Office of the Government Chief Information Officer

INFORMATION SECURITY

Practice Guide

for

Information Security Incident Handling

[ISPG-SM02]

Version 1.5

April 2024

© The Government of the Hong Kong Special Administrative Region
of the People's Republic of China

The contents of this document remain the property of and may not be reproduced in whole or in part without the express permission of the Government of the Hong Kong Special Administrative Region of the People's Republic of China.

COPYRIGHT NOTICE

© 2024 by the Government of the Hong Kong Special Administrative Region of the People's Republic of China

Unless otherwise indicated, the copyright in the works contained in this publication is owned by the Government of the Hong Kong Special Administrative Region of the People's Republic of China. You may generally copy and distribute these materials in any format or medium provided the following conditions are met –

(a) the particular item has not been specifically indicated to be excluded and is therefore not to be copied or distributed;
(b) the copying is not done for the purpose of creating copies for sale;
(c) the materials must be reproduced accurately and must not be used in a misleading context; and
(d) the copies shall be accompanied by the words "copied/distributed with the permission of the Government of the Hong Kong Special Administrative Region of the People's Republic of China. All rights reserved."

If you wish to make copies for purposes other than that permitted above, you should seek permission by contacting the Office of the Government Chief Information Officer.

Amendment History

Change Number	Revision Description	Pages Affected	Revision Number	Date
1	G54 Information Security Incident Handling Guidelines version 5.0 was converted to Practice Guide for Information Security Incident Handling. The Revision Report is available at the government intranet portal ITG InfoStation: (http://itginfo.ccgo.hksarg/content/itsecure/review2016/amendments.shtml)	Whole document	1.0	December 2016
2	Added a new chapter on information security management and aligned references with other practice guides.	Whole document	1.1	November 2017
3	The scope of Government information system was elaborated and assessment and decision for incident was exemplified. The forms for reporting mechanism were fine-tuned.	Page 6. Page 26, Annex C	1.2	June 2021
4	Advise B/Ds to consult GIRO-SO if there are signs indicating the potential for an incident	Page 22, Page 27, Annex F	1.3	September 2022
5	The URL of the PCPD's data breach notification form was updated.	Page 29	1.4	June 2023
6	Updates were made based on the latest updates to IT Security Guidelines (G3) v10.0.	Whole document	1.5	April 2024

Table of Contents

1. Introduction

Effective information security management involves a combination of identification, prevention, detection, response and recovery. In addition to deploying strong security protection, bureaux and departments (B/Ds) should also be able to respond to incidents and invoke proper procedures in case an information security incident (hereafter referred to as security incident or incident) occurs. Proper and advanced planning ensures the incident response and recovery activities are known, coordinated and systematically carried out. B/Ds shall establish, document, test and maintain a security incident handling/reporting procedure for their information systems.

1.1 Purpose

This document provides guidance notes for the management, administration and other technical and operational staff to facilitate the development of information security incident handling and to be used for preparation for, detection of and response to information security incidents. As information security incidents of different information systems will have different effects and lead to different consequences, B/Ds should customise the information security incident response plans for their information systems according to their specific operational needs.

This document is intended to provide practical guidance on and reference for information security incident handling in the Government. It is not intended to cover technical descriptions of a specific computer hardware or operating system platform. B/Ds should consult corresponding system administrators, technical support staff and product vendors for these technical details.

1.2 Normative References

The following referenced documents are indispensable for the application of this document.

- Baseline IT Security Policy [S17] , the Government of the Hong Kong Special Administrative Region
- IT Security Guidelines [G3] , the Government of the Hong Kong Special Administrative Region
- Information technology - Security techniques - Information security management systems - Overview and vocabulary (fifth edition), ISO/IEC 27000:2018

- Information technology - Security techniques - Information security management systems - Requirements (third edition), ISO/IEC 27001:2022

- Information technology - Security techniques - Code of practice for information security controls (third edition), ISO/IEC 27002:2022

- Information technology - Security techniques - Information security incident management - Part 1: Principles of incident management (second edition), ISO/IEC 27035-1:2023

- Information technology - Security techniques - Information security incident management - Part 2: Guidelines to plan and prepare for incident response (second edition), ISO/IEC 27035-2:2023

- NIST SP 800-61 – Computer Security Incident Handling Guide

1.3 Definitions and Conventions

For the purposes of this document, the definitions and conventions given in S17, G3, and the following shall apply.

Abbreviation and Terms	
CPU	The Central Processing Unit (CPU) is the primary component of a computer that acts as its “control center.” The CPU, also referred to as the “central” or “main” processor, is a complex set of electronic circuitry that runs the machine's operating system and apps.
IDS	An intrusion detection system (IDS) is a system that monitors network traffic for suspicious activity and alerts when such activity is discovered.
Information Security Event	Occurrence indicating a possible breach of information security or failure of controls.
Information Security Incident	One or multiple related and identified information security events that can harm the government information systems and/or data assets or compromise its operations.
IoCs	Indicators of compromise (IoCs) serve as forensic evidence of potential intrusions on a host system or network.
RAM	Random Access Memory (RAM) is a type of computer memory that can be searched in any order and changed as necessary.
RPO	Recovery point objective (RPO) is defined as the maximum amount of data – as measured by time – that can be lost after a recovery from a disaster, failure, or comparable event before data loss will exceed what is acceptable to an organisation.
RTO	The recovery time objective (RTO) is the maximum acceptable time that an application, computer, network, or system can be down after an unexpected disaster, failure, or comparable event takes place.
SYN flood	A SYN flood (half-open attack) is a type of denial-of-service (DDoS) attack which aims to make a server unavailable to legitimate traffic by consuming all available server resources.

1.4 Contact

1.4.1 General

This document is produced and maintained by the Office of the Government Chief Information Officer (OGCIO). For comments or suggestions, please send to:

Email:	it_security@ogcio.gov.hk
Lotus Notes mail:	IT Security Team/OGCIO/HKSARG@OGCIO
CMMP mail:	IT Security Team/OGCIO

2. Information Security Management

Information security is about the planning, implementation and continuous enhancement of security controls and measures to protect the confidentiality, integrity and availability of information assets, whether in storage, processing, or transmission and its associated information systems. Information security management is a set of principles relating to the functions of planning, organising, directing, controlling, and the application of these principles in harnessing physical, financial, human and informational resources efficiently and effectively to assure the safety of information assets and information systems.

Information security management involves a series of activities that require continuous monitoring and control. These activities include, but are not limited to, the following functional areas:

- Security Management Framework and the Organisation;
- Governance, Risk Management, and Compliance;
- Security Operations;
- Security Event and Incident Management;
- Awareness Training and Capability Building; and
- Situational Awareness and Information Sharing.

Security Management Framework and Organisation

B/Ds shall establish and enforce departmental information security policies, standards, guidelines and procedures in accordance with the business needs and the government security requirements.

B/Ds shall also define the organisation structure on information security and provide clear definitions and proper assignment of security accountability and responsibility to involved parties.

Governance, Risk Management and Compliance

B/Ds shall adopt a risk based approach to identify, prioritise and address the security risks of information systems in a consistent and effective manner.

B/Ds shall perform security risk assessments for information systems and production applications periodically and when necessary so as to identify risks and consequences associated with vulnerabilities, and to provide a basis to establish a cost-effective security program and implement appropriate security protection and safeguards.

B/Ds shall also perform security audits on information systems regularly to ensure that current security measures comply with departmental information security policies, standards, and other contractual or legal requirements.

Security Operations

To protect information assets and information systems, B/Ds should implement comprehensive security measures based on their business needs, covering different technological areas in their business, and adopt the principle of "Prevent, Detect, Respond and Recover" in their daily operations.

- Preventive measures avoid or deter the occurrence of an undesirable event;
- Detective measures identify the occurrence of an undesirable event;
- Response measures refer to coordinated actions to contain damage when an undesirable event or incident occurs; and
- Recovery measures are for restoring the confidentiality, integrity and availability of information systems to their expected state.

Security Event and Incident Management

In reality, security incidents might still occur due to unforeseeable, disruptive events. In cases where security events compromise business continuity or give rise to the risk of data security, B/Ds shall activate their standing incident management plan to identify, manage, record, and analyse security threats, attacks, or incidents in real-time. B/Ds should also prepare to communicate appropriately with relevant parties by sharing information on response to security risks to subdue distrust or unnecessary speculation. When developing an incident management plan, B/Ds should plan and prepare the right resources as well as develop the procedures to address necessary follow-up investigations.

Awareness Training and Capability Building

As information security is everyone's business, B/Ds should continuously promote information security awareness throughout the organisations and arrange training and education to ensure that all related parties understand the risks, observe the security regulations and requirements, and conform to security best practices.

Situational Awareness and Information Sharing

As the cyber threat landscape is constantly changing, B/Ds should also constantly attend to current vulnerabilities information, threat alerts, and important notices disseminated by the security industry and the GovCERT.HK. The security alerts on impending and actual threats should be disseminated to and shared with those responsible colleagues within B/Ds so that timely mitigation measures could be taken.

B/Ds could make use of the cyber risk information sharing platform to receive and share information regarding security issues, vulnerabilities, and cyber threat intelligence.

Staff may also raise their security awareness by participating in security drills, attending seminars, showcases or visiting theme pages containing security intelligence information (e.g. Cyber Risk Information Sharing Platform) and general security information (e.g. Cyber Security Information Portal, InfoSec website).

3. Introduction to Security Incident Handling

In information security management, the "Security Operations" functional area includes the deployment of proper security protection and safeguards to reduce the risk of successful attacks. However, despite all these measures, security incidents do occur. Therefore, information security incident response plans need to be prepared in advance, and this is a major area under the "Security Event and Incident Management". These plans help B/Ds prepare to respond to security incidents and resume the services from the incidents if the services are degraded or suspended. Assigning appropriate personnel and responsibilities, reserving resources, and planning for the handling procedures should be addressed to prepare for the emergence of security incidents. In case an incident is detected, such preparation will facilitate incident response and allow the information system to recover in a more organised, efficient and effective manner.

3.1. Information Security Incident

A threat is a potential event or any circumstance with the potential to adversely impact the information assets, systems and networks (e.g. exploit vulnerabilities in information systems or networks) to cause information security events. An information security event is an event indicating a possible breach of information security or failure of controls. The occurrence of an information security event does not necessarily mean that an attack has been successful. It does not mean all information security events are classified as information security incidents. The term 'information security incident' used in this document means one or multiple related and identified information security events that can harm the government information systems (including information systems provided by the Government and responsible for the maintenance of such information systems, regardless of whether the information systems is deployed within or outside the Government) and data assets or compromise its operations. For example, an information security incident may refer to information leakage that will be undesirable to the interests of the Government or an adverse event in an information system and/or network, which impacts computer or network security with respect to confidentiality, integrity and availability. As this practice guide focuses on incidents related to information security, adverse events such as natural disasters, hardware/software breakdown, data line failure, power disruption, etc., are outside the scope of this practice guide and should be addressed by the corresponding system maintenance and disaster recovery plan.

Examples of security incidents include: denial of service attacks, compromise of protected information systems or data assets, leaks of classified data in electronic form, malicious destruction or modification of data, abuse of information systems, massive malware infection, website defacement, and malicious scripts affecting networked systems.

The following diagram illustrates the relationship between threats, information security events and information security incidents:

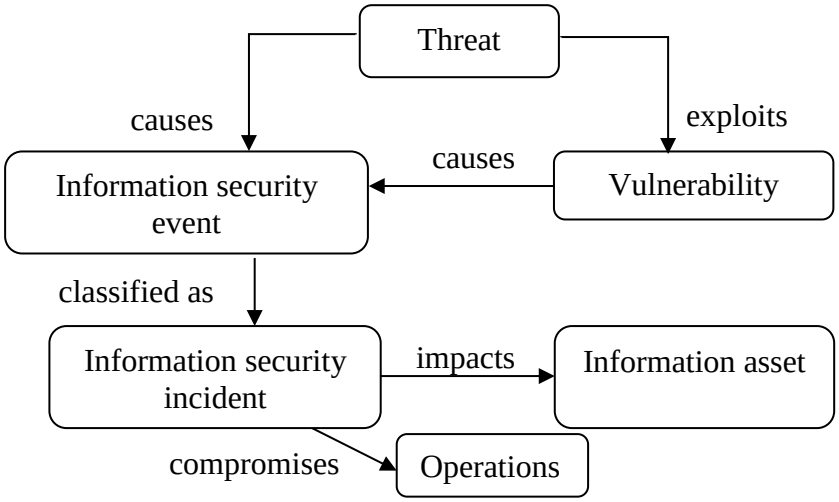


Figure 3.1 Relationship of Security Event and Security Incident

3.1.1 Security Incident Handling

Security incident handling is a set of continuous processes governing the activities before, during and after a security incident occurs.

Security incident handling begins with planning and preparing for the resources and developing proper procedures to be followed, such as the escalation and security incident response procedures.

When a security incident is identified, security incident response shall be made by the responsible parties following the predefined procedures. A security incident response represents the activities or actions carried out to tackle the security incident and to restore the system to normal operation.

When the incident is over, follow-up actions should be taken to evaluate the incident and strengthen security protection to prevent recurrence. The planning and preparation tasks should be reviewed and revised accordingly to ensure that there are sufficient resources (including manpower, equipment and technical knowledge) and properly defined procedures to deal with similar incidents in future.

3.2. Objectives of Security Incident Handling

Below are the major objectives of security incident handling:

- Ensure that the required resources are available to deal with the incidents, including manpower, technology, etc.
- Ensure that all responsible parties have a clear understanding of the tasks they should perform during an incident by following predefined procedures.
- Ensure that the response is systematic and efficient and that there is prompt recovery for the compromised system.
- Ensure that the response activities are recognised and coordinated.
- Minimise the possible impact of the incident in terms of information leakage, corruption and system disruption, etc.
- Share experience in incident response where appropriate.
- Prevent further attacks and damages.
- Deal with related legal issues and refer to the Hong Kong Police Force (HKPF) for criminal investigation when deemed appropriate.
- Report to the Office of the Privacy Commissioner for Personal Data (PCPD) if personal data is involved.
- Preserve information for investigation as far as practicable.

