบบเครือข่าย โดยระบบประเภทนี้จะตรวจจับได้เฉพาะสิ่งที่ตรงกับวิธีการโจมตีที่ระบบรู้จัก

- **Endpoint Security** ซอฟต์แวร์ตรวจจับโปรแกรมประสงค์ร้ายที่พยายามโจมตีต่อระบบคอมพิวเตอร์และเครือข่าย
- **Centralized Log Management** ระบบจัดเก็บและบริหารจัดการข้อมูล Log File แบบศูนย์กลาง
- **Big Data Platforms** ระบบคลังข้อมูล Big Data สำหรับจัดเก็บ และวิเคราะห์ข้อมูลชนิด Machine Data (Logs)

■ แหล่งข่าวสารภัยคุกคามจากภายนอก (Threat intelligence)

Channel 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/
	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

- 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 เป็นการดำเนินการเพื่อจะควบคุมหรือทำให้เกิดความขัดข้องกับบริการของระบบ
Availability (ความพร้อมใช้ของระบบ)	การถูกโจมตีความพร้อมใช้งานของระบบ เช่น DDoS (Denial of Service), Open DNS Resolver, Flood ทำให้เกิดความล่าช้าในการบริการ จนถึงทำให้ระบบไม่สามารถทำงานได้
Phishing (การหลอกลวงโดยใช้อีเมลหรือหน้าเว็บไซต์ปลอมเพื่อให้ได้มาซึ่งข้อมูล)	การถูกสร้างหน้าเว็บไซต์ปลอม (Web Phishing) หรือหลอกลวงเพื่อให้ได้ข้อมูลผ่านทางอีเมล
Web Defacement	การถูกปรับเปลี่ยนหน้าเว็บไซต์
SEO attack	เว็บไซต์ถูกโจมตี ด้วยการฝังสคริปต์โฆษณาเว็บไซต์ การพนันออนไลน์
Vulnerability	ช่องโหว่ของระบบหรือจุดอ่อนของระบบบริหารจัดการเว็บไซต์
Abuse	การละเมิดการใช้งานเครือข่าย เช่น Spam, Copyright

- การจำแนกประเภทภัยคุกคามตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ 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)
6	การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion)
7	การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)
8	เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating)
9	เหตุการณ์ผิดปกติที่ได้รับการวิเคราะห์แล้วว่าไม่ใช่เหตุการณ์ที่เป็นภัยคุกคาม (Explained Anomaly)

9.2.3 การวิเคราะห์ผลกระทบและระดับของภัยคุกคามทางไซเบอร์ (Incident Prioritization)

เพื่อรับมือกับภัยคุกคามทางไซเบอร์ให้ทันท่วงที โดยพิจารณาปัจจัยต่าง ๆ ที่เกี่ยวข้องเช่น ผลกระทบต่อการทำงานของระบบ (functional impact) ผลกระทบต่อข้อมูล (information impact) และความสามารถในการกู้คืน (recoverability effort[2]) 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 หรือเปิดเผยข้อมูลส่วนบุคคล
Integrity Breach	การละเมิดความถูกต้องครบถ้วนของข้อมูลส่วนบุคคลซึ่งมีการเปลี่ยนแปลง แก้ไขข้อมูลส่วนบุคคลให้ไม่ถูกต้อง ไม่สมบูรณ์ หรือไม่ครบถ้วน
Availability Breach	การละเมิดความพร้อมใช้งานของข้อมูลส่วนบุคคลซึ่งทำให้ไม่สามารถเข้าถึงข้อมูลส่วนบุคคลได้ หรือมีการทำลายข้อมูลส่วนบุคคล ทำให้ข้อมูลส่วนบุคคลไม่อยู่ในสภาพที่พร้อมใช้งานได้ตามปกติ

ระดับความสามารถในการกู้คืน

ระดับผลกระทบ	หลักเกณฑ์การพิจารณาระดับของผลกระทบ
Regular	เวลาในการกู้คืนสามารถคาดการณ์ได้ โดยใช้ทรัพยากรที่มี
Supplemented	เวลาในการกู้คืนสามารถคาดการณ์ได้ แต่ต้องมีการจัดหาทรัพยากรเพิ่ม
Extended	เวลาในการกู้คืนไม่สามารถคาดการณ์ได้ ต้องใช้ทรัพยากรและความช่วยเหลือจากภายนอก
Not Recoverable	การกู้คืนไม่สามารถทำได้ ใช้กับสถานการณ์ที่ข้อมูลได้รั่วไหลสู่สาธารณะ แล้ว เป็นต้น ให้ใช้วิธีการติดตามและจำกัดการแพร่กระจายรวมถึงการเยียวยาผลกระทบ

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

9.2.4 การบันทึกภัยคุกคาม

ต้องทำการบันทึกข้อมูลเหตุการณ์ภัยคุกคามเพื่อช่วยในการรับมือและตอบสนองภัยคุกคามอย่างมีประสิทธิภาพ และเป็นระบบ โดยทำการบันทึกตั้งแต่การตรวจพบจนถึงสิ้นสุดของเหตุการณ์ภัยคุกคาม ผ่านระบบรายงานฯ (ITSM) ของหน่วยงาน และหากพบว่าเหตุการณ์ภัยคุกคามที่เกิดขึ้นกระทบต่อบริการที่สำคัญของหน่วยงานให้กรอก แบบฟอร์มการบันทึก ข้อมูลเหตุการณ์ภัยคุกคาม (รายละเอียดปรากฏตามภาคผนวก 2) เพิ่มเติมเพื่อใช้รายงานแก่หน่วยงานควบคุมหรือกำกับดูแล

