

แผนกู้คืนระบบจากภัยพิบัติ

(Disaster Recovery Plan : DR Plan)

สำนักงานปลัดกระทรวงการพัฒนาลังคม
และความมั่นคงของมนุษย์
ประจำปีงบประมาณ พ.ศ. 2569



ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร



แผนกู้คืนระบบจากภัยพิบัติ

(Disaster Recovery Plan : DR Plan)

สำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์

ประจำปีงบประมาณ พ.ศ. 2569



สารบัญ

เรื่อง	หน้า
1. ความเป็นมา.....	1
2. วัตถุประสงค์.....	1
3. ขอบเขตการดำเนินงาน.....	2
4. นิยามศัพท์.....	3
5. โครงสร้างการบริหารจัดการด้าน Disaster Recovery และความรับผิดชอบ.....	4
6. การวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis : BIA).....	5
7. การประเมินความเสี่ยงด้านภัยพิบัติ.....	5
8. การจัดลำดับความสำคัญของระบบสารสนเทศ.....	6
9. เป้าหมายการกู้คืนระบบ (RTO/RPO).....	6
10. การเตรียมความพร้อม.....	7
11. การแก้ปัญหาจากภัยพิบัติ.....	9
12. การกู้คืนและฟื้นฟูระบบ.....	14
13. การแจ้งเหตุ.....	17
14. แนวทางการสื่อสารในภาวะวิกฤต.....	17
15. การประสานงานกับหน่วยงานภายนอก.....	17
16. การติดตามประเมินผล.....	18
ภาคผนวก	



1. ความเป็นมา

สำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ (สป.พม.) มีการนำระบบเทคโนโลยีสารสนเทศและระบบดิจิทัลมาใช้ในการบริหารจัดการ การให้บริการประชาชน และสนับสนุนภารกิจสำคัญของหน่วยงานอย่างต่อเนื่อง โดยระบบสารสนเทศดังกล่าวมีความสำคัญต่อการดำเนินงานขององค์กร หากเกิดเหตุการณ์ภัยพิบัติ เหตุขัดข้องร้ายแรง หรือภัยคุกคามทางไซเบอร์ อาจส่งผลให้ระบบสารสนเทศหยุดชะงัก ข้อมูลสูญหาย หรือไม่สามารถให้บริการได้

ดังนั้น สำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ จึงจัดทำแผนกู้คืนระบบจากภัยพิบัติ (Disaster Recovery Plan : DR Plan) เพื่อใช้เป็นแนวทางในการกู้คืนระบบเทคโนโลยีสารสนเทศ ระบบเครือข่าย ระบบฐานข้อมูล และระบบบริการดิจิทัลของหน่วยงาน ให้สามารถกลับมาให้บริการได้ภายในระยะเวลาที่เหมาะสม ลดผลกระทบต่อการดำเนินงานของหน่วยงานและการให้บริการประชาชน

แผนฉบับนี้จัดทำให้สอดคล้องกับ

1. พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562
2. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
3. ข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ สป.พม.
4. แผนรับมือเหตุภัยคุกคามทางไซเบอร์ของ สป.พม.
5. แผนการสำรองและทดสอบกู้คืนข้อมูลของ สป.พม.
6. แผนเตรียมความพร้อมกรณีฉุกเฉินของ สป.พม.

2. วัตถุประสงค์

2.1 เพื่อกำหนดแนวทางและขั้นตอนในการกู้คืนระบบเทคโนโลยีสารสนเทศเมื่อเกิดเหตุภัยพิบัติหรือเหตุขัดข้องร้ายแรง

2.2 เพื่อให้ระบบสารสนเทศที่สำคัญของ สป.พม. สามารถกลับมาให้บริการได้ภายในระยะเวลาที่กำหนด

2.3 เพื่อลดผลกระทบต่อการดำเนินงานของหน่วยงานและการให้บริการประชาชน

2.4 เพื่อกำหนดบทบาทหน้าที่และความรับผิดชอบของบุคลากรที่เกี่ยวข้องในการดำเนินการกู้คืนระบบ



2.5 เพื่อให้การกู้คืนระบบมีมาตรฐาน สามารถปฏิบัติได้จริง และสอดคล้องกับแผนด้านความมั่นคงปลอดภัยสารสนเทศของหน่วยงาน

2.6 เพื่อใช้เป็นแนวทางในการทดสอบ ทบทวน และปรับปรุงความพร้อมของระบบสำรอง และการกู้คืนระบบอย่างต่อเนื่อง

3. ขอบเขตการดำเนินงาน

3.1 พิจารณาแนวทางเพื่อเตรียมความพร้อมรับภัยพิบัติที่จะเกิดขึ้นกับข้อมูลสารสนเทศและระบบเทคโนโลยีสารสนเทศ และแนวทางการฟื้นฟู โดยแนวทางที่กำหนดขึ้นเป็นการเตรียมความพร้อมเพื่อดำเนินการหลังจากเกิดเหตุการณ์ความเสียหาย ซึ่งมีเนื้อหาครอบคลุมภัยพิบัติที่เกิดจากอัคคีภัย กระแสไฟฟ้า ชัดข้อง/ไฟฟ้าดับ การโจรกรรม การละเมิด และการเข้าถึงโดยมิชอบ อันส่งผลให้คอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย ระบบสารสนเทศ และเครือข่ายหลักเกิดความชำรุดหรือเสียหาย

3.2 กำหนดให้มีการทดสอบ/ประเมิน และปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ 1 ครั้ง เพื่อให้แผนมีความทันสมัยและสามารถใช้งานได้หากเกิดเหตุการณ์ขึ้นจริง

3.3 แผนฉบับนี้ครอบคลุมระบบสารสนเทศ อุปกรณ์ และโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศของ สป.พม. ดังต่อไปนี้

3.3.1 ระบบคอมพิวเตอร์แม่ข่าย (Server)

- Physical Server
- Virtual Machine

3.3.2 ระบบเครือข่ายคอมพิวเตอร์

- Core Switch
- Router
- Firewall
- VPN
- Internet Gateway
- Wireless Controller

3.3.3 ระบบฐานข้อมูล

- Database Server



- File Storage
- Backup Storage

3.3.4 ระบบงานสารสนเทศสำคัญ

- ระบบงานภายในองค์กร
- ระบบบริการประชาชน
- ระบบเว็บไซต์
- ระบบอีเมล
- ระบบจัดเก็บข้อมูลกลาง

3.3.5 ห้อง Data Center และระบบสาธารณูปโภคที่เกี่ยวข้อง

- UPS
- ระบบไฟฟ้าสำรอง
- ระบบควบคุมอุณหภูมิ
- ระบบดับเพลิง
- ระบบควบคุมการเข้าออก

4. นิยามศัพท์

Disaster Recovery (DR) หมายถึง กระบวนการกู้คืนระบบสารสนเทศ ระบบเครือข่าย และข้อมูล ให้สามารถกลับมาดำเนินงานได้หลังเกิดภัยพิบัติหรือเหตุขัดข้องร้ายแรง

Disaster Recovery Site (DR Site) หมายถึง สถานที่หรือระบบสำรองที่ใช้สำหรับดำเนินงานแทนระบบหลักในกรณีที่ระบบหลักไม่สามารถใช้งานได้

Recovery Time Objective (RTO) หมายถึง ระยะเวลาสูงสุดที่ระบบสามารถหยุดให้บริการได้

Recovery Point Objective (RPO) หมายถึง ระยะเวลาสูงสุดของข้อมูลที่ต้องกรยอมรับให้สูญหายได้

Business Continuity หมายถึง ความสามารถของหน่วยงานในการดำเนินภารกิจต่อเนื่องภายหลังเกิดเหตุการณ์ผิดปกติ

Major Incident หมายถึง เหตุการณ์ที่ส่งผลกระทบต่อระบบสารสนเทศหรือบริการสำคัญของหน่วยงานในระดับสูง



5. โครงสร้างการบริหารจัดการด้าน Disaster Recovery และความรับผิดชอบ

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กำหนดให้มีเจ้าหน้าที่ร่วมดำเนินการตามแผนประกอบด้วย

5.1 ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ตำแหน่ง : ผู้อำนวยการแผน DR (DR Director) ทำหน้าที่ อนุมัติการประกาศใช้แผน DR และรายงานผู้บริหารระดับสูง

5.2 ผู้เชี่ยวชาญด้านเทคโนโลยีสารสนเทศและการสื่อสาร ตำแหน่ง : รองผู้อำนวยการแผน DR (Deputy DR Director) ทำหน้าที่ พิจารณาแผน DR สั่งการและกำกับดูแลภาพรวม และรักษาการแทน DR Director เมื่อ DR Director ไม่อยู่ หรือไม่สามารถปฏิบัติหน้าที่ได้

5.3 กลุ่มการพัฒนาระบบเทคโนโลยีและการสื่อสาร (กทส.) ตำแหน่ง : ทีมกู้คืนโครงสร้างพื้นฐาน (Infrastructure Recovery Team) ทำหน้าที่ กู้คืนระบบเครือข่ายและเครื่องแม่ข่าย กู้คืนระบบ Virtualization และตรวจสอบระบบไฟฟ้าและระบบเครือข่าย ประกอบด้วย

- | | |
|----------------------------|--|
| 1) นายพูนพัฒน์ ชันธาโรจน์ | ผู้อำนวยการกลุ่มการพัฒนาระบบเทคโนโลยีและการสื่อสาร |
| 2) จำสับเอกฤทธิเดช แสงแจ่ม | นักวิชาการคอมพิวเตอร์ชำนาญการ |
| 3) นายภูวดล เกตุดี | นักวิชาการคอมพิวเตอร์ปฏิบัติการ |

5.4 กลุ่มการพัฒนาระบบสารสนเทศ (กพส.) ตำแหน่ง : ทีมกู้คืนระบบงาน (Application Recovery Team) ทำหน้าที่ กู้คืนระบบงานและ Application ทดสอบการใช้งานระบบ และประสานงานเจ้าของระบบ ประกอบด้วย

- | | |
|------------------------------|--------------------------------------|
| 1) นางสาวทัศนวรรณ จันทร์อ่อน | ผู้อำนวยการกลุ่มการพัฒนาระบบสารสนเทศ |
| 2) นายศรัณยู สวัสดิ์มงคล | นักวิชาการคอมพิวเตอร์ชำนาญการ |
| 3) นายพลสิทธิ มีไพล่ | นักวิชาการคอมพิวเตอร์ปฏิบัติการ |

5.5 กลุ่มการวิเคราะห์ข้อมูล (กวข.) ตำแหน่ง : ทีมกู้คืนข้อมูล (Data Recovery Team) ทำหน้าที่ กู้คืนฐานข้อมูล ตรวจสอบความถูกต้องของข้อมูล และตรวจสอบความครบถ้วนของข้อมูลหลังการกู้คืน ประกอบด้วย

- | | |
|-------------------------|------------------------------------|
| 1) นางสาวยุภนันท์ สมปาง | ผู้อำนวยการกลุ่มการวิเคราะห์ข้อมูล |
| 2) นายปฏิพัทธ์ ก้อมมะณี | เจ้าพนักงานพัฒนาสังคมปฏิบัติงาน |

5.6 ผู้แทนกองประชาสัมพันธ์ ตำแหน่ง : ทีมสื่อสารองค์กร ทำหน้าที่ แจ้งสถานะเหตุการณ์ สื่อสารผู้ใช้งานและผู้มีส่วนได้ส่วนเสีย

5.7 ผู้แทนกองกฎหมาย ตำแหน่ง : ทีมปรึกษาด้านกฎหมาย ทำหน้าที่ ให้คำปรึกษาด้านกฎหมาย และ PDPA และประสานงานหน่วยงานกำกับดูแล



6. การวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis : BIA)

6.1 ด้านการให้บริการประชาชน

- 1) ไม่สามารถให้บริการผ่านระบบออนไลน์
- 2) การให้บริการล่าช้า
- 3) สูญเสียความเชื่อมั่นจากประชาชน

6.2 ด้านการปฏิบัติงานภายใน

- 1) ไม่สามารถใช้งานระบบงานสำคัญ
- 2) ข้อมูลสูญหาย
- 3) การประสานงานล่าช้า

6.3 ด้านกฎหมายและข้อกำหนด

- 1) เสี่ยงต่อการละเมิด PDPA
- 2) เสี่ยงต่อการไม่ปฏิบัติตามกฎหมายด้านไซเบอร์

6.4 ด้านภาพลักษณ์องค์กร

- 1) เกิดผลกระทบต่อชื่อเสียงของหน่วยงาน
- 2) ลดความเชื่อมั่นจากประชาชนและหน่วยงานภายนอก

7. การประเมินความเสี่ยงด้านภัยพิบัติ

ประเภทภัยพิบัติ	ผลกระทบ	ระดับความเสี่ยง
อัคคีภัย	ห้อง Data Center เสียหาย	สูง
ไฟฟ้าดับ	ระบบหยุดทำงาน	สูง
น้ำท่วม	อุปกรณ์เสียหาย	สูง
Cyber Attack	ระบบถูกเข้ารหัส/ข้อมูลรั่วไหล	สูง
Hardware Failure	ระบบไม่สามารถใช้งานได้	ปานกลาง
Human Error	ข้อมูลสูญหาย	ปานกลาง
Malware/Ransomware	ระบบและข้อมูลถูกทำลาย	สูง
Network Failure	ระบบไม่สามารถเชื่อมต่อได้	ปานกลาง



8. การจัดลำดับความสำคัญของระบบสารสนเทศ

8.1 ระดับวิกฤตสูง (Critical)

- 1) ระบบบริการประชาชน
- 2) ระบบฐานข้อมูลกลาง
- 3) ระบบเครือข่ายหลัก
- 4) ระบบ Firewall/VPN

8.2 ระดับสำคัญมาก (High)

- 1) ระบบอีเมล
- 2) ระบบเว็บไซต์
- 3) ระบบจัดเก็บเอกสาร
- 4) ระบบรายงานข้อมูล

8.3 ระดับปานกลาง (Medium)

- 1) ระบบงานภายในทั่วไป
- 2) ระบบประชุมออนไลน์

8.4 ระดับต่ำ (Low)

- 1) ระบบทดสอบ
- 2) ระบบพัฒนางาน

9. เป้าหมายการกู้คืนระบบ (RTO/RPO)

ระบบ	ระดับความสำคัญ	RTO	RPO
Firewall/VPN	Critical	2 ชั่วโมง	30 นาที
ระบบเครือข่ายหลัก	Critical	4 ชั่วโมง	1 ชั่วโมง
ระบบฐานข้อมูลกลาง	Critical	4 ชั่วโมง	1 ชั่วโมง
ระบบอีเมล	Critical	6 ชั่วโมง	2 ชั่วโมง
ระบบบริการประชาชน	Critical	6 ชั่วโมง	2 ชั่วโมง
เว็บไซต์องค์กร	High	12 ชั่วโมง	4 ชั่วโมง
ระบบเอกสาร	High	24 ชั่วโมง	12 ชั่วโมง
ระบบภายในทั่วไป	Medium	48 ชั่วโมง	24 ชั่วโมง



10. การเตรียมความพร้อม

10.1 การปฏิบัติเพื่อเตรียมรับสถานการณ์จากอัคคีภัย มีดังนี้

- 1) ไม่กระทำการใดๆ อันจะนำไปสู่การเกิดอัคคีภัยในอาคาร
- 2) ศึกษาวิธีการและขั้นตอนการหนีไฟของอาคาร และถือปฏิบัติอย่างเคร่งครัด
- 3) มีระบบดับเพลิงอัตโนมัติ ซึ่งประกอบด้วยอุปกรณ์ตรวจจับควันหรือความร้อนที่ผิดปกติติดตั้งอยู่ในห้องปฏิบัติการศูนย์ข้อมูลสารสนเทศ (Data Center) สป.พม. หากเกิดเพลิงไหม้จะมี Alarm ซึ่งติดตั้งอยู่บริเวณประตูทางเข้าเป็นตัวส่งสัญญาณในลักษณะของแสงและเสียง มีการตรวจสอบความพร้อมของระบบอย่างน้อย 4 เดือน/ครั้ง
- 4) มีคู่มือระบบดับเพลิงด้วยสารสะอาด (NOVEC1230) และปฏิบัติตามหากเกิดเพลิงไหม้
- 5) มีระบบตรวจจับควันความไวสูงติดตั้งภายในห้อง Data Center สป.พม. หากตรวจพบการเปลี่ยนแปลงจะมีการแจ้งเตือนผ่าน SMS และ Line Notification
- 6) มีเครื่องดับเพลิงแบบมือถือชนิดที่ใช้กับอุปกรณ์อิเล็กทรอนิกส์ติดตั้งภายในห้อง Data Center สป.พม. เพื่อการควบคุมเพลิงเบื้องต้น