Due to the rapid development of information technology in the Government, a security incident response plan is considered essential for all B/Ds, in particular for those with the following information systems:

- Systems with external connection, e.g. Internet.
- Systems handling classified data and information.
- Tier 2 and Tier 3 information systems.
- Other systems which would be subject to a highly undesirable impact if a security incident occurs.

3.3. Disclosure of Information about Incident

Staff shall not disclose information about the individuals, B/Ds or specific systems that have suffered from damages caused by computer crimes and computer abuses, or the specific methods used to exploit certain system vulnerabilities, to any people other than those who are handling the incident and responsible for the security of such systems, or authorised investigators involving in the investigation of the crime or abuse.

Any disclosure of information about incidents, including how to compromise and the background of the system such as physical location or operating system, may encourage hackers to intrude other systems with the same vulnerabilities. Moreover, the disclosure may influence the forensic and prosecution processes under investigation by HKPF. However, after post-incident analysis, recommended actions to prevent similar security incidents in the future may be proposed. If the recommendations do not contain specific information about the occurred incident such as the involved individuals, B/Ds and systems, they may be shared among the Government so that other B/Ds can also prevent similar incidents and improve their security handling procedures.

4. Organisation Framework

The following diagram depicts a generic reference model of the organisational framework for making security incident responses in the Government.

According to the Baseline IT Security Policy, an Information Security Incident Response Team (ISIRT) shall be established in each B/D to coordinate the handling of information security incidents related to the B/D. The Government Information Security Incident Response Office (GIRO) provides central coordination and support to the operation of individual ISIRTs of B/Ds. Respective ISIRTs of B/Ds will be responsible for overseeing the incident handling processes of specific information systems, computer services, or functional areas within the B/Ds.

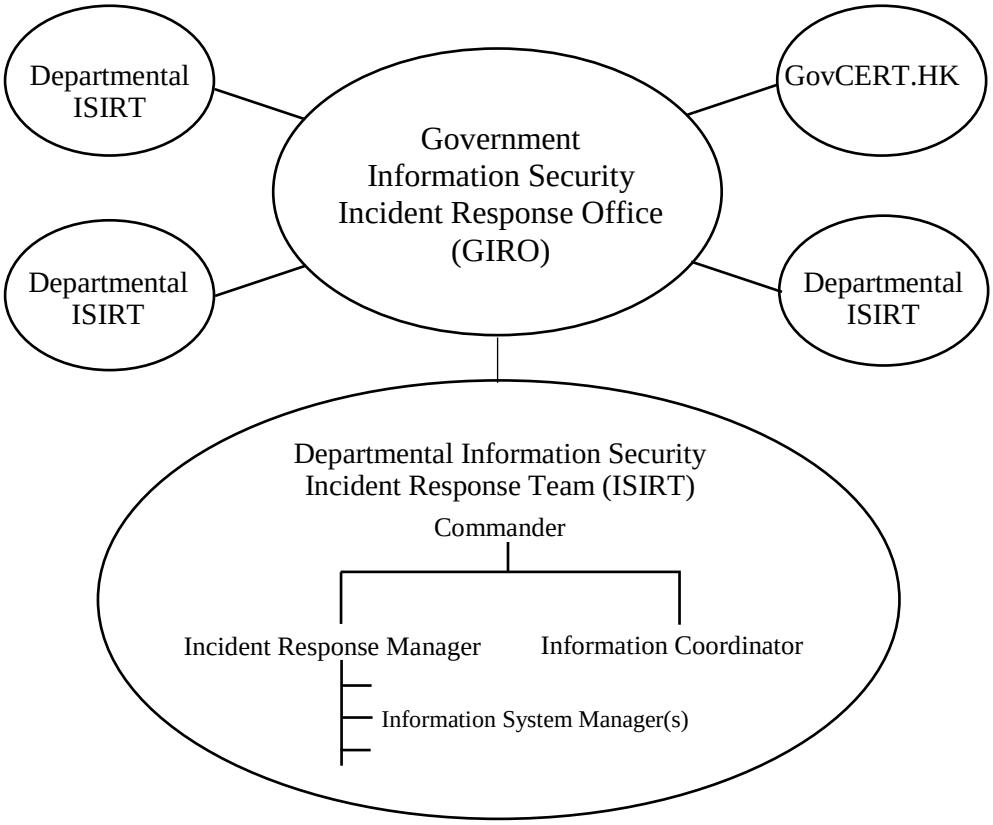


Figure 4.1 Parties Involved in Security Incident Handling

This section gives a high level description of the organisation framework, and the roles and responsibilities of different parties with respect to information security incident handling. The ISIRTs and respective departmental information systems should develop detailed procedures for handling information security incidents in accordance with the specific business needs and operational requirements of the B/Ds or the systems concerned.

4.1 Government Information Security Incident Response Office (GIRO)

GIRO is a government-wide establishment that provides central co-ordination and support to the operation of individual ISIRTs of B/Ds on information security incidents.

The GIRO Standing Office (GIRO-SO) is established to serve as the executive arm of GIRO. The major functions of the GIRO-SO include:

- Act as the central contact point for ISIRT Commanders with regard to information security incident reporting and co-ordination for responding to possible government-wide information security incidents.
- Keep track of the progress and remind the concerned departmental ISIRT for a post-incident report or interim report.
- Work closely with the Government Computer Emergency Response Team Hong Kong (GovCERT.HK) and seek its advice where necessary.
- Collaborate and work closely with the Cyber Security and Technology Crime Bureau (CSTCB) of the HKPF if a criminal act is involved.

4.1.1 Functions of GIRO

The GIRO has the following major functions:

- Maintain a central inventory and oversee the handling of all information security incidents in the Government.
- Prepare periodic statistics reports on government information security incidents.
- Act as a central office to coordinate the handling of multiple-point security attacks (i.e. simultaneous attacks on different government information systems).
- Enable experience sharing and information exchange related to information security incident handling among ISIRTs of different B/Ds.

4.1.2 Formation of GIRO

The core members of GIRO comprise representatives from:

- Office of the Government Chief Information Officer (OGCIO)
- Security Bureau (SB)
- Hong Kong Police Force (HKPF)

Staff members from ISIRT of individual B/Ds and other experts may also be invited to provide assistance in GIRO's operation as and when necessary, depending on the nature of different security incidents.

The GIRO-SO provides secretarial and functional support to GIRO, and acts as the central contact point for ISIRT Commanders with regard to information security incident reporting and co-ordination for responding to possible government-wide information security incidents.

Each B/D shall provide the GIRO-SO with contact information of the ISIRT Commander, and any subsequent update to facilitate effective communication. A copy of the Departmental IT Security Contacts Change Form is available in **Annex A**.

A special task force will be formed under the GIRO, as and when required, in the case of a multiple point attack, to coordinate response to security incidents that affect multiple B/Ds and/or the overall operation and stability of the Government as a whole.

4.2 Government Computer Emergency Response Team Hong Kong (GovCERT.HK)

The GovCERT.HK, established in April 2015, collaborates with the GIRO-SO in coordinating information and cyber security incidents within the Government. It also collaborates with the computer emergency response team community in sharing incident information and threat intelligence and exchanging best practices with a view to strengthening information and cyber security capabilities in the region. The GovCERT.HK has the following major functions:

- Disseminate security alerts on impending and actual threats to B/Ds.
- Act as a bridge between the Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) and other computer security incident response teams in handling cyber security incidents.

4.3 Departmental Information Security Incident Response Team (ISIRT)

An ISIRT shall be established in each B/D according to the Baseline IT Security Policy. It is the central body responsible for coordination, communication, and taking security incident handling actions in the B/D. The size and scale of ISIRT may vary according to the scale and scope of the information systems in different B/Ds, the relative sensitivity of the systems, and the potential impact of security incidents on them.

While the GIRO centrally coordinates the reporting of information security incidents and provides coordination and advisory support to individual ISIRTs, the ISIRT of each B/D remains responsible for the overall command and control in handling the security incidents within the B/D.

4.3.1 Functions of the ISIRT

Major functions of the ISIRT should include:

- Overall supervision and coordination of security incident handling of all information systems within the B/D.
- Collaboration with the GIRO in the reporting of security incidents for central recording and necessary follow-up actions, e.g. report to HKPF for further crime investigation.
- Dissemination of security alerts on impending and actual incidents from the GIRO to responsible parties within the B/D.
- Facilitating experience and information sharing within the B/D on security incident handling and related matters.

4.3.2 Formation of ISIRT

The ISIRT is the central focal point for coordinating all IT security incidents within the respective B/D. Head of B/D should designate an officer from the senior management team to be the Commander of ISIRT. The Commander should have the authority to appoint core team members for the ISIRT.

In the formation of ISIRT, the advice and support from the Departmental IT Security Officer (DITSO) is required to assist the ISIRT Commander to develop system specific security policy and incident response plan for the departmental information systems, and to establish the related logistical arrangements. The DITSO will also need to ensure that the departmental IT security policy is observed and enforced in all the information systems of the respective B/D.

While the exact membership of the ISIRT would vary according to the establishment of different B/Ds, there are a number of key roles that the ISIRT has to play, including ISIRT Commander, Incident Response Manager, Information Coordinator, and Information System Manager. These roles can be performed by different officers, or by a single officer. B/Ds should regularly assess the workload of the team and allocate resources accordingly to avoid bottlenecks and delays.

The following sections describe the responsibities of each role of the ISIRT in detail.

4.3.3 Roles of the ISIRT

4.3.3.1 Commander

The responsibilities of the Commander include:

- Provide overall supervision and co-ordination of information security incident handling for all information systems within the B/D.
- Make decisions on critical matters such as damage containment, system recovery, the engagement of external parties and the extent of involvement, and service resumption logistics after recovery, etc. based on the incident report and analysis provided by the Incident Response Manager.
- Trigger the departmental disaster recovery procedure where appropriate, depending on the impact of the incident on the business operation of the B/D.
- Provide management endorsement on the provision of resources for the incident handling process.
- Provide management endorsement in respect of the line-to-take for publicity on the incident.
- Coordinate and collaborate with GIRO-SO in the reporting of information security incidents for central recording and necessary follow-up actions in particular with the following characteristics:
  - (i) System providing public service and its failure will result in service interruption (e.g. denial of service attack to a government Internet website)
  - (ii) System handling classified information
  - (iii) System supporting mission critical operation
  - (iv) System which would be subject to a highly undesirable impact if a security incident occurs, e.g. affect the Government's public image due to website defacement
- Facilitate experience and information sharing within the B/D on information security incident handling and related matters.
- Coordinate and cooperate with investigation authorities in the investigation of security incidents.

4.3.3.2 Incident Response Manager

The Incident Response Manager is responsible for monitoring all security incidents handling process within the B/D and seeking management resources and support for the handling process. The responsibilities include:

- Overall management and supervision of all matters concerning security incident handling within the B/D.

- Alerting the ISIRT Commander upon receipt of report on security incident affecting the departmental information systems.
- Following up with the Information System Manager and related parties to compile incident report and conduct analysis.
- Reporting the progress of the security incident handling process to the ISIRT Commander.
- Coordinating various external parties, such as HKPF, PCPD, service contractors, support vendors, and security consultants, etc. in handling the incident.
- Seeking necessary resources and support from the ISIRT Commander for the incident handling activities.

4.3.3.3 Information Coordinator

The Information Coordinator is responsible for handling public inquiries regarding the security incident of the B/D. The Information Coordinator is also responsible for the overall control and supervision of information dissemination to the public, including the media.

4.3.3.4 Information System Manager

Dedicated resources should be provided to deal with security incidents that may occur within a specific information system, computer service, or functional area of individual B/Ds.

When handling security incident, the size and structure of the support team under individual departmental information system could be different, depending on the scope and nature of the system or service involved. For example, for a small, non-critical and internal system, one person may be sufficient for carrying out the duties of incident response.

For individual departmental information system, the manager of the respective departmental information system will oversee the whole security incident handling process for the system or functional area the manager is responsible for. The manager should represent the support team under individual departmental information system to provide the following major functions:

- Oversee the security incident handling process for the functional area in-charge.
- Speed up and facilitate the handling process by pre-establishing relevant handling procedures and list of contact points in advance.
- Provide a direct channel for receiving reports about suspected incidents.
- Provide direct and instant response to suspicious activities.
- Assist in minimising damages and recovering the system to normal operation.
- Seek advice on security issues from external parties such as service contractors,

computer product vendors, HKPF, or PCPD.

- Coordinate security incident handling of the respective information system with other external parties.
- Conduct impact analysis on the security alerts received from the ISIRT and the GovCERT.HK in respect of the functional area in-charge.

If a part or all of the operation of a specific information system is outsourced to external service providers and/or covered by the service provided by other government departments, the outsourced service providers and/or the servicing departments should also assign an information system manager and set up similar support teams for that specific information system to provide the corresponding services under their duties.

Apart from performing major functions as mentioned above, the Information System Manager should have the following responsibilities:

- Developing and implementing the system specific security incident response procedures.
- Observing and following security incident response procedures for reporting incident to the ISIRT of the B/D.
- Arranging and coordinating with all the concerned parties, e.g. service providers, contractors, and product support vendors, etc., to take rectification and recovery actions against the incident.
- Reporting the security incident to the ISIRT, and with the management support of the ISIRT, requesting for external assistance, such as HKPF, PCPD or the external service providers, in the course of investigation and evidence collection.
- Keeping abreast of the latest security technology and technique as well as the latest security alerts and vulnerabilities related to the system or functional area in-charge.
- Identifying any suspected attacks or unauthorised access through the use of security tools/software and/or the system logs, and checking audit trail records.
- Providing technical support, including evidence collection, system backup and recovery, system configuration and management, etc. in the course of problem diagnosis and system recovery.
- Arranging regular security assessment, impact analysis, and review of the information system.