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

เมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้นหรือ เมื่อหน่วยงานได้รับแจ้งเตือนการเกิดภัยคุกคามทางไซเบอร์ หน่วยงานต้องมีการกำหนดแนวทางการดำเนินมาตรการเพื่อระงับภัยคุกคามทางไซเบอร์และการฟื้นฟูระบบ ที่ได้รับผลกระทบ (Containment, Eradication, and Recovery) โดยกำหนดให้สอดคลองกับความรุนแรง และระดับของภัยคุกคามทางไซเบอร์แต่ละระดับ จนกระทั่งสามารถกูคืนทรัพย์สินสำคัญทางสารสนเทศให้กลับมา ดำเนินงานหรือให้บริการได้ตามปกติ

9.3.1 วิธีการควบคุมความเสียหาย คือการตัดสินใจเลือกใช้วิธีการที่เหมาะสม ดังนี้

- ปิดระบบ (Shut Down)

- ตัดการเชื่อมต่อทางเครือข่ายทั้งหมด (Network disconnection) ทั้งนี้ อาจมียกเว้นการเชื่อมต่อสำหรับ Endpoint Detection & Response Agent (กระบวนการตรวจสอบและตรวจจับกิจกรรมหรือเหตุการณ์ ที่น่าสงสัยใด ๆ ที่เกิดขึ้นที่ปลายทางแบบเรียลไทม์)

- หยุดการทำงานของฟังก์ชันที่เกี่ยวข้อง (Disabling Certain Functions)

- Redirect Network Traffic และ/หรือความสนใจของผู้บุกรุกไปยัง Blackhole/ Sandbox/ Honeypot

ทั้งนี้ การตัดสินใจเลือกใช้วิธีการควบคุมความเสียหายจะขึ้นอยู่กับลักษณะสถานการณ์ที่กำลังเผชิญ ประเภทของภัยคุกคาม ระบบงานหรือบริการที่ได้รับผลกระทบ ระยะเวลาและทรัพยากรที่จำเป็นต่อการควบคุมความเสียหาย

9.3.2 การจัดเก็บและดูแลรักษาหลักฐานทางดิจิทัล

วัตถุประสงค์หลักของการจัดเก็บหลักฐาน คือเพื่อให้การแก้ไข Incident ส่งผลกระทบต่อธุรกิจให้น้อยที่สุด (Minimizing impact to the business) นอกจากนี้ หลักฐานอาจมีความจำเป็นที่จะต้องใช้ในการดำเนินการตามขั้นตอนทางกฎหมาย ดังนี้ การดำเนินการจัดเก็บหลักฐานทางดิจิทัลสามารถดำเนินการโดยพิจารณา ตามหลักการดังต่อไปนี้

- เป็นไปตามขั้นตอนที่กำหนดไว้ในกฎหมายข้อบังคับที่เกี่ยวกับหลักฐานดิจิทัล 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

9.3.3 การกำจัดสาเหตุและการกู้คืนระบบให้กลับมาทำงานปกติ

เมื่อมีการควบคุมความเสียหาย และมีการเก็บหลักฐานข้อมูลเพิ่มเติมเรียบร้อยแล้วข้อมูลทั้งหมด จะต้องนำกลับมาวิเคราะห์ตามหลักการที่ได้กล่าวไว้ใน "ขั้นตอนที่ 2 เรื่องการตรวจจับและวิเคราะห์ (Detection & Analysis)" จนกว่าจะสามารถกำจัดสาเหตุที่ทำให้เกิด Incident และช่องทางที่ผู้บุกรุกได้สร้างไว้เพื่อเข้ามาในระบบทั้งหมดได้เรียบร้อย ซึ่งการกำจัดสาเหตุที่ทำให้เกิด Incident และผลกระทบ ได้แก่

- การปิดช่องโหว่ของระบบ- การยกเลิก User Account ที่ผู้บุกรุกใช้เข้าสู่ระบบ

- การแจ้งให้ผู้ใช้งานเปลี่ยนรหัสผ่าน

- การลบโปรแกรมประเภท Backdoor ออกจากระบบ

- การใช้ข้อมูล Indicator of Compromise (IOC) ในการสแกนหา Malware หรือร่องรอยอื่น ๆ ในระบบที่ยังหลงเหลือของผู้บุกรุกเพื่อดำเนินการกำจัดให้ออกจากระบบทั้งหมด

หลังจากดำเนินการควบคุมความเสียหาย กำจัดสาเหตุของภัยคุกคามเสร็จเรียบร้อยแล้ว จะเข้าสู่กระบวนการฟื้นฟูระบบให้เข้าสู่สภาวะการทำงานปกติโดยในขั้นตอนนี้สิ่งที่มีความสำคัญเป็นอย่างยิ่ง และควรเตรียมการล่วงหน้าในเรื่องดังต่อไปนี้

- การ Restore Operating System หรือ Application Software ต่าง ๆ จาก Master Image ที่ปลอดภัย

- การ Restore ข้อมูลกลับเข้าระบบจาก Back Up Storage

<u>9.4 ขั้นการดำเนินการภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์</u>

