IT Incident Response Guidelines in PPDH

1. Introduction

A cyber incident is an unauthorised access (or attempted access) to PPDH'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].

For incident reporting and seeking security advice on incident response and recovery, PPDH may contact the Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT)'s 24-hour hotline: **8105 6060**

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

2. Standard Operating Procedure for Common Incident Scenarios

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.)

IT Incident Response Guidelines in PPDH

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. Install protection software such as anti-malware solution and keep the signature up-to date 4. Establish settings for firewall restriction and, if possible, configure the firewalls to deny all traffic by default
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. Block the network communication which is suspected to the carrier of the malware 4. Seek third-party assistance, if required 5. 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 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 maintain 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.)

IT Incident Response Guidelines in PPDH

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. Install protection software such as anti-malware solution and keep the signature up-to date 4. 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.)

3. Incident Handling Checklist

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	◯

IT Incident Response Guidelines in PPDH

	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)	◯

4. Roles of Incident Response

Roles	Responsibilities
Information Technology Office	• Analyse the incident to assess the technical impact of the incident and severity level • 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 user, if necessary • Escalate high severity incidents to both SHA1 and HA1 immediately • 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
Senior Hospital Administrator 1 (or Hospital Administrator in the absence of SHA1)	• Assess whether the case would need to report to any one of the External Parties listed below • Clear with the proposed action with the Comptroller before any reporting • Assess if the Health Bureau and the Board of Governors should be informed about the incident
User	• 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

IT Incident Response Guidelines in PPDH

External Parties

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/

5. Confidentiality

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

Any disclosure of information about incidents, including how to compromise and the background of the system such as physical location or operating system, may encourage hackers to intrude other systems with the same vulnerabilities. Moreover, the disclosure may influence the forensic and prosecution processes under investigation by Hong Kong Police Force.

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	

IT Incident Response Guidelines in PPDH

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