Office of the Government Chief Information Officer

INFORMATION SECURITY

Practice Guide

for

Information Security Incident Handling

[ISPG-SM02]

Version 1.4

June 2023

COPYRIGHT NOTICE

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

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 planning, and to be used for preparation for, detection of and response to information security incidents. As information security incident of different information systems will have different effects and lead to different consequences, B/Ds should customise the information security incident handling procedures 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 (fourth edition), ISO/IEC 27000:2016

- Information technology - Security techniques - Information security management systems - Requirements (second edition), ISO/IEC 27001:2013

- Information technology - Security techniques - Code of practice for information security controls (second edition), ISO/IEC 27002:2013

- Information technology - Security techniques - Information security incident management - Part 1: Principles of incident management, ISO/IEC 27035-1:2016

- Information technology - Security techniques - Information security incident management - Part 2: Guidelines to plan and prepare for incident response, ISO/IEC 27035-2:2016

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	
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.

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

For more information about useful contacts for incident handling in the Government, please refer to the Government intranet portal ITG InfoStation: IT Security Theme Page (https://itginfo.ccgo.hksarg/content/itsecure/sih/contacts.shtml).

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 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 audit 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 risk of data security, B/Ds shall activate their standing incident management plan to identifying, managing, recording, and analysing security threats, attacks, or incidents in real-time. B/Ds should also prepare to communicate appropriately with relevant parties by sharing information on response for 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 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 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 handling 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 for responding to security incidents and resuming 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 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 in respect of confidentiality, integrity and availability. As this practice guide is focusing on incidents related to information security, adverse events such as natural disaster, 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 attack, 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 of threat, information security event and information security incident:

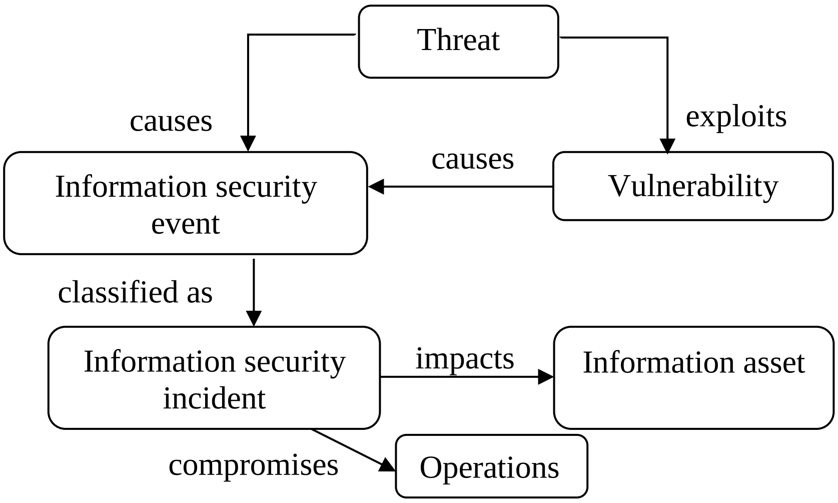


Figure 3.1 Relationship of Security Event and Security Incident

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 the 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 to 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

A well-defined security incident handling plan is vital to the efficient and effective handling of security incidents, minimising impact and damage, and rapidly recovering operation of an information system. 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 clear understanding about 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 handling 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.
- Mission critical 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 of 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 response 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.