การดำเนินกิจกรรมที่เกี่ยวของภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์(Post-incident Activity) นั้น ให้จัดทำข้อกำหนดขั้นตอน วิธีปฏิบัติ ที่เกี่ยวของเพื่อให้มีแนวทางที่ชัดเจน ซึ่งการปฏิบัติตามมาตรการดังกล่าวเพื่อให้สามารถเรียนรู้จากเหตุภัยคุกคามทางไซเบอร์ที่ผ่านมา และสามารถหาแนวทางเพื่อแก้ไขจุดบกพร่อง และพัฒนาแนวทางรับมือกับภัยคุกคามทางไซเบอร์ตอไปในอนาคต โดยให้มีการประชุมหารือเพื่อแลกเปลี่ยนข้อมูลความคิดเห็นในการนำไปพัฒนาและปรับปรุงแนวทางในการรับมือและตอบสนองภัยคุกคามทางไซเบอร์ รวมทั้งการใช้ข้อมูลเพื่อประกอบการพิจารณาปรับปรุง

นอกจากนี้ตองเก็บรักษาข้อมูลและพยานหลักฐานที่จำเป็น เพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์ หรือใช้ในกรณีที่ต้องการร้องทุกขหรือดำเนินคดี เนื่องจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้นนั้น อาจเข้าลักษณะเป็น 12 ความผิดตามประมวลกฎหมายอาญา หรือพระราชบัญญัติวาด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐ และที่แก้ไขเพิ่มเติม หรือกฎหมายอื่น ๆ ที่เกี่ยวข้อง โดยการเก็บข้อมูลบางประเภทนั้นอาจจำเป็นต้องดำเนินการตั้งแต่เมื่อมีการตรวจพบว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้น เนื่องจากข้อมูลดังกล่าวอาจสูญหายไปในระหว่างที่ตองระงับเหตุภัยคุกคามทางไซเบอร์นั้น หรืออาจถูกลบหรือทำลายโดยผู้โจมตีเมื่อมีการเก็บรวบรวมข้อมูลและหลักฐานที่จำเป็นแล้ว ให้นำข้อมูลและหลักฐานที่รวบรวมได้มาใช้ในการจัดทำบันทึกข้อมูลสถิติภัยคุกคาม ทาง

ไซเบอร์โดยอาจจัดทำเป็นรายสัปดาห์หรือรายเดือน เพื่อเสนอต่อผู้ที่มีหน้าที่ดูแลและรับผิดชอบภายใน หน่วยงาน กำหนดขั้นตอนที่หน่วยงานควรดำเนินการ 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 หรือความอ่อนไหวต่อการสูญเสียกระแสไฟฟ้าของ หลักฐาน 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 Handling Checklist)

หน่วยงานจะต้องจัดทำรายการตรวจสอบการจัดการเหตุการณ์ (Incident Handling Checklist) ซึ่งจะช่วยให้แนวทางแก่หน่วยงานเกี่ยวกับขั้นตอนสำคัญที่ควรดำเนินการ โดยหน่วยงานสามารถใช้ข้อมูลเพื่อประกอบการพิจารณาความเหมาะสมในการจัดทำรายการตรวจสอบของตนเองได้ (รายละเอียดปรากฏตามภาคผนวก 3)

ภาคผนวก 1

1. ขั้นตอนการทำงานการรับมือเหตุภัยคุกคามทางไซเบอร์ที่กระทบต่อบริการที่สำคัญของหน่วยงาน

ตรวจสอบเหตุการณ์ด้านความมั่นคงปลอดภัยจากระบบเฝ้าระวังฯ หรือเมื่อได้รับแจ้งเหตุ และหากพบเหตุการณ์ที่เกิดขึ้นกระทบต่อบริการที่สำคัญของหน่วยงานให้เริ่มดำเนินการตามกระบวนการทำงาน ดังนี้

1.1 มีการเฝ้าระวังและตรวจสอบเหตุการณ์ด้านความมั่นคงปลอดภัยฯ (Detection)

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

1.3 พิจารณาการรายงานแจ้งเหตุละเมิดไปยังหน่วยงานที่เกี่ยวข้อง อาทิ สกมช. สคส.

1.4 ดำเนินการควบคุมภัยคุกคามทางไซเบอร์ (Containment) เพื่อให้ส่งผลกระทบน้อยที่สุดและเพื่อป้องกันไม่ให้เกิดการแพร่กระจายไปยังส่วนอื่น ๆ ซึ่งหากเป็นกรณีที่เร่งด่วนและเป็นภัยคุกคามทางไซเบอร์ในระดับร้ายแรงทางมหาวิทยาลัยจะดำเนินการ ปิดกั้น หรือ ตัดการเชื่อมต่อระบบคอมพิวเตอร์เป็นการชั่วคราว