5. Overview of Steps in Security Incident Handling

There are five major steps in security incident handling. An overview of these steps is provided below. The processes involved in each of the steps are described in more details in the corresponding sections.

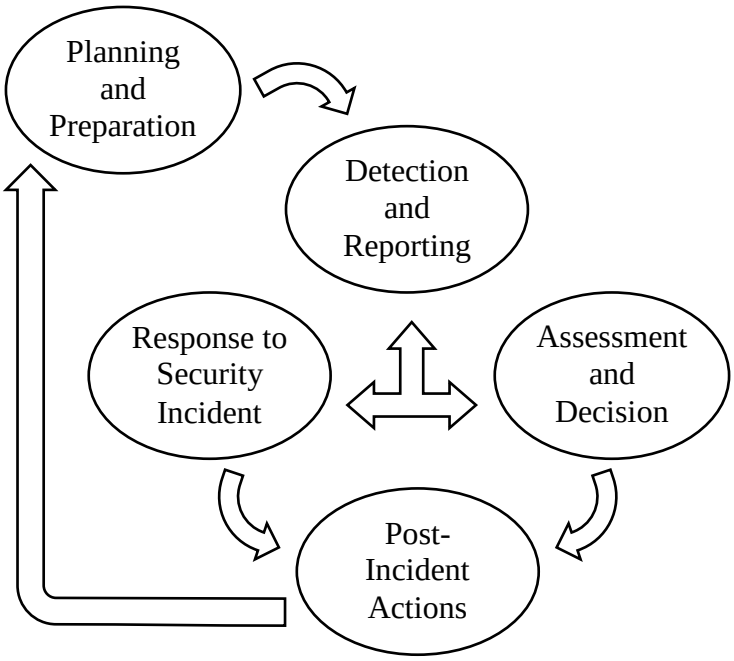


Figure 5.1 Security Incident Handling Cycle

A. Planning and Preparation (Section 6)

In this step, B/Ds should plan and prepare for the resources as well as develop proper procedures to be followed. The major activities involved in this step for planning and preparation are listed below.

- Planning of Incident Monitoring and Detection
- Planning of Security Incident Response
- Planning of Training and Education

B. Detection and Reporting (Section 7)

In this step, B/Ds should detect security events according to the established detection and monitoring mechanism. B/Ds should also follow the reporting procedure to bring the security events to the attention of the ISIRT. There are two major activities in this step:

- Detection Measure
- Reporting

C. Assessment and Decision (Section 8)

After an event has been detected, B/Ds should determine if an incident has actually occurred. If an event is identified to be an information security incident, B/Ds should determine the type of the incident, and assess its scope, damage and impact in order to effectively deal with it. B/Ds should also follow the predefined escalation procedure to notify the appropriate parties and escalate the incident to the appropriate level. The major activities in this step are:

- Assessment of Incident
- Escalation

D. Response to Security Incident (Section 9)

When a security incident is identified, B/Ds should follow the security incident response procedure to carry out actions to tackle the security incident and to restore the system to normal operation. The response procedure is broadly categorised into three stages:

- Containment
- Eradication
- Recovery

E. Post-Incident Actions (Section 10)

When the incident is over, follow-up actions should be taken to evaluate the incident and to strengthen security protection to prevent recurrence. The major follow-up actions are listed below.

- Post-incident Analysis
- Post-incident Report
- Security Assessment
- Review Existing Protection
- Investigation and Prosecution

6. Planning and Preparation

Proper and advanced planning ensures that the incident response and recovery activities are known, co-ordinated and systematically carried out. B/Ds shall maintain an updated inventory list of information systems with emergency contact points for security incident handling. Advanced planning also facilitates the B/D concerned to make appropriate and effective decision in tackling security incident, and in turn minimises the possible damages. The plan includes strengthening of security protection, making appropriate response to the incident, recovery of the system and other follow-up activities.

Major activities which need planning and preparation are as follows:

- Planning of Incident Monitoring and Detection
- Planning of Security Incident Response
- Planning of Training and Education

A checklist on preparation for security incident response is summarised in **Annex B** for reference.

6.1 Planning of Incident Monitoring and Detection

A sufficient level of security measures for incident monitoring shall be implemented to protect the system during normal operation as well as to monitor potential security incidents. The level and extent of measures to be deployed will depend on the importance and sensitivity of the system and its data, as well its functions.

Below are some typical measures for security incident monitoring:

- Install firewall devices and apply authentication and access control measures to protect important system and data resources.
- Install intrusion detection tool to proactively monitor, detect and respond to system intrusions or hacking.
- Install anti-malware tools and malware detection and repair tools to detect and remove malware, and prevent it from affecting system operations.
- Perform periodic security checks by using security scanning tools to identify existing vulnerabilities and perform a gap analysis between the stated security policy and the actual security arrangement.
- Install a content filtering tool to detect malicious contents or codes in emails or web traffic.
- Enable system and network audit logging to facilitate the detection and tracing of unauthorised activities.
- Develop programs and scripts to assist in the detection of suspicious activities, monitoring of system and data integrity, and analysis of audit log information.

- Subscribe the security news, alerts, vulnerability information, reports and other information security publications for raising the awareness of emerging security threats and associated risks.
- Maintain and document a vulnerability management mechanism to identify, assess and mitigate the security risks.
- Apply threat intelligence feeds and data into the monitoring process. Please refer to the Practice Guide for IT Security Threat Management for threat intelligence integration and application.

6.2 Planning of Security Incident Response

B/Ds shall appoint two designated individuals as 7x24 contact points for incident handling to ensure continuous availability and accessibility for immediate response to security incidents. These individuals must be reachable at all times, around the clock, including weekends and holidays, and be prepared to engage in incident handling activities.

The expectation for these contact points includes:

- The appointed contact points must be on standby to receive and respond to emergency calls regarding IT security issues at any hour, even during non-working hours. This is important to facilitate instant communication and swift incident handling to effectively minimise any potential damage and loss incurred due to security incidents.
- The designated contacts are expected to acknowledge and act upon any received communication promptly, ensuring no delay in the incident response process.
- The designated contacts must be capable of handling security incidents directly or have the authority and capability to relay emergency security messages to responsible personnel in a timely manner.
- B/Ds should regularly verify the contact details of the appointed individuals to ensure they are current and that there are no barriers to reaching them immediately when needed.

A security incident response plan shall be established and documented. The security incident response plan shall cover at least the following:

- Structure of the incident response team and the corresponding roles and responsibilities;
- Reporting procedures;
- Procedures for mitigating the impact of an incident, preserving evidence, investigating the cause and impact of an incident;
- Recovery plan;
- Communication plan with stakeholders and the general public; and

  Post-incident review procedures.

Regular security incident response plan review shall be conducted at least once every two years, or when there is any material change in the operating environment of the B/Ds. B/Ds shall ensure all relevant personnel are familiar with the plan, and the plan should be made known to all staff, including management personnel, for their reference and compliance. The plan should be clear, straightforward and easily understood so that all personnel have clear knowledge about what they need to do. B/Ds should include different scenarios and corresponding response procedures in the incident response plan. The plan shall be regularly tested and updated to ensure a quick and effective response to information security incidents. Moreover, B/Ds shall conduct drills at least once every two years, preferably annually, to assess the effectiveness of the plan. The incident response team members shall participate in the drills to familiarise themselves with their roles in the incident response plan to ensure quick and effective responses to security incidents.

For details about incident response drill workflow and action cards for different scenarios, please refer to the IT Security Theme Page at the ITG InfoStation (https://itginfo.ccgo.hksarg/content/itsecure/sih/actioncard/index.html).

6.2.1 Structure of the incident response team and the corresponding roles and responsibilities

The structure of the incident response team and the corresponding roles and responsibilities of all parties participating in the security incident response process should be clearly defined. Section 4 above provides a reference model for defining the roles and responsibilities of those major members of a security incident response team.

6.2.2 Reporting procedures

(a) Reporting

A reporting procedure shall be established and documented to clearly define the steps and processes in reporting any suspicious activities to all parties involved in a timely manner. Comprehensive contact information, such as telephone numbers (office hours, non-office hours and mobile), email addresses, and fax numbers, should be set out in the reporting procedure to ensure effective communication among responsible personnel. Some suggested reporting mechanisms are set out in **Annex C.1** for easy reference.

Proper reporting procedure should be prepared in advance so that in case an incident occurs, all parties involved would know whom they should report to, and in what way, and what should be noted and reported.

To facilitate an effective reporting process, the following points should be noted:

- The reporting procedure should have a clearly identified point of contact, and comprises simple but well-defined steps to follow.
- The reporting procedure should be published to all concerned staff for their information and reference.
- Ensure all concerned staff are familiar with the reporting procedure and are capable of reporting security incidents instantly.
- Prepare a security incident reporting form to standardise the information to be collected.
- Consider whether the reporting procedure should apply during and outside working hours, and if necessary, draw up a separate procedure for non-office hour reporting together with those non-office hour contacts in respect of the concerned staff.
- Information about incidents should be disclosed only on a need-to-know basis, and only the ISIRT Commander has the authority to share, or authorise others to share, information about security incidents with others.

To improve the efficiency and effectiveness of IT security incident handling, advice from the GIRO-SO could be sought if B/Ds identify any signs of compromise that are possibly an indication of incidents and deserve special attention. The suggested indicators of such incidents can be found in **Annex F**.

By consulting with the GIRO-SO, B/Ds can proactively identify and address system abnormalities, ensuring early detection of IT security threats and incidents across the Government. This collaborative approach benefits the Government by safeguarding collective security and creating a resilient and secure environment.

Upon becoming aware of an information security incident, the departmental ISIRT shall:

- Report to the GIRO-SO within **60 minutes** by phone and submit a completed Preliminary Information Security Incident Report (see **Annex C.2**) within **48 hours**;
- Share with the GIRO-SO the following information upon availability if the security incident involves critical e-government services, has significant security implications, or might attract media attention:
  - (i) Type of the incident with an assessment of its scope, damage and impact;
  - (ii) Actions being taken or to be taken to contain the damage and rectify the problem;
  - (iii) Line-to-take if the case may attract media attention; and
  - (iv) Enquiries from media and suggested responses, if any.
- Update the recovery status to the GIRO-SO on a daily basis for those affected critical e-government services until the services are resumed.

- Notify GIRO-SO for any security incident reported to HKPF, PCPD, or issued to media organisations.

The benchmark for B/Ds to be considered “aware” of an incident is established when there is a reasonable degree of certainty that an information security event has caused harm to the confidentially, integrity or availability of government information systems or data assets or has compromised their operations Such awareness generally follows a preliminary assessment of the situation, which may require some time to conduct thoroughly.

Awareness of an incident may arise under several circumstances. For example:

- If unusual system behaviour is detected, such as unexpected data exports or unusual login patterns, and upon investigation, these are found to correlate with unauthorised access or data exfiltration, B/Ds would be considered "aware" of an incident.
- Should a B/D receive reliable information from an external entity indicating unauthorised disclosure, this confirmation would constitute "awareness" of an incident.
- In the event of a ransomware attack where the B/D finds encrypted files and a ransom note from attackers, the B/D would be regarded as “aware” once the attack is verified internally.

The point of awareness is not necessarily when an anomaly is initially spotted, but after a preliminary investigation affirms that a security event has indeed taken place. The specifics of the incident will influence the timeline for confirming an event.

It is critical that B/Ds respond immediately upon detection or notification of a potential incident by initiating a preliminary investigation to determine whether an incident has indeed occurred. This initial stage is pivotal and should not be mistaken for a period of “awareness”. Only when this investigation corroborates the incident with a reasonable degree of certainty is the B/D officially “aware”.

However, the focus should remain on swift action to investigate a security event and, if confirmed, to take corrective measures and report accordingly. The early reporting of suspected security incidents can significantly benefit the Government by contributing to the protection of collective security and fostering a robust and secure environment. It should be noted that after an initial report, B/Ds shall update the OGCIO if subsequent investigations reveal that the suspected security incident did not occur.

A post-incident report should be submitted to GIRO-SO no later than one week after the incident is resolved. For those cases that require a longer time to complete the investigation, the concerned departmental ISIRT shall submit interim reports to the GIRO-SO on the latest recovery and investigation status according to the following:

- Submit to the GIRO-SO the first interim report no later than 14 days after the incident was first reported; and
- Submit to the GIRO-SO the progress of the incident investigation on a three months' interval until the case is closed to keep management informed on the status.

A sample report is prepared in **Annex C.3.1** for reference.

(b) Escalation

The escalation procedure defines the way to escalate the incident to management and relevant parties to ensure that important decisions are promptly taken.

In the course of an incident, when many urgent issues have to be addressed, it could be difficult to find the proper person to handle a variety of matters. Important contact lists for addressing legal, technical, and managerial issues should be prepared in advance to facilitate different stages of security incident handling. As such, establishing an escalation procedure contributes a major task in the preparation and planning stage.

An escalation procedure will set out the points of contact (both internal and external), with corresponding contact information, at various levels for notification based on the type and severity of impact caused by the incident.

Escalation procedures may be different for different kinds of incidents, in terms of the contact points and follow-up actions. Specific contact lists should be maintained to handle different kinds of incidents that involve different expertise or management decisions.

Some recommendations on escalation procedure together with a sample escalation procedure are set out in **Annex D** for reference. A typical workflow on reporting and escalation of government security incidents is also illustrated in **Annex E** for reference.