10.2 การปฏิบัติเพื่อตรวจสอบสภาพแวดล้อมของห้อง Data Center สป.พม. มีดังนี้

- 1) มีการตรวจสอบสภาพแวดล้อมภายในห้องและระบบควบคุมอุณหภูมิ/ความชื้น โดยอุณหภูมิภายในห้อง Data Center สป.พม. จะต้องประมาณ 20 - 25 องศาเซลเซียส และความชื้นประมาณ 40 - 50 เปอร์เซ็นต์ อย่างน้อยสัปดาห์ละ 1 ครั้ง
- 2) มีการตรวจสอบระบบไฟฟ้าอย่างน้อยสัปดาห์ละ 1 ครั้ง

10.3 การปฏิบัติเพื่อเตรียมรับสถานการณ์ที่เกิดจากระบบไฟฟ้าขัดข้อง มีดังนี้

- 1) มีการติดตั้งระบบสำรองและปรับแรงดันไฟฟ้าอัตโนมัติ (UPS) ให้กับเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายคอมพิวเตอร์ภายในห้อง Data Center สป.พม. ซึ่งระบบดังกล่าว ควรสำรองไฟฟ้าเพื่อใช้งานได้นานอย่างน้อย 1 ชั่วโมง และอยู่ในสภาพพร้อมใช้งานเสมอ
- 2) เปิดเครื่องสำรองและปรับแรงดันไฟฟ้าอัตโนมัติตลอดเวลาในการใช้งานเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายคอมพิวเตอร์ภายในห้อง Data Center สป.พม.
- 3) มีการติดตั้งไฟฉุกเฉินเพื่อให้แสงสว่างเมื่อเกิดไฟฟ้าดับ เพื่อเจ้าหน้าที่จะได้เข้าไปแก้ไขปัญหาได้สะดวก
- 4) มีการตรวจสอบความพร้อมของระบบไฟฟ้าอย่างน้อย 6 เดือน/ครั้ง



10.4 การปฏิบัติเพื่อป้องกันการโจรกรรม มีดังนี้

- 1) มีการติดตั้งระบบควบคุมการเข้า - ออกห้อง Data Center สป.พม. ทั้งระบบ Access Control และ Access Alarm
- 2) มีการบันทึกการเข้า - ออกห้อง Data Center สป.พม. โดยห้ามบุคคลที่ไม่มีหน้าที่เกี่ยวข้องเข้าไปในห้อง Data Center สป.พม. หรือหากมีความจำเป็น จะต้องได้รับอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
- 3) มีการติดตั้งกล้องวงจรปิดที่ห้อง Data Center สป.พม.
- 4) มีระบบควบคุมการเข้า - ออกห้อง Data Center สป.พม. ในวันหยุดหรือนอกเวลาราชการ

10.5 การปฏิบัติเพื่อป้องกันการละเมิดระบบสารสนเทศ มีดังนี้

- 1) มีการติดตั้งอุปกรณ์รักษาความปลอดภัยของเครือข่าย เช่น Firewall ในส่วนต่าง ๆ ของเครือข่าย กำหนดค่าและดำเนินการตรวจสอบข้อมูลต่างๆ (Log) ของอุปกรณ์ Firewall และ IDS/IPS
- 2) มีการติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์สำหรับเครื่องคอมพิวเตอร์แม่ข่าย และลูกข่ายที่มีการเข้าถึงเครือข่าย
- 3) ดำเนินการตามนโยบายที่เกี่ยวข้อง ดังนี้
 - ประกาศสำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ เรื่อง ใช้งานเครือข่ายคอมพิวเตอร์และอินเทอร์เน็ต
 - นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของสำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ พ.ศ. 2569

10.6 การปฏิบัติเพื่อป้องกันการโจรกรรมข้อมูล มีดังนี้

- 1) มีการณรงค์ ส่งเสริม ให้ความรู้กับผู้ใช้งานในการปฏิบัติตนเพื่อป้องกันการถูกโจรกรรมข้อมูล
- 2) มีการติดตั้งโปรแกรมป้องกันไวรัส และ Patch ทุกครั้งที่เจ้าของผลิตภัณฑ์อัปเดต
- 3) มีการติดตั้ง Patch ของระบบปฏิบัติการทุกสัปดาห์
- 4) เปลี่ยนรหัสผ่านตามข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของสำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ หรือทุก 6 เดือน
- 5) มีการกำหนดสิทธิ์ผู้ใช้งานและทบทวนสิทธิ์ผู้ใช้งานอย่างสม่ำเสมอ
- 6) ผู้มีสิทธิ์เข้าถึงระบบต้องเข้าผ่านระบบภายใน หรือ VPN ตามข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของสำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์



- 7) ทำการสำรองข้อมูลระบบฐานข้อมูล ตามแผนการสำรองและทดสอบกู้คืนข้อมูล
- 8) จัดเตรียมอุปกรณ์และเครื่องมือที่จำเป็น สำหรับเตรียมพร้อมรับภัยพิบัติที่จะเกิดขึ้นต่อระบบเทคโนโลยีสารสนเทศของหน่วยงาน ในกรณีระบบสารสนเทศหรือระบบเครือข่ายคอมพิวเตอร์ เกิดขัดข้องใช้งานไม่ได้ โดยมีการเตรียมอุปกรณ์ เช่น
 - แผ่นติดตั้งระบบปฏิบัติการ/ระบบเครือข่าย/ระบบงานที่สำคัญ
 - แผ่นสำรองข้อมูลและระบบงานที่สำคัญ
 - แผ่นโปรแกรม Antivirus
 - แผ่น Driver อุปกรณ์ต่างๆ
 - เอกสารที่เกี่ยวข้อง เช่น คู่มือในการติดตั้ง
 - กู้คืนระบบสารสนเทศและระบบเครือข่ายคอมพิวเตอร์หลัก รายการซอฟต์แวร์และฮาร์ดแวร์ รายละเอียดการบันทึกค่าต่างๆ ในการติดตั้งอุปกรณ์ที่จำเป็น ผังเครือข่าย เป็นต้น ทั้งนี้ ให้เก็บแยกไว้ต่างหากจากห้อง Data Center สป.พม.
- 9) กำหนดรายละเอียดการจัดหาเครื่องคอมพิวเตอร์/อุปกรณ์ และติดตั้งซอฟต์แวร์ใหม่ เพื่อทดแทนเครื่องเดิมที่เสียหาย ในกรณีที่เครื่องคอมพิวเตอร์/อุปกรณ์เสียหาย ให้ทำการจัดหาเครื่องคอมพิวเตอร์/อุปกรณ์ใหม่มาทดแทนภายในระยะเวลา 15 วันทำการ โดยกำหนดให้มีคุณสมบัติของเครื่อง ให้เทียบเท่าหรือสูงกว่าเครื่องคอมพิวเตอร์/อุปกรณ์เดิมที่เสียหาย หลังจากนั้นให้ทำการติดตั้งซอฟต์แวร์ระบบสารสนเทศและระบบฐานข้อมูลให้เรียบร้อยภายในเวลา 3 วันทำการ
- 10) หลังจากการกู้คืนระบบเสร็จสมบูรณ์แล้ว ให้ผู้มีหน้าที่ดูแลรับผิดชอบระบบงานสารสนเทศที่ได้กู้คืน ทำการตรวจสอบความถูกต้องอีกครั้ง

11. การแก้ปัญหาจากภัยพิบัติ

11.1 การปฏิบัติเพื่อแก้ไขปัญหาจากสถานการณ์อัคคีภัย มีดังนี้

- 1) ตัดระบบจ่ายไฟ ในกรณีไฟไหม้ ให้ใช้น้ำยาดับเพลิงฉีดควบคุมเพลิงโดยเร็ว (ในกรณีที่ไม่ได้เป็นระบบอัตโนมัติ) เปิดสัญญาณเตือนภัย และปฏิบัติตามแผนการซักซ้อมการหนีไฟอย่างเคร่งครัด
- 2) รีบขนย้ายอุปกรณ์ที่จำเป็นไปไว้ในที่ปลอดภัย
- 3) ประสานขอความช่วยเหลือกับบริษัทที่รับผิดชอบดูแลเครื่องคอมพิวเตอร์แม่ข่ายหรือผู้เชี่ยวชาญระบบเครือข่ายโดยเร็วที่สุด หากพบว่ามีอุปกรณ์ด้านฮาร์ดแวร์เสีย ให้รีบหาอุปกรณ์สำรองมาเปลี่ยนโดยเร็วที่สุด
- 4) รายงานข้อเท็จจริงการเกิดปัญหาและผลการแก้ไขให้ผู้บังคับบัญชาทราบ



11.2 การปฏิบัติเพื่อแก้ไขปัญหาที่เกิดจากระบบไฟฟ้าขัดข้อง มีดังนี้

- 1) กรณีไฟฟ้าดับ/ไฟฟ้าตก ให้ปิดเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย โดยพิจารณาตามลำดับความสำคัญของการให้บริการ ระยะเวลาที่ไฟฟ้าดับ และประสิทธิภาพของเครื่องสำรองไฟฟ้า
- 2) ประสานขอข้อมูลสาเหตุของไฟฟ้าดับ และระยะเวลาดำเนินการแก้ไข
- 3) รายงานข้อเท็จจริงการเกิดปัญหาและผลการแก้ไขให้ผู้บังคับบัญชาทราบ

11.3 การปฏิบัติเพื่อแก้ไขปัญหาที่เกิดจากระบบควบคุมอุณหภูมิ/ความชื้นขัดข้อง มีดังนี้

- 1) กรณีระบบควบคุมอุณหภูมิ/ความชื้นขัดข้อง จะต้องตัดการเชื่อมต่อระบบเครือข่าย โดยการปิดเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายตามลำดับความสำคัญ
- 2) จัดสถานที่และสภาพแวดล้อมให้มีการถ่ายเทอากาศ ให้เครื่องคอมพิวเตอร์แม่ข่ายสามารถทำงานได้เป็นปกติ
- 3) ติดต่อประสานขอความช่วยเหลือกับบริษัทที่รับผิดชอบดูแลระบบควบคุมอุณหภูมิ/ความชื้น เพื่อดำเนินการแก้ไขโดยเร็วที่สุด
- 4) รายงานข้อเท็จจริงการเกิดปัญหาและผลการแก้ไขให้ผู้บังคับบัญชาทราบ

11.4 การปฏิบัติเพื่อแก้ไขปัญหาที่เกิดจากการละเมิดระบบสารสนเทศ มีดังนี้

- 1) หากพบว่ามี การบุกรุกจากภายในระบบ ให้ตรวจสอบแหล่งกระทำผิด ระงับและปิดกั้นการเชื่อมต่อเครือข่าย หากผู้ละเมิด แจ้งเตือนให้ผู้รับผิดชอบระบบอื่นๆ ที่ได้รับผลกระทบทราบ ตรวจสอบความเสียหายของระบบที่ถูกละเมิด ปรับแก้ไข รายงานผู้บังคับบัญชา และลงโทษตามประกาศสำนักงานปลัดกระทรวงการพัฒนาศักยภาพและความมั่นคงของมนุษย์ เรื่อง การใช้งานเครือข่ายคอมพิวเตอร์และอินเทอร์เน็ต พ.ศ. 2553 (ประกาศ ณ วันที่ 21 กรกฎาคม 2553) ในความผิดที่ไม่ร้ายแรง ส่วนกรณีที่เกิดความเสียหายร้ายแรงแก่ทางราชการ หรือเป็นไปตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม ให้ลงโทษทางกฎหมาย
- 2) หากพบว่ามี การบุกรุกจากภายนอก ระบบ ให้ประสานหน่วยงานที่เกี่ยวข้องหาแหล่งกระทำผิด ระงับและปิดกั้นการเข้าถึงระบบทุกกรณี โดยการกำหนดค่าที่อุปกรณ์ Router หรือ Firewall แจ้งเตือนให้ผู้รับผิดชอบระบบอื่นๆ ที่ได้รับผลกระทบทราบ ตรวจสอบความเสียหายของระบบที่ถูกละเมิด แก้ไขจุดอ่อนที่เป็นสาเหตุ รายงานผู้บังคับบัญชา ดำเนินการตามกฎหมายกรณีที่เกิดความเสียหายร้ายแรงแก่ทางราชการ หรือเป็นไปตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม (ถ้าสามารถดำเนินการได้)



3) หากพบการแพร่กระจายของไวรัสคอมพิวเตอร์ ให้ดำเนินการตรวจสอบและแยกแหล่งแพร่กระจายของไวรัสออกจากเครือข่ายหลัก โดยระงับการเชื่อมต่อเครือข่ายของเครื่องคอมพิวเตอร์ที่ตรวจพบ ดำเนินการตรวจสอบและแก้ไขข้อบกพร่องที่เป็นสาเหตุ เช่น การ Update Patch หรือ Service Pack ของระบบปฏิบัติการ การ Update Virus Signature และการ Scan Malware

11.5 กรณีที่ห้อง Data Center สป.พม. ไม่สามารถให้บริการได้ ต้องมีการเตรียมจัดหาระบบศูนย์สำรองระบบเทคโนโลยีสารสนเทศ (Disaster Recovery Site : DR-Site) โดยต้องจัดหาครุภัณฑ์คอมพิวเตอร์ที่มีคุณลักษณะที่จำเป็น ประกอบด้วย

1) เครื่องคอมพิวเตอร์แม่ข่าย จำนวน 4 เครื่อง โดยมีคุณลักษณะพื้นฐาน ดังนี้

- มีหน่วยประมวลผลกลาง (CPU) แบบ 14 แกนหลัก (14 core) หรือดีกว่า สำหรับคอมพิวเตอร์แม่ข่าย (Server) โดยเฉพาะ และมีความเร็วสัญญาณนาฬิกาพื้นฐานไม่น้อยกว่า 2.2 GHz จำนวนไม่น้อยกว่า 2 หน่วย
- หน่วยประมวลผลกลาง (CPU) รองรับการประมวลผลแบบ 64 bit มีหน่วยความจำแบบ Cache Memory ไม่น้อยกว่า 18 MB
- มีหน่วยความจำหลัก (RAM) ชนิด ECC DDR4 หรือดีกว่า ขนาดไม่น้อยกว่า 192 GB
- สนับสนุนการทำงาน RAID ไม่น้อยกว่า RAID 0, 1, 5
- มีหน่วยจัดเก็บข้อมูล (Hard Drive) ชนิด SCSI หรือ SAS ที่มีความเร็วรอบไม่น้อยกว่า 10,000 รอบต่อนาที หรือ ชนิด Solid State Drive หรือดีกว่า และมีความจุไม่น้อยกว่า 600 GB จำนวนไม่น้อยกว่า 4 หน่วย
- มี DVD-ROM หรือดีกว่า แบบติดตั้งภายใน (Internal) หรือภายนอก (External) จำนวน 1 หน่วย
- มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ 10/100/1000 Base-T หรือดีกว่า จำนวนไม่น้อยกว่า 2 ช่อง
- มีจอภาพแบบ LED หรือดีกว่า ขนาดไม่น้อยกว่า 21 นิ้ว จำนวน 1 หน่วย
- มี Power Supply แบบ Redundant หรือ Hot Swap จำนวน 2 หน่วย



2) อุปกรณ์สำหรับจัดเก็บข้อมูลแบบภายนอก (External Storage) จำนวน 1 เครื่อง โดยมีคุณลักษณะพื้นฐาน ดังนี้

- เป็นอุปกรณ์ที่ทำหน้าที่จัดเก็บข้อมูลแบบภายนอก (External Storage) ซึ่งสามารถทำงานในระบบ SAN (Storage Area Network) ได้
- มีส่วนควบคุมอุปกรณ์ (Controller) แบบ Dual Controller มี Cache memory ของระบบรวมไม่น้อยกว่า 16 GB
- มีหน่วยจัดเก็บข้อมูล (Hard Drive) ชนิด SATA หรือ SAS หรือดีกว่า ขนาดความจุไม่น้อยกว่า 900 GB และมีความเร็วรอบไม่น้อยกว่า 10,000 รอบต่อนาที จำนวนไม่น้อยกว่า 24 หน่วย
- สามารถทำงาน แบบ Raid ไม่น้อยกว่า Raid 0, 1, 5

3) อุปกรณ์ป้องกันเครือข่าย (Next Generation Firewall) จำนวน 1 เครื่อง โดยมีคุณลักษณะพื้นฐาน ดังนี้

