The Office of the
Government Chief Information Officer

INFORMATION SECURITY INCIDENT HANDLING GUIDELINES

[G54]

Version: 5.0

September 2012

The Government of the Hong Kong Special Administrative Region

COPYRIGHT NOTICE

TABLE OF CONTENTS

1 PURPOSE

Effective information security management involves a combination of prevention, detection and reaction. In addition to deploying strong security protection, a system should also be able to respond to incidents and invoke proper procedures in case an information security incident occurs. Security incident handling represents a major step in the information security management process.

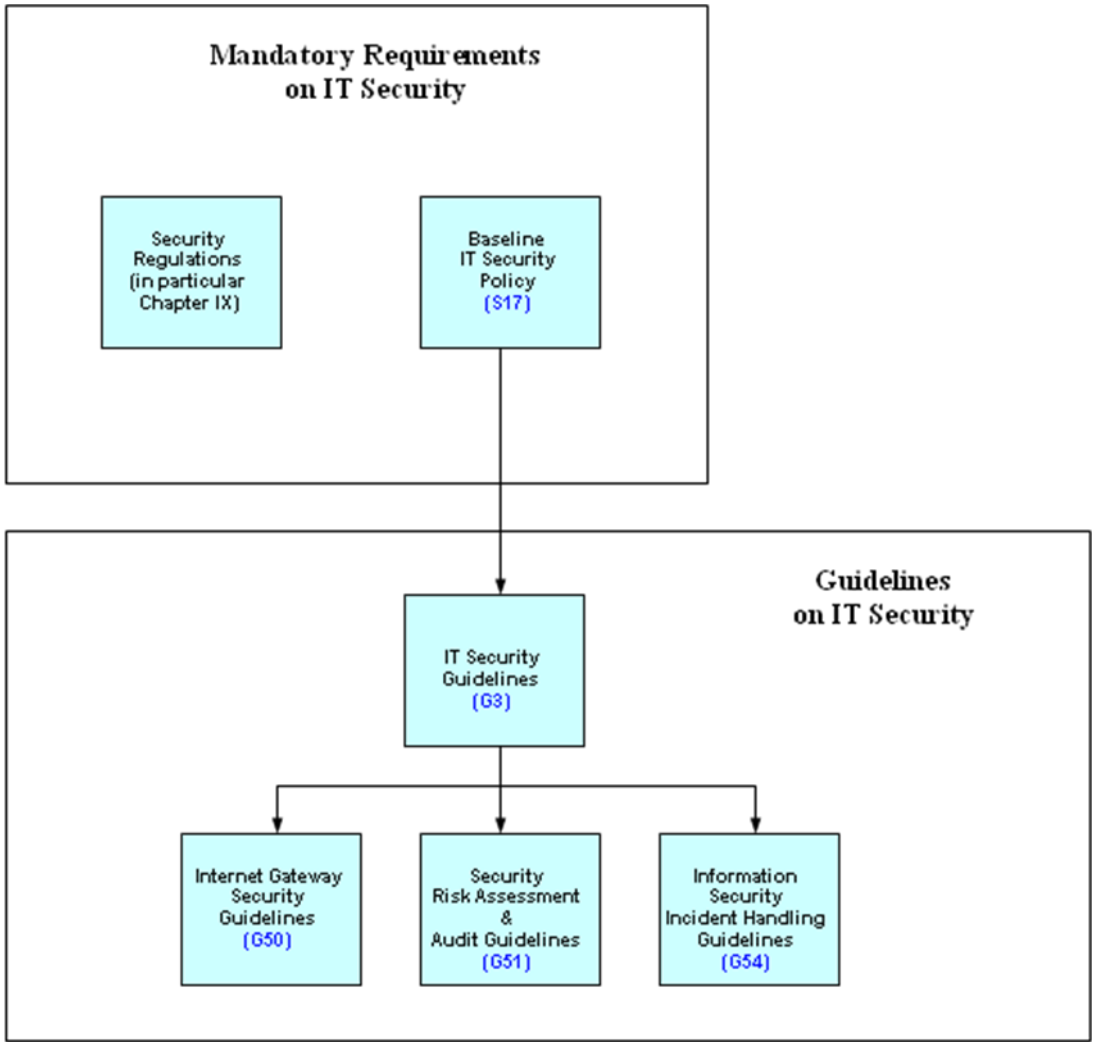
This set of guidelines aims at providing a reference for the management, administration and other technical and operational staff to facilitate the development of security incident handling planning, and to be used for preparation for, detection of and response to information security incidents. As security incident of different computer systems will have different effects and lead to different consequences, bureaux/departments (B/Ds) should customise the security incident handling plan according to their specific operational needs.

2 SCOPE

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

2.1 IT SECURITY DOCUMENT OVERVIEW

The following diagram describes the relationship of various IT security documents within the Government:



IT Security Documents

The purpose and overview of the five core IT security documents are described below:

Baseline IT Security Policy : (S17)	A top-level directive statement that sets the minimum standards of a security specification for all B/Ds. It states what aspects are of paramount importance to a B/D. Thus, the *Baseline IT Security Policy* can be treated as basic rules which must be observed as mandatory while there can still be other desirable measures to enhance the security.
IT Security Guidelines : (G3)	Introduces general concepts relating to IT security and elaborates interpretations on the *Baseline IT Security Policy*. It also provides readers some guidelines and considerations in defining security requirements.
Internet Gateway Security Guidelines : (G50)	Acts as a supplementary document to *IT Security Guidelines* to provide general guidelines on Internet gateway security. These guidelines represent what are regarded as best practices to maintain security risks at an acceptable level under the Internet open platform. It is intended for staff who are involved in the operational and technical functions of Internet gateway services.
Security Risk Assessment & Audit Guidelines : (G51)	Acts as a supplementary document to *IT Security Guidelines* to give an introduction to a generic model for IT security risk assessment and security audit. This document does not focus on how to conduct a security risk assessment or audit. Rather, it provides a reference model to facilitate the alignment on the coverage, methodology, and deliverables of the services to be provided by independent security consultants or auditors.
Information Security Incident Handling Guidelines : (G54)	Acts as a supplementary document to *IT Security Guidelines* to provide a reference for the management, administration and other technical and operational staff to facilitate the development of security incident handling plan, and to be used for preparation for, detection of, and responding to information security incidents.