6.2.3 Response procedures

Depending on different systems and management requirements, examples of incident handling procedures may include:

- Assess the impact and damage of the incident.
- Resume the system to normal operation in the shortest possible time.
- Minimise the impact to other systems.
- Avoid further incidents.

- Identify the root cause of the incident.
- Collect evidence to support subsequent case investigation.
- Update policies and procedures as needed.

Some incidents may be too complicated or large in scale that it is difficult to address all issues at the same time. Defining priorities is essential to allow the personnel involved to focus on the most critical events first. The following are some suggested priorities to be focused on:

- Protect human life and safety.
- Protect critical resources.
- Protect sensitive or important data which is costly when lost or damaged.
- Prevent damage to systems with costly downtime and recovery cost.
- Minimise disruption of service.
- Protect public image of the B/D or the Government as a whole.

6.2.4 Recovery Plan

An effective recovery plan is critical for restoring systems to normal operations after a security incident. The recovery plan should be comprehensive, well-documented, and include steps to ensure the security and integrity of the system upon restoration.

The recovery plan should cover:

- The procedures for damage assessment and identification of affected services.
- The prioritisation of system restoration and service resumption.
- The steps to securely re-install damaged or compromised components.
- The verification process to ensure systems are restored to a state of normalcy.
- Communication protocols for notifying relevant parties about the status of recovery.

The recovery procedure should encompass the following steps:

- Conduct a thorough damage assessment to determine the extent and impact of the incident.
- Determine the order in which functions and services should be restored, prioritising essential services and those impacting the majority of users.
- Re-install damaged or deleted files from a trusted source, ensuring the integrity and security of the software.
- Resume functions/services in a controlled manner, starting with the most critical services.
- Verify that the system has been restored to normal operations and that no traces of the security incident remain.
- Inform all related parties about the resumption of system operations, ensuring that operators, administrators, and senior management are aware of the current status.

- Turn off any services that are not essential to minimise the system's attack surface.
- Document all actions taken during the recovery process.

Section 9 below provides a reference model for dealing with security incidents, in particular containment, eradication, and recovery processes.

6.2.5 Communication Plan

Communication procedures with stakeholders and the general public should be established. Communication is essential to control the messaging surrounding the incident, including where, when, what and how this messaging is delivered. Internal communication is necessary for an effective response and recovery, and external communication is indispensable for safeguarding the government's image. Uncontrolled communication about an incident can have serious consequences. Only duly mandated and prepared personnel should be allowed to communicate on behalf of B/Ds to tell what is necessary, at the best moment, and in the appropriate form.

An effective communication plan should begin by identifying the key audiences that need to be informed during an incident. These typically include internal stakeholders such as users, management, and the incident response team and external stakeholders like citizens, partners, regulators, and the media. For each audience, the plan should designate specific messages, channels for communication, and the frequency with which updates should be provided.

The plan should detail the communication infrastructure, including primary and backup communication methods, to ensure uninterrupted information flow. This could involve emails, internal bulletins, press releases, social media, and press conferences. The infrastructure must be robust enough to handle the increased communication volume during a crisis.

Roles and responsibilities must be clearly defined within the communication plan. This includes appointing a spokesperson or a team of spokespersons trained in crisis communication who will deliver messages to the public and media. There should also be protocols for the approval and dissemination of messages to ensure consistency and accuracy.

The plan should also include pre-drafted templates for various scenarios to expedite communication. These templates can be quickly adapted to fit the specific details of an incident, ensuring a rapid response.

The communication plan must be flexible and adapt to the incident's changing nature. It should include a feedback loop to assess the communication's effectiveness and make necessary adjustments. After the incident is resolved, reviewing the communication process is essential to identify what worked well and

what could be improved for future incidents. This review process ensures that the communication plan is a living document that evolves based on past experiences.

6.2.6 Post-incident review procedures

The post-incident review is an essential component of the security incident response plan. It thoroughly analyses the incident, its response, and the recovery steps. The post-incident review procedures should be methodical and documented, incorporating lessons learned to improve future response and prevention measures. The review should evaluate the security incident's handling, identify successes and failures, and detail actions to improve future incident response capabilities. The review should encompass:

- The initial detection and reporting of the incident.
- The effectiveness of the response and containment strategies.
- The accuracy and efficiency of the communication plan execution.
- The adequacy of the recovery plan and its execution.
- The restoration of normal operations and services.
- The process of evidence preservation and its role in the analysis.

The review procedure should be structured as follows:

- The review should be initiated after the recovery phase and normal operations are restored.
- All documentation and logs related to the incident should be collected and reviewed to reconstruct the timeline and actions taken.
- Evaluate the response performance against the established metrics and identify any deviations from the response plan.
- Conduct meetings with the incident response team, management, and other relevant stakeholders to discuss the incident and gather feedback.
- Prepare a comprehensive report that includes:
  - A summary of the incident and its impact.
  - The strengths and weaknesses of the response.
  - Recommendations for future improvement.
  - Actionable steps to address identified weaknesses.
- A meeting should be held to discuss the report findings, ensuring that all stakeholders have an understanding of the outcomes and the necessary improvements.

The incident response team shall be responsible for the following:

- Tracking the implementation of improvements identified during the review.
- Updating policies, procedures, and response plans as required.
- Conducting training and awareness sessions to address the gaps identified.

- Re-evaluating metrics and adjusting them to better measure future incident responses.

Records of all post-incident reviews should be maintained to inform future incident responses and compliance requirements. These records should be secure and accessible only to authorised personnel. The post-incident review process should be iterative, with each incident providing insights for continuous improvement in the security incident response plan.

6.3 Planning of Training and Education

B/Ds shall ensure all staff observe and follow the security incident response plan for information systems accordingly. Staff should be familiar with the procedures to handle the incident from incident reporting, identification, and taking the appropriate actions to recover the system to normal operation. Drills on incident handling should also be organised regularly for staff to practise the procedures. B/Ds shall also participate in security drills designated by OGCIO. After a drill is conducted, the result should be reviewed and recommendations should be proposed to improve the incident handling procedures where appropriate.

In addition, sufficient training for system operation and support staff on security precaution knowledge is also important, in order to strengthen the security protection of the system or functional area, and reduce the chance that an incident may occur. As end users are often the first to notice that something is wrong, they should be encouraged to report anomalies or suspected breaches of security.

7. Detection and Reporting

7.1 Detection Measure

B/Ds should ensure detection and monitoring mechanism to detect security events is in place. B/Ds should detect and report the occurrence of an information security event aided by the following:

- Alerts from network monitoring devices, such as firewalls, network flow analysis tools, or web filtering tools.
- Alerts from security monitoring devices, such as intrusion detection systems, intrusion prevention systems, anti-malware solutions, log monitoring systems, or security information management systems.
- Analysis of log information from devices, services, hosts, and various systems.
- Reports from users or help desk.
- External notifications coming from outsiders such as threat intelligence platforms, other ISIRTs, telecommunication service providers, Internet service providers (ISPs), general public, media, or external service providers.

ISIRT should maintain an inventory for all information security events of the B/D.

7.2 Reporting

A staff should follow the reporting procedures to bring the security events to the attention of the ISIRT. It is essential that all staff are well aware of and have access to the report procedures for reporting different types of possible information security events. The following information should be the basis of reporting an information security event:

- Date/time for detection
- Systems affected
- Observations
- Contact information of the person who reports the security event

8. Assessment and Decision

Upon discovery of suspicious activities, the information system's user, operator or administrator should follow the predefined reporting procedure to report the incident to the respective information system manager. A standard security incident report form may be used to collect information, and to support further investigation and analysis. On the other hand, monitoring tools, such as intrusion detection tools and system audit logs, can be used to aid in identifying unauthorised or abnormal activities.

After abnormality has been detected, the respective information system manager should start to identify the incident, which involves the following steps:

- Determine if an incident has occurred and perform a preliminary assessment.
- Log the incident.
- Obtain system snapshots, if necessary.

To determine if an incident has occurred, B/Ds should consider the following circumstances, including but not be limited to:

- whether the concerned system is deployed in the Government;
- if the concerned system is deployed not in the Government,

(i) whether the system is being provided and maintained by the Government; and

(ii) whether the incident is caused by vulnerabilities of the system or factors not under the control of the Government; for example, the party who deployed the system has done something at fault or omitted doing something against the advice of the Government.

For instance, a B/D discovers a vulnerability in its provided and maintained system which is deployed not in the Government. Subsequently, the B/D makes available patch for the vulnerability and informs the users who deployed the system to install the patch. If the users fail to do so and then the system deployed is hacked, this should normally not be regarded as a government security incident. It also excludes the case in which a security breach occurred on a smart phone installed with a mobile app with security patch already available but the user has failed to install the patch.

8.1 Assessment of Incident

First of all, the respective information system manager should determine whether or not an incident has actually occurred. However, it is often difficult to determine whether the abnormality found is a symptom of an incident. Some evidences may reveal that the abnormality is caused by something else, for example, hardware failures or user errors.

To determine if an abnormality is a result of system problems or actual incidents, ISIRT should collect information about the detection of an information security event and seek any clarification from the person who reports the security event. Advice from GIRO-SO could be sought, when needed, if there are signs indicating the potential for an information security incident. Some typical indications of an incident that deserve special attention, typical security incidents as well as the criteria to be considered when determining the scope and impact of the incident are suggested in **Annex F** for reference.

8.2 Escalation

After an event is identified to be an information security incident, the information system manager should then determine the type of the incident, and assess its scope, damage and impact in order to effectively deal with it. This initial analysis process plays a critical role in understanding the incident and formulating an appropriate response. By implementing a structured initial analysis process, we can ensure that the incident is thoroughly evaluated and that the necessary precautions and defensive measures are promptly taken. A standardised checklist that serves as a guide for gathering incident details and evaluating critical factors should be leveraged to aid in this process.

The checklist should integrate seamlessly into the escalation process when notifying the appropriate parties and escalating the incident to the appropriate level. When describing the incident during the escalation process, the following information is suggested to be included:

A. ***Incident Details:*** Capture the date and time of the incident, along with a brief summary description. This information will provide a snapshot of the incident's timeline and nature.

    1. ***Date and Time:*** Record the exact date and time when the incident occurred or was first detected. This timestamp will serve as a reference point for tracking the incident's progression and response timeline.
    2. ***Incident Summary:*** Provide a concise description of the incident. Include relevant details such as the nature of the incident (e.g., security breach, system outage, data loss), the affected system(s), and any initial observations

or symptoms. This summary will help stakeholders quickly grasp the incident's context and initiate appropriate response actions.

3. ***Incident Classification:*** Classify the incident based on predefined categories or severity levels. Common classifications may include security incidents, technical failures, human errors, or natural disasters. Assigning a classification to the incident aids in prioritising response efforts and allocating resources effectively.
4. ***Incident Source:*** Identify the source or origin of the incident, if known. This could be a specific event, action, or external factor that triggered the incident. Understanding the incident source can provide valuable insights into potential causes and assist in identifying preventive measures.
5. ***Reporting Party:*** Note the individual or team that reported the incident. Include their contact information for further communication or clarification, if necessary. This information helps establish a direct line of communication with the reporting party for additional incident details or updates.
6. ***Notification and Escalation:*** Document any initial notifications or escalations made regarding the incident. Include the individuals or teams notified, the communication channels used, and the time of notification. This information can help ensure that the incident response process is properly initiated and communicated to the relevant stakeholders.
    i. Informed Parties: Document which parties were informed about the incident, including HKPF, PCPD, and media if relevant.
    ii. Action Taken: Record the immediate actions taken following the incident. This could include isolation of the affected system, initiation of forensics, or activation of a crisis management team.

B. ***System Information:*** Include details about the affected system(s) and their respective owners. If multiple departments co-own a system, note the relevant departments involved. Understanding ownership is vital for effective communication and collaboration.

1. ***System Owner Contact Information:*** Provide a sub-field to capture the contact details (name, email, phone number) of the system owner or the person responsible for the affected system. This information will facilitate communication and coordination during the incident response.

2. ***System Criticality:*** The system criticality helps determine the level of impact and urgency associated with the incident. Consider the following factors when assessing system criticality:

    2.1. ***System Tiering:*** System tier(s) assigned to each affected system.
    2.2. ***Business Impact:*** Evaluate the impact that the loss or degradation of the affected system would have on critical business operations. Consider factors such as revenue generation, user service, regulatory compliance, and reputation.
    2.3. ***Availability Requirements:*** Determine the expected level of system availability based on business and operational needs. Consider factors

such as service level agreements (SLAs), uptime requirements, and the system's role in supporting time-sensitive processes.

2.4. ***Data Sensitivity:*** Assess the sensitivity and confidentiality of the data processed, stored, or transmitted by the affected system.

2.5. ***Recovery Time Objectives (RTO):*** The RTO represents the maximum tolerable duration for restoring the system to full functionality after an incident. It helps prioritise response efforts and allocate resources effectively.

2.6. ***Recovery Point Objectives (RPO):*** The RPO represents the maximum tolerable amount of data that could be lost during recovery. It helps establish backup and data recovery strategies to minimise potential data loss.

3. ***System Description***: Provide an overview of the system impacted by the incident. Include details such as the purpose of the system/application, its primary functionalities, and the role it plays in supporting business processes. This description will help stakeholders understand the importance of the application and its relevance to the B/D's operations.

    3.1. ***Workflow Overview***: Describe the typical workflow or process flow within the system. Identify the key steps, actions, or interactions involved in using the application to achieve specific outcomes. This overview will provide a high-level understanding of how the application is used and its critical paths.

    3.2. ***Functionalities Affected:*** Identify the specific functionalities or features of the system that have been impacted by the incident. Describe the extent to which these functionalities are affected and the potential consequences of their unavailability or degradation. Understanding the impacted functionalities will help assess the severity of the incident and prioritise response actions.

