มหาวิทยาลัยเทคโนโลยีราชมงคลสุวรรณภูมิ

คู่มือการปฏิบัติงานตามมาตรฐานขั้นตอนการปฏิบัติงาน การรับมือภัยคุกคามทางไซเบอร์

รหัสเอกสาร : SOP 202-25

ISSUE : 01

วันที่บังคับใช้ : - 7 มี.ค. 2568

คณบดี/ผู้อำนวยการสถาบัน สำนัก	ผู้ช่วยอธิการบดี/รองอธิการบดี ที่กำกับ
..... (ผู้ช่วยศาสตราจารย์กฤตย์ตนัย ธารารัตนสุวรรณ) ผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ	..... (นายเอกวิศว์ สงเคราะห์) รองอธิการบดี

ผู้อนุมัติ

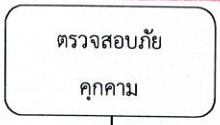
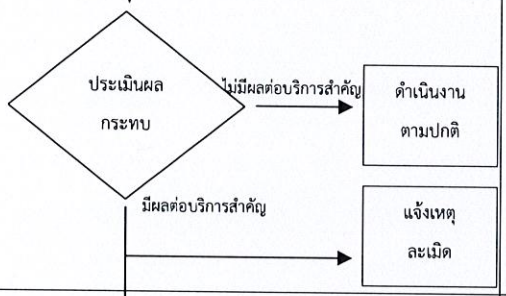
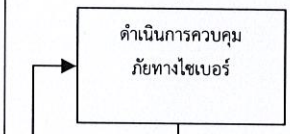
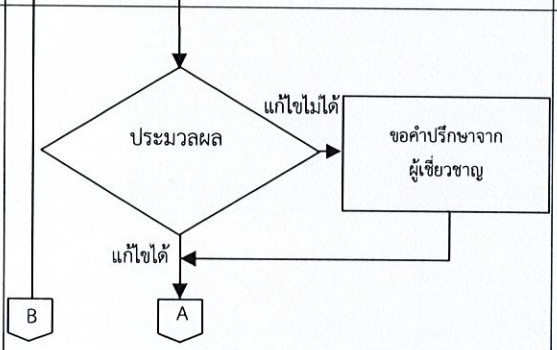
.....
(รองศาสตราจารย์ประมุข อุณหเลขกะ)
อธิการบดีมหาวิทยาลัยเทคโนโลยีราชมงคลสุวรรณภูมิ

1. **วัตถุประสงค์** : 1. เพื่อเป็นแนวทางการปฏิบัติงานของเจ้าหน้าที่ในระดับปฏิบัติการ
   2. เพื่อเป็นกลไกในการเพิ่มประสิทธิภาพการปฏิบัติงานของหน่วยงาน
2. **ขอบข่าย** : เป็นแนวทางในการปฏิบัติงานตามขั้นตอนการรับมือภัยคุกคามทางไซเบอร์
3. **เกณฑ์คุณภาพ** : ไม่มี
4. **เอกสารอ้างอิง** : แผนการรับมือภัยคุกคามทางด้านไซเบอร์
5. **เอกสารประกอบการทำงาน**

ชื่อเอกสารแนบ	รหัสเอกสาร
1. แบบฟอร์ม เอกสาร ก๑ ข้อมูลที่ต้องแจ้ง	FM-SOP 202-19-01
2. แบบฟอร์ม เอกสาร ก๒ แบบรายงานภัยคุกคามทางไซเบอร์	FM-SOP 202-19-02
3. แบบฟอร์ม หมวด ข. ข้อมูลการตรวจพบภัยคุกคามไซเบอร์	FM-SOP 202-19-03
4. แบบฟอร์ม หมวด ค. ข้อมูลการรับมือภัยคุกคาม	FM-SOP 202-19-04
5. แบบฟอร์ม หมวด ง : รายละเอียดภัยคุกคาม	FM-SOP 202-19-05
6. แบบฟอร์ม เอกสาร ก๓ แบบรายงานสรุปภัยคุกคามทางไซเบอร์ในหนึ่งรอบประเมิน	FM-SOP 202-19-06
7. แผนการรับมือภัยคุกคามทางด้านไซเบอร์	FM-SOP 202-19-07
8. ระบบการตรวจสอบภัยคุกคามไซเบอร์รายวัน	FM-SOP 202-19-08