3 REFERENCES

a) "IT Security Guidelines [G3]", The Government of the Hong Kong Special Administrative Region. http://www.ogcio.gov.hk/en/infrastructure/methodology/security_policy/doc/g3_pub.pdf

b) "Expectations for Computer Security Incident Response", RFC 2350, IETF. http://www.ietf.org/rfc/rfc2350.txt

c) "Computer Security Incident Handling Guide", SP 800-61, NIST. http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf

4 DEFINITIONS AND CONVENTIONS

4.1 DEFINITIONS

N/A

4.2 CONVENTIONS

N/A

5 INTRODUCTION TO SECURITY INCIDENT HANDLING

5.1 SECURITY INCIDENT HANDLING IN INFORMATION SECURITY MANAGEMENT

Information security management can be described as a cycle of iterative and ongoing processes. It involves a series of activities, examples of which are illustrated in Figure 5.1 below:

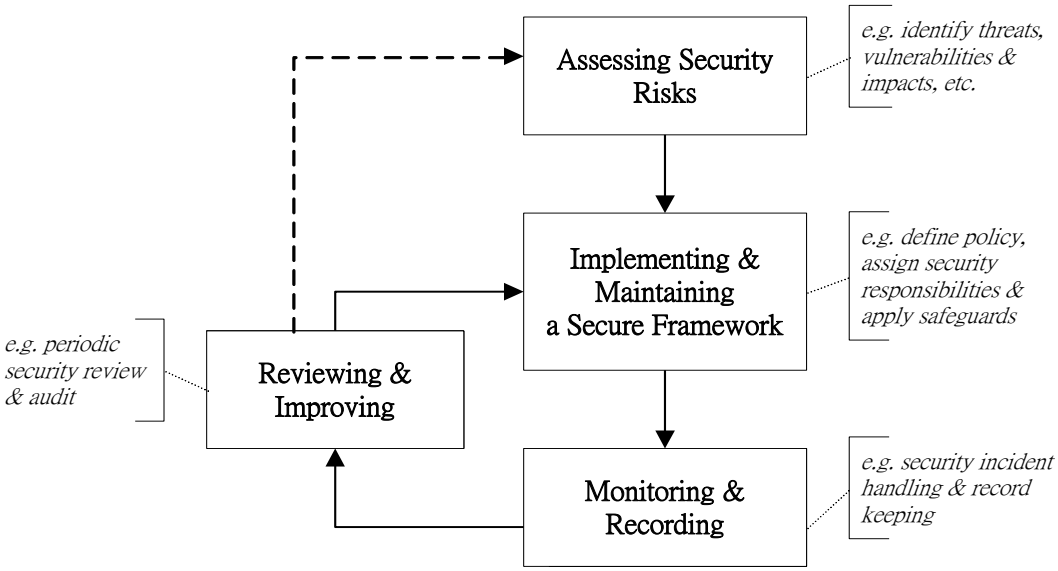


Figure 5.1 An Iterative Process of Information Security Management

The deployment of proper security protection and safeguards reduces the risk of successful attacks. Security measures to strengthen the protection include performing risk assessment to identify risks and vulnerabilities, developing security policies and guidelines, implementing technical protection and so on.

However, despite all these measures, security incidents do occur. It is necessary to prepare for responding to security incidents. 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 computer system to recover in a more organised, efficient and effective manner.

5.2 WHAT IS SECURITY INCIDENT HANDLING

5.2.1 Information Security Incident

The term 'security incident' used in this guideline refers to any incident related to information security. It refers 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 poses a threat to computer or network security in respect of confidentiality, integrity and availability. However, adverse events such as natural disaster, hardware/software breakdown, data line failure, power disruption etc. are outside the scope of this guideline, and should be addressed by the system maintenance and disaster recovery plan.

Examples of security incidents include: unauthorised access, unauthorised utilisation of services, denial of services, compromise of protected data / program / network system privileges, leaks of classified data in electronic form, malicious destruction or modification of data, penetration and intrusion, misuse of system resources, computer viruses and hoaxes, and malicious codes or scripts affecting networked systems.

5.2.2 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 detected, security incident response is made by the responsible parties following the predefined procedures. B/D should consult and update the Government Information Security Incident Response Office (GIRO) Standing Office as soon as possible. A security incident response represents the activities or actions carried out to tackle the security incident and to restore the system to normal operation. Specific incident response teams are usually established to perform the required tasks.

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.

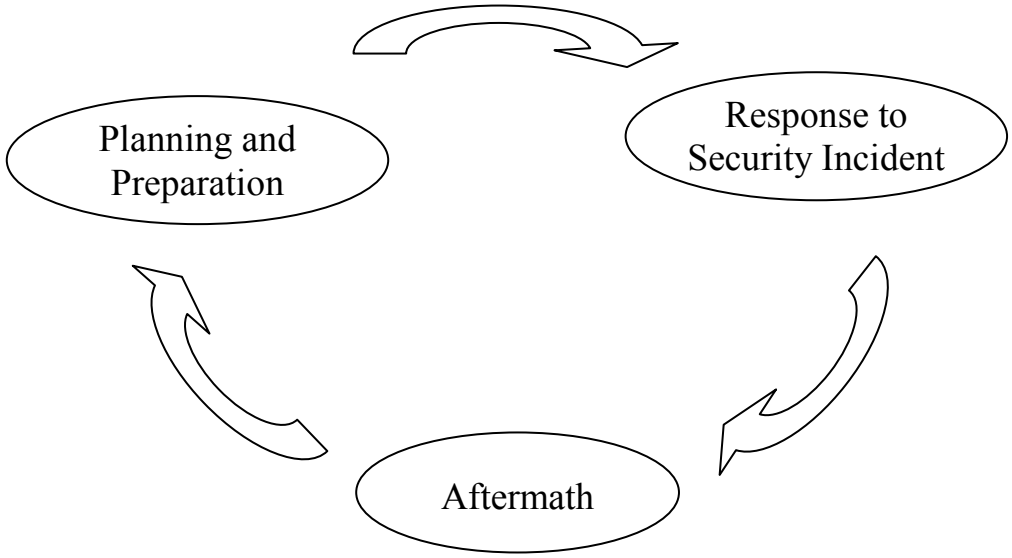


Figure 5.2 Security Incident Handling Cycle

The three processes of the security incident handling cycle will be described in more details in the following sections.