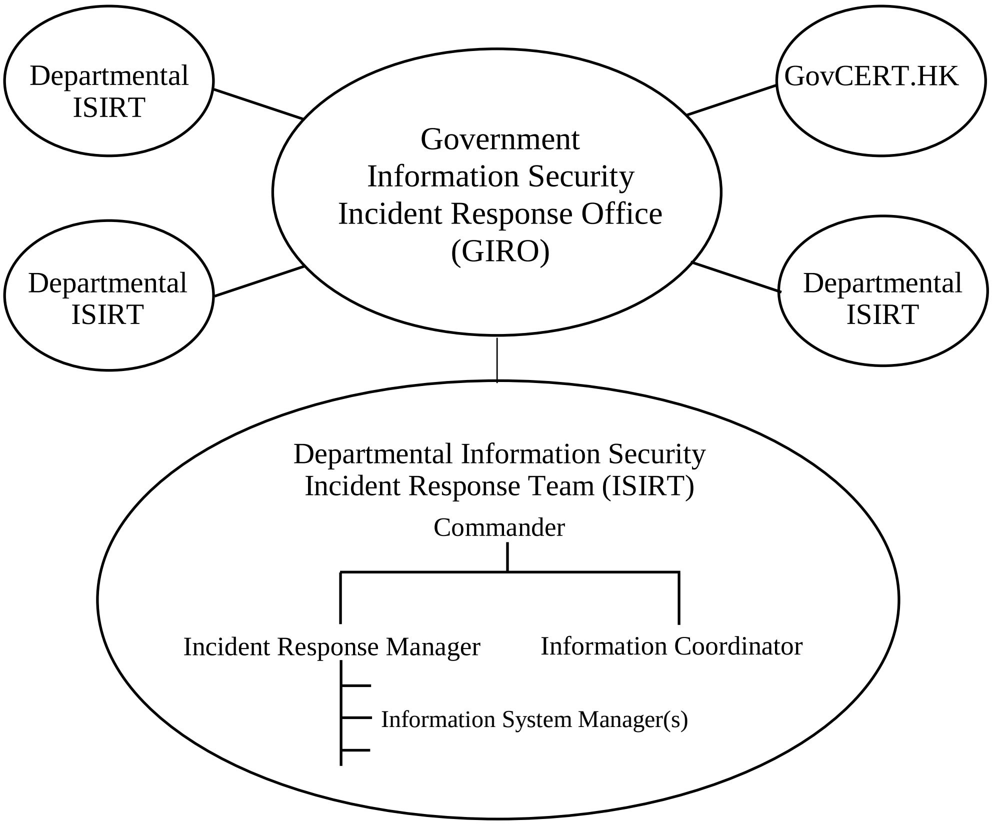

Departmental ISIRT
GovCERT.HK
Government Information Security Incident Response Office (GIRO)
Departmental ISIRT
Departmental ISIRT
Departmental Information Security Incident Response Team (ISIRT)
Commander
Incident Response Manager
Information Coordinator
Information System Manager(s)

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 on 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 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 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 incident 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 handling 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.

The following sections describe each of the roles and functions 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.

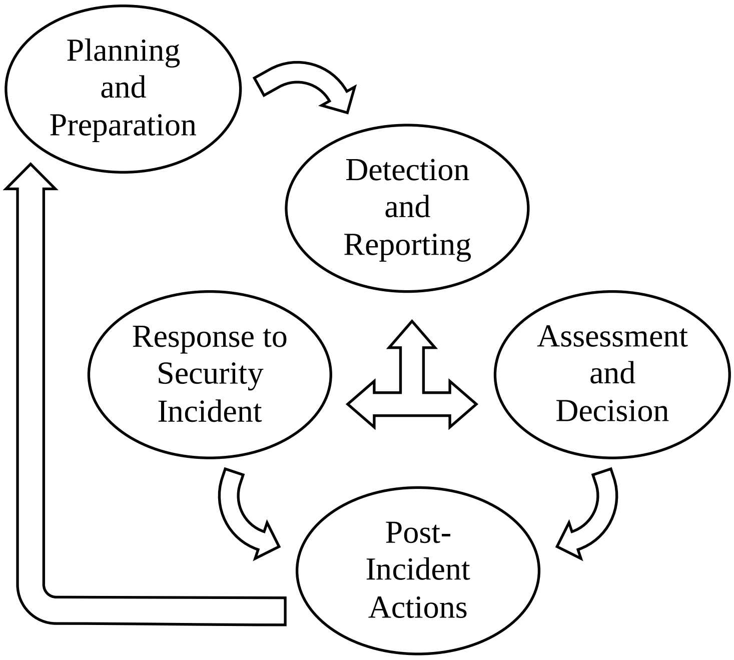


Figure 5.1 Security Incident Handling Cycle

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 are listed below.

- Security Incident Handling Plan
- Reporting Procedure
- Escalation Procedure
- Security Incident Response Procedure
- Training and Education
- Incident Monitoring Measure

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, coordinated 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 involved in planning and preparation are as follows:

- Security Incident Handling Plan
- Reporting Procedure
- Escalation Procedure
- Security Incident Response Procedure
- Training and Education
- Incident Monitoring Measure

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

6.1 Security Incident Handling Plan

In general, a security incident handling plan shall align with S17 and G3, and should cover the following major items:

- Scope
- Goals and Priorities
- Roles and Responsibilities
- Constraints

6.1.1 Scope

The scope will define the functional area that the security incident response team will be responsible for. It may be for the whole B/D (i.e. the ISIRT) or for a specific information system or application within the B/D.