- เป็นอุปกรณ์ Firewall ชนิด Next Generation Firewall แบบ Appliance
- มี Firewall Throughput ไม่น้อยกว่า 25 Gbps
- มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ 10/100/1000 Base-T หรือดีกว่า จำนวนไม่น้อยกว่า 8 ช่อง
- สามารถตรวจสอบและป้องกันการบุกรุกรูปแบบต่างๆ ดังนี้ Syn Flood, UDP Flood, ICMP Flood, IP Address Spoofing, Port Scan, DoS or DDoS, Teardrop Attack, Land Attack, IP Fragment, ICMP Fragment ได้เป็นอย่างดี
- สามารถทำการกำหนด IP Address และ Service Port แบบ Network Address Translation (NAT) และ Port Address Translation (PAT) ได้
- สามารถทำงานลักษณะ Transparent Mode ได้
- สามารถ Routing แบบ Static, Dynamic Routing ได้
- มี Power Supply แบบ Redundant หรือ Hot Swap จำนวน 2 หน่วย
- สามารถบริหารจัดการอุปกรณ์ผ่านมาตรฐาน HTTPS หรือ SSH ได้เป็นอย่างดี
- สามารถเก็บและส่งรายละเอียด ตลอดจนตรวจสอบการใช้งาน (Logging/Monitoring) ในรูปแบบ Syslog ได้
- สามารถใช้งานตามมาตรฐาน IPv6 ได้



4) อุปกรณ์กระจายสัญญาณ (L3 Switch) ขนาด 24 ช่อง จำนวน 1 เครื่อง โดยมีคุณลักษณะพื้นฐาน ดังนี้

- มีลักษณะการทำงานไม่น้อยกว่า Layer 3 ของ OSI Model
- สามารถค้นหาเส้นทางเครือข่ายโดยใช้โปรโตคอล (Routing Protocol) RIPv2, OSPF ได้เป็นอย่างดี
- มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ 10/100/1000 Base-T หรือดีกว่า จำนวนไม่น้อยกว่า 24 ช่อง
- มีช่องสำหรับรองรับการเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ 1/10 Gbps (SFP/SFP+) จำนวนไม่น้อยกว่า 2 ช่อง
- มีสัญญาณไฟแสดงสถานะการทำงานของช่องเชื่อมต่อระบบเครือข่ายทุกช่อง
- รองรับ Mac Address ได้ไม่น้อยกว่า 16,000 Mac Address
- สามารถบริหารจัดการอุปกรณ์ผ่านทางโปรแกรม Web Browser ได้
- สามารถส่งข้อมูล Log File ในรูปแบบ Syslog ได้เป็นอย่างดี
- สามารถใช้งานตามมาตรฐาน IPv6 ได้

5) อุปกรณ์กระจายสัญญาณ (L2 Switch) ขนาด 24 ช่อง จำนวน 1 เครื่อง โดยมีคุณลักษณะพื้นฐาน ดังนี้

- มีลักษณะการทำงานไม่น้อยกว่า Layer 2 ของ OSI Model
- มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ 10/100/1000 Base-T หรือดีกว่า จำนวนไม่น้อยกว่า 24 ช่อง
- มีสัญญาณไฟแสดงสถานะการทำงานของช่องเชื่อมต่อระบบเครือข่ายทุกช่อง
- รองรับ Mac Address ได้ไม่น้อยกว่า 16,000 Mac Address
- สามารถบริหารจัดการอุปกรณ์ผ่านทางโปรแกรม Web Browser ได้
- สามารถส่งข้อมูล Log File ในรูปแบบ Syslog ได้เป็นอย่างดี
- สามารถใช้งานตามมาตรฐาน IPv6 ได้



6) เช่าพื้นที่ตู้ Rack สำหรับวางระบบคอมพิวเตอร์ (Rack Data Center Co-location)

ขนาด 42U โดยมีคุณลักษณะพื้นฐาน ดังนี้

- มีหมายเลข Public IP Address รุ่น 4 (IPv4) จำนวนไม่น้อยกว่า 4 หมายเลข
- มีหมายเลข Public IP Address รุ่น 6 (IPv6) จำนวนไม่น้อยกว่า 1,000 หมายเลข
- มีเต้าเสียบไฟฟ้าจำนวนไม่น้อยกว่า 16 เต้าเสียบ
- มีช่องเชื่อมต่อระบบเครือข่ายพร้อมใช้งานระบบอินเทอร์เน็ต แบบ 10/100 Base-T

หรือดีกว่า จำนวนไม่น้อยกว่า 4 ช่อง

- มีระบบกล้องวงจรปิด พร้อมระบบบันทึกภาพ ระบบควบคุมประตูเข้า - ออก (Access Control) ระบบไฟฟ้าสำรอง ระบบปรับอากาศและควบคุมความชื้น ระบบตรวจจับควันไฟ ระบบดับเพลิง และระบบตรวจจับน้ำรั่วซึม

12. การกู้คืนและฟื้นฟูระบบ

12.1 ขั้นตอนการกู้คืนระบบจากภัยพิบัติ

ระยะที่ 1 การประเมินสถานการณ์

- ตรวจสอบประเภทและขอบเขตความเสียหาย
- ตรวจสอบระบบที่ได้รับผลกระทบ
- ประเมินความพร้อมของระบบสำรอง
- บันทึกเหตุการณ์ทั้งหมด

ระยะที่ 2 การควบคุมความเสียหาย

- ตัดการเชื่อมต่อระบบที่ได้รับผลกระทบ
- ป้องกันการแพร่กระจายของมัลแวร์
- แยกระบบที่ถูกโจมตีออกจากเครือข่าย
- ปิดบริการที่ไม่จำเป็น

ระยะที่ 3 การกู้คืนระบบโครงสร้างพื้นฐาน

- เปิดใช้งานระบบไฟฟ้าสำรอง
- กู้คืนระบบเครือข่ายหลัก
- กู้คืนระบบ Firewall/VPN
- กู้คืนระบบ Server
- ตรวจสอบระบบ Virtual Machine



ระยะที่ 4 การกู้คืนข้อมูลและระบบงาน

- กู้คืนฐานข้อมูลจาก Backup ล่าสุด
- ตรวจสอบความถูกต้องของข้อมูล
- กู้คืนระบบ Application
- ทดสอบการใช้งานระบบ

ระยะที่ 5 การทดสอบและเปิดให้บริการ

- ทดสอบการเชื่อมต่อระบบ
- ทดสอบการใช้งานโดยเจ้าของระบบ
- เปิดให้บริการตามลำดับความสำคัญ
- ฝ้าระวังระบบอย่างใกล้ชิด

ระยะที่ 6 การสรุปผลหลังเหตุการณ์

- วิเคราะห์สาเหตุ
- ประเมินผลกระทบ
- จัดทำรายงานสรุป
- ปรับปรุงมาตรการป้องกัน

12.2 ขั้นตอนการกู้คืนระบบเครือข่าย

1) ระบบเครือข่ายหลัก

- ตรวจสอบสถานะอุปกรณ์เครือข่าย
- ตรวจสอบระบบไฟฟ้าและ UPS
- เปิดใช้งาน Core Switch
- เปิดใช้งาน Router และ Internet Gateway
- ตรวจสอบเส้นทางการเชื่อมต่อ
- ทดสอบการเชื่อมต่อภายในและภายนอก

2) ระบบ Firewall/VPN

- Restore Configuration
- ตรวจสอบ Security Policy
- ตรวจสอบ VPN Tunnel
- ทดสอบการเชื่อมต่อจากภายนอก



3) ระบบ Wireless

- เปิดใช้งาน Wireless Controller
- ตรวจสอบ Access Point
- ทดสอบการเชื่อมต่อผู้ใช้งาน

12.3 ขั้นตอนการกู้คืนฐานข้อมูลและข้อมูลสำรอง

1) ขั้นตอนการกู้คืนข้อมูล

- ตรวจสอบ Backup ล่าสุด
- ตรวจสอบความสมบูรณ์ของไฟล์ Backup
- เตรียมพื้นที่จัดเก็บข้อมูล
- Restore Database
- ตรวจสอบความถูกต้องของข้อมูล
- ทดสอบการเชื่อมต่อ Application

2) หลักเกณฑ์การใช้ Backup

- ใช้ Backup ที่สมบูรณ์ล่าสุด
- ต้องผ่านการตรวจสอบ Malware ก่อนใช้งาน
- ต้องเก็บ Log การกู้คืนข้อมูล

3) การตรวจสอบหลังการกู้คืน

- ตรวจสอบความครบถ้วนของข้อมูล
- ตรวจสอบสิทธิ์ผู้ใช้งาน
- ตรวจสอบความถูกต้องของ Transaction
- ตรวจสอบการทำงานร่วมกับระบบอื่น

12.4 ขั้นตอนการกู้คืนระบบรักษาความมั่นคงปลอดภัยไซเบอร์

1) การกู้คืนหลังถูกโจมตีทางไซเบอร์

- แยกระบบที่ติดมัลแวร์ออกจากเครือข่าย
- ตรวจสอบ IOC (Indicators of Compromise)
- สแกน Malware
- เปลี่ยนรหัสผ่านผู้ดูแลระบบ
- Patch ช่องโหว่
- Restore ระบบจาก Backup ที่ปลอดภัย
- ตรวจสอบ Log ย้อนหลัง



13. การแจ้งเหตุ

กรณีเกิดเหตุภัยคุกคามทางไซเบอร์ที่มีนัยสำคัญ ให้ดำเนินการตาม Incident Response Plan และแจ้งสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) และ ThaiCERT หากเป็นกรณีข้อมูลส่วนบุคคลรั่วไหลสำนักงานคุ้มครองข้อมูลส่วนบุคคล

14. แนวทางการสื่อสารในภาวะวิกฤต

14.1 การสื่อสารภายใน

- แจ้งผู้บริหารระดับสูง
- แจ้งเจ้าหน้าที่ผู้เกี่ยวข้อง
- รายงานสถานะทุก 2 ชั่วโมง หรือเมื่อมีความคืบหน้า

14.2 การสื่อสารกับผู้ใช้งาน

- แจ้งสถานะระบบผ่านเว็บไซต์
- แจ้งผ่านอีเมล/Line Official
- แจ้งระยะเวลาคาดการณ์การกู้คืน

14.3 การสื่อสารกับสาธารณะ

ให้กองประชาสัมพันธ์เป็นผู้ดำเนินการสื่อสารเพียงหน่วยงานเดียว เพื่อป้องกันข้อมูลคลาดเคลื่อน โดยต้องส่งข้อมูลการสื่อสารให้แก่เจ้าหน้าที่สายด่วน 1300 สำหรับให้ข้อมูลแก่ประชาชน

15. การประสานงานกับหน่วยงานภายนอก

หน่วยงาน	บทบาท
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)	ให้คำปรึกษาและรับแจ้งเหตุ
ThaiCERT	สนับสนุนด้าน Incident Response
สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล	รับแจ้งเหตุข้อมูลรั่วไหล
ผู้ให้บริการอินเทอร์เน็ต	สนับสนุนโครงข่ายสื่อสาร
ผู้ให้บริการระบบ/Software	สนับสนุนด้านเทคนิค
ตำรวจไซเบอร์	รับแจ้งความและตรวจสอบ



16. การติดตามประเมินผล

16.1 ตรวจสอบจากเอกสารรายงานการบำรุงรักษาว่ามีการดำเนินงานครบถ้วนหรือไม่ ในกรณีที่มีปัญหาเกิดขึ้นจะต้องแสดงรายละเอียดเกี่ยวกับปัญหาและวิธีการแก้ปัญหา โดยที่เอกสารดังกล่าวจะต้องผ่านการตรวจสอบจากเจ้าหน้าที่ผู้รับผิดชอบ

16.2 ตรวจสอบอุปกรณ์ที่จำเป็นที่ได้จัดเตรียมไว้สำหรับเตรียมพร้อมรับภัยพิบัติที่จะเกิดขึ้นว่ามีความครบถ้วนหรือไม่ โดยจัดทำเป็นบันทึกผลการตรวจสอบ ซึ่งแสดงให้เห็นถึงผลการดำเนินงานในเรื่องดังกล่าว เช่น วันที่ทำการตรวจสอบ เอกสารหลักฐาน/ซอฟต์แวร์ที่ควรจัดเตรียม เป็นต้น

16.3 ตรวจสอบระบบควบคุมการเข้า - ออกห้อง Data Center สป.พม. ในวันหยุดหรือนอกเวลาราชการ ว่าได้ดำเนินการครบถ้วนหรือไม่ หากพบว่าไม่เป็นไปตามแนวทางที่กำหนด ให้จัดทำเอกสารรายงานต่อผู้รับผิดชอบในเรื่องดังกล่าว เพื่อดำเนินการแก้ไขต่อไป

16.4 ในกรณีที่เกิดปัญหาและดำเนินการแก้ไขแล้ว จะต้องตรวจสอบว่าได้ดำเนินการแก้ไขปัญหานั้นหรือไม่ โดยการตรวจสอบจากเอกสารรายงานข้อเท็จจริงการเกิดปัญหาและผลการแก้ไขให้ผู้บังคับบัญชาทราบ

16.5 สรุปผลการดำเนินงานรายปี โดยการวิเคราะห์ผลการปฏิบัติงานให้ผู้บังคับบัญชาได้รับทราบ มีประเด็นต่างๆ อย่างน้อย ดังนี้

- สรุปผลการดำเนินงาน
- ปัญหาอุปสรรคและวิธีการแก้ไข (ถ้ามี)
- ข้อเสนอแนะ



ภาคผนวก



ตารางแสดงรายละเอียดระบบงานสารสนเทศและข้อมูลที่ทำกรสำรวจ
ภายใต้แผนการสำรวจและทดสอบภูคินข้อมูล สป.พม.
ประจำปีงบประมาณ พ.ศ. 2569

ตารางแสดงรายละเอียดระบบงานสารสนเทศและข้อมูลที่ใช้การสำรอง
ภายใต้แผนการสำรองและทดสอบกู้คืนข้อมูล สป.พม. ประจำปีงบประมาณ พ.ศ. 2569

ที่	ชื่อระบบ	Domain Name	Frequency (ความถี่ในการสำรอง)	At Time	สื่อที่ใช้สำรอง	ผู้รับผิดชอบ			หน่วยงาน เจ้าของระบบ
						กทส.	กพส.	กวช.	
1	เครื่องบันทึกการลงเวลา	-	Daily	23.30	- Backup server - NAS	จ.ส.อ.ฤทธิเดช แสงแจ่ม	-	-	ศทส.
2	ระบบเยียวยาผู้ได้รับผลกระทบ จากเหตุการณ์ชายแดนใต้	4southern.m-society.go.th	Daily	00.30	- Backup server - NAS	จ.ส.อ.ฤทธิเดช แสงแจ่ม	นายอัศราวุฒิ ต่อโมกข์ นายศรัณยู สวัสดิ์มงคล	-	กตร.
3	ระบบทะเบียนพัสดุ (ใหม่)	asset.m-society.go.th	Daily	01.30	- Backup server - NAS	จ.ส.อ.ฤทธิเดช แสงแจ่ม	นายศรัณยู สวัสดิ์มงคล นายพลสิทธิ มีไปล์	-	กก.
4	ระบบสารบรรณอิเล็กทรอนิกส์ (document.m-society.go.th)	app5.m-society.go.th	Monthly	04.30	- Backup server - NAS	จ.ส.อ.ฤทธิเดช แสงแจ่ม	นายศรัณยู สวัสดิ์มงคล	-	-
5	ระบบงาน Intranet สป.พม.	intranet.m-society.go.th	Daily	00.00	- Backup server - NAS	จ.ส.อ.ฤทธิเดช แสงแจ่ม	นายพลสิทธิ มีไปล์	-	-
6	ระบบฐานข้อมูล Oracle 2	oranuxdb.m-society.go.th	Daily	04.00	- Backup server - NAS	จ.ส.อ.ฤทธิเดช แสงแจ่ม	นายศรัณยู สวัสดิ์มงคล	-	-
7	ระบบฐานข้อมูลงานสารบรรณ	drora.m-society.go.th	Weekly	01.00	- Backup server - NAS	จ.ส.อ.ฤทธิเดช แสงแจ่ม	นายศรัณยู สวัสดิ์มงคล	-	-

ที่	ชื่อระบบ	Domain Name	Frequency (ความถี่ในการ สำรอง)	At Time	สื่อที่ใช้สำรอง	ผู้รับผิดชอบ			หน่วยงาน เจ้าของระบบ
						กทส.	กพส.	กวช.	
8	ระบบฐานข้อมูลผู้ประสบ ปัญหาทางสังคมกรณีฉุกเฉิน	msowelfare.m-society.go.th	Daily	02.00	- Backup server - NAS	จ.ส.อ.ฤทธิเดช แสงแจ่ม	นายอัศราวุฒิ ต่อโมกข์	-	-
9	ระบบสำรองฐานข้อมูล	-	Daily	03.00	- Backup server - NAS - External HDD	จ.ส.อ.ฤทธิเดช แสงแจ่ม	-	-	ศทส.
10	เว็บไซต์กระทรวงการพัฒนา สังคมและความมั่นคงของมนุษย์	www.m-society.go.th www.msds.go.th	Daily	22.00	- Backup server - NAS	จ.ส.อ.ฤทธิเดช แสงแจ่ม	นายอัศราวุฒิ ต่อโมกข์	-	ศทส.
11	โดเมนเนม	-	Weekly [date] : Fri.	01.30	- Backup server - NAS	จ.ส.อ.ฤทธิเดช แสงแจ่ม	-	-	ศทส.
12	ระบบติดตามแผนงาน ต่างประเทศและ ASCC	aseandata.m-society.go.th	Weekly [date] : Fri.	03.00	- Backup server - NAS	จ.ส.อ.ฤทธิเดช แสงแจ่ม	นายอัศราวุฒิ ต่อโมกข์	-	-
13	ระบบจองทรัพยากร	msobooking.m-society.go.th	Daily	03.00	- Backup server - NAS	จ.ส.อ.ฤทธิเดช แสงแจ่ม	นายอัศราวุฒิ ต่อโมกข์ นายศรัณยู สวัสดิ์มงคล	-	ศทส.
14	ระบบบริหารจัดการผู้ใช้งาน	usercenter.m-society.go.th	Weekly [date] : Fri.	03.00	- Backup server - NAS	จ.ส.อ.ฤทธิเดช แสงแจ่ม	นายพลสิทธิ มีไพล่	-	-
15	ระบบลูกค้าสัมพันธ์ สป.พม.	helpdesk.m-society.go.th	Weekly [date] : Fri.	22.00	- Backup server - NAS	จ.ส.อ.ฤทธิเดช แสงแจ่ม	นายศรัณยู สวัสดิ์มงคล นายอัศราวุฒิ ต่อโมกข์ นายพลสิทธิ มีไพล่	-	-