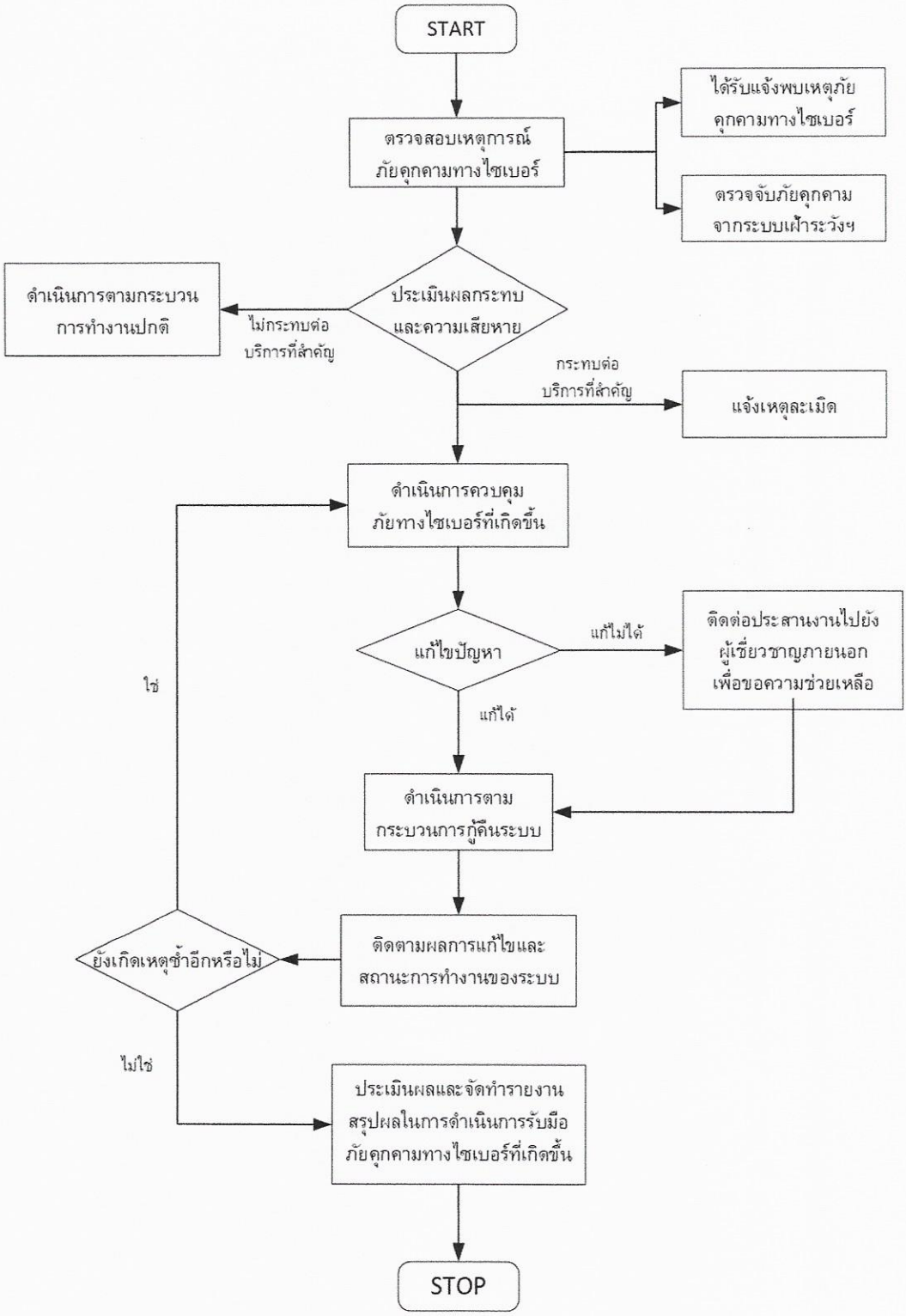
1.5 ดำเนินการแก้ไข (Eradication) กู้คืนระบบ และในการกรณีที่ไม่สามารถแก้ไขปัญหาได้จะดำเนินการติดต่อประสานงานไปยังศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) หรือผู้เชี่ยวชาญภายนอกเพื่อขอคำแนะนำหรือขอความช่วยเหลือ

1.6 ติดตามผลการแก้ไขและสถานะการทำงานของระบบ หากพบว่าเหตุการณ์ยังไม่สิ้นสุดให้ดำเนินการควบคุม แก้ไข และติดตามสถานการณ์ต่อไปจนกว่าระบบที่ได้รับผลกระทบกลับมาทำงานได้ตามปกติ

1.7 ประเมินผลและจัดทำรายงานสรุปผลการดำเนินการรับมือภัยคุกคามทางไซเบอร์ที่เกิดขึ้น

กระบวนการทำงาน

การรับมือเหตุภัยคุกคามทางไซเบอร์ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. 2564



2. ขั้นตอนการทำงานการเฝ้าระวังเหตุการณ์ด้านความมั่นคงปลอดภัยจากหน่วยงานภายใน/ภายนอกมหาวิทยาลัย (ไม่กระทบต่อบริการที่สำคัญ)

ตรวจสอบเหตุการณ์ด้านความมั่นคงปลอดภัยจากระบบเฝ้าระวังฯ หากพบเหตุการณ์ด้านความมั่นคงปลอดภัยที่ผิดปกติ หรือ ได้รับการแจ้งเตือนพบเหตุการณ์ที่ผิดปกติจากหน่วยงานภายนอกจุฬาฯ ให้เริ่มดำเนินการตามกระบวนการทำงาน ดังนี้

1.1 บันทึกข้อมูลเหตุการณ์ด้านความมั่นคงปลอดภัยที่ผิดปกติที่ได้ตรวจสอบพบหรือได้รับการแจ้งเตือนลงในระบบรายงานฯ

1.2 รวบรวมข้อมูลต่าง ๆ ที่เกี่ยวข้องกับภัยคุกคามที่ตรวจสอบพบ หรือ ได้รับการแจ้งเตือนจากหน่วยงานภายนอก จากอุปกรณ์ด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

1.3 วิเคราะห์ข้อมูลภัยคุกคามที่ตรวจสอบพบเป็นการโจมตีประเภทใด

1.4 บันทึกข้อมูลลงในระบบรายงานฯ

1.5 จัดระดับความเร่งด่วนในการแก้ไขปัญหาภัยคุกคาม รายละเอียดดังนี้

- 1.5.1 เร่งด่วน : มีความเสี่ยงส่งผลกระทบในวงกว้างทั่วทั้งมหาวิทยาลัย
- 1.5.2 มาก : มีความเสี่ยงส่งผลกระทบต่อคณะ ส่วนงาน หน่วยงาน ตั้งแต่ 2 แห่งขึ้นไป
- 1.5.3 ปานกลาง : มีความเสี่ยงส่งผลกระทบต่อคณะ ส่วนงาน หน่วยงาน ที่โดนโจมตีเท่านั้น
- 1.5.4 ปกติ : ยังมิได้มีผลกระทบเกิดขึ้น แต่หากไม่ดำเนินการจะส่งผลกระทบในอนาคต

