Cybersecurity Incident Response Plan

Osotspa Public Company Limited and subsidiaries

Effective from 1 April 2025 onwards

Document Control

Approved by  (Wannipa Bhakdibutr) Chief Executive Officer	
Reviewed by  (Pajaree Saengcum) Head of Digital Technology	**Prepared by**  (Anupas Siriwej) Head of Digital Service Excellence

Revision History

Revision	Effective Date	Author(s)	Change Description
00	01-Jul-22	Anupas S.	- Initial revision.
01	01-Apr-24	Anupas S.	- Update member name and position. - Revise escalation path. - Revise financial criteria.
02	01-Apr-25	Anupas S.	- Update member name and position.

1. Objective

This document describes the process that is required to ensure an organized approach to managing cybersecurity incidents within Osotspa Public Company Limited (“Osotspa”) and coordinating response and resolution efforts to prevent or limit damage that maybe caused.

2. Scope

This document governs how the Computer Security Incident Response Team (CSIRT) should respond to all forms of cybersecurity incidents and includes the roles and responsibilities of stakeholders across Osotspa (both within and outside IT).

3. Definition

Term	Definition
Event	Any observable occurrence in a system or network.
Alert	A notification that an event or sequence of events may be an incident. Alerts may originate from many sources, such as security tools, employees, customers, and threat intelligence feeds.
Cybersecurity Incident	A violation or imminent threat of violation of IT security policies, acceptable use policies, or standard security practices that requires corrective action because it threatens the confidentiality, availability, and integrity of an information system or the information the system processes, stores or transmits. Sometimes shortened to “security incident” or just “incident” within this document. Examples of incidents include (but are not limited to): - Violations of an explicit or implied security policy - Virus or malware outbreak (including ransomware) - Attempts to gain unauthorized access to IT systems or data - Denial of service to IT systems or endpoints - Unauthorized use IT systems or endpoints - Unauthorized modification of information - Extortion related to the theft and/or encryption of IT systems or enterprise data - Compromise, disclosure, or loss of sensitive or personal information

4. Roles and Responsibilities

The CSIRT is responsible for managing responses to cybersecurity incidents. The members of the CSIRT are identified below.

Name	Title	CSIRT Role	Contact Information
Core members			
Pajaree Saengcum	Head of Digital Technology	Head of IT	pajaree.sae@osotspa.com Tel. 084-356-1035
Anupas Siriwej	Head of Digital Service Excellence	Incident Coordinator	anupas.sir@osotspa.com Tel. 065-983-5208
Chairat Jongrakthaitae	Service Owner	IT Support – Network & Security	chairat.jon@osotspa.com Tel. 063-206-0706
Noppon Klinpol	Service Owner	IT Support – Infrastructure	noppon.kli@osotspa.com Tel. 065-716-7214
Kulprapat Puangthongthip	Associate Service Owner	IT Support – Service Desk	kulprapat.pua@osotspa.com Tel. 063-206-0697
Cybertron Co., Ltd.		Security Operation Center (SOC)	cyber911@cybertron.co.th Tel. 094-986-4115
Optional members that may be activated only if required, based on the circumstances of an incident.			
Nichayada Ragkhitwetsagul	Head of Legal and Compliance	Legal and Regulatory Compliance Data Protection Officer (DPO)	nichayada.rag@osotspa.com Tel. 063-206-1945
Rujapa Hamnilrat	Head of Human Capital and Organization Excellence	Human Resources (HR)	rujapa.ham@osotspa.com Tel. 088-787-9419
Sutida Siamharn	Head of Corporate Communication and CSR	Public Relations (PR)	sutida.sia@osotspa.com Tel. 095-869-9595
Thanatt Louhalertdecha	Head of Risk Management, Internal Control, and Process Improvement	Insurance, Risk, Internal Control (RMIC)	thanatt.lou@osotspa.com Tel. 094-741-6354
BU Leader	Head of Function	BU Leader – owner of affected systems/data	

