



สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ
Office of the National Land Policy Board

แผนการรับมือ

ภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร

โครงการจัดทำแผนบริหารจัดการความปลอดภัยด้านเทคโนโลยีสารสนเทศ
และการสื่อสารของสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ





สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ

แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร

	ชื่อเอกสาร แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร		
	ระดับชั้นความลับ ใช้ภายในสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น	เวอร์ชัน 1.0	หน้า 1

คำนำ

แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสารเป็นส่วนหนึ่งของแผนบริหารจัดการความปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสารถูกจัดทำขึ้นเพื่อสร้างกรอบแนวทางในการป้องกัน ตรวจสอบ และฟื้นฟูจากเหตุภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร แผนนี้ได้รับการพัฒนาภายใต้การพิจารณาถึงสภาพแวดล้อมทางเทคโนโลยีในปัจจุบัน กฎหมายและมาตรฐานที่เกี่ยวข้อง ตลอดจนประสบการณ์และกรณีศึกษาจากภัยคุกคามทางไซเบอร์ทั้งในระดับประเทศและระดับสากล ทั้งนี้ การจัดทำแผนฉบับนี้เกิดจากการบูรณาการข้อมูลและผลการศึกษาอย่างรอบด้าน เช่น การวิเคราะห์สถานการณ์ภัยคุกคามทางเทคโนโลยีสารสนเทศ การทบทวนกฎหมายและมาตรฐานระดับชาติ การประเมินบริบทขององค์กร ตลอดจนการพิจารณาความเหมาะสมในการนำเทคโนโลยีใหม่ ๆ มาปรับใช้ในองค์กร

	ชื่อเอกสาร แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร		
	ระดับชั้นความลับ ใช้ภายในสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น	เวอร์ชัน 1.0	หน้า 2

สารบัญ

1	บทนำ.....	7
1.1	คำนิยาม	9
1.1.1	คำนิยามทั่วไป.....	9
1.1.2	คำนิยามเหตุการณ์ (Event Definition)	18
1.1.3	ตัวชี้วัดของแผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร.....	19
1.1.4	ข้อมูลติดต่อและการยกระดับการดำเนินการ (Contact Information and Escalation Level).....	20
1.1.5	หน้าที่และความรับผิดชอบ (Roles and Responsibilities)	22
2	กรอบการรับมือเหตุการณ์คุกคามทางไซเบอร์ (Incident Response Framework)	27
2.1	ขั้นตอนที่ 1 รายละเอียดการเตรียมการ (Preparation).....	30
2.1.1	การรายงานเหตุการณ์คุกคามทางไซเบอร์ (Reporting Incidents).....	31
2.2	ขั้นตอนที่ 2 การตรวจจับและวิเคราะห์ (Detection and Analysis)	32
2.2.1	การตรวจจับ (Detection).....	32
2.2.2	เหตุการณ์กับภัยคุกคามทางไซเบอร์ (Events Versus Incidents).....	32
2.2.3	การวิเคราะห์ (Analysis)	33
2.3	ขั้นตอนที่ 3 การจำกัดขอบเขต (Containment) การกำจัด (Eradication) และการกู้คืน (Recovery).....	41
2.3.1	ขั้นตอนที่ 3.1 การจำกัดขอบเขต (Containment).....	41
2.3.2	ขั้นตอนที่ 3.2 รายละเอียดการกำจัด (Eradication).....	47
2.3.3	ขั้นตอนที่ 3.3 รายละเอียดการกู้คืน (Recovery Details).....	48
2.4	ขั้นตอนที่ 4 การทบทวนหลังการดำเนินการ (After-Action Review Process).....	49
2.4.1	เอกสาร (Documentation).....	49
2.4.2	บทเรียนที่ได้รับและการแก้ไข (Lessons Learned and Remediation).....	50
2.4.3	การวิเคราะห์ทางนิติวิทยาศาสตร์และการเก็บรักษาข้อมูล	51

	ชื่อเอกสาร แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร		
	ระดับชั้นความลับ ใช้ภายในสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น	เวอร์ชัน 1.0	หน้า 3

2.4.4	การตัดสินใจที่สำคัญสำหรับการออกจากขั้นตอนบทเรียนที่เรียนรู้	51
3	การแจ้งเตือนและการสื่อสาร (Notification and Communication)	52
3.1	การปฏิสัมพันธ์กับการบังคับใช้กฎหมาย (InterAction with Law Enforcement)	52
3.2	หน่วยงานควบคุมหรือกำกับดูแล (Regulatory Authorities)	52
3.3	ผู้รับบริการ (Customers)	53
3.4	การจัดการสื่อสารสาธารณะ (Public Media Handling)	53
4	แผนการทดสอบและทบทวน (Plan Testing and Review)	54
5	รายละเอียดการซ่อมแผนบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยทางไซเบอร์	55
6	ภาคผนวกแผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร	57
6.1	ภาคผนวก 1 รายการกิจกรรมการบันทึก (Logging) การแจ้งเตือน (Alerting) และการเฝ้าระวัง (Monitoring)	57
6.2	ภาคผนวก 2 การอ้างอิงการประเมินเหตุการณ์สองนาที (Two Minute Incident Assessment Reference)	58
6.3	ภาคผนวก 3 รายการตรวจสอบการตอบสนองเหตุการณ์ (Incident Response Checklist)	60
6.4	ภาคผนวก 4 ข้อกำหนดการแจ้งเตือน (Notification Requirements)	62
6.5	ภาคผนวก 5 แฉงการณ์ของสื่อ	66
6.5.1	สคริปต์ที่เตรียมไว้ (Pre-scripted) การรับมือทันทีต่อการสอบถามของสื่อ	66
6.5.2	การตอบกลับแบบมีสคริปต์ล่วงหน้า (Pre-scripted Responses)	66
6.5.3	“หน่วยงานได้ทราบเกี่ยวกับ [สถานการณ์ (Situation) เหตุภัยคุกคามทางไซเบอร์ (Incident) เหตุการณ์ (Event)] และกำลังพยายามหาข้อมูลให้ครบถ้วนมากขึ้นในขณะนี้ เราจะติดต่อคุณได้อย่างไรเมื่อมีข้อมูลเพิ่มเติม”	67
6.5.4	เคล็ดลับการเขียนคำชี้แจง (Statement Writing Tips)	67
6.6	ภาคผนวก 6 เทมเพลตจดหมายผู้รับบริการ (Customer Letter Template)	71
6.6.1	เทมเพลตอีเมลและ/หรือจดหมายอย่างเป็นทางการ (Formal Email and/or Letter Template)	71

	ชื่อเอกสาร แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร		
	ระดับชั้นความลับ ใช้ภายในสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น	เวอร์ชัน 1.0	หน้า 4

6.7 ภาคผนวก 7 หน่วยงานเกี่ยวข้องกับการตอบสนองเหตุภัยคุกคามทางไซเบอร์ (Incident Response Organizations)	72
6.8 ภาคผนวก 8 กลยุทธ์การจำกัดขอบเขต (Containment Strategies)	73
6.8.1 ข้อมูลประจำตัวที่ถูกขโมย (Stolen Credentials)	73
6.8.2 แรนซัมแวร์ (Ransomware)	73
6.8.3 การระบาดของไวรัส (Virus Outbreak)	74
6.9 ภาคผนวก 9 ข้อตกลงการประกันภัยทางไซเบอร์และการบริการบุคคลที่สาม (Cyber Insurance and Third-Party Service Agreements)	75
6.10 ภาคผนวก 10 การสื่อสารแผนการรับมือภัยคุกคามทางไซเบอร์ไปยังบุคลากรที่เกี่ยวข้องทั้งหมด ..	78

	ชื่อเอกสาร แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร		
	ระดับชั้นความลับ ใช้ภายในสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น	เวอร์ชัน 1.0	หน้า 5

สารบัญรูปภาพ

รูปที่ 1-1: ข้อมูลติดต่อและการยกระดับการดำเนินการ	22
รูปที่ 1-2: ข้อมูลสมาชิกทีม CIRT (CIRT Team Members)	27
รูปที่ 2-1: ขั้นตอนการดำเนินการที่เกี่ยวข้องเพื่อจัดการภัยคุกคามทางไซเบอร์(Incident Handling Cycle)	27
รูปที่ 2-2: วงจรชีวิตของการตอบสนองเหตุภัยคุกคามทางไซเบอร์ (Incident Response Life Cycle)	28
รูปที่ 2-3: เปรียบเทียบแนวทางปฏิบัติและประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. 2564.....	28
รูปที่ 2-4: แนวทางการรายงานเหตุภัยคุกคามทางไซเบอร์ (Incident Reporting Guide).....	31
รูปที่ 2-5: การจำแนกหมวดหมู่เหตุภัยคุกคามทางไซเบอร์ (Incident Categorization).....	34
รูปที่ 2-6: ตัวอย่างลักษณะภัยคุกคามทางไซเบอร์แยกตามระดับต่าง ๆ	35
รูปที่ 2-7: จัดหมวดหมู่ภัยคุกคามทางไซเบอร์ตามกรอบงาน MITER ATT&CK	35
รูปที่ 2-8: ตัวอย่างการจัดหมวดหมู่ภัยคุกคามทางไซเบอร์ตามที่กำหนดโดยหน่วยงานหรือนโยบาย การบริหารความเสี่ยงของหน่วยงาน.....	36
รูปที่ 2-9: ตัวอย่างเกณฑ์ผลกระทบการทำงาน (Functional Impact).....	37
รูปที่ 2-10: ตัวอย่างเกณฑ์ผลกระทบต่อสารสนเทศ (Informational Impact)	38
รูปที่ 2-11: การจำแนกระดับการตอบสนอง.....	39
รูปที่ 2-12: ระดับความรุนแรงและการตอบสนองตาม SLA	39
รูปที่ 2-13: ระดับการรับมือช่วยระบุความรุนแรงของภัยคุกคามทางไซเบอร์และความเร่งด่วนของกิจกรรม การรับมือ	40
รูปที่ 2-14: ตัวเลือกการใช้ทรัพยากรตามความรุนแรงของเหตุภัยคุกคามทางไซเบอร์	43
รูปที่ 6-1: รายการกิจกรรมการบันทึก (Logging) การแจ้งเตือน (Alerting) และการเฝ้าระวัง (Monitoring) จัดเตรียมโดย (Prepared by): วันที่ปรับปรุง (Date updated):.....	57
รูปที่ 6-2: การประเมินผลกระทบ/ผลกระทบที่อาจเกิดขึ้น และแนวทางการตอบสนอง	59
รูปที่ 6-3: แนวทางการสื่อสาร.....	60

	ชื่อเอกสาร แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร		
	ระดับชั้นความลับ ใช้ภายในสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น	เวอร์ชัน 1.0	หน้า 6

รูปที่ 6-4: รายการตรวจสอบการตอบสนองเหตุการณ์ (Incident Response Checklist).....	62
รูปที่ 6-5: ตัวอย่างการระบุข้อกำหนดทั้งหมดที่ใช้กับหน่วยงาน	63
รูปที่ 6-6: ตัวอย่างกำหนดระยะเวลาในการแจ้งและรายงานภัยคุกคามทางไซเบอร์	64
รูปที่ 6-7: ตัวอย่างการกำหนดช่องทางสื่อสารและวิธีการเผยแพร่ข้อมูล	65
รูปที่ 6-8: หน่วยงานเกี่ยวข้องกับการตอบสนองเหตุภัยคุกคามทางไซเบอร์.....	72
รูปที่ 6-9: เกณฑ์ Service Level Agreement	76
รูปที่ 6-10: การสนับสนุนและการตอบสนองของบุคคลที่สาม	77
รูปที่ 6-11: ความคุ้มครองประกันภัยและข้อมูลการติดต่อ	77
รูปที่ 6-12: ตัวอย่างการกำหนดการสื่อสารแผนการรับมือภัยคุกคามทางไซเบอร์.....	79

	ชื่อเอกสาร แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร		
	ระดับชั้นความลับ ใช้ภายในสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น	เวอร์ชัน 1.0	หน้า 7

1 บทนำ

แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร เป็นส่วนหนึ่งของ แผนบริหารจัดการความปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ มีรายละเอียดของแผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสารครอบคลุม 4 ประเด็น ได้แก่

1. ป้องกัน (Prevention)

- วัตถุประสงค์: ลดความเสี่ยงที่จะเกิดเหตุการณ์ภัยคุกคาม
- กิจกรรม:
 - การติดตั้งระบบรักษาความปลอดภัย เช่น ไฟร์วอลล์, ระบบป้องกันไวรัส
 - การสร้างความตระหนักรู้ให้กับพนักงานเกี่ยวกับภัยคุกคามทางไซเบอร์
 - การทำการสำรวจและทดสอบความปลอดภัยของระบบเป็นประจำ
 - การอัปเดตซอฟต์แวร์และระบบปฏิบัติการให้เป็นปัจจุบันอยู่เสมอ

2. ตรวจจับและวิเคราะห์ (Detection and Analysis)

- วัตถุประสงค์: ค้นหาและระบุเหตุการณ์ที่ผิดปกติหรือเป็นภัยคุกคาม
- กิจกรรม:
 - การติดตั้งระบบตรวจจับภัยคุกคาม (IDS)
 - การวิเคราะห์ล็อกไฟล์
 - การตรวจสอบกิจกรรมของผู้ใช้ที่ผิดปกติ
 - การตรวจสอบความผิดปกติของระบบเครือข่าย

3. ตอบสนองและควบคุม (Response and Containment)

- วัตถุประสงค์: ควบคุมสถานการณ์และป้องกันไม่ให้เกิดความเสียหายเพิ่มเติม
- กิจกรรม:
 - การตัดการเชื่อมต่อระบบที่ถูกโจมตี
 - การทำการสำเนาข้อมูลที่เกี่ยวข้อง
 - การวิเคราะห์เชิงลึกเพื่อหาสาเหตุของเหตุการณ์
 - การประสานงานกับหน่วยงานที่เกี่ยวข้อง เช่น ตำรวจไซเบอร์

	ชื่อเอกสาร แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร		
	ระดับชั้นความลับ ใช้ภายในสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น	เวอร์ชัน 1.0	หน้า 8

4. กู้คืนและปรับปรุง (Recovery and Lessons Learned)

- วัตถุประสงค์: พ้นพหุระบบให้กลับสู่สภาวะปกติและป้องกันไม่ให้เกิดเหตุการณ์ซ้ำ
- กิจกรรม:
 - การกู้คืนข้อมูลที่เสียหาย
 - การแก้ไขช่องโหว่ที่ถูกใช้ในการโจมตี
 - การทบทวนและปรับปรุงแผนรับมือเหตุการณ์
 - การจัดทำรายงานสรุปเหตุการณ์และบทเรียนที่ได้

จากรายละเอียดของแผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสารครอบคลุม 4 ประเด็น ความเชื่อมโยงของแต่ละประเด็น ดังนี้

- ป้องกัน: เป็นขั้นตอนแรกที่สำคัญในการลดความเสี่ยงที่จะเกิดเหตุการณ์
- ตรวจสอบและวิเคราะห์: ต่อเนื่องจากขั้นตอนการป้องกัน หากมีเหตุการณ์เกิดขึ้น ระบบตรวจสอบจะทำหน้าที่ระบุและวิเคราะห์เหตุการณ์
- ตอบสนองและควบคุม: เมื่อตรวจพบเหตุการณ์แล้ว จะต้องดำเนินการตอบสนองและควบคุมสถานการณ์โดยเร็ว
- กู้คืนและปรับปรุง: เป็นขั้นตอนสุดท้ายที่สำคัญ เพื่อให้มั่นใจว่าองค์กรจะสามารถฟื้นตัวจากเหตุการณ์ได้อย่างรวดเร็ว และป้องกันไม่ให้เกิดเหตุการณ์ซ้ำในอนาคต

แผนการรับมือภัยคุกคามทางไซเบอร์เป็นวงจรที่ต่อเนื่องกัน โดยแต่ละขั้นตอนมีความสำคัญและเชื่อมโยงกัน หากองค์กรมีการวางแผนและปฏิบัติตามขั้นตอนเหล่านี้ จะสามารถลดความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ ทั้งนี้จะมีการจัดการฝึกซ้อมเพื่อจำลองเหตุการณ์ภัยคุกคามจริง เพื่อเตรียมความพร้อมและประเมินความสามารถของทีมในการตอบสนอง

แผนการรับมือเหตุภัยคุกคามทางไซเบอร์ (Incident Management Plan) ได้รับการพัฒนาขึ้นเพื่อให้ทิศทางและเน้นการจัดการภัยคุกคามทางไซเบอร์สารสนเทศที่ส่งผลกระทบต่อของหน่วยงาน ทรัพยากรสารสนเทศ (Information Resources) แผนการรับมือเหตุภัยคุกคามทางไซเบอร์ของหน่วยงาน ใช้กับบุคคลหรือนิติบุคคลใด ๆ ที่ประกาศใช้โดยผู้บัญชาการการรับมือเหตุภัยคุกคามทางไซเบอร์ของหน่วยงานกับการรับมือเหตุภัยคุกคามทางไซเบอร์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศในหน่วยงานและโดยเฉพาะเหตุการณ์ที่ส่งผลกระทบต่อของหน่วยงาน ทรัพยากรสารสนเทศ

วัตถุประสงค์ของแผนการรับมือเหตุภัยคุกคามทางไซเบอร์ คือ เพื่อให้ของหน่วยงานสามารถตอบสนองต่อภัยคุกคามทางไซเบอร์สารสนเทศได้อย่างรวดเร็วและเหมาะสม

แผนการรับมือเหตุภัยคุกคามทางไซเบอร์นี้ไม่ใช้กับเหตุการณ์ที่เกิดจากภัยธรรมชาติไฟฟ้าขัดข้อง ฯลฯ

	ชื่อเอกสาร แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร		
	ระดับชั้นความลับ ใช้ภายในสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น	เวอร์ชัน 1.0	หน้า 9

1.1 คำนิยาม

1.1.1 คำนิยามทั่วไป

คำนิยามในส่วนนี้เป็นการให้คำจำกัดความสำหรับศัพท์ที่ใช้งานใน แผนบริหารจัดการความปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติฉบับนี้ เพื่อให้มีความหมายที่ชัดเจนและเข้าใจตรงกัน

คำศัพท์	ความหมาย
การกู้คืน (Recovery)	การนำข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ และระบบสารสนเทศ ที่เกิดความเสียหายกลับมาใช้งานได้อย่างถูกต้องครบถ้วน
การเข้าถึง (Access)	การอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งานเข้าถึง หรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ
การพิสูจน์และยืนยันตัวตน (Identification and Authentication)	กระบวนการพิสูจน์และยืนยันความถูกต้องของตัวบุคคล (อ้างอิงจาก พ.ร.บ. ว่าด้วย ธูรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2562)
การสำรองข้อมูล (Backup)	การเก็บรักษาข้อมูลคอมพิวเตอร์ลงในสื่อที่ได้เตรียมการไว้แล้ว และจะถูกนำมาใช้งานแทนในกรณีที่ข้อมูลหลักที่กำลังถูกใช้ในการปฏิบัติงาน อยู่เกิดความเสียหาย
ความมั่นคงปลอดภัยด้านไซเบอร์และสารสนเทศ (Cyber and Information Security)	มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกัน รับมือ และลด ความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอก หน่วยงาน
เครือข่าย (Network)	ระบบที่เกิดจากการนำเครื่องคอมพิวเตอร์ตั้งแต่ 2 เครื่องขึ้นไป มา ต่อเชื่อมโยงเข้าด้วยกัน เพื่อแลกเปลี่ยนข้อมูลข่าวสาร หรือใช้ ทรัพยากรต่าง ๆ
ซอฟต์แวร์ (Software)	โปรแกรมคอมพิวเตอร์หรือโปรแกรมประยุกต์ประเภทใด ๆ ก็ได้ ตั้งแต่ ระบบปฏิบัติการเช่น ดอส (Dos) โปรแกรมอำนวยความสะดวก ระบบงาน จนกระทั่งโปรแกรมที่เก็บอยู่ในรอม (Rom)
ไซเบอร์ (Cyber)	ข้อมูลและการสื่อสารที่เกิดจากการให้บริการหรือการประยุกต์ใช้ เครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต หรือโครงข่ายโทรคมนาคม รวมทั้งการให้บริการโดยปกติของดาวเทียมและระบบเครือข่ายที่ คล้ายคลึงกันที่เชื่อมต่อกันเป็นการทั่วไป (อ้างอิงจาก พ.ร.บ. การรักษา ความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562)

	ชื่อเอกสาร แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร		
	ระดับชั้นความลับ ใช้ภายในสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น	เวอร์ชัน 1.0	หน้า 10

คำศัพท์	ความหมาย
ทรัพย์สิน (Assets)	สิ่งที่มีมูลค่าต่อ สคทช. และเป็นเจ้าของ เช่น ว่าจ้าง หรือพัฒนา เป็นต้น
ทรัพย์สินสารสนเทศ	- ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ - ตัวเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ เครื่องบันทึกข้อมูล และอุปกรณ์อื่นใด - ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์ (อ้างอิงจาก พระราชกฤษฎีกา ว่าด้วย วิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2553)
ผู้ใช้งาน (Users)	ผู้ทดลองงาน พนักงาน และลูกจ้างของ สคทช. รวมถึงหน่วยงานภายนอก บุคลากรของหน่วยงานภายนอกที่ปฏิบัติงานให้ สคทช. ที่ได้รับสิทธิเข้าถึงสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศของ สคทช.
ผู้ดูแลระบบ (Administrator)	ผู้ปฏิบัติงาน (Employee)
ผู้พัฒนาระบบ (Developer)	ผู้ที่ได้รับมอบหมายให้มีหน้าที่รับผิดชอบในการพัฒนาและปรับปรุงระบบงานสารสนเทศ
ระบบสารสนเทศ (Information System)	ระบบคอมพิวเตอร์และการเก็บบันทึกข้อมูลซึ่งมีการประมวลผลด้วยระบบคอมพิวเตอร์
สารสนเทศ (Information)	ข้อมูลคอมพิวเตอร์หรือข้อความที่ได้มีการประมวลผล เช่น ทรัพย์สินประเภทฐานข้อมูล (Database) และไฟล์ข้อมูล (Data file) สัญญา (Contract) และข้อตกลง (Agreement) เอกสารและคู่มือระบบงาน (System Document) ข้อมูลวิจัย (Research Document) คู่มือผู้ใช้งาน (User Manual) เอกสารการฝึกอบรม (Training Document) ขั้นตอนการปฏิบัติงาน (Operational or Support Procedure) แผนรองรับความต่อเนื่องทางธุรกิจ (Business Continuity Plan) เอกสาร และข้อมูลจัดเก็บสำรอง (Archived Information) เป็นต้น
สิทธิของผู้ใช้งาน (User Rights)	สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใด ที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน
สิทธิพิเศษ	สิทธิสูงสุดของระบบ หรือสิทธิสำหรับผู้ดูแลระบบหรือเทียบเท่า เช่น บัญชีผู้ใช้ Administrators (Windows), Root (Unix) เป็นต้น

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

	ชื่อเอกสาร แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร		
	ระดับชั้นความลับ ใช้ภายในสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น	เวอร์ชัน 1.0	หน้า 11

คำศัพท์	ความหมาย
(Privileged Access Right)	
เหตุการณ์ (Event Definition)	การเกิดขึ้นที่สังเกตได้ใด ๆ (Observable Occurrence) ในระบบเครือข่าย สภาพแวดล้อม กระบวนการ ลำดับการดำเนินการ หรือบุคลากร เหตุการณ์อาจมีหรือไม่มีลักษณะที่ส่งผลเชิงลบก็ได้
เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Adverse Events)	เหตุการณ์ที่มีผลเชิงลบ (Events with a Negative Consequence)” หรือ “เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์” หมายความว่า เหตุการณ์ที่เกิดจากการกระทำหรือการดำเนินการใด ๆ ที่มีขอบซึ่งกระทำการผ่านทางคอมพิวเตอร์หรือระบบคอมพิวเตอร์ซึ่งอาจเกิดความเสียหายหรือผลกระทบต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือความมั่นคงปลอดภัยไซเบอร์ของคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์
เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยด้านไซเบอร์และสารสนเทศ (Cyber and Information Security Event)	เหตุการณ์ที่เกิดจากการกระทำหรือการดำเนินการใด ๆ ที่มีขอบซึ่งกระทำการผ่านทางคอมพิวเตอร์หรือระบบคอมพิวเตอร์ ซึ่งอาจเกิดความเสียหายหรือผลกระทบต่อการรักษาความมั่นคงปลอดภัยไซเบอร์คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์
ภัยคุกคามทางไซเบอร์ (Incident)	การกระทำหรือการดำเนินการใด ๆ โดยมีขอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้าย ต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นอันตรายที่ใกล้จะถึง ที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือ ข้อมูลอื่นที่เกี่ยวข้อง ภัยคุกคามทางไซเบอร์ อาจมีลักษณะดังต่อไปนี้อย่างน้อยหนึ่งอย่าง ดังนี้: ก. การละเมิด (Violation) นโยบายความมั่นคงปลอดภัยโดยชัดแจ้งหรือโดยนัย ข. ความพยายามในการเข้าถึง (Unauthorized Access) ทรัพยากรสารสนเทศของหน่วยงานโดยไม่ได้รับอนุญาต ค. การปฏิเสธการให้บริการ (Denial of Service) แก่ทรัพยากรสารสนเทศของหน่วยงาน

	ชื่อเอกสาร แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร		
	ระดับชั้นความลับ ใช้ภายในสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น	เวอร์ชัน 1.0	หน้า 12

คำศัพท์	ความหมาย
	ง. การใช้ทรัพยากรสารสนเทศ (Unauthorized Use) ของหน่วยงาน โดยไม่ได้รับอนุญาต จ. การแก้ไขข้อมูล (Unauthorized Modification) ของหน่วยงาน โดยไม่ได้รับอนุญาต ฉ. การสูญเสีย (Loss) ข้อมูลที่เป็นความลับหรือได้รับการคุ้มครองของหน่วยงาน
“ไซเบอร์”	ข้อมูลและการสื่อสารที่เกิดจากการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต หรือโครงข่ายโทรคมนาคม รวมทั้งการให้บริการโดยปกติของ ดาวเทียมและระบบเครือข่ายที่คล้ายคลึงกัน ที่เชื่อมต่อกันเป็นการทั่วไป
อิเล็กทรอนิกส์ (Electronic)	การประยุกต์ใช้วิธีการทางอิเล็กทรอนิกส์ ไฟฟ้า คลื่นแม่เหล็กไฟฟ้า หรือวิธีอื่นใดในลักษณะคล้ายกัน และให้หมายความรวมถึง การประยุกต์ใช้วิธีการทางแสง วิธีการทางแม่เหล็กหรืออุปกรณ์ที่เกี่ยวข้องกับการประยุกต์ใช้วิธีต่าง ๆ เช่นว่านั้น (อ้างอิงจากพ.ร.บ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544)
อุปกรณ์สารสนเทศ (Information Processing Facilities)	เครื่องมือ เครื่องใช้ วัสดุ และอุปกรณ์ต่าง ๆ ที่ประมวลผลหรือจัดเก็บสารสนเทศ เช่น คอมพิวเตอร์ กล้องดิจิทัล สื่อบันทึกข้อมูล สแกนเนอร์ เครื่องพิมพ์
การจ้างงาน (Employment)	การว่าจ้างผู้ปฏิบัติงาน หรือหน่วยงานภายนอก เพื่อปฏิบัติงานหรือให้บริการแก่ สคทช.
การปฏิบัติงานจากระยะไกล (Teleworking)	การทำงานที่บ้านหรือที่สถานที่ตั้งภายนอกองค์กรอื่น ๆ ที่มีการเชื่อมต่อทางอิเล็กทรอนิกส์โดยผ่านทาง เครื่องคอมพิวเตอร์ หรืออุปกรณ์คอมพิวเตอร์พกพาหรือเครื่องโทรสาร เป็นต้น ไปยัง สคทช. หรือสถานที่อื่นอันเป็นสถานที่ทำงานหลัก
ข้อมูลส่วนบุคคล (Personal Data)	ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ (อ้างอิงจาก พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562)
เปลี่ยนแปลงการจ้างงาน (Change of Employment)	เปลี่ยนแปลงหน้าที่รับผิดชอบของผู้ปฏิบัติงานในหน่วยงานต้นสังกัด หรือเงื่อนไขการว่าจ้างของหน่วยงานภายนอก

	ชื่อเอกสาร แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร		
	ระดับชั้นความลับ ใช้ภายในสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น	เวอร์ชัน 1.0	หน้า 13

คำศัพท์	ความหมาย
ดัดแปลง (Tamper)	ทำซ้ำโดยเปลี่ยนรูปแบบใหม่ ปรับปรุงแก้ไขเพิ่มเติม หรือจำลองงานต้นฉบับในส่วนอันเป็นสาระสำคัญโดยไม่มีลักษณะเป็นการจัดทำขึ้นใหม่ ทั้งนี้ ไม่ว่าทั้งหมดหรือบางส่วน ในส่วนที่เกี่ยวกับโปรแกรมประยุกต์ ให้หมายความรวมถึง ทำซ้ำโดยเปลี่ยนรูปแบบใหม่ ปรับปรุงแก้ไขเพิ่มเติมโปรแกรมประยุกต์ในส่วนอันเป็นสาระสำคัญ โดยไม่มีลักษณะเป็นการจัดทำขึ้นใหม่ (อ้างอิงจาก พ.ร.บ. ลิขสิทธิ์ พ.ศ. 2537)
ทำซ้ำ (Copy)	คัดลอกไม่ว่าโดยวิธีใด ๆ เลียบแบบ ทำสำเนา ทำแม่พิมพ์ บันทึกเสียง บันทึกภาพ หรือ บันทึกเสียงและภาพ จากต้นฉบับ หรือจากการโฆษณาในส่วนอันเป็นสาระสำคัญ ทั้งนี้ ไม่ว่าทั้งหมดหรือบางส่วน สำหรับในส่วนที่เกี่ยวกับโปรแกรมประยุกต์ ให้หมายความถึง คัดลอกหรือทำสำเนาโปรแกรมประยุกต์จากสื่อบันทึกใด ๆ ไม่ว่าด้วยวิธีใด ๆ ในส่วนอันเป็นสาระสำคัญ โดยไม่มีลักษณะเป็นการจัดทำขึ้นใหม่ ทั้งนี้ ไม่ว่าทั้งหมดหรือบางส่วน (อ้างอิงจาก พระราชบัญญัติลิขสิทธิ์ พ.ศ. 2537)
ลิขสิทธิ์ (Copyright)	สิทธิแต่ผู้เดียวที่จะทำการใด ๆ ตามพระราชบัญญัติลิขสิทธิ์ พ.ศ. 2537 เกี่ยวกับงานที่ผู้สร้างสรรค์ได้ทำขึ้น (อ้างอิงจาก พ.ร.บ. ลิขสิทธิ์ พ.ศ. 2565)
โปรแกรมประยุกต์ (Program)	คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่นำไปใช้กับเครื่องคอมพิวเตอร์ เพื่อให้เครื่องคอมพิวเตอร์ทำงานหรือเพื่อให้ได้รับผลอย่างหนึ่งอย่างใด ทั้งนี้ ไม่ว่าจะเป็นภาษาโปรแกรมในลักษณะใด
โปรแกรมไม่พึงประสงค์ (Malicious Software)/ มัลแวร์ (Malware)	โปรแกรมหรือชุดโปรแกรมที่ทำให้สารสนเทศ หรือระบบสารสนเทศเกิดความเสียหายโดยตั้งใจ เช่น ไวรัส (Virus) เวิร์ม (Worm) โทรจัน (Trojan) แอดแวร์ (Adware) หรือสปายแวร์ (Spyware) เป็นต้น
ผู้ปฏิบัติงาน (Employee)	ผู้ทดลองงาน พนักงาน พนักงานสัญญาจ้างพิเศษ ลูกจ้างทดลองงาน และลูกจ้างของ สศทช.
ผู้ดูแลห้องคอมพิวเตอร์ (Computer Room Administrator)	ผู้ที่ได้รับมอบหมายให้มีหน้าที่ดูแลรับผิดชอบห้องคอมพิวเตอร์