1.6 บันทึกข้อมูลลงในระบบรายงานฯ

1.7 เตรียมแนวทางการแก้ไขปัญหา หากมีข้อมูลเดิมที่ได้จัดทำไว้แล้ว ให้นำข้อมูลดังกล่าวนำส่งต่อไป หากยังไม่มีแนวทางการแก้ไขปัญหา ต้องค้นคว้าหาข้อมูลแนวทางการแก้ไขปัญหาเพิ่มเติม

1.8 ตรวจสอบข้อมูลเหตุการณ์ด้านความมั่นคงปลอดภัยที่ตรวจสอบพบนั้น เป็นของหน่วยงานใดหรือผู้ใช้งานใด

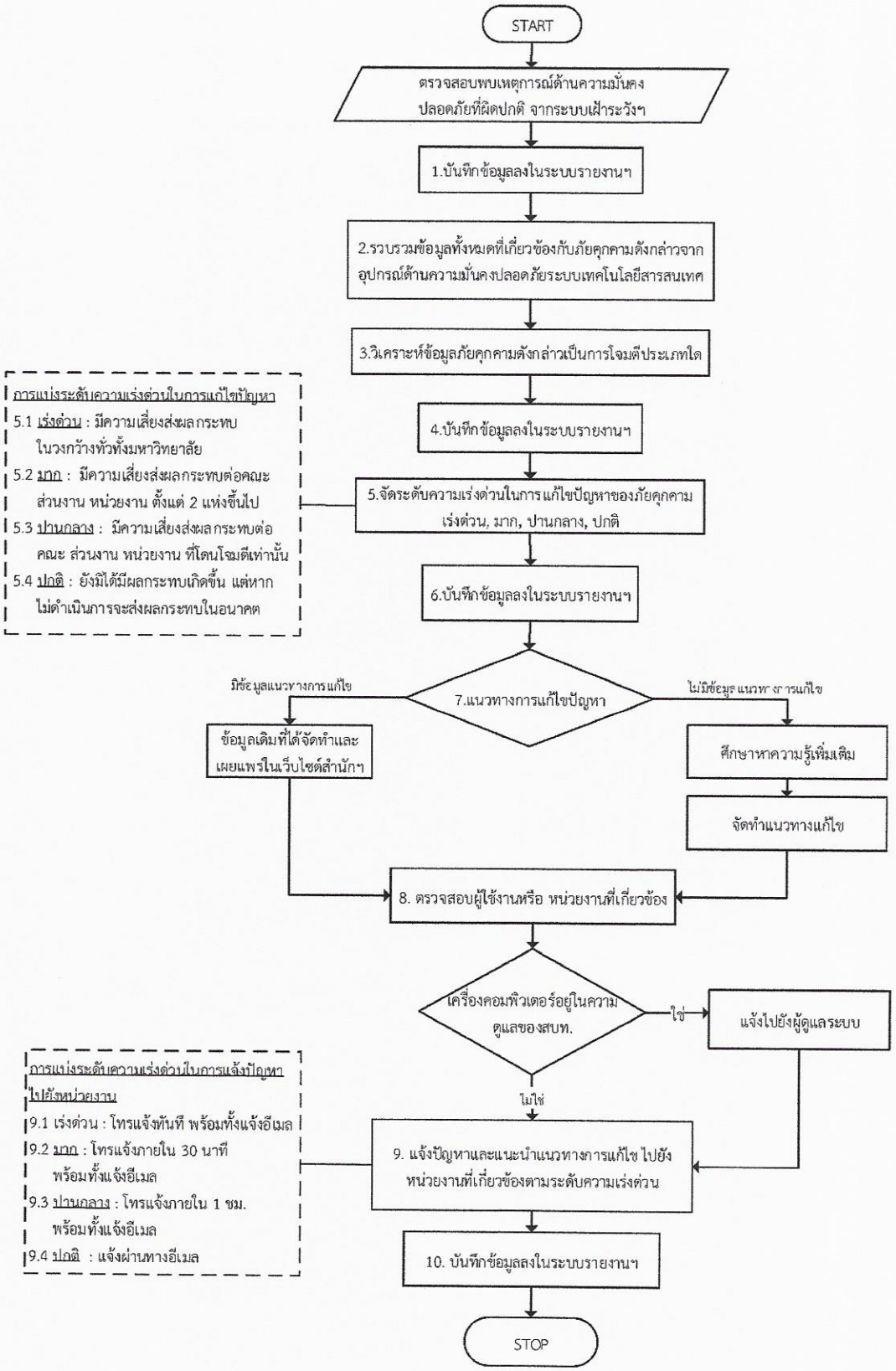
1.9 แจ้งปัญหาพร้อมทั้งแนะนำแนวทางการแก้ไขปัญหา ไปยังหน่วยงานที่เกี่ยวข้อง ตามระดับความเร่งด่วน รายละเอียดดังนี้

- 1.9.1 เร่งด่วน : โทรแจ้งทันที พร้อมทั้งแจ้งอีเมล
- 1.9.2 มาก : โทรแจ้งภายใน 30 นาที พร้อมทั้งแจ้งอีเมล
- 1.9.3 ปานกลาง : โทรแจ้งภายใน 1 ชม. พร้อมทั้งแจ้งอีเมล
- 1.9.4 ปกติ : แจ้งผ่านทางอีเมล