RACI Chart

Optional position that may be activated only if required

			Head of IT	Incident Coordinator	IT Support	SOC	DPO	BU Leader	Legal	PR	HR	RMIC
Detect and Analyze	1	Declare incident		AR	CI	CI						
	2	Assign category and severity	CI	AR	C		CI	C	C			
	3	Resolve Using BAU Process		I	AR	I		CI				
	4	Mobilize CSIRT	I	AR	CI							
	5	Collect incident data		A	R	R		C				
	6	Identify whether Personal data is potentially impacted	CI	A	C	CI	R	R				
	7	Determine if notification is required	I	CI			AR*	AR	C			
	8	Determine notification coms.	I	CI			CI*	R	A	R	R	
	9	Notify relevant parties	I	CI			CI*	R	A	R	R	R
Contain	10	Develop resolution action plan	I	AR	R	C	C*	C				
	11	Execute resolution action plan	I	A	R	I	C*					
Post-Incident Activity	12	Conduct a post incident review	CI	A	R	R	C*	C	C	C	C	C
	13	Update controls and policies	AR	I	R	I	I*					
	14	Demobilize CSIRT	CI	AR		I	I*			I		
	15	Close Ticket	I	AR		I	I*	I		I	I	I
	16	Documentation / update ticket	I	AR	C	I	C*					
	17	Overall coordination / communication	A	R	C	I	C*	I	I	I	I	I

Responsible: Person or function that is responsible for executing the activity

Accountable: Person or function that owns the activity, approves work and is held accountable for it

Consulted: Person or function that has information relevant to the activity

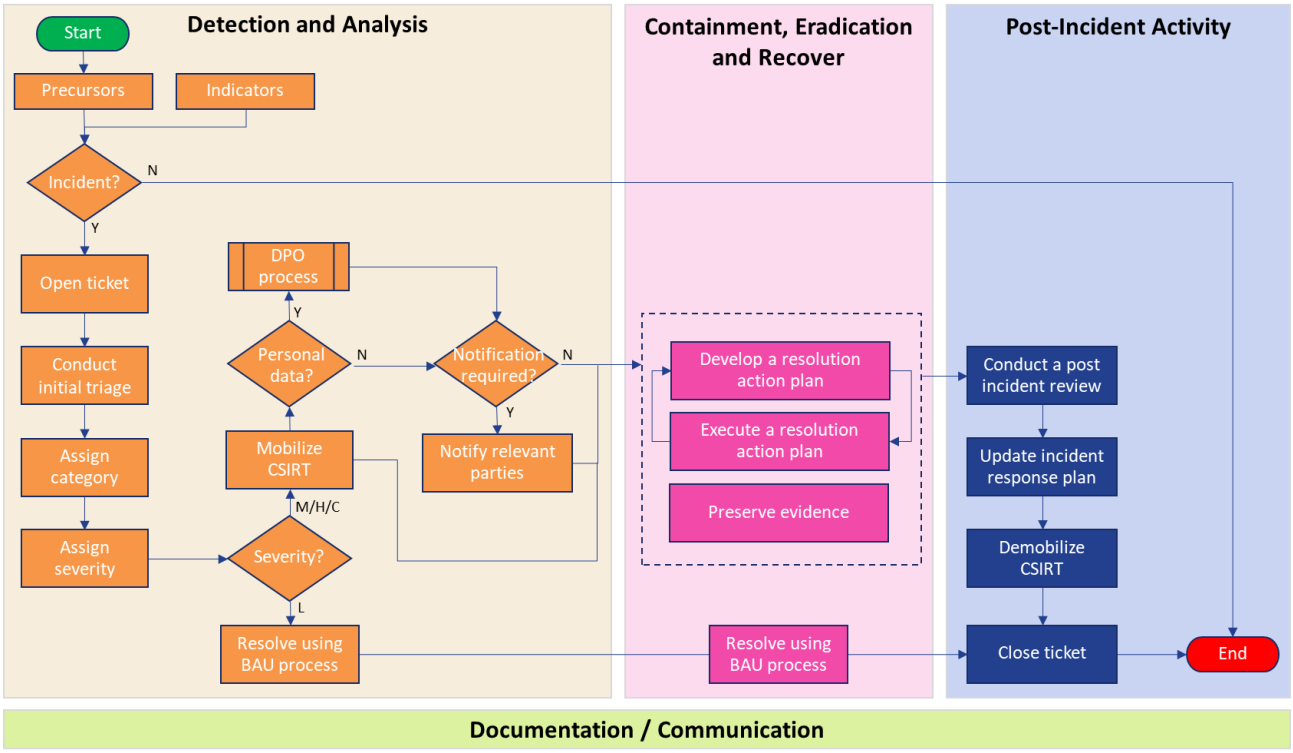
Informed: Person or function to be informed of progress and results

5. Related Documents

- Information Security Policy
- National Institute of Standards and Technology (NIST) SP 800-61, Computer Security Incident Handling Guide

6. Work Process

The CSIRT adheres to the following process during incident response. The Incident Coordinator ensures that each step is completed and that all progress is tracked on a rolling basis.