	ชื่อเอกสาร แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร		
	ระดับชั้นความลับ ใช้ภายในสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น	เวอร์ชัน 1.0	หน้า 14

คำศัพท์	ความหมาย
ภัยคุกคามทางไซเบอร์ (Cyber Threats)	การกระทำหรือการดำเนินการใด ๆ โดยมีขอบ โดยใช้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภัยอันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง (อ้างอิงจาก พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562)
ระบบคอมพิวเตอร์ (Computer System)	อุปกรณ์คอมพิวเตอร์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ (อ้างอิงจากพ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550)
ศูนย์คอมพิวเตอร์ (Data Center)	สถานที่ที่ใช้ในการจัดวางอุปกรณ์ประมวลผลสารสนเทศ ที่ประมวลผลหรือจัดเก็บสารสนเทศที่มีระดับการป้องกันความมั่นคงปลอดภัย “สูง” หรือ “สูงสุด”
สื่อบันทึกข้อมูล (Removable Media Device)	เอกสารที่เป็นกระดาษ หรืออุปกรณ์ที่ใช้ในการบันทึกข้อมูลอิเล็กทรอนิกส์ เช่น เทป ดิสก์ CD DVD Thumb drive เป็นต้น
ห้องคอมพิวเตอร์ (Computer Room)	สถานที่ที่ใช้ในการจัดวางอุปกรณ์ประมวลผลสารสนเทศ ที่ประมวลผลหรือจัดเก็บสารสนเทศที่มีระดับการป้องกันความมั่นคงปลอดภัย “ปานกลาง”
หัวหน้าศูนย์คอมพิวเตอร์ (Data Center Manager)	หัวหน้างานของศูนย์คอมพิวเตอร์
อุปกรณ์คอมพิวเตอร์พกพา (Mobile Device)	อุปกรณ์คอมพิวเตอร์ หรืออุปกรณ์สื่อสารที่สะดวกในการพกพา เช่น คอมพิวเตอร์โน้ตบุ๊ก (Notebook/Laptop) โทรศัพท์มือถือ (Smartphone) เป็นต้น
อุปกรณ์ประมวลผลสารสนเทศ (Information Processing Facilities)	ระบบสารสนเทศ ระบบเครือข่าย สถานที่ตั้งทางกายภาพของระบบสารสนเทศและระบบเครือข่าย ตลอดจนอุปกรณ์และระบบสนับสนุนต่าง ๆ เช่น ระบบไฟฟ้า ระบบการสื่อสาร ระบบแหล่งจ่ายน้ำ แก๊ส ระบบบำบัด ระบบระบายอากาศ ระบบทำความเย็น ระบบปรับอากาศ ระบบควบคุมอุณหภูมิและความชื้น เป็นต้น

	ชื่อเอกสาร	แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร		
	ระดับชั้นความลับ	ใช้ภายในสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น	เวอร์ชัน 1.0	หน้า 15

คำศัพท์	ความหมาย
แอปพลิเคชัน (Application)	โปรแกรมประยุกต์หรือกลุ่มของโปรแกรม ซึ่งทำหน้าที่เพื่อจุดประสงค์อย่างใดอย่างหนึ่ง เช่น เวิร์ดโปรเซสเซอร์ (Word Processor) สเปรดชีต (Spreadsheet) ฐานข้อมูล (Database) เป็นต้น
บล็อกเชน (blockchain)	วิธีการเก็บข้อมูลรายการเปลี่ยนแปลงตามหลักการทางบัญชี โดยการเข้ารหัสและจัดเรียงข้อมูลเหล่านี้ต่อกันตามลำดับเวลาที่ข้อมูลเข้ามา กลุ่มข้อมูลดังกล่าวจะเผยแพร่ไปให้ผู้ใช้ในเครือข่ายที่กำหนดได้ทราบทั่วกัน ทั้งนี้ ผู้ใช้ทุกคนจะทราบการแก้ไขเพิ่มเติมรายการเปลี่ยนแปลงในบล็อกเชนทุกรายการตลอดเวลา
ปัญญาประดิษฐ์ (เอไอ) (artificial intelligence (AI))	สาขาหนึ่งของวิทยาการคอมพิวเตอร์ ซึ่งเน้นเรื่องที่จะทำให้คอมพิวเตอร์ทำงานได้ใกล้เคียงมนุษย์มากขึ้น แบ่งย่อยออกเป็นสาขาต่าง ๆ เช่น การแปลภาษาด้วยเครื่อง ระบบผู้เชี่ยวชาญ วิทยาการหุ่นยนต์ การรู้จำแบบ การรับรู้เยี่ยงมนุษย์ (human perception) ฯลฯ
“การละเมิดข้อมูลส่วนบุคคล”	การละเมิดมาตรการรักษาความมั่นคงปลอดภัย ที่ทำให้เกิดการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคล โดยปราศจาก อำนาจหรือโดยมิชอบ ไม่ว่าจะเกิดจากเจตนา ความจงใจ ความประมาทเลินเล่อ การกระทำโดย ปราศจากอำนาจหรือโดยมิชอบ การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ภัยคุกคามทางไซเบอร์ ข้อผิดพลาดบกพร่องหรืออุบัติเหตุ หรือเหตุอื่นใด
การละเมิดความลับของข้อมูลส่วนบุคคล (Confidentiality Breach)	มีการเข้าถึง หรือเปิดเผยข้อมูลส่วนบุคคล โดยปราศจากอำนาจหรือโดยมิชอบ หรือเกิดจากข้อผิดพลาดบกพร่อง หรืออุบัติเหตุ
การละเมิดความถูกต้องครบถ้วนของข้อมูลส่วนบุคคล (Integrity Breach)	มีการ เปลี่ยนแปลง แก้ไขข้อมูลส่วนบุคคลให้ไม่ถูกต้อง ไม่สมบูรณ์ หรือไม่ครบถ้วน โดยปราศจากอำนาจ หรือโดยมิชอบ หรือเกิดจากข้อผิดพลาดบกพร่องหรืออุบัติเหตุ
การละเมิดความพร้อมใช้งานของข้อมูลส่วนบุคคล (Availability Breach)	ทำให้ ไม่สามารถเข้าถึงข้อมูลส่วนบุคคลได้ หรือมีการทำลายข้อมูลส่วนบุคคล ทำให้ข้อมูลส่วนบุคคลไม่อยู่ใน สภาพที่พร้อมใช้งานได้ตามปกติ
ฝาแฝดดิจิทัล (Digital Twin)	แบบจำลองจำลองเสมือนจากวัตถุทางกายภาพ ทำให้สามารถทำงานได้เหมือนกับวัตถุจริง ซึ่งวัตถุในนี้อาจจะเป็น รถยนต์ ตึก หรือแม้กระทั่งเมืองหนึ่งในโลก มีการติดตั้งตัวเซนเซอร์บนวัตถุจริงหลายตัว ทำหน้าที่เป็นกลไกเชื่อมต่อกันระหว่างตัววัตถุทางกายภาพกับวัตถุเสมือนเชื่อมต่อกันแบบ Real-time ข้อมูลที่เชื่อมเป็นข้อมูลในมุมมองต่าง ๆ ของวัตถุกายภาพเช่น ข้อมูลการใช้พลังงาน อุณหภูมิ สภาพอากาศ ข้อมูลพวกนี้ก็จะถูกนำมาใช้ให้กับตัวแบบโมเดลจำลองนี้ที่อยู่

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

	ชื่อเอกสาร แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร		
	ระดับชั้นความลับ ใช้ภายในสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น	เวอร์ชัน 1.0	หน้า 16

คำศัพท์	ความหมาย
	ในรูปแบบของดิจิทัล จะถูกใช้ในการสร้างแบบจำลอง ศึกษา ประสิทธิภาพ หรือทดลองการพัฒนา ทำให้สามารถนำกลับไปปรับใช้ ในการพัฒนาของวัตถุทางกายภาพได้ ทั้งนี้ตัว Digital Twin จะต่างกับ การทำ Simulation ตรงที่ตัว Digital Twin จะมีการแลกเปลี่ยน ข้อมูลของสภาพแวดล้อมจริง และแลกเปลี่ยนข้อมูลไปกลับระหว่าง วัตถุจริง กับวัตถุเสมือนแบบ Real-time
“ข้อมูลส่วนบุคคล”	ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรง หรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ
ข้อมูลส่วนบุคคลอ่อนไหว	ข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็น ทาง การเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพ แรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใด ซึ่งกระทบ ต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการ ประกาศกำหนด
“ผู้ควบคุมข้อมูลส่วนบุคคล”	บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจ เกี่ยวกับการเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
“ผู้ประมวลผลข้อมูลส่วนบุคคล”	บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับ การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ ควบคุมข้อมูลส่วนบุคคล
“มาตรการที่ใช้แก้ปัญหาเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์”	การแก้ไข ปัญหาความมั่นคงปลอดภัยไซเบอร์โดยใช้บุคลากร กระบวนการ และเทคโนโลยี โดยผ่านคอมพิวเตอร์ ระบบ คอมพิวเตอร์ โปรแกรมคอมพิวเตอร์ หรือบริการที่เกี่ยวข้องกับ คอมพิวเตอร์ใด ๆ เพื่อสร้างความมั่นใจ และเสริมสร้างความมั่นคง ปลอดภัยไซเบอร์ของคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบ คอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์
“โครงสร้างพื้นฐานสำคัญทางสารสนเทศ”	คอมพิวเตอร์หรือระบบคอมพิวเตอร์ ซึ่งหน่วยงานของรัฐหรือ หน่วยงานเอกชนใช้ในกิจการของตนที่เกี่ยวข้องกับการรักษาความ มั่นคงปลอดภัย ของรัฐ ความปลอดภัยสาธารณะ ความมั่นคงทาง เศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็น ประโยชน์ สาธารณะ
“หน่วยงานโครงสร้างพื้นฐานสำคัญทาง สารสนเทศ”	หน่วยงานของรัฐหรือ หน่วยงานเอกชน ซึ่งมีภารกิจหรือให้บริการ โครงสร้างพื้นฐานสำคัญทางสารสนเทศ

	ชื่อเอกสาร แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร		
	ระดับชั้นความลับ ใช้ภายในสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น	เวอร์ชัน 1.0	หน้า 17

คำศัพท์	ความหมาย
“ระบบคอมพิวเตอร์”	อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ
“ข้อมูลคอมพิวเตอร์”	ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทาง อิเล็กทรอนิกส์ด้วย
“ข้อมูลจราจรทางคอมพิวเตอร์”	ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการ หรืออื่นๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น
Managed Security Service Provider: MSSP	บริษัทหรือผู้ที่ให้บริการดูแลรักษาความปลอดภัยข้อมูลองค์กรและป้องกันภัยจากอินเทอร์เน็ต โดยมีหน้าที่ให้บริการคอยเป็นยามตรวจสอบระบบและป้องกันภัยอันตรายที่อาจเกิดขึ้นกับข้อมูล ไม่ว่าจะเป็นการแยกข้อมูลจากผู้บุกรุก การตรวจสอบและเตือนภัยจากไวรัส ในอินเทอร์เน็ต การคัดกรองเว็บไซต์ (Content Filtering) และอีกหลายๆ หน้าที่ที่เกี่ยวข้องกับระบบการรักษาความมั่นคงปลอดภัยสารสนเทศ
Security Operation Center: SOC	ศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ที่ทำหน้าที่เฝ้าระวังและป้องกันระบบหรืออุปกรณ์สำคัญขององค์กรจากการถูกบุกรุกหรือการเข้าถึงโดยไม่ได้รับอนุญาต ซึ่งหากมีเหตุการณ์ด้านความมั่นคงปลอดภัย (Security Incident) เกิดขึ้น เช่น ระบบถูกบุกรุก หรือการเปลี่ยนแปลงแก้ไขข้อมูลโดยไม่ได้รับอนุญาต SOC จะทำหน้าที่ประเมิน ตรวจสอบและแก้ไขเหตุการณ์ที่เกิดขึ้น เพื่อลดผลกระทบและความเสียหายที่อาจเกิดขึ้นกับองค์กรให้อยู่ในระดับที่ไม่รุนแรง
Recovery Time Objective (RTO)	ระยะเวลาในการกู้คืนระบบ
Recovery Point Objective (RPO)	ระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย
Maximum Tolerance Period of Disruption (MTPD)	ระยะเวลาสูงสุดที่ยอมให้ธุรกิจหยุดชะงัก เพื่อรองรับการดำเนินธุรกิจอย่างต่อเนื่องของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและรองรับการเกิดเหตุการณ์ผิดปกติต่าง ๆ

	ชื่อเอกสาร แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร		
	ระดับชั้นความลับ ใช้ภายในสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น	เวอร์ชัน 1.0	หน้า 18

คำศัพท์	ความหมาย
	ที่อาจส่งผลให้เกิดการหยุดชะงักหรือเกิดความเสียหายต่อระบบ เช่น ภัยคุกคามการทำงานได้ตามปกติให้เร็วที่สุด
แผนดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan: BCP)	แผนที่กำหนดแนวทางการดำเนินการของหน่วยงานเมื่อเกิดสภาวะวิกฤตหรือภัยต่าง ๆ ที่ส่งผลให้กระบวนการทำงานของหน่วยงานหยุดชะงัก เพื่อให้สามารถกลับมาดำเนินการได้อย่างต่อเนื่อง โดยเฉพาะงานบริการภาครัฐที่สำคัญต่อประชาชน

1.1.2 คำนิยามเหตุการณ์ (Event Definition)

การเกิดขึ้นที่สังเกตได้ใด ๆ (Observable Occurrence) ในระบบ เครือข่าย สภาพแวดล้อม กระบวนการ ลำดับการดำเนินการ หรือบุคลากร เหตุการณ์อาจมีหรือไม่มีลักษณะที่ส่งผลเชิงลบก็ได้

1.1.2.1 คำนิยามเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Adverse Events Definition)

“เหตุการณ์ที่มีผลเชิงลบ (Events with a Negative Consequence)” หรือ “เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์” หมายความว่า เหตุการณ์ที่เกิดจากการกระทำหรือการดำเนินการใด ๆ ที่มีขอบซึ่งกระทำการผ่านทางคอมพิวเตอร์หรือระบบคอมพิวเตอร์ซึ่งอาจเกิดความเสียหายหรือผลกระทบต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือความมั่นคงปลอดภัยไซเบอร์ของคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์

แผนการรับมือเหตุภัยคุกคามทางไซเบอร์นี้ไม่ใช้กับเหตุการณ์ที่เกิดจากภัยธรรมชาติ ไฟฟ้าขัดข้อง ฯลฯ

1.1.2.2 นิยามภัยคุกคามทางไซเบอร์ (Incident Definition)

“เหตุภัยคุกคามทางไซเบอร์” หมายความว่า เหตุการณ์ที่มีผลเชิงลบที่เกิดจากการกระทำหรือการดำเนินการใด ๆ โดยมีขอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องและเป็นอันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

ภัยคุกคามทางไซเบอร์¹ อาจมีลักษณะดังต่อไปนี้อย่างน้อยหนึ่งอย่าง ดังนี้:

- ก. การละเมิด (Violation) นโยบายความมั่นคงปลอดภัยโดยชัดแจ้งหรือโดยนัย
- ข. ความพยายามในการเข้าถึง (Unauthorized Access) ทรัพยากรสารสนเทศของหน่วยงาน โดยไม่ได้รับอนุญาต

¹ Blue Team Handbook: Incident Response Edition, Don Murdoch และ NIST SP800-61r2: Computer Security Incident Handling Guide

	ชื่อเอกสาร แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร		
	ระดับชั้นความลับ ใช้ภายในสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น	เวอร์ชัน 1.0	หน้า 19

- ค. การปฏิเสธการให้บริการ (Denial of Service) แก่ทรัพยากรสารสนเทศของหน่วยงาน
- ง. การใช้ทรัพยากรสารสนเทศ (Unauthorized Use) ของหน่วยงาน โดยไม่ได้รับอนุญาต
- จ. การแก้ไขข้อมูล (Unauthorized Modification) ของหน่วยงาน โดยไม่ได้รับอนุญาต
- ฉ. การสูญเสีย (Loss) ข้อมูลที่เป็นความลับหรือได้รับการคุ้มครองของหน่วยงาน

1.1.3 ตัวชี้วัดของแผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร

ตัวชี้วัดของแผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร ครอบคลุมเรื่อง การทบทวนแผน การฝึกซ้อมแผน ซึ่งมีรายละเอียดของเป้าหมายและวิธีวัดผล ดังนี้

1. ตัวชี้วัดด้านการทบทวนแผน (Plan Review Metrics)

1.1 ความถี่ในการทบทวนแผน (Plan Review Frequency)

- เป้าหมาย: ทบทวนแผนไม่น้อยกว่า 1 ครั้งต่อปี หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ
- วิธีวัด: ตรวจสอบจำนวนครั้งที่มีการทบทวนแผนต่อปี และเปรียบเทียบกับเป้าหมายที่กำหนด

1.2 อัตราการปรับปรุงแผนตามข้อเสนอแนะ (Plan Improvement Implementation Rate)

- เป้าหมาย: นำข้อเสนอแนะจากการทบทวนมาปรับปรุงแผนไม่น้อยกว่า 90%
- วิธีวัด: เปรียบเทียบจำนวนข้อเสนอแนะที่นำไปปรับปรุงกับจำนวนข้อเสนอแนะทั้งหมด

1.3 การครอบคลุมความเสี่ยงใหม่ในการทบทวนแผน (Coverage of New Risks)

- เป้าหมาย: รวมความเสี่ยงใหม่ ๆ ที่ระบุได้จากการประเมินความเสี่ยงเข้ามาในแผน 100%
- วิธีวัด: ตรวจสอบรายการความเสี่ยงที่เพิ่มเข้ามาในแผนหลังการทบทวน

1.4 ระดับความสอดคล้องของแผนกับมาตรฐานและกฎหมาย (Compliance Alignment Rate)

- เป้าหมาย: แผนที่ทบทวนต้องสอดคล้องกับกฎหมายและมาตรฐานที่เกี่ยวข้อง 100%
- วิธีวัด: ใช้ผลการตรวจสอบความสอดคล้องกับกฎหมายและมาตรฐาน

2. ตัวชี้วัดด้านการฝึกซ้อมแผน (Plan Drill Metrics)

2.1 ความถี่ในการฝึกซ้อมแผน (Drill Frequency)

- เป้าหมาย: ดำเนินการฝึกซ้อมไม่น้อยกว่า 2 ครั้งต่อปี (อย่างน้อย 1 ครั้งแบบเต็มรูปแบบ)
- วิธีวัด: นับจำนวนครั้งของการฝึกซ้อมแผนต่อปี

	ชื่อเอกสาร แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร		
	ระดับชั้นความลับ ใช้ภายในสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น	เวอร์ชัน 1.0	หน้า 20

2.2 อัตราการเข้าร่วมฝึกซ้อมของบุคลากรที่เกี่ยวข้อง (Participant Attendance Rate)

- เป้าหมาย: บุคลากรที่เกี่ยวข้องเข้าร่วมไม่น้อยกว่า 90%
- วิธีวัด: เปรียบเทียบจำนวนผู้เข้าร่วมกับจำนวนบุคลากรทั้งหมดที่เกี่ยวข้อง

2.3 ระดับความเข้าใจของผู้เข้าร่วมหลังการฝึกซ้อม (Post-Drill Knowledge Level)

- เป้าหมาย: คะแนนการประเมินหลังฝึกซ้อมเฉลี่ยไม่น้อยกว่า 80%
- วิธีวัด: ใช้แบบทดสอบหรือประเมินผลความรู้หลังการฝึกซ้อม

2.4 การแก้ไขจุดอ่อนที่พบจากการฝึกซ้อม (Weakness Resolution Rate)

- เป้าหมาย: แก้ไขจุดอ่อนที่พบจากการฝึกซ้อม 100% ภายในระยะเวลาที่กำหนด
- วิธีวัด: ตรวจสอบจำนวนจุดอ่อนที่แก้ไขสำเร็จเทียบกับจำนวนจุดอ่อนทั้งหมด

2.5 ระยะเวลาที่ใช้ในการดำเนินการฝึกซ้อม (Drill Execution Time)

- เป้าหมาย: การฝึกซ้อมต้องดำเนินการเสร็จสิ้นภายในระยะเวลาที่กำหนด
- วิธีวัด: บันทึกเวลาที่ใช้ในการดำเนินการฝึกซ้อมและเปรียบเทียบกับเป้าหมาย

1.1.4 ข้อมูลติดต่อและการยกระดับการดำเนินการ (Contact Information and Escalation Level)

ชื่อ	ตำแหน่ง	บทบาท	ข้อมูลการติดต่อ	ระดับที่เกี่ยวข้อง (Escalation 1-3)*
นายสกุล ยุช ศรุตานนท์	ผู้อำนวยการศูนย์เทคโนโลยี สารสนเทศที่ ดิน และ ทรัพยากรดิน (กลุ่มงานบริหารระบบ เทคโนโลยีสารสนเทศและ การสื่อสาร, กลุ่มงานพัฒนาเครือข่าย และนวัตกรรม)	IR Commander, CIRT manager, CIRT member		1
ว่าที่ ร้อยตรี ไพรัช มั่นจิตต์	รองผู้อำนวยการสำนักงาน คณะกรรมการนโยบาย ที่ดินแห่งชาติ	CIO		2

	ชื่อเอกสาร แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร		
	ระดับชั้นความลับ ใช้ภายในสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น	เวอร์ชัน 1.0	หน้า 21

ชื่อ	ตำแหน่ง	บทบาท	ข้อมูลการติดต่อ	ระดับที่เกี่ยวข้อง (Escalation 1-3)*
XXXXXX XXXXXX	ผู้อำนวยการสำนักงาน ผู้อำนวยการ (กลุ่มงานอำนวยการและ ประชาสัมพันธ์)	IHT member		3
XXXXXX XXXXXX	ผู้อำนวยการกองกฎหมาย (กลุ่มงานกฎหมายและ ระเบียบ)	IHT member		3
XXXXXX XXXXXX	กลุ่มพัฒนาระบบบริหาร (การควบคุมความเสี่ยง ภายใน)	IHT member		3
XXXXXX XXXXXX	ผู้อำนวยการสำนักงาน ผู้อำนวยการ (กลุ่มงานบริหารทรัพยากร บุคคล)	IHT member		3
XXXXXX XXXXXX	ผู้อำนวยการสำนักงาน ผู้อำนวยการ (กลุ่มงานอำนวยการและ ประชาสัมพันธ์) ดูแลเรื่อง อาคารสถานที่	IHT member		3
XXXXXX XXXXXX	3 rd Party Support สำนักงานคณะกรรมการ การรักษาความมั่นคง ปลอดภัยไซเบอร์แห่งชาติ (สกมช.)	CIRT member	XXXXXXXX	3
XXXXXX XXXXXX	Vendor, Supplier	CSIRT member		1

	ชื่อเอกสาร แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร		
	ระดับชั้นความลับ ใช้ภายในสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น	เวอร์ชัน 1.0	หน้า 22

ชื่อ	ตำแหน่ง	บทบาท	ข้อมูลการติดต่อ	ระดับที่เกี่ยวข้อง (Escalation 1-3)*
	บำรุงรักษา, สำรองข้อมูล, กู้คืนระบบ			

รูปที่ 1-1: ข้อมูลติดต่อและการยกระดับการดำเนินการ

การยกระดับการดำเนินการ (Escalation Level) กำหนดลำดับที่การแจ้งเตือนควรเกิดขึ้น:

1. แจ้งก่อน (Notify First) จำเป็นทุกกรณี
2. จำเป็นสำหรับเหตุภัยคุกคามทางไซเบอร์ระดับร้ายแรงหรือวิกฤตทั้งหมด (Required on all Moderate or High-severity Incidents)
3. มีส่วนร่วมตามความจำเป็น (Involve as Needed)

1.1.5 หน้าที่และความรับผิดชอบ (Roles and Responsibilities)

1.1.5.1 ทีมจัดการเหตุภัยคุกคามทางไซเบอร์ (Cyber Security Incident Handling Team: IHT)

- ประกอบด้วยผู้เชี่ยวชาญด้านกฎหมาย ผู้จัดการความเสี่ยง และผู้จัดการแผนกอื่น ๆ ที่อาจให้คำปรึกษาหรือแจ้งในระหว่างการเผชิญเหตุ
- ให้คำแนะนำเกี่ยวกับกิจกรรมรับมือเหตุภัยคุกคามทางไซเบอร์ที่เกี่ยวข้องกับความเชี่ยวชาญ
- รักษาความเข้าใจทั่วไปเกี่ยวกับแผนและนโยบายของหน่วยงาน
- ตรวจสอบให้แน่ใจว่ากิจกรรมรับมือเหตุภัยคุกคามทางไซเบอร์เป็นไปตามข้อกำหนดทางกฎหมาย สัญญา และข้อบังคับ
- เข้าร่วมในการทดสอบแผนและขั้นตอนการรับมือเหตุภัยคุกคามทางไซเบอร์
- รับผิดชอบในการสื่อสารภายในและภายนอกที่เกี่ยวข้องกับเหตุภัยคุกคามทางไซเบอร์

1.1.5.2 ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer: CIO หรือ CTO) หรือผู้บริหารระดับสูง ที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Chief Information Security Officer : CISO)

- ขออนุมัติจากผู้บริหารระดับสูง (Executive Management) สำหรับการบริหารชุดโครงการการรับมือเหตุภัยคุกคามทางไซเบอร์ (Incident Response Program) ที่เกิดขึ้น
- ประสานงานกิจกรรมตอบสนองกับแผนกเสริมและทรัพยากรภายนอกตามความจำเป็นเพื่อลดความเสียหายต่อทรัพยากรสารสนเทศ

	ชื่อเอกสาร	แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร		
	ระดับชั้นความลับ	ใช้ภายในสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น	เวอร์ชัน 1.0	หน้า 23

- ให้ข้อมูลเป็นปัจจุบันเกี่ยวกับกิจกรรมรับมือเหตุภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับทีมจัดการเหตุภัยคุกคามทางไซเบอร์ (Incident Handling Team: IHT) และผู้มีส่วนได้ส่วนเสียอื่น ๆ ในระหว่างเหตุการณ์
- ตรวจสอบให้แน่ใจว่าข้อตกลงระดับการบริการกับผู้ให้บริการกำหนดความคาดหวังของหน่วยงานและผู้ให้บริการอย่างชัดเจนเกี่ยวกับการรับมือเหตุภัยคุกคามทางไซเบอร์
- ตรวจสอบให้แน่ใจว่านโยบายที่เกี่ยวข้องกับการรับมือเหตุภัยคุกคามทางไซเบอร์แสดงถึงเป้าหมายของหน่วยงานได้อย่างถูกต้อง
- ทบทวนแผนรับมือเหตุภัยคุกคามทางไซเบอร์ (“แผน”) เพื่อให้แน่ใจว่าเป็นไปตามวัตถุประสงค์ของนโยบายและสะท้อนเป้าหมายของหน่วยงานได้อย่างถูกต้อง ขออนุมัติแผนจาก IHT
- ทำงานร่วมกับผู้บัญชาการ IR เพื่อประเมินประสิทธิภาพของแผนและ CIRT เป็นระยะ ๆ
- ทบทวนให้แน่ใจว่าผู้จัดการ CIRT ได้รับอำนาจที่จำเป็น (Necessary Authority) ในการยึดทรัพย์สินและหยุดให้บริการอย่างรวดเร็วเพื่อควบคุมเหตุภัยคุกคามทางไซเบอร์ระดับร้ายแรงหรือระดับวิกฤต (Moderate or Critical-severity Incident) (เทียบเคียงกับ (2) ภัยคุกคามทางไซเบอร์ในระดับร้ายแรง และ (3) ภัยคุกคามทางไซเบอร์ในระดับวิกฤติ มาตรา 60 พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562)
- อนุมัติการปิดเหตุภัยคุกคามทางไซเบอร์ระดับร้ายแรงหรือระดับวิกฤต (Moderate or Critical-Severity Incident)
- ตรวจสอบให้แน่ใจว่ามีการรักษา Cyber Insurance ตามความจำเป็นและแจ้งผู้มีส่วนได้ส่วนเสียที่เหมาะสม (ดูภาคผนวก 9)
- ตรวจสอบให้แน่ใจว่าบทเรียนที่เรียนรู้ถูกนำไปใช้/ซึ่งน้ำหนักตามความเสี่ยงสำหรับเหตุภัยคุกคามทางไซเบอร์ ความรุนแรงระดับ 1 (Severity 1 Incidents)

หมายเหตุ: อ้างถึงพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มาตรา 60 การพิจารณาเพื่อใช้อำนาจในการป้องกันภัยคุกคามทางไซเบอร์ คณะกรรมการจะกำหนดลักษณะของภัยคุกคามทางไซเบอร์ โดยแบ่งออกเป็นสามระดับ

(1) ภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง หมายถึง ภัยคุกคามทางไซเบอร์ที่มีความเสี่ยงอย่างมีนัยสำคัญถึงระดับที่ทำให้ระบบคอมพิวเตอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศหรือการให้บริการของรัฐด้อยประสิทธิภาพลง

(2) ภัยคุกคามทางไซเบอร์ในระดับร้ายแรง หมายถึง ภัยคุกคามที่มีลักษณะการเพิ่มขึ้นอย่างมีนัยสำคัญของการโจมตีระบบคอมพิวเตอร์ คอมพิวเตอร์ หรือข้อมูลคอมพิวเตอร์ โดยมุ่งหมายเพื่อโจมตีโครงสร้างพื้นฐานสำคัญของประเทศและการโจมตีดังกล่าวมีผลทำให้ระบบคอมพิวเตอร์หรือโครงสร้างสำคัญทางสารสนเทศที่เกี่ยวข้องกับการให้บริการของโครงสร้างพื้นฐานสำคัญของประเทศ ความมั่นคงของรัฐ

	ชื่อเอกสาร	แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร		
	ระดับชั้นความลับ	ใช้ภายในสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น	เวอร์ชัน 1.0	หน้า 24

