



Procedure

แผนรับมือเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ ของ ทอท. (AOT Cyber Incident Response Plan)

รหัสเอกสาร : Document No. PR-1608010-010

Version: 1

ผู้จัดทำเอกสาร


ส่วนมาตรฐานเทคโนโลยีสารสนเทศและการสื่อสาร



ฝ่ายกลยุทธ์เทคโนโลยีสารสนเทศและการสื่อสาร

โทรศัพท์ (800) 55300,55305


เจ้าของเอกสาร

สายงานเทคโนโลยีดิจิทัลและนวัตกรรม (สงทว.)

	แผนรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ ของ ทอท.	รหัสเอกสาร : PR-1608010-010
	(AOT Cyber Incident Response Plan)	เวอร์ชัน : 1
	สายงานเทคโนโลยีดิจิทัลและนวัตกรรม	วันที่บังคับใช้ : 1 พฤศจิกายน 2568
ฝ่ายกลยุทธ์เทคโนโลยีสารสนเทศและการสื่อสาร		หน้า (2) ของ (49) หน้า


รายละเอียดเอกสาร	
ประเภทเอกสาร :	ขั้นตอนการปฏิบัติงาน (Procedure: PR)
ผู้จัดทำเอกสาร :	ส่วนมาตรฐานเทคโนโลยีสารสนเทศและการสื่อสาร ฝ่ายกลยุทธ์เทคโนโลยีสารสนเทศและการสื่อสาร
ผู้ทบทวน  (..... นายสุชาติ.ปิตีพัฒน์.....) ตำแหน่ง ผอ.ก.ฝกท. วันที่ 28 ธ.ค. 68	ผู้อนุมัติ  (..... นายกิตติพงษ์ เวณุนันท์.....) ตำแหน่ง รณท. วันที่ 28 ธ.ค. 68

Version	วันที่บังคับใช้	ชื่อผู้จัดทำเอกสาร	สาระสำคัญของการแก้ไข/ปรับปรุง	หมายเหตุ
1	1 พฤศจิกายน 2568	น.ส.ฉัตรวดี ศิริโชค นายชนาธิป จินสุนทร	เอกสารประกาศใช้ครั้งแรก	ขึ้นทะเบียน ครั้งแรก
2				
3				

	แผนรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ ของ ทอท.	รหัสเอกสาร : PR-1608010-010
	(AOT Cyber Incident Response Plan)	เวอร์ชัน : 1
	สายงานเทคโนโลยีดิจิทัลและนวัตกรรม	วันที่บังคับใช้ : 1 พฤศจิกายน 2568
ฝ่ายกลยุทธ์เทคโนโลยีสารสนเทศและการสื่อสาร		หน้า (3) ของ (49) หน้า

สารบัญ

	หน้า
1. หลักการและเหตุผล	5
2. วัตถุประสงค์	5
3. ขอบเขต	5
4. หน้าที่การทบทวน	5
5. หน้าที่ในการดำเนินการตามแผน	5
6. คำนิยาม	6
7. กรอบแนวคิด (Framework)	8
8. โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team : CIRT)	10
9. หน้าที่และความรับผิดชอบ	11
10. โครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure)	23
10.1 หน่วยงานภายในที่เกี่ยวข้อง	24
10.2 หน่วยงานภายนอกที่เกี่ยวข้อง	25
11. ขั้นตอนและวิธีปฏิบัติงาน	27
ขั้นตอนและวิธีปฏิบัติงาน กระบวนการจัดการเหตุการณ์ด้านไซเบอร์ที่อาจส่งผลกระทบต่อความมั่นคง ปลอดภัยของระบบสารสนเทศ (Cybersecurity Incident Management)	27
11.1 แผนภูมิขั้นตอนการปฏิบัติ	27
11.2 คำอธิบายขั้นตอนการปฏิบัติ	31
12. การเก็บรักษาหลักฐาน (Preservation of Evidence) ก่อนกู้คืน รวมถึงบันทึกการยึดหลักฐาน คอมพิวเตอร์และอุปกรณ์อื่น ๆ เพื่อการสอบสวน	42
คำอธิบายขั้นตอนด้านนิติคอมพิวเตอร์ (Computer Forensic Procedure)	43
13. เกณฑ์และขั้นตอนในการเรียกใช้งาน (Activate) การรับมือต่อเหตุการณ์และ CIRT	46
13.1 ระดับความรุนแรงพิจารณาจากระดับผลกระทบ (Incident Impact) และระดับความเร่งด่วน (Urgency)	46
13.2 ระดับความสำคัญ (Priority)	47

	แผนรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ ของ ทอท.	รหัสเอกสาร : PR-1608010-010
	(AOT Cyber Incident Response Plan)	เวอร์ชัน : 1
	สายงานเทคโนโลยีดิจิทัลและนวัตกรรม	วันที่บังคับใช้ : 1 พฤศจิกายน 2568
ฝ่ายกลยุทธ์เทคโนโลยีสารสนเทศและการสื่อสาร		หน้า (4) ของ (49) หน้า

หน้า

13.3 ลำดับในการรับมือต่อเหตุการณ์ และระยะเวลาในการดำเนินการแก้ไขเหตุขัดข้อง ดังต่อไปนี้.....	47
14. ระเบียบวิธีการมีส่วนร่วม (Engagement Protocols) กับบุคคลภายนอก หรือแนวปฏิบัติ การบริหารจัดการบุคคลภายนอก.....	48
ภาคผนวก ก. การจำแนกหมวดหมู่เหตุภัยคุกคามทางไซเบอร์.....	49

สารบัญตาราง

หน้า

ตารางที่ 1 ผู้รับผิดชอบ/ผู้มีส่วนได้เสีย (Stakeholder) และคำอธิบายหน้าที่ความรับผิดชอบ	11
ตารางที่ 2 รายชื่อของบุคลากรที่มีความเกี่ยวข้องกับการรับมือเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์.....	24
ตารางที่ 3 รายชื่อของบุคลากรที่สนับสนุนการรับมือเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์	24
ตารางที่ 4 รายชื่อเจ้าหน้าที่ปฏิบัติการของศูนย์เฝ้าระวังฯ (SOC)	25
ตารางที่ 5 รายชื่อติดต่อหน่วยงานกำกับและภายนอกที่เกี่ยวข้อง	25

สารบัญรูปภาพ

หน้า

รูปที่ 1 แนวทางการจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ NIST SP 800-61.....	8
รูปที่ 2 ความเชื่อมโยงระหว่างทีมรับมือเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์และหน่วยงานอื่น ๆ ..	10
รูปที่ 3 โครงสร้างทีมรับมือเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT)	10
รูปที่ 4 ขั้นตอนการรายงานเหตุการณ์ทางไซเบอร์ของ ทอท.....	23
รูปที่ 5 ขั้นตอนการตรวจจับและวิเคราะห์เหตุการณ์ (Detect and Analysis)	27
รูปที่ 6 ขั้นตอนการจำกัดขอบเขตและการเก็บหลักฐาน (Containment and Preservation of Evidence)	28
รูปที่ 7 ขั้นตอนการกำจัดภัยคุกคามและกู้คืนระบบ (Eradication and Recovery).....	29
รูปที่ 8 ขั้นตอนการถอดบทเรียนหลังเหตุการณ์ (Post-incident Activity).....	30
รูปที่ 9 การเก็บหลักฐานและวิเคราะห์ทางนิติคอมพิวเตอร์ (Computer Forensic Procedure).....	42