6.1 Detection and Analysis

Detection and analysis determines when an event is a cybersecurity incident, the priority of the incident, and the appropriate response. Every incident must be prioritized to ensure that resources are correctly allocated and that incidents are handled within the correct time frame.

6.1.1 Incident Detection

There is no single process for detecting a cybersecurity incident. Detection often involves:

- Precursors: detecting that a cyber-attack might occur in the future, such as the receipt of a threatening email, news of a global malware/ransomware attack, intelligence feeds for threat or vulnerability advisories from a variety of sources.
- Indicators: detection that an incident may have occurred (e.g., intrusion detection alerts, file names with odd characters, configuration changes).

The table below provides some common indicators that suggest you might be experiencing a cybersecurity incident.

Indicators	Examples
Reports of unusual or suspicious activity by staff or external stakeholders.	A staff member receives an email asking them to confirm their usernames/passwords or to provide other personal or sensitive information.
	Multiple staff report being “locked out” of their accounts.
	An external stakeholder reports receiving spam or phishing emails from Osotspa.
System(s)/service(s) not operating or functioning as expected	For example, one or more IT systems or services may cease functioning, or may not function as expected, and there is not a readily identifiable cause (such as a planned upgrade or outage).
	SSL Certificates broken; for example customers complaining that organization’s website has a broken link.
Unusual Activity	Network administrators observe a large number of bounced emails containing suspicious or unexpected content; or there is a substantial change in network traffic flows with no readily identifiable cause.
	Network or application logs show multiple failed login attempts from unfamiliar remote systems, such as overseas locations.
	Anti-virus alerts – a notification from anti-virus service or a managed service provider that it has detected suspicious activity or files on your network, which require analysis and remediation.
	Service or admin accounts modifying permissions; admin accounts adding standard users to groups; service accounts logging into a workstation.
	A system administrator observes a filename with unusual characters, or expected files are no longer visible on the network.

6.1.2 Incident Analysis

After considering the indicators of a potential cyber incident, it is important to confirm whether an incident has, or continues, to occur. The following table identifies steps that are useful in confirming the presence of a cyber incident.

Action	Description
Updated Resources	Ensure that the following documents are up to date: - Network diagrams - IP addressing schemas - Port lists

Action	Description
	- Documentation that may include system designs/architecture, security plans, GPO configuration, etc.
Reviewing log entries and security alerts	Are there any unusual entries or signs of suspicious behavior on the network or applications?
Have Work Instructions (WIs) for different operating systems	For Windows workstations, follow a WI on what to look for or review (i.e., specific event log sources, the types of events to search for, etc.). The same applies for Linux and Unix Operating Systems.
Consult with network and application experts	Is there a legitimate explanation for the unusual or suspicious activity that has been observed?
Conduct research	Research and review any open source materials (including via Internet search engines) relating to the unusual or suspicious activity that is observed (for example, consider performing a search on any unusual filenames that are observed on the network).
Watch list / monitor list	Develop a list where suspected accounts or IPs can be added to monitor their ongoing activity.
IMPORTANT	Do not 'ping' or try to communicate with a suspected IP address or URL from Osotspa network, as this may tip off the attacker that their activity have been detected. This should be conducted by a third party that is able to conduct this activity securely and anonymously.

It is important to consider the timeliness of your analysis. Lengthy analysis is useful for developing a comprehensive understanding of an incident but can also impede the overall response process. Generally, it is advisable to spend up to 1 hour on the initial incident analysis phase before seeking outside assistance.

6.1.3 Incident Declaration and Categorization

The CSIRT is responsible for declaring a security incident. The CSIRT uses its expertise, tools, information sources (e.g., threat intelligence feeds), and judgment to declare a security incident. Incidents typically fall into the following incident categories and types.