ความสัมพันธ์ระหว่างประเทศ การป้องกันประเทศ เศรษฐกิจ การสาธารณสุข ความปลอดภัยสาธารณะ หรือความสงบเรียบร้อยของประชาชนเสียหาย จนไม่สามารถทำงานหรือให้บริการได้

(3) ภัยคุกคามทางไซเบอร์ในระดับวิกฤติ หมายถึง ภัยคุกคามทางไซเบอร์ในระดับวิกฤติที่มีลักษณะ ดังต่อไปนี้

(ก) เป็นภัยคุกคามทางไซเบอร์ที่เกิดจากการโจมตีระบบคอมพิวเตอร์ คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ในระดับที่สูงขึ้นกว่าภัยคุกคามทางไซเบอร์ในระดับร้ายแรง โดยส่งผลกระทบต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศในลักษณะที่เป็นวงกว้าง จนทำให้การทำงานของหน่วยงานรัฐหรือการให้บริการของโครงสร้างพื้นฐานสำคัญของประเทศที่ให้กับประชาชนล้มเหลวทั้งระบบ จนรัฐไม่สามารถควบคุมการทำงานส่วนกลางของระบบคอมพิวเตอร์ของรัฐได้ หรือการเข้ามาตรการเยียวยาตามปกติในการแก้ไขปัญหาภัยคุกคามไม่สามารถแก้ไขปัญหาได้และมีความเสี่ยงที่จะลุกลามไปยังโครงสร้างพื้นฐานสำคัญอื่น ๆ ของประเทศ ซึ่งอาจมีผลทำให้บุคคลจำนวนมากเสียชีวิตหรือระบบคอมพิวเตอร์ คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์จำนวนมากถูกทำลายเป็นวงกว้างในระดับประเทศ

(ข) เป็นภัยคุกคามทางไซเบอร์อันกระทบหรืออาจกระทบต่อความสงบเรียบร้อยของประชาชนหรือเป็นภัยต่อความมั่นคงของรัฐหรืออาจทำให้ประเทศหรือส่วนใดส่วนหนึ่งของประเทศตกอยู่ในภาวะคับขันหรือมีการกระทำความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา การรบหรือการสงคราม ซึ่งจำเป็นต้องมีมาตรการเร่งด่วนเพื่อรักษาไว้ซึ่งการปกครองระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุขตามรัฐธรรมนูญแห่งราชอาณาจักรไทย เอกراهและบูรณภาพแห่งอาณาเขตผลประโยชน์ของชาติ การปฏิบัติตามกฎหมาย ความปลอดภัยของประชาชน การดำรงชีวิตโดยปกติสุขของประชาชน การคุ้มครองสิทธิเสรีภาพ ความสงบเรียบร้อยหรือประโยชน์ส่วนรวม หรือการป้องกันหรือแก้ไขเยียวยาความเสียหายจากภัยพิบัติสาธารณะอันมีมาอย่างฉุกเฉินและร้ายแรง

นอกจากนี้ หน่วยงานควรศึกษาดูรายละเอียดเพิ่มเติมเกี่ยวกับลักษณะภัยคุกคามทางไซเบอร์ได้ที่ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปรามปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. 2564

1.1.5.3 ทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT)

CIRT ประกอบด้วยการจัดการด้านเทคโนโลยีสารสนเทศและบุคลากรที่มีประสบการณ์ บทบาทของ CIRT คือการจัดการกับเหตุการณ์ในทันที เพื่อให้สามารถกักกัน สืบสวนสอบสวน และกู้คืนได้อย่างรวดเร็ว ในกรณีที่มีการยกระดับบริการของบุคคลที่สาม ตรวจสอบให้แน่ใจว่าพวกเขามีส่วนร่วมตามความจำเป็น บทบาทภายใน CIRT รวมถึง:

1.1.5.3.1 ผู้บัญชาการ IR (IR Commander)

ผู้บัญชาการการรับมือเหตุภัยคุกคามทางไซเบอร์จะดูแลและจัดลำดับความสำคัญของการดำเนินการระหว่างการตรวจจับ การวิเคราะห์ และการจำกัดขอบเขตเหตุการณ์ และยังมีหน้าที่รับผิดชอบในการถ่ายทอดความต้องการพิเศษของเหตุการณ์ที่มีความรุนแรงสูงไปยังส่วนอื่น ๆ ของหน่วยงานตลอดจนการสื่อสาร

	ชื่อเอกสาร แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร		
	ระดับชั้นความลับ ใช้ภายในสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น	เวอร์ชัน 1.0	หน้า 25

ผลกระทบที่อาจเกิดขึ้นกับ CIO นอกจากนี้ ยังมีหน้าที่รับผิดชอบในการทำความเข้าใจข้อตกลงระดับการบริการ (Service Level Agreement: SLA) กับบุคคลที่สาม และบทบาทของบุคคลที่สามอาจมีบทบาทในสถานการณ์การรับมือที่เฉพาะเจาะจง

ความรับผิดชอบเพิ่มเติม:

- ทำหน้าที่เป็นผู้ประสานงานสำหรับการสื่อสารทั้งหมดไปยังและจาก CIO
- รวบรวมทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Incident Response Team: CIRT)
- ตรวจสอบให้แน่ใจว่าบุคลากรที่ได้รับมอบหมายให้รับผิดชอบในการรับมือเหตุภัยคุกคามทางไซเบอร์ได้รับการฝึกอบรมและมีความรู้เกี่ยวกับวิธีการรับมือเหตุภัยคุกคามทางไซเบอร์
- ปรับปรุงข้อมูลที่เป็นปัจจุบันของแผนและขั้นตอนตามความจำเป็นตามผลการทดสอบ บทเรียนการรับมือเหตุภัยคุกคามทางไซเบอร์ที่ได้เรียนรู้ การพัฒนาอุตสาหกรรม และแนวปฏิบัติที่ดีที่สุด
- ทบทวนแผนและขั้นตอนปฏิบัติอย่างน้อยปีละครั้ง
- เริ่มการทดสอบแผนและขั้นตอนอย่างน้อยปีละครั้ง
- ตรวจสอบให้แน่ใจว่ากิจกรรมของทีมเป็นไปตามข้อกำหนดทางกฎหมายและของอุตสาหกรรมสำหรับขั้นตอนการรับมือเหตุภัยคุกคามทางไซเบอร์
- ทำหน้าที่เป็นผู้บัญชาการการรับมือเหตุภัยคุกคามทางไซเบอร์หลัก รับผิดชอบในการประกาศภัยคุกคามทางไซเบอร์ จัดการกิจกรรมการรับมือของทีม และอนุมัติการปิดภัยคุกคามทางไซเบอร์ระดับความรุนแรง 2 และ 3 (Severity 2 and Severity 3 Incidents)
- ตระหนักถึงนโยบายการประกันภัยทางไซเบอร์ (Cyber Insurance Policies) กลไกการติดต่อและเมื่อใดที่จะรวมผู้ให้บริการ (ดูภาคผนวก 9)

1.1.5.3.2 สมาชิกทีมจัดการเหตุภัยคุกคามทางไซเบอร์ (Incident Response Team Members)

Incident Response Manager ได้รับการสนับสนุนโดยทีมเจ้าหน้าที่ด้านเทคนิคที่ทำงานโดยตรงกับระบบข้อมูลที่ได้รับผลกระทบ เพื่อค้นหาเวลา สถานที่ และรายละเอียดของเหตุการณ์ สมาชิกในทีมมักประกอบด้วยผู้เชี่ยวชาญเฉพาะด้าน (Subject Matter Experts: SMEs) เจ้าหน้าที่เทคโนโลยีสารสนเทศระดับอาวุโส บุคคลภายนอก การรักษาความมั่นคงปลอดภัยจากภายนอก หรือพันธมิตรทางนิติวิทยาศาสตร์

ความรับผิดชอบเพิ่มเติม:

- ช่วยเหลือในการรับมือเหตุภัยคุกคามทางไซเบอร์ตามที่ร้องขอ ความรับผิดชอบของ CIRT ควรมีความสำคัญมากกว่าหน้าที่ปกติ
- ทำความเข้าใจของหน่วยงาน แผนรับมือเหตุภัยคุกคามทางไซเบอร์และขั้นตอนในการรับมือเหตุภัยคุกคามทางไซเบอร์อย่างเหมาะสม
- พัฒนาทักษะต่อไปสำหรับการจัดการการรับมือเหตุภัยคุกคามทางไซเบอร์
- ตรวจสอบให้แน่ใจว่าเครื่องมือได้รับการกำหนดค่าและจัดการอย่างเหมาะสมเพื่อแจ้งเตือนเหตุการณ์/ภัยคุกคามทางไซเบอร์ (Incidents/events)

	ชื่อเอกสาร แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร		
	ระดับชั้นความลับ ใช้ภายในสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น	เวอร์ชัน 1.0	หน้า 26

- วิเคราะห์การรับส่งข้อมูลเครือข่ายเพื่อหาสัญญาณของการปฏิเสธบริการ (Denial of Service) การปฏิเสธบริการแบบกระจาย (Distributed Denial of Service) หรือการโจมตีภายนอกอื่น ๆ
- ตรวจสอบล็อกไฟล์ของระบบที่สำคัญสำหรับกิจกรรมที่ผิดปกติ
- สังเกตการณ์แอปพลิเคชันและบริการทางธุรกิจสำหรับการหาสัญญาณการโจมตี (Signs of Attack)
- รวบรวมข้อมูลที่เกี่ยวข้องเกี่ยวกับภัยคุกคามทางไซเบอร์ตามคำร้องขอของผู้บัญชาการ IR
- ปรึกษากับเจ้าหน้าที่รักษาความมั่นคงปลอดภัยสารสนเทศที่มีคุณสมบัติเหมาะสมเพื่อขอคำแนะนำเมื่อจำเป็น
- ตรวจสอบให้แน่ใจว่าการรวบรวมหลักฐานห่วงโซ่การอารักขา (Chain of Custody) และการเก็บรักษามีความเหมาะสม
- เข้าร่วมในการทดสอบแผนและขั้นตอนการรับมือเหตุการณ์คุกคามทางไซเบอร์
- มีความรู้เกี่ยวกับข้อตกลงระดับการให้บริการกับผู้ให้บริการเกี่ยวกับการรับมือเหตุการณ์คุกคามทางไซเบอร์

1.1.5.3.3 ผู้บันทึก (Recorder)

ผู้บัญชาการการรับมือเหตุการณ์คุกคามทางไซเบอร์อาจมอบหมายให้สมาชิกในทีมเริ่มกระบวนการทางเอกสารอย่างเป็นทางการของภัยคุกคามทางไซเบอร์

ลำดับที่	สมาชิก CIRT	บทบาท
1	XXXXXX XXXXXX	ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศที่ดินและทรัพยากรดิน (Information Security Manager)
2	XXXXXX XXXXXX	บริษัท ไอเน็กซ์ บรอดแบนด์ จำกัด (iNEXT Broadband Co., Ltd.) บำรุงรักษา, สำรองข้อมูล, กู้คืนระบบ
3	หัวหน้ากลุ่มงานบริหารระบบเทคโนโลยีสารสนเทศและการสื่อสาร	ดูแลระบบเทคโนโลยีสารสนเทศและการสื่อสาร
4	หัวหน้ากลุ่มงานพัฒนาเครือข่ายและนวัตกรรม	ดูแลงานพัฒนาเครือข่ายและนวัตกรรม
7	XXXXXX XXXXXX	Vendor, Supplier บำรุงรักษา, สำรองข้อมูล, กู้คืนระบบ
8	XXXXXX XXXXXX	บริษัท ไอเน็กซ์ บรอดแบนด์ จำกัด (iNEXT Broadband Co., Ltd.) ใช้บริการที่อาคารไทยซัมมิท ทาวเวอร์

	ชื่อเอกสาร แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร		
	ระดับชั้นความลับ ใช้ภายในสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น	เวอร์ชัน 1.0	หน้า 27

ลำดับที่	สมาชิก CIRT	บทบาท
		ที่วาง Server สำรองข้อมูลใส่ Hard Disk และเก็บรักษาไว้สำหรับการกู้คืน (ระบบ DR Site)

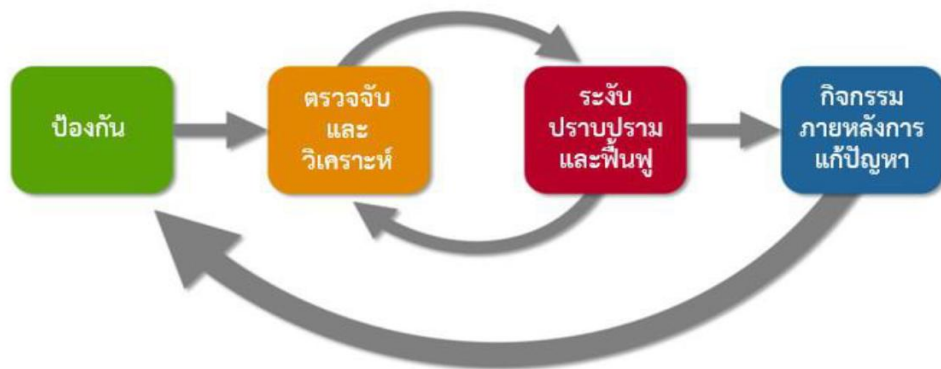
รูปที่ 1-2: ข้อมูลสมาชิกทีม CIRT (CIRT Team Members)

2 กรอบการรับมือเหตุภัยคุกคามทางไซเบอร์ (Incident Response Framework)

หน่วยงานตระหนักดีว่าถึงแม้จะมีความพยายามอย่างสมเหตุสมผลและมีความสามารถในการปกป้องทรัพยากรสารสนเทศ แต่อาจมีการละเมิดหรือการสูญเสียข้อมูลอื่น ๆ หน่วยงานต้องใช้ความพยายามอย่างสมเหตุสมผลและดำเนินการอย่างเหมาะสมเพื่อรับมือเหตุภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นในลักษณะที่ลดการสูญหายของข้อมูลและความเสียหายที่อาจเกิดขึ้นกับลูกค้า คู่ค้า และหน่วยงานเอง

การพัฒนากรอบการรับมือเหตุภัยคุกคามทางไซเบอร์ที่กำหนดไว้อย่างชัดเจนมีความสำคัญต่อแผนการรับมือเหตุภัยคุกคามทางไซเบอร์ที่มีประสิทธิภาพ กรอบงานการรับมือเหตุภัยคุกคามทางไซเบอร์ของหน่วยงาน ประกอบด้วย 4 ขั้นตอนเพื่อให้แน่ใจว่ามีแนวทางที่สอดคล้องกันและเป็นระบบ (Consistent and Systematic Approach)

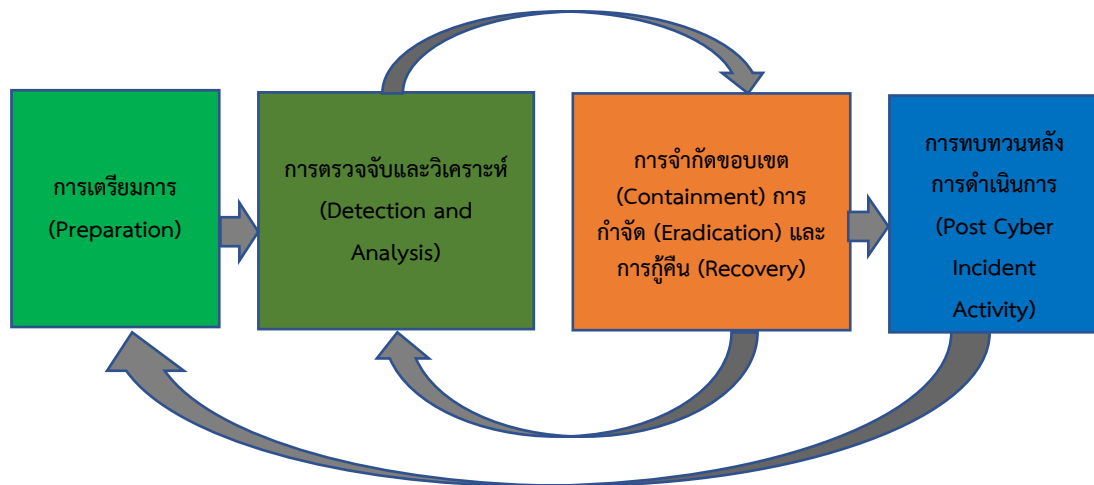
โดยเทียบเคียงกับประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปรามปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. 2564 ได้ดังนี้



รูปที่ 2-1: ขั้นตอนการดำเนินการที่เกี่ยวข้องเพื่อจัดการภัยคุกคามทางไซเบอร์ (Incident Handling Cycle)

ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปรามปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. 2564

	ชื่อเอกสาร แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร		
	ระดับชั้นความลับ ใช้ภายในสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น	เวอร์ชัน 1.0	หน้า 28



รูปที่ 2-2: วงจรชีวิตของการตอบสนองเหตุภัยคุกคามทางไซเบอร์ (Incident Response Life Cycle)

ดังนั้น จึงเปรียบเทียบคำศัพท์ที่มีการใช้งานระหว่างเอกสารทั้งสองฉบับ เพื่อให้ผู้อ่านนำไปใช้งานสามารถเข้าใจได้ง่ายขึ้นดังนี้

แนวทางปฏิบัติในเอกสารนี้	ขั้นตอนการดำเนินการมาตรการที่เกี่ยวข้องเพื่อจัดการภัยคุกคามทางไซเบอร์
ขั้นตอนที่ 1 การเตรียมการ (Preparation)	ขั้นตอนที่ 1: การเตรียมการและป้องกันการเกิดภัยคุกคามทางไซเบอร์
ขั้นตอนที่ 2 การตรวจจับและวิเคราะห์ (Detection and Analysis)	ขั้นตอนที่ 2: การตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์
ขั้นตอนที่ 3 การจำกัดขอบเขต (Containment) การกำจัด (Eradication) และการกู้คืน (Recovery)	ขั้นตอนที่ 3: การระงับภัยคุกคามทางไซเบอร์ ปรามปรามภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ
ขั้นตอนที่ 4 การทบทวนหลังการดำเนินการ (Post Cyber Incident Activity)	ขั้นตอนที่ 4: การดำเนินการภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์

รูปที่ 2-3: เปรียบเทียบแนวทางปฏิบัติและประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปรามปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. 2564

จากตารางข้างต้นสามารถอธิบายรายละเอียดของขั้นตอนต่าง ๆ ตั้งแต่การเตรียมการ (Preparation) จนถึงการทบทวนหลังการดำเนินการ (Post Cyber Incident Activity) พอสังเขปได้ดังนี้

	ชื่อเอกสาร แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร		
	ระดับชั้นความลับ ใช้ภายในสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น	เวอร์ชัน 1.0	หน้า 29

ขั้นตอนที่ 1 การเตรียมการ (Preparation)

จำเป็นอย่างยิ่งที่จะต้องจัดตั้งทีมจัดการเหตุภัยคุกคามทางไซเบอร์ (Cyber Incident Response Team (CIRT)) กำหนดแนวทางการสื่อสารที่เหมาะสม สื่อสารการบริการที่จำเป็นเพื่อสนับสนุนกิจกรรมการรับมือและจัดหาเครื่องมือที่จำเป็น (ดูหัวข้อ 4 ขั้นตอนที่ 1 รายละเอียดการเตรียมการ (Preparation))

ขั้นตอนที่ 2 การตรวจจับและวิเคราะห์ (Detection and Analysis)

การตรวจจับและระบุเหตุการณ์และการดำเนินการประเมินควรดำเนินการเพื่อยืนยันการมีอยู่ของภัยคุกคามทางไซเบอร์ การประเมินควรรวมถึงการกำหนดขอบเขต ผลกระทบ และขอบเขตของความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ ในกรณีที่อาจมีการดำเนินการทางกฎหมาย หลักฐานดิจิทัลจะได้รับการเก็บรักษาไว้ และการวิเคราะห์ทางนิติวิทยาศาสตร์อาจดำเนินการตามข้อกำหนดทางกฎหมายและกฎระเบียบที่เกี่ยวข้อง (ดูหัวข้อ 5 ขั้นตอนที่ 2 การตรวจจับและวิเคราะห์ (Detection and Analysis))

ขั้นตอนที่ 3 การจำกัดขอบเขต (Containment) การกำจัด (Eradication) และการกู้คืน (Recovery)

ประกอบไปด้วย 3 ขั้นตอนย่อย (ดูหัวข้อ 6 ขั้นตอนที่ 3 การจำกัดขอบเขต (Containment) การกำจัด (Eradication) และการกู้คืน (Recovery)) ดังนี้

ขั้นตอนที่ 3.1 การจำกัดขอบเขต (Containment)

การจำกัดขอบเขตเหตุการณ์เป็นสิ่งจำเป็นเพื่อลดและแยกความเสียหายที่เกิดขึ้น ต้องดำเนินการตามขั้นตอนเพื่อให้แน่ใจว่าขอบเขตของเหตุการณ์ไม่กระจายไปถึงระบบอื่น ๆ และทรัพยากรสารสนเทศจำเป็นต้องมีการวิเคราะห์สาเหตุที่แท้จริง (Root Cause Analysis) ก่อนที่จะก้าวข้ามขั้นตอนการจำกัดขอบเขต และอาจต้องใช้ผู้เชี่ยวชาญจากบุคคลภายนอก

ขั้นตอนที่ 3.2 การกำจัด (Eradication)

การกำจัดต้องมีการลบ (Removal) หรือจัดการ (Addressing) ส่วนประกอบและอาการของภัยคุกคามทางไซเบอร์ทั้งหมด นอกจากนี้ ต้องดำเนินการตรวจสอบความถูกต้อง (Validation) เพื่อให้แน่ใจว่าภัยคุกคามทางไซเบอร์จะไม่เกิดขึ้นอีก

ขั้นตอนที่ 3.3 การกู้คืน (Recovery)

การกู้คืนเกี่ยวข้องกับขั้นตอนที่จำเป็นในการกู้คืนข้อมูลและระบบให้อยู่ในสถานะการทำงานที่ดี ซึ่งช่วยให้การดำเนินธุรกิจสามารถกลับมาดำเนินการได้

ขั้นตอนที่ 4 การทบทวนหลังการดำเนินการ (Post Cyber Incident Activity)

การทบทวนหลังการดำเนินการเกี่ยวข้องกับการทบทวนบทเรียนที่เรียนรู้รวมถึงการวิเคราะห์หลังเหตุการณ์เกี่ยวกับระบบที่ได้รับผลกระทบจากภัยคุกคามทางไซเบอร์และระบบอื่น ๆ ที่อาจมีความเสี่ยง บทเรียนที่เรียนรู้จากภัยคุกคามทางไซเบอร์นั้นจะถูกสื่อสารไปยังผู้บริหารระดับสูง และแผนปฏิบัติการที่พัฒนาขึ้นเพื่อปรับปรุงแนวทางปฏิบัติในการรับมือเหตุภัยคุกคามทางไซเบอร์ในอนาคตและลดความเสี่ยง (ดูขั้นตอนที่ 4 –การทบทวนหลังการดำเนินการ (After-Action Review Process))

	ชื่อเอกสาร แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร		
	ระดับชั้นความลับ ใช้ภายในสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น	เวอร์ชัน 1.0	หน้า 30

ในการดำเนินการตามขั้นตอนต่าง ๆ ในมีการระบุรายละเอียดตามข้อมูลด้านล่าง เพื่อเป็นแนวทางการปฏิบัติจริงสำหรับ สคทช. ดังนี้

2.1 ขั้นตอนที่ 1 รายละเอียดการเตรียมการ (Preparation)

ขั้นตอนการเตรียมการเป็นขั้นตอนที่สำคัญที่สุดและมักถูกมองข้ามอย่างง่ายดาย หากไม่มีการเตรียมการที่เหมาะสม กิจกรรมการรับมือเหตุภัยคุกคามทางไซเบอร์อาจไม่เป็นระเบียบ มีราคาสูง และอาจก่อให้เกิดอันตรายต่อหน่วยงานที่ไม่สามารถแก้ไขได้ ลักษณะงานที่รวมอยู่ในขั้นตอนการเตรียมการมีต่อไปนี้

- จัดตั้งทีมจัดการเหตุภัยคุกคามทางไซเบอร์ (Cyber Security Incident Handling Team: IHT) และทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT)
- ตรวจสอบให้แน่ใจว่าฝ่ายที่เกี่ยวข้องตระหนักถึงกระบวนการรายงานเหตุภัยคุกคามทางไซเบอร์ (ดูการรายงานเหตุภัยคุกคามทางไซเบอร์ (Reporting Incidents))
- จัดทำเอกสารและแบ่งปันรายละเอียดการประกันภัยทางไซเบอร์กับฝ่ายที่เกี่ยวข้อง (ดูภาคผนวก 9)
- ตรวจสอบการปฏิบัติตามนโยบายการบันทึก การแจ้งเตือน และการเฝ้าระวัง (Monitoring)
- ตรวจสอบให้แน่ใจว่า CIRT ได้รับการฝึกอบรมที่เหมาะสมตามการวิเคราะห์ช่องว่างทักษะ ความพยายามในการพัฒนาอาชีพ (Career Development Efforts) และความต้องการในการรักษาทักษะ (Skill Retention Needs)
- ตรวจสอบให้แน่ใจว่า CIRT สามารถเข้าถึงเครื่องมือและอุปกรณ์ที่จำเป็นตาม ROI โดยประมาณความเสี่ยงของหน่วยงาน
- กำหนดและจัดทำเอกสารขั้นตอนการปฏิบัติงานมาตรฐานและลำดับการดำเนินการสำหรับทั้ง IHT และ CIRT
- ปรับปรุงเอกสาร รายการตรวจสอบ ข้อมูลอ้างอิง ฯลฯ
- รักษาและตรวจสอบความถูกต้องของโคดแแกรมเครือข่ายและทะเบียนทรัพย์สิน
- ตรวจสอบรายงานการทดสอบการเจาะระบบ (Penetration Test) และตรวจสอบความถูกต้องของการแก้ไขสิ่งที่ค้นพบ
- ตรวจสอบรายงานการจัดการช่องโหว่และตรวจสอบความพยายามในการแก้ไข
- สร้างข้อมูลประจำตัวของผู้ดูแลระบบที่ใช้เฉพาะกิจและปิดใช้งาน (Disposable and Disabled Administrative Credentials) เพื่อใช้สำหรับการสืบสวนสอบสวน
- สุดท้าย ควรสังเกตว่าขั้นตอนที่ 1 เป็นไปอย่างต่อเนื่องหรืออย่างน้อยเป็นวัฏจักรเมื่อภัยคุกคามทางไซเบอร์ต่าง ๆ ได้รับการสรุปผล

หมายเหตุ: หน่วยงานต้องพิจารณาดำเนินมาตรการตามรายละเอียดที่ระบุใน ประกาศ คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทาง

	ชื่อเอกสาร แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร		
	ระดับชั้นความลับ ใช้ภายในสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น	เวอร์ชัน 1.0	หน้า 31

ไซเบอร์ มาตราการป้องกัน รับมือ ประเมิน ปรามปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. 2564

2.1.1 การรายงานเหตุภัยคุกคามทางไซเบอร์ (Reporting Incidents)

วิธีที่มีประสิทธิภาพสำหรับทั้งฝ่ายภายในและภายนอกในการรายงานเหตุภัยคุกคามทางไซเบอร์มีความสำคัญเท่าเทียมกัน เนื่องจากบางครั้งผู้ใช้ระบบของหน่วยงาน และข้อมูลอาจเป็นคนแรกที่สังเกตเห็นปัญหา ทบทวนประเภทของเหตุการณ์ที่เกิดขึ้นในขั้นตอนที่ 2 ภายใต้การจำแนกหมวดหมู่เหตุภัยคุกคามทางไซเบอร์ (Incident Categorization) และแสดงรายการหรือกำหนดวิธีการรายงานสำหรับภัยคุกคามทางไซเบอร์ประเภทต่าง ๆ ดังตารางด้านล่าง

ประเภทเหตุภัยคุกคามทางไซเบอร์ (Incident Type)	วิธีการรายงาน (Reporting Method)	พร้อมสำหรับ (Available To)	ทำให้นิรนาม (Anonymous)
การเปลี่ยนแปลงเว็บไซต์ให้เสียหาย การแก้ไขข้อมูล หรือการนำข้อมูลมาเปิดเผยโดยไม่ได้รับอนุญาต (Website Defacement, Data Modification or Exposure)	ติดต่อฝ่ายสนับสนุนเว็บไซต์	ลูกค้า/ผู้รับบริการ	ใช่
การบุกรุกโดยการใช้มัลแวร์ (Malicious Logic)	ติดต่อศูนย์ปฏิบัติการฯ SOC ผ่านระบบ Email และโทรศัพท์	ลูกค้า/ผู้รับบริการ และพนักงาน	ไม่
การพยายามเข้าถึงระบบที่ไม่สำเร็จ (	ติดต่อศูนย์ปฏิบัติการฯ SOC ผ่านระบบ Email และโทรศัพท์	ลูกค้า/ผู้รับบริการ และพนักงาน	ไม่

รูปที่ 2-4: แนวทางการรายงานเหตุภัยคุกคามทางไซเบอร์ (Incident Reporting Guide)

หมายเหตุ : อ้างอิงจากรายงานเหตุภัยคุกคามทางไซเบอร์จากโครงการจ้างบริการเฝ้าระวังภัยคุกคามทางไซเบอร์ (Security Operations Center)

	ชื่อเอกสาร แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร		
	ระดับชั้นความลับ ใช้ภายในสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น	เวอร์ชัน 1.0	หน้า 32

2.2 ขั้นตอนที่ 2 การตรวจจับและวิเคราะห์ (Detection and Analysis)

2.2.1 การตรวจจับ (Detection)

เมื่อพนักงานของหน่วยงาน หรือบุคคลภายนอกสังเกตเห็นความผิดปกติที่น่าสงสัยในข้อมูลระบบ หรือเครือข่าย หรือการแจ้งเตือนของระบบที่สร้างเหตุการณ์ (Event) ขึ้นมา ฝ่ายปฏิบัติการด้านความมั่นคงปลอดภัย แผนกช่วยเหลือ หรือ CIRT จะต้องดำเนินการตรวจสอบเบื้องต้นและยืนยันเหตุการณ์

2.2.2 เหตุการณ์กับภัยคุกคามทางไซเบอร์ (Events Versus Incidents)

ตามที่กำหนดไว้ข้างต้น เหตุการณ์คือการสังเกตเห็นการเปลี่ยนแปลงในลักษณะการทำงานปกติของระบบ สภาพแวดล้อม กระบวนการ ลำดับการดำเนินการ หรือบุคลากร

ภัยคุกคามทางไซเบอร์ คือ เหตุการณ์ที่บ่งชี้ถึงการถูกโจมตีด้านความมั่นคงปลอดภัยหรือการไม่ปฏิบัติตามนโยบายของหน่วยงาน ที่ส่งผลกระทบในทางลบ (หรืออาจส่งผลกระทบในทางลบ) ต่อหน่วยงาน

เพื่ออำนวยความสะดวกในการระบุภัยคุกคามทางไซเบอร์ (Incident) ต่อไปนี้คือรายการอาการทั่วไปของภัยคุกคามทางไซเบอร์ ซึ่งอาจรวมถึงสิ่งต่อไปนี้บางส่วนหรือทั้งหมด:

- 1) อีเมลหรือการแจ้งเตือนทางโทรศัพท์จากเครื่องมือตรวจจับการบุกรุก
- 2) รายการที่น่าสงสัยในระบบหรือบัญชีเครือข่ายหรือล็อก
- 3) ความคลาดเคลื่อนระหว่างล็อก
- 4) การพยายามเข้าสู่ระบบที่ไม่สำเร็จซ้ำ ๆ ภายในช่วงเวลาสั้น ๆ
- 5) บัญชีผู้ใช้ใหม่ที่เกิดขึ้นโดยไม่ทราบที่มา
- 6) ไฟล์ใหม่ที่ไม่สามารถอธิบายได้หรือชื่อไฟล์ที่ไม่คุ้นเคย
- 7) การแก้ไขที่เกิดขึ้นโดยไม่ทราบที่มา ที่เกิดขึ้นต่อความยาวและ/หรือวันที่ของไฟล์ โดยเฉพาะในไฟล์ระบบ
- 8) ความพยายามที่ไม่สามารถอธิบายได้ในการเขียนไปยังไฟล์ระบบหรือการเปลี่ยนแปลงในไฟล์ระบบ
- 9) การแก้ไขหรือการลบข้อมูลโดยไม่สามารถอธิบายได้
- 10) การปฏิเสธ/การหยุดชะงักของบริการหรือการไม่สามารถเข้าสู่ระบบบัญชีของผู้ใช้ตั้งแต่หนึ่งรายขึ้นไป
- 11) ระบบล่ม
- 12) ประสิทธิภาพของระบบที่ต่ำกว่าปกติของเซิร์ฟเวอร์

	ชื่อเอกสาร	แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร		
	ระดับชั้นความลับ	ใช้ภายในสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น	เวอร์ชัน 1.0	หน้า 33

- 13) การทำงานของโปรแกรมหรืออุปกรณ์ดักจับ (Sniffer Device) ที่ใช้ในการจับการรับส่งข้อมูลเครือข่าย
- 14) เวลาใช้งานที่ผิดปกติ (เช่น ผู้ใช้เข้าสู่ระบบในช่วงเวลาที่ไม่ปกติ)
- 15) การใช้ทรัพยากรระบบที่ผิดปกติ (การใช้งาน CPU สูง)
- 16) การเข้าสู่ระบบครั้งล่าสุด (หรือการใช้งาน) สำหรับบัญชีผู้ใช้ไม่ตรงกับครั้งสุดท้ายจริงที่ผู้ใช้เข้าใช้บัญชี
- 17) รูปแบบการใช้งานที่ผิดปกติ (เช่น บัญชีผู้ใช้ที่เชื่อมโยงกับผู้ใช้ใน Finance กำลังถูกใช้เพื่อเข้าสู่ระบบฐานข้อมูล HR)
- 18) การเปลี่ยนแปลงการอนุญาตหรือการเข้าถึงของผู้ใช้โดยไม่ได้รับอนุญาต

แม้ว่าจะไม่มีอาการใดที่จะพิสูจน์ได้อย่างชัดเจนว่าเกิดภัยคุกคามทางไซเบอร์ขึ้น การสังเกตอาการเหล่านี้อย่างน้อยหนึ่งอย่างควรกระตุ้นให้ผู้สังเกตการณ์ตรวจสอบอย่างใกล้ชิดยิ่งขึ้น อย่าใช้เวลามากเกินไปกับการระบุเหตุการณ์เบื้องต้น เนื่องจากสิ่งนี้จะผ่านการพิจารณาอีกครั้งในขั้นตอนการจำกัดขอบเขต (Containment Phase)

หมายเหตุ: ควรยกเลิกการเชื่อมต่อระบบ (Disconnected) ที่ถูกบุกรุกจากเครือข่ายแทนที่จะปิดสวิตช์ (Powered Off) การปิดระบบที่ถูกบุกรุกอาจนำไปสู่การสูญเสียข้อมูล ข้อมูล หรือหลักฐานที่จำเป็นสำหรับการสืบสวนสอบสวนทางนิติวิทยาศาสตร์ในภายหลัง

2.2.3 การวิเคราะห์ (Analysis)

เมื่อมีเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ และถูกวิเคราะห์ (อ้างอิงกระบวนการคัดแยกระหว่างเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์และเหตุภัยคุกคามทางไซเบอร์ (Security Event and an Incident) ในแนวทางการจัดทำกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เรื่องมาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)) และระบุว่าเป็นเหตุภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้น CIRT บางส่วนหรือทั้งหมดจะถูกเปิดใช้งาน (Activate) โดยผู้บัญชาการ IR (IR Commander) เพื่อสืบสวนสอบสวน (Investigate) สถานการณ์ การวิเคราะห์จะกำหนดประเภท (Category) ขอบเขต (Scope) และผลกระทบ (Impact) ที่อาจเกิดขึ้นจากเหตุภัยคุกคามทางไซเบอร์ CIRT ควรทำงานอย่างรวดเร็วเพื่อวิเคราะห์และตรวจสอบแต่ละเหตุภัยคุกคามทางไซเบอร์ ตามกระบวนการที่ระบุไว้ด้านล่าง และจัดทำเอกสารแต่ละขั้นตอนที่ดำเนินการ

ควรใช้การประเมินเหตุภัยคุกคามทางไซเบอร์ 2 นาที (2 Minute Incident Assessment) ที่พบในภาคผนวก 2 เพื่อพิจารณาอย่างรวดเร็วว่าจำเป็นต้องมีการสืบสวนสอบสวนเพิ่มเติมหรือไม่ นอกจากนี้ยังสามารถแก้ไขและใช้เพื่อรายงานภัยคุกคามทางไซเบอร์ต่อผู้บริหารที่เหมาะสมตามความจำเป็น

ผู้บัญชาการการรับมือเหตุภัยคุกคามทางไซเบอร์จะมอบหมายให้สมาชิกในทีมเป็น “ผู้บันทึก” เพื่อเริ่มเอกสารอย่างเป็นทางการของภัยคุกคามทางไซเบอร์ การจำแนกหมวดหมู่ ขอบเขต และผลกระทบที่กำหนดไว้ด้านล่างจะต้องรวมอยู่ในเอกสารของภัยคุกคามทางไซเบอร์

	ชื่อเอกสาร แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร		
	ระดับชั้นความลับ ใช้ภายในสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น	เวอร์ชัน 1.0	หน้า 34

การจำแนกหมวดหมู่เหตุภัยคุกคามทางไซเบอร์ (Incident Categorization)

หมวดหมู่	คำอธิบาย
0	เหตุการณ์จำลอง และ การฝึกซ้อม ของหน่วยงานเอง (Training and Exercises)
1	การพยายามเข้าถึงระบบที่ไม่สำเร็จ (Unsuccessful Activity Attempt)
2	การพยายามบุกรุกเพื่อสำรวจข้อมูลหน่วยงานเพื่อโจมตี (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	เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สืบสวนสอบสวน (Investigating)
9	เหตุการณ์ผิดปกติที่ได้รับการวิเคราะห์แล้วว่าไม่ใช่เหตุการณ์ที่เป็นภัยคุกคาม (Explained Anomaly)

รูปที่ 2-5: การจำแนกหมวดหมู่เหตุภัยคุกคามทางไซเบอร์ (Incident Categorization)

หมายเหตุ: อ้างอิงตามภาคผนวก ท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปรามปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. 2564

ตัวอย่างลักษณะภัยคุกคามทางไซเบอร์แยกตามระดับต่าง ๆ ท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปรามปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. 2564

	ชื่อเอกสาร แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร		
	ระดับชั้นความลับ ใช้ภายในสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น	เวอร์ชัน 1.0	หน้า 35

ประเภทอุปกรณ์เครือข่าย	หมวดหมู่ภัยคุกคาม						
	1	2	3	4	5	6	7
Backbone	ไม่ร้ายแรง	ไม่ร้ายแรง	ไม่ร้ายแรง	ไม่ร้ายแรง	วิกฤต	วิกฤต	วิกฤต
เราเตอร์	ไม่ร้ายแรง	ไม่ร้ายแรง	ร้ายแรง	ไม่ร้ายแรง	วิกฤต	วิกฤต	วิกฤต
เครื่องแม่ข่ายสำหรับการจัดการเครือข่าย หรือ ดูแลความปลอดภัย	ไม่ร้ายแรง	ไม่ร้ายแรง	ร้ายแรง	ร้ายแรง	วิกฤต	วิกฤต	วิกฤต
เครื่องแม่ข่ายที่ไม่ได้ให้บริการกับสาธารณะ	ไม่ร้ายแรง	ไม่ร้ายแรง	ร้ายแรง	ร้ายแรง	ร้ายแรง	ร้ายแรง	ร้ายแรง
เครื่องแม่ข่ายที่เปิดให้บริการกับสาธารณะ	ไม่ร้ายแรง	ไม่ร้ายแรง	ไม่ร้ายแรง	ร้ายแรง	ไม่ร้ายแรง	ไม่ร้ายแรง	ร้ายแรง
เครื่องเวิร์กสเตชัน	ไม่ร้ายแรง	ไม่ร้ายแรง	ไม่ร้ายแรง	ร้ายแรง	ไม่ร้ายแรง	ไม่ร้ายแรง	ร้ายแรง

รูปที่ 2-6: ตัวอย่างลักษณะภัยคุกคามทางไซเบอร์แยกตามระดับต่าง ๆ

นอกจากนี้ หน่วยงานอาจพิจารณาใช้งานกรอบงาน MITER ATT&CK ซึ่งเป็นฐานความรู้ที่เข้าถึงได้ทั่วโลกเกี่ยวกับทศวิถีและเทคนิคของฝ่ายตรงข้าม (Adversary Tactics and Techniques) และควรใช้เมื่อจัดหมวดหมู่ภัยคุกคามทางไซเบอร์ แม้ว่าอาจใช้เทคนิคหลายอย่างในเหตุภัยคุกคามทางไซเบอร์เดียว ให้เลือกวิธีการที่ฝ่ายตรงข้ามใช้ประโยชน์เป็นหลัก ตัวอย่างบางส่วนอาจเป็น:

- Phishing
- UnSecured Credentials
- Network Sniffing
- Man-in-the-Middle
- Data Destruction
- OS Credential Dumping
- Event Triggered Execution
- Account Creation
- Disk Wipe
- Network Denial of Service
- Resource Hijacking
- Defacement
- File and Directory Permissions Modification

รูปที่ 2-7: จัดหมวดหมู่ภัยคุกคามทางไซเบอร์ตามกรอบงาน MITER ATT&CK

	ชื่อเอกสาร แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร		
	ระดับชั้นความลับ ใช้ภายในสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น	เวอร์ชัน 1.0	หน้า 36

สังเกตว่ากรอบงาน MITER ATT&CK อาจไม่สามารถระบุสถานการณ์บางสถานการณ์ โดยเฉพาะสถานการณ์ที่ไม่มีเจตนาร้ายที่ก่อให้เกิดแผนการจัดการการรับมือเหตุภัยคุกคามทางไซเบอร์ ข้อยกเว้นต่อไปนี้ อาจต้องใช้หมวดหมู่ของตนเองตามที่กำหนดโดยหน่วยงานหรือนโยบายการบริหารความเสี่ยงของหน่วยงาน:

- Data Loss
- Administrative Errors
- UnSecured Credentials
- Data Destruction
- Lax File and Directory Permissions
- Account Creation
- Disk Wipe
- Network Denial of Service
- Resource Misuse (non-malicious)
- ADD OTHERS AS APPLICABLE TO THE ORGANIZATION/INDUSTRY

รูปที่ 2-8: ตัวอย่างการจัดหมวดหมู่ภัยคุกคามทางไซเบอร์ตามที่กำหนดโดยหน่วยงานหรือนโยบายการบริหารความเสี่ยงของหน่วยงาน

ขอบเขตภัยคุกคามทางไซเบอร์ (Incident Scope)

การกำหนดขอบเขตจะช่วยให้ CIRT เข้าใจถึงผลกระทบทางธุรกิจที่อาจเกิดขึ้นจากภัยคุกคามทางไซเบอร์ดังกล่าว ต่อไปนี้เป็นปัจจัยบางประการที่ควรพิจารณาเมื่อกำหนดขอบเขต:

- มีกี่ระบบที่ได้รับผลกระทบจากภัยคุกคามทางไซเบอร์นี้?
- ข้อมูลที่เป็นความลับหรือได้รับการคุ้มครองเกี่ยวข้องหรือไม่?
- อะไรคือ/เป็นจุดเริ่มต้นของภัยคุกคามทางไซเบอร์ (เช่น อินเทอร์เน็ต เครือข่าย กายภาพ)?
- ความเสียหายที่อาจเกิดขึ้นจากภัยคุกคามทางไซเบอร์คืออะไร?
- เวลาโดยประมาณในการกู้คืนจากภัยคุกคามทางไซเบอร์คือเท่าไร?
- ทรัพยากรใดบ้างที่จำเป็นในการจัดการสถานการณ์?
- การวิเคราะห์สามารถทำได้โดยมีประสิทธิภาพสูงสุดได้อย่างไร?

ผลกระทบจากเหตุภัยคุกคามทางไซเบอร์ (Incident Impact)

เมื่อมีการกำหนดประเภทและขอบเขตของภัยคุกคามทางไซเบอร์แล้ว จะต้องตกลงกันถึงผลกระทบที่อาจเกิดขึ้นจากภัยคุกคามทางไซเบอร์ ความรุนแรงของภัยคุกคามทางไซเบอร์จะเป็นตัวกำหนดแนวทางการดำเนินการแก้ไข อย่างไรก็ตาม ในทุกกรณี รายงานภัยคุกคามทางไซเบอร์จะต้องกรอก และตรวจสอบโดยผู้บัญชาการรับมือเหตุภัยคุกคามทางไซเบอร์ ผลกระทบด้านการดำเนินงานและข้อมูลถูกกำหนดด้วยกิจกรรมการรับมือ ดังตาราง

	ชื่อเอกสาร แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร		
	ระดับชั้นความลับ ใช้ภายในสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น	เวอร์ชัน 1.0	หน้า 37

ระดับความรุนแรง	ผลกระทบการทำงาน (Functional Impact)	คำนิยาม	ลักษณะของภัยคุกคามทางไซเบอร์ มาตรา 60	การตอบสนองของ CIRT
น้อยที่สุด (1)	ไม่มี (Incidental)	ไม่มีผลกระทบต่อความสามารถของหน่วยงานในการให้บริการทั้งหมดแก่ผู้ใช้ทั้งหมด (All Users)	(1) ไม่มี	สร้างตั๋ว (Ticket) และมอบหมายให้แก้ไข
น้อย (2)	ไม่ร้ายแรง (Minor)	ผลน้อยที่สุด (Minimal Effect) หน่วยงานยังคงสามารถให้บริการที่สำคัญทั้งหมดแก่ผู้ใช้ทั้งหมด แต่ประสิทธิภาพด้อยลง	(2) ภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง	- สร้างตั๋วและมอบหมายให้แก้ไข - แจ้ง CIO และ IHT
ปานกลาง (3)	เริ่มร้ายแรง (Moderate)	หน่วยงานสูญเสียความสามารถในการให้บริการที่สำคัญแก่ผู้ใช้ระบบบางส่วน (Subset of System Users) กระบวนการให้บริการศูนย์คอมพิวเตอร์เกิน 3-6 ชั่วโมง	(3) ภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง (แต่มีแนวโน้มจะร้ายแรงขึ้น)	- เริ่ม CIRT เต็มรูปแบบ - เกี่ยวข้องกับ CIO และ IHT
สูง (4)	ร้ายแรง (Major)	หน่วยงานสูญเสียความสามารถในการให้บริการที่สำคัญแก่ผู้ใช้ระบบบางส่วน (Subset of System Users) กระบวนการให้บริการระบบสารสนเทศกลางเกิน 6-12 ชั่วโมง	(4) ภัยคุกคามทางไซเบอร์ในระดับร้ายแรง	- เริ่ม CIRT เต็มรูปแบบ - เกี่ยวข้องกับ CIO และ IHT - CIO และ IHT พิจารณาเปิดใช้งานแผนฟื้นฟูจากภัยพิบัติ (
สูงมาก (5)	วิกฤติ (Extreme)	หน่วยงานไม่สามารถให้บริการที่สำคัญบางอย่าง (Some Critical Services) แก่ผู้ใช้ได้อีกต่อไป	(5) ภัยคุกคามทางไซเบอร์ในระดับวิกฤติ	- เริ่ม CIRT เต็มรูปแบบ - CIO และ IHT พิจารณาเปิดใช้งานแผนฟื้นฟูจากภัยพิบัติ (Disaster Recovery Plan) หรือแผนความต่อเนื่องจากธุรกิจ (Business Continuity Plan: BCP)

รูปที่ 2-9: ตัวอย่างเกณฑ์ผลกระทบการทำงาน (Functional Impact)

	ชื่อเอกสาร แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร		
	ระดับชั้นความลับ ใช้ภายในสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น	เวอร์ชัน 1.0	หน้า 38

ผลกระทบต่อสารสนเทศ (Functional Impact)	คำนิยาม	การตอบสนองของ CIRT
(1) ไม่มี (Incidental/None)	ไม่มีการเข้าถึงข้อมูล นำข้อมูลออก เปลี่ยนแปลง ลบ หรือถูกบุกรุก	● ไม่ต้องดำเนินการใด ๆ
(2) ไม่ร้ายแรง ((Minor /Limited)	มีการเข้าถึงข้อมูลสาธารณะ (Public) หรือข้อมูลที่ไม่ละเอียดอ่อน (Non-sensitive) นำข้อมูลออก เปลี่ยนแปลง ลบ หรือถูกบุกรุก	● แจ้งเจ้าของข้อมูลเพื่อกำหนดแนวทางปฏิบัติที่เหมาะสม
(3) ปานกลาง (Moderate)หรือ เริ่ม ร้ายแรง	ข้อมูลภายในถูกเข้าถึง นำข้อมูลออก เปลี่ยนแปลง ลบ หรือถูกบุกรุก	● แจ้ง CIO และ IHT ● CIO จะทำงานร่วมกับผู้บริหาร ฝ่ายกฎหมาย และเจ้าของข้อมูลเพื่อกำหนดแนวทางปฏิบัติที่เหมาะสม
(4) ร้ายแรง ร้ายแรง(Major/High)	ข้อมูลภายในถูกเข้าถึง นำข้อมูลออก เปลี่ยนแปลง ลบ หรือถูกบุกรุก จำนวนมากอย่างต่อเนื่อง	● แจ้ง CIO และ IHT ● CIO จะทำงานร่วมกับผู้บริหาร ฝ่ายกฎหมาย และเจ้าของข้อมูลเพื่อกำหนดแนวทางปฏิบัติที่เหมาะสม
(5) วิกฤติ (Extreme/Critical)	ข้อมูลที่ได้รับการคุ้มครอง (Protected Data) ถูกเข้าถึง นำข้อมูลออก เปลี่ยนแปลง ลบ หรือถูกบุกรุก	● แจ้ง CIO และ IHT ● CIO จะทำงานร่วมกับฝ่ายกฎหมายเพื่อพิจารณาว่าสามารถรายงานได้หรือไม่ และขอกำหนดการแจ้งเตือนที่เหมาะสม

รูปที่ 2-10: ตัวอย่างเกณฑ์ผลกระทบต่อสารสนเทศ (Informational Impact)

ภัยคุกคามทางไซเบอร์ทั้งหมดต้องถูกบันทึกไว้ในบันทึกกิจกรรมการรับมือเหตุภัยคุกคามทางไซเบอร์และเครื่องมือการประเมิน (Incident Handling Log & Assessment Tool) บันทึกของการดำเนินการทั้งหมดเพื่อแก้ไขเหตุภัยคุกคามทางไซเบอร์ รวมถึงบันทึกห่วงโซ่การดูแล (Chain of Custody) และการเบี่ยงเบนจาก SOP จะต้องรวมอยู่ในเอกสาร

ตารางบันทึกกิจกรรมการรับมือเหตุภัยคุกคามทางไซเบอร์และเครื่องมือประเมิน และระดับการรับมือด้านล่างจะช่วยระบุความรุนแรงของภัยคุกคามทางไซเบอร์และความเร่งด่วนของกิจกรรมการรับมือ

	ชื่อเอกสาร แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร		
	ระดับชั้นความลับ ใช้ภายในสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น	เวอร์ชัน 1.0	หน้า 39

การจำแนกระดับการตอบสนอง (Response Level Classification)		ผลกระทบต่อสารสนเทศ (Informational Impact)			
		ไม่มี (None)	ไม่ร้ายแรง (Limited)	ร้ายแรง (Moderate)	วิกฤต (Critical)
ผลกระทบการทำงาน (Functional Impact)	(1) ไม่มี (Incidental/None)	N/A	Sev. 3	Sev. 2	Sev. 1
	(2) ไม่ร้ายแรง ((Minor /Limited)	Sev. 3	Sev. 3	Sev. 2	Sev. 1
	(3) ปานกลาง (Moderate)หรือ เริ่ม ร้ายแรง	Sev. 3	Sev. 3	Sev. 2	Sev. 1
	(4) ร้ายแรง ร้ายแรง(Major/High)	Sev. 2	Sev. 2	Sev. 2	Sev. 1
	(5) วิกฤติ (Extreme/Critical)	Sev. 1	Sev. 1	Sev. 1	Sev. 1

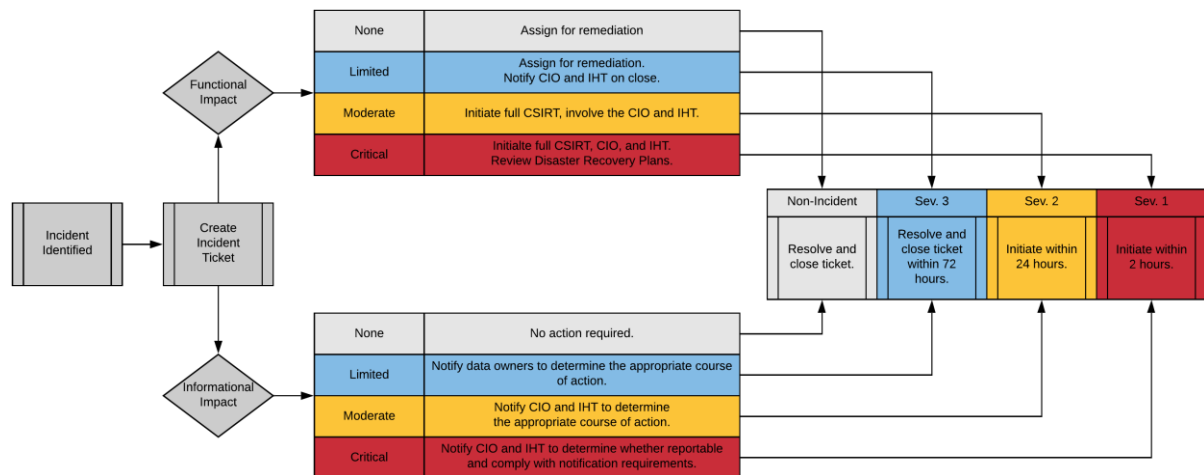
รูปที่ 2-11: การจำแนกระดับการตอบสนอง

ควรใช้ระดับความรุนแรง (Severity Level) เพื่อกำหนดว่ากิจกรรมตอบสนองเริ่มต้นควรเกิดขึ้นเร็วเพียงใด

ระดับความรุนแรง	SLA
Sev. 3	ภายใน 1-12 ชั่วโมง
Sev. 2	ภายใน 1-6 ชั่วโมง
Sev. 1	ภายใน 1 ชั่วโมง

รูปที่ 2-12: ระดับความรุนแรงและการตอบสนองตาม SLA

	ชื่อเอกสาร แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร		
	ระดับชั้นความลับ ใช้ภายในสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น	เวอร์ชัน 1.0	หน้า 40



รูปที่ 2-13: ระดับการรับมือช่วยระบุความรุนแรงของภัยคุกคามทางไซเบอร์และความเร่งด่วนของกิจกรรมการรับมือ

การตัดสินใจที่สำคัญสำหรับการออกจากขั้นตอนการตรวจจับและวิเคราะห์ (Key Decisions for Exiting Detection and Analysis Phase):

- หากกระบวนการตรวจจับและวิเคราะห์ได้กำหนดว่าเหตุการณ์นั้นเป็นภัยคุกคามทางไซเบอร์จริง กระบวนการ IR จะต้องดำเนินต่อไป
- รายละเอียดทั้งหมดในขั้นตอนการตรวจจับจะต้องบันทึกไว้ในแบบฟอร์มการรายงานภัยคุกคามทางไซเบอร์ หากเหตุการณ์นั้นถูกกำหนดให้เป็นภัยคุกคามทางไซเบอร์

หมายเหตุ: หน่วยงานต้องพิจารณาดำเนินการตามมาตรการตามรายละเอียดที่ระบุใน ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปรามปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. 2564

	ชื่อเอกสาร แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร		
	ระดับชั้นความลับ	ใช้ภายในสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น	เวอร์ชัน 1.0 หน้า 41

2.3 ขั้นตอนที่ 3 การจำกัดขอบเขต (Containment) การกำจัด (Eradication) และการกู้คืน (Recovery)

2.3.1 ขั้นตอนที่ 3.1 การจำกัดขอบเขต (Containment)

วัตถุประสงค์ของขั้นตอนการจำกัดขอบเขตในการรับมือเหตุภัยคุกคามทางไซเบอร์คือเพื่อควบคุมสถานการณ์ได้อีกครั้งและจำกัดขอบเขตของความเสียหาย เพื่อให้บรรลุวัตถุประสงค์ของหน่วยงาน ได้กำหนดกลยุทธ์การจำกัดขอบเขตจำนวนหนึ่งที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ประเภทต่าง ๆ อ้างอิงขั้นตอนที่เกี่ยวข้องกับกลยุทธ์การจำกัดขอบเขตอย่างน้อยหนึ่งรายการตามรายการด้านล่าง

2.3.1.1 กลยุทธ์การจำกัดขอบเขต (Containment Strategies)

ใช้รายการกลยุทธ์ด้านล่างเพื่อเลือกขั้นตอนที่เหมาะสมที่สุดสำหรับสถานการณ์ ขั้นตอนทั้งหมดสำหรับแต่ละกลยุทธ์ที่ระบุไว้ด้านล่างมีอยู่ในภาคผนวก VIII หากไม่มีกลยุทธ์ใดที่ตรงกับสถานการณ์ปัจจุบันให้อ้างอิงถึงขั้นตอนการจำกัดขอบเขตทั่วไปที่แสดงด้านล่าง

- ข้อมูลประจำตัวที่ถูกขโมย (Stolen Credentials) ปิดใช้งานข้อมูลประจำตัวของบัญชี รีเซ็ตการเชื่อมต่อที่ใช้งานอยู่ทั้งหมด ตรวจสอบกิจกรรมของผู้ใช้ ย้อนกลับการเปลี่ยนแปลง (Reverse Changes) ไปสู่สถานะเดิม เพิ่มการแจ้งเตือน เสริมความแข็งแกร่งจากการโจมตีในอนาคต
- แรนซัมแวร์ (Ransomware) แยกระบบที่ได้รับผลกระทบ ตรวจสอบการเรียกค่าไถ่ ติดต่อผู้ให้บริการประกันภัย ระบุว่าจะระบบเพิ่มเติมได้รับผลกระทบหรือไม่ และแยกตามความจำเป็น
- DOS/DDOS ควบคุม WAN/ISP
- การระบาดของไวรัส (Virus Outbreak) แยก LAN/ระบบ ออกจากการเชื่อมต่อเครือข่าย
- การสูญหายของข้อมูล (Data Loss) ตรวจสอบกิจกรรมของผู้ใช้ ดำเนินการตามขั้นตอนการรับมือต่อการละเมิดข้อมูล
- การทำให้เว็บไซต์เสียหาย (Website Defacement) ซ่อมแซมเว็บไซต์ เสริมความแข็งแกร่งจากการโจมตีในอนาคต
- API โดนโจมตี (Compromised API) – ตรวจสอบการเปลี่ยนแปลงที่เกิดขึ้น ซ่อมแซม API เสริมความแข็งแกร่งจากการโจมตีในอนาคต

2.3.1.2 ขั้นตอนการจำกัดขอบเขตทั่วไป (Common Containment Steps)

การจำกัดขอบเขตต้องมีการตัดสินใจที่สำคัญเกี่ยวกับธรรมชาติของภัยคุกคามทางไซเบอร์ ผู้จัดการรับมือเหตุภัยคุกคามทางไซเบอร์ (Incident Response Manager) ร่วมกับผู้บัญชาการการรับมือเหตุภัยคุกคามทางไซเบอร์ (Incident Response Commander) และสมาชิกคนอื่น ๆ ของฝ่ายบริหารควรทบทวนขั้นตอนการจำกัดขอบเขตทั้งหมดที่ระบุไว้ด้านล่างเพื่อกำหนดกลยุทธ์ในการจำกัดขอบเขตและจำกัดความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์

ความพยายามทั้งหมดในการยับยั้งภัยคุกคามจะต้องพิจารณาทุกความพยายามเพื่อลดผลกระทบต่อการดำเนินธุรกิจให้เหลือน้อยที่สุด อาจจำเป็นต้องแจ้งบุคคลที่สามหรือผู้มีส่วนได้ส่วนเสีย ในกรณีที่น่า

	ชื่อเอกสาร แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร		
	ระดับชั้นความลับ	ใช้ภายในสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น	เวอร์ชัน 1.0 หน้า 42

มีการบังคับใช้กฎหมายเข้ามาเกี่ยวข้อง จะต้องพยายามรักษาความสมบูรณ์ของข้อมูลทางนิติวิทยาศาสตร์หรือบันทึกข้อมูลที่เกี่ยวข้อง และรักษาห่วงโซ่การควบคุม (Chain-of-custody) ที่ชัดเจน ในกรณีที่ไม่สามารถรักษาหลักฐานอย่างเหมาะสมเนื่องจากความพยายามในการจำกัดขอบเขต จะต้องจัดทำเอกสารความคลาดเคลื่อน (Discrepancy) ที่เกิดขึ้น

เมื่อประเมินขั้นตอนการจำกัดขอบเขต ให้พิจารณาสิ่งต่อไปนี้:

- เปิดใช้งานบัญชีการดูแลระบบแบบใช้แล้วสิ้นสุด (ใช้เฉพาะกิจ) เพื่อใช้ในช่วงการสืบสวนสอบสวนและรีเซ็ตรหัสผ่านที่เกี่ยวข้องหากเชื่อว่ามีความเสี่ยงที่จะถูกโจมตีขณะใช้งาน (ดูขั้นตอนที่ 1 รายละเอียดการจัดเตรียม)
- ความสามารถในการให้บริการที่สำคัญจะได้รับผลกระทบหรือไม่? ยังไง? นานแค่ไหน?
- ควรแจ้งผู้ให้บริการประกันภัยไซเบอร์เมื่อใด (ดูข้อมูลการติดต่อ)
- มีการสืบสวนสอบสวนทางกฎหมายหรือการดำเนินการอื่น ๆ หรือไม่? หลักฐานต้องเก็บไว้หรือไม่? (ดูการเก็บรักษาหลักฐาน)
- เป็นไปได้แค่ไหนที่ขั้นตอนการจำกัดขอบเขตจะสำเร็จ? ผลลัพธ์ที่ได้คืออะไร สมบูรณ์หรือบางส่วน?
- ทรัพยากรใดบ้างที่จำเป็นในการสนับสนุนกิจกรรมการจำกัดขอบเขต?
- ความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์และทรัพยากรอื่น ๆ คืออะไร?
- ระยะเวลาที่คาดหวังของการแก้ปัญหาคือเท่าไร? (ชั่วคราว ระยะสั้น ระยะยาว หรือถาวร)
- สมาชิกในทีม IR ควรดำเนินการอย่างไม่ต่อเนื่อง (Act Discretely) เพื่อพยายามซ่อนกิจกรรมของตนจากผู้โจมตีหรือไม่?
- จำเป็นต้องมีความช่วยเหลือจากบุคคลที่สามหรือไม่? เวลาตอบสนองที่คาดหวังคืออะไร?
- ต้องแจ้งผู้มีส่วนได้เสีย (ลูกค้า คู่ค้า นักลงทุน) หรือไม่? ถ้าเป็นเช่นนั้นเมื่อไหร่? (ดูภาคผนวก IV)
- ผลกระทบต่ออุปกรณ์ เครือข่าย หรือสิ่งอำนวยความสะดวก (ของหน่วยงาน) มีความจำเป็นต่อการเปิดใช้งานแผนฟื้นฟูจากภัยพิบัติ (Disaster Recovery Plan) หรือไม่?
- ข้อมูลที่ได้รับผลกระทบรวมถึงข้อมูลที่ได้รับการคุ้มครอง เช่น ข้อมูลผู้ถือบัตรหรือไม่ ถ้าใช่ โปรดดูข้อกำหนดการแจ้งเตือน

	ชื่อเอกสาร แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร		
	ระดับชั้นความลับ ใช้งานในสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น	เวอร์ชัน 1.0	หน้า 43

2.3.1.3 การใช้ทรัพยากร (Engage Resources)

CIRT ควรเลือกตัวเลือกตามความรุนแรงของเหตุภัยคุกคามทางไซเบอร์ ความเสียหายที่เกิดขึ้น โดยของหน่วยงาน และข้อพิจารณาทางกฎหมาย

	การสืบสวนสอบสวนภายใน (In-house Investigation)	การบังคับใช้กฎหมาย (Law Enforcement)	ผู้เชี่ยวชาญด้านนิติวิทยาศาสตร์เอกชน (Private Forensic Specialist)
เวลาในการตอบสนอง	ตอบสนองอย่างรวดเร็ว	แตกต่างกันไปตามพื้นที่และหน่วยงาน	ตอบสนองอย่างรวดเร็ว
ความสามารถ	ทักษะแตกต่างกันไป	ขึ้นอยู่กับกรบังคับใช้กฎหมายในท้องถิ่น	มีทักษะสูง มักมีพื้นฐานด้านการบังคับใช้กฎหมาย
การเก็บรักษาหลักฐาน	ไม่รับรองความถูกต้องของหลักฐาน	รักษาความสมบูรณ์ของหลักฐานและนำเสนอหลักฐานในศาล	รักษาความสมบูรณ์ของหลักฐานและนำเสนอหลักฐานในศาล
ผลกระทบด้านชื่อเสียง	ผลกระทบน้อยที่สุด	อาจสูญเสียชื่อเสียงหากเกิดเหตุภัยคุกคามทางไซเบอร์บางอย่างขึ้นสู่สาธารณะ	อาจสูญเสียชื่อเสียงหากเกิดเหตุภัยคุกคามทางไซเบอร์บางอย่างขึ้นสู่สาธารณะ

รูปที่ 2-14: ตัวเลือกการใช้ทรัพยากรตามความรุนแรงของเหตุภัยคุกคามทางไซเบอร์

2.3.1.4 เก็บรักษาหลักฐาน (Preserve Evidence)

การเก็บหลักฐานตามลำดับของการสูญสลาย (Order of Volatility)

ตามลำดับของการสูญสลาย (Order of Volatility) หมายถึงลำดับที่หน่วยงานควรรวบรวมหลักฐานที่ไม่ถาวร (หมายถึงเมื่อไม่มีแหล่งพลังงานไฟฟ้าหรือรีสาธเครื่อง ข้อมูลเหล่านั้นจะหายไป) โดยทั่วไป หน่วยงานควรรวบรวมหลักฐานโดยเริ่มจากจุดที่มีการสูญสลายเร็วมากที่สุดและเคลื่อนไปสู่จุดที่มีการสูญสลายน้อยที่สุดตัวอย่างเช่น หน่วยความจำเข้าถึงโดยสุ่ม (Random Access Memory: RAM) จะหายไปหลังจากปิดเครื่องคอมพิวเตอร์ ด้วยเหตุนี้ จึงเป็นสิ่งสำคัญที่ต้องตระหนักว่า ไม่ควรปิดเครื่องคอมพิวเตอร์หากสงสัยว่าคอมพิวเตอร์เกี่ยวข้องกับเหตุการณ์ด้านความปลอดภัยและอาจมีหลักฐานอันมีค่า

โปรเซสเซอร์สามารถทำงานได้กับข้อมูลใน RAM เท่านั้น ดังนั้นข้อมูลทั้งหมดใน RAM จะบ่งบอกว่าระบบกำลังทำอะไรอยู่ ซึ่งรวมถึงข้อมูลที่ผู้ใช้กำลังดำเนินการอยู่ กระบวนการของระบบ (System Processes) กระบวนการเครือข่าย (Network Processes) ส่วนที่เหลือของแอปพลิเคชัน (Application Remnants) และอื่น ๆ อีกมากมาย ทั้งหมดนี้อาจเป็นหลักฐานอันมีค่าในการสืบสวน แต่หากช่างเทคนิคมือใหม่ปิดคอมพิวเตอร์ หลักฐานก็จะสูญหายไป

เครื่องมือทางนิติวิทยาศาสตร์หลายอย่างมีความสามารถในการเก็บข้อมูลที่มีการสูญสลายตัวอย่างเช่น Kali Linux มีแอปพลิเคชัน Volatility (มีอยู่ใน Applications > Forensics > Volatility)

	ชื่อเอกสาร แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร		
	ระดับชั้นความลับ ใช้งานในสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น	เวอร์ชัน 1.0	หน้า 44

ที่สามารถจับเนื้อหาของ RAM ได้ เมื่อบันทึกข้อมูลแล้ว ผู้เชี่ยวชาญจะสามารถวิเคราะห์และรับข้อมูลเชิงลึกว่าคอมพิวเตอร์และผู้ใช้กำลังทำอะไรอยู่

ในทางตรงกันข้าม ข้อมูลบนดิสก์ไทรฟ์จะยังคงอยู่ในไทรฟ์แม้ว่าจะปิดระบบไปแล้วก็ตาม ซึ่งรวมถึงไฟล์ใด ๆ และแม้แต่ข้อมูลระดับต่ำ เช่น Master Boot Record บนไทรฟ์ อย่างไรก็ตาม การปกป้องข้อมูลบนดิสก์ก่อนที่จะวิเคราะห์เป็นสิ่งสำคัญ และวิธีการทั่วไปคือการจับภาพของดิสก์ (Capturing an Image of the Disk)

ลำดับของการสูญสลายมากที่สุดไปการสูญสลายน้อยที่สุด คือ:

- ข้อมูลในหน่วยความจำแคช (Cache Memory) รวมถึงแคชของโปรเซสเซอร์และแคชของฮาร์ดไทรฟ์
- ข้อมูลใน RAM รวมถึงโปรเซสของระบบและเครือข่าย (System and Network Processes)
- ไฟล์เก็บเพจ (Paging File) (บางครั้งเรียกว่าไฟล์สวอป (Paging File)) บนดิสก์ไทรฟ์ระบบ
- ข้อมูลที่จัดเก็บไว้ในดิสก์ไทรฟ์ภายในเครื่อง (Local Disk Drives)
- บันทึกที่จัดเก็บไว้ในระบบระยะไกล (Remote Systems)
- สื่อเก็บถาวร (Archive Media)

การดำเนินการเก็บหลักฐานต้องดำเนินการโดยผู้ที่ผ่านการฝึกอบรมและมีความเชี่ยวชาญ และดำเนินการตามขั้นตอนมาตรฐานที่เป็นที่ยอมรับ เพื่อให้หลักฐานนั้นมีความเชื่อถือและสามารถนำไปใช้ได้

การดำเนินการเก็บหลักฐานต้องดำเนินการโดยผู้ที่ผ่านการฝึกอบรมและมีความเชี่ยวชาญ และดำเนินการตามขั้นตอนมาตรฐานที่เป็นที่ยอมรับ เพื่อให้หลักฐานนั้นมีความเชื่อถือและสามารถนำไปใช้ได้

หมายเหตุ: หากมีเหตุผลหนักแน่นที่เชื่อได้ว่ามีแนวโน้มว่าจะมีการดำเนินคดีทางอาญาหรือทางแพ่งแบบฟอร์มห่วงโซ่การคุ้มครอง (Chain of Custody Form) ของหน่วยงาน จะต้องถูกใช้ทุกครั้งที่มีการนำหลักฐานเข้าควบคุม หรือโอนสิทธิ์การดูแลเพื่อวัตถุประสงค์ในการสืบสวนสอบสวน

กฎหมายเกี่ยวกับกฎหมายและระเบียบข้อบังคับที่เกี่ยวข้องกับการรวบรวมและการรักษามีรายละเอียดดังนี้

- หลักฐาน สร้างบันทึกโดยละเอียดสำหรับหลักฐานทั้งหมดที่รวบรวม รวมถึง:
- ข้อมูลการระบุ (เช่น หมายเลขซีเรียล รุ่น ชื่อโฮสต์ ที่อยู่ MAC ที่อยู่ IP หรือตัวระบุอื่น ๆ)
- ชื่อและข้อมูลติดต่อของบุคคลทั้งหมดที่จัดการหลักฐานในระหว่างการสืบสวนสอบสวน
- วันที่และเวลาของการโอนหรือการจัดการหลักฐานในแต่ละครั้ง
- รายชื่อสถานที่ทั้งหมดที่จัดเก็บหลักฐาน
- การเบี่ยงเบนจาก SOP และเหตุผลที่เกี่ยวข้อง

	ชื่อเอกสาร	แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร		
	ระดับชั้นความลับ	ใช้ภายในสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น	เวอร์ชัน 1.0	หน้า 45

2.3.1.5 ลดผลกระทบ (Reduce Impact)

ขึ้นอยู่กับประเภทของภัยคุกคามทางไซเบอร์ ทีมต้องดำเนินการอย่างรวดเร็วเพื่อลดผลกระทบต่อระบบที่ได้รับผลกระทบและ/หรือลดการเข้าถึงของผู้โจมตี การดำเนินการอาจรวมถึงแต่ไม่จำกัดเพียงสิ่งต่อไปนี้:

- หยุดผู้โจมตีโดยใช้การควบคุมการเข้าถึง (Access Controls) เช่น ปิดใช้งานบัญชี รีเซ็ตการเชื่อมต่อที่ใช้งานอยู่ เปลี่ยนรหัสผ่าน ใช้ ACL ของหน่วยงานเตอร์หรือกฎไฟร์วอลล์ ฯลฯ)
- แยกระบบที่ถูกบุกรุกออกจากเครือข่าย
- หลีกเลี่ยงการเปลี่ยนแปลงข้อมูลที่สูญสลายได้ง่าย (Volatile State Data) หรือข้อมูลสถานะของระบบตั้งแต่ต้น
- ระบุระบบภายนอกที่สำคัญที่ต้องทำงานอยู่ (เช่น อีเมล แอปพลิเคชันไคลเอนต์ DNS) และปฏิเสธกิจกรรมอื่น ๆ ทั้งหมด
- รักษาโปรไฟล์ให้ต่ำ (Maintain a Low Profile) ถ้าเป็นไปได้ เพื่อหลีกเลี่ยงการแจ้งเตือนผู้โจมตีว่าหน่วยงานทราบถึงการปรากฏตัวของพวกเขาหรือให้ออกาสพวกเขาเรียนรู้กลวิธีเทคนิคหรือขั้นตอนของ CIRT
- ในขอบเขตที่เป็นไปได้ ให้พิจารณาการรักษาสถานะของระบบไว้สำหรับการตรวจสอบเพิ่มเติมหรือใช้เป็นหลักฐาน

2.3.1.6 รวบรวมข้อมูลและเพิ่มการบันทึกกิจกรรม (Collect Data and Increase Activity Logging)

เพิ่มการเฝ้าระวังและดักจับแพ็กเก็ตบนระบบที่ได้รับผลกระทบ ในขณะที่ CIRT ตรวจสอบขอบเขตและผลกระทบของภัยคุกคามทางไซเบอร์ ดำเนินการบันทึกและติดตามเพิ่มขึ้นต่อไปเมื่อหน่วยงานเข้าสู่ขั้นตอนการกำจัดและการกู้คืน (Eradication and Recovery Phases)

- เปิดใช้งานการดักจับแพ็กเก็ตแบบเต็ม (Enable Full Packet Capture)
- รวบรวมและตรวจสอบระบบ เครือข่าย และล็อกอื่น ๆ ที่เกี่ยวข้อง
- สร้างอิมเมจหน่วยความจำ (Memory Image) ของระบบที่ได้รับผลกระทบ
- เก็บอิมเมจทางนิติวิทยาศาสตร์ (Forensic Image) ของระบบที่ได้รับผลกระทบ
- เฝ้าระวังช่องทางการสื่อสารของผู้โจมตีที่เป็นไปได้

2.3.1.7 ทำการค้นหาข้อมูลเพิ่มเติม (Conduct Research)

ดำเนินการค้นหาทางอินเทอร์เน็ต ปรึกษาทรัพยากรบุคคลที่สาม และ/หรือปรึกษากับผู้ให้บริการประกันภัยเทคโนโลยีสารสนเทศ (IT Insurance) โดยใช้ข้อมูลจากอาการที่ชัดเจนและข้อมูลอื่น ๆ ที่เกี่ยวข้องกับเหตุภัยคุกคามทางไซเบอร์ที่หน่วยงานกำลังประสบอยู่ อาจนำไปสู่ข้อมูลเพิ่มเติมเกี่ยวกับการโจมตีตัวอย่างเช่น หากผู้ให้บริการประกันภัยได้รับรายงานภัยคุกคามทางไซเบอร์ที่คล้ายคลึงกันหลายฉบับ หรือหาก

	ชื่อเอกสาร	แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร		
	ระดับชั้นความลับ	ใช้ภายในสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น	เวอร์ชัน 1.0	หน้า 46

ข้อความรายชื่อผู้รับจดหมาย (Mailing List Message) มี IP หรือข้อความเดียวกันของข้อความที่หน่วยงานได้รับ

2.3.1.8 แจ้งผู้ที่เกี่ยวข้อง (Notify Interested Parties)

เมื่อระบุเหตุภัยคุกคามทางไซเบอร์ได้แล้ว ให้พิจารณาว่ามีผู้อื่นที่จำเป็นต้องได้รับแจ้งหรือไม่ทั้งภายใน เช่น ทรัพยากรบุคคล กฎหมาย การเงิน สื่อสารหน่วยงาน เจ้าของธุรกิจ เป็นต้น และภายนอก เช่น ผู้ให้บริการ หน่วยงานควบคุมหรือกำกับดูแล งานสาธารณะ สื่อ สัมพันธ์ ลูกค้า ประชาชนทั่วไป เป็นต้น ปฏิบัติตามหลักการ “จำเป็นต้องรู้ (Need to Know)” เสมอในการสื่อสารทั้งหมด ที่สำคัญที่สุด ยังคงเป็นการสื่อสารข้อเท็จจริงและหลีกเลี่ยงการคาดเดา

ทั้งนี้ขึ้นอยู่กับระดับความอ่อนไหวของเหตุภัยคุกคามทางไซเบอร์ ฝ่ายกฎหมาย/ฝ่ายจัดการอาจจำเป็นต้องกำหนดให้พนักงานลงนามข้อตกลงรักษาความลับ (NDA) หรือออกคำสั่งให้รักษาความลับกับพนักงานที่จำเป็นต้องมีส่วนร่วม ทั้งนี้ขึ้นอยู่กับระดับความอ่อนไหวของเหตุภัยคุกคามทางไซเบอร์

2.3.1.9 การตัดสินใจที่สำคัญสำหรับการออกจากขั้นตอนการจำกัดขอบเขต (Key Decisions for Exiting Containment Phase)

- ความสามารถของผู้โจมตีในการส่งผลกระทบต่อเครือข่ายได้รับการควบคุม/หยุดอย่างมีประสิทธิภาพ
- ระบบที่ได้รับผลกระทบ
- ระบบที่ถูกบุกรุก ข้อมูลที่สูญสลายได้ (volatile Data) ที่สามารถรวบรวมได้ อิมเมจหน่วยความจำที่รวบรวม และดิสก์ที่ถูกอิมเมจสำหรับการวิเคราะห์

2.3.1.10 การสืบสวนสอบสวน (Investigation)

ในขณะที่ CIRT ทำงานเพื่อจำกัดขอบเขต (Contain) กำจัด (Eradicate) และฟื้นฟู (Recover) จากเหตุภัยคุกคามทางไซเบอร์ดังกล่าว การสืบสวนสอบสวนจะดำเนินต่อไป ในขณะที่การสืบสวนสอบสวนดำเนินไป หน่วยงานอาจพบว่าเหตุภัยคุกคามทางไซเบอร์นั้นไม่ได้ถูกจำกัดขอบเขต กำจัด หรือกู้คืนอย่างสมบูรณ์หากเป็นสถานการณ์ดังกล่าว อาจจำเป็นต้องทบทวนขั้นตอนก่อนหน้านี้เพิ่มเติม ขั้นตอนการจำกัดขอบเขต การกำจัด และการกู้คืนมักเป็นวัฏจักร

การสืบสวนสอบสวนพยายามระบุระบบ บริการ และข้อมูลทั้งหมดที่ได้รับผลกระทบจากเหตุภัยคุกคามทางไซเบอร์อย่างครบถ้วน รวมถึงการวิเคราะห์สาเหตุที่แท้จริง (Root Cause) ซึ่งช่วยในการระบุจุดเริ่มต้นของผู้โจมตีหรือจุดอ่อนในระบบที่ทำให้เหตุการณ์ขยายไปสู่ภัยคุกคามทางไซเบอร์ได้

อาจต้องทำสัญญากับบุคคลที่สาม หากการสืบสวนสอบสวนอยู่นอกเหนือทักษะของ CIRT เช่น ระบบที่ได้รับผลกระทบนั้นเป็นของผู้ให้บริการคลาวด์ หรือจำเป็นต้องมีการวิเคราะห์ทางนิติวิทยาศาสตร์

2.3.1.11 การสืบสวนสอบสวนสาเหตุเบื้องต้นและสาเหตุที่แท้จริง (Root Cause)

ควรดำเนินการสืบสวนสอบสวนโดยคำนึงถึงผลกระทบอย่างต่อเนื่องต่อการดำเนินธุรกิจที่สำคัญตามหลักการแล้ว ควรสรุปการสืบสวนสอบสวนสาเหตุเบื้องต้นก่อนออกจากขั้นตอนการกำจัด อย่างไรก็ตาม

	ชื่อเอกสาร แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร		
	ระดับชั้นความลับ ใช้งานในสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น	เวอร์ชัน 1.0	หน้า 47

ในบางครั้ง อาจจำเป็นหรือเหมาะสมที่จะดำเนินการสืบสวนสอบสวนต่อไปในระหว่างหรือหลังการกำจัดและการกู้คืน การล่าช้าในการสืบสวนสอบสวนควรพิจารณาเมื่อ CIRT มั่นใจว่าเหตุการณ์ได้รับการควบคุมอย่างสมบูรณ์และทราบขอบเขตทั้งหมดของผลกระทบแล้ว ความล่าช้าหรือการปรับเปลี่ยนขอบเขตของกิจกรรมการสืบสวนสอบสวนต้องได้รับอนุมัติจากผู้บัญชาการการรับมือเหตุภัยคุกคามทางไซเบอร์

เทคนิคการสืบสวนสอบสวนที่ใช้จะแตกต่างกันไปตามประเภทของเหตุการณ์ การสืบสวนสอบสวนอาจอาศัยบางส่วน (หรือทั้งหมด) ต่อไปนี้:

- สัมภาษณ์พยานและ/หรือบุคคลที่ได้รับผลกระทบ
- การทำอิมเมจ สแน็ปช็อต หรือดัมป์หน่วยความจำ (Memory Dumps) ของระบบที่ได้รับผลกระทบ
- การได้เอกสารที่เกี่ยวข้อง
- ดำเนินการสังเกตการณ์
- การถ่ายภาพสถานที่ทางกายภาพ
- ตรวจสอบภาพจากกล้องวงจรปิด
- วิเคราะห์ล็อกของอุปกรณ์ เทคโนโลยี และโฮสต์ต่างๆ ที่เกี่ยวข้อง (เช่น ไฟร์วอลล์ หน่วยงานเตอร์ แอนตี้ไวรัส การตรวจจับการบุกรุก (Intrusion Detection) โฮสต์)
- การตรวจสอบกฏอีเมล (บัญชีอีเมลที่ถูกบุกรุก)
- เปรียบเทียบระบบที่ถูกบุกรุกกับสำเนาที่ดีที่รู้จัก (Known Good Copy)
- การตรวจจับความผิดปกติ/การเฝ้าระวังพฤติกรรม (เปรียบเทียบกับค่าขั้นต่ำที่กำหนดไว้ล่วงหน้า (Pre-established Baseline))

2.3.2 ขั้นตอนที่ 3.2 รายละเอียดการกำจัด (Eradication)

การกำจัดประกอบด้วยการกำจัดองค์ประกอบทั้งหมดของภัยคุกคามทางไซเบอร์ทั้งหมด

2.3.2.1 การกำจัด (Eradication)

หมายเหตุ: เครื่องมือการดูแลระบบที่อยู่บนโฮสต์ที่ถูกบุกรุกสามารถแก้ไขเวอร์ชันดั้งเดิมได้ ให้ใช้ชุดเครื่องมือการดูแลระบบแยกต่างหาก (เช่น ดิสก์สำหรับบูต) มากกว่าชุดเครื่องมือบนโฮสต์ที่ถูกบุกรุกเพื่อสืบสวนสอบสวนทุกครั้งที่ทำได้

ขั้นตอนในการกำจัดองค์ประกอบของภัยคุกคามทางไซเบอร์อาจรวมถึง:

- ปิดการใช้งานบัญชีผู้ใช้ที่ถูกละเมิด
- รีเซ็ตเซสชันที่ใช้กันอยู่สำหรับบัญชีที่ละเมิด
- ระบุและบรรเทาช่องโหว่ที่ผู้โจมตีใช้
- ปิดพอร์ตที่เปิดโดยไม่จำเป็น
- เพิ่มมาตรการรักษาความมั่นคงปลอดภัยในการตรวจพิสูจน์ตัวตน (Authentication Security Measures) เช่น ใช้ MFA, เพิ่มการจำกัดตำแหน่งทางภูมิศาสตร์

	ชื่อเอกสาร	แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร		
	ระดับชั้นความลับ	ใช้ภายในสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น	เวอร์ชัน 1.0	หน้า 48

- เพิ่มการล็อกการรักษาความมั่นคงปลอดภัย (Security Logging) การแจ้งเตือน และการเฝ้าระวัง (Monitoring)
- ล้างการติดตั้งระบบปฏิบัติการและแอปพลิเคชันที่ได้รับผลกระทบ

ระบบปฏิบัติการและแอปพลิเคชันที่ติดตั้งใหม่ทั้งหมดจะต้องติดตั้งตามมาตรฐานการสร้างระบบ (System Build Standards) ซึ่งรวมถึงแต่ไม่จำกัดเพียง:

- 1) การใช้แพตช์ความมั่นคงปลอดภัยล่าสุด (Latest Security Patches) ทั้งหมด
- 2) ปิดการใช้งานบริการที่ไม่จำเป็นทั้งหมด
- 3) การติดตั้งซอฟต์แวร์ป้องกันไวรัส
- 4) ใช้ค่าขั้นต่ำการกำหนดค่าระบบที่แข็งแกร่ง (Hardened System Configuration Baselines)
- 5) การเปลี่ยนรหัสผ่านของบัญชีทั้งหมด (รวมถึงโดเมน ผู้ใช้ และบัญชีบริการ)

หมายเหตุ: อาจเป็นไปได้ที่จะกู้คืนระบบโดยไม่ต้องทำการติดตั้งใหม่ทั้งหมด บุคลากรด้านเทคโนโลยีสารสนเทศจะดำเนินการตามทิศทางของ CIRT ที่จะทำการตัดสินใจนี้

2.3.2.2 การตัดสินใจที่สำคัญสำหรับการออกจากขั้นตอนการกำจัด (Key Decisions for Exiting Eradication Phase)

- มีการระบุสาเหตุที่แท้จริงและช่องโหว่ที่ระบุได้รับการแก้ไขแล้วหรือไม่?
- บัญชีที่ได้รับผลกระทบทั้งหมด รวมถึงข้อมูลประจำตัวของเครื่องเขียน CIRT (CIRT Burner Credentials) ถูกรีเซ็ตหรือไม่
- CIRT มั่นใจว่าเครือข่ายและระบบได้รับการกำหนดค่าให้จัดการเกิดขึ้นซ้ำ
- ไม่มีหลักฐานของเหตุการณ์หรือภัยคุกคามทางไซเบอร์ที่เกิดขึ้นซ้ำ
- การลงชื่อจาก IR Manager สำหรับภัยคุกคามทางไซเบอร์ที่มีความรุนแรงจำกัด (Limited-severity Incidents) หรือ CIO สำหรับภัยคุกคามทางไซเบอร์ระดับร้ายแรงและระดับวิกฤต

2.3.3 ขั้นตอนที่ 3.3 รายละเอียดการกู้คืน (Recovery Details)

ก่อนที่จะกู้คืนระบบสู่การทำงานปกติ เป็นสิ่งสำคัญที่ CIRT ตรวจสอบระบบเพื่อพิจารณาว่าการกำจัด (Eradication) สำเร็จ และเครือข่ายมีความมั่นคงปลอดภัย เมื่อหน่วยงานถูกโจมตีสำเร็จ ผู้โจมตีมักจะโจมตีอีกครั้งโดยใช้เครื่องมือและเทคนิคเดิมที่ใช้ในการโจมตีครั้งแรก เมื่อเข้าถึงระบบหรือเครือข่ายที่ถูกบุกรุกได้เพียงครั้งเดียว ผู้โจมตีจะมีข้อมูลเพิ่มเติมพร้อมใช้ในการโจมตีในอนาคต

หากเป็นไปได้ ควรติดตั้งระบบในสภาพแวดล้อมการทดสอบ (Test Environment) เพื่อกำหนดฟังก์ชันการทำงานก่อนที่จะนำกลับมาใช้ใหม่ในสภาพแวดล้อมการใช้งานจริง (Production Environment)

นอกจากนี้ ควรมีการเฝ้าระวังเครือข่ายนานเท่าที่จำเป็นเพื่อตรวจหาความพยายามในการเข้าถึงโดยไม่ได้รับอนุญาต

	ชื่อเอกสาร แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร		
	ระดับชั้นความลับ	ใช้ภายในสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น	เวอร์ชัน 1.0 หน้า 49

ขั้นตอนการกู้คืนอาจรวมถึง:

- การกู้คืนระบบจากการสำรองข้อมูลที่ปลอดภัย (Lean Backup)
- แทนที่ข้อมูลที่เสียหายจากการสำรองข้อมูลที่ปลอดภัย (Clean Backup)
- การกู้คืนการเชื่อมต่อเครือข่ายและกฎการเข้าถึง
- การสื่อสารกับผู้มีส่วนได้ส่วนเสียเกี่ยวกับการเปลี่ยนแปลงที่เกี่ยวข้องกับความมั่นคงปลอดภัยที่เพิ่มขึ้น
- เพิ่มกิจกรรมการเฝ้าระวังเครือข่ายและระบบ (ระยะสั้นหรือระยะยาว)
- เพิ่มการสื่อสารภายใน/การรายงานที่เกี่ยวข้องกับการเฝ้าระวัง
- ว่าจ้างบุคคลที่สามเพื่อสนับสนุนการตรวจจับหรือป้องกันการโจมตีในอนาคต

2.3.3.1 การตัดสินใจที่สำคัญสำหรับการออกจากขั้นตอนการกู้คืน (Key Decisions for Exiting Recovery Phase)

- มีการกู้คืนการดำเนินธุรกิจแล้วหรือไม่? (Have Business Operations Been Restored)

หมายเหตุ: หน่วยงานต้องพิจารณาดำเนินมาตรการตามรายละเอียดที่ระบุใน ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปรามปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. 2564

2.4 ขั้นตอนที่ 4 การทบทวนหลังการดำเนินการ (After-Action Review Process)

การทบทวนหลังการดำเนินการเป็นการติดตามผล (Follow-up) ซึ่งประกอบด้วยกรายงานและการวิเคราะห์หลังภัยคุกคามทางไซเบอร์เกี่ยวกับระบบที่เป็นเป้าหมายของภัยคุกคามทางไซเบอร์และระบบอื่น ๆ ที่อาจมีความเสี่ยง วัตถุประสงค์ของขั้นตอนนี้คือการปรับปรุงอย่างต่อเนื่องในการดำเนินการด้านความมั่นคงปลอดภัย ความสามารถในการรับมือ และขั้นตอนต่าง ๆ

2.4.1 เอกสาร (Documentation)

รายละเอียดทั้งหมดที่เกี่ยวข้องกับกระบวนการรับมือเหตุภัยคุกคามทางไซเบอร์จะต้องได้รับการจัดทำเป็นเอกสารอย่างเป็นทางการและเป็นไฟล์เพื่อให้ง่ายต่อการอ้างอิง ต้องบำรุงรักษารายการต่อไปนี้เมื่อทำได้:

- 1) เหตุการณ์ของระบบทั้งหมด (All System Events) ดูจากบันทึกการตรวจสอบ (Audit Records) หรือล็อก (Log)
- 2) การดำเนินการทั้งหมด รวมถึงวันที่และเวลาที่ดำเนินการ
- 3) การสื่อสารภายนอกทั้งหมด
- 4) บันทึกของผู้สืบสวนสอบสวนที่รวบรวม

	ชื่อเอกสาร แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร		
	ระดับชั้นความลับ ใช้ภายในสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น	เวอร์ชัน 1.0	หน้า 50

5) การเบี่ยงเบนใด ๆ จาก SOP และการให้เหตุผล

รายงานภัยคุกคามทางไซเบอร์ที่จัดทำเป็นเอกสารต่อไปนี้จะถูกเขียนโดย CIRT เมื่อสิ้นสุดการตอบสนอง (Response):

- 1) คำอธิบายลำดับเหตุการณ์ที่แน่นอน
- 2) วิธีการค้นพบ
- 3) มาตรการป้องกันที่มีใช้งานอยู่
- 4) การประเมินเพื่อพิจารณาว่าการกู้คืนเพียงพอหรือไม่และควรพิจารณาข้อเสนอแนะอื่นใด