6. **คำจำกัดความ** : **ภัยคุกคามทางไซเบอร์** หมายถึง การกระทำหรือการดำเนินการใด ๆ ผ่านการใช้ระบบสารสนเทศหรือเครือข่าย ที่ก่อให้เกิดผลเสียต่อระบบข้อมูล เครือข่าย และข้อมูลภายใน

7. ขั้นตอนการทำงาน

ลำดับ	ผู้รับผิดชอบ	แผนภูมิสายงาน (Flowchart)	ขั้นตอน/วิธีการดำเนินงาน	ระยะเวลาดำเนินการ	เอกสารที่เกี่ยวข้อง
1	ผู้ใช้บริการและงานเทคโนโลยีสารสนเทศ		1. มีการแจ้งเหตุจากผู้ใช้งาน หรือตรวจจับการคุกคามทางไซเบอร์ได้ จากอุปกรณ์ป้องกันระบบเครือข่าย หรือเครื่องมือต่างๆ 2. ได้รับแจ้งเหตุจากภายนอกหน่วยงาน เช่น สกมช. เป็นต้น	ภายใน 2 ชม.	1. เอกสารแจ้งเหตุการบุกรุก / การโจมตี / บันทึกข้อความ / อีเมล
2	งานเทคโนโลยีสารสนเทศ		ประเมินผลกระทบที่และความเสียหาย หากไม่มีผลต่อบริการสำคัญให้ดำเนินการตามปกติ แต่หากมีผลกระทบต่อบริการสำคัญให้ดำเนินการดังนี้ 1. แจ้งผู้ที่เกี่ยวข้อง 2. แจ้งเหตุละเมิดไปที่ศูนย์รับแจ้งเหตุภัยคุกคามทางไซเบอร์ (สกมช.)	ภายใน 72 ชม.	1. รายงานความเสียหายของระบบเครือข่าย ระบบสารสนเทศ 2. บันทึกข้อความ หรือ เอกสารต่างๆ สำหรับแจ้งข่าวสาร 3. รายงานเหตุภัยคุกคามทางไซเบอร์ (สกมช.) / มหาวิทยาลัย
3	งานเทคโนโลยีสารสนเทศ		ดำเนินการควบคุมภัยคุกคามทางไซเบอร์ ตรวจหาช่องโหว่ โดยอุปกรณ์ตรวจสอบช่องโหว่ระบบเครือข่าย และหาวิธีเพื่อป้องกันการเกิดภัยคุกคามไซเบอร์ในลักษณะเดิม	ภายใน 1 วัน	รายงานวิธีการควบคุมและป้องกัน
4	งานเทคโนโลยีสารสนเทศและหน่วยงานภายนอก		**หากแก้ไขไม่ได้** 1. ติดต่อศูนย์ประสานการสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อขอคำแนะนำหรือขอความช่วยเหลือ **หากแก้ไขได้** 1. ดำเนินการหาวิธีป้องกัน	ภายใน 1 วัน	รายงานการขอความร่วมมือจากหน่วยงานภายนอก และแนวทางการแก้ไข

ลำดับ	ผู้รับผิดชอบ	แผนภูมิสายงาน (Flowchart)	ขั้นตอน/วิธีการดำเนินงาน	ระยะเวลาดำเนินการ	เอกสารที่เกี่ยวข้อง
5	งานเทคโนโลยีสารสนเทศ	B (A) ดำเนินตามกระบวนการกู้คืนระบบ	กู้คืนข้อมูล และระบบที่เสียหาย	ภายใน 1 วัน	1. รายงานการดำเนินการป้องกันภัยคุกคามทางไซเบอร์ 2. รายงานการกู้คืนข้อมูล
6	งานเทคโนโลยีสารสนเทศ	ทดสอระบบ ไม่สมบูรณ์ สมบูรณ์	**กู้คืนระบบสมบูรณ์** ตรวจสอบการทำงานของข้อมูล และระบบโครงสร้างพื้นฐานสำคัญทางสารสนเทศ สามารถทำงานได้สมบูรณ์ เปิดการใช้งานระบบ **กู้คืนระบบไม่สมบูรณ์** ในกรณีที่พบว่าการทำงานไม่สมบูรณ์ หรือข้อมูลสำคัญสูญหายไปจะดำเนินการตรวจสอบไฟล์สำรองข้อมูล และกู้คืนระบบใหม่อีกครั้ง	ภายใน 1 วัน	รายงานการทดสอบระบบ
7	งานเทคโนโลยีสารสนเทศ	เกิดเหตุซ้ำ ติดตามสถานะการทำงานของระบบ	**สถานะปกติ** ติดตามสถานะของระบบ **หากเกิดเหตุซ้ำ** ย้อนกลับไปดำเนินตามกระบวนการกู้คืนระบบ	ภายใน 1 วัน	เอกสารแจ้งเหตุการบุกรุก / การโจมตี / บันทึกข้อความ / อีเมล
8	งานเทคโนโลยีสารสนเทศ	รายงานผลการดำเนินการ	สรุปผลในการรับมือภัยคุกคามทางไซเบอร์ และแจ้งผลการดำเนินงานให้แก่ผู้เกี่ยวข้อง 1. สรุปผลรายงานผู้บังคับบัญชา 2. สรุปผลรายงาน สกมช.	ภายใน 1 วัน	1. รายงานการโจมตี 2. รายงานการกู้คืนข้อมูล 3. รายงานการป้องกัน