1.10 บันทึกข้อมูลลงในระบบรายงานฯ

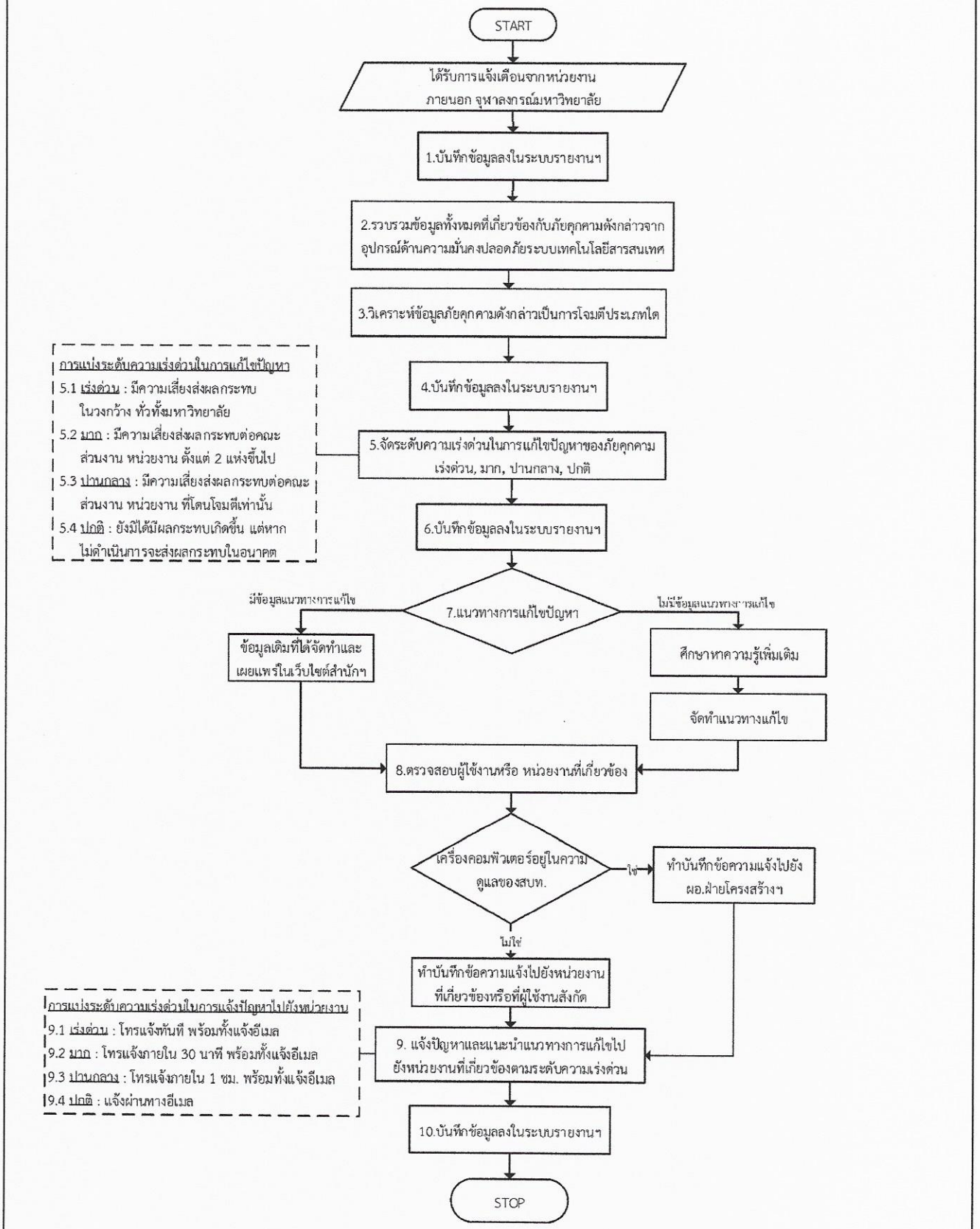
กระบวนการทำงาน

เฝ้าระวังเหตุการณ์ด้านความมั่นคงปลอดภัยจากหน่วยงานภายใน จุฬาลงกรณ์มหาวิทยาลัย



กระบวนการทำงาน

เฝ้าระวังเหตุการณ์ด้านความมั่นคงปลอดภัยจากหน่วยงานภายนอก จุฬาลงกรณ์มหาวิทยาลัย



3. ขั้นตอนการทำงานการประสานงานติดตามเหตุการณ์ด้านความมั่นคงปลอดภัย จุฬาลงกรณ์มหาวิทยาลัย

2.1 ติดตาม Ticket ในระบบรายงานฯ

2.2 ตรวจสอบตามระดับความเร่งด่วนในการแก้ไข รายละเอียดดังนี้

2.2.1 เร่งด่วน : มีความเสี่ยงส่งผลกระทบในวงกว้างทั่วทั้งมหาวิทยาลัย

2.2.2 มาก : มีความเสี่ยงส่งผลกระทบต่อคณะ ส่วนงาน หน่วยงาน ตั้งแต่ 2 แห่งขึ้นไป

2.2.3 ปานกลาง : มีความเสี่ยงส่งผลกระทบต่อคณะ ส่วนงาน หน่วยงาน ที่โดนโจมตีเท่านั้น