5.3 IMPORTANCE OF SECURITY INCIDENT HANDLING

A well-defined security incident handling plan is vital to the efficient and effective handling of security incident, minimising impact and damage, and rapidly restoring operation of a computer system. Below are the major objectives of security incident handling:

a. Ensure that the required resources are available to deal with the incidents, including manpower, technology, etc.
b. Ensure that all responsible parties have clear understanding about the tasks they should perform during an incident by following predefined procedures.
c. Ensure that the response is systematic and efficient and that there is prompt recovery for the compromised system.
d. Ensure that the response activities are recognised and coordinated.
e. Minimise the possible impact of the incident in terms of information leakage, corruption and system disruption etc.
f. Share experience in incident response within B/Ds.
g. Prevent further attacks and damages.
h. Deal with related legal issues.

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:

a. Systems with external connection, e.g. Internet.
b. Systems handling sensitive data and information.
c. Mission critical systems.
d. Other systems which would be subject to a highly undesirable impact if a security incident occurs.

6 ORGANISATION FRAMEWORK FOR INFORMATION SECURITY INCIDENT HANDLING IN THE GOVERNMENT

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

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

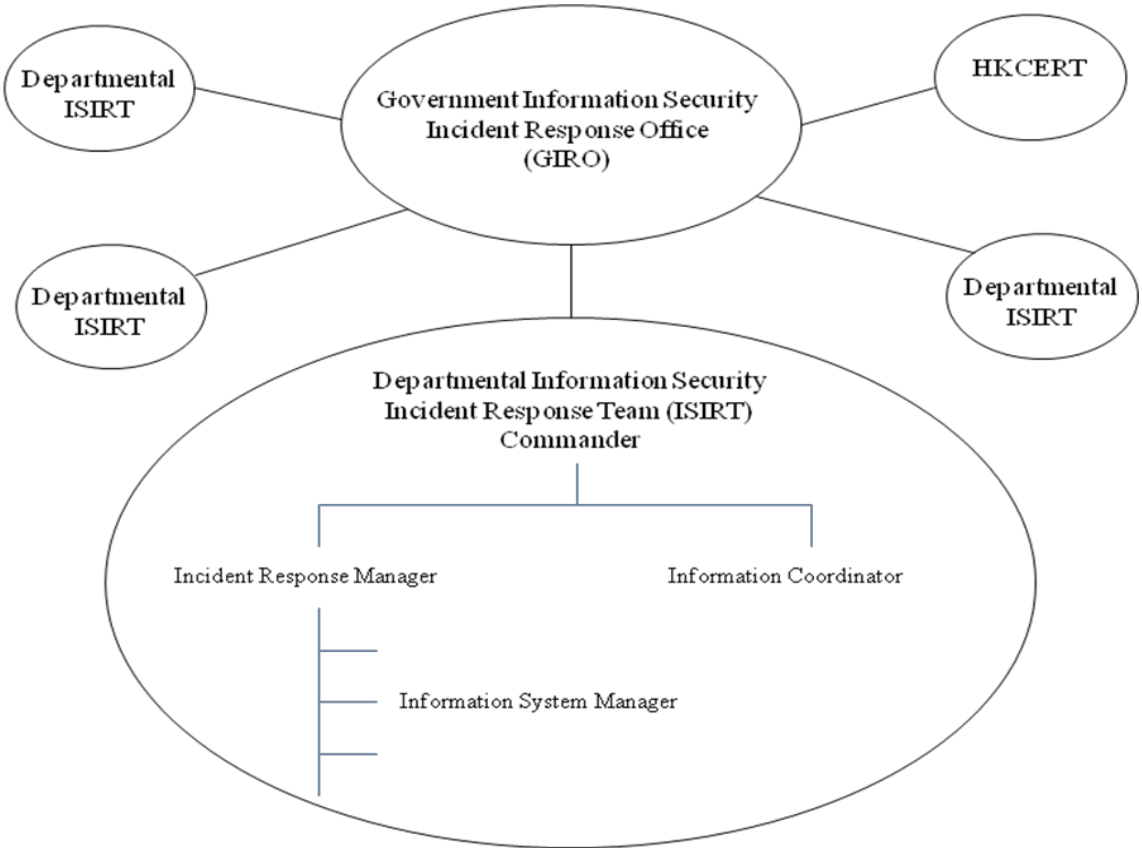


Figure 6.1 Parties Involved in Security Incident Handling

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. The GIRO will also develop its own procedures as appropriate.

6.1 HONG KONG COMPUTER EMERGENCY RESPONSE TEAM COORDINATION CENTRE

In response to the needs to cope with security threats, the Government has funded the Hong Kong Productivity Council (HKPC) to establish the Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT), with the following objectives:

a. To serve as a focal point in Hong Kong for computer security incident reporting and response.
b. To raise the awareness of computer security issues and to promote international standards and practices.
c. To help improve the security of computer systems and the prevention of computer security related incidents.
d. To assist and coordinate recovery actions for computer security incidents.
e. To maintain connection with overseas computer emergency response centres to facilitate cooperation and coordination.

The HKCERT, serves as a one-stop centre for computer security incident response, performs the following major functions:

a. Broadcasts computer security alerts and advisories through a dedicated website and other appropriate channels.
b. Handles computer security incident reports and provides assistance in recovery actions.
c. Disseminates computer security related technical information and materials through its website, newsletters and reports and recommends preventive and intrusion detection tools against security incidents.
d. Promotes computer security awareness through seminars and workshops;
e. Collates incident report statistics and summary report.
f. Collaborates with tertiary institutions, computer vendors, Internet service providers and other computer emergency response centres in identifying solutions to computer security incidents.

6.2 GOVERNMENT INFORMATION SECURITY INCIDENT RESPONSE OFFICE

The Government Information Security Incident Response Office (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.

6.2.1 Functions of GIRO

The GIRO has the following major functions:

a. Disseminate security alerts on impending and actual threats to B/Ds.
b. Maintain a central inventory and oversee the handling of all information security incidents in the Government.
c. Prepare periodic statistics reports on Government information security incidents.
d. Act as a central office to coordinate the handling of multiple-point security attacks (i.e. simultaneous attacks on different Government information systems).
e. Act as a bridge between the HKCERT and the Government regarding Government's information security incidents.
f. Enable experience sharing and information exchange related to information security incident handling among ISIRTs of different B/Ds, and the HKCERT.