ที่	ชื่อระบบ	Domain Name	Frequency (ความถี่ในการ สำรอง)	At Time	สื่อที่ใช้สำรอง	ผู้รับผิดชอบ			หน่วยงาน เจ้าของระบบ
						กทส.	กฟส.	กวช.	
16	ระบบงานบริการทางสังคม	ossprovince.m-society.go.th	Archived เก็บ ข้อมูลไว้	-	-	-	-	-	-
17	ฐานข้อมูลระบบฐานข้อมูล กฎหมาย	lawdbs	Archived เก็บ ข้อมูลไว้	-	-	-	-	-	-
18	ระบบฐานข้อมูลกฎหมาย	law.m-society.go.th	Weekly [date] : Fri.	21.00	- Backup server - NAS	จ.ส.อ.ฤทธิเดช แสงแจ่ม	นายพลสิทธิ มีไปล์	-	-
19	ระบบฐานข้อมูลครุภัณฑ์ คอมพิวเตอร์	ictc-asset.m-society.go.th	Archived เก็บ ข้อมูลไว้	-	-	-	-	-	-
20	ระบบแลกเปลี่ยนข้อมูลกลาง การจัดสวัสดิการของกระทรวง	msolinkage.m-society.go.th	Weekly [date] : Sun.	02.00	- Backup server - NAS	จ.ส.อ.ฤทธิเดช แสงแจ่ม	นายอัศวิน ตอโมกซ์ นายพลสิทธิ มีไปล์	-	-
21	JsonWebservice	iservice.m-society.go.th	Weekly [date] : Fri.	08.00	- Backup server - NAS	จ.ส.อ.ฤทธิเดช แสงแจ่ม	นายอัศวิน ตอโมกซ์	-	-
22	-	PDC.m-society.go.th	Monthly [date] : 30	11.00	- Backup server - NAS	จ.ส.อ.ฤทธิเดช แสงแจ่ม	-	-	ศทส.
23	ระบบเชื่อมต่อทะเบียนราษฎร์ กรมการปกครอง	broker.m-society.go.th	Monthly [date] : 1	05.00	- Backup server - NAS	จ.ส.อ.ฤทธิเดช แสงแจ่ม	นายอัศวิน ตอโมกซ์	-	-
24	เว็บบริหารกองทุน	fund.m-society.go.th	Monthly [date] : 30	03.00	- Backup server - NAS	จ.ส.อ.ฤทธิเดช แสงแจ่ม	นายศรีณัฐ สวัสดิ์มงคล	-	กคม.

ที่	ชื่อระบบ	Domain Name	Frequency (ความถี่ในการ สำรอง)	At Time	สื่อที่ใช้สำรอง	ผู้รับผิดชอบ			หน่วยงาน เจ้าของระบบ
						กทส.	กพส.	กวช.	
25	ระบบห้องสมุดอิเล็กทรอนิกส์	ebooks.m-society.go.th	Weekly [date] : Fri.	02.30	- Backup server - NAS	จ.ส.อ.ฤทธิเดช แสงแจ่ม	นายอัศราวุฒิ ต่อโมกษ์	-	-
26	ระบบทำเนียบหน่วยงาน อิเล็กทรอนิกส์	directory.m-society.go.th	Monthly [date] : 30	01.30	- Backup server - NAS	จ.ส.อ.ฤทธิเดช แสงแจ่ม	นายศรัณยู สวัสดิ์มงคล	-	-
27	ระบบงานบริหารราชการ	boffice.m-society.go.th	Monthly [date] : 30	02.00	- Backup server - NAS	จ.ส.อ.ฤทธิเดช แสงแจ่ม	นายศรัณยู สวัสดิ์มงคล นายอัศราวุฒิ ต่อโมกษ์	-	-
28	ระบบเทียบเวลาเครื่องแม่ข่าย	time.m-society.go.th	Yearly	22.00	- Backup server - NAS	จ.ส.อ.ฤทธิเดช แสงแจ่ม	-	-	ศทส.
29	DMP Database Server	DMP Database Server	Archived เก็บข้อมูลไว้	05.00	- Backup server - NAS	จ.ส.อ.ฤทธิเดช แสงแจ่ม	-	นายปฏิพัทธ์ ก้อมมะณี	-
30	DMP Processing Server	DMP Processing Server	Archived เก็บข้อมูลไว้	05.00	- Backup server - NAS	จ.ส.อ.ฤทธิเดช แสงแจ่ม	-	นายปฏิพัทธ์ ก้อมมะณี	-
31	DMP Service Gateway	DMP Service Gateway	Archived เก็บข้อมูลไว้	05.00	- Backup server - NAS	จ.ส.อ.ฤทธิเดช แสงแจ่ม	-	นายปฏิพัทธ์ ก้อมมะณี	-
32	DMP WebApp Server	DMP WebApp Server	Archived เก็บข้อมูลไว้	05.00	- Backup server - NAS	จ.ส.อ.ฤทธิเดช แสงแจ่ม	-	นายปฏิพัทธ์ ก้อมมะณี	-

ที่	ชื่อระบบ	Domain Name	Frequency (ความถี่ในการ สำรอง)	At Time	สื่อที่ใช้สำรอง	ผู้รับผิดชอบ			หน่วยงาน เจ้าของระบบ
						กทส.	กฟส.	กวช.	
33	Platform_sFTP	Platform_sFTP	Daily	05.00	- Backup server - NAS	จ.ส.อ.ฤทธิเดช แสงแจ่ม	-	นายปวิพท์ ก้อมมะณี	-
34	Database_Server	Database_Server	Daily	05.00		จ.ส.อ.ฤทธิเดช แสงแจ่ม	-	-	ศทส.
35	NginX_01	NginX_01	Daily	05.00	- Backup server - NAS	จ.ส.อ.ฤทธิเดช แสงแจ่ม	-	-	ศทส.
36	Web_and_Application_64	Web_and_Application_64	Daily	05.00	- Backup server - NAS	จ.ส.อ.ฤทธิเดช แสงแจ่ม	-	-	-
37	WebCenter_SQL	WebCenter_SQL	Weekly [date] : Sat.	0:00	- Backup server - NAS	จ.ส.อ.ฤทธิเดช แสงแจ่ม	นายศรัณยู สวัสดิ์มงคล	-	-
38	GIS_socialmap	GIS_socialmap	Weekly [date] : Sat.	0:00	- Backup server - NAS	จ.ส.อ.ฤทธิเดช แสงแจ่ม	-	-	-
39	GIS_WebApp	GIS_WebApp	Weekly [date] : Sat.	0:00	- Backup server - NAS	จ.ส.อ.ฤทธิเดช แสงแจ่ม	-	-	-
40	nagios	nagios	Weekly [date] : Sat.	0:00	- Backup server - NAS	จ.ส.อ.ฤทธิเดช แสงแจ่ม	-	-	-
41	service1300	service1300	Weekly [date] : Mon. Wed. Fri.	22:00	- Backup server - NAS	จ.ส.อ.ฤทธิเดช แสงแจ่ม	-	-	-

ที่	ชื่อระบบ	Domain Name	Frequency (ความถี่ในการ สำรอง)	At Time	สื่อที่ใช้สำรอง	ผู้รับผิดชอบ			หน่วยงาน เจ้าของระบบ
						กทส.	กพส.	กวช.	
42	nhic_61	nhic_61	Weekly [date] : Mon. Wed. Fri.	22:00	- Backup server - NAS	จ.ส.อ.ฤทธิเดช แสงแจ่ม	-	-	-
43	FingerScan_Tpso62	FingerScan_Tpso62	Daily	23:00	- Backup server - NAS	จ.ส.อ.ฤทธิเดช แสงแจ่ม	-	-	ศทส.
44	owncloud_61	owncloud_61	Daily	22:00	- Backup server - NAS	จ.ส.อ.ฤทธิเดช แสงแจ่ม	-	-	ศทส.
45	มาตรฐานกลางข้อมูล	datastandard	Daily	22:00	- Backup server - NAS	จ.ส.อ.ฤทธิเดช แสงแจ่ม	-	นางสาวอภิสร่า ศรีขนิณ นายปฏิพัทธ์ ก้อมมะณี	ศทส.
46	ระบบทะเบียนข้อมูล ผู้ทรงคุณวุฒิ	expertcommittee.m- society.go.th	Daily	22:00	- Backup server - NAS	จ.ส.อ.ฤทธิเดช แสงแจ่ม	นายศรัณยู สวัสดิ์มงคล	-	-
47	ระบบบริหารจัดการบัญชี ผู้ใช้งาน	CPPM-VM	Daily	22:00	- Backup server - NAS	จ.ส.อ.ฤทธิเดช แสงแจ่ม	-	-	-
48	ระบบจัดการความรู้ศูนย์ ช่วยเหลือสังคม	1300_APP_WIKI_NEW	Daily	22:00	- Backup server - NAS	จ.ส.อ.ฤทธิเดช แสงแจ่ม	-	-	-
49	ระบบออกบัตรข้าราชการ	App_Card	Daily	22:00	- Backup server - NAS	จ.ส.อ.ฤทธิเดช แสงแจ่ม	-	-	กก.

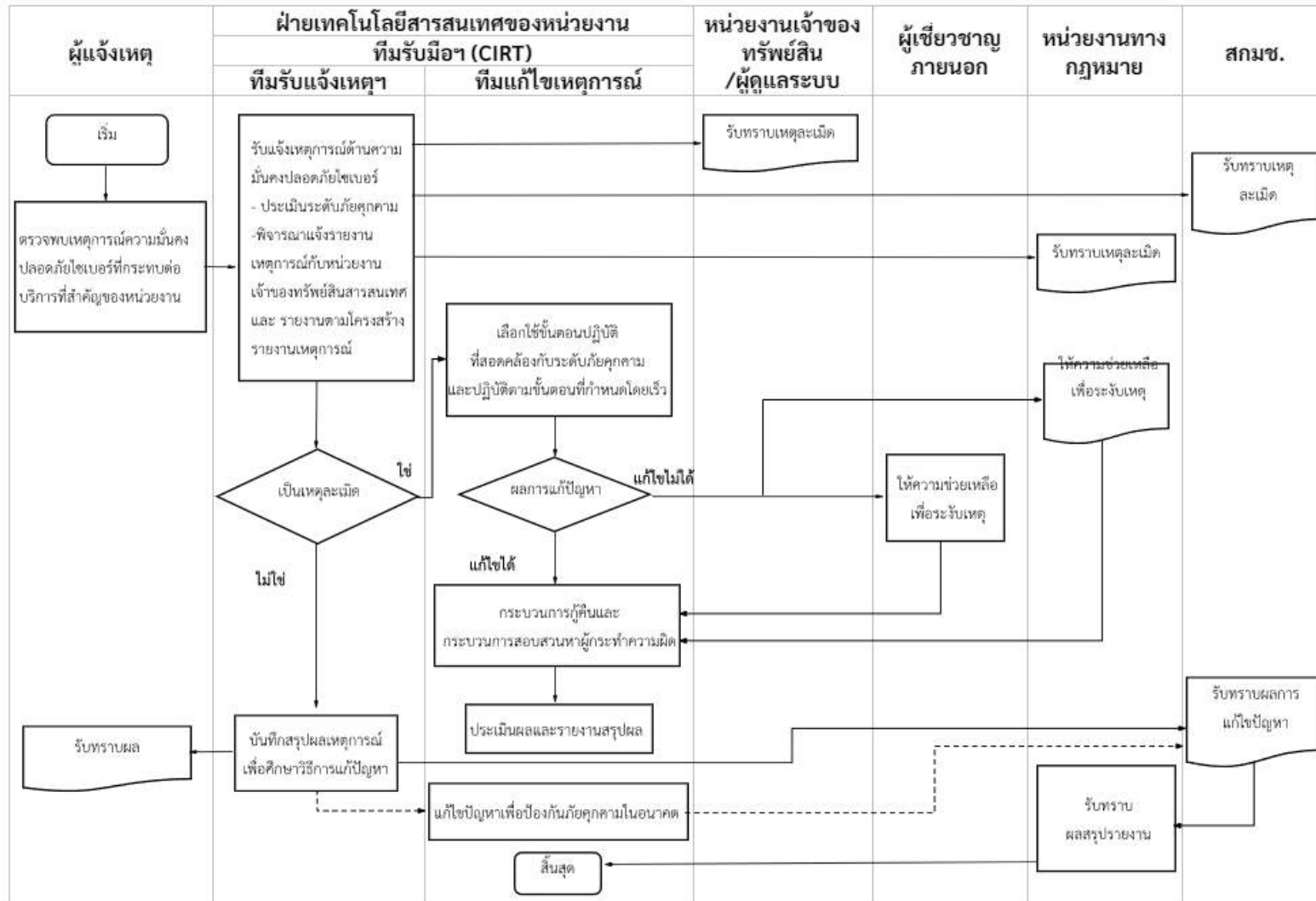
ที่	ชื่อระบบ	Domain Name	Frequency (ความถี่ในการ สำรอง)	At Time	สื่อที่ใช้สำรอง	ผู้รับผิดชอบ			หน่วยงาน เจ้าของระบบ
						กทส.	กฟส.	กวช.	
50	ระบบออกบัตรข้าราชการ	App_card_windows	Daily	22:00	- Backup server - NAS	จ.ส.อ.ฤทธิเดช แสงแจ่ม	-	-	กก.
51	ระบบออกบัตรข้าราชการ	DB_Card	Daily	22:00	- Backup server - NAS	จ.ส.อ.ฤทธิเดช แสงแจ่ม	-	-	กก.
52	ฐานข้อมูลระบบต่อต้านการ ทุจริต	DB_corruption	Daily	22:00	- Backup server - NAS	จ.ส.อ.ฤทธิเดช แสงแจ่ม	นายศรีณยู สวัสดิ์มงคล นายพลสิทธิ มีไพล่	-	ศปท.
53	ระบบติดตามและประเมินผล	project	Daily	22:00	- Backup server - NAS	จ.ส.อ.ฤทธิเดช แสงแจ่ม	นายอัศราวุฒิ ต่อโมกษ์ นายศรีณยู สวัสดิ์มงคล	-	-
54	จัดเก็บแคชเว็บ พมจ.	nginxreverseproxypmj	Daily	22:00	- Backup server - NAS	จ.ส.อ.ฤทธิเดช แสงแจ่ม	-	-	ศทส.
55	เว็บไซต์สถาบันพระประชาบดี	Web_Phraprachabodi	Daily	22:00	- Backup server - NAS	จ.ส.อ.ฤทธิเดช แสงแจ่ม	-	-	สพพ.
56	ระบบบริหารจัดการ Anti Virus	Server_Anti Virus	Daily	22:00	- Backup server - NAS	จ.ส.อ.ฤทธิเดช แสงแจ่ม	-	-	ศทส.
57	MSO-VCenter	MSO-VC7	Daily	22:00	- Backup server - NAS	จ.ส.อ.ฤทธิเดช แสงแจ่ม	-	-	ศทส.