6.1.2 Goals and Priorities

A set of goals under the security incident handling plan should be clearly defined in advance and prioritised according to the system and management requirements. The security incident response procedures, prepared at a later stage, should tally with these predefined goals.

Depending on different systems and management requirements, examples of incident handling goals 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 followings 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.

6.1.3 Roles and Responsibilities

The roles and responsibilities of all parties participating in the security incident handling 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.

6.1.4 Constraints

Constraints like resources, technology and time should be considered. They may affect the result of the security incident handling process. For example, if there is a lack of internal technical expertise, it may be necessary to acquire external consultants or service contractors. Such preparation should also be made in advance to ensure a smooth handling process in case of a security incident.

6.2 Reporting Procedure

A reporting procedure should 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 address, and fax number, 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 incident 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 on 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. Typical indications of an incident that deserve special attention are suggested in **Annex F.1**.

Upon an information security incident is confirmed, the departmental ISIRT is required to:

- Report to the GIRO-SO within **60 minutes** by phone and submit a completed Preliminary Information Security Incident Report 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 assessment on 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.

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 longer time to complete the investigation, the concerned departmental ISIRT is required to submit an interim report on a three months' interval to the GIRO-SO on the latest recovery and investigation status:

- Submit to the GIRO-SO the first interim report no later than three months after the incident was confirmed; 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.

6.3 Escalation Procedure

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.

6.4 Security Incident Response Procedure

The security incident response procedure defines the steps to be followed in case an incident occurs, which aims at minimising damage, eradicating the cause of the incident and restoring the system to normal operation, etc., in accordance with the predefined goals and priorities.

A security incident response procedure to guide the security incident response team through the handling process shall be established and documented. The procedure should be made known to all staff, including management personnel, for their reference and compliance. The procedure should be clear, straightforward and easily understood so that all the personnel have clear knowledge about what they need to do. The procedure shall be regularly tested and updated to ensure a quick and effective response to the information security incidents. Moreover, drill shall be conducted at least once every two years, preferably annually, to assess the effectiveness of the procedure.

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).

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

6.5 Training and Education

B/Ds shall ensure all staff observe and follow the security incidents handling / reporting procedures. Staff should be familiar with the procedures to handle the incident from incidents 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. 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 to 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.

6.6 Incident Monitoring Measure

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 device 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 tool and malware detection and repair tool to detect and remove malware, and prevent them from affecting system operations.
- Perform periodic security check by using security scanning tools to identify existing vulnerabilities and perform a gap analysis between stated security policy and actual security arrangement.
- Install 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.

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 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 the intrusion detection tools and system audit logs, can be used to aid in identifying unauthorised or abnormal activities.

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

- Determine if an incident occurs and perform preliminary assessment.
- Log the incident.
- Obtain system snapshot, if necessary.

To determine if an incident occurs, B/Ds should consider the following circumstances, including but not 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. Knowledge in respect of the type of the incident can help to identify suitable response to deal with the incident. Moreover, some precautions or defensive measures can be taken promptly in the light of the damage made and the impact involved.

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.

The following information is suggested to be included when describing the incident during the escalation process:

- Brief description of the incident: what was the incident, when did it occur, how was the system compromised, and what was the damage/impact made.
- Indicate if the attacker, if any, is still active in the system.
- Information of the system such as system name, functions, and other technical information such as host name, IP address, operating system and version, etc.
- Supporting information, if necessary, such as screen capture, system messages, etc.

The information provided during the escalation process should be clear, concise, accurate and factual. 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.

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.

For purposes of recording and co-ordination on handling of the incident, the ISIRT Commander should also provide a Preliminary Information Security Incident Report (see **Annex C.2**) for reporting of information security incidents including, but not limited to, the following categories (please refer to **Annex F.3** 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 disaster, 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 destroy of classified data due to system or human error.
- Fraudulent email or website 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 website (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).