    3.3. ***System Dependencies:*** Identify and document any dependencies that the affected system has on other systems/applications or services. This can include databases, APIs, network connections, or third-party integrations. Understanding these dependencies is crucial for assessing the potential impact of the incident on interconnected systems.

    3.4. ***Interactions with Users:*** Describe how users interact with the system. This can include user interfaces, input mechanisms, or communication channels. Understanding the user interactions will help assess the impact of the incident on user experience, productivity, and user satisfaction.

4. ***System Documentation:*** Include a sub-field to note the availability of system documentation, such as user manuals, or architecture diagrams. This information will assist the incident response team in gaining a comprehensive understanding of the system's structure and functionalities.

    4.1. ***User Manuals***: Document the availability of user manuals or guides associated with the affected system. These manuals provide detailed instructions on the system's setup, configuration, and operation. Note whether the manuals are readily accessible and if they cover relevant aspects of the system that are impacted by the incident. Having user

manuals at hand helps the incident response team understand the intended use of the system, its features, and any specific configuration requirements.

4.2. ***Architecture Diagrams:*** Document the availability of architecture diagrams that depict the affected system's overall design and integration with other systems or components. Architecture diagrams provide insights into the system's modules, interfaces, and dependencies. Indicate whether architecture diagrams are accessible and if they accurately represent the current state of the system. Understanding the system's architecture helps in identifying potential weaknesses, assessing the impact of the incident on the system's functionalities, and planning an effective response.

4.3. ***Backup and Recovery Procedures:*** Attach the backup and recovery procedures in place for the affected system. Include details such as backup frequency, storage location, and the availability of recent backups. This information will be valuable for assessing the recovery options and planning the restoration process.

4.4. ***Other Relevant Documentation:*** Consider any additional documentation that may be relevant to the affected system. This could include system specifications, configuration guides, security policies, or any other documentation that provides insights into the system's structure, configuration, or security controls. Note the availability and accessibility of such documentation. Additional documentation enhances the incident response team's understanding of the system and assists in making informed decisions throughout the investigation and mitigation process.

5. ***System Configuration:*** Include a sub-field to document the configuration details of the affected system, such as hardware specifications, software versions, and installed patches. This information will help in understanding the system's vulnerabilities and potential areas of compromise.

5.1. ***Hardware Specifications:*** Document the hardware specifications of the affected system. This includes details such as the processor type and speed, amount of RAM, storage capacity, and any other relevant hardware components. Understanding the hardware specifications helps in assessing the system's capabilities, performance, and potential impact on incident response activities.

5.2. ***Software Versions:*** Identify and document the software versions installed on the affected system. This includes the operating system, applications, frameworks, libraries, and any other software components. Specify the exact version numbers to provide precise information. Knowing the software versions helps in identifying known vulnerabilities, security patches, and potential areas of compromise.

5.3. ***Installed Patches:*** Document the installed patches and updates on the affected system. This includes operating system patches, application updates, firmware updates, and any other relevant patches that have been applied. Specify the patch names, version numbers, and dates of installation. Understanding the patch status helps in assessing the

system's resilience to known vulnerabilities and determining if any missing patches could have contributed to the incident.

5.4. ***Configuration Changes:*** Document any recent configuration changes made to the affected system. This includes changes to firewall rules, user privileges, network settings, or any other relevant configuration modifications. Specify the nature of the changes, when they were made, and the individuals responsible. Tracking configuration changes helps in identifying potential misconfigurations, unauthorised modifications, or policy violations that may have contributed to the incident.

6. ***Network Diagram:*** Document the internal IP addresses associated with the incident and provide a network topology relevant to the incident. This will assist in identifying potential attack vectors and understanding the incident's scope.

6.1. ***Network Topology Overview:*** Provide an overview of the network topology relevant to the incident. This includes the layout and structure of the network infrastructure, including routers, switches, firewalls, and other network devices. Describe how different components are interconnected and the overall architecture of the network.

6.2. ***Internal IP Addresses:*** Document the internal IP addresses associated with the incident. This includes the IP addresses of the affected systems, servers, and network devices. By noting these IP addresses, you can identify the specific components involved in the incident and track their connectivity within the network.

6.3. ***Subnet Information:*** Identify the subnets or network segments relevant to the incident. This includes the range of IP addresses associated with each subnet and any relevant subnet masks. Understanding the subnet structure will help in analyzing network traffic patterns and potential areas of vulnerability.

6.4. ***Network Device Configuration:*** Document the configuration details of network devices involved in the incident, such as routers, switches, firewalls, and intrusion detection systems. Include relevant information such as device models, firmware versions, and any specific configurations or rules that may impact the incident.

6.5. ***Attack Vectors:*** Analyse the network diagram to identify potential attack vectors or paths that could be exploited by an attacker. This includes examining the connectivity between systems, access control mechanisms, and potential security weaknesses in the network infrastructure. By identifying the possible attack vectors, you can assess the incident's scope and potential impact on the network.

6.6. ***Incident Scope:*** Based on the network diagram, assess the scope of the incident in terms of the affected network segments, systems, and services. Determine the extent to which the incident has spread within the network and identify any critical assets or sensitive areas that may be

at risk. This assessment will help prioritise response actions and containment efforts.

C. ***Indicators of Compromise (IoCs):*** List any impacted IP addresses, hostnames, and usernames related to the incident. Identify suspicious files or processes and any evidence of unauthorised access or activities.

1. ***Impacted IP Addresses:*** Identify and list the IP addresses that have been impacted or associated with the incident. This includes both internal and external IP addresses that are relevant to the investigation. Documenting impacted IP addresses helps in tracking the source and destination of network traffic, identifying potential attack vectors, and understanding the scope of the incident.
2. ***Impacted Hostnames:*** Document any hostnames or domain names that have been impacted by the incident. This could include compromised websites, unauthorised subdomains, or unusual DNS resolution patterns. Listing impacted hostnames provides insights into potential areas of compromise and indicates which systems or services may have been targeted.
3. ***Impacted Usernames:*** Identify any usernames or accounts that have been affected or compromised during the incident. This includes user accounts associated with the impacted systems, applications, or services. Documenting impacted usernames helps in tracking unauthorised access, identifying potential insider threats, and assessing the extent of the compromise.
4. ***Suspicious Files or Processes:*** Document any suspicious files or processes discovered during the investigation. This includes malware, malicious scripts, unauthorised executables, or any other files or processes that raise suspicion. Provide details such as file names, file locations, and associated process names, if applicable. Identifying suspicious files or processes helps in understanding the nature of the incident, detecting potential malware infections, and initiating appropriate response actions.
5. ***Evidence of Unauthorised Access or Activities:*** Document any evidence or indicators that suggest unauthorised access or malicious activities. This could include log entries, timestamps, unusual network traffic patterns, or any other anomalies observed during the investigation. Capturing evidence of unauthorised access or activities helps in understanding the attacker's techniques, identifying potential data breaches, and mitigating further risks.

D. ***Remarks:*** In this section, include supporting details for each indicator of compromise. Explain why the indicators are considered a compromise and indicate the confidence level. Additionally, note any additional observations or information relevant to the incident.

1. ***Indicator of Compromise (IoCs) Details:*** For each identified indicator of compromise (IP addresses, hostnames, usernames, suspicious files or processes, evidence of unauthorised access or activities), provide supporting details explaining why they are considered a compromise. Include specific observations, behaviours, or characteristics that led to their inclusion as

indicators. This can include log entries, network traffic analysis, system logs, or any other evidence collected during the investigation.

2. ***Rationale for Compromise:*** Explain the rationale behind considering each indicator as a compromise. Describe the potential impact or risk associated with the indicator and how it aligns with known attack patterns, vulnerabilities, or malicious activities. This rationale will provide context and justification for the inclusion of each indicator as a compromise.
3. ***Confidence Level:*** Indicate the confidence level associated with each indicator of compromise. This can range from low to high, reflecting the level of certainty in the assessment. Consider factors such as the quality of evidence, reliability of sources, and the expertise of the investigators. Assigning a confidence level helps in prioritising response actions and allocating resources appropriately.
4. ***Additional Observations:*** Note any additional observations or information that are relevant to the incident but may not fit under specific indicators of compromise. This can include unusual system behaviours, findings from vulnerability assessments, or any other insights that may help in understanding the incident or its potential impact. These additional observations provide valuable context and contribute to a comprehensive understanding of the incident.

The information provided during the escalation process should be clear, concise, accurate and factual. It is imperative that B/Ds maintain constant availability of system information/documentation to support the veracity and completeness of the communication. Providing inaccurate, misleading or incomplete information may hinder the response process or may even worsen the situation. B/Ds should also consider whether some sensitive information could be given to external parties or not.

The manager of the respective information system, with the Incident Response Manager of the ISIRT as the overall coordinator, should notify the appropriate parties and escalate the incident to the appropriate level following the predefined escalation procedure.

If a B/D confirms that an incident occurs, the relevant ISIRT Commander should report the incident to GIRO-SO within 60 minutes after the incident is first identified. Reporting an incident does not mark the end of ISIRT responsibilities. ISIRT are expected to remain available and actively engaged. Leaving work immediately after reporting an incident may result in delays or gaps in the incident response process, compromising ISIRT's ability to safeguard the B/D.

For purposes of recording and co-ordination on handling of the incident, the ISIRT Commander should also complete the initial analysis and provide a Preliminary Information Security Incident Report (see **Annex C.2**) for reporting of information security incidents including, but not be limited to, the following categories (please refer to **Annex F** for further description) to the GIRO-SO.

- Abuse of information systems.

- Compromise of information systems or data assets.
- Denial of service attack (including the central or departmental Internet gateway, email systems, the government websites and/or systems delivering electronic services to the public).
- Leaking of classified data in electronic form.
- Loss of mobile devices or removable media that contain classified data.
- Masquerading.
- Massive malware infection.
- Ransomware.
- Website defacement.

Incidents that are not security related (listed below) are not required to report to the GIRO-SO. Instead, the prevailing standards and procedures on system administration and operation should be followed.

- System affected by natural disasters, e.g. typhoon, flooding, fire, etc.
- Hardware or software problem.
- Data/communication line failure.
- Power disruption.
- Scheduled system downtime or maintenance slot.
- System failure due to administration/operation error.
- Loss or destruction of classified data due to system or human error.
- Fraudulent emails or websites not affecting government systems and data.

In case of incident with major impact to government services and/or image, the GIRO-SO will closely monitor the development with ISIRT Commander. If the incident is a potential multiple point attack targeting at the Government as a whole, the Standing Office will immediately notify GIRO for information and necessary action.

In handling an event of data breach, B/D may consider to take remedial steps as below:

- Immediate gathering of essential information related to the breach.
- Adopting appropriate measures to contain the breach.
- Assessing the risk of harm.
- Considering the giving of data breach notification.

If personal data is involved in a security incident, B/D should report the case to PCPD as soon as possible by using the data breach notification form available at PCPD's web site (https://www.pcpd.org.hk/english/resources_centre/publications/forms/files/DBN_e.pdf). The data breach notification form can also be submitted online through PCPD's website

(https://www.pcpd.org.hk/english/enforcement/data_breach_notification/dbn_form.html).

In addition, B/Ds may refer to the "Guidance on Data Breach Handling and Data Breach Notifications" issued by PCPD.

(https://www.pcpd.org.hk/english/resources_centre/publications/files/guidance_note_dbn_e.pdf)

B/Ds should also notify affected individuals as far as practicable. Justifiable exception on reporting needs to be approved by the Head of B/D.

The Cyber Security and Technology Crime Bureau of HKPF should be contacted if a B/D suspects a computer crime has been committed. Advice and endorsement from the senior management of the ISIRT should be sought along with the initial analysis completion before reporting the case to HKPF. In addition, for any security incident reported to HKPF or PCPD, the GIRO-SO should also be notified for central recording and coordination support.

Please refer to **Annex D** for a sample escalation procedure and other related information about security incident escalation. A typical workflow on reporting and escalation of government security incidents is illustrated in **Annex E** for reference.

8.3 Log the Incident

All security incidents, actions taken and the corresponding results shall be recorded. The records should be stored securely with cryptography, locks or access control. This can facilitate incident identification, assessment, and provide evidence for prosecution and other useful information for subsequent stages of incident handling. Logging should be carried out throughout the whole security incident response process. An incident reference number may be assigned to each incident to facilitate follow-up and tracing during the whole incident handling process.

As a minimum requirement, the following information shall be logged:

- System events and other relevant information, such as audit logs.
- All actions taken, including the date, time and personnel involved.
- All external correspondence, including the date, time, content and parties involved.

8.4 Obtain System Snapshot

A snapshot of the compromised system should be obtained as soon as suspicious activities are detected, and as far as technically and operationally feasible. This can prevent the attacker from destroying the evidence and support subsequent case investigation, such as forensic evidence collection. The snapshot of the system may include the following items:

- System log files such as server log, network log, firewall/router log, access log, etc.
- Information of active system login or network connection, and corresponding process status.
- An image of the compromised system built for investigation purpose and as evidence for subsequent follow-up action.

9. Response to Security Incident

Response to security incident involves developing procedure to evaluate incidents and to respond in order to restore affected system components and services as soon as possible. The procedure is broadly categorised into three stages: *Containment, Eradication and Recovery* as shown in Figure 9.1 below. Understanding the activities of each stage can facilitate the development of an effective security incident response procedure.

The response procedure may not strictly follow the order of the three stages, which has to be customised to meet practical needs.