ที่	ชื่อระบบ	Domain Name	Frequency (ความถี่ในการ สำรอง)	At Time	สื่อที่ใช้สำรอง	ผู้รับผิดชอบ			หน่วยงาน เจ้าของระบบ
						กทส.	กพส.	กวช.	
58	ระบบ eform	eform.m-society.go.th	Daily	02.30	- Backup server - NAS	จ.ส.อ.ฤทธิเดช แสงแจ่ม	นายศรัณยู สวัสดิ์มงคล	-	ศทส.
59	ระบบการแจ้งเหตุด่วนเหตุร้าย แจ้งปัญหาสังคม และขอรับ บริการ กระทรวงการพัฒนาสังคมและ ความมั่นคงของมนุษย์ (พม.) โดย ศูนย์ช่วยเหลือสังคม (1300)	https://eservice1300.m- society.go.th/	Daily	02.30	- Backup server - NAS	จ.ส.อ.ฤทธิเดช แสงแจ่ม	-	-	กตร. (1300)
60	ระบบสมุดปกครอบครัว อิเล็กทรอนิกส์ MSO - LOGBOOK	mso-logbook.m- society.go.th/	Daily	22:00	- Backup server - NAS	จ.ส.อ.ฤทธิเดช แสงแจ่ม	-	นายปฏิพัทธ์ ก้อมมะณี	ศทส.
61	Tableau Server	tableau.m-society.go.th	Daily	22:01	- Backup server - NAS	จ.ส.อ.ฤทธิเดช แสงแจ่ม		นายปฏิพัทธ์ ก้อมมะณี	ศทส.
62	ระบบฐานข้อมูลขนาดใหญ่ (Big Data)		Daily	22:00	- Backup server - NAS	จ.ส.อ.ฤทธิเดช แสงแจ่ม	-	นายปฏิพัทธ์ ก้อมมะณี	ศทส.
63	ระบบบัญชีข้อมูลภาครัฐ กระทรวงการพัฒนาสังคมและ ความมั่นคงของมนุษย์	ckan.m-society.go.th	Daily	22:00	- Backup server - NAS	จ.ส.อ.ฤทธิเดช แสงแจ่ม	-	-	

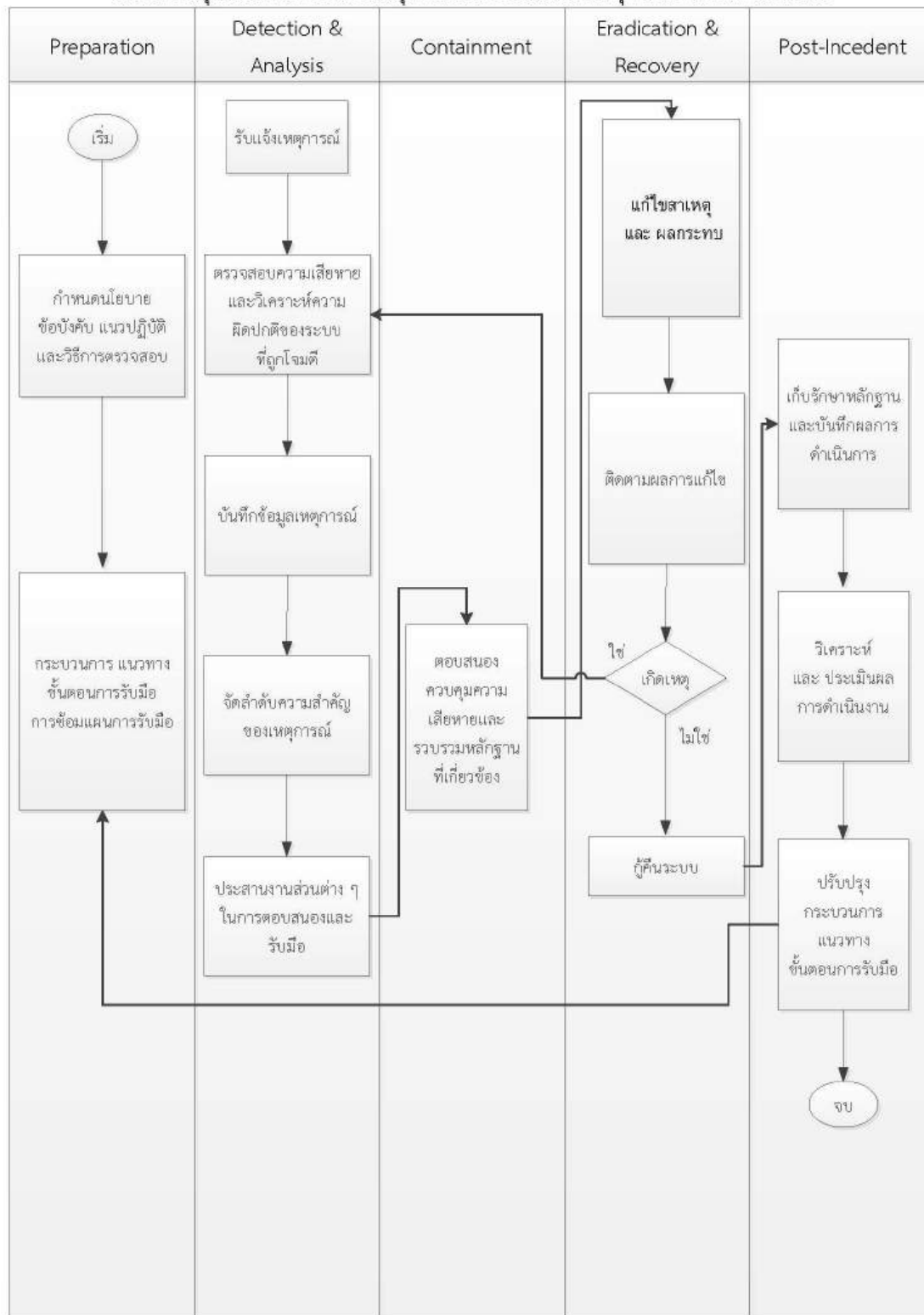
ที่	ชื่อระบบ	Domain Name	Frequency (ความถี่ในการ สำรอง)	At Time	สื่อที่ใช้สำรอง	ผู้รับผิดชอบ			หน่วยงาน เจ้าของระบบ
						กทส.	กพส.	กวช.	
64	ระบบแจ้งเตือนสิทธิ		Daily	22:00	- Backup server - NAS	จ.ส.อ.ฤทธิเดช แสงแจ่ม	นายศรัณยู สวัสดิ์มงคล นายพลสิทธิ มีไพล่	-	-
65	ฐานข้อมูลระบบแจ้งเตือนสิทธิ		Daily	22:00	- Backup server - NAS	จ.ส.อ.ฤทธิเดช แสงแจ่ม	นายศรัณยู สวัสดิ์มงคล นายพลสิทธิ มีไพล่	-	-
66	ระบบจัดเก็บเอกสาร	kpb.m-society.go.th	Daily	22:00	- Backup server - NAS	จ.ส.อ.ฤทธิเดช แสงแจ่ม	-	-	-
67	M-file	m-file.m-society.go.th	Daily	22:00	- Backup server - NAS	จ.ส.อ.ฤทธิเดช แสงแจ่ม	-	-	ศทส.
68	ระบบตรวจราชการดิจิทัล พม.	https://volunteer-smart-beta.nu.ac.th/beta-inspectorNew/index.php	Daily	22:00	- Backup server - NAS	จ.ส.อ.ฤทธิเดช แสงแจ่ม	-	-	-
69	ระบบงานแพลตฟอร์มบริจาค และการรับบริจาค เครื่อง Reverse Proxy	172.21.100.173	Monthly	22:00	- Backup server - NAS	จ.ส.อ.ฤทธิเดช แสงแจ่ม	นายอัศราวุฒิ ต่อโมกข์	-	กตร. (ศบจ.)
70	ระบบงานแพลตฟอร์มบริจาค และการรับบริจาค เครื่อง Application Server	172.21.102.175	Weekly	22:00	- Backup server - NAS	จ.ส.อ.ฤทธิเดช แสงแจ่ม	นายอัศราวุฒิ ต่อโมกข์	-	กตร. (ศบจ.)
71	ระบบงานแพลตฟอร์มบริจาค และการรับบริจาค เครื่อง Database Server	172.21.104.175	Daily	22:00	- Backup server - NAS	จ.ส.อ.ฤทธิเดช แสงแจ่ม	นายอัศราวุฒิ ต่อโมกข์	-	กตร. (ศบจ.)

ภาคผนวก ๒

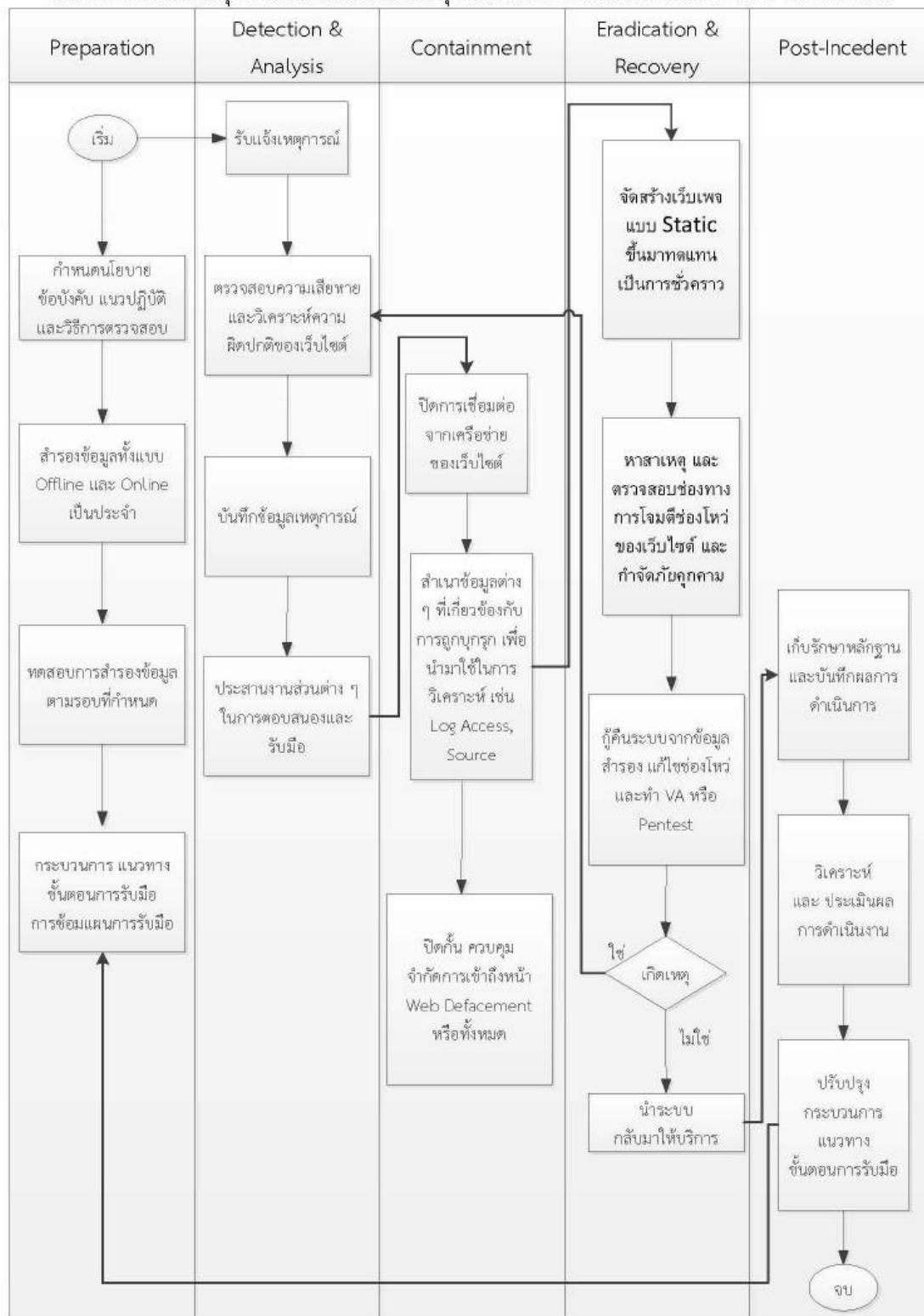
แผนผังโครงสร้างขั้นตอนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response)



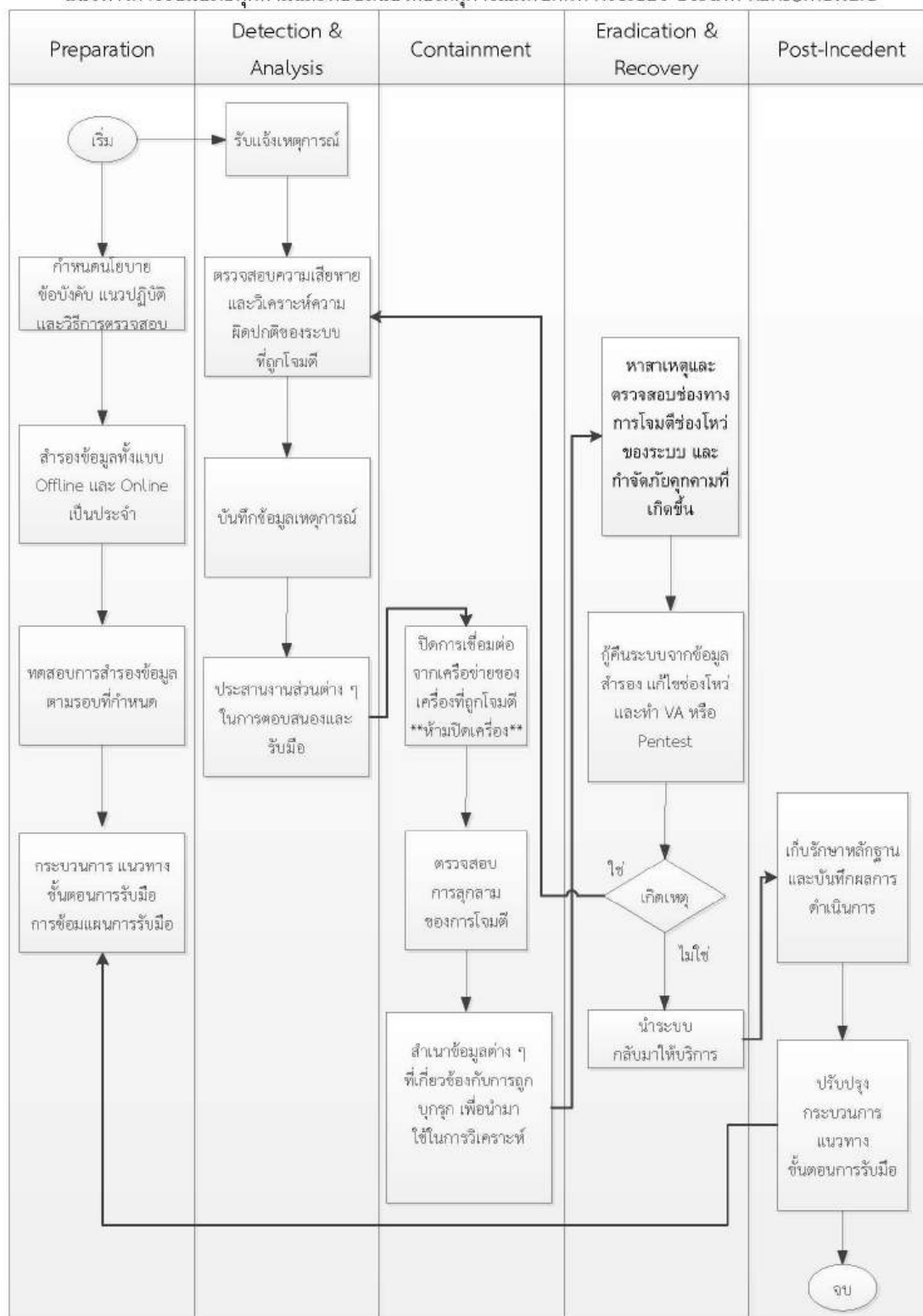
แผนภาพสรุปแนวทางการรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์