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 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 should 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 log.
- 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

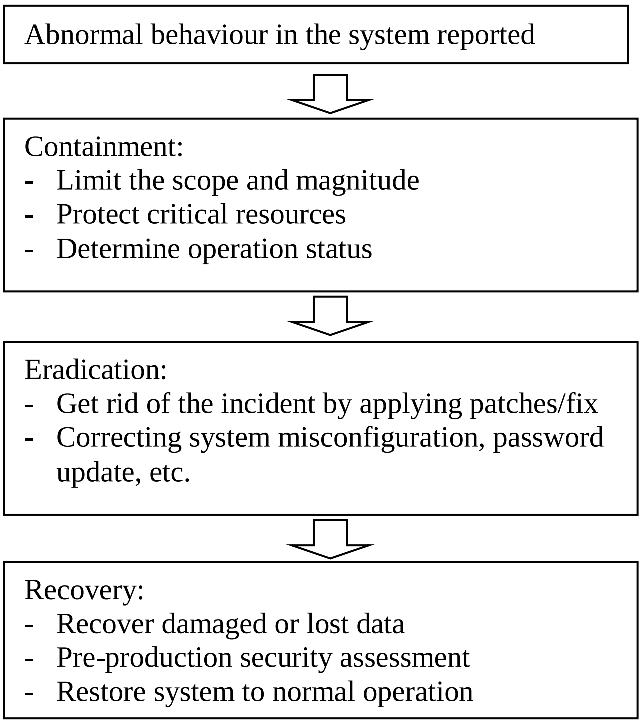
A snapshot of the compromised system should be obtained as soon as suspicious activities are detected, and as far as technically and operationally feasible. This can prevent the attacker from destroying the evidence and support subsequent case investigation, such as forensic evidence collection. The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



Abnormal behaviour in the system reported

Containment:
- Limit the scope and magnitude
- Protect critical resources
- Determine operation status

Eradication:
- Get rid of the incident by applying patches/fix
- Correcting system misconfiguration, password update, etc.

Recovery:
- Recover damaged or lost data
- Pre-production security assessment
- Restore system to normal operation

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 handling 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 non mission-critical system 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 restore 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 critical 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.

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 legal proceedings and produce 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 exception on reporting needs 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 Handling Preparation

B.1 Sample Checklist for Incident Handling Preparation

	Item	Details	Status
1	Security incident handling plan	Plan for security incident handling	
2	Reporting procedure	Design and prepare for the reporting mechanism(s)	
		Publish the reporting mechanism(s) to all staff	
3	Escalation procedure	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	
4	Security incident response procedure	Prepare security incident response procedure	
		Publish the security incident response procedure to all personnel involved	
5	Training and education	Provide training to operation and support staff in handling security incidents	
		Ensure staff are familiar with the incident response process	
6	Incident monitoring measure	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	

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 enquiry and/or security incident report.

For 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 submission of detailed information that may not be reported clearly and accurately by telephone. However, fax machine used for incident reporting should be promptly attended to, preferably by dedicated staff. Besides, special attention should also be paid in handling fax reports to prevent disclosure of the incident information to unauthorised person. 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 on 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:	***Report 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

☐ Denial of service attack

☐ Masquerading

☐ Massive malware infection

☐ Website defacement

☐ Compromise of information systems or data assets

☐ Leaking of classified data in electronic form

☐ Loss of mobile devices or removable media that contain classified data

☐ Ransomware

☐ Others: __________________

Components/Assets Affected:

☐ Email System

☐ Information / Data

☐ Software

☐ Others: ____________________

☐ Hardware

☐ Network

☐ Website

Details of Components/Assets Affected:

____

Impacts:

☐ Confidentiality

☐ Availability

☐ Others: ___________________

☐ Integrity

☐ Government’s image

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

☐ Incident Response Manager

☐ GIRO Standing Office

☐ Information Coordinator

☐ ISIRT Commander

☐ 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 on 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:	***Report 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 on 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:	***Report 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

□ Denial of service attack

□ Masquerading

□ Massive malware infection

□ Website defacement

□ Compromise of information systems or data assets

□ Leaking of classified data in electronic form

□ Loss of mobile devices or removable media that contain classified data

□ Ransomware

□ Others: ____________________

Components/Assets Affected:

□ Email System

□ Information / Data

□ Software

□ Others: ____________________

□ Hardware

□ Network

□ Website

Details of Components/Assets Affected:

____

Other Affected Sites/Systems (if any):

____

Impacts:

□ Confidentiality

□ Availability

□ Others: ____________________

□ Integrity

□ Government’s image

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:

____

<table>
<tr><td colspan="2">Whether the affected individuals have been informed: Yes/No. If No, why:
Remarks:</td></tr>
<tr><td colspan="2"><b>Cost Factor (including loss caused by the incident and the recovery cost/manpower):</b></td></tr>
<tr><td colspan="2"><b>Recommended Action to Prevent Recurrence:</b></td></tr>
<tr><td colspan="2"><b>Experience Learnt:</b></td></tr>
<tr><td colspan="2"><b>Media / Public Enquiry (If applicable)</b></td></tr>
<tr><td><b>No. of Media Enquiry Received:</b></td><td><b>No. of Public Enquiry Received:</b></td></tr>
</table>

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 requirement. For example, 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 could not be solved, it may need to seek advice from external supporting parties, such as service contractor, 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 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.