6.2.2 GIRO Formation

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.

A standing office is established in OGCIO to provide 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 should provide the GIRO Standing Office 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 Appendix F.

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.

6.3 INFORMATION SECURITY INCIDENT RESPONSE TEAM (ISIRT)

An ISIRT shall be established in each B/D. 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 computer 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.

6.3.1 Functions of the ISIRT

Major functions of the ISIRT should include:

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

6.3.2 ISIRT Formation

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 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: ISIRT Commander, Incident Response Manager, and Information Coordinator. 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 more details.

6.3.3 Roles of the ISIRT

6.3.3.1 Commander

The responsibilities of the Commander include:

a. Making decisions on critical matters such as 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.
b. Depending on the impact of the incident on the business operation of the B/D, triggering the departmental disaster recovery procedure where appropriate.
c. Providing management endorsement on the provision of resources for the incident handling process.
d. Providing management endorsement in respect of the line-to-take for publicity on the incident.
e. Coordinating with the GIRO on incident reporting and necessary follow up actions.
f. Collaboration with GIRO Standing Office in reporting of any information security incident happened, in particular with the following characteristics:
    - System providing public service and its failure will result in service interruption (e.g. denial of service attack to a Government Internet website)
    - System handling sensitive data and information
    - System supporting mission critical operation
    - System which would be subject to a highly undesirable impact if a security incident occurs, e.g. affect Government's public image due to website defacement

6.3.3.2 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:

a. Overall management and supervision of all matters concerning security incident handling within the B/D.
b. Alerting the ISIRT Commander upon receipt of report on security incident affecting the departmental information systems.
c. Reporting the progress of the security incident handling process to the ISIRT Commander.
d. Coordinating various external parties, such as Police, service contractors, support vendors, and security consultants etc. in handling the incident.
e. Seeking necessary resources and support from the ISIRT Commander for the incident handling activities.

6.3.3.3 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.

6.4 DEPARTMENTAL INFORMATION SYSTEM

For individual departmental information system, 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.

The size and structure of the incident response team for an information system/service 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 the incident response team.

Major functions of an incident response team should include:

a. Oversee the security incident handling process for the functional area in-charge.
b. Speed up and facilitate the handling process by pre-establishing relevant handling procedures and list of contact points in advance.
c. Provide a direct channel for receiving reports about suspected incidents.
d. Provide direct and instant response to suspicious activities.
e. Assist in minimising damages and restoring the system to normal operation.
f. Seek advice on security issues from external parties such as service contractors, computer product vendors, or Police.
g. Coordinate security incident handling of the respective information system with other external parties.

h. Conduct impact analysis on the security alerts received from the ISIRT and the GIRO 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 set up similar incident response teams to provide the corresponding services under their duties.

6.4.1 Information System Manager

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 responsibilities include:

a. Developing and implementing the system specific security incident response procedures.
b. Observing and following security incident response procedures for reporting incident to the ISIRT of the B/D.
c. 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.
d. Reporting the security incident to the ISIRT, and with the management support of the ISIRT, requesting for external assistance, such as Police or the HKCERT, in the course of investigation and evidence collection.
e. 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.
f. Identifying any suspected attacks or unauthorised access through the use of security tools/software and/or the system logs, and checking audit trail records.
g. Providing technical support, including evidence collection, system backup and recovery, system configuration and management etc. in the course of problem diagnosis and system recovery.
h. Arranging regular security assessment, impact analysis, and review of the computer system.