2.2.4 ปกติ : ยังมิได้มีผลกระทบเกิดขึ้น แต่หากไม่ดำเนินการจะส่งผลกระทบในอนาคต

2.3 แบ่งประเภทของการประสานงาน

2.3.1 กรณีประสานงานภายนอกจุฬาฯ

2.3.1.1 ตรวจสอบการแก้ไขปัญหาจากระบบหากพบว่าแก้ไขสำเร็จ ทำการบันทึกข้อมูลลงในระบบรายงานฯ

2.3.1.2 ตรวจสอบการแก้ไขปัญหาจากระบบหากพบว่าแก้ไขไม่สำเร็จ ให้ติดต่อไปยังหน่วยงานถึงปัญหาที่ยังคงอยู่อีกครั้ง

2.3.2 กรณีประสานงานภายในจุฬาฯ

2.3.2.1 ติดตามการแก้ไขปัญหากรณีหน่วยงานแก้ไขสำเร็จ ทำการทดสอบการแก้ไขปัญหาดังกล่าว พร้อมทั้งสอบถามเกี่ยวกับการดำเนินการ

2.3.2.2 ติดตามการแก้ไขปัญหากรณีหน่วยงานแก้ไขไม่สำเร็จ ให้ทำการติดต่อและให้ความช่วยเหลือไปยังหน่วยงาน กรณีที่ทางหน่วยงานมีการร้องขอ

2.3.3 กรณีประสานงานภายในสบท.

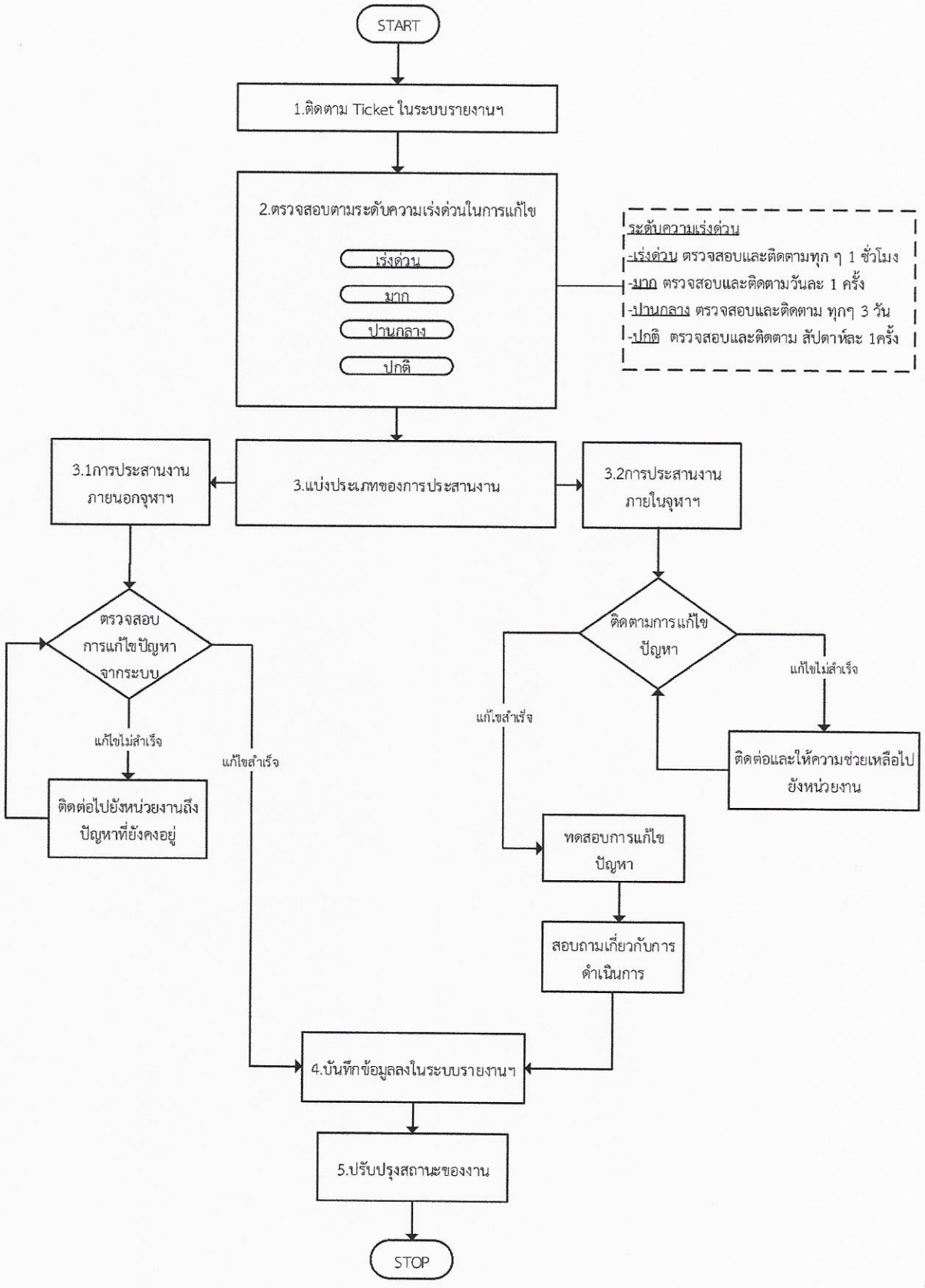
2.3.3.1 ตรวจสอบการแก้ไขปัญหาจากระบบหากพบว่าแก้ไขสำเร็จ ทำการทดสอบการแก้ไขปัญหาดังกล่าว พร้อมทั้งสอบถามเกี่ยวกับการดำเนินการ

2.3.3.2 ตรวจสอบการแก้ไขปัญหาจากระบบหากพบว่าแก้ไขไม่สำเร็จ ให้ติดต่อผู้ดูแลระบบถึงปัญหาที่ยังคงอยู่

2.3.4 บันทึกข้อมูลลงในระบบรายงานฯ

2.3.5 ปรับปรุงสถานะของงาน

กระบวนการทำงาน
การประสานงานติดตามเหตุการณ์ด้านความมั่นคงปลอดภัย จุฬาลงกรณ์มหาวิทยาลัย



ภาคผนวก 2

แบบรายงานภัยคุกคามทางไซเบอร์

วันที่ :	เวลา :	ผู้บันทึกรายงาน : ติดต่อ :

ข้อมูลทั่วไป (General Information)

ชื่อหน่วยงาน.....