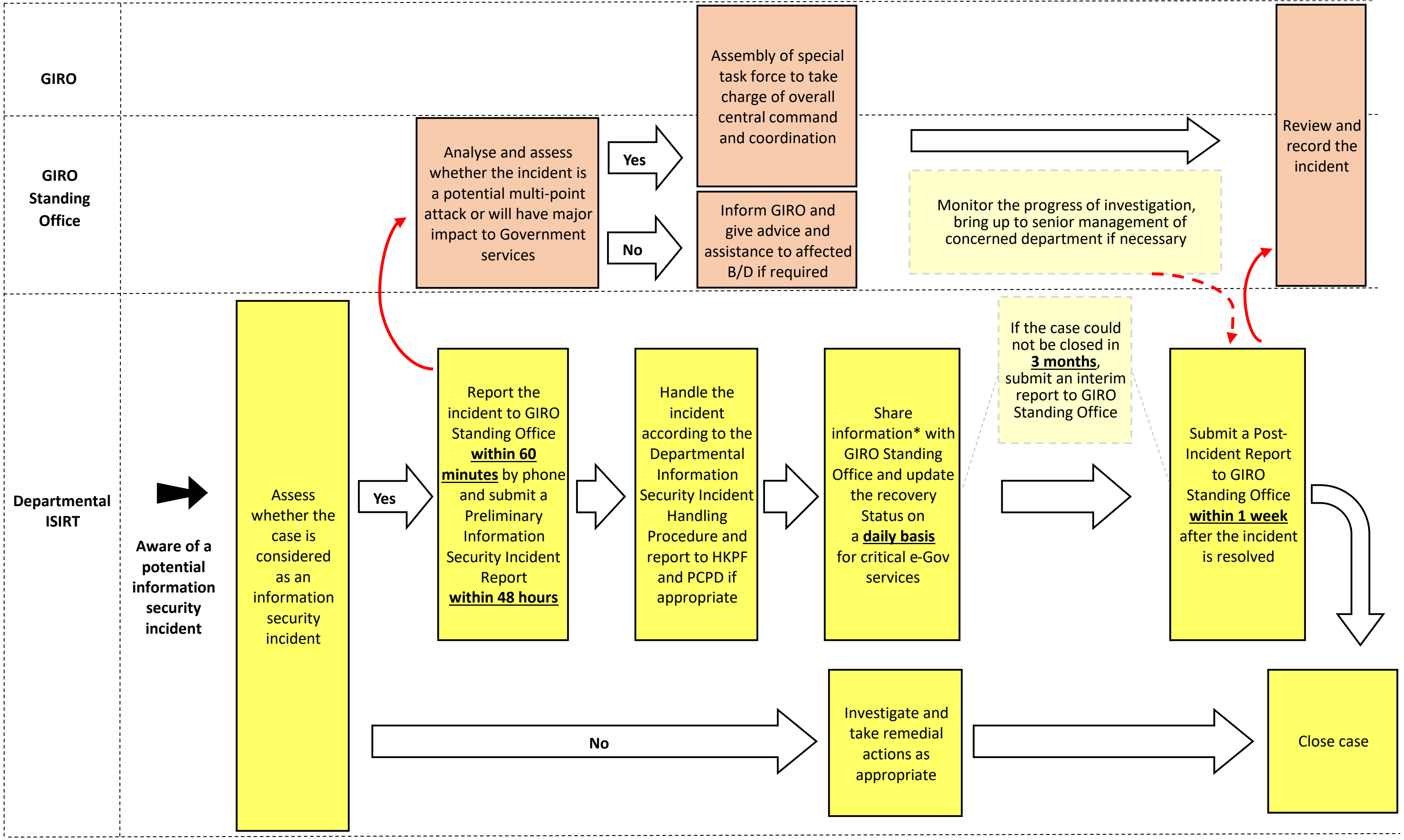
Duration of report	**Contact List**	**Contact method**
Within 15 minutes of the incident	Respective information system manager, technical support staff, related supporting vendors and service contractors	*Mobile phone & vendors' 24 hours hotline*
Within 30 minutes of the incident	All of the above, Incident 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:


GIRO
GIRO Standing Office
Departmental ISIRT
Aware of a potential information security incident
Assess whether the case is considered as an information security incident
Yes
No
Report the incident to GIRO Standing Office within 60 minutes by phone and submit a Preliminary Information Security Incident Report within 48 hours
Analyse and assess whether the incident is a potential multi-point attack or will have major impact to Government services
Yes
No
Assembly of special task force to take charge of overall central command and coordination
Inform GIRO and give advice and assistance to affected B/D if required
Handle the incident according to the Departmental Information Security Incident Handling Procedure and report to HKPF and PCPD if appropriate
Share information* with GIRO Standing Office and update the recovery Status on a daily basis for critical e-Gov services
Monitor the progress of investigation, bring up to senior management of concerned department if necessary
If the case could not be closed in 3 months, submit an interim report to GIRO Standing Office
Submit a Post-Incident Report to GIRO Standing Office within 1 week after the incident is resolved
Review and record the incident
Investigate and take remedial actions as appropriate
Close case

*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 Indication 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 indications of security incidents include any or all of the followings:

Related to system operations:

- A system alarm or similar indication from intrusion detection, anti-malware or malware detection tools.
- Suspicious entries in system or network accounting (e.g. a user obtains root access without going through the normal process).
- Accounting discrepancies.
- A part of or the entire system log is missing or altered.
- System crashes.
- Unexpected significant drop in system performance.
- Unauthorised operation of a program.
- Suspicious probes, such as numerous unsuccessful login attempts.
- Suspicious browsing activities, such as account with root privilege accessing many files of different user accounts.
- Unexpected large deviation on system clock.
- Unusual deviation from typical network traffic flows, (e.g. unexpected network scanning activities).

Related to user account:

- Creation or deletion of unexpected user accounts.
- High activity on a previously low usage or idle account.
- Inability to login due to modifications of account.
- Unexpected change of user password.
- Unusual time of usage.
- A suspicious last time login or usage of a user account.
- Unusual usage patterns (e.g. programs are being compiled in the account of a user who is not involved in programming).
- Computer system displays strange messages.
- Computer system becomes inaccessible without explanation.
- Large number of bounced emails with suspicious content.
- User calls to report a threatening email message.

Related to file and data:

- Unexpected files or data creation, modification or deletion.
- Unfamiliar file names.
- Unexpected modification to file size or date, especially for system executable files.
- Unexpected attempts to write to system files or changes in system files.
- File and data inaccessible.
- Sensitive material found unattended in common areas, e.g. printer output tray.

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.

Only commonly observed indications are listed above and the list is by no means exhaustive. B/Ds should pay attention to any unusual or suspicious activities with respect to their own installation/environment to detect and identify potential security events or incidents as early as possible.

F.2 Information Collected for Identification

The following information should also be examined during incident identification:

- Audit trails or log files such as system log, firewall/router log, server log, and intrusion detection system log, etc.
- Active network connection and system process status information.
- Any other documentation that would help the investigating team better understand the function of the system, its network infrastructure, and external connectivity, etc.

F.3 Types of Incidents

All information security incidents should be reported. The following table lists some of the incident types and its description:

IT Security Incident	Description
Abuse of information systems	Abuse occurs when someone uses an information system for other than the permitted purposes, e.g. to cause an adverse impact to the information assets.
Compromise of information systems or data assets	Physical or logical access to whole or part of an information system and/or its data without the prior permission of the system owner. A compromise can occur either through manual interaction by the untrusted source or through automation.
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 in order to disable the system from delivering normal service to its users.
Leaking of classified data in electronic form	Classified data was exposed or accessible by unauthorised persons.
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.
Masquerading	The use of another person’s identity to gain excess privilege in accessing information system.
Massive malware infection	Malware infection can corrupt files, alter or delete data, encrypt files, stealthily steal data, disable hardware or software operation, or deny legitimate user access, etc. B/Ds have to identify and assess if there is a significant impact to their business operations.
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.
Website defacement	Unauthorised alteration of the content of one or more web pages of the website.

F.4 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 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.