7 OVERVIEW OF STEPS IN SECURITY INCIDENT HANDLING

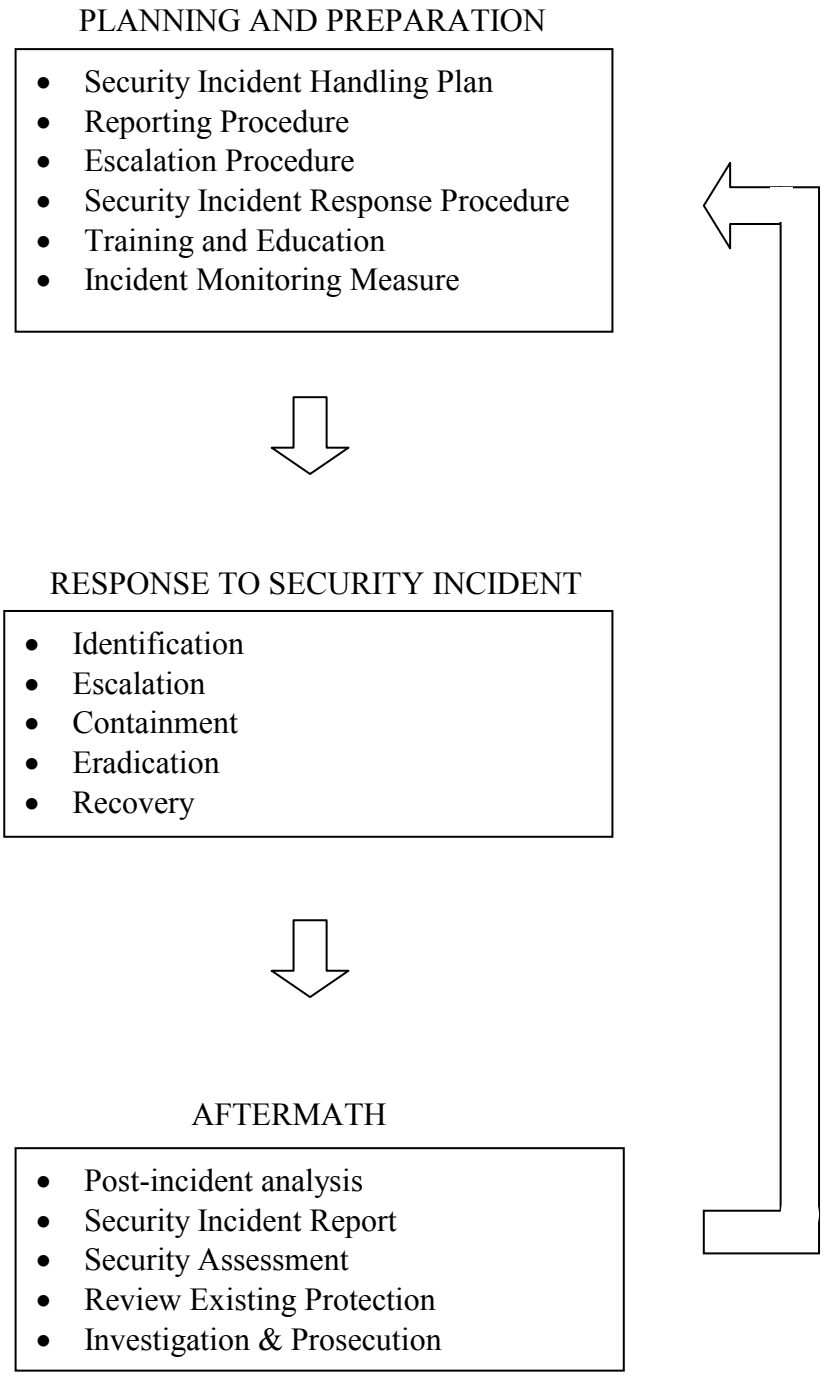


Figure 7.1 Security Incident Handling Steps

The three major steps in security incident handling are summarised in Figure 7.1 above. The processes involved in each of the steps are described in more details in the following sections.

8 PLANNING AND PREPARATION

Proper and advanced planning ensures the incident response activities are known, coordinated and systematically carried out. It 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:

a. Security Incident Handling Plan
b. Reporting Procedure
c. Escalation Procedure
d. Security Incident Response Procedure
e. Training and Education
f. Incident Monitoring Measure

A checklist on preparation for security incident handling is summarised in Appendix A for reference.

8.1 SECURITY INCIDENT HANDLING PLAN

In general, a security incident handling plan should cover the following major items:

a. Scope
b. Goals and Priorities
c. Roles and Responsibilities
d. Constraints

8.1.1 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.

8.1.2 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:

a. Return the system to normal operation in the shortest possible time.
b. Minimise the impact to other systems.
c. Avoid further incidents.
d. Identify the root cause of the incident.
e. Assess the impact and damage of the incident.
f. Update policies and procedures as needed.
g. Collect evidence to support subsequent case investigation.

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:

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

8.1.3 Roles and Responsibilities

The roles and responsibilities of all parties participating in the security incident handling process should be clearly defined. Section 6 above provides a reference model for defining the roles and responsibilities of those major members of a security incident response team.

8.1.4 Constraints

Constraints like resources, technology and time should be considered. This 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.

8.2 REPORTING PROCEDURE

The reporting procedure should 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 Appendix B.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:

a. The reporting procedure should have a clearly identified point of contact, and comprises simple but well-defined steps to follow.
b. The reporting procedure should be published to all concerned staff for their information and reference.
c. Ensure all concerned staff are familiar with the reporting procedure and are capable of reporting security incident instantly.
d. Prepare a security incident reporting form to standardise the information to be collected.
e. 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.
f. 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.

8.3 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 Appendix C for reference. A typical workflow on reporting and escalation of Government security incidents is also illustrated in Appendix E for reference.

8.4 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.

The system or functional area's manager should establish a security incident response procedure to guide the security incident response team through the handling process. The procedure should be made known to all staff, including management personnel, for their reference and compliance. It should be clear, straightforward and easily understood so that all the personnel have clear knowledge about what they need to do. The procedure should be regularly tested (e.g. drill) and updated.

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

8.5 TRAINING AND EDUCATION

It is essential to provide adequate staff training to ensure all concerned staff and management are capable of handling security incidents. Staff should be familiar with the procedures to handle the incident from incidents reporting, identification, and taking the appropriate actions to restore the system to normal operation. Drills on incident handling should also be organised regularly for staff to practise the procedures.

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.

8.6 INCIDENT MONITORING MEASURE

A sufficient level of security measures for incident monitoring should 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.

Listed below are some typical measures for security incident monitoring:

a. Install firewall device and apply authentication and access control measures to protect important system and data resources.
b. Install intrusion detection tool to proactively monitor, detect and respond to system intrusions or hacking.
c. Install anti-virus tool and malicious code detection and repair tool to detect and remove computer virus and malicious codes, and prevent them from affecting system operations.
d. 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.
e. Install content filtering tool to detect malicious contents or codes in emails or web traffic.
f. Enable system and network audit logging to facilitate the detection and tracing of unauthorised activities.
g. Develop programs and scripts to assist in the detection of suspicious activities, monitoring of system and data integrity, and analysis of audit log information.

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 five stages: *Identification*, *Escalation*, *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 five stages, which has to be customised to suit practical needs. For instance, escalation may have already taken place for some incidents as soon as they are reported.