Incident Category	Incident Types
Abusive Content or Activities	- Spam - Harassment - Pornography / child abuse/ violence

Incident Category	Incident Types
Account Compromise	- Privileged account compromise - Unprivileged account compromise - Unauthorized privilege escalation - Application account compromise
Availability	- System outage (malicious) - Data availability (malicious)
Breach	- Unauthorized access to information - Unauthorized data modification - Data Exfiltration - Privacy Violation
Social Engineering	- Phishing - Vishing - Smishing
Impersonation / Spoofing	- Business email compromise - Spoofing - Rogue wireless access point - IoT device impersonation
Information Gathering	- Scanning - Sniffing - Social engineering
System Intrusion	- Exploiting known vulnerabilities - Login attempts - Point of Sales terminal intrusion - Network intrusion
Lost or Stolen Asset	- Mobile device - Laptop computer - Media (USB drive, etc.) - IoT device
Malware & Malicious Code	- Virus - Worm - Trojan - Spyware - Bot - Ransomware
Website Attack	- Website defacement - SQL injection - XSS - DoS/DDoS

6.1.4 Incident Severity Tiers

All security incidents must be assigned a severity tier. Severity tiers help guide incident escalations, assign SLAs, and otherwise inform the potential or realized impact of an incident on the organization. An incident's severity tier can change over the course of the response as more information is gathered and as the investigation unfolds.

Incidents will be assigned a severity tier based on the criteria defined below:

Severity	Business Impact				Technical Attributes	
Tier	Safety	Regulatory	Financial	Reputational	Data Class	Operations
4-Critical	Severe Injuries/Death	Any non-compliance which leads to litigation or claim with significant amount of damages including any class-action lawsuit	> 250 mTHB	Very negative news, offline/online/social media coverage in long-term (> 72 hours)	Top secret, restricted distribution	Critical systems offline with no known resolution
3-High	Serious Injuries	Any non-compliance which leads to investigation by or to be reported to the regulator/authority or lead to lawsuit and/or claim	100-250 mTHB	Negative news, online/social media coverage in short-term (≤ 72 hours)	Sensitive, proprietary, or personal data	Critical systems affected with known (quick) resolution
2-Medium	First Aid	Any non-compliance which is complained by employee and can be rectified immediately by the company	< 100 mTHB	Offline media coverage in short-term (≤ 72 hours)	Internal, non-sensitive data	Small number of non-critical systems affected with known resolutions
1-Low	No Injuries	Any non-compliance which has no impact	No loss	No harm	Public	One or two non-sensitive / non-critical machines affected

6.1.5 CSIRT Activation

If a cybersecurity incident is confirmed and the severity is 2-Medium or higher, the Incident Coordinator will activate the CSIRT. The low severity incidents will be resolved using Business-As-Usual (BAU) process without activation of the CSIRT.

The CSIRT operations room is located at room 7.1, building P3, floor 7, Osotspa Hua Mak Office. Microsoft Teams will be used as a collaboration hub.

6.1.6 Incident Escalation

The escalation path below indicates who should be notified at each severity tier. Keep in mind that escalations are cumulative, so all individuals at and below the severity tier level should be notified. In some cases, an incident's severity tier will increase as the investigation unfolds or the incident cannot be resolved within SLA.

In addition to the escalation path below, some roles should be notified based on attributes of the incident beyond severity tier. If the incident:

- Includes breach of personal data, notify Legal and Data Protection Officer.
- Includes a ransom demand, notify Legal, Group CFO, and CEO.

Severity Tier	Escalation Path
4-Critical	Same as severity 3-High
3-High	Group Chief Financial Officer (chair of Digital and Cybersecurity Committee), Chief Executive Office, Risk Management Committee
2-Medium	Head of Digital Technology
1-Low	Incident Coordinator

Note: Escalations are cumulative as the severity tier increases

6.1.8 Documentation

Upon establishment, the CSIRT should immediately begin documenting information about the incident. This documentation includes:

The Situation Updates (Appendix 7.1) should be prepared and disseminated to Osotspa internal stakeholders at regular intervals. It is important to be proactive with the development and dissemination of your situation reports, to reduce the need for stakeholders to approach you with various questions about the incident.

The Incident Log (Appendix 7.2) should be maintained by a member of the CSIRT (or a delegate). The incident log should capture minutes from each CSIRT meeting, details of all critical decisions (including the rationale for a decision), operational actions taken, action items and future meeting dates and times. Each entry to the incident log should include date, time and author details.

6.2 Containment and Eradication

6.2.1 Resolution Action Plan

The CSIRT should develop a Resolution Action Plan (Appendix 7.3) for resolving the incident. The Resolution Action Plan should consider the immediate and future steps required for containing the incident and eradicating any threats that might exist; and the future steps required for restoring systems and services. The Resolution Action Plan should be reviewed throughout the process as it may change depending on what evidence is acquired during the detection and analysis steps.