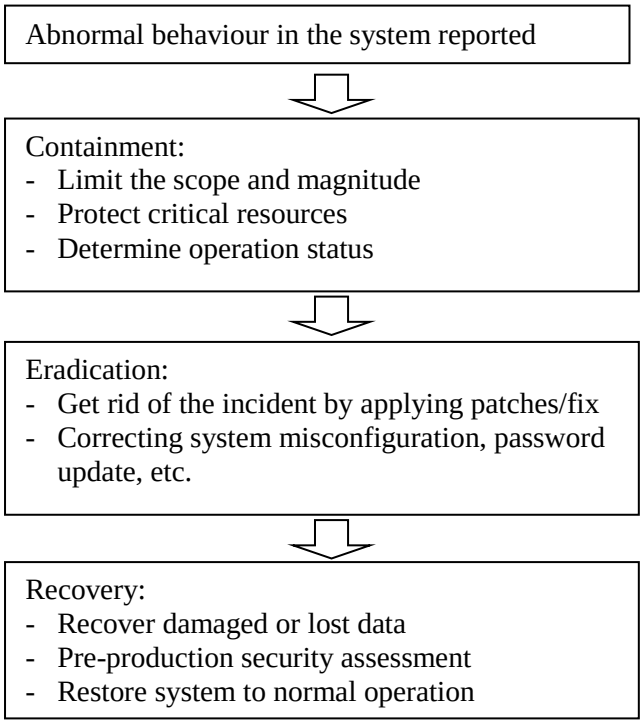


Figure 9.1 Major Stages in Security Incident Response

9.1 Containment

The first stage of response to incidents is containment. The purpose of containment is to limit the scope, magnitude and impact of an incident. There exist some incidents, like malware infection, which can spread rapidly and cause extensive damages. Hence, B/Ds should limit the extent of an incident before it causes further damages.

Strategies and procedures for responding to different incidents with different resources should be predetermined and stated clearly in the security incident response procedure. For critical action, one may also need to seek management advice and approval from the ISIRT (which may also need to consult the GIRO if necessary).

Activities in this stage may include:

- Conducting impact assessment of the incident on data and information system involved to confirm if the data or service has already been damaged by or infected in the incident.
- Protecting classified or critical information and system. For instance, move the critical information to other media (or other systems) which are separated from the compromised system or network.
- Deciding on the operation status of the compromised system.
- Building an image of the compromised system for investigation purpose and as evidence for subsequent follow-up action.
- Keeping a record of all actions taken during this stage.
- Checking any systems associated with the compromised system through shared network-based services or through any trusting relationship.

ISIRT should conduct review periodically to determine if the incident is under control. If it is not under control or it is going to have a severe impact on the B/D's core services, follow the predefined escalation procedures for crisis management.

9.1.1 Operation Status of the Compromised System

One of the important decisions to be made is whether to continue or suspend the operation and service of the compromised system. This will very much depend on the type and severity of the incident, the system requirement and the impact on public service and the image of the B/D and the Government as a whole, as well as the predefined goals and priorities in the incident response plan of the system.

Actions to be taken may include:

- Shutting down or isolating the compromised computer or system temporarily to prevent further damage to other interconnected systems, in particular for incidents that will spread rapidly, for computers with sensitive information, or to prevent the compromised system from being used to launch attack on other connected systems.
- Stopping operation of the compromised information system.
- Disabling some of the system's functions.
- Removing user access or login to the system.
- Continuing the operation to collect evidence for the incident. This may only be applied to Tier 1 information systems that could accept some risks in service interruption or data damage, and it must be handled with extreme care and under close monitoring.

9.2 Eradication

The next task following containment is eradication. Eradicating an incident is to remove the cause of the incident from the system, such as removing a malware from the infected system and media.

Prior to removing any files or stopping/killing any processes, it is advisable to collect all the necessary information, including all the log files, active network connections and process status information. It helps to collect evidence for subsequent investigation, which may be deleted or reset during system clean up.

9.2.1 Possible Actions for Incident Eradication

During the eradication stage, the following actions may need to be performed depending on the type and nature of the incidents as well as the system requirement:

- Stop or kill all processes created or activated by hacker to stop the damage and force the hacker out.
- Delete all files created by the hacker. System operators should archive the files before deletion for the purpose of case investigation.
- Eliminate all the backdoors and malicious programs installed by the hacker.
- Apply patches and fixes to vulnerabilities found on all operating systems, servers, network devices, etc. Test the system thoroughly before restoring it to normal operation.
- Correct any improper settings in the system and network, e.g. mis-configuration in firewall and router.
- In case of a malware incident, follow the advices of anti-malware tool vendor to inoculate or remove the malware from all infected systems and media as appropriate.
- Provide assurance that the backups are clean to prevent the system from being re-infected at a later stage when system recovery from backup is needed.
- Make use of some other security tools to assist in the eradication process, for instance, security scanning tools to detect any intrusion, and apply the recommended solution. These tools should be kept up-to-date with the latest detection patterns.
- Update the access passwords of all login accounts that may have been accessed by the hacker.
- In some cases, the supporting staff may need to reformat all the infected media and reinstall the system and data from backup, especially when they are not certain about the extent of the damage in a Tier 2 or above information system or it is difficult to completely clean up the system.
- Keep a record of all actions performed.

The above are only examples of commonly adopted actions during security incidents. Eradication actions may vary depending on the nature of the incident and its impact on the systems affected. On some occasions, the B/D may need to seek advice from external parties, such as HKPF, PCPD and/or the external service providers, and to make reference to other B/Ds with similar incident handling experience. Management advice and coordination support from the ISIRT and the GIRO should be sought accordingly.

9.3 Recovery

The last stage in incident response is recovery. The purpose of this stage is to restore the system to its normal operation. Examples of tasks include:

- Perform damage assessment.
- Re-install the deleted/damaged files or the whole system, whenever required, from the trusted source.
- Bring up function/service by stages, in a controlled manner, and in order of demand, e.g. the most essential services or those serving the majority may resume first.
- Verify that the restoring operation was successful and the system is back to its normal operation.
- Prior notification to all related parties on resumption of system operation, e.g. operators, administrators, senior management, and other parties involved in the escalation procedure.
- Disable unnecessary services.
- Keep a record of all actions performed.

Prior to restoring the system to normal operation, one important action is to conduct a pre-production security assessment to ensure that the compromised system and its related components are secured. It may involve the use of security scanning tools to confirm that the problem source of the incident is cleared, as well as to reveal any other possible security loopholes in the system. The assessment may focus in a particular area, or may cover the entire system, depending on the severity of the incident and the service level requirement of the system.

Approval from the senior management in the ISIRT shall be obtained for all recovery actions to be conducted, and if considered necessary, support and advice from the GIRO may also be sought.

10. Post-Incident Actions

Restoring a system to normal operation does not mark the end of a security incident handling process. It is also important to perform the necessary follow-up actions. Actions may include evaluation of the damage caused, system refinement to prevent recurrence of the incident, security policies and procedures update, and case investigation for subsequent prosecution.

Follow-up actions can lead to the following:

- Improve incident response procedure.
- Improve security measures to protect the system against future attacks.
- Prosecute those who have breached the law.
- Help others to familiarise with security incident response process.
- Help to educate those parties involved about the experience learnt.

Follow-up actions include:

- Post-incident analysis.
- Post-incident report.
- Security assessment.
- Review existing protection.
- Investigation and prosecution.

10.1 Post-Incident Analysis

Post-incident analysis involves conducting analysis on the incident and response actions for future reference. It helps to gain a better understanding of the system's threats and vulnerabilities so that more effective safeguards can be put in place.

Examples of aspects of analysis include:

- Recommended actions to prevent further attack.
- Information that is needed quickly and the way to get the information.
- Additional tools used or needed to aid in the detection and eradication process.
- Sufficiency in respect of preparation and response.
- Adequacy in communication.
- Practical difficulties.

- Damage of incident, which may include:
  (i) Manpower costs required to deal with the incident.
  (ii) Monetary cost.
  (iii) Cost of operation disruption.
  (iv) Value of data, software and hardware lost or damaged, including sensitive data disclosed.
  (v) Legal liability of entrusted confidential data.
  (vi) Public embarrassment or loss of goodwill.
- Other experiences learnt.

The analysis should be incorporated into the IT security risk management and continuous improvement processes to strengthen the security protection of the B/D and reduce the chance of an incident.

10.2 Post-Incident Report

Based on the post-incident analysis, a post-incident report should be prepared with brief description of the incident, response, recovery action, damage and experience learnt. The report should be prepared by the concerned information system manager and be disseminated to the ISIRT for reference, so that prompt preventive actions could be taken to avoid the recurrence of similar security incident in other systems and services.

The report should include the following items:

- Type, scope and extent of the incident.
- Details of events: source, time and possible method of attack, and method of discovery, etc.
- Brief description of the system under attack, including its scope and function, technical information such as system hardware, software and operating system deployed with versions, network architecture, and programming languages, etc.
- Response to the incident and eradication methods.
- Recovery procedures.
- Other experiences learnt.

The report should be submitted to the GIRO no later than one week after the security incident is resolved. A sample post-incident report is prepared in **Annex C.3.2** for reference.

10.3 Security Assessment

A periodic security risk assessment and audit exercise is recommended for systems under security exposure, especially for those that have been affected by security incident. Security review and audit of a system should be an ongoing exercise to promptly identify possible security loopholes and/or areas of improvement to the system as a result of technology advancement in both security protection as well as attack/intrusion.

Information collected during a security incident is also useful to subsequent security assessment exercises, in particular for identification of security vulnerabilities and threats of the system.

10.4 Review Existing Protection

From the post-incident analysis and periodic security assessment exercise, areas for improvement can be identified in respect of the system's security policies, procedures and protection mechanisms. Due to rapid advancement of technology, security related policies, procedures and protection mechanisms must be updated regularly to ensure the effectiveness of the overall security protection to an information system. In the case of a post-incident event, policies, standards, guidelines and procedures should also be reviewed and modified as necessary in order to align with preventive measures.

10.5 Investigation and Prosecution

If appropriate, case investigation, disciplinary action or legal prosecution against individuals who caused the incident should also be conducted.

Incidents assessed to be caused by a criminal offence should be reported to the Cyber Security and Technology Crime Bureau of HKPF for case investigation and evidence collection. Advice and endorsement from the senior management of the ISIRT should be sought before reporting the case to HKPF. B/Ds may need to follow up on legal proceedings and produce the evidence required.

If personal data is involved in a security incident, the B/D should report the case to PCPD as soon as possible. The B/D should also notify the affected individuals as far as practicable. Justifiable exceptions on reporting need to be approved by the Head of B/D.

In addition, for any security incident reported to HKPF or PCPD, the GIRO-SO should also be notified for central recording and coordination support.

*** ENDS ***

Annex A: Departmental IT Security Contacts Change Form

Name of Bureau/Department	
Role of the Officer	
☐ Departmental IT Security Officer (DITSO) ☐ Deputy DITSO ☐ Departmental Information Security Incident Response Team (ISIRT) Commander ☐ Deputy Departmental ISIRT Commander	
The officer to be replaced: _____ (*please use a separate form for each officer*)	
Contact Information	
Name:	Designation:
Office Phone No.:	Mobile Phone No. : (*For 7x24 emergency contact*)
Email Address:	
Other email contacts for receiving IT security related information:	
Informed By	
Name of DITSO / ISIRT* Commander:	Designation:
Signature of DITSO / ISIRT* Commander:	Effective Date:
Submission to IT Security Team/OGCIO	
Please submit the completed form to the IT Security Team via any of the following means: *Email:* *it_security@ogcio.gov.hk* *Fax:* *2989 6073*	

**Cross-out as appropriate*

Annex B: Checklist for Incident Response Preparation

B.1 Sample Checklist for Incident Response Preparation

	Item	Details	Status
1	Incident Monitoring and Detection	Install firewall devices and access control measures to protect important system and data resources	
		Install anti-malware and repair tools, perform scanning and update signature regularly	
		Install monitoring tools, e.g. intrusion detection system	
		Enable audit logging in system and network equipment	
2	Security Incident Response	Prepare security incident response plan	
		Design and prepare for the reporting mechanism(s)	
		Publish the reporting mechanism(s) to all staff	
		Gather contact information for all personnel to be contacted/involved, both internal and external	
		Prepare an escalation procedure	
		Publish the escalation procedure to all personnel involved	
		Publish the security incident response plan to all personnel involved	
3	Training and Education	Provide training to operation and support staff in handling security incidents	
		Ensure staff are familiar with the incident response process	

Annex C: Reporting Mechanism

C.1 Suggestions on Reporting Mechanism

Telephone hotline

This is the most convenient and rapid way of reporting incidents. Some systems may already have a hotline for handling enquiries and/or security incident reports.

For a system that is running round-the-clock, it may be necessary to provide a 24-hour hotline.

Email address

Reporting incidents through email is also an efficient way. However, if the incident is in the form of a network attack or targeted at the email system, the reporting channel may be affected. Alternative measures should be adopted to address such limitations, e.g. by using other reporting channels such as telephone or fax.

Fax number

Reporting by fax is a supplementary mechanism, in particular for the submission of detailed information that may not be reported clearly and accurately by telephone. However, the fax machine used for incident reporting should be promptly attended to, preferably by dedicated staff. Besides, special attention should also be paid to handling fax reports to prevent disclosure of the incident information to unauthorised persons. In view of these additional security measures for reporting by fax, reporting by email is often used instead as it is efficient and more cost-effective.

In person

This method is considered not effective and inconvenient. It should only be used if detailed information has to be obtained from or discussed with the person reporting the incident, or the location in question is very close to that of the incident report contact person.

C.2 Preliminary Information Security Incident Report

RESTRICTED

Incident Ref. No.: _____

(For GIRO Standing Office Use)

Preliminary Information Security Incident Report

Background Information	
Name of Bureau/Department (B/D):	
Brief description of the affected system (e.g. system name, function, URLs):	
Physical location of the affected system: ☐ Within B/D ☐ External service provider facility ☐ Central Service: _____ **System administered/operated by:** ☐ In-house staff ☐ End user ☐ Outsourced service provider	
Reporting Entity Information	
Name:	***Designation:***
Office Contact:	***24 hours Contact:***
Email Address:	***Preliminary Information Security Incident Report Submission Date:***
Incident Details	
Date/Time (Occurred):	
Date/Time (Discovered):	**Date/Time (Reported to GIRO Standing Office):**
Description of Incident: ***What Occurred*:** _____	

Initial Findings (if any):

How Occurred:

_____

Why Occurred*:*

_____

Vulnerabilities Identified*:*

_____

Categories:

- ☐ Abuse of information systems
- ☐ Compromise of information systems or data assets
- ☐ Denial of service attack
- ☐ Leaking of classified data in electronic form
- ☐ Masquerading
- ☐ Loss of mobile devices or removable media that contain classified data
- ☐ Massive malware infection
- ☐ Ransomware
- ☐ Website defacement
- ☐ Others: _____

Components/Assets Affected:

- ☐ Email System
- ☐ Hardware
- ☐ Information / Data
- ☐ Network
- ☐ Software
- ☐ Website
- ☐ Others: _____

Details of Components/Assets Affected:

_____

Impacts:

- ☐ Confidentiality
- ☐ Integrity
- ☐ Availability
- ☐ Government's image
- ☐ Others: _____

Please provide details on the impact and service interruption period (if any):

_____

Is classified data involved in the incident?

☐ Yes, ☐RESTRICTED ☐CONFIDENTIAL data is involved

☐ No

Please provide details on the classified data involved (e.g. whether the data is encrypted, type of the data, etc.):

_____

Is personal data involved in the incident?

☐ Yes, What personal data is involved: _____

☐ No

Internal Individuals/Entities Notified:

☐ Information System Manager ☐ Information Coordinator

☐ Incident Response Manager ☐ ISIRT Commander

☐ GIRO Standing Office ☐ Others: _____

External Individuals/Entities Notified (date/time):

☐ CSTCB of HKPF: _____

Case Ref. No.: _____

☐ PCPD: _____

☐ Others: _____

Actions Taken to Resolve Incident:

Actions Planned to Resolve Incident:

Outstanding Actions:

Current System Status:

Other Information:

Media / Public Enquiry (If applicable)	
No. of Media Enquiry Received:	**No. of Public Enquiry Received:**

C.3.1 Interim-Incident Report

RESTRICTED

Incident Ref. No.: _____

(For GIRO Standing Office Use)

Interim-Incident Report

Background Information	
Name of Bureau/Department (B/D):	
Brief description of the affected system (e.g. system name, function, URLs):	
Physical location of the affected system: ☐ Within B/D ☐ External service provider facility ☐ Central Service: _____ **System administered/operated by:** ☐ In-house staff ☐ End user ☐ Outsourced service provider	
Reporting Entity Information	
Name:	***Designation:***
Office Contact:	***24 hours Contact:***
Email Address:	***Interim-Incident Report Submission Date:***
Incident Details	
Date/Time (Occurred):	
Date/Time (Discovered):	**Date/Time (Reported to GIRO Standing Office):**
Description of Incident: ***What Occurred:*** _____	

Findings:

How Occurred:

_____

Why Occurred*:*

_____

Vulnerabilities Identified*:*

_____

Status Update:

C.3.2 Post-Incident Report

RESTRICTED

Incident Ref. No.: _____

(For GIRO Standing Office Use)

Post-Incident Report

Background Information	
Name of Bureau/Department (B/D):	
Brief description of the affected system (e.g. system name, function, URLs):	
Physical location of the affected system: ☐ Within B/D ☐ External service provider facility ☐ Central Service: _____ **System administered/operated by:** ☐ In-house staff ☐ End user ☐ Outsourced service provider	
Reporting Entity Information	
Name:	***Designation:***
Office Contact:	***24 hours Contact:***
Email Address:	***Post-Incident Report Submission Date:***
Incident Details	
Date/Time (Occurred):	
Date/Time (Discovered):	**Date/Time (Reported to GIRO Standing Office):**
Description of Incident: ***What Occurred*:** _____	

Findings:

How Occurred:

_____

Why Occurred*:*

_____

Vulnerabilities Identified*:*

_____

Categories:

- ☐ Abuse of information systems
- ☐ Compromise of information systems or data assets
- ☐ Denial of service attack
- ☐ Leaking of classified data in electronic form
- ☐ Masquerading
- ☐ Loss of mobile devices or removable media that contain classified data
- ☐ Massive malware infection
- ☐ Ransomware
- ☐ Website defacement
- ☐ Others: _____

Components/Assets Affected:

- ☐ Email System
- ☐ Hardware
- ☐ Information / Data
- ☐ Network
- ☐ Software
- ☐ Website
- ☐ Others: _____

Details of Components/Assets Affected:

_____

Other Affected Sites/Systems (if any):

_____

Impacts:

- ☐ Confidentiality
- ☐ Integrity
- ☐ Availability
- ☐ Government's image
- ☐ Others: _____

Please provide details on the impact and service interruption period (if any):

_____

Internal Individuals/Entities Notified:

☐ Information System Manager ☐ Information Coordinator

☐ Incident Response Manager ☐ ISIRT Commander

☐ GIRO Standing Office ☐ Others: _____

External Individuals/Entities Notified (date/time):

☐ CSTCB of HKPF: _____

Case Ref. No.: _____

☐ PCPD: _____

☐ Others: _____

***Investigation Result from HKPF (if available)*:**

_____

Events Sequence:

Date / Time	***Event***

Actions Taken and Result:

Current System Status:

Personnel Involved:

Name	***Designation***	***Phone No.***	***Email Address.***	***Role***

Perpetrator Details (if any):

_____

Perpetrator(s) Involved:

☐ Person ☐ Organised Group

☐ No Perpetrator ☐ Unknown

☐ Other: _____

Perceived Motivation for Incident:

☐ Financial Gain ☐ Hacking

☐ Political ☐ Revenge

☐ Unknown ☐ Other: _____

Malware Details (if any):

If classified data was involved in the incident, please provide details (e.g. whether the data is encrypted, type of the data, etc.):

Classification: ☐RESTRICTED ☐CONFIDENTIAL

Remarks:

_____

If personal data was involved in the incident, please provide details (e.g. number of affected individuals, type of personal data (e.g. HKID) involved, whether the affected individuals have been informed, etc.):

No. of affected individuals: _____

(breakdown the number of internal staff and citizens)

Type of personal data involved:

_____

Whether the affected individuals have been informed: Yes/No. If No, why: _____ Remarks: _____
Cost Factor (including loss caused by the incident and the recovery cost/manpower):
Recommended Action to Prevent Recurrence:
Experience Learnt:

Media / Public Enquiry (If applicable)	
No. of Media Enquiry Received:	**No. of Public Enquiry Received:**

Annex D: Escalation Procedure

D.1 Parties to be Notified

The parties involved in the escalation procedure would depend on the nature and severity of the incident, as well as system requirements. For example, an outbreak of an incident initially may only involve internal support staff to tackle the problem. The senior management may be alerted at a later stage. If the problem cannot be solved, it may need to seek advice from external supporting parties, such as service contractors, product vendors, HKPF, and PCPD, as appropriate.

Every system should have a specific escalation procedure and points of contact which meet their specific operational needs.

Different persons may be notified at different stages, depending on the damage or sensitivity of the system. Points of contact may include, but are not limited to, the following parties:

Internal:

- Operation and technical support staff.
- Respective information system manager, the ISIRT/DITSO and the GIRO Standing Office.
- Operation team of the affected/involved systems or functions.
- The Cyber Security and Technology Crime Bureau of HKPF.
- Information Coordinator for preparation of line-to-take and dissemination of information to the media.

External:

- Supporting vendors, including the system's hardware or software vendors, application developers, and security consultants, etc.
- Service providers (e.g. telecommunication service providers, ISP).
- The Office of the Privacy Commissioner for Personal Data.
- The affected individuals.

D.2 Contact List

Contact list of the parties involved should include the following information:

- Name of a dedicated person.
- His/her post title.
- Email addresses.
- Contact phone numbers (for 24 hours contact, if necessary).
- Fax number.

D.3 Sample Escalation Procedure

The following is a sample escalation procedure for an information security incident.

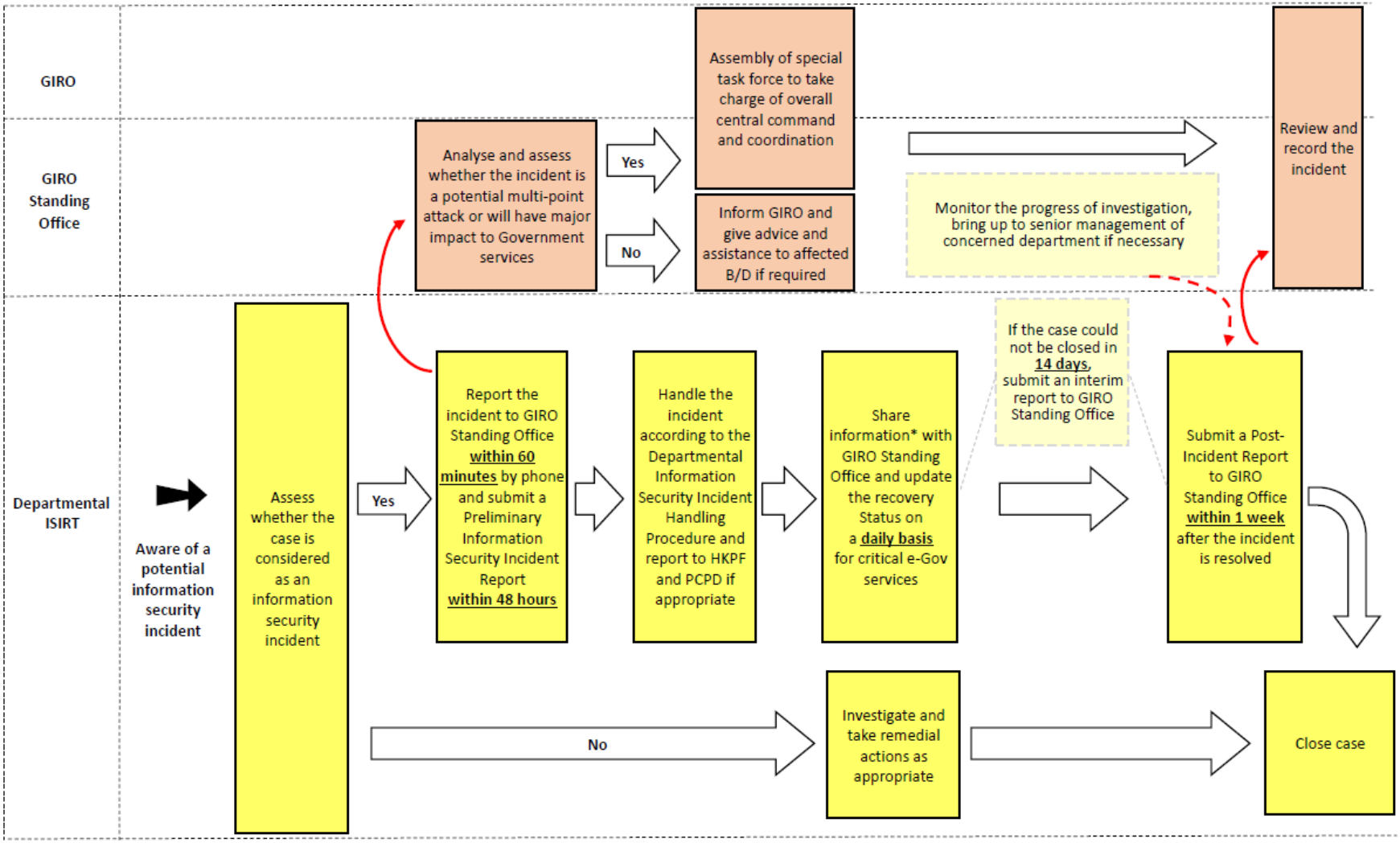
Duration of report	**Contact List**	**Contact method**
Within 15 minutes of the incident	Respective information system manager, technical support staff, related supporting vendors and service contractors	*Mobile phone & vendors' 24 hours hotline*
Within 30 minutes of the incident	All of the above, Incident Response Manager and Information Coordinator of the ISIRT	*Mobile phone*
Within 60 minutes of the incident	Notify the ISIRT Commander	*Mobile phone*
Within 60 minutes of the incident	The ISIRT to notify the GIRO (And to provide the Preliminary Information Security Incident Report to GIRO Standing Office within 48 hours of the incident)	*Pre-arranged hotline or email*
Every 30 minutes onward	All of the above for status update	*Mobile phone or email*
Periodic	The ISIRT to update GIRO on the status of the incident	*Email*
After system recovery (within 1 week)	The ISIRT to submit a post-incident report to GIRO for record	*Email*
If suspected to involve criminal offence, subject to ISIRT's decision	Report to HKPF for case investigation	*Pre-arranged hotline*
If personal data is involved	Report to Privacy Commissioner for Personal Data (And notify affected individuals as far as practicable)	*Pre-arranged hotline or any other means*

Reports should include the following information:

- Brief description of the problem: what, when and how did it occur and the duration.
- Indicate if the system is under attack.
- Indicate if the attacker, if any, is still active on the system.
- Indicate if it is a local source of attack.
- Status update on system recovery

Annex E: Workflow of Information Security Incident Response Mechanism

A typical workflow on reporting and escalation of government security incidents is illustrated in the following flowchart:



*Information to share include assessment on scope, damage and impact of the incident, actions being or to be taken, line-to-take or enquires from media, if any.