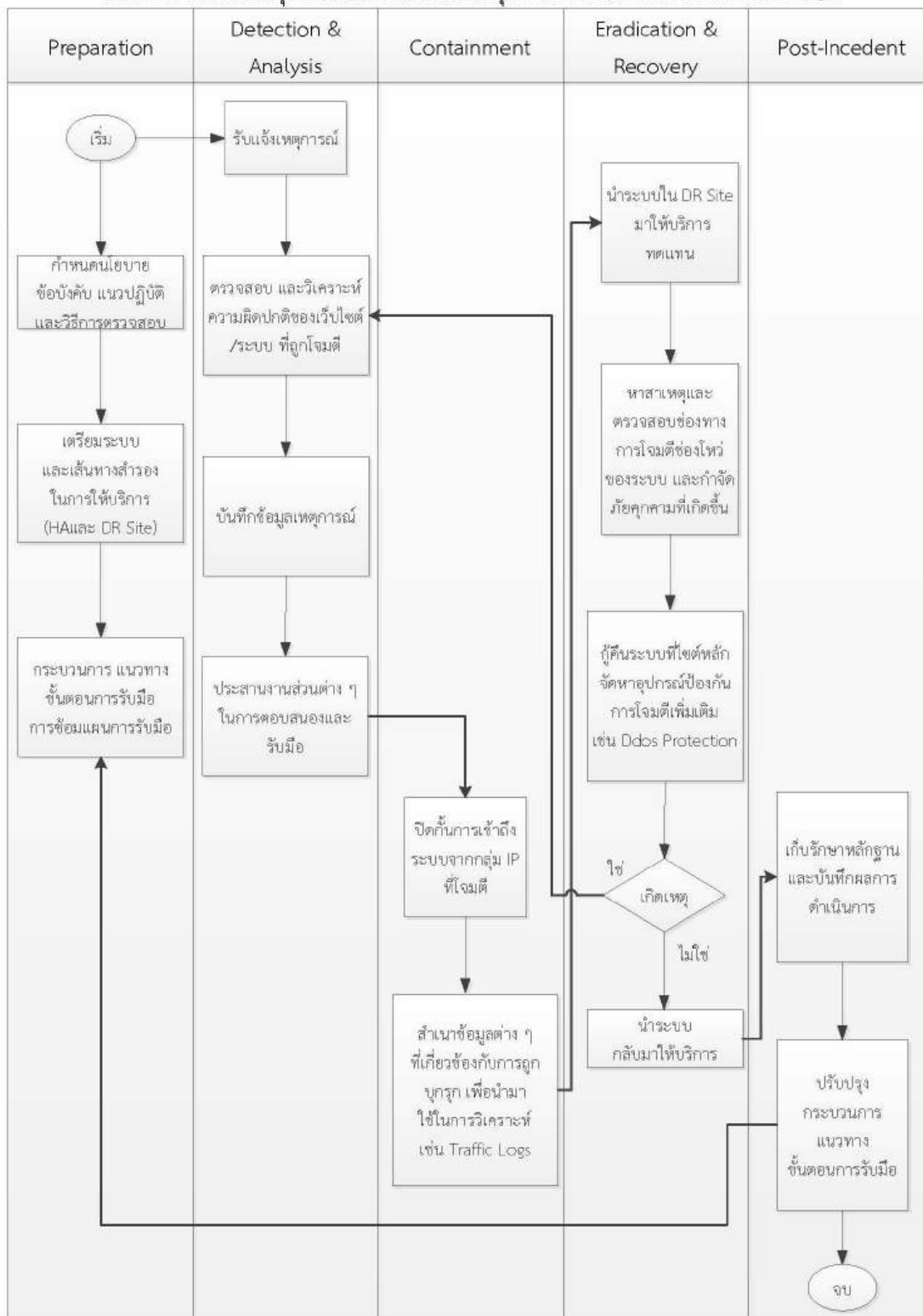
แนวทางการรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ ประเภท Web Defacement

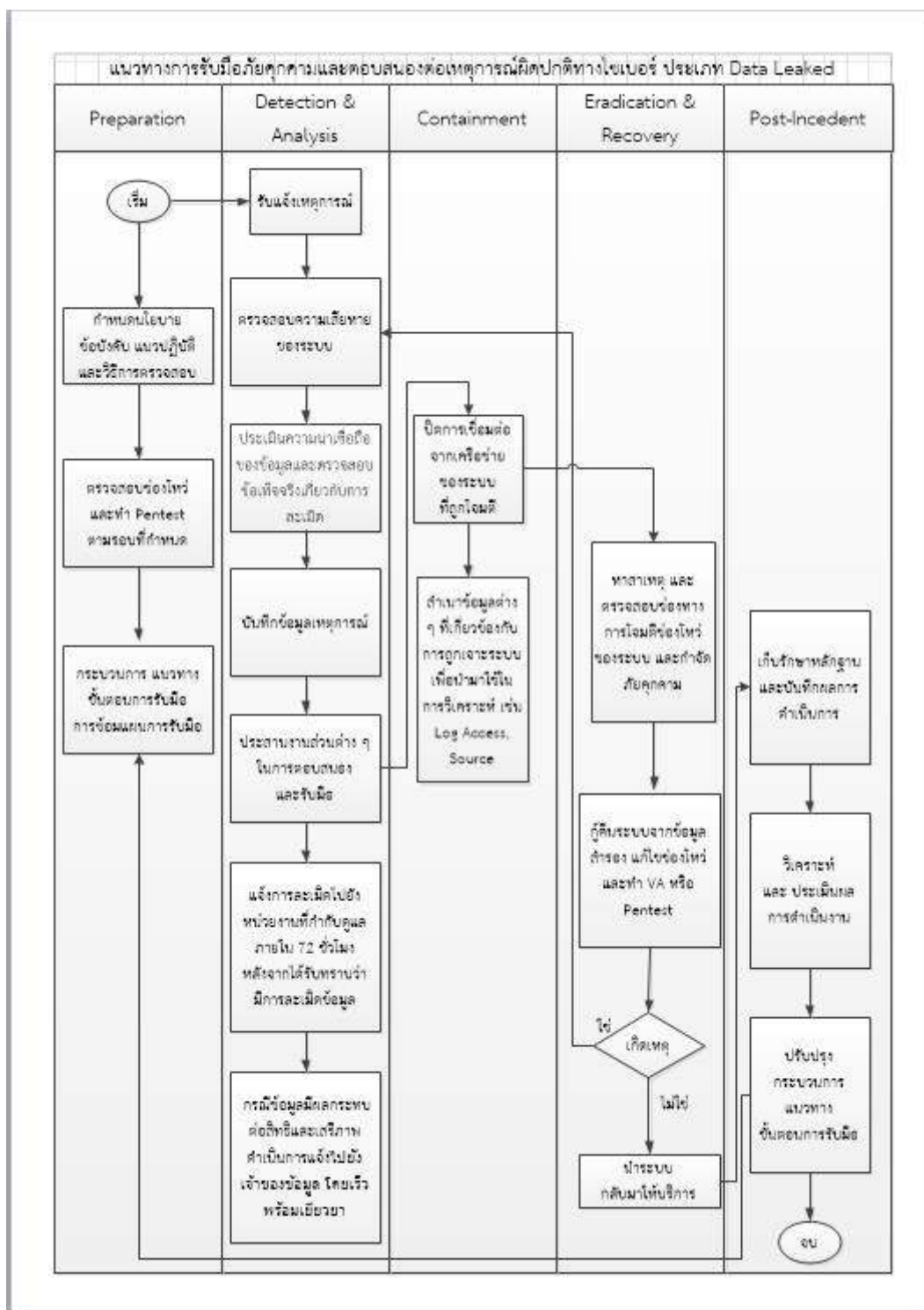


แนวทางการรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ ประเภท Ransomware



แนวทางการรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ ประเภท DDoS





ภาคผนวก ๓

การดำเนินการมาตรการเพื่อเตรียมการและป้องกันการเกิดภัยคุกคามทางไซเบอร์ (preparation)

ระดับ	แนวปฏิบัติพื้นฐาน (Security Control Baselines)
กรณีบริการ ระบบ หรือ อุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง กรณีบริการ ระบบ หรือ อุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับร้ายแรง กรณีบริการ ระบบ หรือ อุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับวิกฤติ	(๑) จัดเตรียมข้อมูลและอุปกรณ์การติดต่อสื่อสารที่จำเป็น เช่น ข้อมูลการติดต่อของบุคคลหรือองค์กรต่าง ๆ คู่มือการปฏิบัติงานเพื่อรับมือกับภัยคุกคามทางไซเบอร์ และกลไกอื่นใด ที่ช่วยสนับสนุนการรายงานเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น เป็นต้น (๒) จัดเตรียมอุปกรณ์หรือทรัพยากรสนับสนุนที่จำเป็นสำหรับการรับมือกับภัยคุกคามทางไซเบอร์ (๓) ดำเนินการให้มีการจัดหมวดหมู่ข้อมูลและระบบสารสนเทศให้สอดคล้องกับแนวทางของกฎหมาย กฎเกณฑ์ หรือนโยบายต่าง ๆ ที่เกี่ยวข้อง เพื่อธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) ตลอดจนสภาพพร้อมใช้งาน(availability) ของข้อมูลและระบบสารสนเทศดังกล่าว (๔) จัดเตรียมข้อมูลสนับสนุนที่จำเป็นสำหรับการวิเคราะห์เหตุภัยคุกคามทางไซเบอร์ เช่น รายการทรัพย์สินสำคัญทางสารสนเทศ และแผนผังโครงสร้างเครือข่าย (Network diagrams) เป็นต้น (๕) พิจารณาช่องบริการหรือระบบที่ผู้โจมตีสามารถค้นพบในเครือข่ายได้ง่าย โดยไม่ต้องใช้ความพยายามเจาะระบบ เช่น การค้นหาผ่านกลไกการสืบค้น (discovery protocol) เป็นต้น (๖) ดำเนินการควบคุมการเปลี่ยนแปลงการตั้งค่าของอุปกรณ์ต่าง ๆ (configuration change control และจัดทำแผนการบริหารจัดการการตั้งค่าหรือการเปลี่ยนแปลงค่าของอุปกรณ์ (configuration management plan) (๗) กำหนดตัวบุคคลหรือมอบหมายให้เจ้าหน้าที่ที่มีความชำนาญเป็นผู้ดำเนินการที่เกี่ยวข้องกับการเปลี่ยนแปลงการตั้งค่าของอุปกรณ์ต่าง ๆ รวมถึงการทำหน้าที่ในการประสานงานหรือหารือกับผู้ที่เกี่ยวข้อง (๘) จัดให้มีกระบวนการในการพิสูจน์ตัวตนผู้ใช้งานก่อนทำการเปลี่ยนแปลงการตั้งค่าของอุปกรณ์ใด ๆ เช่น การเข้ารหัสข้อมูลและการบริหารจัดการคีย์สำหรับการเข้าถึงระบบต่าง ๆ (cryptography / key managements) เป็นต้น

	(๙) ตรวจสอบแอปพลิเคชันที่ให้บริการโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้มีความปลอดภัยเพียงพอ โดยมีการคัดกรองนักพัฒนา (developer screening) ที่ได้รับมอบหมายให้ดำเนินการใด ๆ กับเครือข่าย แอปพลิเคชัน หรือระบบงานต่าง ๆ (๑๐) ดำเนินการให้มีการทดสอบความสามารถในการตอบสนองต่อภัยคุกคามทางไซเบอร์ (incident respond capability testing) (๑๑) รวบรวมข่าวกรองเกี่ยวกับภัยคุกคามทางไซเบอร์ (threat Intelligence) (๑๒) พิจารณาจัดให้มีกลไกที่สามารถทำงานได้โดยอัตโนมัติ เพื่อดำเนินการทดสอบการเจาะระบบเป็นประจำ และสามารถแจ้งเตือนได้อย่างทันท่วงทีเมื่อพบช่องโหว่หรือจุดอ่อนต่าง ๆ (ถ้าหน่วยงานมีความพร้อม) (๑๓) กำหนดแนวทางและระยะเวลาการเก็บรักษาหลักฐานเกี่ยวกับการก่อภัยคุกคามทางไซเบอร์ (๑๔) ดำเนินการควบคุมการเปลี่ยนแปลงการตั้งค่าของอุปกรณ์ต่าง ๆ (configuration change control) และจัดทำแผนการบริหารจัดการการตั้งค่าหรือการเปลี่ยนแปลงค่าของอุปกรณ์ (configuration management plan) โดยจะต้องจัดให้มีกลไกที่สามารถบันทึกประวัติการเปลี่ยนแปลงการตั้งค่าของอุปกรณ์ที่เป็นลายลักษณ์อักษรการแจ้งเตือนเมื่อมีการเปลี่ยนแปลงค่าของอุปกรณ์ที่ตั้งไว้ และให้พิจารณาจัดให้มีกลไกที่สามารถป้องกันการเปลี่ยนแปลงค่าของอุปกรณ์ต่าง ๆ โดยอัตโนมัติ(ถ้าหน่วยงานมีความพร้อม) (๑๕) จัดให้มีการฝึกอบรมเพื่อเตรียมพร้อมรับมือกับสถานการณ์ฉุกเฉินเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น (simulated events) เพื่อให้ผู้ปฏิบัติรับทราบบทบาทและความรับผิดชอบของตนเมื่อต้องรับมือกับสถานการณ์ดังกล่าว (๑๖) สร้างเครือข่ายความร่วมมือเพื่อแบ่งปันข้อมูลและประสานงานเกี่ยวกับการจัดการภัยคุกคามทางไซเบอร์
--	---

ภาคผนวก ๔

ตัวอย่าง : บันทึกรายงานสถานการณ์เหตุการณ์ความมั่นคงปลอดภัยไซเบอร์

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

ภาคผนวก ๕

บันทึกข้อมูลกิจกรรมเหตุการณ์ความปลอดภัยทางไซเบอร์ (Incident Documentation)

[illegible]

ภาคผนวก ๖

เอกสาร ก๑ ข้อมูลที่ต้องแจ้ง

ข้อมูลการประสานงานและผลการตรวจสอบภัยคุกคามเบื้องต้น	
๑. ข้อมูลการประสานงาน ชื่อหน่วยงานที่รับผิดชอบติดตามเหตุภัยคุกคาม วันที่และเวลาที่แจ้ง	
๒. ด้านภารกิจหรือบริการของหน่วยงาน และ ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม ที่อยู่ของหน่วยงานหรือหน่วยงานย่อยที่เกิดเหตุภัยคุกคาม	
๓. ข้อมูลการติดต่อสำหรับการประสานงานเหตุภัยคุกคาม ชื่อ-นามสกุล ตำแหน่งงาน ชื่อหน่วยงาน อีเมล โทรศัพท์ (ที่ทำงาน / มือถือ)	
๔. ความต่อเนื่องของเหตุภัยคุกคาม ☐ เหตุภัยคุกคามใหม่ ☐ การรายงานข้อมูลต่อเนื่องจากเหตุภัยคุกคามเดิม	
๕. ลักษณะภัยคุกคามทางไซเบอร์ ระบบที่ได้รับผลกระทบมีความสำคัญต่อพันธกิจหลักของหน่วยงานหรือไม่ เหตุการณ์ที่เกิดขึ้นเกิดจากภัยคุกคามทางไซเบอร์ ในระดับใด (มาตรา ๖๐) ☐ ไม่ร้ายแรง ☐ ร้ายแรง ☐ วิกฤต (ก) ☐ วิกฤต (ข) ☐ ยังไม่สามารถระบุได้	

๖. หมวดหมู่ของภัยคุกคาม (แจ้งได้มากกว่า ๑ รายการ)

หมวดหมู่*	คำอธิบาย
หมวดหมู่ที่ ๒	การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance)
หมวดหมู่ที่ ๓	การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยของหน่วยงาน (Non-Compliance Activity)
หมวดหมู่ที่ ๔	การบุกรุกโดยการใช้มัลแวร์ (Malicious Logic)
หมวดหมู่ที่ ๕	การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion)
หมวดหมู่ที่ ๖	การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion)
หมวดหมู่ที่ ๗	การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)
หมวดหมู่ที่ ๘	เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating)

* อ้างอิงหมวดหมู่ตามภาคผนวกท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปรามปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ (ทั้งนี้ ภัยคุกคามทางไซเบอร์หมวดหมู่ที่ ๐ หมวดหมู่ที่ ๑ และหมวดหมู่ที่ ๙ ไม่เข้าข่ายเป็นภัยคุกคามทางไซเบอร์ที่ต้องรายงาน)

เอกสาร ก๒ แบบรายงานภัยคุกคามทางไซเบอร์

ส่วนที่ ๑	
หมวด ก. ข้อมูลการประสานงานและผลการตรวจสอบภัยคุกคามเบื้องต้น	
หมายเลขอ้างอิง (สำหรับเจ้าหน้าที่ สกมช.): โปรดระบุ หน่วยงานที่รับผิดชอบติดตามเหตุภัยคุกคาม (ถ้ามี): โปรดระบุ วันที่: เลือกวันที่ เวลา: โปรดระบุ	
ก๑. ด้านภารกิจหรือบริการของหน่วยงาน และ ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม: โปรดระบุ ที่อยู่ของหน่วยงานหรือหน่วยงานย่อยที่เกิดเหตุภัยคุกคาม: โปรดระบุ	
ก๒. ข้อมูลการติดต่อสำหรับการประสานงานเหตุภัยคุกคาม ชื่อ-นามสกุล: โปรดระบุ ตำแหน่งงาน: โปรดระบุ ชื่อหน่วยงาน: โปรดระบุ อีเมล: โปรดระบุ โทรศัพท์ (ที่ทำงาน / มือถือ) : โปรดระบุ	
ก๓. ความต่อเนื่องของเหตุภัยคุกคาม ☐ เหตุภัยคุกคามใหม่ ☐ การรายงานข้อมูลต่อเนื่องจากเหตุภัยคุกคามเดิม	
ก๔. ลักษณะภัยคุกคามทางไซเบอร์ ระบบที่ได้รับผลกระทบมีความสำคัญต่อพันธกิจหลักของหน่วยงาน ☐ ใช่ ☐ ไม่ใช่ เหตุการณ์ที่เกิดขึ้นเกิดจากภัยคุกคามทางไซเบอร์ ในระดับใด (มาตรา ๖๐) ☐ ไม่ร้ายแรง ☐ ร้ายแรง ☐ วิฤต (ก) ☐ วิฤต (ข) ☐ ยังไม่สามารถระบุได้	