The key elements of the Resolution Action Plan are:

- **Containment actions**: to limit the potential damage of a cybersecurity incident, reducing the overall impact to the enterprise. The CSIRT must use an assortment of containment actions, such as:
  - Shutdown systems
  - Disconnect systems from a network
  - Disable specific ports, protocols, services, functions, etc.
  - Disable access to compromised systems
  - Examine code in sandboxes
- **Eradication actions**: to remove the cause(s), as well as the effects of the incident, reducing the risk of the same threat potentially re-emerging. Potential eradication actions include but are not limited to:
  - Identify and mitigate all exploited vulnerabilities
  - Remove malware, inappropriate materials, and other attack components
  - Conduct ongoing detection and analysis actions to identify all affected hosts, and complete the containment and eradication actions for all affected systems
- **Recovery actions**: to restore normal operations once the incident is contained and eradicated. Depending on the type and severity of an incident, the CSIRT may need to develop this plan in conjunction with business continuity and IT services advisors. Common steps in the recovery step include:
  - Return affected systems to an operationally ready state
  - Confirm that the affected systems are functioning normally
  - Implement, as necessary, additional monitoring to look for future related activity
- **Communications actions**: what messages are communicating, to whom, when and how.

The details of the Resolution Action Plan will vary depending on the type of incident that you experience. There is no one-size-fits-all approach. When developing the Resolution Action Plan, it is important to consider:

- How long will it take to resolve the incident?
- What resources are required to resolve the incident (if not already included in the CSIRT)?
- What systems/services will be affected during the resolution process? What services are impacted?

The following table provides a list of common incident types, along with the corresponding response activities (which form the typical minimum response).

Type / Description	Initial response to minimize potential harm
Ransomware: a tool used to encrypt or lock victims'	Immediately remove the infected device(s) from the network to limit the spread of ransomware. Capture all available logs relevant to the device. Isolate the devices while containment and eradication activities are determined. The ransom payments will be approved by Executive Committee.
Malware Infections: a virus, worm, Trojan horse, or other code-based malicious entity that successfully infects a host.	Immediately remove the infected device(s) from the network to limit the spread of malware. Capture all available logs relevant to the device. Isolate the devices while containment activities are confirmed and eradication efforts are determined.

Type / Description	Initial response to minimize potential harm
Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks: overwhelming the network with traffic that it cannot process, sometimes causing the network to fail.	Request gateway services provider to identify DoS/DDoS nature, attack vector and implement suitable solutions. Liaise with gateway services and network team to apply filters at network edge and / or increase capacity.
Phishing and Social Engineering: deceptive communications designed to elicit users' sensitive information (including network credentials).	Review logs of affected users (web and email logs) to determine whether malicious links/attachments were accessed. Consult users to confirm what actions they took, and whether any personal/sensitive information was provided in response to a phishing/social engineering attempt. Consider resetting user passwords and monitoring accounts for any unauthorized access.
Data breach: unauthorized access to sensitive or personal data.	Contain the data loss/spill as soon as possible. Alert privacy, legal and communications/media teams. Investigate the cause of the data loss/spill.

6.2.2 Evidence Preservation

The CSIRT will collect and record evidence about the cybersecurity incident to support detailed forensic investigations, including law enforcement efforts to identify and prosecute potential cyber-attackers. To the best of its ability, and where relevant to the incident, the CSIRT should collect and record the following evidence:

- Hard drive images and raw images
- RAM images
- IP addresses
- Network packet captures and flows
- Network diagrams
- Log and configuration files
- Databases
- IR/investigation notes
- Screenshots
- Social media posts
- CCTV, video, and audio recordings
- Documents detailing the monetary cost of remediation or loss of business activity.

When gathering evidence, it is important to consider the following steps:

- Nominate a member of the CSIRT to be responsible for collating, recording, and storing all evidence that is collected.
- The CSIRT will create and maintain a log of all evidence collected, detailing the date and time evidence was collected, who it was collected by, and details of each item collected. See Evidence Register Template (Appendix 7.4) for a template to use for this task.

- Ensure that all evidence is securely stored and handled only by the nominated CSIRT member, with limited access provided to other staff.
- Any access to evidence should be clearly recorded in the evidence log, including the rationale for access.
- Minimize the number of times evidence is transferred between staff. Record details of any evidence transfer between staff.