Annex F: Identification of Incident

F.1 Typical Types and Indicators of Security Incidents

To determine if an abnormality is a result of system problems or actual incidents, there are certain indications of an incident that deserve special attention. Typical types and indications of security incidents include any of the following. This list is indicative only and non-exhaustive.

IT Security Incident	Description	Indicators	Initial Analysis/Handling	Information required for identification/analysis
Abuse of information systems	Abuse occurs when someone uses an information system for other than permitted purposes, e.g. to cause an adverse impact to the information assets.	• Unusual or unauthorised activities on the information system. • Evidence of deliberate misuse or unauthorised access. • Actions causing an adverse impact on information assets.	1. Collect information about the reported activities or incidents of abuse. 2. Identify the individuals or accounts involved. 3. Analyse system logs and audit trails to determine the extent of the abuse. 4. Interview relevant personnel or users to gather additional information. 5. Assess the impact of the abuse on information assets and determine any immediate actions required, such as revoking access or	• Logs of system access and user activity. • Records of unauthorised system actions or policy violations. • Communication logs (emails, chat logs, etc.) related to the abuse incident. • Any captured evidence, such as screenshots or recordings.

			blocking unauthorised activities. 6. If necessary, document the incident and report it to the appropriate stakeholders or authorities.	
Compromise of information systems or data assets	Physical or logical access to the whole or part of an information system and/or its data without the prior permission of the system owner. A compromise can occur through manual interaction by the untrusted source or automation.	• Unusual account activity, such as unauthorised access attempts or privilege escalation. • Anomalous system or network log entries. • Unauthorised changes to system configurations or data. • Presence of unknown or unauthorised user accounts. • Unexpected system behaviour or performance degradation. • Evidence of unauthorised	1. Identify and isolate affected systems or accounts to prevent further compromise. 2. Collect and preserve relevant logs and system artefacts for analysis. 3. Analyse system logs, network traffic, and other available data to identify the entry point and extent of the compromise. 4. Conduct a thorough investigation to determine the nature of the compromise, including the identification of any malware, backdoors, or unauthorised modifications. 5. Assess the impact of the compromise, such as data exfiltration or unauthorised access, and	• Logs indicating unauthorised access or suspicious activities. • System or application logs showing signs of compromise or intrusion. • Malware samples (if available). • Network traffic logs indicating communication with malicious entities. • User account credentials or accounts used for the compromise. • Any captured evidence, such as system snapshots or forensic images.

		access or exfiltration of data. • Indicators of malware or intrusion detected by security tools. • Unauthorised remote access or control of systems. • Unusual network traffic patterns or connections.	take appropriate remedial actions to mitigate further damage. 6. Notify relevant stakeholders, such as system owners, users, and management, about the incident.	
Denial of service attack	Prevention of the use of information resources, either intentionally or unintentionally, which affects the availability of the information resources. Examples of such attacks are SYN flood, Ping of death and Ping flooding, which try to overload either the information system or the network connection	• Unusual increase in network traffic or network congestion. • Degraded or disrupted system performance. • Inability to access or use specific resources or services. • Unusual patterns of incoming requests or connections.	1. Identify the affected systems or services experiencing the denial-of-service conditions. 2. Determine the type and nature of the attack, such as network-based or application-based. 3. Analyse network traffic logs, system logs, or intrusion detection system (IDS) alerts to identify patterns or signatures of the attack. 4. Mitigate the impact of the attack by implementing	• Traffic logs, including source IP addresses and attack patterns. • Duration and intensity of the attack. • Any captured evidence of the attack, such as traffic captures or logs. • Communication logs indicating any ransom demands or threats associated with the attack.

	in order to disable the system from delivering normal service to its users.	• Presence of known denial-of-service attack signatures in network traffic or logs. • Unexpected system or application crashes.	traffic filtering, rate limiting, or other countermeasures. 5. Work with LAN/System administrators or service providers to identify the source or origin of the attack. 6. Document the incident, including the observed attack patterns and impact on systems or services, for further analysis and reporting.	• Logs from firewalls, routers, or other security devices.
Leaking of classified data in electronic form	Classified data was exposed or accessible by unauthorised persons.	• Unusual or unauthorised access to classified data. • Unusual data transfers or copying activities. • Presence of unauthorised users accessing classified data. • Unusual access patterns, such as accessing classified data	1. Identify the source and nature of the classified data leak or exposure. 2. Determine the scope and sensitivity of the leaked data, including the classification level and potential impact. 3. Collect and analyse system logs, access records, and other relevant evidence to identify unauthorised access or activities.	• Logs indicating unauthorised access or data exfiltration. • System or application logs showing signs of data leakage. • Communication logs (emails, chat logs, etc.) related to the incident. • Information about the leaked data, including its nature and sensitivity.

		outside of normal working hours or from unauthorised locations. • Evidence of data exfiltration or unauthorised sharing of classified information. • Unauthorised disclosure or publication of classified data.	4. Preserve any available forensic evidence for further analysis or legal action. 5. Notify appropriate stakeholders, such as information owners, IT Security Management Unit, or management, about the incident. 6. Assess the impact of the data leak and take immediate action to contain further exposure or unauthorised access. 7. Conduct a thorough investigation to determine the root cause of the incident, including potential vulnerabilities or weaknesses in security controls.	• Any captured evidence, such as screenshots or recordings.
Loss of mobile devices or removable media that contain classified data	A mobile device/removable media with classified data was lost due to accidental loss or theft.	• Misplacement or loss of mobile devices or removable media. • Unauthorised access attempts on lost or stolen devices.	1. Gather information about lost or stolen mobile devices or removable media, including device identifiers, content, and classification of data stored.	• Information about the lost device or media, including its make, model, and serial number. • Details of the data stored on the lost device or media.

		• Unusual user behaviour or patterns, such as accessing classified data on unauthorised devices. • Evidence of unauthorised access to data or accounts associated with the lost or stolen devices.	2. Determine the date, time, and location of the loss or theft. 3. Interview the individuals involved or witnesses to gather additional details. 4. Analyse system logs, access records, or security camera footage, if available, to identify any unauthorised access attempts or suspicious activities related to the lost or stolen devices. 5. Assess the potential impact of the loss or theft, such as the sensitivity of the data and the likelihood of unauthorised access. 6. Notify appropriate stakeholders, such as data owners, security personnel, or management, about the incident. 7. Implement measures to mitigate the risk of data exposure, such as remote wiping, password resets, or account suspensions.	• Any encryption or security measures applied to the device or media. • Reports or logs indicating the time and location of the loss. • Any captured evidence, such as photos or witness statements.

Masquerading	The use of another person’s identity to gain excess privilege in accessing information systems.	• Unusual or unauthorised login attempts using other user's credentials. • Anomalous patterns of user account usage, such as accessing sensitive data or systems without a legitimate reason. • Evidence of unauthorised access or misuse of user accounts. • Complaints or reports of unauthorised access or suspicious behaviour from users. • Evidence of attempts to bypass authentication mechanisms or impersonate legitimate users.	1. Identify the affected user accounts or systems where masquerading attempts have been observed. 2. Collect relevant logs, audit records, or system artefacts to analyse the activities associated with the masquerading incidents. 3. Analyse login attempts, account usage patterns, or system access records to identify unauthorised access or suspicious behaviour. 4. Verify the authenticity of reported complaints or incidents related to masquerading. 5. Assess the impact and potential risk of masquerading incidents, such as unauthorised access to sensitive data or systems. 6. Take immediate actions to prevent further unauthorised access, such as disabling compromised	• Logs indicating unauthorised access or impersonation attempts. • System or application logs showing signs of masquerading activities. • User account credentials or accounts used for masquerading. • Communication logs (emails, chat logs, etc.) related to the incident. • Any captured evidence, such as screenshots or recordings.

		• Unusual changes in user account settings or permissions.	accounts or enhancing authentication mechanisms.	
Massive malware infection	A malware infection can corrupt files, alter or delete data, encrypt files, stealthily steal data, disable the hardware or software operation, or deny legitimate user access, etc. B/Ds have to identify and assess if there is a significant impact on their business operations.	• Unusual system behaviour, such as frequent crashes or freezes. • Unexpected pop-ups or error messages. • Slow system performance or unresponsiveness. • Unusual network traffic patterns, such as frequent connections to suspicious or malicious domains. • Detection of known malware signatures or indicators by security software. • Unusual disk activity or high CPU usage.	1. Identify affected systems or network segments exhibiting signs of malware infection. 2. Isolate infected systems from the network to prevent further spread and damage. 3. Collect malware samples for further analysis and identification. 4. Analyse system logs, network traffic, and security software reports to identify patterns or indicators of malware activity. 5. Determine the type and behaviour of the malware, such as its propagation methods, persistence mechanisms, and payload. 6. Assess the impact of the malware infection on the	• Malware samples (if available). • Indicators of compromise (IoCs) or known malware signatures. • System logs showing suspicious activities or connections. • Network traffic logs indicating communication with malicious domains or IP addresses. • Files or directories affected by the malware. • Information about the malware's behaviour or payload.

		• Unauthorised access or changes to files or system configurations. • Reports or complaints from users about suspicious files or activities. • Unexpected encryption or encryption-related activity. • Evidence of data exfiltration or communication with command-and-control servers.	B/D's systems, data, and operations. 7. Conduct a preliminary investigation to understand the infection vector and potential entry points. 8. Deploy appropriate tools and techniques to remove or mitigate the malware infection. 9. Identify and close any security vulnerabilities or weaknesses that allowed the malware to infiltrate the systems. 10. Restore affected systems from clean backups or rebuild them if necessary.	
Ransomware	Ransomware is a type of malware that prevents and limits users from accessing their systems or files through encryption and demands payment for decryption.	• Inability to access or open files with ransom messages or warnings displayed. • Unusual file extensions or changes in file names. • Encrypted files or file modifications	1. Identify the affected systems or network segments. 2. Isolate infected systems from the network to prevent further spread. 3. Collect ransomware samples for further analysis, if available. 4. Analyse system logs, network traffic, and	• Ransomware samples (if available). • Ransom notes or communication from the attackers. • Indicators of compromise (IoCs) or known ransomware signatures.

		without user intervention. • Unusual network traffic patterns, such as communication with known ransomware command-and-control servers. • Presence of ransomware-related files or executables on the system. • Unusual system behaviour, such as slow performance or crashes, after the onset of ransomware infection. • Requests for ransom payment or communication from the attackers.	security software reports to identify indicators of ransomware activity. 5. Determine the type and variant of the ransomware. 6. Assess the impact of the ransomware infection on systems and data. 7. Identify the entry point or infection vector. 8. Decrypt any available ransom notes or communication from the attackers. 9. Determine the ransom amount and cryptocurrency wallet address, if provided. 10. Gather information on the affected files and their encryption status. 11. Investigate any potential backup systems or data recovery options.	• System logs showing suspicious activities or connections. • Network traffic logs indicating communication with malicious domains or IP addresses. • Encrypted files or file extensions appended by the ransomware. • Information about the ransom amount and cryptocurrency wallet address. • Backup systems and data recovery information. • Any relevant system or network configurations.
Website defacement	Unauthorised alteration of the content of one or	• Noticeable changes in the appearance or	1. Identify the defaced website(s).	• URLs or web addresses of the defaced website(s).

	more web pages of the website.	content of web pages. • Addition, deletion, or modification of content without authorisation. • Defaced or vandalised web pages with unauthorised messages or content. • Unexpected redirection to unknown or malicious websites. • Unusual web server logs, such as multiple failed login attempts or access to sensitive directories. • Reports or complaints from users about suspicious or altered web content.	2. Capture screenshots or records of the defaced content. 3. Analyse web server logs to determine the extent and duration of the defacement. 4. Identify any unauthorised access or modifications in the logs. 5. Assess the impact of the defacement on the website's functionality and reputation. 6. Determine the method used for the defacement (e.g., exploiting vulnerabilities, unauthorised access). 7. Investigate any potential security misconfigurations or weaknesses. 8. Restore the website to its original state from clean backups, if available.	• Screenshots or records of the defaced content. • Web server logs showing unauthorised access or modifications. • Information about the impact on website functionality and reputation. • Details of any security misconfigurations or vulnerabilities. • Backup copies of the original website content (if available). • Any relevant system or network configurations.

		• Evidence of unauthorised access or modifications to website configurations or files. • Unexpected changes in search engine rankings or website visibility.		

Nevertheless, the occurrence of an incident may not be confirmed by one single symptom. Skilful personnel who possess sufficient security and technical knowledge should be involved to determine the incident from one or more of the above symptoms. Moreover, seeking others' comments and collective judgment may help in identifying if an incident has really occurred.

Detecting and identifying potential security events or incidents as early as possible is crucial. Therefore, it is essential for B/Ds to remain vigilant and pay attention to any unusual or suspicious activities within their own installation/environment. Only commonly observed indications are listed above, and the list is by no means exhaustive. B/Ds should proactively monitor their systems and promptly investigate any signs of abnormal behaviour or security-related anomalies. The initial analysis steps and information required for identification/analysis provided above are served as reference only. As each B/D's circumstances and incident response procedures may vary, B/Ds should adapt their response accordingly. B/Ds should prioritise continuous monitoring and remain alert to any unusual or suspicious activities to enhance their ability to detect and identify potential security events or incidents promptly, allowing for timely response and mitigation.

F.2 Factors Affecting the Scope and Impact of Incident

Factors affecting the scope and impact of an incident include:

- The extent of the incident: affecting single or multiple systems.
- Possible impact on public service and/or image of the Government.
- Press involvement.
- Crime involvement.
- Potential damage of the incident.
- Whether there is classified information involved.
- Entry point of the incident, such as network, Internet, phone line, local terminal, etc.
- Possibility of a local source of attack.
- Estimated time to recover from the incident.
- Resources required to handle the incident, including staff, time and equipment.
- The possibility of further damage.