Office of the Commissioner of Critical Infrastructure (Computer-system Security)
Security Bureau
The Government of the Hong Kong Special Administrative Region of the People's Republic of China

Written Report for Computer-System Security Incident

Pursuant to section 28(4) of the Protection of Critical Infrastructures (Computer Systems) Ordinance

*All fields should be completed as far as practicable based on the information available.

A. Background Information

1) Information of Critical Infrastructure Operator ("CI Operator")

Full Name:

2) Critical Computer System(s) Affected

Name	**Physical Location** *(address in Hong Kong, or specify the country name if located outside Hong Kong)*

(if insufficient space, please attach a separate signed sheet with details)

B. Incident Overview

1) Nature †

- ☐ Phishing / social engineering
- ☐ Ransomware / malware attack
- ☐ Data breach (leakage / tempering)
- ☐ Denial-of-service (DoS / DDoS) attack
- ☐ Others (please specify):
- ☐ Trojan horse
- ☐ Supply chain attack
- ☐ Website defacement
- ☐ Unauthorized system access / intrusion
- ☐ Spoofing
- ☐ Insider threat
- ☐ Man-in-the-Middle attack

2) Brief Incident Description

3) Initial Attack Vector / Point of Intrusion

4) Root Cause Analysis Summary

Root cause(s) of the incident and contributing factor(s):

Whether the root cause was identified in previous security assessment or audit:
(if yes, why the incident could not have been prevented; if not, why it was not identified)

5) Earliest Identifiable Time of the Incident	***Date*** (dd/mm/yyyy)**:**	***Time*** (hh:mm)**:**
6) Time Becoming Aware of the Incident	***Date*** (dd/mm/yyyy)**:**	***Time*** (hh:mm)**:**

7) How was the incident first detected?

By External Means

- ☐ Threat Actor Disclosure
- ☐ Customer/Client
- ☐ External Audit
- ☐ Third Party Vendor
- ☐ Peer/Competitors
- ☐ Anonymous Source

By Internal Means

- ☐ Computer-system Security Management
- ☐ Unit Internal Audit Personnel
- ☐ Other Employee

By Other Means

- ☐ Please specify:

8) Hardware or software where vulnerabilities are found

(for hardware, please specify name, manufacturer, model and firmware version; for software, please specify name, publisher and version)

Item	Hardware/ Software	Descriptions
1		
2		
3		

(if insufficient space, please attach a separate signed sheet with details)

C. Impact Assessment

1) Scope of Impact (*which parts of the CCS were affected*):

2) Operational/ Service Impact (*how operations or services of CI were disrupted*):

3) Data Impact (*if any sensitive information was compromised, altered or lost*)**:**

4) Customer/Third-party Impact (*any effect on customers or third parties*)**:**

5) Financial Impact (*any direct financial loss as a result of the incident*)**:**

Estimated HK$

6) Other Impact(s) (*if any*)**:**

7) Duration of Disruption (*how long the incident impacted operations or services*)**:**

D. Response Actions

1) Follow-up action(s) taken †

Damage Containment:

- ☐ Affected systems or network segments have been isolated
- ☐ Compromised accounts have been removed or isolated
- ☐ Malicious IPs / domains have been blocked
- ☐ Others (please specify):

Remediation and Recovery

- ☐ Malware have been removed
- ☐ Affected systems have been restored
- ☐ Security patches have been applied / Vulnerabilities have been fixed
- ☐ Others (please specify):

2) What is the current status of operation of the CCS(s)?

- ☐ Operation is still not available
- ☐ Operation is being provided by resilience site
- ☐ Operation in primary site has resumed normal

3) Measures planned to strengthen security and prevent re-occurrence †

- ☐ Policy / procedure updates
- ☐ Training / awareness building
- ☐ Review security assessment or audit procedures
- ☐ Others (please specify)
- ☐ Security monitoring
- ☐ Configuration changes
- ☐ Security patches / updates

Description of planned measures:

4) Timeline for implementing the remedial measures?

5) Any external team or services engaged †?

- ☐ External consultant:
- ☐ Vendor:
- ☐ Internet service provider:
- ☐ Others (please specify):

E. Stakeholder and Media Communication

1) Has the incident been communicated with relevant stakeholders †?

- ☐ The Board of Directors / senior management
- ☐ Designated authority (via. HKMA / OFCA)
- ☐ Police (case reference number:)
- ☐ Office of the Privacy Commissioner for Personal Data
- ☐ Affected customers / Clients
- ☐ Third parties (vendors / business partners)
- ☐ Others (please specify):

2) Has the incident been communicated to the media?

- ☐ Yes† Please specify the date (dd/mm/yyyy):
  - ☐ Press conference:
  - ☐ Press release:
  - ☐ Reply to press enquiry was made/issued:
- ☐ No

F. Reporting Entity Information

Name:	Post Title:
Office & Mobile Contact:	Email Address:
Report Submission Date (dd/mm/yyyy):	

Personal Information Collection Statement: The personal information provided will be used for the purpose of exercising the powers and duties vested in the Commissioner of Critical Infrastructure (Computer-system Security) ("the Commissioner") under the Protection of Critical Infrastructures (Computer Systems) Ordinance ("the Ordinance") and be retained by the Commissioner for an appropriate period of time necessary for the fulfilment of the relevant purposes or as required by the Ordinance. The Commissioner may disclose the personal information to the parties permitted by section 57(3) of the Ordinance. The data subject or relevant persons as defined in section 2 or 17A of the Personal Data (Privacy) Ordinance ("the PDPO") have a right of access and correction with respect to personal information as provided for in sections 18 and 22 and Principle 6 of Schedule 1 of the PDPO. The right of access includes the right to obtain a copy of the personal information provided in this form. Enquiries concerning the personal information collected by means of this form, including access and corrections, should be addressed to the Commissioner via email at protection_ci@sb.gov.hk.