6.3 Communications

6.3.1 Internal Communications

Beyond the regular situation reports, it may be necessary to brief employees about a cybersecurity incident. This is important if IT networks, systems, or applications no longer operate as expected, or if the situation has potential to generate media or public interest.

Key messages to consider when communicating with employees include:

- What happened and why did it happen?
- What will happen in the immediate future?
- What are employees expected to do?
- Who can employees contact if they have questions?

All internal communications must be reviewed and approved by Head of Corporate Communication and CSR prior to release. The Risk Management Committee shall be informed of communications regarding incidents classified as severity 3-High or higher.

6.4.2 External Communications

Depending on the impact and severity of a cyber incident, it may be necessary to communicate with external stakeholders (including media, customers, and the public). This is particularly important if the incident affects IT networks, systems, or applications relied upon by third-parties, such as public facing websites or services.

Key messages to consider when communicating with external stakeholders include:

- What happened and why did it happen?
- What systems/services are affected?
- What steps are being taken to resolve the situation?
- Is it possible to say when the situation will be resolved?
- What are external stakeholders expected to do?
- Who can external stakeholders contact if they have questions/concerns?

All external communications must be reviewed and approved by Head of Corporate Communication and CSR prior to release. The Risk Management Committee shall be informed of communications regarding incidents classified as severity 3-High or higher.

6.5 Post-Incident Activity

6.5.1 Post-incident review

This step is one of the most important phases in the incident response process and the one that is most often overlooked. Learning from each incident enables the CSIRT to continually improve its processes and procedures for managing cybersecurity incidents.

The CSIRT should come together for a post-incident review to discuss:

- Exactly what happened, and at what times?
- How well did staff and management perform in dealing with the incident? Were the documented procedures followed? Were they adequate?
- What information was needed sooner?
- Were any steps or actions taken that might have inhibited the recovery?
- What would the staff and management do differently the next time a similar incident occurs?
- How could information sharing with other organizations have been improved?
- What corrective actions can prevent similar incidents in the future?
- What precursors or indicators should be watched for in the future to detect similar incidents?
- What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

All lessons learned should be documented and assigned to an owner to implement.

6.5.2 Update Incident Response Plan

This plan will be continually updated to reflect better practice in cybersecurity incident response activities, including following any relevant post-incident reviews.

6.5.3 CSIRT Demobilization

Following the implementation and execution of an agreed recovery plan, the Incident Coordinator should advise the CSIRT that it is acceptable to stand down. The Incident Coordinator closes the incident once reporting is properly logged and communicated to relevant stakeholders.

7. Appendix

7.1 Situation Update Template

Date of Entry:	**Time of Entry:**	**Author:**
Date and Time Incident Detected		
Current Status	New / In Progress / Resolved	
Incident Type		
Scope – list the affected networks, systems and/or applications; highlight any change to scope since the previous log entry		
Impact – list the affected stakeholder(s); highlight any change in impact since the previous log entry		
Severity – outline the impact of the incident on the stakeholder(s); highlight any change to severity since the previous log entry		
Notifications Actioned/Pending		
Additional Notes		
Contact Details for Incident Coordinator		
Date and Time Of Next Update		

7.2 Incident Log Template

Date / Time	**Notes** (log, record facts, decisions, and rationale)
Start time	Start of Incident

7.3 Resolution action plan Template

Date and Time	**Category** (Contain / Eradicate / Recover / Communications)	**Action**	**Action Owner**	**Status** (Unallocated / In Progress / Closed)

7.4 Evidence Register Template

Date, Time and Location of Collection	**Collected By** (name, title, contact and phone number)	**Item Details** (quantity, serial number, model number, hostname, MAC address, and IP addresses)	**Storage Location and Label Number**	**Access –** date, time, person and rationale for access after collection

7.5 External Contact

Role	Party	Contact Information
Police	Hua Mak Police Station สถานีตำรวจนครบาลหัวหมาก	Tel. 0-2314-3340 huamark@royalthaipolice.go.th
Police	Technology Crime Suppression Division กองบังคับการปราบปรามการกระทำความผิด เกี่ยวกับอาชญากรรมทางเทคโนโลยี (บก.ปอท.)	Tel. 1441
Thai CERT	ศูนย์แจ้งเหตุภัยคุกคามทางไซเบอร์ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)	Tel. 02-114-3531 thaicert@ncsa.or.th
Personal Data Protection	Office of the Personal Data Protection Commission สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.)	Tel. 02-111-8800 saraban@pdpc.or.th