1. วัตถุประสงค์

1. เพื่อเป็นแนวทางการปฏิบัติงานของเจ้าหน้าที่ในระดับปฏิบัติการ
2. เพื่อเป็นเครื่องมือในการติดตามและประเมินผลการดำเนินงาน
3. เพื่อเป็นกลไกในการเพิ่มประสิทธิภาพการปฏิบัติงานของหน่วยงาน
4. ลดความเสี่ยงในการเกิดปัญหาที่อาจกระทบต่อการทำงาน

2. ขอบข่าย

การรับมือภัยคุกคามทางไซเบอร์ มหาวิทยาลัยเทคโนโลยีราชมงคลสุวรรณภูมิ (ส่วนกลาง)

3. วิธีปฏิบัติงาน

1.ตรวจสอบเหตุการณ์ด้านความมันคงปลอดภัยจากระบบเฝ้าระวังฯ หากพบเหตุการณ์ด้านความมันคงปลอดภัยที่ผิดปกติ หรือ ได้รับการแจ้งเตือนพบเหตุการณ์ที่ผิดปกติจากหน่วยงานภายนอกให้เริ่มดำเนินการตามกระบวนการทำงาน ดังนี้

1.1 บันทึกข้อมูลเหตุการณ์ด้านความมันคงปลอดภัยที่ผิดปกติที่ได้ตรวจสอบพบหรือได้รับการแจ้งเตือนลงในระบบรายงานฯ

1.2 รวบรวมข้อมูลต่าง ๆ ที่เกี่ยวข้องกับภัยคุกคามที่ตรวจสอบพบ หรือ ได้รับการแจ้งเตือนจากหน่วยงานภายนอกจากอุปกรณ์ด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

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 : มีความเสียงส่งผลกระทบต่อคณะ 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 ตามระดับความเร่งด่วนรายละเอียดดังนี้

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

บันทึกการตรวจสอบระบบเครือข่าย แม่ข่าย Cyber security

กรุณาตรวจสอบระบบก่อน 12.00 น.

ผู้ตรวจสอบต้อง VPN ผ่าน : https://203.158.225.181:4430/ (ใน มทร.)
https://203.158.225.188:4430/ (นอก มทร.)

คู่มือบันทึกการตรวจสอบระบบเครือข่าย แม่ข่าย Cyber security : t.ly/uyNG9

jirawat.p@rmutsb.ac.th Switch account

Not shared

* Indicates required question

ผู้ตรวจสอบระบบ *

Choose

วันที่บันทึกข้อมูล *

ตัวอย่าง : 30/2/2554

MM DD YYYY

/ /

รูปที่ 1 แบบฟอร์มการตรวจสอบและรายงานระบบสารสนเทศ

แบบฟอร์มบันทึกการแก้ไขระบบสารสนเทศ

jirawat.p@rmutsb.ac.th Switch account

* Indicates required question

Email *

Your email

ผู้บันทึก *
ชื่อ นามสกุล

Your answer

ประเภทของปัญหา *

- ○ Server
- ○ Network
- ○ Website

รูปที่ 2 แบบฟอร์มการแก้ไขระบบสารสนเทศ

1. วัตถุประสงค์

1. เพื่อเป็นแนวทางการปฏิบัติงานของเจ้าหน้าที่ในระดับปฏิบัติการ
2. เพื่อเป็นเครื่องมือในการติดตามและประเมินผลการดำเนินงาน
3. เพื่อเป็นกลไกในการเพิ่มประสิทธิภาพการปฏิบัติงานของหน่วยงาน

2. ขอบข่าย การรับมือภัยคุกคามทางไซเบอร์ มหาวิทยาลัยเทคโนโลยีราชมงคลสุวรรณภูมิ (ส่วนกลาง)

3. วิธีปฏิบัติงาน

1 ติดตาม Ticket ในระบบรายงานฯ

2 ตรวจสอบตามระดับความเร่งด่วนในการแก้ไข รายละเอียดดังนี้

2.1 เร่งด่วน : มีความเสี่ยงผลกระทบในวงกว้างทั่วทั้งมหาวิทยาลัย

2.2 มาก : มีความเสี่ยงส่งผลกระทบต่อคณะ ส่วนงาน หน่วยงาน ตั้งแต่ 2 แห่งขึ้นไป

2.3 ปานกลาง : มีความเสี่ยงส่งผลกระทบต่อคณะ ส่วนงาน หน่วยงาน ที่โดนโจมตีเท่านั้น

2.4 ปกติ : ยังมิได้มีผลกระทบเกิดขึ้น แต่หากไม่ดำเนินการจะส่งผลกระทบในอนาคต

3 แบ่งประเภทของการประสานงาน

3.1 กรณีประสานงานภายนอกมหาวิทยาลัย

3.1.1 ตรวจสอบการแก้ไขปัญหาจากระบบหากพบว่าแก้ไขสำเร็จ ทำการบันทึกข้อมูลลงในระบบรายงานฯ

3.1.2 ตรวจสอบการแก้ไขปัญหาจากระบบหากพบว่าแก้ไขไม่สำเร็จ ให้ติดต่อไปยังหน่วยงานถึงปัญหาที่ยังคงอยู่

3.2 กรณีประสานงานภายในมหาวิทยาลัย

3.2.1 ติดตามการแก้ไขปัญหากรณีหน่วยงานแก้ไขสำเร็จ ทำการทดสอบการแก้ไขปัญหาดังกล่าว พร้อมทั้งสอบถามเกี่ยวกับการดำเนินการ

3.2.2 ติดตามการแก้ไขปัญหากรณีหน่วยงานแก้ไขไม่สำเร็จ ให้ทำการติดต่อและให้ความช่วยเหลือไปยังหน่วยงาน กรณีที่ทางหน่วยงานมีการร้องขอ

3.3 กรณีประสานงานภายในสำนักวิทยบริการฯ

3.3.1 ตรวจสอบการแก้ไขปัญหาจากระบบหากพบว่าแก้ไขสำเร็จ ทำการทดสอบการแก้ไขปัญหาดังกล่าว พร้อมทั้งสอบถามเกี่ยวกับการดำเนินการ

3.3.2 ตรวจสอบการแก้ไขปัญหาจากระบบหากพบว่าแก้ไขไม่สำเร็จ ให้ติดต่อผู้ดูแลหากปัญหาที่ยังคงอยู่

3.4 บันทึกข้อมูลลงในระบบรายงานฯ

3.5 ปรับปรุงสถานะของงาน

เอกสาร ก๒ 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[2] ในระดับใด (มาตรา 60)

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

☐ ยังไม่สามารถระบุได้

รูปที่ 1 แบบรายงานภัยคุกคามไซเบอร์

หมวด ข. ข้อมูลการตรวจพบภัยคุกคามไซเบอร์

ข1. วัน เวลา ที่เกิดเหตุภัยคุกคาม

วันที่ : เลือกวันที่ เวลา : โปรดระบุ

วัน เวลา ที่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศทราบเหตุภัยคุกคาม

วันที่ : เลือกวันที่ เวลา : โปรดระบุ

ข2. วัน เวลา ที่แจ้งเหตุภัยคุกคามให้หน่วยงานควบคุมหรือกำกับดูแลทราบ

☐ ยังไม่ได้แจ้ง ☐ แจ้งแล้ว _____

ข3. หมวดหมู่ของภัยคุกคาม (เลือกได้มากกว่า 1 รายการ)

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

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

ข4. ข้อมูลเบื้องต้นเกี่ยวกับระบบคอมพิวเตอร์ คอมพิวเตอร์ บริการ หรือข้อมูลที่ได้รับผลกระทบ:

สถานที่ตั้งของเครื่อง ข้อมูล หรือสินทรัพย์ที่ได้รับผลกระทบ (เช่น จังหวัด ตำบล ตึก ห้อง):
โปรดระบุ

ชื่อผู้ให้บริการเครือข่ายที่ให้บริการแก่ระบบ บริการ หรือข้อมูลที่ได้รับผลกระทบ :
โปรดระบุ

บริการของระบบ ข้อมูล หรือสินทรัพย์ที่ได้รับผลกระทบ (เช่น บริการการโอนเงิน):
โปรดระบุ

ฮาร์ดแวร์ ซอฟต์แวร์ที่ได้รับผลกระทบ (โปรดระบุรายละเอียด เช่น ผู้ผลิตหรือยี่ห้อ รุ่นของเครื่องคอมพิวเตอร์): โปรดระบุรายละเอียด

มีผลกระทบต่อการสื่อสาร (ทางโทรศัพท์ หรือ การใช้งานเครือข่าย): โปรดระบุ

รายละเอียดอื่น ๆ: โปรดระบุ

รูปที่ 2 แบบรายงานภัยคุกคามไซเบอร์(ต่อ)

หมวด ค: ข้อมูลการรับมือภัยคุกคาม

ค1. สถานการณ์หรือการแก้ไขเหตุภัยคุกคาม (เลือกได้มากกว่า 1 รายการ)

- ☐ เพิ่งพบเหตุการณ์
- ☐ อยู่ในขั้นตอนการขอความช่วยเหลือ
- ☐ อยู่ในขั้นตอนการสอบสวน
- ☐ กำลังลุกลาม
- ☐ อยู่ในขั้นตอนการระงับภัย
- ☐ สามารถระงับภัยได้แล้ว
- ☐ รายงานปิดเหตุการณ์ภัยคุกคามแล้ว
- ☐ อื่น ๆ: โปรดระบุ

ค2. สิ่งที่ได้ดำเนินการหรือได้แก้ไขไปแล้ว

- ☐ ยังไม่ได้ดำเนินการแก้ไขใด ๆ
- ☐ ยกเลิกการเชื่อมต่อระบบออกจากเครือข่ายแล้ว
- ☐ ตรวจสอบข้อมูลจราจร (Log) แล้ว
- ☐ ตรวจสอบโปรแกรม (แฟ้ม binaries/.exe) แล้ว
- ☐ กู้คืนกลับมาด้วยระบบหรือข้อมูลสำรองที่ตรวจสอบความถูกต้องแล้ว
- ☐ รายละเอียดการแก้ไขภัยคุกคามที่เกิดขึ้นเพิ่มเติม: โปรดระบุ

ค3. รายละเอียดการรับมือภัยคุกคามอื่น ๆ (ถ้ามี)

โปรดระบุ

รูปที่ 3 แบบรายงานภัยคุกคามไซเบอร์(ต่อ)

ส่วนที่ 2

หมวด ง : รายละเอียดภัยคุกคาม

ง1. ข้อมูลการตรวจจับและการวิเคราะห์

ง1.1 วัน เวลา ที่ผู้โจมตีได้เริ่มต้นเข้าถึงระบบ (System Access)

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

ง1.2 ข้อมูลการพบเห็นเหตุภัยคุกคามทางไซเบอร์

รายละเอียดแหล่งที่มา หรือต้นเหตุของเหตุภัยคุกคาม (เท่าที่ทราบ เช่น คน, ความผิดพลาดของระบบ, ภัยธรรมชาติ, การจู่โจม, ความผิดพลาดจากคนนอกองค์กร):

โปรดระบุ

บุคคล วิธี หรือเครื่องมือที่ตรวจพบภัยคุกคาม (เช่น ผู้ใช้, ผู้ดูแลระบบ, โปรแกรม Anti-virus, IDS, การวิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์, ไม่ทราบ):

โปรดระบุ

รายละเอียดของปัญหาลักษณะคล้ายกันที่หน่วยงานเคยพบมาก่อน (ถ้ามี โปรดระบุรายละเอียด):

โปรดระบุ

ง1.3 รายละเอียดผลกระทบจากเหตุภัยคุกคาม (ระบุผลกระทบที่มีเกิดขึ้นต่อ ระบบ คน หรือข้อมูล)

จำนวนระบบ บริการ หรือสินทรัพย์ที่เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่ได้รับผลกระทบ (โดยประมาณ) : โปรดระบุ

ทรัพย์สินที่สำคัญอื่น ๆ ที่อาจได้รับผลกระทบ: โปรดระบุ

จำนวนผู้ได้รับผลกระทบ (โดยประมาณ): โปรดระบุ

มูลค่าความเสียหาย (โดยประมาณ): โปรดระบุ

ในกรณีที่ข้อมูลที่ระบุตัวบุคคลได้รั่วไหล (หรือถูกขโมย):

จำนวนบุคคลที่เป็นเจ้าของข้อมูล : โปรดระบุ

ชนิดของข้อมูล (เลือกทุกข้อที่ใช่):

☐ ข้อมูลไบโอเมตริกซ์ ☐ ข้อมูลการติดต่อ

☐ ข้อมูลการเงิน ☐ ข้อมูลบุคลากรของรัฐ

☐ หมายเลขบัตรประชาชน ☐ ข้อมูลการติดต่อกับหน่วยงานต่าง ๆ

☐ ข้อมูลทางการแพทย์

☐ อื่น ๆ : โปรดระบุ

จำนวนข้อมูล (Record) ที่ได้รับผลกระทบ: โปรดระบุ

ผลกระทบอื่น ๆ ที่เกิดขึ้น: โปรดระบุ

รูปที่ 4 แบบรายงานภัยคุกคามไซเบอร์(ต่อ)

ง1.4 รายละเอียดของระบบ หรือข้อมูลที่ได้รับผลกระทบ (Information of Affected System)

หมายเลข CVE: โปรดระบุ

ช่องโหว่ที่ถูกใช้จู่โจม: โปรดระบุ

การใช้ระบบหรือเครื่องที่ได้รับผลกระทบเป็นฐานเพื่อจู่โจมขยายผลไปยังระบบหรือเครื่องอื่น: โปรดระบุ

อาการหรือสิ่งผิดปกติ (เลือกได้มากกว่า 1 รายการ)

- ☐ ระบบล่ม
- ☐ รายการข้อมูลจราจรทางคอมพิวเตอร์ที่ผิดปกติ
- ☐ บัญชีผู้ใช้ถูกสร้างขึ้นมาใหม่โดยไม่ทราบสาเหตุ หรือ บัญชีผู้ใช้มีความผิดปกติ
- ☐ การจู่โจมด้วยวิศวกรรมสังคม (Social Engineering) ทั้งที่สำเร็จและไม่สำเร็จ
- ☐ ประสิทธิภาพของระบบด้อยลง (ทั้งที่รู้ว่าเป็นเพราะเหตุภัยคุกคามและที่ไม่รู้สาเหตุ)
- ☐ การเปลี่ยนแปลงใน DNS หรือ กฎของ Router หรือกฎไฟร์วอลล์ โดยไม่ทราบสาเหตุ
- ☐ การยกระดับสิทธิ์การเข้าถึงระบบโดยไม่ทราบสาเหตุ
- ☐ การตรวจพบการทำงานของโปรแกรมหรืออุปกรณ์ Sniffer เพื่อจับการรับส่งข้อมูลภายในเครือข่าย
- ☐ การเข้าใช้งานครั้งสุดท้ายของผู้ใช้ที่ไม่สอดคล้องกับการใช้งานครั้งสุดท้ายที่เกิดขึ้นจริง
- ☐ การแจ้งเตือนจากเครื่องมือตรวจจับการบุกรุก
- ☐ การเข้ามาลาดตระเวน (Probing) หรือการเรียกดู (Browsing) ที่น่าสงสัย
- ☐ รูปแบบการใช้งานที่ผิดปกติ
- ☐ การเปลี่ยนแปลงขนาดไฟล์ไปจากเดิมแบบผิดปกติ
- ☐ ความพยายามที่จะเขียนไฟล์ของระบบ
- ☐ การเปลี่ยนแปลงวันที่ของไฟล์ไปจากเดิมแบบผิดปกติ
- ☐ การแก้ไขหรือลบข้อมูลที่ผิดปกติ
- ☐ การจู่โจมให้เกิดการปฏิเสธการให้บริการ (DOS, DDOS)
- ☐ ไฟล์ใหม่ถูกสร้างขึ้นโดยไม่ทราบสาเหตุ
- ☐ การใช้งานหรือมีกิจกรรมที่เกิดในเวลาที่ผิดปกติ
- ☐ การแก้ไขหน้าเว็บ
- ☐ การสร้างแฟ้มข้อมูล setuid หรือ setgid ใหม่ที่ผิดปกติเกิดขึ้น
- ☐ การเปลี่ยนแปลงในไดเรกทอรีและแฟ้มข้อมูลของระบบปฏิบัติการที่ผิดปกติ
- ☐ การตรวจพบโปรแกรมเจาะระบบ (Crack utility)
- ☐ สิ่งที่ผิดปกติไปจากเดิมอื่น ๆ: โปรดระบุ

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

โปรดระบุ

ง1.6 รายละเอียดอื่น ๆ ที่พบเกี่ยวข้องกับเหตุภัยคุกคาม: โปรดระบุ

ง2. ข้อมูลการระงับ ปราบปราม และฟื้นฟู

ง2.1 รายละเอียดการดำเนินการเพื่อแก้ไขเหตุภัยคุกคาม: โปรดระบุ

ง2.2 การคาดการณ์ความสามารถฟื้นฟู

โปรดระบุรายละเอียดการฟื้นฟู ทรัพยากรที่ต้องใช้และที่ต้องการเพิ่ม และประมาณระยะเวลาการฟื้นฟู

ง3. ข้อมูลกิจกรรมภายหลังการแก้ปัญหา (ถ้ามี)

ง3.1 วัน เวลา ที่เหตุภัยคุกคามสิ้นสุด วันที่: เลือกวันที่ **เวลา:** โปรดระบุ

ง3.2 การดำเนินการเพื่อป้องกันเหตุภัยคุกคามที่คล้ายคลึงกัน: โปรดระบุ

ง3.3 บทเรียนที่ได้จากเหตุภัยคุกคาม: โปรดระบุ

รูปที่ 5 แบบรายงานภัยคุกคามไซเบอร์(ต่อ)

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, จัดเก็บและดูแลรักษาหลักฐานเกี่ยวกับเหตุการณ์ทั้งหมดก่อนเริ่มกระบวนการกู้คืนซึ่งรวมถึงการได้มาของบันทึกการยึดหลักฐานคอมพิวเตอร์ที่ได้มา หรืออุปกรณ์อื่น ๆ เพื่อสนับสนุนการสอบสวน	
5	จำกัดขอบเขต (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์	
6	ดำเนินการสอบสวน (Investigate) สาเหตุและผลกระทบของเหตุการณ์	
7	ทำการกำจัดสาเหตุ (Eradicate the incident)	
7.1	ระบุช่องโหว่ของระบบที่โดนโจมตีและบรรเทาผลกระทบที่เกิดขึ้น	
7.2	กำจัด หรือลบมัลแวร์ และสาเหตุภัยคุกคามอื่นๆ	
7.3	หากมีการตรวจพบว่ามีระบบใหม่ได้รับผลกระทบ (เช่น การติดมัลแวร์ใหม่) ให้ทำซ้ำขั้นตอนการตรวจจับและการวิเคราะห์ภัยคุกคามทางไซเบอร์ (detection and analysis)	
8	เรียกใช้งานกระบวนการกู้คืน (Recovery Process)	
8.1	ระบบที่ได้รับผลกระทบจากภัยคุกคามกลับสู่สถานะพร้อมใช้งาน	
8.2	ยืนยันว่าระบบที่ได้รับผลกระทบกลับมาทำงานได้ตามปกติ	
8.3	หากจำเป็น ให้ดำเนินการติดตามสถานการณ์ต่อไป เพื่อค้นหาเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ที่อาจเกี่ยวข้องในอนาคต	
การดำเนินการภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ (Post-Incident Activity)		
9	จัดทำรายงานการติดตามผล	
10	จัดการประชุมทบทวนบทเรียนที่เกิดจากเหตุการณ์ดังกล่าว	

ตารางที่ 1 ตัวอย่างการตรวจสอบการจัดการณ์เหตุการณ์