วัตถุประสงค์ของการรายงาน คือ เพื่อระบุจุดที่อาจต้องปรับปรุงในการรับมือเหตุภัยคุกคามทางไซเบอร์และขั้นตอนการรายงาน ดังนั้น การทบทวนรายงานโดยฝ่ายบริหารควรจัดทำเป็นเอกสารพร้อมกับบทเรียนที่ได้รับ เพื่อปรับปรุงพื้นที่ที่ระบุและใช้เป็นข้อมูลอ้างอิงสำหรับภัยคุกคามทางไซเบอร์ในอนาคต

2.4.2 บทเรียนที่ได้รับและการแก้ไข (Lessons Learned and Remediation)

CIRT จะหารือกับฝ่ายที่เกี่ยวข้อง เช่น เจ้าหน้าที่ด้านเทคนิค ผู้บริหาร ผู้ขาย ทีมรักษาความมั่นคงปลอดภัย เป็นต้น เพื่อรวบรวมบทเรียนที่ได้รับจากภัยคุกคามทางไซเบอร์ดังกล่าวเพื่อลดความเสี่ยงของเหตุการณ์ในอนาคต ตามความเข้าใจในสาเหตุที่แท้จริง หน่วยงานจะดำเนินการตามขั้นตอนต่าง ๆ เพื่อเสริมสร้างและปรับปรุง ระบบสารสนเทศ นโยบาย ขั้นตอน การป้องกัน และ/หรือการฝึกอบรมตามความจำเป็น ในกรณีที่มีการบรรเทาผลกระทบหรือการเปลี่ยนแปลงที่เสนอถูกปฏิเสธ จะต้องปฏิบัติตามกระบวนการยอมรับความเสี่ยง ควรมีการวิเคราะห์ภัยคุกคามทางไซเบอร์เพื่อค้นหาแนวโน้ม ควรพิจารณาการดำเนินการแก้ไขสาเหตุ (Corrective Action) ตามความเหมาะสม

การอภิปรายบทเรียนที่ได้รับ ควรครอบคลุม:

- ทบทวนการค้นพบและการรับมือเหตุภัยคุกคามทางไซเบอร์
- พนักงานและผู้บริหารทำงานได้ดีเพียงใดและปฏิบัติตามขั้นตอนที่เป็นเอกสารหรือไม่
- ทบทวนการกระทำที่ชะลอหรือขัดขวางความพยายามในการกู้คืน
- เสนอการปรับปรุงเพื่อการรับมือในอนาคตและความพยายามในการสื่อสาร
- คำแนะนำเพื่อเพิ่มความเร็วในการตรวจจับและตอบสนองในอนาคต
- คำแนะนำสำหรับความพยายามในการแก้ไขในระยะยาวและระยะสั้น

เมื่อสิ้นสุดการประชุมบทเรียนที่เรียนรู้ ต้องมีการแก้ไขบางอย่าง ไม่ว่าจะเป็นการแก้ไขปัญหาดิตติงการควบคุมการชดเชย (Compensating Controls) หรืออย่างน้อยก็ประเมินและยอมรับความเสี่ยงอย่างเป็นทางการ ต้องมีการเพิ่มข้อเสนอแนะสำหรับความพยายามในการแก้ไขในระยะยาวและระยะสั้นลงในแผนการจัดการความเสี่ยง (Treatment Plan) โดยรวม

ควรพิจารณาและรวมการปรับปรุงขั้นตอนการรับมือเหตุภัยคุกคามทางไซเบอร์เมื่อพบส่วนต่าง ๆ ที่สามารถปรับปรุงได้

	ชื่อเอกสาร	แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร		
	ระดับชั้นความลับ	ใช้ภายในสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น	เวอร์ชัน 1.0	หน้า 51

การแบ่งปันข้อมูลโดยสมัครใจควรเกิดขึ้นเมื่อใดก็ตามที่เป็นไปได้กับผู้มีส่วนได้ส่วนเสียภายนอก เพื่อให้เกิดการรับรู้ถึงสถานการณ์ความมั่นคงปลอดภัยทางไซเบอร์ในวงกว้าง ต้องปรึกษาฝ่ายกฎหมายและการจัดการก่อนที่จะทำเช่นนั้น หากไม่มีนโยบายและกระบวนการแบ่งปันข้อมูลอย่างเป็นทางการ

2.4.3 การวิเคราะห์ทางนิติวิทยาศาสตร์และการเก็บรักษาข้อมูล

ในกรณีที่มีอาชญากรรมทางกฎหมาย การวิเคราะห์ทางนิติวิทยาศาสตร์ (Forensic Analysis) จะเกิดขึ้นในลักษณะที่จะรักษาหลักฐานดิจิทัล (Preserve Digital Evidence) ที่สอดคล้องกับข้อกำหนดทางกฎหมายและกฎระเบียบที่เกี่ยวข้อง อาจจำเป็นต้องมีที่ปรึกษากฎหมายภายนอกและผู้เชี่ยวชาญด้านนิติวิทยาศาสตร์

พิจารณาสิ่งต่อไปนี้เมื่อตัดสินใจว่าจะเก็บหลักฐานที่เกี่ยวข้องกับเหตุการณ์หรือไม่และนานแค่ไหน:

- **การดำเนินคดี (Prosecution)** เป็นไปได้ไหมที่ผู้โจมตีจะถูกดำเนินคดี? หากเป็นเช่นนั้น อาจต้องเก็บหลักฐานไว้หลายปี
- **การเกิดซ้ำ (Reoccurrence)** พิจารณาว่าหลักฐานที่รวบรวมอาจเป็นประโยชน์ในกรณีที่ผู้โจมตีหรือการโจมตีที่คล้ายกันจะเกิดขึ้นในอนาคต
- **นโยบายการเก็บรักษาข้อมูล (Data Retention Policies)** พิจารณาเนื้อหาของหลักฐานที่เก็บไว้ เช่น การจับภาพระบบ (System Image Capture) เป็นต้น และนโยบายการเก็บรักษาเกี่ยวข้องกับข้อมูลนี้ เช่น นโยบายการเก็บรักษาอีเมล เป็นต้น
- **ต้นทุน (Cost)** ขึ้นอยู่กับชนิดและปริมาณของข้อมูลหรืออุปกรณ์ที่เก็บรักษาไว้เป็นหลักฐาน ต้นทุนอาจเป็นปัจจัยจำกัด

2.4.4 การตัดสินใจที่สำคัญสำหรับการออกจากขั้นตอนบทเรียนที่เรียนรู้

- ผู้บริหารพอใจที่เหตุภัยคุกคามทางไซเบอร์สิ้นสุด
 - ผู้จัดการ IR ทำการตัดสินใจสำหรับเหตุภัยคุกคามทางไซเบอร์ที่มีความรุนแรงจำกัด (Limited-severity Incidents)
 - CIO เป็นผู้ตัดสินใจสำหรับเหตุภัยคุกคามทางไซเบอร์ระดับร้ายแรงและระดับวิกฤต (Moderate and Critical-severity Incidents)
- มีแผนปฏิบัติการเพื่อตอบสนองต่อปัญหาการดำเนินงาน (Operational Issues) ที่เกิดขึ้นจากเหตุภัยคุกคามทางไซเบอร์นี้ ณ จุดนี้ ได้เวลากลับสู่ขั้นตอนที่ 1 การเตรียมการ

หมายเหตุ: หน่วยงานต้องพิจารณาดำเนินมาตรการตามรายละเอียดที่ระบุใน ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปรามปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. 2564

	ชื่อเอกสาร	แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร		
	ระดับชั้นความลับ	ใช้ภายในสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น	เวอร์ชัน 1.0	หน้า 52

3 การแจ้งเตือนและการสื่อสาร (Notification and Communication)

การแจ้งเตือนและการสื่อสารที่จำเป็นทั้งภายในและกับบุคคลที่สาม เช่น ลูกค้า ผู้ขาย สมกช. หน่วยงานบังคับใช้กฎหมาย เป็นต้น ตามข้อกำหนดทางกฎหมาย ระเบียบข้อบังคับ และสัญญาต้องดำเนินการในเวลาที่เหมาะสม

- ผู้บัญชาการรับมือเหตุภัยคุกคามทางไซเบอร์ต้องรายงานเหตุการณ์ต่อผู้บริหารระดับสูง
- ผู้บริหารระดับสูงต้องรายงานการละเมิดที่อาจเกิดขึ้นและ/หรือเหตุการณ์ที่เกี่ยวข้องกับข้อมูลลูกค้าไปยัง Incident Handling Team (IHT) ทันที
- IHT มีหน้าที่รับผิดชอบในการแจ้งที่เหมาะสมไปยัง:
 - บุคลากร
 - ลูกค้าและ/หรือคู่ค้าที่ได้รับผลกระทบ ภายในระยะเวลาที่กำหนดไว้ เช่น 24 หรือ 48 ชั่วโมง เป็นต้น ตาม SLA ตามการปฏิบัติตามกฎหมาย หรือกฎระเบียบที่เกี่ยวข้องแล้วแต่ระยะเวลาใดจะสั้นกว่า
 - เจ้าหน้าที่กฎหมายท้องถิ่น หรือรัฐบาลตามที่กำหนดโดยกฎเกณฑ์และ/หรือระเบียบข้อบังคับที่บังคับใช้

ขึ้นอยู่กับประเภทและขอบเขตของการละเมิด อาจพิจารณาใช้รายงานการละเมิดข้อมูลลูกค้า (Customer Data Breach Report) เพื่อแจ้งหน่วยงานธุรกิจที่ได้รับผลกระทบ

3.1 การปฏิสัมพันธ์กับการบังคับใช้กฎหมาย (InterAction with Law Enforcement)

การปฏิสัมพันธ์ระหว่างเจ้าหน้าที่บังคับใช้กฎหมายกับเจ้าหน้าที่บริการฉุกเฉิน (Emergency Services Personnel) ควรได้รับการประสานงานโดยผู้บัญชาการรับมือเหตุภัยคุกคามทางไซเบอร์

ผู้บัญชาการรับมือเหตุภัยคุกคามทางไซเบอร์จะจัดการการสื่อสารอย่างต่อเนื่อง (Ongoing Communication) กับเจ้าหน้าที่ อย่างไรก็ตาม ต้องสังเกตว่าลำดับความสำคัญของการบังคับใช้กฎหมายคือการดำเนินคดีกับผู้กระทำความผิดในท้ายที่สุด และไม่จำเป็นต้องทำให้บริษัทกลับสู่สถานะการทำงานปกติ ตรวจสอบให้แน่ใจว่ามีการปรึกษาหารือและให้คำแนะนำด้านกฎหมายก่อนและขณะสื่อสารกับหน่วยงานบังคับใช้กฎหมาย

3.2 หน่วยงานควบคุมหรือกำกับดูแล (Regulatory Authorities)

- หน่วยงานอยู่ภายใต้การกำกับดูแลด้านกฎระเบียบต่าง ๆ ขึ้นอยู่กับข้อมูลที่ได้รับผลกระทบ หากมีความเป็นไปได้ที่ข้อมูลที่ถูกควบคุมอาจถูกละเมิด อาจจำเป็นต้องแจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ตามที่กำหนดไว้ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หากหน่วยงานต้องปฏิบัติตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มาตรา 58 ในกรณีที่เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ต่อระบบสารสนเทศซึ่งอยู่ในความดูแลรับผิดชอบของหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศใดให้หน่วยงาน

	ชื่อเอกสาร แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร		
	ระดับชั้นความลับ ใช้ภายในสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น	เวอร์ชัน 1.0	หน้า 53

นั้นดำเนินการตรวจสอบข้อมูลที่เกี่ยวข้อง ข้อมูลคอมพิวเตอร์ และระบบคอมพิวเตอร์ของหน่วยงานนั้น รวมถึงพฤติการณ์แวดล้อมของตน เพื่อประเมินว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้นหรือไม่ หากผลการตรวจสอบปรากฏว่าเกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ขึ้น ให้ดำเนินการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานนั้น ต้องแจ้งต่อ สกมช. และหน่วยงานควบคุมหรือกำกับดูแล ทั้งนี้ขึ้นอยู่กับลักษณะของการละเมิด อาจจำเป็นต้องติดต่อหน่วยงานกำกับดูแลของรัฐบาลอื่น ๆ ของหน่วยงาน

- เฉพาะสมาชิกของ IHT เท่านั้นที่ได้รับอนุญาตให้หารือเกี่ยวกับลักษณะและ/หรือรายละเอียดของเหตุการณ์กับหน่วยงานควบคุมหรือกำกับดูแลใด ๆ
- IHT ควรติดต่อหน่วยงานควบคุมหรือกำกับดูแลโดยเร็วที่สุดเท่าที่เป็นไปได้

3.3 ผู้รับบริการ (Customers)

- ผู้รับบริการทุกคนที่ได้รับผลกระทบจากเหตุภัยคุกคามทางไซเบอร์จะต้องได้รับแจ้งตามที่ระบุไว้ในสัญญาที่เกี่ยวข้อง ข้อตกลงระดับการบริการ (Service Level Agreements: SLA) กฎเกณฑ์และ/หรือระเบียบข้อบังคับที่เกี่ยวข้อง
- การสื่อสารกับผู้รับบริการต้องสอดคล้องกัน โดยมีข้อมูลที่เหมือนกันหรือคล้ายกันที่ส่งถึงแต่ละบุคคล ข้อความที่ส่งถึงลูกค้าจะถูกสร้างขึ้นโดยสมาชิกของทีมสื่อสาร (Communications Team)
- ฝ่ายสื่อสารองค์กรจะสื่อสารกับลูกค้าตามข้อความที่ทีมสื่อสารจัดทำขึ้น

3.4 การจัดการสื่อสารสาธารณะ (Public Media Handling)

ข้อมูลทั้งหมดที่เกี่ยวข้องกับเหตุภัยคุกคามทางไซเบอร์จะถูกพิจารณาเป็นความลับ และไม่ควรมีการหารือข้อมูลใด ๆ กับบุคคลภายนอกของหน่วยงาน โดยไม่ได้รับการอนุมัติจากผู้บริหารระดับสูงและที่ปรึกษากฎหมายของหน่วยงาน

แถลงการณ์สาธารณะหรือสื่อต้องได้รับการจัดการอย่างระมัดระวังเพื่อให้แน่ใจว่าการสืบสวนสอบสวน/การดำเนินการทางกฎหมายใด ๆ จะไม่ตกอยู่ในอันตราย และลดความเสียหายต่อชื่อเสียงให้เหลือน้อยที่สุด การตัดสินใจเกี่ยวกับการเปิดเผยและวิธีการเปิดเผยข้อมูลเหตุภัยคุกคามทางไซเบอร์ของหน่วยงานจะกระทำโดยโฆษกที่ได้รับมอบหมายซึ่งได้รับมอบหมายจาก IHT เท่านั้น ซึ่งมีแนวโน้มว่ามาจากทีมสื่อสารหรือตัวแทนที่ได้รับการฝึกอบรมหรือสอนโดยทีมสื่อสาร

การสอบถามจากเอเจนซีสื่อต้องส่งตรงไปยังตัวแทน IHT ที่ได้รับมอบหมาย พนักงานที่พบว่ากำลังพูดคุยถึงเหตุภัยคุกคามทางไซเบอร์โดยไม่ได้รับอนุมัติจากผู้บริหารระดับสูง/ที่ปรึกษากฎหมาย จะถูกลงโทษทางวินัย สูงสุดและรวมถึงการเลิกจ้าง

	ชื่อเอกสาร แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร		
	ระดับชั้นความลับ ใช้ภายในสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น	เวอร์ชัน 1.0	หน้า 54

4 แผนการทดสอบและทบทวน (Plan Testing and Review)

แผนรับมือเหตุภัยคุกคามทางไซเบอร์ของหน่วยงาน และขั้นตอนต้องได้รับการทดสอบอย่างน้อยทุกปี ผู้บัญชาการ IR จะดำเนินการฝึกอบรมโดยใช้เหตุการณ์จำลองตามกำหนดเวลาเพื่อเป็นแนวทางและทดสอบขั้นตอน แผนและขั้นตอนจะต้องได้รับการอัปเดตเพื่อสะท้อนถึงบทเรียนที่ได้เรียนรู้และเพื่อรวมการพัฒนาอุตสาหกรรมใหม่ ๆ

สมาชิก CIRT, CIO และสมาชิกของ IHT ต้องเข้าร่วมในแบบฝึกหัดทดสอบอย่างน้อยปีละครั้ง

แผนรับมือเหตุภัยคุกคามทางไซเบอร์และขั้นตอนต่าง ๆ จะต้องได้รับการทบทวนทุกปี และมีการติดตามการอัปเดตในประวัติเวอร์ชัน (Version History) ของเอกสาร

การทบทวนแผนควรรวมถึง:

- ทบทวนเอกสารประกอบและแบบฟอร์มที่อยู่ในรายการเอกสารประกอบ (Supporting Document List) เพื่อให้แน่ใจว่าถูกต้องและมีประสิทธิภาพ
- ทบทวนภาคผนวกเพื่อให้แน่ใจว่าถูกต้องและมีประสิทธิภาพ
- ทบทวนแบบฟอร์มการรายงานเหตุภัยคุกคามทางไซเบอร์ (Incident Reporting Forms) ที่กรอกแล้วและแผนปฏิบัติการแก้ไข (Corrective Action Plans) สำหรับการปรับปรุงแผนและขั้นตอนที่แนะนำ
- เปรียบเทียบการเปลี่ยนแปลงล่าสุดกับโครงสร้างพื้นฐานของหน่วยงานและโครงสร้างการจัดการ (Organization's Infrastructure and Management Structure) กับแผนและขั้นตอนที่จัดทำเป็นเอกสาร

	ชื่อเอกสาร แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร		
	ระดับชั้นความลับ ใช้ภายในสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น	เวอร์ชัน 1.0	หน้า 55

5 รายละเอียดการซ้อมแผนบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยทางไซเบอร์

1. การเตรียมการ (Preparation)

- จัดตั้ง ทีมรับมือเหตุการณ์ภัยคุกคามทางไซเบอร์ (Cyber Incident Response Team - CIRT) ประกอบด้วยบุคลากรที่มีบทบาทสำคัญ ได้แก่ Information Security Manager, SOC Manager, และผู้เกี่ยวข้อง
- กำหนด แนวทางการสื่อสารและกระบวนการแจ้งเตือน ภายในองค์กร รวมถึงการประสานงานกับหน่วยงานภายนอกที่เกี่ยวข้อง
- ตรวจสอบและเตรียมความพร้อมของ เครื่องมือ และ ระบบรักษาความมั่นคงปลอดภัย อาทิ Firewall, IDS/IPS, และ SIEM
- จัด การฝึกอบรมบุคลากร เพื่อสร้างความเข้าใจในแผนการบริหารจัดการเหตุการณ์ และขั้นตอนการตอบสนองอย่างเหมาะสม

2. การตรวจจับและวิเคราะห์ (Detection and Analysis)

- ใช้ ระบบตรวจจับภัยคุกคาม (Intrusion Detection System - IDS) และการวิเคราะห์ Log Files เพื่อระบุเหตุการณ์ที่ผิดปกติ
- กำหนด เกณฑ์การแจ้งเตือนเหตุการณ์ เมื่อพบพฤติกรรมที่อาจเป็นภัยคุกคาม เช่น การเข้าถึงระบบโดยไม่ได้รับอนุญาต
- ดำเนินการ วิเคราะห์เหตุการณ์ เพื่อยืนยันลักษณะของภัยคุกคามและจัดหมวดหมู่ระดับความรุนแรงของเหตุการณ์

3. การตอบสนองและควบคุมสถานการณ์ (Response and Containment)

- ดำเนินการ ควบคุมสถานการณ์ (Containment) โดยแยกระบบหรือเครือข่ายที่ได้รับผลกระทบ เพื่อลดความเสียหาย
- ดำเนินการแก้ไขเหตุการณ์ ตามขั้นตอนที่กำหนดในแผน และจัดทำรายงานเหตุการณ์อย่างละเอียด
- ประสานงานกับ ทีมที่เกี่ยวข้อง เช่น ทีมกฎหมาย หรือหน่วยงานภายนอกที่มีบทบาทสำคัญ ในการจัดการปัญหา

	ชื่อเอกสาร แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร		
	ระดับชั้นความลับ ใช้ภายในสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น	เวอร์ชัน 1.0	หน้า 56

4. การกู้คืนและปรับปรุง (Recovery and Lessons Learned)

- ดำเนินการ **กู้คืนระบบและข้อมูล** ให้กลับเข้าสู่สถานการณ์ปกติอย่างปลอดภัย
- ตรวจสอบและแก้ไข **ช่องโหว่ในระบบ** ที่อาจเป็นต้นเหตุของเหตุการณ์
- ทบทวนและปรับปรุง **แผนบริหารจัดการเหตุการณ์** โดยอิงจากบทเรียนที่ได้จากการซ้อมแผน

ตัวอย่างรูปแบบการซ้อมแผน

1. การจำลองสถานการณ์ (Scenario Simulation)

- ใช้เหตุการณ์จำลอง เช่น การโจมตีด้วย Ransomware หรือการโจมตีแบบ DDoS
- ให้ทีม CIRT ดำเนินการตาม **ขั้นตอนที่ระบุในแผน** เพื่อประเมินประสิทธิภาพ

2. การวัดผลและการปรับปรุง

- ประเมินผลการดำเนินงานจาก **เวลาในการตอบสนอง** ความถูกต้องของการวิเคราะห์เหตุการณ์ และความรวดเร็วในการกู้คืนระบบ
- ใช้ **บทเรียนที่ได้จากการซ้อมแผน** ในการปรับปรุงกระบวนการทำงานและเพิ่มความพร้อมในการรับมือเหตุการณ์ในอนาคต

ประโยชน์ที่ได้รับจากการซ้อมแผน

- เพิ่มความพร้อมและความมั่นใจให้แก่บุคลากรในการรับมือเหตุการณ์ภัยคุกคาม
- ลดผลกระทบทางธุรกิจและเสริมสร้างความน่าเชื่อถือขององค์กร
- พัฒนา **กระบวนการและกลยุทธ์** ในการบริหารจัดการเหตุการณ์ที่เหมาะสมกับภัยคุกคามที่เปลี่ยนแปลง

การดำเนินการตามแนวทางนี้จะช่วยให้สำนักงานสามารถตอบสนองต่อภัยคุกคามได้อย่างมีประสิทธิภาพและรักษาความมั่นคงปลอดภัยของข้อมูลที่สำคัญต่อองค์กรและหน่วยงานที่เกี่ยวข้อง

	ชื่อเอกสาร แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร		
	ระดับชั้นความลับ ใช้ภายในสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น	เวอร์ชัน 1.0	หน้า 57

6 ภาคผนวกแผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร

6.1 ภาคผนวก 1 รายการกิจกรรมการบันทึก (Logging) การแจ้งเตือน (Alerting) และการเฝ้าระวัง (Monitoring)

กิจกรรมการบันทึก การแจ้งเตือน และการเฝ้าระวังอาจกำหนดเป้าหมายของระบบแต่ละระบบหรือกิจกรรมต่าง ๆ ในหลายระบบและแอปพลิเคชัน เก็บรายการการบันทึก การแจ้งเตือน และการเฝ้าระวังกิจกรรม และทบทวน (Review) รายการอย่างสม่ำเสมอเพื่อให้แน่ใจว่าฝ่ายเทคนิคสามารถรับมือเหตุการณ์ที่ผิดปกติได้อย่างรวดเร็ว หากหน่วยงานมีการจัดการทะเบียนทรัพย์สิน กิจกรรมเหล่านี้อาจถูกเพิ่มลงในรายการที่มีอยู่ดังตาราง

ชื่อระบบ/ แอปพลิเคชัน (System/ Application Name)	ระบบจัดเก็บล็อก (Logging System)	เหตุการณ์ที่ได้จัดเก็บไว้ (Events Logged)	เจ้าของระบบ (System Owner)	ความถี่ในการ เฝ้าระวัง (Monitoring frequency)	การแจ้งเตือน (Alerting)
ระบบเครื่องเสมือน (Virtual Machines:VM)	เก็บไว้ที่เว็บ เซิร์ฟเวอร์เอง (Local) HCI (Hyper- Converged Infrastructure)	รายละเอียดและวิธีเก็บ log ตาม พรบ.และประกาศที่เกี่ยวข้อง	เจ้าของ โครงการแต่ละ VM	รายวัน	Line Notification
ระบบร้องทุกข์	เก็บไว้ที่เว็บ เซิร์ฟเวอร์เอง (Local) HCI (Hyper- Converged Infrastructure)	รายละเอียดและวิธีเก็บ log ตาม พรบ.และประกาศที่เกี่ยวข้อง	ศูนย์เทคโนโลยี สารสนเทศ ที่ดินและ ทรัพยากรดิน	รายวัน	Line Notification

รูปที่ 6-1: รายการกิจกรรมการบันทึก (Logging) การแจ้งเตือน (Alerting) และการเฝ้าระวัง (Monitoring) จัดเตรียมโดย
(Prepared by): วันที่ปรับปรุง (Date updated):

รวมถึงสคทช. ได้ว่าจ้างให้บริษัท ไอเน็กซ์ บรอดแบนด์ จำกัด (iNEXT Broadband Co., Ltd.)
ให้บริการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Logs) สำหรับการเข้า-ออกอินเทอร์เน็ต

	ชื่อเอกสาร แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร		
	ระดับชั้นความลับ ใช้ภายในสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น	เวอร์ชัน 1.0	หน้า 58

ข้อมูลจราจรทางคอมพิวเตอร์ (Logs) ของเครื่องคอมพิวเตอร์และอุปกรณ์ภายใต้ HCI (Hyper-Converged Infrastructure) แต่ละผู้รับผิดชอบโครงการจะทำการเก็บ Logs เองภายใต้ระบบนั้น ๆ ทั้งนี้มีระยะเวลาจัดเก็บ Log แบบ On-line จะเก็บอย่างน้อย 90 วัน แต่ยังไม่ได้ระบุอายุการจัดเก็บและทำลาย

บริษัท ไอเน็กซ์ บรอดแบนด์ จำกัด จะทำการจัดเก็บสำรองข้อมูลระบบทั้งหมดที่อยู่ภายใต้ HCI (ในนี้มี Logs ของแต่ละระบบรวมอยู่ด้วยแล้ว) ด้วยการ Snapshot ไปที่ NAS เก็บที่ สคทช.

6.2 ภาคผนวก 2 การอ้างอิงการประเมินเหตุการณ์สองนาที (Two Minute Incident Assessment Reference)

ขั้นตอนที่ 1: ทำความเข้าใจผลกระทบ (Impact)/ผลกระทบที่อาจเกิดขึ้น (Potential Impact) และความเป็นไปได้ (Likelihood) หากไม่ใช่เหตุการณ์ที่เกิดขึ้น

- มูลค่าของทรัพย์สิน (Value of the Asset) คืออะไร? ถ้าไม่สำคัญ ทำไมต้องตอบสนอง?
- ประมาณจำนวนผลกระทบที่อาจเกิดขึ้นในกรณีที่เลวร้ายที่สุด (Potential Worst-case Impact)
- คาดการณ์ความเป็นไปเป็นไป (Estimate of Likelihood) ที่จะได้รับผลกระทบนี้

ขั้นตอนที่ 2: ระบุสาเหตุที่น่าสงสัย/ที่เป็นไปได้ของปัญหา

- ควรพิจารณาสถานการณ์ที่เป็นไปได้อย่างทั้งหมด
- กำหนดสิ่งที่สามารถพิสูจน์ได้ว่าไม่ถูกต้องอย่างรวดเร็ว
- แบ่งปันสถานการณ์ที่เป็นไปได้มากที่สุดเมื่อสื่อสาร

ขั้นตอนที่ 3: อธิบายกิจกรรมการแก้ไขที่แนะนำ (Remediation Activities)

- ปิดช่องโหว่ และลดผลกระทบเฉพาะหน้าอย่างไร?
- ดำเนินการขั้นตอนต่าง ๆ ที่อาจลดผลกระทบที่เกิดขึ้น
- พิจารณาเกี่ยวกับความเสียหายของชื่อเสียงและความคาดหวังทางกฎหมายด้วย

ขั้นตอนที่ 4: สื่อสารกับผู้บริหาร

- อธิบายปัญหาในระดับสูง (High Level) เกิดอะไรขึ้นและอย่างไร
- อธิบายความหมายในทางธุรกิจ เช่น การเงิน ชื่อเสียง ฯลฯ
- แบ่งปันการดำเนินการในขั้นตอนในระยะสั้น ๆ (Short-term Actions) ที่จำเป็นในการย้ายความเสี่ยงจากวิกฤต/สูงไปสู่ความเสี่ยงที่ยอมรับได้มากขึ้น

	ชื่อเอกสาร แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร		
	ระดับชั้นความลับ ใช้ภายในสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น	เวอร์ชัน 1.0	หน้า 59

การประเมินผลกระทบ/ผลกระทบที่อาจเกิดขึ้น และแนวทางการตอบสนอง

มูลค่าทรัพย์สิน (Value of the Asset) สูง (H)/กลาง (M)/ต่ำ (L)	ตัวอย่างมูลค่าทรัพย์สินระดับสูง เช่น อาจเข้าถึงฐานข้อมูลโคลเอ็นต์ได้อย่างเต็มที่เมื่อเทียบกับมูลค่าทรัพย์สินระดับต่ำ เช่น อาจเป็นเอกสารกระบวนการภายใน
ผลกระทบที่อาจเกิดขึ้น	การสูญเสียหรือจะเกิดผลกระทบอย่างไรหากเหตุการณ์เกิดขึ้นจริงและรุนแรงอย่างเต็มที่ พยายามหาปริมาณทั้งจำนวนเงิน และผลกระทบเช่นชื่อเสียงหรือความรับผิดชอบทางกฎหมาย
ความน่าจะเป็นของผลกระทบ	ความเสี่ยงในทันที (Immediate Risk) ที่ไม่น่าจะเป็นที่รู้จักในวงกว้างและมีความซับซ้อน เช่น การเข้าถึงทางอินเทอร์เน็ตโดยการหาประโยชน์จากช่องโหว่เล็ก ๆ น้อย ๆ ที่มีในหน่วยงานนั้น โดยต้องใช้ความเชี่ยวชาญที่ซับซ้อนและสถานการณ์เฉพาะเจาะจงเพื่อใช้ประโยชน์จากช่องโหว่นั้น
สาเหตุที่น่าสงสัย (ระบุสาเหตุที่เป็นไปได้ทั้งหมดที่ควรสืบสวนสอบสวน)	ข้อผิดพลาดในการกำหนดค่า (Configuration Error) การใช้ประโยชน์จากช่องโหว่จากระยะไกล อุปกรณ์ที่สูญหาย การปฏิเสธบริการโดยมีเป้าหมาย (Targeted Denial of Service) จากพรรคการเมืองหรือฝ่ายที่มีแรงจูงใจทางการเงิน เช่น การทำ DDOS เพื่อปิดกั้นการฉ้อโกง เป็นต้น
สาเหตุที่เป็นไปได้มากที่สุด	ทรัพยากรสารสนเทศเหล่านี้ ควรได้รับการติดตามอย่างรวดเร็วเพื่อพิสูจน์ว่าถูกต้องหรือไม่ถูกต้อง
แนวทางแก้ไขระยะสั้น (Short-term) ที่แนะนำ	ตัดการเชื่อมต่อหรือปิดอินเทอร์เน็ต (Turn Off Internet) นำเซิร์ฟเวอร์ออก (Remove) จากการเข้าถึงภายนอก ใช้แพตช์หรือการเปลี่ยนแปลง การกำหนดค่า (Configuration Change) สื่อสารปัญหากับพนักงานหรือลูกค้า ฯลฯ
การดำเนินการระยะยาว (Long-term Actions)	การเปลี่ยนแปลงในกระบวนการหรือสถาปัตยกรรม การได้มาซึ่งเครื่องมือหรือระบบ เพื่อลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ในระยะยาว