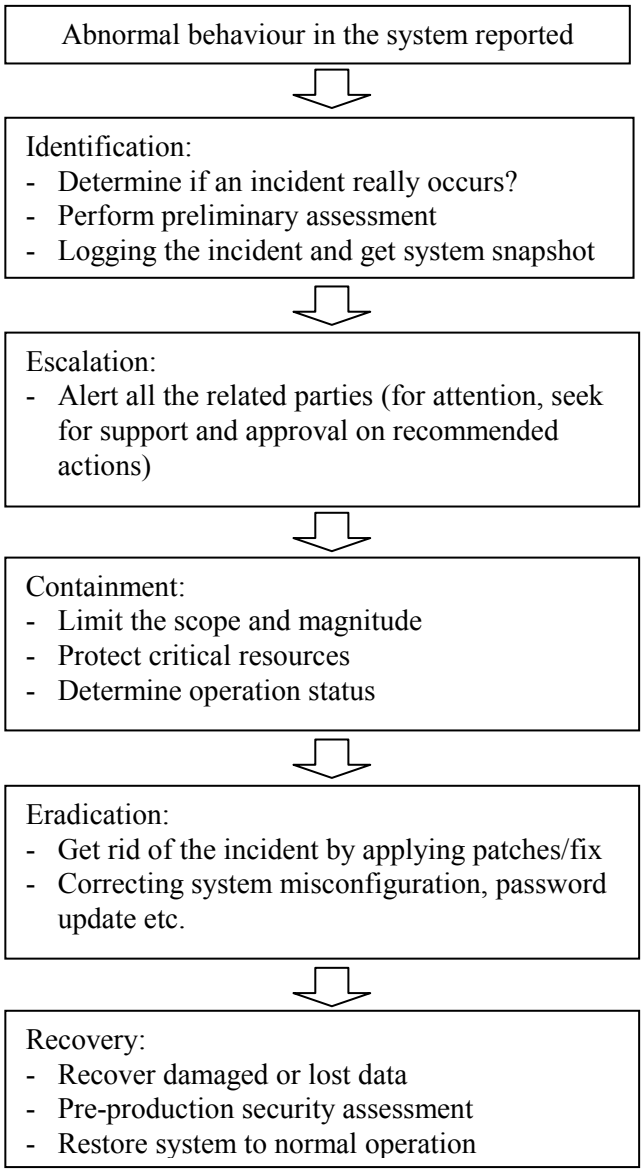


Figure 9.1 Major Stages in Security Incident Response

9.1 IDENTIFICATION OF INCIDENT

Upon discovery of suspicious activities, the computer system's user, operator or administrator should follow the predefined reporting procedure to report the incident to the respective system's 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:

a. Determine if an incident occurs.
b. Perform preliminary assessment.
c. Log the incident.
d. Obtain system snapshot, if necessary.

9.1.1 Determine if an Incident Occurs

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, several aspects have to be considered. Some typical indications of an incident that deserve special attention are suggested in Appendix D for reference.

If a B/D considers that an incident really occurs, the relevant ISIRT Commander should report the incident to GIRO Standing Office **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 complete a Preliminary Information Security Incident Reporting Form (see Appendix B.2) for reporting of information security incidents including, but not limited to, the following categories (please refer to Appendix D.3 for further description) to the GIRO Standing Office.

- 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).
- Email bombing.
- Large scale malicious code attack.

- Defacement of web pages, or web pages injected with malicious code.
- Eavesdropping.
- Compromise/modification of data, program or network system privileges.
- System penetration/intrusion.
- Masquerading.
- Unauthorised access to system and/or data.
- Misuse of system, resource and/or data.
- Fraudulent website or email.
- Leaking of classified data in electronic form.

Incidents that are not security related (listed below) are not required to report to GIRO Standing Office. 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 down or maintenance.
- System failure due to administration/operation error.
- Loss or destroy of sensitive data due to system or human error.

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

9.1.2 Perform Preliminary Assessment

After an incident is identified to be a security incident, the 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.

Some typical security incidents as well as the criteria to be considered when determining the scope and impact of the incident can be found in Appendix D.

9.1.3 Log the Incident

The information system manager should record all security incidents, actions taken and the corresponding results. 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 should be logged:

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

9.1.4 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:

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

9.2 ESCALATION

The second stage in incident response is to notify the appropriate parties and escalate the incident to the appropriate level following the predefined escalation procedure. The escalation task is performed by the manager of the respective information system, with the Incident Response Manager of the ISIRT as the overall coordinator.

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

a. Brief description of the incident: what was the incident, when did it occur, how was the system compromised, and what were the damage/impact made.
b. Indicate if the attacker, if any, is still active in the system.

c. Information of the system such as system name, functions, and other technical information such as host name, IP address, operating system and version etc.
d. 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.

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

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

If personal data is involved in a security incident, B/D should report the case to the Office of the Privacy Commissioner for Personal Data (PCPD) as soon as possible by using the reporting template available at http://www.pcpd.org.hk/english/publications/files/Notification_Form_e.pdf.

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

The Technology Crime Division of the Hong Kong Police Force Commercial Crime Bureau 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 the Police. In addition, for any security incident reported to the Police or PCPD, the GIRO should also be notified for central recording and coordination support.

Please refer to Appendix C 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 Appendix E for reference.

9.3 CONTAINMENT

The third 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 computer virus, worms and malicious code, 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:

a. Conducting impact assessment of the incident on data and information system involved to confirm if the data or service had already been damaged by or infected in the incident.
b. Protecting sensitive 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.
c. Deciding on the operation status of the compromised system.
d. Building an image of the compromised system for investigation purpose and as evidence for subsequent follow up action.
e. Keeping a record of all actions taken during this stage.
f. Checking any systems associated with the compromised system through shared network-based services or through any trusting relationship.

9.3.1 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:

a. 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 machines with sensitive information, or to prevent the compromised system from being used to launch attack on other connected systems.
b. Stopping operation of the compromised information system.
c. Disabling some of the system's functions.
d. Removing user access or login to the system.
e. 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.

9.4 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 computer virus 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.

9.4.1 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:

a. Stop or kill all active processes of hacker to force the hacker out.
b. Delete all fake files created by the hacker. System operators may need to archive the fake files before deletion for the purpose of case investigation.
c. Eliminate all the backdoors and malicious programs installed by the hacker.
d. Apply patches and fixes to vulnerabilities found on all operating systems, servers, network devices, and etc. Test the system thoroughly before restore it to normal operation.
e. Correct any improper settings in the system and network, e.g. mis-configuration in firewall and router.
f. In case of a computer virus incident, follow the advices of anti-virus tool vendor to inoculate or remove the malicious code or computer virus from all infected systems and media as appropriate.
g. 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.
h. 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.
i. Update the access passwords of all login accounts that may have been accessed by the hacker.
j. 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.
k. 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 Police and/or the HKCERT, 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.

9.5 RECOVERY

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

a. Perform damage assessment.
b. Re-install the deleted/damaged files or the whole system, whenever required, from the trusted source.
c. 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.
d. Verify that the restoring operation was successful and the system is back to its normal operation.
e. 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.
f. Disable unnecessary services.
g. 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 must be obtained for all recovery actions to be conducted, and if considered necessary, support and advice from the GIRO may also be sought.

10 AFTERMATH

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 action. 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:

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

Follow up actions include:

a. Post-incident analysis.
b. Post-incident report.
c. Security assessment.
d. Review existing protection.
e. 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:

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

g. 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.
h. 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 manager of the concerned information system 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:

a. Type, scope and extent of the incident.
b. Details of events: source, time and possible method of attack, and method of discovery etc.
c. 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.
d. Response to the incident and eradication methods.
e. Recovery procedures.
f. Other experiences learnt.

The report should be submitted to the GIRO no later than one week after the system is successfully recovered. A sample post-incident report is prepared in Appendix B.3 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 a computer system. In the case of a post-incident event, policies, procedure and guidelines 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 suspected to be caused by a criminal offence should be reported to the Technology Crime Division of the Hong Kong Police Force Commercial Crime Bureau for case investigation and evidence collection. Advice and endorsement from the senior management of the ISIRT should be sought before reporting the case to the Police. In addition, for any security incident reported to the Police, the GIRO should also be notified for central recording and coordination support.

*** End ***

APPENDIX A CHECKLIST FOR INCIDENT HANDLING PREPARATION

A.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-virus, malicious code detection 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	

APPENDIX B REPORTING PROCEDURE

B.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.

Fax number

Reporting by fax is a good supplementary mechanism, in particular for submission of detailed information that may not be reported clearly and accurately by telephone. 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.

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.

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.

RESTRICTED

B.2 PRELIMINARY INFORMATION SECURITY INCIDENT REPORTING FORM

Background Information	
Name of Bureau/Department (B/D):	
Brief description on the affected system (e.g. function, URLs):	
Physical location of the affected system: ❒ Within B/D ❒ External service provider facility **System administered/operated by:** ❒ In-house staff ❒ End user ❒ Outsourced service provider	
Reporting Entity Information	
Name:	***Designation:***
Office Contact:	***24 hours Contact:***
Email Address:	***Fax Number:***
Incident Details	
Date/Time (Detected):	**Date/Time (Reported to GIRO Standing Office):**
Symptoms of Incidents:	

RESTRICTED

RESTRICTED

Impacts:

- ❒ Defacement of website
- ❒ Service interruption (denial of service attack / mail bomb / system failure)
- ❒ Massive infection of computer viruses, hoaxes, or malicious code attack
- ❒ Lost/damage/unauthorised alteration of information
- ❒ Compromise/leakage of sensitive information
- ❒ Intrusion/unauthorised access
- ❒ Others, please specify: _____

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

_____

Is personal data involved in the incident?

- ❒ Yes
- ❒ No

If yes, when the Office of the Privacy Commissioner for Personal Data has been informed: _____(date/time)

Actions Taken:

Current System Status:

Other Information:

RESTRICTED

RESTRICTED

B.3 POST-INCIDENT REPORT

Incident Ref. No.: _____

Post-Incident Report

Bureau/Department	_____
Reporting Officer Details	
Report Date	_____
Reported By	
Name **:**	_____
Designation **:**	_____
Phone No. **:**	_____
Email Addr. **:**	_____
文字	
Incident Details	
Incident Date	_____
Type of Incident:	
System Name and Description:	
Summary of Incident:	
Event Sequence:	
Date / Time ***Event***	

RESTRICTED

RESTRICTED

Action Taken and Result:

Current System Status:

Personnel Involved:

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

Hacker Details (if any):

Computer Virus Details (if any):

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, and etc.):

No. of affected individuals: _____

(breakdown the number of internal staff and citizens)

Type of personal data involved: _____

Whether the affected individuals have been informed: Yes/No. If no, why:

_____

Remarks:

RESTRICTED

Other Affected Sites/Systems:
Damage (including disruption/suspension of service):
Cost Factor (including loss caused by the incident and the recovery cost/manpower):
Recommended Action to Prevent Recurrence:
Other Comments:
Experience Learnt:

RESTRICTED

APPENDIX C ESCALATION PROCEDURE

C.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, and the Police 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:

a. Operation and technical support staff.
b. Respective information system manager, the ISIRT/DITSO and the GIRO Standing Office.
c. Operation team of the affected/involved systems or functions.
d. Technology Crime Division of the Police Commercial Crime Bureau.
e. Information Coordinator for preparation of line-to-take and dissemination of information to the media.

External:

a. Supporting vendors, including the system's hardware or software vendors, application developers, and security consultants etc.
b. Service providers (e.g. data communication providers, ISP).
c. The Office of the Privacy Commissioner for Personal Data.
d. The affected individuals.

C.2 CONTACT LIST

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

a. Name of a dedicated person.
b. His/her post title.
c. Email addresses.

d. Contact phone numbers (for 24 hours contact, if necessary).
e. Fax number.

C.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 Reporting Form to GIRO Standing Office as soon as possible)	*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 Police 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.

APPENDIX D IDENTIFICATION OF INCIDENT

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

Related to user account:

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

Related to file and data:

a. Unexpected files or data creation, modification or deletion.
b. Unfamiliar file names.
c. Unexpected modification to file size or date, especially for system executable files.
d. Unexpected attempts to write to system files or changes in system files.
e. File and data inaccessible.
f. 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.

D.2 INFORMATION COLLECTED FOR IDENTIFICATION

The following information should also be examined during incident identification:

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

D.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
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 trying to overload either the computer system or the network connection in order to disable the system from delivering the normal service to its users.

IT Security Incident	Description
Email bombing	By either sending large volume of unsolicited email to a mail server with a view to launching a type of denial of service attack to the email service, or using the victim's system as a base to launch such attack to a third party's mail server so as to frame the victim.
Large scale malicious code attack	Malicious code attacks include attacks by programs such as computer viruses, Trojan horse programs, worms, and scripts used by crackers/hackers to gain privileges, capture passwords, and/or modify audit logs to hide unauthorised activity. Self-replicating malicious code such as computer viruses and worms can furthermore replicate rapidly, thereby making containment difficult.
Defacement of web page	Unauthorised alteration of the content of one or more web pages of the website.
Eavesdropping	Unauthorised capturing and stealing of data, packet through network or other means of communication.
Compromise	A violation of a security policy in which an unauthorised disclosure or loss of sensitive information may be resulted.
Penetration	The successful unauthorised access to an information system.
Intrusion	Any set of actions that attempt to compromise the confidentiality, integrity or availability of a resource.
Masquerading	The use of another person’s identity to gain excess privilege in accessing system.
Unauthorised access	Physical or logical access to whole or part of an information system and/or its data without the prior permission of the system owner.
Misuse	Misuse occurs when someone uses a computing system for other than the permitted purposes, e.g. when a genuine user uses a Government computer and email account to launch an email bombing attack to others.

IT Security Incident	Description
Fraudulent website or email	The use of fake Government websites or spoofed emails claimed to be sent from the Government with an aim to deceiving recipients or for fraudulent activities. Common attack techniques include *phishing*[1] and *pharming*[2].
Leaking of classified data	Classified data was exposed or accessible by unauthorised persons.

D.4 FACTORS AFFECTING THE SCOPE AND IMPACT OF INCIDENT

Factors affecting the scope and impact of an incident include:

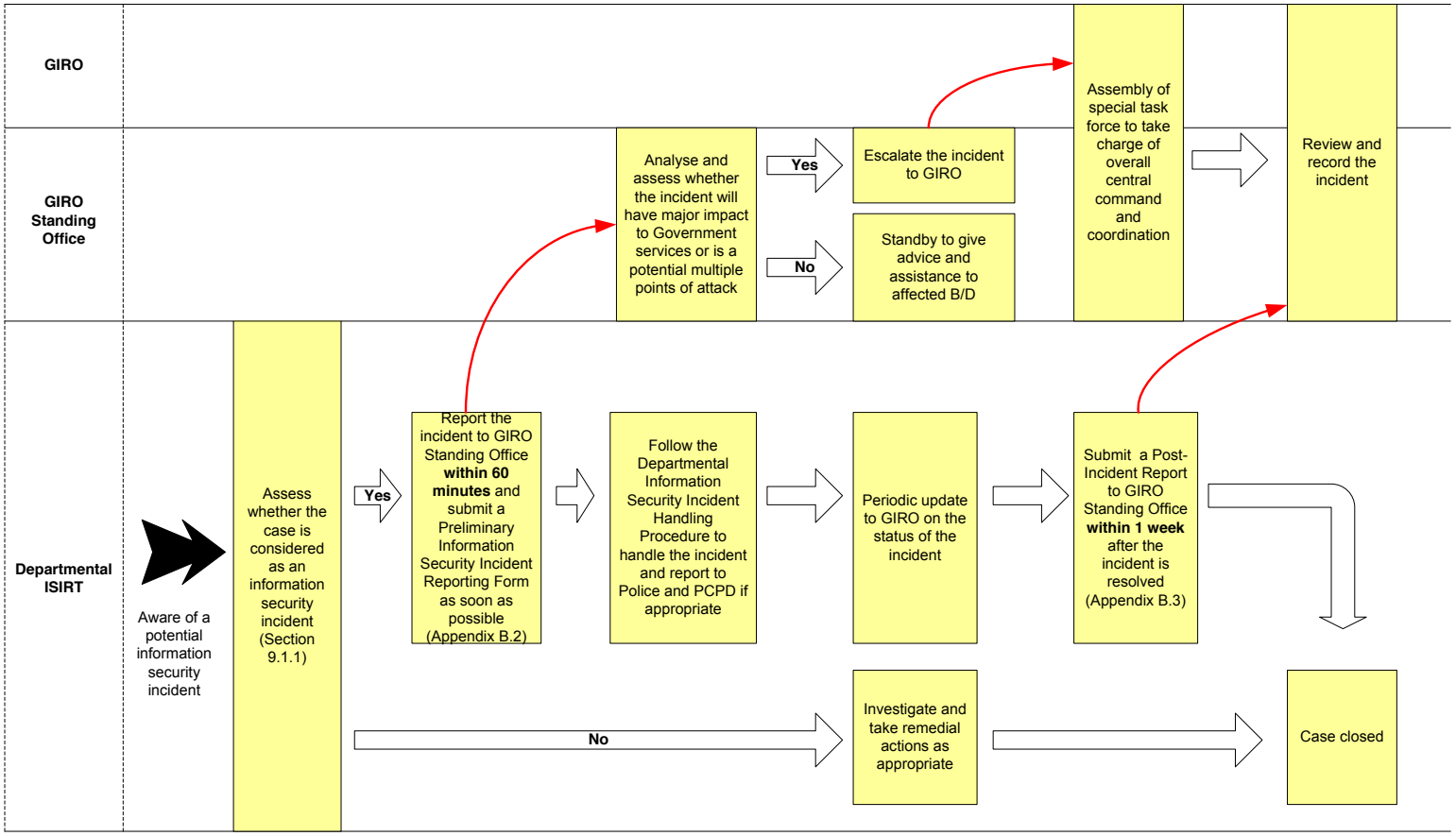
a. The extent of the incident: affecting single or multiple systems.
b. Possible impact on public service and/or image of the Government.
c. Press involvement.
d. Police involvement.
e. Potential damage of the incident.
f. Whether there is sensitive information involved.
g. Entry point of the incident, such as network, Internet, phone line, local terminal, etc.
h. Possibility of local source of attack.
i. Estimated time to recover from the incident.
j. Resources required to handle the incident, including staff, time and equipment.
k. The possibility of further damage.

[1] Phishing: usage of fraudulent or spoofed email to fool recipients into divulging personal information for the purpose of identity theft. The fraudulent email usually directs recipients to a fraudulent website that appears to be a legitimate one.

[2] Pharming: misdirects users to fraudulent sites or proxy servers, typically through DNS hijacking or poisoning.

APPENDIX E SECURITY INCIDENT ESCALATION WORKFLOW

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



APPENDIX F DEPARTMENTAL IT SECURITY CONTACTS CHANGE FORM

Name of Bureau/Department	
Role of the Officer	
☐ Departmental IT Security Officer (DITSO) ☐ Standby Departmental IT Security Officer (DITSO) ☐ Departmental ISIRT Commander ☐ Standby Departmental ISIRT Commander ☐ Departmental Internet System Administrator (System Name: _____) ☐ Standby Departmental Internet System Administrator (System Name: _____) ☐ IT Security SMS Alert Service Subscriber	
The officer to be replaced: _____(*please use separated sheet if more than one officer to be replaced*)	
Contact Information	
Name:	Designation:
Office Phone No.:	Fax No.:
7 X 24 Contact:	Mobile Phone No.: (*Required for IT Security SMS Alert Service Subscriber*)
Lotus Notes Email Address: (*All security contacts will receive emails on IT security related information*)	
Other Lotus Notes email contacts for receiving IT security related information from IT Security Team:	
Nomination By	
Name of DITSO / ISIRT Commander:	Designation:
Signature of DITSO / ISIRT Commander: *(Digital signed by Notes system is accepted)*	Date of Nomination:
Submission to the IT Security Team of the OGCIO	
Please submit the completed form to the IT Security Team via any of the following means: *Email:* *xxxxxxxxxxxxxxxxx* *Fax:* *xxxx xxxx* *Post:* *xxxx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx* *xxxx xxxxxxxx xxxx*	