ชื่อระบบงาน / โครงการ.....

ชื่อผู้ประสานงานของหน่วยงาน	ระบบปฏิบัติการ .....
โทรศัพท์	IP Address .....
E-mail.....	MAC Address.....

ข้อมูลเกี่ยวกับภัยคุกคามไซเบอร์

วันและเวลาที่เกิดเหตุการณ์ :	
สถานะเหตุการณ์ปัจจุบัน :	☐ เพิ่งพบเหตุการณ์ ☐ อยู่ในขั้นตอนการขอความช่วยเหลือ ☐ อยู่ในขั้นตอนการสอบสวน ☐ กำลังลุกลาม ☐ อยู่ในขั้นตอนการระงับภัย ☐ สามารถระงับภัยได้แล้ว ☐ รายงานปิดเหตุการณ์ภัยคุกคามแล้ว ☐ อื่น ๆ: โปรดระบุ
ประเภทเหตุการณ์ :	(ทั้งนี้ ภัยคุกคามหมวดหมู่ที่ 0 1 และ 9 ไม่เข้าข่ายเป็นภัยคุกคามทางไซเบอร์ที่ต้องรายงาน)
ระดับความรุนแรง และผลกระทบที่เกิดขึ้น :	ระบบที่ได้รับผลกระทบมีความสำคัญต่อพันธกิจหลักของหน่วยงานหรือไม่ ☐ ใช่ ☐ ไม่ใช่ เหตุการณ์ที่เกิดขึ้นเกิดจากภัยคุกคามทางไซเบอร์ ในระดับใด (มาตรา 60) ☐ ไม่ร้ายแรง ☐ ร้ายแรง ☐ วิกฤต (ก) ☐ วิกฤต (ข) ☐ ยังไม่สามารถระบุได้
รายละเอียดเหตุการณ์ :	
ความเสียหายที่เกิดขึ้น :	

หมวดหมู่	คำอธิบาย
☐ 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)

ข้อมูลการรับมือภัยคุกคาม

การสำรองข้อมูล (backup)	☐ มี ☐ ไม่มี
การดำเนินการตอบสนองต่อเหตุการณ์ :	☐ ยังไม่ได้ดำเนินการแก้ไขใด ๆ ☐ ยกเลิกการเชื่อมต่อระบบออกจากเครือข่ายแล้ว ☐ ตรวจสอบข้อมูลจราจร (Log) แล้ว ☐ ตรวจสอบโปรแกรม (แฟ้ม binaries/.exe) แล้ว ☐ กู้คืนกลับมาด้วยระบบหรือข้อมูลสำรองที่ตรวจสอบความถูกต้องแล้ว ☐ รายละเอียดการแก้ไขภัยคุกคามที่เกิดขึ้นเพิ่มเติม: โปรดระบุ
รายละเอียดการรับมือภัยคุกคามอื่น ๆ :	

มาตรา ๖๐ การพิจารณาเพื่อใช้อำนาจในการป้องกันภัยคุกคามทางไซเบอร์ คณะกรรมการจะกำหนดลักษณะของภัยคุกคามทางไซเบอร์ โดยแบ่งออกเป็นสามระดับ ดังต่อไปนี้

(๑) ภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง หมายถึง ภัยคุกคามทางไซเบอร์ที่มีความเสี่ยงอย่างมีนัยสำคัญถึงระดับที่ทำให้ระบบคอมพิวเตอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศหรือการให้บริการของรัฐด้อยประสิทธิภาพลง

(๒) ภัยคุกคามทางไซเบอร์ในระดับร้ายแรง หมายถึง ภัยคุกคามที่มีลักษณะการเพิ่มขึ้นอย่างมีนัยสำคัญของการโจมตีระบบคอมพิวเตอร์ คอมพิวเตอร์ หรือข้อมูลคอมพิวเตอร์ โดยมุ่งหมายเพื่อโจมตีโครงสร้างพื้นฐานสำคัญของประเทศและการโจมตีดังกล่าวมีผลทำให้ระบบคอมพิวเตอร์หรือโครงสร้างสำคัญทางสารสนเทศที่เกี่ยวข้องกับการให้บริการของโครงสร้างพื้นฐานสำคัญของประเทศความมั่นคงของรัฐ ความสัมพันธ์ระหว่างประเทศ การป้องกันประเทศ เศรษฐกิจ การสาธารณสุข ความปลอดภัยสาธารณะ หรือความสงบเรียบร้อยของประชาชนเสียหาย จนไม่สามารถทำงานหรือให้บริการได้

(๓) ภัยคุกคามทางไซเบอร์ในระดับวิกฤติ หมายถึง ภัยคุกคามทางไซเบอร์ในระดับวิกฤติที่มีลักษณะ ดังต่อไปนี้

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

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

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

<u>แหล่งที่มา</u>

- 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

- คู่มือการตอบสนองภัยคุกคามทางไซเบอร์สำหรับบริษัทประกันภัย