รูปที่ 6-2: การประเมินผลกระทบ/ผลกระทบที่อาจเกิดขึ้น และแนวทางการตอบสนอง

	ชื่อเอกสาร	แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร		
	ระดับชั้นความลับ	ใช้ภายในสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น	เวอร์ชัน 1.0	หน้า 60

แนวทางการสื่อสาร

การสื่อสาร	
อธิบายปัญหาแบบเข้าใจง่าย	อธิบายปัญหาในบริบททางธุรกิจหากเป็นไปได้ การใช้ตัวอย่าง (Examples) มีประโยชน์ในการอธิบายปัญหาในแง่การปฏิบัติงาน
อธิบายปัจจัย “แล้วยังไงต่อ (So What)”	ทำไมสิ่งนี้จึงสำคัญต่อธุรกิจของหน่วยงาน จะต้องเสียอะไรหากหน่วยงาน ไม่ลงมือทำ
แนะนำให้ดำเนินการทันที	เสนอคำตอบที่เฉพาะเจาะจงและเหตุผลที่หน่วยงานควรรับไว้ การดำเนินการดังกล่าวจะทำให้ธุรกิจได้รับผลกระทบหรือความรับผิดชอบ (Liability) ที่ลดลงอย่างไร อาจมีมากกว่าหนึ่งแนวทางที่เป็นไปได้ หากมีตัวเลือกที่เหมาะสมก็ควรนำเสนอเพื่อการตัดสินใจ
การแก้ไขอื่น ๆ ที่เสนอ	มีความเสี่ยงที่ตามมา (Follow-on Risks) ที่ต้องดำเนินการเพิ่มเติมหรือไม่? ตัวอย่าง เช่น กลยุทธ์การสื่อสาร กิจกรรมการตระหนักรู้ของผู้ใช้ (User Awareness) การเปลี่ยนแปลงกระบวนการ การปรับปรุงระบบ/เครื่องมือหรือการใช้งานซึ่งเป็นการดำเนินการระยะยาว

รูปที่ 6-3: แนวทางการสื่อสาร

6.3 ภาคผนวก 3 รายการตรวจสอบการตอบสนองเหตุการณ์ (Incident Response Checklist)

ลำดับที่	คำอธิบาย	หมายเหตุ
	ขั้นตอนการเตรียมการ (Preparation) โดยผู้บัญชาการ IR)	
1	จัดทำรายชื่อผู้ติดต่อและเผยแพร่ให้ผู้ที่เกี่ยวข้องทราบ	
	การตรวจจับ (Detection) โดยฝ่ายสนับสนุนด้านไอที (IT Support)	
2	กรอกรายละเอียดแบบฟอร์มการตอบสนองเหตุการณ์ (Incident Response Form)	
	การวิเคราะห์ (Analysis) โดย CIRT	
3	วิเคราะห์และประเมินเหตุภัยคุกคามทางไซเบอร์	
4	แจ้งผู้ที่เกี่ยวข้อง	

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

	ชื่อเอกสาร แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร		
	ระดับชั้นความลับ ใช้ภายในสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น	เวอร์ชัน 1.0	หน้า 61

ลำดับ ที่	คำอธิบาย	หมายเหตุ
	การจำกัดขอบเขต (Containment) โดย CIRT/Support	
5	ทำการสำรองข้อมูลระบบเพื่อรักษาสถานะปัจจุบันของระบบ	
6	เปลี่ยนรหัสผ่านในเครื่องสำหรับระบบที่ได้รับผลกระทบ	
	การกำจัด (Eradication) (CIRT/Support)	
7	อย่าใช้เครื่องมือการดูแลระบบ (System Administrative Tools) ให้ใช้ชุดเครื่องมือการดูแลระบบแยกต่างหาก (Separate Administrative Tool Sets) สำหรับการสืบสวนสอบสวน	
8	ติดตั้งระบบปฏิบัติการใหม่ทั้งหมด	
9	ทำให้ระบบปฏิบัติการแข็งแกร่งขึ้น (Harden the Operating System) เช่น ใช้แพตช์ ปิดบริการที่ไม่จำเป็น ติดตั้งซอฟต์แวร์ป้องกันไวรัส เป็นต้น	
	การกู้คืน (Recovery) (CIRT/Support)	
10	ตรวจสอบความถูกต้องว่าระบบได้รับการทำให้แข็งแกร่งแล้ว	
11	กู้คืนข้อมูลระบบด้วยการสำรองข้อมูลที่มั่นใจได้ว่าปลอดภัย (Clean Backup)	
12	พิจารณาระบบที่ได้รับผลกระทบภายใต้การเฝ้าระวังเครือข่ายสำหรับความพยายามที่ไม่ได้รับอนุญาตในอนาคต (Network Surveillance for Future Unauthorized Attempts)	
	ติดตามผล (Follow-up) โดยผู้บัญชาการ IR	
13	ทำการวิเคราะห์หลังเหตุการณ์บนระบบที่ได้รับผลกระทบเพื่อระบุพื้นที่เสี่ยงที่มีจุดอ่อนที่เป็นไปได้ (Potential Vulnerable Areas)	
14	ส่งรายงานการตอบสนองเหตุภัยคุกคามทางไซเบอร์สำหรับการทบทวนของฝ่ายบริหาร (Management Review)	
15	จัดเก็บเอกสารทั้งหมดเกี่ยวกับกระบวนการตอบสนองเหตุภัยคุกคามทางไซเบอร์เพื่อใช้อ้างอิงในอนาคต	

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

	ชื่อเอกสาร แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร		
	ระดับชั้นความลับ ใช้ภายในสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น	เวอร์ชัน 1.0	หน้า 62

รูปที่ 6-4: รายการตรวจสอบการตอบสนองเหตุการณ์ (Incident Response Checklist)

6.4 ภาคผนวก 4 ข้อกำหนดการแจ้งเตือน (Notification Requirements)

ตัวอย่างการระบุข้อกำหนดทั้งหมดที่ใช้กับหน่วยงาน

ข้อกำหนดหรือกฎหมายที่เกี่ยวข้อง	กลุ่มเป้าหมาย	กำหนดเวลาการแจ้งเตือน	หมายเหตุ
พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37(4)	สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล	โดยไม่ชักช้า ภายใน 72 ชั่วโมง นับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้	กรณีมีแนวโน้มว่ามีความเสี่ยงต่อเจ้าของข้อมูล
พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37(4)	เจ้าของข้อมูลที่ได้รับผลกระทบ	โดยไม่ชักช้า (แต่ไม่ได้ระบุเวลาไว้ หน่วยงานควรกำหนดระยะเวลาเองด้วย)	กรณีมีแนวโน้มว่ามีความเสี่ยงสูงต่อเจ้าของข้อมูล
พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มาตรา 58 ในกรณีที่เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ต่อระบบสารสนเทศซึ่งอยู่ในความดูแลรับผิดชอบของหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศใด ให้หน่วยงานนั้นดำเนินการตรวจสอบข้อมูลที่เกี่ยวข้องข้อมูลคอมพิวเตอร์ และระบบคอมพิวเตอร์ของหน่วยงาน รวมถึงพฤติกรรมแวดล้อมของตน เพื่อประเมินว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้นหรือไม่ หากผลการตรวจสอบปรากฏว่าเกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ขึ้น ให้ดำเนินการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ตามประมวลแนวทางปฏิบัติ และกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานนั้น	- สภมช. - หน่วยงานควบคุมหรือกำกับดูแล (กระทรวงพลังงาน)	โดยเร็ว (แต่ไม่ได้ระบุเวลาไว้ หน่วยงานควรกำหนดระยะเวลาเองด้วย)	

	ชื่อเอกสาร แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร		
	ระดับชั้นความลับ ใช้ภายในสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น	เวอร์ชัน 1.0	หน้า 63

ข้อกำหนดหรือกฎหมายที่เกี่ยวข้อง	กลุ่มเป้าหมาย	กำหนดเวลาการแจ้งเตือน	หมายเหตุ
อื่น ๆ โปรดระบุ			

รูปที่ 6-5: ตัวอย่างการระบุข้อกำหนดทั้งหมดที่ใช้กับหน่วยงาน

อ้างอิงตามภาคผนวก ท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปรามปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. 2564

ตัวอย่างกำหนดระยะเวลาในการแจ้งและรายงานภัยคุกคามทางไซเบอร์

หมวดหมู่ภัยคุกคามทางไซเบอร์	ระดับภัยคุกคามทางไซเบอร์	การแจ้งเบื้องต้นตามช่องทางที่กำหนด (ภายในเวลา)	การส่งรายงานให้หน่วยงานควบคุมหรือกำกับดูแล (ภายในเวลา)	การส่งรายงานให้สำนักงาน (ภายในเวลา)
1	ทุกเหตุการณ์	10 นาที	2 ชั่วโมง	4 ชั่วโมง
2	ทุกเหตุการณ์	ตามหน่วยงานกำหนด	ตามหน่วยงานกำหนด	ตามหน่วยงานกำหนด
3	ทุกเหตุการณ์	30 นาที	2 ชั่วโมง	8 ชั่วโมง
4	วิกฤต	10 นาที	30 ชั่วโมง	1 ชั่วโมง
	ร้ายแรง	20 นาที	1 ชั่วโมง	2 ชั่วโมง
	ไม่ร้ายแรง	ตามหน่วยงานกำหนด	ตามหน่วยงานกำหนด	ตามหน่วยงานกำหนด
5	วิกฤต	10 นาที	30 นาที	1 ชั่วโมง
	ร้ายแรง	20 นาที	1 ชั่วโมง	2 ชั่วโมง
	ไม่ร้ายแรง	30 นาที	2 ชั่วโมง	4 ชั่วโมง
6	วิกฤต	10 นาที	30 นาที	1 ชั่วโมง
	ร้ายแรง	20 นาที	1 ชั่วโมง	2 ชั่วโมง
	ไม่ร้ายแรง	30 นาที	2 ชั่วโมง	4 ชั่วโมง
7	วิกฤต	10 นาที	30 นาที	1 ชั่วโมง
	ร้ายแรง	10 นาที	1 ชั่วโมง	1 ชั่วโมง

	ชื่อเอกสาร แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร		
	ระดับชั้นความลับ ใช้ภายในสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น	เวอร์ชัน 1.0	หน้า 64

หมวดหมู่ภัยคุกคามทางไซเบอร์	ระดับภัยคุกคามทางไซเบอร์	การแจ้งเตือนต้นตอตามช่องทางที่กำหนด(ภายในเวลา)	การส่งรายงานให้หน่วยงานควบคุมหรือกำกับดูแล(ภายในเวลา)	การส่งรายงานให้สำนักงาน(ภายในเวลา)
	ไม่ร้ายแรง	ตามหน่วยงานกำหนด	ตามหน่วยงานกำหนด	ตามหน่วยงานกำหนด
8	-	20 นาที	ตามเวลาที่ต้องการใช้ในการสืบสวน	4 ชั่วโมง
9	-	-	4 ชั่วโมง	12 ชั่วโมง

รูปที่ 6-6: ตัวอย่างกำหนดระยะเวลาในการแจ้งและรายงานภัยคุกคามทางไซเบอร์

ตัวอย่างการกำหนดช่องทางสื่อสารและวิธีการเผยแพร่ข้อมูล

เหตุการณ์	กลุ่มเป้าหมาย	แพลตฟอร์ม/ช่องทางเผยแพร่	วิธีการเผยแพร่ข้อมูล	โฆษกหลักและผู้เชี่ยวชาญด้านเทคนิค
ระบบคอมพิวเตอร์หลักของหน่วยงานโดนโจมตีจนให้บริการไม่ได้	บุคลากรของหน่วยงาน ลูกค้า	ระบบสื่อสารภายใน สื่อสังคมออนไลน์ อีเมล SMS	- สื่อสารกับบุคลากรภายในหน่วยงาน เพื่อให้มีความเข้าใจ และช่วยกันบรรเทาปัญหาสื่อสารกับลูกค้า เพื่อสร้างความเข้าใจที่ถูกต้อง ป้องกันการตื่นตระหนก และรักษาภาพลักษณ์ ของหน่วยงาน	โฆษกหลัก: ภายใน -ศูนย์เทคโนโลยีสารสนเทศ ที่ดินและทรัพยากรดิน ภายนอก -กองกฎหมาย -ผู้อำนวยการสำนักงาน คณะกรรมการนโยบายที่ดิน แห่งชาติ ผู้เชี่ยวชาญด้านเทคนิค: -ศูนย์เทคโนโลยีสารสนเทศ ที่ดินและทรัพยากรดิน อ้างอิง ผู้ให้บริการภายนอก ในรายการ

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

	ชื่อเอกสาร แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร		
	ระดับชั้นความลับ ใช้ภายในสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น	เวอร์ชัน 1.0	หน้า 65

เหตุการณ์	กลุ่มเป้าหมาย	แพลตฟอร์ม/ ช่องทางการ เผยแพร่	วิธีการเผยแพร่ข้อมูล	โฆษกหลักและ ผู้เชี่ยวชาญด้านเทคนิค
ข้อมูลส่วนบุคคลในระบบถูกเจาะและนำไปเผยแพร่หรือขายหรือเรียกค่าไถ่ และเป็นที่รับรู้ของสาธารณะ	บุคลากรของหน่วยงาน ลูกค้า สาธารณชน	ระบบสื่อสารภายใน สื่อสังคมออนไลน์ อีเมล SMS สื่อมวลชน	แถลงข่าวโดย -กองกฎหมาย (Issue Management) -ผู้อำนวยการสำนักงาน คณะกรรมการนโยบายที่ดิน แห่งชาติ	โฆษกหลัก: ภายใน -ศูนย์เทคโนโลยีสารสนเทศ ที่ดินและทรัพยากรดิน ภายนอก -กองกฎหมาย -ผู้อำนวยการสำนักงาน คณะกรรมการนโยบายที่ดิน แห่งชาติ ผู้เชี่ยวชาญด้านเทคนิค: -ศูนย์เทคโนโลยีสารสนเทศ ที่ดินและทรัพยากรดิน อ้างอิง ผู้ให้บริการภายนอก ในรายการ

รูปที่ 6-7: ตัวอย่างการกำหนดช่องทางสื่อสารและวิธีการเผยแพร่ข้อมูล

	ชื่อเอกสาร	แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร		
	ระดับชั้นความลับ	ใช้ภายในสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น	เวอร์ชัน 1.0	หน้า 66

6.5 ภาคผนวก 5 แฉงการณข์ของสื่อ

ด้านล่างนี้คือตัวอย่างข้อความที่จะใช้หากสื่อมวลชนมีการสอบถามก่อนการแถลงข่าว (Press Release) การสื่อสารทั้งหมดกับสื่อมวลชนควรส่งตรงไปยังผู้บัญชาการการรับมือเหตุภัยคุกคามทางไซเบอร์ หรือตัวแทนอื่น ๆ ที่ได้รับมอบหมายจากผู้บริหารระดับสูง การรับทราบข้อเท็จจริงที่ถูกต้องเป็นสิ่งสำคัญ ห้ามให้ข้อมูลกับสื่อมวลชนก่อนยืนยันข้อเท็จจริงกับบุคลากรภายในและผู้บริหาร การเปลี่ยนแปลงข้อมูลหลังจากเผยแพร่อาจนำไปสู่ความสับสนของสื่อมวลชนและสูญเสียการโฟกัสข้อความสำคัญ

6.5.1 สคริปต์ที่เตรียมไว้ (Pre-scripted) การรับมือทันทีต่อการสอบถามของสื่อ

ใช้เทมเพลตนี้หากสื่อมวลชน “อยู่ที่หน้าประตูของหน่วยงาน” และหน่วยงานยังต้องการเวลาในการรวบรวมข้อเท็จจริงสำหรับคำแถลงการแถลงข่าวเบื้องต้น

การยอมรับข้อเท็จจริงเป็นสิ่งสำคัญ ดังนั้นเป็นสิ่งสำคัญที่ของหน่วยงานที่จะไม่กดดันให้ยืนยันหรือเปิดเผยข้อมูลก่อนที่จะได้รับการยืนยันข้อมูลที่ถูกต้อง

คำตอบต่อไปนี้ทำให้หน่วยงานมีเวลาที่จำเป็นในการรวบรวมข้อเท็จจริง

6.5.2 การตอบกลับแบบมีสคริปต์ล่วงหน้า (Pre-scripted Responses)

หากโทรศัพท์ออกสื่อ: หากผู้สื่อข่าวโทรศัพท์มาสอบถามเรื่องเหตุการณ์หรือข้อมูลที่เกี่ยวข้อง และหน่วยงานยังอยู่ระหว่างการรวบรวมข้อเท็จจริง คำตอบต้องมุ่งเน้นการควบคุมสถานการณ์และให้ข้อมูลพื้นฐานในขณะที่ปฏิเสธที่จะเปิดเผยข้อมูลที่ยังไม่ได้ได้รับการยืนยัน

สคริปต์ตัวอย่างสำหรับการตอบกลับ:

- การยืนยันการรับรู้เหตุการณ์:** “ขอบคุณสำหรับการติดต่อเข้ามา ทางเราทราบถึงสถานการณ์ที่เกิดขึ้นแล้ว และขณะนี้อยู่ระหว่างการตรวจสอบข้อมูลเพิ่มเติมเพื่อให้ได้ข้อเท็จจริงที่ถูกต้องที่สุดค่ะ/ครับ”
- การให้ข้อมูลพื้นฐาน:** “ในขณะนี้หน่วยงานของเราให้ความสำคัญสูงสุดกับการตรวจสอบข้อเท็จจริงและการแก้ไขสถานการณ์ เรามีทีมที่ทำงานอย่างใกล้ชิดเพื่อให้แน่ใจว่าทุกอย่างได้รับการดูแลอย่างรอบคอบ”
- การขอเวลาในการรวบรวมข้อมูล:** “ขอให้ท่านรอการแถลงข่าวอย่างเป็นทางการ ซึ่งเราจะแจ้งให้ทราบทันทีเมื่อเรารวบรวมข้อเท็จจริงทั้งหมดได้ครบถ้วนค่ะ/ครับ”
- การปฏิเสธคำถามเฉพาะเจาะจง:** “ขอภัยที่ไม่สามารถตอบคำถามเพิ่มเติมในขณะนี้ได้ เนื่องจากยังอยู่ระหว่างการตรวจสอบข้อมูล เราจะติดต่อกลับไปพร้อมข้อมูลที่ชัดเจนอีกครั้งค่ะ/ครับ”
- การเสนอช่องทางติดตามข่าวสาร:** “ท่านสามารถติดตามข่าวสารและแถลงการณ์เพิ่มเติมได้ผ่านทางเว็บไซต์หรือช่องทางโซเชียลมีเดียของหน่วยงานเราค่ะ/ครับ”

	ชื่อเอกสาร แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร		
	ระดับชั้นความลับ	ใช้ภายในสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น	เวอร์ชัน 1.0 หน้า 67

6.5.3 “หน่วยงานได้ทราบเกี่ยวกับ [สถานการณ์ (Situation) เหตุภัยคุกคามทางไซเบอร์ (Incident) เหตุการณ์ (Event)] และกำลังพยายามหาข้อมูลให้ครบถ้วนมากขึ้นในขณะนี้ เรา จะติดต่อคุณได้อย่างไรเมื่อมีข้อมูลเพิ่มเติม”

- “ความพยายามทั้งหมดของหน่วยงานมุ่งไปที่ [ทำให้สถานการณ์อยู่ภายใต้การควบคุม] เราจะไม่คาดเดาเกี่ยวกับ [สถานการณ์นี้] เราจะติดต่อคุณได้อย่างไรเมื่อมีข้อมูลเพิ่มเติม”
- “ฉันไม่ใช่ผู้มีอำนาจในเรื่องนี้ ให้ฉันได้ทราบ [ชื่อและข้อมูลการติดต่อกลับ] เราจะโทรหาคุณทันทีเมื่อมีข้อมูลเพิ่มเติม”
- “ตอนนี้หน่วยงานกำลังเตรียมแถลงการณ์ เราจะติดต่อกลับคุณภายใน [จำนวนนาที่หรือ ชั่วโมง] ได้ไหม”
- “คุณสามารถตรวจสอบเว็บไซต์ของหน่วยงานสำหรับข้อมูลพื้นฐาน และเราจะแฟกซ์/ อีเมลถึงคุณพร้อมกับการอัปเดตครั้งต่อไปของหน่วยงาน”

หากมาด้วยตนเองที่จุดเกิดเหตุภัยคุกคามทางไซเบอร์หรือหน่วยงานแถลงข่าว:

- นี่คือ [สถานการณ์ (Situation) เหตุภัยคุกคามทางไซเบอร์ (Incident) เหตุการณ์ (Event)] ที่กำลังดำเนินการอยู่ และเรารู้ว่าคุณต้องการข้อมูลให้ได้มากที่สุดขณะนี้ ในขณะที่เราพยายามหาคำตอบสำหรับคำถามของคุณ เราต้องการบอกคุณสิ่งที่หน่วยงานสามารถยืนยันได้ในตอนนี้:
- ในเวลาประมาณ [เวลา] [คำอธิบายสั้น ๆ ว่าเกิดอะไรขึ้น]
- ณ จุดนี้ เราไม่ทราบว่า [การสรุปผลจะดำเนินการนานแค่ไหน ลูกค้าได้รับผลกระทบกี่ ราย ฯลฯ]
- หน่วยงานมี [ระบบ, แผน, ขั้นตอน, การดำเนินงาน] ในสถานที่ ที่หน่วยงานกำลังได้รับความช่วยเหลือจาก [เจ้าหน้าที่ท้องถิ่น ผู้เชี่ยวชาญ ทีมกฎหมายของหน่วยงาน] ซึ่งเป็น ส่วนหนึ่งของแผนดังกล่าว
- สถานการณ์ [อยู่ภายใต้ ยังไม่อยู่ภายใต้] การควบคุม หน่วยงานกำลังทำงานร่วมกับ หน่วยงาน [ท้องถิ่น รัฐบาล] เพื่อ [แก้ไขสถานการณ์นี้ พิจารณาว่าสิ่งนี้เกิดขึ้นได้อย่างไร]
- หน่วยงานจะดำเนินการรวบรวมข้อมูลและเผยแพร่ให้คุณทราบโดยเร็วที่สุด เราจะติดต่อกลับภายใน [ระยะเวลาเป็นนาที่หรือ ชั่วโมง] เพื่อให้ข้อมูลอัปเดตแก่คุณ ทันทีที่หน่วยงาน ได้ยืนยันข้อมูลที่ได้รับ
- เราขอให้คุณอดทนรอในขณะที่หน่วยงานตอบสนองต่อ [สถานการณ์ (Situation) เหตุภัยคุกคามทางไซเบอร์ (Incident) เหตุการณ์ (Event)] นี้

6.5.4 เคล็ดลับการเขียนคำชี้แจง (Statement Writing Tips)

ข้อมูล/เคล็ดลับต่อไปนี้อาจใช้เพื่อสร้างคำแถลงสื่อที่ดีได้ ไม่จำเป็นต้องรวมทุกรายการ แต่โดยทั่วไปแล้วสองหรือสามรายการนี้จะรับรองได้ว่าเป็นคำชี้แจงที่มีประสิทธิภาพ

	ชื่อเอกสาร แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร		
	ระดับชั้นความลับ ใช้ภายในสำนักงานคณะกรรมการการนโยบายที่ดินแห่งชาติ เท่านั้น	เวอร์ชัน 1.0	หน้า 68

6.5.4.1 ความซื่อสัตย์ (Honesty)

ถ้าหน่วยงานเป็นฝ่ายผิด ยอมรับ หากพยายามที่จะเบี่ยงเบนความรับผิดชอบ นักข่าวและสาธารณชนจะให้อภัยน้อยลงเมื่อรายละเอียดเกี่ยวกับเหตุภัยคุกคามทางไซเบอร์ถูกเปิดเผยและถูกพบว่าหน่วยงานมีการปฏิบัติได้ไม่เพียงพอ แม้ในภาวะวิกฤติจริง ๆ ก็ยังสามารถได้รับความเคารพในการยอมรับข้อเท็จจริง

หากไม่ใช่ความผิดของหน่วยงาน ต้องทำให้ชัดเจนโดยไม่กล่าวโทษบุคคลหรือหน่วยงานอื่นอย่างเปิดเผย

- คำที่ใช้: รับผิดชอบ (Take or Share Responsibility) มุ่งมั่นในการเปิดกว้าง โปร่งใส
- คำที่ไม่ควรใช้: ตำหนิ (Blame) ความผิดพลาด (Fault)

6.5.4.2 บริบท (Context)

การนำเสนอเชิงลบในบริบทกว้าง ๆ สามารถช่วยลดผลกระทบของข่าวร้ายได้อย่างมาก

หากเรื่องราวเป็นเรื่องเกี่ยวกับผู้ใช้บริการที่มีประสบการณ์ไม่ดี หน่วยงานสามารถอ้างอิงถึงผู้ใช้บริการคนอื่น ๆ ที่มีประสบการณ์ที่ดีได้ นี่คือจุดที่ผู้สนับสนุนภายนอกมีประโยชน์ โดยเฉพาะผู้ใช้บริการรายอื่น

บริบทที่กว้างขึ้นยังหมายถึงการแยกเหตุภัยคุกคามทางไซเบอร์ออก เพียงแต่กรณีที่เราพบว่าเหตุการณ์เชิงลบนั้น “หายากมาก” / “ถูกแยกออก” และวางไว้ในกรอบที่กว้างขึ้นและเป็นบวกมากขึ้น

- คำที่ใช้: หายากมาก (Very Rare) แยกออกมา (Isolated)
- คำที่ไม่ควรใช้: ผิดพลาดบ่อย (Frequent Mistakes) ข้อผิดพลาดอื่น (Another Error)

6.5.4.3 การระบุขอบเขตของผลกระทบ (Framing Effect)

การระบุขอบเขตของผลกระทบเป็นรูปแบบหนึ่งของความลำเอียงทางปัญญา (Form of Cognitive Bias) ซึ่งทำให้ผู้คนชอบข้อความที่ฟังดูเป็นบวกมากกว่าคำพูดเชิงลบ แม้ว่าจะเป็นเรื่องเดียวกันก็ตาม ตัวอย่างเช่น เมื่อพูดถึงการผ่าตัดที่มีความเสี่ยง ผู้ป่วยจะมีแนวโน้มที่จะเข้ารับการผ่าตัดมากขึ้น เมื่อมีการอธิบายว่า “โอกาสรอดชีวิตหนึ่งเดือนหลังการผ่าตัดคือ 90%” เมื่อเทียบกับ “การเสียชีวิตภายในหนึ่งเดือนของการผ่าตัดคือ 10%” แม้ว่าข้อความทั้งสองจะมีความเสี่ยงเท่ากัน ฟังระว่างอคติทางปัญญารูปแบบนี้เมื่อพัฒนาและส่งข้อความสู่สาธารณะ

6.5.4.4 พันธมิตร (Partnership)

มีบางครั้ง que การเตือนผู้ฟังที่มีวิจารณญาณอย่างละเอียดจะเป็นประโยชน์ว่าหน่วยงานไม่ได้รับผิดชอบแต่ผู้เดียวสำหรับพฤติกรรมของบุคคลใดบุคคลหนึ่งโดยเฉพาะ สิ่งนี้สามารถบรรลุได้โดยไม่ปรากฏว่าหน่วยงานกำลัง “ยอมเสียเปรียบ” หรือละทิ้งความรับผิดชอบและไม่ทำให้ความสัมพันธ์กับพันธมิตรหลักอื่น ๆ ไม่พอใจ ตัวอย่างเช่น อาจกล่าวง่าย ๆ ว่า “ในฐานะหนึ่งในหลายหน่วยงานที่เกี่ยวข้องกับการสนับสนุนบุคคลที่เกี่ยวข้อง เรามุ่งมั่นที่จะให้บริการที่ดีที่สุดสำหรับผู้ให้บริการในพื้นที่”

	ชื่อเอกสาร แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร		
	ระดับชั้นความลับ ใช้ภายในสำนักงานคณะกรรมการการนโยบายที่ดินแห่งชาติ เท่านั้น	เวอร์ชัน 1.0	หน้า 69

- คำที่ใช้: การทำงานร่วมกัน (Working Together) ความรับผิดชอบร่วมกัน (Joint Responsibility) เป็นหนึ่งในหลายหน่วยงาน
- คำที่ไม่ควรใช้: X คือการตำหนิ (Blame) หน่วยงานไม่รู้ว่าคนอื่นคิดอย่างไรกับเรื่องนี้ แต่...

6.5.4.5 การดำเนินการ (Action)

แถลงการณ์ของสื่อไม่ควรพูดถึงปัญหาเพียงอย่างเดียว ควรเน้นการดำเนินการในส่วนของหน่วยงาน หน่วยงานจะไม่สามารถปรับปรุงสถานการณ์กับของสื่อใด ๆ หากหน่วยงานถูกมองว่าไม่ได้ตอบในกรณีของสถานการณ์เชิงลบหรือวิกฤตของสื่อ

คำเตือน: หลีกเลี่ยงการพูดว่าเราจะถือว่า “การสืบสวน/การสอบสวน” ในกรณีนี้ คำเหล่านี้เป็นพาดหัวข่าวสำหรับสื่อและอาจบ่งบอกถึงความรู้สึกมีความผิด

- คำที่ใช้: ดำเนินการทันที (Taking Immediate Action) ใช้มาตรการที่เหมาะสม ทำงานอย่างใกล้ชิดกับ
- คำที่ไม่ควรใช้: หน่วยงานกำลังทำการสืบสวนสอบสวน หน่วยงานจะพิจารณามัน

6.5.4.6 แง่บวก (Positives)

อย่ากลัวที่จะชี้ให้เห็นว่าหน่วยงานประสบความสำเร็จเพียงใดในแถลงการณ์ของสื่อ ข้อผิดพลาดเกิดขึ้นและเน้นย้ำสิ่งที่หน่วยงานได้ทำไปแล้วสามารถช่วยให้คนอื่นมองเห็นจุดบกพร่องเล็ก ๆ น้อย ๆ ในอดีตได้

- คำที่ใช้: เราได้เห็นผลลัพธ์ที่ดี เราประสบความสำเร็จ เราจะให้บริการที่ดีที่สุดต่อไป
- คำที่ไม่ควรใช้: มีหลายส่วนที่หน่วยงานต้องแก้ไข (เว้นแต่จะมาพร้อมกับข้อความเชิงบวก เช่น จะใช้มาตรการเพื่อเปลี่ยนแปลงสิ่งนี้)

6.5.4.7 ความเข้าอกเข้าใจ (Empathy)

เห็นได้ชัดว่าสถานการณ์สื่อเชิงลบสร้างช่องว่างระหว่างหน่วยงานกับสาธารณะที่เกี่ยวข้อง การแสดงความเห็นอกเห็นใจสามารถช่วยลดช่องว่างได้

- คำที่ใช้: เราเข้าใจ เราซาบซึ้ง เราารู้ เรารับรู้
- คำพูดที่ไม่ควรใช้: สิ่งเหล่านี้เกิดขึ้น ทุกคนต้องเผชิญกับปัญหาเหล่านี้

6.5.4.8 กระชับ (Be Concise)

นักข่าวมักไม่สนใจข้อความที่ยาวเหยียด พวกเขาอยากจะใช้ความพยายามในรายละเอียดของเหตุการณ์/เหตุภัยคุกคามทางไซเบอร์ นอกจากนี้ หากผู้พูดกับสื่อไม่คุ้นเคยกับการทำเช่นนั้น คำพูดที่ยาวอาจส่งผลให้ผู้พูดทำผิด

ตามกฎหมายแล้ว ข้อความสำหรับสื่อสิ่งพิมพ์ไม่ควรยาวเกินสองย่อหน้า – หนึ่งประโยคแน่นต่อย่อหน้า

	ชื่อเอกสาร แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร		
	ระดับชั้นความลับ ใช้ภายในสำนักงานคณะกรรมการการนโยบายที่ดินแห่งชาติ เท่านั้น	เวอร์ชัน 1.0	หน้า 70

สื่อออกอากาศอาจทำให้หน่วยงานมีพื้นที่มากขึ้น แต่ควรคำนึงถึงความยาว เนื่องจากผู้ผลิต/บรรณาธิการอาจต้องการจัดทำคำแถลงของหน่วยงานในแบบที่สั้นลงเพื่อส่งไปยังกระดานข่าวในภายหลัง

6.5.4.9 ข้อความควรหลีกเลี่ยง (Statements Should Avoid)

- **การเผชิญหน้า (Confrontation)** วัตถุประสงค์ของคำแถลงของสื่อในภาวะวิกฤตคือเพื่อคลี่คลายสถานการณ์ ไม่ทำให้สถานการณ์แย่ลง หลีกเลี่ยงการกล่าวโทษ/โยนความผิดเพราะจะส่งผลให้เกิดการโต้เถียงกันตามสื่อระหว่างฝ่ายตรงข้าม จำไว้ว่านักข่าวชอบเรื่องราวการเผชิญหน้า เช่น พวกเขาติดตามไม่ใช่ความผิดของหน่วยงาน
- **ความคลุมเครือ (Ambiguity)** ข้อความที่ไม่ชัดเจนและคลุมเครือไม่ช่วยในการจัดการกับสถานการณ์ของสื่อเชิงลบ และอาจเปิดโอกาสให้นักข่าวตีความคำตอบใหม่ จงเข้มแข็งและชัดเจนตลอดเวลาใช้คำพูดเชิงบวกที่แข็งแกร่งเช่น “หน่วยงานมุ่งมั่นที่จะ X และจะไม่ยอมให้ Y” ตรวจสอบให้แน่ใจว่าข้อความของหน่วยงานมีความชัดเจนอย่างสมบูรณ์
- **คำสรรพนามส่วนบุคคล (Personal Pronouns)** พยายามหลีกเลี่ยงการอ้างถึงหน่วยงาน โดยใช้ชื่อในคำแถลงของสื่อ เนื่องจากการทำเช่นนี้อาจช่วยเสริมความเชื่อมโยงระหว่างหน่วยงานกับประเด็นเชิงลบที่เกี่ยวข้อง สามารถใช้พหูพจน์แรก เช่น เรา พวกเรา เป็นต้น สิ่งนี้ยังมีข้อได้เปรียบในการเพิ่มความรู้สึกส่วนตัวเล็กน้อยและให้ความรู้สึกเป็นข้าราชการน้อยลงในแถลงการณ์

	ชื่อเอกสาร	แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร	
	ระดับชั้นความลับ	ใช้ภายในสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น	เวอร์ชัน 1.0 หน้า 71

6.6 ภาคผนวก 6 เทมเพลตจดหมายผู้รับบริการ (Customer Letter Template)

6.6.1 เทมเพลตอีเมลและ/หรือจดหมายอย่างเป็นทางการ (Formal Email and/or Letter Template)

เรียน ผู้รับบริการ

อย่างที่ท่านอาจทราบ เครือข่ายคอมพิวเตอร์ในสำนักงานบางแห่งของเราถูกบุกรุกที่อาจส่งผลให้มีการขโมยชื่อ-นามสกุล ข้อมูลการติดต่อ ข้อมูลการถือครองกรรมสิทธิ์ และข้อมูลอื่น ๆ เราอยู่ระหว่างตรวจสอบข้อมูลสมาชิกที่ผู้บุกรุกอาจเข้าถึง แต่ขณะนี้ยังไม่มีหลักฐานของการใช้ข้อมูลดังกล่าวในทางที่ผิด

เราจัดทำประกาศนี้ด้วยความระมัดระวังอย่างยิ่งต่อผู้ใช้บริการทุกคนที่ให้ข้อมูลติดต่อของท่านกับหน่วยงานของเราไม่ได้รับผลกระทบที่ร้ายแรง โดยเราประเมินว่าระบบที่อาจได้รับผลกระทบถูกบุกรุกในช่วงระยะเวลา <ระบุวันที่เริ่ม> ถึง <ระบุวันที่สิ้นสุด>

เมื่อทราบการบุกรุกแล้ว เราได้ดำเนินการทันทีเพื่อรักษาความมั่นคงปลอดภัยเครือข่ายส่วนที่ได้รับผลกระทบ โดยได้รับการสนับสนุนจากผู้เชี่ยวชาญด้านนิติวิทยาศาสตร์ดำเนินการสืบสวนข้อเท็จจริงและขอบเขตของภัยคุกคามทางไซเบอร์นี้ ขอให้ท่านเชื่อมั่นว่าการบุกรุกดังกล่าวอยู่ภายใต้การควบคุม และปัจจุบันยังไม่ปรากฏหลักฐานว่ามีข้อมูลอื่นใดถูกขโมยนอกเหนือจากที่กล่าวข้างต้น อย่างไรก็ตาม เราจะแจ้งให้ทราบโดยเร็วหากมีความคืบหน้าเพิ่มเติมจากการสืบสวนที่ดำเนินอยู่

เราได้แจ้งเหตุต่อหน่วยงานรัฐบาลและให้ความร่วมมือตามกฎหมายเพื่อนำไปสู่การพิสูจน์ทราบบุคคลที่อยู่เบื้องหลัง แกล้งข่าวและจดหมายฉบับนี้เป็นการปฏิบัติตามที่กฎหมายกำหนดให้แจ้งผู้มีส่วนเกี่ยวข้องทราบข้อเท็จจริงโดยเร็วที่สุด

ทั้งนี้ หน่วยงานได้จัดตั้งศูนย์บริการทางโทรศัพท์ขึ้นเพื่อตอบข้อซักถามจากผู้ให้บริการเกี่ยวกับเหตุการณ์บุกรุก และการให้บริการปกป้องความปลอดภัยข้อมูลส่วนบุคคล โดยจะมีเจ้าหน้าที่ประจำการวันจันทร์ถึงวันศุกร์ ระหว่างเวลา 08.00 น. - 16.00 น.

ต้องขอภัยในความไม่สะดวกที่อาจเกิดขึ้น หน่วยงานของเราจะปรับปรุงแก้ไขจุดอ่อนด้านความปลอดภัยของระบบ เพื่อไม่ให้เกิดเหตุการณ์ลักษณะนี้ขึ้นอีกในอนาคต

ขอแสดงความนับถือ,

<ข้อควรพิจารณาอื่น ๆ ขึ้นอยู่กับลักษณะของเหตุการณ์>

	ชื่อเอกสาร แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร		
	ระดับชั้นความลับ ใช้ภายในสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น	เวอร์ชัน 1.0	หน้า 72

6.7 ภาคผนวก 7 หน่วยงานเกี่ยวข้องกับการตอบสนองเหตุภัยคุกคามทางไซเบอร์ (Incident Response Organizations)

รายชื่อหน่วยงานที่เกี่ยวข้องกับการตอบสนองเหตุภัยคุกคามทางไซเบอร์ที่อาจเป็นประโยชน์ในการวางแผนหรือตอบสนองต่อเหตุการณ์:

หน่วยงาน	URL
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ	https://www.ncsa.or.th/ncsc.html
Anti-Phishing Working Group (APWG)	https://www.antiphishing.org/
Computer Crime and Intellectual Property Section (CCIPS), US Department of Justice	https://www.justice.gov/criminal-ccips
CERT Coordination Center	https://www.sei.cmu.edu/about/divisions/cert/index.cfm
European Network and Information Security Agency (ENISA)	https://www.enisa.europa.eu/
Government Forum of Incident Response and Security Teams (GFIRST)	https://www.us-cert.gov/government-Users/collaboration/gfirst
High Technology Crime Investigation Association (HTCIA)	https://htcia.org/
InfraGard	https://www.infragard.org/
Internet Storm Center (ISC)	https://isc.sans.edu/
National Council of ISACs	https://www.nationalisacs.org/
United States Computer Emergency Response Team (US-CERT)	https://www.us-cert.gov/

รูปที่ 6-8: หน่วยงานเกี่ยวข้องกับการตอบสนองเหตุภัยคุกคามทางไซเบอร์

	ชื่อเอกสาร แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร		
	ระดับชั้นความลับ ใช้นายในสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น	เวอร์ชัน 1.0	หน้า 73

6.8 ภาคผนวก 8 กลยุทธ์การจำกัดขอบเขต (Containment Strategies)

กลยุทธ์การจำกัดขอบเขตต่อไปนี้จะได้รับการกำหนดเพื่อช่วยในการรับมือเหตุการณ์ภัยคุกคามทางไซเบอร์ หากไม่มีกลยุทธ์การจำกัดขอบเขตที่สรุปไว้ด้านล่างที่เหมาะสมกับสถานการณ์ปัจจุบัน ให้อ้างอิงกับขั้นตอนที่ 3.1 การจำกัดขอบเขตทั่วไป (Containment)

6.8.1 ข้อมูลประจำตัวที่ถูกลักขโมย (Stolen Credentials)

6.8.1.1 การจำกัดขอบเขต (Containment)

การลดผลกระทบ:

- เปลี่ยนรหัสผ่านหรือปิดการใช้งานบัญชีที่ได้รับผลกระทบ
- หากบัญชีที่ถูกบุกรุกมีสิทธิการเข้าถึงของผู้ดูแลระบบ (Administrator Access) ทบทวนบันทึกกิจกรรม (Review Activity Logs) สำหรับบัญชีเพิ่มเติมที่อาจสร้างขึ้น ปิดการใช้งานบัญชีใด ๆ ที่สร้างโดยผู้โจมตี

แจ้งผู้ที่เกี่ยวข้อง:

- แจ้งผู้ใช้ที่รับผิดชอบบัญชีที่ได้รับผลกระทบ
- การสืบสวนสอบสวน:
- พยายามระบุวันที่และเวลาที่บัญชีถูกบุกรุก
- ทบทวนกิจกรรมทั้งหมดที่เกิดขึ้นแล้วโดยบัญชีที่ถูกบุกรุกในช่วงระยะเวลาของการโจมตี หากไม่มีบันทึกกิจกรรม (Logs) ให้ตรวจสอบการกำหนดค่าทั้งหมด (All Configurations) ที่บัญชีนั้นมีสิทธิ์เข้าถึงเพื่อแก้ไข เช่น สำหรับบัญชีอีเมลที่ถูกบุกรุก ให้ตรวจสอบกฎการส่งต่อ (Forwarding Rules) ที่เพิ่มหรือเปลี่ยนแปลง เป็นต้น

6.8.1.2 การกำจัดและการกู้คืน (Eradication and Recovery)

- ย้อนกลับการเปลี่ยนแปลง (Reverse Changes) ที่ทำโดยบัญชีที่ถูกบุกรุกในช่วงเวลาของการโจมตี

6.8.2 แรนซัมแวร์ (Ransomware)

6.8.2.1 การจำกัดขอบเขต (Containment)

- 1) บล็อกการเข้าถึงเซิร์ฟเวอร์คำสั่งและการควบคุม (Command and Control: C2)
- 2) ตั้งค่าการแชร์ไฟล์เป็นโหมดอ่านอย่างเดียว (Read-only Mode)
- 3) ตรวจสอบความเป็นเจ้าของไฟล์ที่ถูกเข้ารหัส (Encrypted Files) เพื่อระบุผู้ใช้ที่ติดไวรัส
- 4) เรียกคืน (Recall) อีเมลฟิชชิงที่รู้จักจากกล่องจดหมายของผู้ใช้
- 5) ออฟไลน์ระบบที่ติดมัลแวร์

	ชื่อเอกสาร	แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร		
	ระดับชั้นความลับ	ใช้ภายในสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น	เวอร์ชัน 1.0	หน้า 74

6.8.2.2 การกำจัดและการกู้คืน (Eradication and Recovery)

- 1) แพตช์แอปพลิเคชันบุคคลที่สามโดยเร็วที่สุด
- 2) ทดสอบและตรวจสอบความถูกต้องของกระบวนการสำรองข้อมูล
- 3) ปรับใช้ GPO เพื่อบล็อกไฟล์เรียกทำงานและปิดใช้งานมาโคร
- 4) บล็อกไฟล์แนบอีเมลตามลายเซ็นไฟล์ (File Signature) และ/หรือนามสกุล
- 5) ลบสิทธิ์ของผู้ดูแลระบบบนเครื่องหรือบนระบบนั้น (Local Administrative Rights)

6.8.3 การระบาดของไวรัส (Virus Outbreak)

6.8.3.1 การจำกัดขอบเขต (Containment)

- 1) อัปเดตซอฟต์แวร์ป้องกันไวรัส
 - ก. รับลายเซ็นการตรวจจับ (Detection Signature) และคำอธิบายทางเทคนิคสำหรับไวรัสจากผู้จำหน่าย Antivirus (AV)
 - ข. ทดสอบการอัปเดตลายเซ็นการตรวจจับในสภาพแวดล้อมการทดสอบ
 - ค. กระจายการแก้ไขสู่สิ่งแวดล้อมจริง (Distribute Fix to Environment)
- 2) ส่งไฟล์ตัวอย่างไปยังผู้จำหน่าย AV หากลายเซ็นไวรัสล่าสุดตรวจไม่พบการติดไวรัส

6.8.3.2 การกำจัดและการกู้คืน (Eradication and Recovery)

- 1) กำจัดไวรัส ถ้าจำเป็น
 - ก. จำกัดขอบเขตของไวรัส/การโจมตี โดยขึ้นอยู่กับไวรัสซึ่งอาจรวมถึงการแบ่งพาร์ติชันเครือข่าย การปิดใช้งานอีเมล SMTP (Disabling SMTP Email) การเปลี่ยนการกรองเนื้อหา (Content Filtering) เพื่อบล็อกไฟล์แนบหรือสตรีมข้อความเฉพาะ การลบเวิร์กสเตชันออกจากเครือข่าย ฯลฯ
 - ข. ระบุระบบที่ติดไวรัส (Infected Systems)
- 2) การชำระล้างสภาพแวดล้อม (Environment Cleanup):
 - ก. รับลายเซ็นการตรวจจับและเครื่องมือแก้ไขที่จำเป็นสำหรับไวรัสจากผู้จำหน่ายโปรแกรมป้องกันไวรัสของหน่วยงาน
 - ข. ทดสอบการแก้ไขที่ผู้ขายของหน่วยงานจัดหาให้สำหรับไวรัสในสภาพแวดล้อมทดสอบของหน่วยงาน (Virus Signatures Staging Lab) ซึ่งอาจรวมถึงเครื่องมือซ่อมแซม (Repair Tools) แยกต่างหากที่หน่วยงานต้องเรียกใช้ก่อนที่จะใช้ลายเซ็นไวรัสที่อัปเดต
 - ค. พัฒนาวิธีการปรับใช้สำหรับกระบวนการแก้ไข (Fix Process)
 - ง. สร้างแผนการชำระล้าง (Cleanup Plan) และตรวจสอบความถูกต้องกับทีมที่ได้รับผลกระทบทั้งหมดและผู้จำหน่ายโปรแกรมป้องกันไวรัสของหน่วยงาน

	ชื่อเอกสาร แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร		
	ระดับชั้นความลับ ใช้งานในสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น	เวอร์ชัน 1.0	หน้า 75

จ. ทำการชำระล้างขอบเขตและเซิร์ฟเวอร์อีเมลที่ติดไวรัสทั้งหมด (Clean all Infected Perimeter and Email Servers) และอัปเดตลายเซ็นไวรัสของซอฟต์แวร์ป้องกันไวรัสซึ่งให้การป้องกันช่องทางการติดไวรัสเหล่านี้

ฉ. แจกจ่ายโปรแกรมแก้ไขไปยังเวิร์กสเตชันและเซิร์ฟเวอร์ทั้งหมดในสภาพแวดล้อมของหน่วยงาน โดยใช้วิธีการใดก็ตามที่มีเพื่อการปรับใช้อย่างรวดเร็ว

ช. แยก (Isolate) ระบบที่ติดไวรัสและต้องการการซ่อมแซมออก

ซ. เรียกใช้เครื่องมือแก้ไขที่จำเป็นทั้งหมดบนระบบที่ติดไวรัสทั้งหมด เพื่อลบไวรัสออกจากหน่วยความจำหรือปิดใช้งาน

ฌ. สแกนระบบทั้งหมดด้วยลายเซ็นไวรัสที่อัปเดตเพื่อลบไฟล์ที่ติดไวรัสทั้งหมด

ญ. กำจัดไฟล์ชั่วคราวและไฟล์ที่น่าสงสัยทั้งหมด รวมถึงไดเรกทอรีและไฟล์ที่ซ่อนอยู่

ฎ. ลบหรือแก้ไขข้อมูลการกำหนดค่าที่ใช้สำหรับการทำงานของไวรัสหรือที่อาจอนุญาตให้ไวรัสปรากฏขึ้นอีกครั้ง

ฏ. ลบข้อมูลการกำหนดค่าที่อาจทำให้ระบบล้มเหลว

ฐ. ค้นหาพาร์ติชันที่ติดตั้งใหม่ที่สร้างโดยไวรัสและกำจัดออก

ฑ. ค้นหาพาร์ติชันการบันทึก (Log Partitions) ที่หายไปและกู้คืน

ฒ. ค้นหาบัญชีผู้ใช้ที่เพิ่มหรือเปลี่ยนแปลง แล้วลบหรือกู้คืน

ณ. กู้คืนไฟล์ที่เปลี่ยนแปลงหรือถูกลบ

ด. แจกจ่ายการอัปเดตแพตช์ไปยังทุกระบบและอัปเดตระดับการแพตช์ (Update Patch Levels)

6.9 ภาคผนวก 9 ข้อตกลงการประกันภัยทางไซเบอร์และการบริการบุคคลที่สาม (Cyber Insurance and Third-Party Service Agreements)

ในกรณีที่เกี่ยวข้องกับการประกันภัยทางไซเบอร์หรือบริการจากบุคคลภายนอก การมีความเข้าใจที่ชัดเจนเกี่ยวกับบริการรับมือและตรวจจับเหตุภัยคุกคามทางไซเบอร์ (Incident Response and Detection Services) เป็นสิ่งสำคัญ ตัวอย่างเช่น ผู้ให้บริการประกันภัยทางไซเบอร์จำนวนมากต้องการให้หน่วยงานที่ดูแลดำเนินการตามกระบวนการที่กำหนดไว้ล่วงหน้า เป็นต้น ตัวอย่างของผู้ให้บริการบุคคลที่สามที่อาจเกี่ยวข้องกับกิจกรรม IR ได้แก่ ผู้ให้บริการประกันภัย ผู้ให้บริการอินเทอร์เน็ต (Internet Service Provider: ISP) ผู้ให้บริการระบบคลาวด์ (Cloud Service Provider: CSP) ผู้จำหน่ายซอฟต์แวร์ หรือผู้ให้บริการหลายบริการ (Multiservice Provider: MSP) เป็นต้น

CIO มีหน้าที่ตรวจสอบ SLA ทั้งหมดกับผู้ให้บริการเพื่อให้แน่ใจว่ามีการกำหนดความรับผิดชอบและความคาดหวังที่เกี่ยวข้องกับการรับมือเหตุภัยคุกคามทางไซเบอร์

	ชื่อเอกสาร แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร		
	ระดับชั้นความลับ ใช้อยู่ในสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น	เวอร์ชัน 1.0	หน้า 76

ผู้บัญชาการ IR มีหน้าที่รับผิดชอบในการทำความเข้าใจ SLA กับผู้ให้บริการและรู้ว่าเมื่อใดที่ทีมควรมีส่วนร่วมกับผู้ให้บริการ

การสนับสนุนและการตอบสนองของบุคคลที่สาม สคทช. ได้ว่าจ้างให้บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) ให้บริการเฝ้าระวังภัยคุกคาม วิเคราะห์ความเกี่ยวข้องของเหตุการณ์ ภัยคุกคามด้านความปลอดภัยสารสนเทศ (IT Security Monitoring Services) และเหตุการณ์ผิดปกติทางด้านการบริหารจัดการระบบคอมพิวเตอร์และระบบเครือข่ายสื่อสารและอินเทอร์เน็ต จากข้อมูลจราจรทางคอมพิวเตอร์ (Log) ของอุปกรณ์ต่าง ๆ ของ สคทช. โดยต้องมีการวิเคราะห์แบบรวมศูนย์และเงื่อนไขการโจมตี (Correlation and Use case) เพื่อช่วยในการเฝ้าระวังและแจ้งเตือนภัยคุกคาม ที่เกี่ยวข้องทุกวันตลอด 24 ชั่วโมง ต่อวัน 7 วัน ต่อสัปดาห์ (24/7) และดำเนินการแจ้งเตือนเมื่อเกิดเหตุการณ์ภัยคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อสารตาม Service Level Agreement (SLA) ที่กำหนด รวมทั้ง ให้คำแนะนำด้านเทคนิคในการแก้ไขเหตุการณ์ภัยคุกคามดังกล่าวแก่สคทช. ตลอดระยะเวลาสัญญา

ตามสัญญากับบริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) จะต้องให้บริการเฝ้าระวังภัยคุกคาม วิเคราะห์ความเกี่ยวข้องของเหตุการณ์ ภัยคุกคามด้านความปลอดภัยสารสนเทศ (IT Security Monitoring Services) และเหตุการณ์ผิดปกติทางด้านการบริหารจัดการระบบคอมพิวเตอร์และระบบเครือข่ายสื่อสารและอินเทอร์เน็ต จากข้อมูลจราจรทางคอมพิวเตอร์ (Log) ของอุปกรณ์ต่าง ๆ ของ สคทช. โดยต้องมีการวิเคราะห์แบบรวมศูนย์และเงื่อนไขการโจมตี (Correlation and Usecase) เพื่อช่วยในการเฝ้าระวังและแจ้งเตือนภัยคุกคาม ที่เกี่ยวข้องทุกวันตลอด 24 ชั่วโมง ต่อวัน 7 วัน ต่อสัปดาห์ (24/7) และดำเนินการแจ้งเตือนเมื่อเกิดเหตุการณ์ภัยคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อสารตาม Service Level Agreement (SLA) ที่กำหนด รวมทั้ง ให้คำแนะนำด้านเทคนิคในการแก้ไขเหตุการณ์ภัยคุกคามดังกล่าวแก่สคทช. ตลอดระยะเวลาสัญญา โดย สคทช. กำหนดเกณฑ์ Service Level Agreement เบื้องต้น โดยต้องมีการแจ้งเตือนภายหลังการตรวจพบและวิเคราะห์เหตุ ภายในระยะเวลาอย่างน้อย ดังนี้

ระดับความรุนแรง (Severity)	Incident Notification
Critical	15 นาที
Non-Critical	30 นาที

รูปที่ 6-9: เกณฑ์ Service Level Agreement

นอกจากนี้ การสนับสนุนและการตอบสนองของบุคคลที่สาม สคทช. ยังได้ว่าจ้างให้บริษัท ไอเน็กซ์ บรอดแบนด์ จำกัด หากเกิดสถานการณ์ฉุกเฉินขึ้นกับระบบเทคโนโลยีสารสนเทศ ดังนี้

	ชื่อเอกสาร แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร		
	ระดับชั้นความลับ ใช้ภายในสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น	เวอร์ชัน 1.0	หน้า 77

การสนับสนุนและการตอบสนองของบุคคลที่สาม

ผู้ให้บริการ (Service Provider)	แอปพลิเคชัน/บริการ (Applications/Services)	เมื่อไหร่จะติดต่อ (When to contact)	ระดับการบริการ/เวลาตอบสนอง (Service Level/ Response Time)
บริษัท ไอเน็กซ์ บรอดแบนด์ จำกัด (iNEXT Broadband Co., Ltd.)	- อินเทอร์เน็ต - ดูแลอุปกรณ์	หากเกิดสถานการณ์ฉุกเฉินขึ้นกับระบบเทคโนโลยีสารสนเทศ	ภายใน 12 ชั่วโมง

รูปที่ 6-10: การสนับสนุนและการตอบสนองของบุคคลที่สาม

ความคุ้มครองประกันภัยและข้อมูลการติดต่อ

ผู้ให้บริการประกันภัย (Insurance Provider)	ข้อจำกัด (Limits)	วันที่กรมธรรม์มีผลและสิ้นสุด (Term Dates)	เมื่อไหร่จะติดต่อ (When to contact)	ข้อมูลติดต่อ (Contact Information)
XXXX	เฉพาะทรัพย์สินคอมพิวเตอร์ เช่น ไฟไหม้ เป็นต้น แต่ไม่รวมประกันภัยไซเบอร์	ตามรอบปีงบประมาณ	ในทันที เมื่อมีการสูญเสียทางการเงินหรือข้อมูลใด ๆ	XXXX

รูปที่ 6-11: ความคุ้มครองประกันภัยและข้อมูลการติดต่อ

*อาจมีการจำกัดความคุ้มครองเพิ่มเติมต่อการเรียกร้อง (Additional Coverage Sub-limits May Apply per Claim)

ค้นหาสำเนาหน้าใบประกาศประกันภัย (Insurance Declaration Page) ได้ที่ฝ่ายบริหารงานองค์กรส่งคำถามโดยตรงเกี่ยวกับวงเงินประกัน (Insurance Coverage) ต่อผู้จัดการความเสี่ยง (Risk Manager) แจ้งผู้จัดการความเสี่ยงเพื่อเปิดใช้งานแผนประกัน (Activate the Insurance Plan)

	ชื่อเอกสาร แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร		
	ระดับชั้นความลับ ใช้ภายในสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น	เวอร์ชัน 1.0	หน้า 78

6.10 ภาคผนวก 10 การสื่อสารแผนการรับมือภัยคุกคามทางไซเบอร์ไปยังบุคลากรที่เกี่ยวข้องทั้งหมด

กลุ่มเป้าหมาย	แพลตฟอร์ม/ช่องทางการเผยแพร่	เป้าหมาย
บุคลากรที่รับแจ้งเหตุการณ์	- แจ้งผ่านเบอร์โทรศัพท์มือถือ - แจ้งผ่าน Email - แจ้งเหตุเบอร์โทรของสำนักงาน - สื่อสารและเผยแพร่ผ่าน Line Group - สื่อสารและเผยแพร่ผ่าน Website - สื่อสารและเผยแพร่ผ่าน Facebook - หนังสือแจ้ง - การประชุม	- เพื่อสื่อสารกับบุคลากรภายในหน่วยงาน เพื่อให้มีความเข้าใจ และช่วยกันบรรเทาปัญหา - เพื่อให้พนักงานบุคลากรที่รับแจ้งเหตุการณ์สามารถรายงานข้อมูลเหตุการณ์ทางไซเบอร์ได้อย่างทันกาล
ทีมตอบสนองเหตุการณ์	- แจ้งผ่านเบอร์โทรศัพท์มือถือ - แจ้งผ่าน Email - แจ้งเหตุเบอร์โทรของสำนักงาน - สื่อสารและเผยแพร่ผ่าน Line Group - สื่อสารและเผยแพร่ผ่าน Website - สื่อสารและเผยแพร่ผ่าน Facebook - หนังสือแจ้ง - การประชุม	- เพื่อสื่อสารกับทีมตอบสนองเหตุการณ์เพื่อให้เข้าใจแนวทางการดำเนินการ - สื่อสารและการส่งต่อข้อมูลเหตุการณ์ทางไซเบอร์ไปยังผู้ที่เกี่ยวข้อง เพื่อให้พนักงานทีมตอบสนองเหตุการณ์สามารถตอบสนองต่อเหตุการณ์ทางไซเบอร์ได้อย่างทันกาล
ผู้บริหาร CIRT	- แจ้งผ่านเบอร์โทรศัพท์มือถือ - แจ้งผ่าน Email - แจ้งเหตุเบอร์โทรของสำนักงาน - สื่อสารและเผยแพร่ผ่าน Line Group	เพื่อให้เข้าใจบทบาทและกำกับดูแลการดำเนินการ ได้อย่างเหมาะสม

	ชื่อเอกสาร แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร		
	ระดับชั้นความลับ ใช้ภายในสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น	เวอร์ชัน 1.0	หน้า 79

กลุ่มเป้าหมาย	แพลตฟอร์ม/ช่องทางการเผยแพร่	เป้าหมาย
	• สื่อสารและเผยแพร่ผ่าน Website • สื่อสารและเผยแพร่ผ่าน Facebook • หนังสือแจ้ง • การประชุม	
ผู้ให้บริการสนับสนุนบริการสำคัญ	• แจ้งผ่านเบอร์โทรศัพท์มือถือ • แจ้งผ่าน Email • แจ้งเหตุเบอร์โทรของสำนักงาน • สื่อสารและเผยแพร่ผ่าน Line Group • สื่อสารและเผยแพร่ผ่าน Website • สื่อสารและเผยแพร่ผ่าน Facebook • หนังสือแจ้ง • การประชุม	- เพื่อสื่อสารเหตุการณ์ผิดปกติทางไซเบอร์ไปยังองค์กรหรือหน่วยงานภายนอกที่เกี่ยวข้องหรือที่ได้รับผลกระทบ - เพื่อให้สามารถดำเนินการได้อย่างเหมาะสมและทันการณ์ - เพื่อร่วมกันพัฒนาปรับปรุงการรักษาความมั่นคงปลอดภัยของการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอกอย่างต่อเนื่อง

รูปที่ 6-12: ตัวอย่างการกำหนดการสื่อสารแผนการรับมือภัยคุกคามทางไซเบอร์



สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ
Office of the National Land Policy Board

สำนักงานชั่วคราว สคทช.
อาคารอารีย์ ฮิลล์ ชั้น 19-20
เลขที่ 428 ถนนพหลโยธิน แขวงสามเสนใน เขตพญาไท
กรุงเทพฯ 10400

โทรศัพท์ 0 2265 5400
โทรสาร 0 2265 5401
อีเมล saraban@onlb.go.th