Incident Handling Checklist (รายการตรวจสอบการจัดการเหตุการณ์ภัยที่เป็นคุกคาม)

	Action	Completed
	Detection and Analysis	
1.	Determine Whether an incident has occurred พิจารณาว่ามีเหตุการณ์ภัยที่เป็นคุกคามเกิดขึ้นหรือไม่	
1.1	Analyze the precursors and indicators วิเคราะห์สารตั้งต้นและตัวชี้วัด	
1.2	Look for correlating information ค้นหาข้อมูลที่สัมพันธ์กัน	
1.3	Perform research (e.g., search engines, knowledge base) ดำเนินการวิจัย (เช่น เครื่องมือค้นหา ฐานความรู้)	
1.4	As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence ทันทีที่ผู้ดำเนินการเชื่อว่ามีเหตุการณ์เกิดขึ้น ให้เริ่มบันทึกการสอบสวนและรวบรวมหลักฐาน	
2.	Prioritize handling the incident based on the relevant factor (functional impact, information impact, recoverability effort, etc.) จัดลำดับความสำคัญในการจัดการเหตุการณ์ตามปัจจัยที่เกี่ยวข้อง (ผลกระทบด้านการทำงาน ผลกระทบของข้อมูล ความพยายามในการฟื้นตัว ฯลฯ)	
3.	Report the incident to the appropriate internal personal and external organizations รายงานเหตุการณ์ดังกล่าวต่อองค์กรภายในและภายนอกที่เหมาะสม	
	Containment, Eradication, and Recovery	
4.	Acquire, preserve, secure, and document evidence รวบรวม เก็บรักษา รักษาความปลอดภัย และจัดทำเอกสารหลักฐาน	
5	Contain the incident ; มีเหตุการณ์ภัยที่เป็นคุกคามเกิดขึ้น	
6.	Eradicate the incident ; ขจัดเหตุการณ์ภัยที่เป็นคุกคามที่เกิดขึ้น	
6.1	Identify and mitigate all vulnerabilities that were exploited ระบุและบรรเทาช่องโหว่ทั้งหมดที่ถูกนำไปใช้ประโยชน์	
6.2	Remove malware, inappropriate materials, and other components ลบมัลแวร์ สื่อที่ไม่เหมาะสม และส่วนประกอบอื่นๆ	
6.3	If more affected hosts are discovered (e.g.. new malware infections), repeat the Detection and Analysis step (1.1, 1.2) to identify all other affected hosts, then contain (5) and eradicate (6) the incident for then หากมีการค้นพบโฮสต์ที่ได้รับผลกระทบมากขึ้น (เช่น การติดมัลแวร์ใหม่) ให้ทำซ้ำขั้นตอนการตรวจจับและการวิเคราะห์ (1.1, 1.2) เพื่อระบุโฮสต์อื่นๆ ที่ได้รับผลกระทบทั้งหมด จากนั้นบรรจุ (5) และกำจัด (6) เหตุการณ์ที่เกิดขึ้น	
7.	Recover from the incident ; ฟื้นตัวจากเหตุการณ์ที่เกิดขึ้น	
7.1	Return affected systems to an operationally ready state คืนระบบที่ได้รับผลกระทบกลับสู่สถานะพร้อมใช้งาน	
7.2	Confirm that the affected system are functioning normally ยืนยันว่าระบบที่ได้รับผลกระทบทำงานได้ตามปกติ	

Incident Handling Checklist (รายการตรวจสอบการจัดการเหตุการณ์ภัยที่เป็นคุกคาม)

	Action	Completed
7.3	If necessary, implement additional monitoring to look for future related activity หากจำเป็น ให้ดำเนินการติดตามเพิ่มเติมเพื่อค้นหากิจกรรมที่เกี่ยวข้องในอนาคต	
	Post-Incident Activity	
8.	Create a follow-up report ; สร้างรายงานการติดตามผล	
9.	Hold a lessons learned meeting (mandatory for major incident, optional otherwise) จัดการประชุมบทเรียน (บังคับสำหรับเหตุการณ์ที่เป็นภัยคุกคามสำคัญ หรือไม่บังคับ)	

Reference : Incident Handling Checklist (NIST 800-61 r2)