หมวด ข. ข้อมูลการตรวจพบภัยคุกคามไซเบอร์	
ข๑. วัน เวลา ที่เกิดเหตุภัยคุกคาม วันที่ : เลือกวันที่ เวลา : โปรดระบุ วัน เวลา ที่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศทราบเหตุภัยคุกคาม วันที่ : เลือกวันที่ เวลา : โปรดระบุ	
ข๒. วัน เวลา ที่แจ้งเหตุภัยคุกคามให้หน่วยงานควบคุมหรือกำกับดูแลทราบ ☐ ยังไม่ได้แจ้ง ☐ แจ้งแล้ว _____	
ข๓. หมวดหมู่ของภัยคุกคาม (เลือกได้มากกว่า ๑ รายการ)	
หมวดหมู่*	คำอธิบาย
☐ หมวดหมู่ที่ ๒	การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance)
☐ หมวดหมู่ที่ ๓	การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยของหน่วยงาน (Non-Compliance Activity)
☐ หมวดหมู่ที่ ๔	การบุกรุกโดยการใช้มัลแวร์ (Malicious Logic)
☐ หมวดหมู่ที่ ๕	การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion)
☐ หมวดหมู่ที่ ๖	การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion)
☐ หมวดหมู่ที่ ๗	การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)
☐ หมวดหมู่ที่ ๘	เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating)
☐ อื่น ๆ	โปรดระบุ
* อ้างอิงหมวดหมู่ตามภาคผนวกท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปรามปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ (ทั้งนี้ ภัยคุกคามหมวดหมู่ที่ ๐ ๑ และ ๙ ไม่เข้าข่ายเป็นภัยคุกคามทางไซเบอร์ที่ต้องรายงาน)	
ข๔. ข้อมูลเบื้องต้นเกี่ยวกับระบบคอมพิวเตอร์ คอมพิวเตอร์ บริการ หรือข้อมูลที่ได้รับผลกระทบ: สถานที่ตั้งของเครื่อง ข้อมูล หรือสินทรัพย์ที่ได้รับผลกระทบ (เช่น จังหวัด ตำบล ตึก ห้อง): โปรดระบุ ชื่อผู้ให้บริการเครือข่ายที่ให้บริการแก่ระบบ บริการ หรือข้อมูลที่ได้รับผลกระทบ : โปรดระบุ บริการของระบบ ข้อมูล หรือสินทรัพย์ที่ได้รับผลกระทบ (เช่น บริการการเงิน): โปรดระบุ ฮาร์ดแวร์ ซอฟต์แวร์ที่ได้รับผลกระทบ (โปรดระบุรายละเอียด เช่น ผู้ผลิตหรือยี่ห้อ รุ่นของเครื่องคอมพิวเตอร์): โปรดระบุรายละเอียด	

มีผลกระทบต่อสารสื่อสาร (ทางโทรศัพท์ หรือ การใช้งานเครือข่าย): โปรดระบุ
รายละเอียดอื่น ๆ: โปรดระบุ

หมวด ค: ข้อมูลการรับมือภัยคุกคาม

ค๑. สถานการณ์หรือการแก้ไขเหตุภัยคุกคาม (เลือกได้มากกว่า ๑ รายการ)

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

ค๒. สิ่งที่ได้ดำเนินการหรือได้แก้ไขไปแล้ว

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

ค๓. รายละเอียดการรับมือภัยคุกคามอื่น ๆ (ถ้ามี)

โปรดระบุ

ส่วนที่ ๒
หมวด ง : รายละเอียดภัยคุกคาม
ง๑. ข้อมูลการตรวจจับและการวิเคราะห์
ง๑.๑ วัน เวลา ที่ผู้โจมตีได้เริ่มต้นเข้าถึงระบบ (System Access) วันที่: เลือกวันที่ เวลา: โปรดระบุ ไม่ทราบ: ☐
ง๑.๒ 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
ง๑.๓ รายละเอียดผลกระทบจากเหตุภัยคุกคาม (ระบุผลกระทบที่มีเกิดขึ้นต่อ ระบบ คน หรือข้อมูล) จำนวนระบบ บริการ หรือสินทรัพย์ที่เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่ได้รับผลกระทบ (โดยประมาณ): โปรดระบุ ทรัพย์สินที่สำคัญอื่น ๆ ที่อาจได้รับผลกระทบ: โปรดระบุ จำนวนผู้ได้รับผลกระทบ (โดยประมาณ): โปรดระบุ มูลค่าความเสียหาย (โดยประมาณ): โปรดระบุ ในกรณีที่ข้อมูลที่ระบุตัวบุคคลได้รั่วไหล (หรือถูกขโมย): จำนวนบุคคลที่เป็นเจ้าของข้อมูล : โปรดระบุ ชนิดของข้อมูล (เลือกทุกข้อที่ใช้): ☐ ข้อมูลไบโอเมตริกซ์ ☐ ข้อมูลการติดต่อ ☐ ข้อมูลการเงิน ☐ ข้อมูลบุคลากรของรัฐ ☐ หมายเลขบัตรประชาชน ☐ ข้อมูลการติดต่อกับหน่วยงานต่าง ๆ ☐ ข้อมูลทางการแพทย์ ☐ อื่น ๆ : โปรดระบุ จำนวนข้อมูล (Record) ที่ได้รับผลกระทบ: โปรดระบุ ผลกระทบอื่น ๆ ที่เกิดขึ้น: โปรดระบุ

ง๑.๔ รายละเอียดของระบบ หรือข้อมูลที่ได้รับผลกระทบ (Information of Affected System)

หมายเลข CVE: โปรตระกูล

ช่องโหว่ที่ถูกใช้โจมตี: โปรตระกูล

การใช้ระบบหรือเครื่องที่ได้รับผลกระทบเป็นฐานเพื่อโจมตีขยายผลไปยังระบบหรือเครื่องอื่น:

โปรตระกูล

อาการหรือสิ่งผิดปกติ (เลือกได้มากกว่า ๑ รายการ)

- | | |
|--|---|
| ☐ ระบบล่ม | ☐ รายการข้อมูลจราจรทางคอมพิวเตอร์ที่ผิดปกติ |
| ☐ บัญชีผู้ใช้ถูกสร้างขึ้นใหม่โดยไม่ทราบสาเหตุ หรือ บัญชีผู้ใช้มีความผิดปกติ | |
| ☐ การโจมตีด้วยวิศวกรรมสังคม (Social Engineering) ทั้งที่สำเร็จและไม่สำเร็จ | |
| ☐ ประสิทธิภาพของระบบด้อยลง (ทั้งที่รู้ว่าเป็นเพราะเหตุภัยคุกคามและที่ไม่รู้สาเหตุ) | |
| ☐ การเปลี่ยนแปลงใน DNS หรือ กฎของ Router หรือกฎไฟร์วอลล์ โดยไม่ทราบสาเหตุ | |
| ☐ การยกระดับสิทธิ์การเข้าถึงระบบโดยไม่ทราบสาเหตุ | |
| ☐ การตรวจพบการทำงานของโปรแกรมหรืออุปกรณ์ Sniffer เพื่อจับการรับส่งข้อมูลภายในเครือข่าย | |
| ☐ การเข้าใช้งานครั้งสุดท้ายของผู้ใช้ที่ไม่สอดคล้องกับการใช้งานครั้งสุดท้ายที่เกิดขึ้นจริง | |
| ☐ การแจ้งเตือนจากเครื่องมือตรวจจับการบุกรุก | |
| ☐ การเข้ามาลาดตระเวน (Probing) หรือการเรียกดู (Browsing) ที่น่าสงสัย | |
| ☐ รูปแบบการใช้งานที่ผิดปกติ | ☐ การเปลี่ยนแปลงขนาดไฟล์ไปจากเดิมแบบผิดปกติ |
| ☐ ความพยายามที่จะเขียนไฟล์ของระบบ | ☐ การเปลี่ยนแปลงวันที่ของไฟล์ไปจากเดิมแบบผิดปกติ |
| ☐ การแก้ไขหรือลบข้อมูลที่ผิดปกติ | ☐ การโจมตีให้เกิดการปฏิเสธการให้บริการ (DOS, DDOS) |
| ☐ ไฟล์ใหม่ถูกสร้างขึ้นโดยไม่ทราบสาเหตุ | ☐ การใช้งานหรือมีกิจกรรมที่เกิดในเวลาที่ไม่ปกติ |
| ☐ การแก้ไขหน้าเว็บ | ☐ การสร้างแฟ้มข้อมูล setuid หรือ setgid ใหม่ที่ผิดปกติเกิดขึ้น |
| ☐ การเปลี่ยนแปลงในไดเรกทอรีและแฟ้มข้อมูลของระบบปฏิบัติการที่ผิดปกติ | |
| ☐ การตรวจพบโปรแกรมเจาะระบบ (Crack utility) | |
| ☐ สิ่งผิดปกติไปจากเดิมอื่น ๆ: โปรตระกูล | |

ง๑.๕ รายละเอียดของเหตุภัยคุกคามตามลำดับเวลา ตั้งแต่การโจมตีครั้งแรก จนถึงปัจจุบัน

(เช่น ลำดับของการโจมตี, Attack vector, เทคนิคหรือเครื่องมือที่ผู้โจมตีใช้ ฯลฯ) โปรดระบุ
ง๑.๖ รายละเอียดอื่น ๆ ที่เกี่ยวข้องกับเหตุภัยคุกคาม: โปรดระบุ
ง๒. ข้อมูลการระงับปราบปราม และฟื้นฟู
ง๒.๑ รายละเอียดการดำเนินการเพื่อแก้ไขเหตุภัยคุกคาม: โปรดระบุ
ง๒.๒ การคาดการณ์ความสามารถฟื้นฟู โปรดระบุรายละเอียดการฟื้นฟู ทรัพยากรที่ต้องใช้และที่ต้องการเพิ่ม และประมาณระยะเวลาการฟื้นฟู
ง๓. ข้อมูลกิจกรรมภายหลังการแก้ปัญหา (ถ้ามี)
ง๓.๑ วัน เวลา ที่เหตุภัยคุกคามสิ้นสุด วันที่: เลือกวันที่ เวลา: โปรดระบุ
ง๓.๒ การดำเนินการเพื่อป้องกันเหตุภัยคุกคามที่คล้ายคลึงกัน: โปรดระบุ
ง๓.๓ บทเรียนที่ได้จากเหตุภัยคุกคาม: โปรดระบุ

เอกสาร ก๓ แบบรายงานสรุปภัยคุกคามทางไซเบอร์ในหนึ่งรอบปี

ข้อ ๑ สถิติรายปีจำแนกตามหมวดหมู่ของภัยคุกคามทางไซเบอร์

หมวดหมู่	คำอธิบาย	จำนวน
๐	เหตุการณ์จำลองและการฝึกโจมตีของหน่วยงาน (Training and Exercises)	
๑	การพยายามเข้าถึงระบบที่ไม่สำเร็จ (Unsuccessful Activity Attempt)	
๒	การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance)	
๓	การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยที่หน่วยงานกำหนด (Non-Compliance Activity)	
๔	การบุกรุกโดยการโจมตีด้วยมัลแวร์ (Malicious Logic)	
๕	การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion)	
๖	การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion)	
๗	การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)	
๘	เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating)	
๙	เหตุการณ์ผิดปกติที่ได้รับการวิเคราะห์แล้วว่าไม่ใช่เหตุการณ์ที่เป็นภัยคุกคาม (Explained Anomaly)	

ข้อ ๒ สถิติรายปีจำแนกตามทรัพย์สินที่ได้รับผลกระทบ

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

ข้อ ๓ สถิติรายปีจำแนกตามระดับภัยคุกคามทางไซเบอร์

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

ภาคผนวก ๗

การดำเนินการมาตรการในการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (detection and analysis)

ระดับ	แนวปฏิบัติพื้นฐาน (Security Control Baselines)
กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับร้ายแรง	(๑) จัดให้มีกลไกที่สามารถตรวจจับสิ่งบ่งชี้หรือลักษณะเบื้องต้นของการเกิดภัยคุกคามทางไซเบอร์ได้ในเวลาอันเหมาะสม โดยอาจอาศัยข้อมูลจากแหล่งข้อมูลต่าง ๆ เช่น ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เป็นต้น (๒) จัดให้มีกลไกที่สามารถรับการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์ (๓) จัดให้มีข้อพึงปฏิบัติพื้นฐานเกี่ยวกับการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (logs) ข้อความการแจ้งข้อผิดพลาด หรือข้อความเตือนภัยจากเครื่องมือรักษาความปลอดภัยด้านไซเบอร์ และการตรวจสอบระบบงานที่มีความสำคัญ (critical systems) โดยจะต้องจัดให้มีข้อพึงปฏิบัติที่สูงขึ้นสำหรับทุกระบบงานที่มีความสำคัญมากขึ้น (๔) วิเคราะห์ข้อมูลและประวัติการใช้งานต่าง ๆ เช่น ลักษณะการใช้งานเครือข่ายและระบบงาน (profile networks and systems) เป็นต้น เพื่อทำความเข้าใจพฤติกรรมการใช้งานในช่วงเวลาปกติ (normal behaviors) ทำการศึกษาวิจัยและค้นหาความสัมพันธ์ของข้อมูลในระบบกับสถานการณ์ต่าง ๆ (event correlation) (๕) ทันทิที่พบว่ามี หรืออาจมีภัยคุกคามทางไซเบอร์เกิดขึ้น ให้ดำเนินการสืบหาและรวบรวมข้อมูลทั้งหมด เช่น ลักษณะภัยคุกคามทางไซเบอร์, ช่องโหว่ที่อาจถูกใช้ในการโจมตี, สถานการณ์ของการโจมตี (อาทิ กำลังเกิดเหตุหรือสถานการณ์ได้สิ้นสุดแล้ว การโจมตีเป็นผลสำเร็จหรือไม่สำเร็จ ฯลฯ) จำนวนระบบหรือบริการที่ได้รับผลกระทบ, โโฮสต์เนม ตำแหน่งหรือสถานที่ของระบบหรือบริการที่ได้รับผลกระทบ ข้อมูลผู้ใช้ เวลาประทับ ข้อมูล payload ข้อมูลแจ้งเตือนจาก IDS (ถ้ามี) และข้อมูลจราจรทางคอมพิวเตอร์ (log) เป็นต้น โดยหน่วยงานจะต้องเก็บรักษาข้อมูลดังกล่าว (safeguard incident data) ให้มีความปลอดภัย เพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์

	และใช้เป็นพยานหลักฐานในการดำเนินคดี รวมถึงการจัดทำรายงานที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ (๖) ระบุหมวดหมู่ของภัยคุกคามทางไซเบอร์ตามสถานการณ์ที่เกิดขึ้น และติดตามเพื่อระบุหมวดหมู่ของภัยคุกคามทางไซเบอร์ที่เปลี่ยนแปลงไปจนกว่าสถานการณ์ดังกล่าวจะสิ้นสุด โดยอาจพิจารณาจากข้อมูลตามที่ระบุในข้อ ๒ ของภาคผนวกแนบท้ายนี้ (๗) จัดลำดับความสำคัญของการดำเนินการเพื่อรับมือกับภัยคุกคามทางไซเบอร์ให้ทันทั่วทั้งที่ โดยพิจารณาปัจจัยต่าง ๆ ที่เกี่ยวข้อง เช่น ผลกระทบต่อการทำงานของระบบ (functional impact) ผลกระทบต่อข้อมูล (information impact) และความสามารถในการกู้คืน (recoverability effort) เป็นต้น (๘) ศึกษาวิธีและลักษณะการโจมตี พร้อมทั้งระบุสาเหตุที่แท้จริงของภัยคุกคามทางไซเบอร์รวมถึงจุดอ่อนของระบบที่ถูกโจมตี (๙) ดำเนินการแจ้งไปยังผู้ที่เกี่ยวข้องในการเผชิญเหตุหรือผู้ที่เกี่ยวข้องผ่านช่องทางที่มีความปลอดภัย โดยคำนึงถึงระดับชั้นความลับและความสำคัญของข้อมูล เพื่อให้บุคคลดังกล่าวสามารถปฏิบัติหน้าที่ในการรับมือกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้น (๑๐) รายงานภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับบริการของโครงสร้างพื้นฐานสำคัญทางสารสนเทศอย่างมีนัยสำคัญให้ผู้ที่เกี่ยวข้องทราบ ภายในระยะเวลาที่หน่วยงานควบคุมหรือกำกับดูแลกำหนด (โดยหน่วยงานควบคุมหรือกำกับดูแลอาจกำหนดให้นำข้อปฏิบัติตามแผนการกู้คืนของหน่วยงานมาประกอบการพิจารณาด้วยก็ได้) หรืออาจเทียบเคียงจากตัวอย่างตามที่ระบุในข้อ ๓ ของภาคผนวกแนบท้ายนี้ แล้วแต่กรณี
--	---

กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับวิกฤติ	ให้หน่วยงานดำเนินการตามข้อ ๑ ถึงข้อ ๒ และดำเนินการมาตรการเพิ่มเติม ดังนี้ (๑) จัดให้มีกลไกที่สามารถแจ้งเตือนได้ทันที (real-time alerts) เมื่อพบว่าภัยคุกคามทางไซเบอร์เกิดขึ้น (๒) จัดให้มีกลไกหรือระบบงานที่สามารถติดตามเหตุการณ์ และสามารถจัดเก็บและวิเคราะห์ข้อมูลต่าง ๆ เพื่อตรวจจับการเกิดภัยคุกคามทางไซเบอร์ได้โดยอัตโนมัติ(ถ้าหน่วยงานมีความพร้อม) (๓) จัดให้มีการแจ้งเตือนเกี่ยวกับความผิดปกติของการใช้ทรัพยากรของระบบงาน เช่นแจ้งเตือนเมื่อหน่วยความจำที่ใช้ในการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์เหลือน้อย(storage capacity warning) เมื่อมีการใช้หน่วยประมวลผลกลาง (CPU) หรือมีการใช้หน่วยความจำหลัก (RAM) ของอุปกรณ์เครือข่ายหรือระบบงานหลักที่สูงผิดปกติ หรือเมื่อมีการส่งข้อมูลออกนอกเครือข่ายมากผิดปกติ เป็นต้น (๔) วิเคราะห์ข้อมูลและค้นหาความสัมพันธ์ของข้อมูลกับเหตุการณ์ต่าง ๆ (information correlation) โดยอาจรับข้อมูลจากแหล่งข้อมูลอื่น ๆ นอกเหนือจากข้อมูลในระบบเพื่อเพิ่มความสามารถในการรับรู้และดำเนินการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ
---	--

ภาคผนวก ๘

การดำเนินการมาตรการเพื่อระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคามทางไซเบอร์และการฟื้นฟูระบบงานที่ได้รับผลกระทบ (containment, eradication, and recovery)

ระดับ	แนวปฏิบัติพื้นฐาน (Security Control Baselines)
กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง	(๑) ดำเนินการตามแนวทางหรือวิธีการในการจำกัดขอบเขตและระงับภัยคุกคามทางไซเบอร์ โดยที่แนวทางหรือวิธีการดังกล่าวจะต้องมีหลักเกณฑ์ที่ชัดเจนเพื่อใช้ประกอบการตัดสินใจในการดำเนินการ ทั้งนี้ แนวทางดังกล่าวรวมถึง (๑.๑) การดำเนินการเชิงเทคนิค เช่น การลบมัลแวร์ การปิดการใช้งานบัญชีของผู้ใช้งานที่ถูกละเมิด การปิดระบบหรือตัดการเชื่อมต่อของระบบจากเครือข่ายภายหลังการเก็บหลักฐานหรือข้อมูลที่จำเป็นเพื่อใช้ในการกระบวนการทางนิติวิทยาศาสตร์และใช้เป็นพยานหลักฐานในการดำเนินคดีแล้ว เป็นต้น (๑.๒) การดำเนินการเชิงบริหาร เช่น กำหนดแนวทางดำเนินการหรือการตัดสินใจของฝ่ายบริหารของหน่วยงาน การสื่อสารทั้งภายในและภายนอกหน่วยงาน เป็นต้น (๑.๓) การเตรียมการเพื่อดำเนินการทางกฎหมายกับผู้กระทำความผิด (๒) ดำเนินการตามแนวปฏิบัติที่เกี่ยวข้องเพื่อเก็บรวบรวมและจัดการหลักฐานต่าง ๆ ที่เกี่ยวข้องกับการก่อภัยคุกคามทางไซเบอร์โดยทันทีหลังจากที่ตรวจพบ เช่น การจัดการกับข้อมูลที่บันทึกอยู่ในหน่วยความจำประเภทที่สามารถสูญหายได้เมื่อปิดอุปกรณ์ (volatile data) การเก็บข้อมูลจราจรทางคอมพิวเตอร์ (logs) ข้อมูลเกี่ยวกับมัลแวร์ ข้อมูลสถานะของระบบ (system snapshot) หรือข้อมูลอื่น ๆ ที่จำเป็นให้เพียงพอสำหรับใช้วิเคราะห์ในเชิงเทคนิค และเพื่อใช้ในการกระบวนการทางนิติวิทยาศาสตร์และใช้เป็นพยานหลักฐานในการดำเนินคดี (๓) ดำเนินการเพื่อให้มีการระบุแหล่งที่มาของการโจมตี (attacking host) เช่น การระบุหมายเลขประจำเครื่อง (IP address) การระบุช่องทางที่ผู้โจมตีใช้ การค้นหาและวิจัยที่มาของการโจมตีจากแหล่งข้อมูลต่าง ๆ เช่น ฐานข้อมูลภัยคุกคามทางไซเบอร์ที่รวบรวมข้อมูลจากหลายแหล่ง เป็นต้น

	(๔) ประสานงานเพื่อแจ้งหรือรายงานสถานการณ์การรับมือภัยคุกคามทางไซเบอร์และความคืบหน้าในการตอบสนองไปยังบุคคลหรือหน่วยงานที่เกี่ยวข้อง ตลอดจนผู้ที่อาจได้รับผลกระทบ อย่างทันท่วงที โดยอาจขอความช่วยเหลือไปยังบุคคลหรือหน่วยงานต่าง ๆ โดยเฉพาะการเกิดภัยคุกคามทางไซเบอร์ที่จัดอยู่ในหมวดหมู่ที่ ๑, ๒, ๔, ๕ และ ๗ ตามที่ระบุในข้อ ๑ ของภาคผนวกแนบท้ายนี้ ทั้งนี้ ในการแจ้งหรือรายงานสถานการณ์นั้น หน่วยงานควรเลือกใช้ช่องทางที่มีความเหมาะสมและปลอดภัยและดำเนินการแจ้งหรือรายงานเหตุภายในระยะเวลาที่หน่วยงานควบคุมหรือกำกับดูแลกำหนด หรืออาจเทียบเคียงจากตัวอย่างตามที่ระบุในข้อ ของภาคผนวกแนบท้ายนี้ แล้วแต่กรณี ดำเนินการจัดการกับช่องโหว่ทั้งหมดที่ได้รับผลกระทบจากภัยคุกคามทางไซเบอร์และดำเนินการตามวิธีการป้องกันระบบจากความเสียหายที่อาจเกิดขึ้นเพิ่มเติม เช่น การปรับเปลี่ยนการควบคุมการเข้าถึงเครือข่าย (อาทิ ไฟร์วอลล์) การติดตั้งลายเซ็นของAnti-Virus หรือ IDS / IPS ใหม่ หรือการเปลี่ยนแปลงทางกายภาพในโครงสร้างพื้นฐานและดำเนินการระงับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นโดยทันทีหลังจากที่ตรวจพบเป็นต้น (๖) ดำเนินการที่เกี่ยวข้องเพื่อให้มั่นใจว่าระบบงานต่าง ๆ ยังคงสามารถใช้งานได้ตามปกติภายในกรอบระยะเวลาที่กำหนด (restore within time period) เช่น การกู้คืนระบบให้กลับมาดำเนินการได้ตามปกติ (integrity restoration) การสร้างระบบงานขึ้นใหม่(rebuild) การแทนที่ไฟล์ที่ได้รับผลกระทบ (replace) การติดตั้งโปรแกรมคอมพิวเตอร์(install) การเปลี่ยนแปลงรหัสผ่าน และการรักษาความปลอดภัยทางเครือข่าย(securing network) เป็นต้น
--	---

	(๗) สร้างมาตรการป้องกันทั้งเชิงรุกและเชิงรับเพื่อป้องกันไม่ให้เกิดภัยคุกคามทางไซเบอร์ที่มีลักษณะคล้ายคลึงกันเกิดขึ้นอีกในอนาคต เช่น การเพิ่มมาตรการเฝ้าระวังสัญญาณเตือนและเหตุการณ์ต่าง ๆ ที่มีความเกี่ยวข้องกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นแล้ว เป็นต้น
กรณีบริการ ระบบ หรือ อุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับร้ายแรง	ให้หน่วยงานดำเนินการตามข้อ ๑ และดำเนินการมาตรการเพิ่มเติมดังนี้ (๑) หากมีความจำเป็น ให้หน่วยงานดำเนินการใช้ระบบงานสำรองสำหรับการประมวลผล (attornate processing) การจัดเก็บข้อมูล (storage ite) และกู้คืนข้อมูลที่เกี่ยวข้องกับการทำรายการหรือการดำเนินธุรกรรมต่าง ๆ (transaction recovery) (๒) ส่งคำแจ้งเตือนเพื่อขอรับการสนับสนุน ความช่วยเหลือ หรือประสานความร่วมมือไปยังหน่วยงานที่เกี่ยวข้อง (supply chain coordination) รวมถึงแจ้งไปยังศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (๓) ดำเนินการตามนโยบายการรายงานเกี่ยวกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นภายในหน่วยงานซึ่งครอบคลุมถึงรูปแบบ ระดับ ความลับ และเนื้อหาที่ต้องรายงาน ลำดับขั้น การรายงาน กำหนดเวลา เครื่องมือที่ใช้รายงาน (โดยอาจพิจารณาใช้เครื่องมือที่สามารถช่วยรายงานภัยคุกคามโดยอัตโนมัติ (ถ้าหน่วยงานมีความพร้อม) ให้การช่วยเหลือ สนับสนุน หรือปฏิบัติงานร่วมกับสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ หน่วยงานควบคุมหรือกำกับดูแล พนักงาน เจ้าหน้าที่ หรือบุคคลอื่นใดที่ปฏิบัติหน้าที่ หรือได้รับมอบหมายให้ปฏิบัติหน้าที่ ตามกฎหมาย พิจารณาจัดให้มีกลไกที่สามารถทำงานได้โดยอัตโนมัติ ในการรับมือหรือสนับสนุน การรับมือเมื่อเกิดภัยคุกคามทางไซเบอร์ (automated incident handling processes) (ถ้าหน่วยงานมีความพร้อม)

กรณีบริการ ระบบ หรือ อุปกรณ์มีแนวโน้มที่จะเกิด ผลกระทบเป็นภัยคุกคามทาง ไซเบอร์ในระดับวิกฤติ	ให้หน่วยงานดำเนินการตามข้อ ๑ ถึงข้อ ๒ และดำเนินมาตรการ เพิ่มเติม ดังนี้ (๑) ดำเนินการตามแผนการทำงานในการกู้คืนระบบงานต่าง ๆ เพื่อให้ระบบสามารถให้บริการได้ภายในกรอบระยะเวลาที่ กำหนด (restore within time period) โดยอาศัยความรู้จาก ทีมผู้เชี่ยวชาญด้านต่าง ๆ เพื่อให้การกู้คืนระบบและเครือข่าย ของหน่วยงานทำได้อย่างรวดเร็ว
--	---

ภาคผนวก ๙

การดำเนินการมาตรการเพื่อระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคามทางไซเบอร์และการฟื้นฟูระบบงานที่ได้รับผลกระทบ (containment, eradication, and recovery)

ระดับ	แนวปฏิบัติพื้นฐาน (Security Control Baselines)
กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับร้ายแรง กรณีบริการ ระบบ หรือ อุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับวิกฤติ	ภายหลังการแก้ไขปัญหาภัยคุกคามทางไซเบอร์ ให้หน่วยงานพิจารณาดำเนินการดังนี้ (๑) นำเหตุการณ์ที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นและมีลักษณะเป็นภัยคุกคามทางไซเบอร์ที่มีนัยสำคัญมาป็นกรณีศึกษา เช่น การพิจารณาถึงจุดอ่อนของโครงสร้างพื้นฐานของบริการ นโยบายและกระบวนการ การฝึกอบรม การระบุผู้มีอำนาจดำเนินงาน และเครื่องมือที่ใช้ เป็นต้น และหาแนวทางเพื่อเตรียมการรับมือและป้องกันการเกิดภัยคุกคามทางไซเบอร์ที่มีลักษณะดังกล่าวร่วมกับบุคคลหรือหน่วยงานที่เกี่ยวข้อง (๒) รวบรวมข้อมูลการดำเนินงานที่เกี่ยวข้องกับการรับมือภัยคุกคามทางไซเบอร์ (โดยอาจดำเนินการเป็นรายสัปดาห์หรือรายเดือน) เช่น จำนวนของภัยคุกคามทางไซเบอร์ที่เกิดขึ้น เวลาที่ใช้ในการจัดการกับภัยคุกคามทางไซเบอร์ประเภทต่าง ๆ และวัตถุประสงค์ของการโจมตี เป็นต้น เพื่อเสนอต่อผู้ที่มีหน้าที่ดูแลและรับผิดชอบภายในหน่วยงาน (๓) ปรับปรุงมาตรการเตรียมการและป้องกัน รับมือปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับให้มีความเหมาะสม และเป็นปัจจุบัน (๔) เก็บรักษาข้อมูลและหลักฐานที่จำเป็น เพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์ หรือใช้ในกรณีที่ต้องการร้องทุกข์หรือดำเนินคดี ตามแนวทางและระยะเวลาการเก็บรักษาหลักฐานเกี่ยวกับการก่อภัยคุกคามทางไซเบอร์ที่หน่วยงานได้กำหนด

ภาคผนวก ๑๐

ตัวอย่าง : รายการตรวจสอบการจัดการเหตุการณ์ (Incident Handling Checklist)

รายการตรวจสอบการจัดการเหตุการณ์		Complete
ขั้นการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (detection and analysis)		
๑	ตรวจสอบว่ามีเหตุการณ์เกิดขึ้นหรือไม่	
๑.๑	วิเคราะห์ตรวจจับสัญญาณเหตุการณ์ความปลอดภัยทางไซเบอร์	
๑.๒	ค้นหาข้อมูลเพิ่มเติมที่มีความสัมพันธ์กัน	
๑.๓	ดำเนินการสืบค้นข้อมูล (เช่น search engines, ฐานข้อมูลอื่น ๆ เป็นต้น)	
๑.๔	ทันทีที่ผู้จัดการรับมือฯ เหตุการณ์เชื่อว่ามีเหตุการณ์เกิดขึ้น ให้เริ่มบันทึกการสอบสวนและรวบรวมหลักฐาน	
๒	จัดลำดับความสำคัญในการจัดการเหตุการณ์ตามระดับความรุนแรงของภัยคุกคามที่เกิดขึ้น	
๓	รายงานเหตุการณ์ดังกล่าวต่อผู้บริหารและหน่วยงานภายนอกที่เกี่ยวข้อง	
ขั้นการระงับภัยคุกคาม ปรามปราม และฟื้นฟูระบบงานที่ได้รับผลกระทบ (containment, eradication, and recovery)		
๔	บันทึกเหตุการณ์, จัดเก็บและดูแลรักษาหลักฐานเกี่ยวกับเหตุการณ์ทั้งหมดก่อนเริ่มกระบวนการกู้คืนซึ่งรวมถึงการได้มาของบันทึกการยึดหลักฐานคอมพิวเตอร์ที่ได้มา หรืออุปกรณ์อื่น ๆ เพื่อสนับสนุนการสอบสวน	
๕	จำกัดขอบเขต (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์	
๖	ดำเนินการสอบสวน (Investigate) สาเหตุและผลกระทบของเหตุการณ์	
๗	ทำการกำจัดสาเหตุ (Eradicate the incident)	
๗.๑	ระบุช่องโหว่ของระบบที่โดนโจมตีและบรรเทาผลกระทบที่เกิดขึ้น	
๗.๒	กำจัด หรือลบมัลแวร์ และสาเหตุภัยคุกคามอื่นๆ	
๗.๓	หากมีการตรวจพบว่ามีระบบใหม่ได้รับผลกระทบ (เช่น การติดมัลแวร์ใหม่) ให้ทำซ้ำขั้นตอนการตรวจจับและการวิเคราะห์ภัยคุกคามทางไซเบอร์ (detection and analysis)	

๘	เรียกใช้งานกระบวนการกู้คืน (Recovery Process)	
๘.๑	ระบบที่ได้รับผลกระทบจากภัยคุกคามกลับสู่สถานะพร้อมใช้งาน	
๘.๒	ยืนยันว่าระบบที่ได้รับผลกระทบกลับมาทำงานได้ตามปกติ	
๘.๓	หากจำเป็น ให้ดำเนินการติดตามสถานการณ์ต่อไป เพื่อค้นหาเหตุการณ์ ความมั่นคงปลอดภัยไซเบอร์ที่อาจเกี่ยวข้องในอนาคต	
การดำเนินการภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ (Post-Incident Activity)		
๙	จัดทำรายงานการติดตามผล	
๑๐	จัดการประชุมทบทวนบทเรียนที่เกิดจากเหตุการณ์ดังกล่าว	

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร