Hong Kong Computer
Emergency Response Team
Coordination Centre
HKCERT 香港電腦保安事故協調中心

INCIDENT RESPONSE GUIDELINE FOR SMES

Disclaimer

The Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) of the Hong Kong Productivity Council (HKPC) reserves the right to amend the document from time to time without prior notice.

While every attempt has been made to ensure that the information contained in this document is obtained from reliable sources, HKCERT is not responsible for any errors or omissions, or for the results obtained from the use of this information. All information in this document is provided "as is", with no guarantee of completeness, accuracy, timeliness or of the results obtained from the use of this information, and without warranty of any kind, express or implied, including, but not limited to warranties of performance, merchantability and fitness for a particular purpose.

The information contained in this document is intended to provide general information and for reference only. Reliance or use of this information shall be at the reader's own risk. Nothing herein shall to any extent substitute for the independent investigations and the sound technical and business judgment of the reader. In no event will HKCERT, HKPC or its partners, employees or agents, be liable to you or anyone else for any decision made or action taken in reliance on the information in this document, or for any consequential, special or similar damages, even if advised of the possibility of such damages.

Licence

Table of Contents

1. Introduction

1.1 Purpose and Scope

Cyber attacks evolve rapidly as the costs and efforts required for hackers to launch cyber attacks are decreasing due to the development of automation and computing powers. This leads to the increase of various cyber attacks targeting different organisations, public or private, multinational or local. As most small and medium enterprises (SMEs) lack resources to build a wider scope of cyber defence to prevent or block cyber attacks, this makes them an easy target.

This Incident Response Guideline for SMEs aims to help organisations to:

- Understand the roles and responsibilities of incident response handling
- Maintain and maximise their systems' defences with limited resources
- Minimise business and financial impacts in cyber incidents
- Prevent and minimise the reoccurrence of similar cyber attacks

1.2 Definition of Incident and Incident Response

The National Cyber Security Centre (NCSC) of the United Kingdom has defined a cyber incident as an unauthorised access (or attempted access) to an organisation's information technology (IT) systems. These may be breaches or malicious attacks (such as denial of service (DoS) attacks, malware infection, ransomware or phishing attacks).

The National Institute of Standards and Technology (NIST) from the United States has defined "incident handling" (response) as the process of detecting and analysing incidents and limiting their effect. The incident handling process should detect the security breaches, and the incident handlers will then analyse the data and determine how severe the attacks are. The incidents will be prioritised, and the incident handlers will take action to halt the incidents and ensure that the affected systems return to normal operation as soon as possible.

1.3 Reporting and Seeking Advice of an Incident

Local enterprises and Internet users can call the Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT)'s 24-hour hotline: **8105 6060** for incident reporting and seeking security advice on incident response and recovery.

HKCERT accepts reports on information security related incidents such as malware, phishing, web defacement, denial of service attack, etc. HKCERT will assist the investigation of the reported incident, provide information or technical advice, and coordinate the case with appropriate local or overseas parties.

Further details and the report channels of HKCERT are listed in the link below:
https://www.hkcert.org/incident-reporting

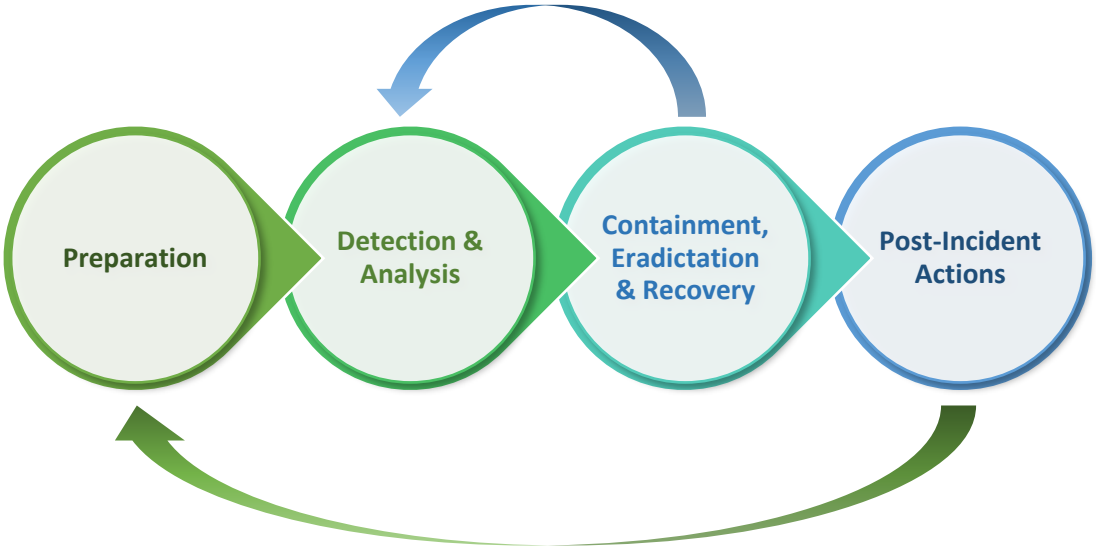
1.4 Document Structure

This Incident Response Guideline for SMEs defines and explains the Incident Response Life Cycle, and outlines the tasks to be performed before, during and after the occurrences of security incidents. Others include setting up a security framework in the organisation, defining roles and responsibilities, etc. Key steps for encountering common incident scenarios are highlighted to guide the organisation to fast-absorb different steps in response to the security incidents.

2. Incident Response Procedure

2.1 Security Incident Response Life Cycle

To manage incident response within the organisation, various incident response life cycle models have been introduced by different authorities. A simplified model from NIST's Computer Security Incident Handling Guide (2012), which divides the incident response life cycle into four phases, is applied and illustrated in the diagram below.



Security Incident Response Life Cycle Diagram referenced from NIST

Preparation

The first phase is Preparation. This is to establish an incident response capability for the organisation to get ready to respond to incidents, and prevent incidents by ensuring that systems, networks and applications are sufficiently secured.

Detection & Analysis

In the Detection and Analysis phase, the aim is to maintain the efficiency and the accuracy in detecting security breaches, thus uncovering the details of the incident by using analytic strategies. The organisation can identify what incident has occurred and be ready to move to the next phase – Containment, Eradication & Recovery.

Containment, Eradication & Recovery

In keeping with the severity of the incident, the organisation can mitigate the impact of the incident by containing it and then ultimately recover from it. During this phase, activities often go back to Detection & Analysis, for example, to see if additional hosts are infected by malware while eradicating a malware incident.

Post-Incident Actions

Once the incident is settled, the organisation should issue a report to detail the cause and cost of the incident and any enhancement measures to prevent future incidents. These are included in the Post-Incident Actions phase. Most importantly, the documents of actions in containment, remediation and resolution of incident should be centrally stored and encrypted, and backed up.

2.2 Formulating the Master Procedure for Incident Response

The organisation should develop a "Master Incident Response Procedure" to provide the general guidelines for incident response. The following scenario questions help direct an incident response planner to decide which elements and information would need to be considered and documented into the master incident response procedure for each phase. A template of incident response procedure is included in **Annex A** for reference.

Preparation:

1. What are the important systems, data and assets to the organisation's business?
2. What are the roles and responsibilities of the organisation's incident response team? Does the organisation maintain an updated contact list for stakeholders?
3. Will the organisation classify this security matter as an incident? If so, which of the organisation's policies does this activity violate?
4. What measures are in place to prevent this type of incident from occurring or to limit its impact?

Detection & Analysis:

1. What precursors of the incident, if any, may the organisation detect? Will any precursors cause the organisation to act before the incident occurred?
2. What indicators of the incident may the organisation detect? Which indicators will suggest that an incident may have occurred?
3. What tools are needed to detect the incident?
4. How will the incident response team analyse and validate this incident? Which personnel will be involved in the analysis and validation process?
5. To whom and which groups inside the organisation should the incident be reported?
6. How will the team prioritise the handling of this incident?

Containment, Eradication and Recovery:

1. What strategy should the organisation take to contain the incident? Why is this strategy preferable to others?
2. What will happen if the incident is not contained?
3. What additional tools will be needed to respond to this particular incident?
4. Which personnel will be involved in the containment, eradication, and/or recovery processes?
5. What evidence (e.g. auditing and accounting logs), if any, should the organisation collect or preserve? How will the evidence be collected? Where will it be stored? How long should it be retained?

Post-Incident Actions:

1. Who should attend the lessons learned meeting regarding this incident?
2. What can be done to prevent similar incidents from occurring in the future?
3. What can be done to improve detection of similar incidents?

2.3 Standard Operating Procedure for Common Incident Scenarios

In handling different incident scenarios, some specific handling steps need to be considered. In addition to the master incident response procedure, it is advised to document those steps into a standard operating procedure for different incident scenarios. The following tables include the key steps in each phase when encountering some common cyber incident scenarios.

Note: Further explanation of "Master Incident Response Procedure" and "Security Incident Response Standard Operating Procedures (SIR SOPs)" will be introduced in **Section 3**.

Scenario 1 – Distributed Denial of Service (DDoS)

Major Phases	Key Steps to Conduct
Preparation	1. Prepare a communication channel for DDoS incidents 2. Define incident escalation paths 3. Evaluate and secure critical system access, and restrict unnecessary permissions 4. Adopt security solutions such as Intrusion Detection and Prevention Systems (IDPS), anti-DDoS services, etc. 5. Establish settings for firewall restriction and, if possible, configure the firewalls to deny all traffic by default
Detection & Analysis	1. Identify abnormal loading by comparing the current usage and baseline loading 2. Determine any systems being affected, retrieve the source from network traffic log 3. Identify how the attack is carried out, such as if the attack is volumetric, vulnerability exploitation, direct attack, reflection attack, through network or application layer, etc. 4. Record the time and volume of the attacks 5. Communicate with affected parties and keep up-to-date communication
Containment, Eradication & Recovery	1. Block the related traffic from IDPS or firewall / Request ISP to block the related traffic nearest to the source 2. Disable possible credentials that may be used for DDoS attack against the affected system 3. Halt traffic by regions, subject to the locations of the major users 4. Stop non-essential services and responses to minimise workload of the system 5. Clear unwanted connections or processes on servers and routers 6. Seek third-party assistance, if required (e.g. some systems may be supported by third-parties such as vendors, use traffic-scrubbing service, etc.)

	7. Update the affected system, if applicable, to fix the DoS vulnerability 8. Restart the suspended services 9. Ascertain the normal resumption of traffic and keep monitoring for abnormal traffic
Post-Incident Actions	1. Review the security of the systems: check firewall configuration, application security, system design, etc. 2. Create an incident report and list out the actions that had been taken 3. Hold discussion(s) for improvement (lessons learned) 4. Contact law enforcement if further actions are required (e.g. report of financial loss due to affected service, etc.)

Scenario 2 – Malware (Includes Ransomware)

Major Phases	Key Steps to Conduct
Preparation	1. Prepare a communication channel for malware incident 2. Define incident escalation paths 3. Evaluate and secure critical system backups, create a possible recovery point and maintain at least one offline backup 4. Install protection software such as anti-malware solution and keep the signature up-to date 5. Establish settings for firewall restriction and, if possible, configure the firewalls to deny all traffic by default 6. Maintain offline backup for important data
Detection & Analysis	1. Isolate the infected system as soon as possible and keep it within powered state 2. Determine the malware and its characteristics, verify if the malware is still running or communicating 3. Analyse the affected area (i.e. how broadly affected in the view of software/systems, file systems, databases, etc.) 4. Check the network and system log for malicious activities, and identify the infection vectors (e.g. email attachments, remote protocols, removable drives, links clicked, etc.) 5. Communicate with affected parties and maintain up-to-date communication
Containment, Eradication & Recovery	1. Quarantine the malware and ensure its complete removal before resuming the normal operation of the system 2. When encountering ransomware attack, find out if a decryptor is available from a trusted source 3. If no decryptor is available, identify possible offline backup and recover the data into unaffected systems/machines 4. Block the network communication which is suspected to the carrier of the malware 5. Seek third-party assistance, if required 6. Proceed data recovery once the malware has been contained

Post-Incident Actions	1. Review the security of the systems: check firewall configuration, check if the malware signature is updated, etc. 2. Create an incident report and list out the actions that have been taken 3. Hold discussion(s) for improvement (lessons learned) 4. Conduct user awareness training 5. Contact law enforcement if further actions are required (e.g. leakage of personal data, etc.)

Scenario 3 – Phishing Email (Includes Scam)

Major Phases	Key Steps to Conduct
Preparation	1. Prepare a communication channel for phishing incident 2. Define incident escalation paths 3. Adopt possible security solutions, such as email gateways, etc. 4. Perform security awareness training, such as phishing drills and phishing trend sharing sessions
Detection & Analysis	1. Run a full scanning of the affected workstation with anti-malware software to find out if any malware has been planted 2. Collect the phishing deliverables (e.g. phishing email), investigate its header and discover the sending source 3. Investigate with the staff, ask for a description and verify if any information has been entered in the phishing site embedded in the email 4. Identify if any files had been downloaded from the link or attachment embedded in the email 5. Check for any unusual activities on the computer 6. Contact the affected parties and mainatain up-to-date communication
Containment, Eradication & Recovery	1. Remove the related phishing email from the computer 2. Identify if other colleagues have also received the email and request them to remove the email from their mailbox 3. Block the related phishing incoming source if possible, through related communication gateways 4. Change the credentials (e.g. passwords) of affected user accounts as soon as possible
Post-Incident Actions	1. Review the rules in communication gateway: check if it is possible to raise the phishing detection level, etc. 2. Create an incident report and list out the actions that have been taken 3. Conduct phishing drills 4. Hold discussion(s) for improvement (lessons learned) 5. Contact law enforcement if further actions are required (e.g. staff has interacted with the phishing source, inform the relevant bank if transactions were made, etc.)

Scenario 4 – Web Defacement / Intrusion

Major Phases	Key Steps to Conduct
Preparation	1. Prepare communication channel for web defacement or intrusion incident 2. Define incident escalation paths 3. Evaluate and secure critical system backups, create possible recovery point 4. Install protection software such as anti-malware solution and keep the signature up-to date 5. Establish settings for firewall restriction and, if possible, configure the firewalls to deny all traffic by default
Detection & Analysis	1. Determine any unnecessary or unauthorised access connected to the affected system, and block the access if it is still in connection state 2. Analyse the affected area (i.e. how broadly affected in the view of software/systems, file systems, databases, etc.) 3. Check network and system log for malicious activities and analyse if any vulnerabilities within the affected system are being used in the attack 4. Contact affected parties and maintain up-to-date communication
Containment, Eradication & Recovery	1. Offline the affected web server, if possible, and redirect the user to a substitute webpage 2. Block the related network traffic from IDPS or firewall 3. Disable possible credentials that may be used for the attack against the affected system 4. Update the affected system if possible, to fix the vulnerability 5. Seek third-party assistance if required
Post-Incident Actions	1. Rebuild the system with updated software, patches, secure configurations and reliable content backup 2. Create an incident report and list out the actions that have been taken 3. Conduct security risk assessment before system launch 4. Hold discussion(s) for improvement (lessons learned) 5. Contact law enforcement if further actions are required (e.g. leakage of personal data, etc.)

2.4 Incident Handling Checklist

To make the adoption of the incident response life cycle methodology for security incidents a simple exercise, the following checklist lists out the common security best practices of incident handling actions. The checklist can be used to self-check against whether the necessary action steps are covered in the formulated incident procedures and during the actual handling of an incident. These steps sorted by phases can ensure that most of the IT systems are ready and prepared for security incidents.

Action		Completed
Preparation		
1	Ensure good behaviour in systems and applications	◯
1.1	Understand the normal behaviours of networks, systems, and applications (Profile networks and systems)	◯
1.2	Identify precursors and indicators through alerts generated by several types of security software	◯
1.3	Create a log retention policy, establish a baseline level for logging and auditing on all systems, and a higher baseline level on all critical systems	◯
1.4	Use and maintain a knowledge database on the normal operation and incident handling steps of the systems and applications	◯
1.5	Keep all host clocks synchronised	◯
2	Enhance data protection	◯
2.1	Identify and verify sensitive data, and enhance its protection	◯
2.2	Safeguard incident data	◯
2.3	Obtain system snapshots through full forensic disk images in addition to file system backups	◯
3	Prepare Handling and Recovery Plan	◯
3.1	Acquire tools and resources that may be of value during incident handling	◯
3.2	Include provisions regarding incident reporting in the organisation's incident response policy	◯
3.3	Follow established procedures for evidence gathering and handling	◯
3.4	Establish mechanisms for incidents reporting and maintain an updated list of contact information	◯
3.5	Ability to capture volatile data from systems as evidence	◯
3.6	Perform incident response drills for the plan	◯
3.7	Review and update the plan regularly	◯

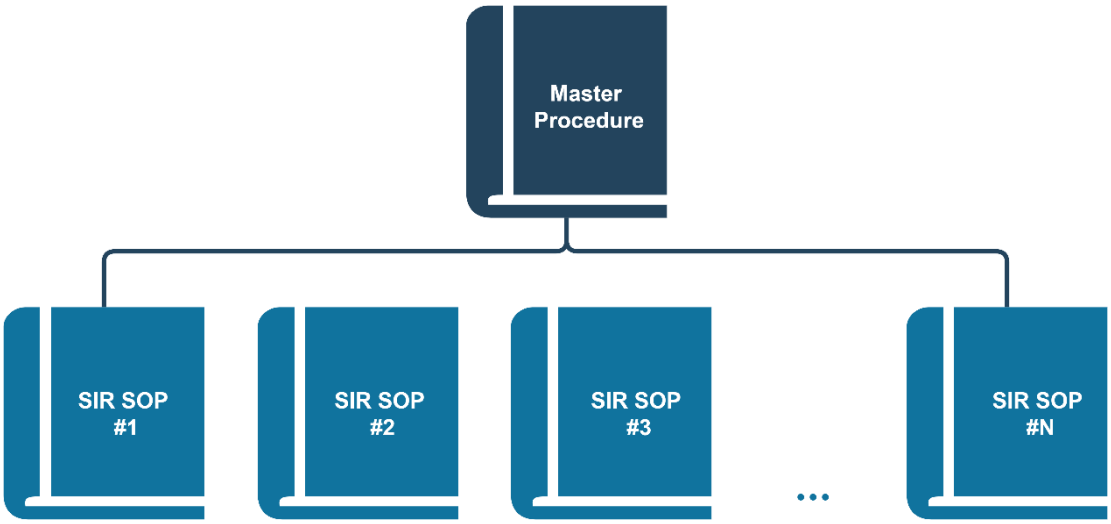
	Action	Completed
Detection and Analysis		
4	Determine whether an incident has occurred	◯
4.1	Analyse the precursors and indicators	◯
4.2	Perform event correlation to look for correlating information	◯
4.3	Perform research (e.g. search engines, knowledge base)	◯
4.4	As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering the evidence, especially volatile data from the systems	◯
5	Prioritise the handling of the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.)	◯
6	Report the incident to the appropriate internal personnel and external parties	◯
Containment, Eradication, and Recovery		
7	Acquire, preserve, secure, and document evidence	◯
8	Contain the incident	◯
9	Eradicate the incident	◯
9.1	Identify and mitigate all vulnerabilities that were exploited	◯
9.2	Remove malware, inappropriate materials, and other components	◯
9.3	If more affected systems are discovered (e.g. new malware infections), repeat the Detection and Analysis steps (4.1, 4.2) to identify all other affected systems, then contain (8) and eradicate (9) the incident for them	◯
10	Recover from the incident	◯
10.1	Resume affected systems to an operationally ready state	◯
10.2	Confirm that the affected systems are functioning normally	◯
10.3	If necessary, implement additional monitoring measures to look for future related activities	◯
Post-Incident Actions		
11	Create a follow-up report	◯
12	Conduct a lessons learned meeting (mandatory for major incidents, optional otherwise)	◯

3. Management of Incident Response

The security policy of an organisation should outline the procedures for security incident response to cover the roles and responsibilities of all parties involved in security incidents, communication with different external parties, the security incident response life cycle, etc.

3.1 Procedures for Incident Response

Although the response to different kinds of security incidents can vary due to the nature of the incidents, it is advised to have a "Master Incident Response Procedure" to provide the general guidelines for incident response in the organisation. For critical and frequently occurring security incidents such as ransomware, data breach, CEO scam and phishing, it is best to have in place dedicated security incident response standard operating procedures (SIR SOPs). New SOPs can be developed for new attacks from time to time while the Master Procedure can be kept intact. The structure can be depicted as the following diagram.



Security Incident Response Standard Operating Procedures link to one Master Procedure

A template of incident response procedure has been included in **Annex A** for the organisation to customise their incident response procedure.

An organisation is obliged to ensure that its incident response procedure is both realistic and efficient to handle security incidents. In addition to the procedure, the followings are some recommended practises for securing networks, systems, and applications, to ensure the security controls are sufficient and facilitate the overall responses to security incident.

- Conduct risk assessment when any change has been made
- Enhance security according to results from risk assessment
- Maintain and monitor host security continuously
- Maintain and monitor network security continuously
- Obtain and customise prevention of cyber attacks
- Run drill-test on incident response procedures and verify the recovery plan
- Carry out user awareness trainings

3.2 Roles and Responsibilities in Incident Response

Robust business practices should include the discussions of organisational risk. Management meetings should feature the discussions of any organisational risks and their updates periodically. Incident response is not solely the responsibility of IT Department. Below is a list of key roles and responsibilities of each party in incident response. SMEs with less resources should pre-assign personnel to take up certain roles and responsibilities to ensure proper response in case of security incidents.

Roles	Responsibilities
IT Management	• Analyse the incident with Business Management to assess the technical impact of the incident and severity level (High, Low or otherwise) • Collect and preserve information regarding the incident • Coordinate incident response and ensure that sufficient resources are provided for incident response • Contain, remediate and resolve the incident, and document the actions with timestamp • Determine if production service should be taken offline until incident resolution with inputs from Business Management • Escalate high severity incidents • Manage the post-incident process and work with business unit to compile the evaluation report to document lessons learned and follow-up • Perform regular system monitoring • Prepare the organisation to respond to security incidents, such as providing guidelines and training to first responders (system administrators) and setting up communicating protocol with business units • Provide a hotline for reports of incidents and respond to them

Business Management	• Assess the business impact of the incident • Be the owner of business data and business systems • Collect information regarding the incident at the request of IT Management • Determine if the incident is related to an abuse • Determine if contingency plans need to kick in for prolonged outage • Join IT Management in compiling the incident evaluation report and follow-up • Implement security controls as specified and monitor systems for signs of attack or unauthorised/inappropriate access • Provide physical and procedural safeguards for information resources • Report suspicious events which may lead to incident occurring to IT Management
Other Teams	There are other teams which may be involved in incident response, such as Business Continuity / Disaster Recovery Management, Crisis Management. They should be under the security management team of the organisation.
Out-sourced Parties	Organisations may have some hardware or software that are out-sourced to other IT companies to maintain their operation. The organisation should always communicate with the out-sourced parties to keep them up-to-date on incident response handling procedures, and find out "who is responsible when certain issue occurs" and "how to resume normal operation". The mentioned two scenarios should be included in the Service Level Agreement (SLA), and discussed at length between the two parties.

Managing a list of Report Channels with the most up-to-date contact information for the stakeholders while handing the incident is essential and the contact list should be reviewed regularly and easily accessible. The protocol for reporting incidents is listed in **Annex B**, with IT Management being notified of all High Severity incidents. External parties as well as local and overseas parties may need to be acknowledged, depending on different scenarios of security incidents.

Annex A – Incident Response Procedure Template

Information	Details
Short Description	
Incident Type	☐ DDoS ☐ Intrusion ☐ Malware ☐ Phishing ☐ Ransomware ☐ Web Defacement ☐ Others:
Affected IT Systems	Hardware: Software:
Severity	Low 0 | 1 | 2 | 3 | 4 | 5 High
CIA Triad Involved	Confidentiality ☐ Integrity ☐ Availability ☐
Size of Impact	Business Impact:
Date/Time of Occurrence	
Date/Time of Discovery	
Initial Findings	How occurred: Why occurred: Vulnerabilities identified:
Personal Data Involved	☐ Yes / ☐ No If yes, what personal data is involved? Reported to PCPD? ☐ Yes / ☐ No
Maximum Tolerable Period	

Life Cycle Phases	Action Taken
Preparation	
Detection & Analysis	
Containment, Eradication & Recovery	
Post-Incident Actions	

Annex B – Incident Report Channel

Organisations should identify a standard set of incident-related data to be collected for each incident and establish an incident report channel to facilitate more effective and consistent incident handling.

Report Channel for Internal Contacts & IT Service Providers
Any of the following resources may be used to report an incident for investigation and remediation by Report Channel.

> Name: XXX Company / XXX Team
>
> Location: Office, x/F, Office Building
>
> Phone Number: +852 XXXXXXXX (24-hour hotline)
>
> Email Address: [email address of service desk]
>
> Service Level: 8 x 5 x NBD / 7 x 24 x 4
>
> Corresponding Incident / System: [Incidents / Systems]

Security incidents communication must be treated on a 'need-to-know' basis. Individuals who are not directly involved in the handling of the incident must not be given information about the existence of the incident or the methods used to contain or remediate the incident, especially external parties such as IT service providers.

External Parties
Incident response might involve communication with external parties other than IT service providers. There should be dedicated contact points for each external party, and the line-to-take should be consented among senior management, such as:

- Law enforcement – report potential cyber crimes
- Regulator – report security incident within time limit mandated by regulation
- Press – announce company response to security incident

The following table lists the report channels of various official parties whom incident response handlers might find helpful when encountering different scenarios of security incident.

Incident Types	Report Parties
Criminal Offences (e.g. Online Fraud, Cases with Financial Loss)	Cyber Security and Technology Crime Bureau of the Hong Kong Police: https://www.erc.police.gov.hk/index_en.html
Complaint relating to Personal Data	Office of the Privacy Commissioner for Personal Data (PCPD), Hong Kong: https://www.pcpd.org.hk/english/enforcement/data_breach_notification/dbn.html
Unsolicited Electronic Messages (Spam)	Office of the Communication Authority, Hong Kong: https://eform.one.gov.hk/form/oca014/en/

Annex C - List of Reference Publications

Publisher	Publication Name
HKCERT	SME Information Security Guideline (2007) https://www.hkcert.org/f/guideline/180877/def2c7e6-4fdb-42f5-b68a-98250b397a93-DLFE-810.pdf
HKCERT	Self Help Guide for Security Incidents https://www.hkcert.org/resources/faq/self-help-guide-for-security-incidents
HKCERT	Seven Habits of Cyber Security for SMEs (2018) https://www.hkcert.org/security-guideline/seven-habits-of-cyber-security-for-smes
GovCERT.HK / OGCIO	Practice Guide for Information Security Incident Handling (2021) https://www.govcert.gov.hk/doc/ispg-sm02-v1.2_en.pdf
InfoSec / OGCIO	Security Incident Handling for Companies https://www.infosec.gov.hk/en/best-practices/business/security-incident-handling-for-companies
NIST US	Computer Security Incident Handling Guide (2012) https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
NCSC UK	Small Business Guide Collection: Cyber Security Response and Recovery (2020) https://www.ncsc.gov.uk/files/NCSC_A5%20Response%20and%20Recovery%20Guide_v3_OCT20.pdf
SANS	Incident Handler's Handbook (2011) https://www.sans.org/white-papers/33901
SANS	Incident Handling for SMEs (Small to Medium Enterprises) (2008) https://www.sans.org/white-papers/32764

Hong Kong Computer
Emergency Response Team
Coordination Centre
香港電腦保安事故協調中心

HKCERT