CITY UNIVERSITY OF HONG KONG
Information Security Incident Management Standard

(Approved by the Information Strategy and Governance Committee in December 2013; revision 1.1 approved by Chief Information Officer in September 2015)

Document Control

Document Owner	Classification	Publication Date
OCIO	INTERNAL	2015-10-19

Revision History

Version	Date	Summary of Changes
1.0	2013-12-19	Initial Release
1.1	2015-08-25	Typo correction

Distribution

Copy	Issued to	Location
Master	Public	http://www6.cityu.edu.hk/infosec/isps/docs/?page=00.about

Contents

1 Objective

The objective of this standard is to establish the procedure for dealing with a security incident that occurs, in form of intervention to contain, negate or minimize the impact of the security incident; for communicating to the relevant parties to get their attentions; and to ensure a quick, effective, and orderly response to security incidents.

This procedure also governs the reporting and management of information security related incidents within the University.

2 Definitions

2.1 Information Security Incident

An information security incident is defined as:

"Successful unauthorized access, use, disclosure, modification or destruction of information; interference with information technology operation; or violation of explicit or implied acceptable usage policy"

Examples of security incidents are as follows:

- Service experienced an unplanned outage
- Unauthorized modification or deletion of data
- Unauthorized modification of system software, hardware or connections
- Modification of system hardware, software or connections in breach of the Information Security Policy
- Hacking or attempted hacking by insiders or outsiders
- Suspected or actual illegal activity
- Unauthorized use of systems
- Unauthorized copying of information or software

2.2 Personal Data Incident

A personal data incident is a breach of personal data. A classic example is the unintended leakage of personal data to unauthorized parties. The "Personal Data (Privacy) Issues - Code of Practice" of the University provides guidance on the use of personal data. Any breach of personal data must be reported to the Data Protection Officer of the University.

3 Information Security Incident Response Team ("ISIRT")

The University shall establish its ISIRT, which directly responsible for information security incidents that will cause or have caused impact on the University's information systems, information resources, operations or members.

The ISIRT shall be led by the University's Information Security Unit. Members of the IRIST shall include staff members from IT team specialized in particular topics, such as Operating Systems, Networking, Database, etc. The ISIRT may also comprise personnel from other Units of the University.

A Departmental ISIRT is recommended to be established in each University Unit who are managing substantial information systems, or frequently involved in information security incidents.

4 Roles and Responsibilities

4.1 All Staff members, Contractors and Students

- Report security weakness and suspicious security incidents to the Help Desk of Computing Services Centre ("CSC") or ISIRT
- Keep appropriate records of systems so that exceptional events are noticed and can be presented to Information Security Incident Response Team ("ISIRT") for investigation and handling
- Assist the ISIRT members in investigating and resolving the incidents

4.2 Information Security Incident Response Team ("ISIRT")

- Ensuring that all incidents are comprehensively recorded, assessed for impact, investigated and handled by IT security staff with sufficient knowledge and appropriate skill set
- Timely report to the management and escalate to management for appropriate actions if necessary
- Assessing the improvement areas by coordinating with relevant University Units
- Help detecting the occurrence of security incidents, contain the scope of damages, eradicate the root cause of security incidents, coordinate the recovery of affected networks and systems by security incidents, and prevent the same security incident from happening again
- Departmental ISIRT is responsible for handling local incidents, with scope of impact limited to individual units
- For incidents affecting several units, Departmental ISIRTs are responsible for providing support and liaison to ISIRT of Central IT

4.3 Management

- Investigating and following up escalated information security incidents by notifying appropriates, such as media and government authorities, and mobilizing the University's resources for incident resolution
- Monitoring and tracking the status of escalated incidents
- Initiating disciplinary procedure if the incidents are resulted from staff misconduct
- Reviewing the deficiencies or improvement opportunities identified by internal or external audits or post information security incident review and supervise the execution of any remediation actions required

5 Reporting

The ISIRT and Departmental ISIRT must ensure that the following information is recorded and available for further process:

- Incident date and time
- Name and contact information of the reporter

- Incident category (e.g. software, hardware or data)
- Affected information systems/resources
- Detailed description of incident
- Incident Impact level
- ISIRT member assigned
- Estimation of number of affected user
- All actions taken, including the date, time and personnel (internal or external) who take the action
- Incident duration and actual time of service interruption of each affected IT service

Any breach of personal data must be reported to the Data Protection Officer of the University.

Any Information Security Incident with impact level evaluated to "Important", "Significant" or "Critical" (refer to section 6 for impact level) must be reported to the Office of the Chief Information Officer for recording purpose.

Information about incident should be disclosed only on a need-to-know basis.

6 Incident Analysis

Upon receiving report on security weakness or security incident, the ISIRT shall analyze and validate the incident.

When there are evidence showing that an incident has occurred, ISIRT should perform an initial analysis to determine the scope of the incident, and assess the impact on the University's information system, information resources and operations.

The ISIRT shall evaluate the impact level:

Critical	If not resolved immediately, the incident will result in unscheduled service interruption of critical service, or severe security breach together with financial loss or reputation damage.
Significant	If not resolved timely, the incident may affect the normal operation of core services and lead to security breach. Financial loss or reputation damage is also probable.
Important	If not resolved within a reasonable period of them, may introduce additional vulnerabilities and expose the information systems or resource to higher risk of service interruption. Financial loss or reputation damage is possible if such vulnerabilities are exploited accidentally or by malicious parties.
Low	The incident is related to non-critical information systems or non-sensitive data, and the possibilities or causing service interruption, financial loss or reputation is remote. However, it may require additional controls or alternative operational procedures to retain service level and could lead to downgrade of efficiency
Minimal	The incident has no impact on information systems or resources of the University.

When in doubt, ISIRT should assume the worst until additional analysis indicates otherwise.

7 Containment

The ISIRT shall deploy a handling team to contain the incident to limit the scope, impact and magnitude; before the spread of it overwhelms resources or the damage increases.

Handlers should keep the process a low profile. Handlers should avoid tracing back the attacker with obvious method (e.g. ping, tracert, nslookup or telnet).

Activities in incident containment may include:

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

Handlers should not assume that further damage could be prevented by disconnecting a host from the network, as a compromised host may malicious process that overwrite all data on the host's hard drive when it is disconnected.

8 Escalation and Notification

The ISIRT must escalate any "Critical" and "Significant" information security incidents to the University's senior management as soon as possible, and within 2 working days validating the incident has one or more of the following characteristics:

- The incident is assessed to have the impact level of "Critical" and "Significant"
- The incident has the potential of impacting the third parties, other Institutions or even the general public
- The incident cannot be resolved within the required time period based on its impact level
- The incident is escalated from external parties, such as other Institutions, government authorities or third parties

The University's senior management shall keep track of the escalated incidents throughout the entire handling process till resolution. Affected parties, including staff, students, contractors, third parties or the general public should be notified in accordance with the scale of the impact.

9 Eradication and Recovery

During eradication, the ISIRT shall identify the root causes, and eliminate components of the incident, such as deleting malicious code, and disabling breached user accounts.

In recovery, systems, applications and data are restored from trusted backup to normal operation. The ISIRT shall validate the system security. If applicable, administrators shall harden the systems to prevent similar incidents.

10 Lessons Learnt

The ISIRT shall prepare a draft follow-up report, and submit the draft report to all parties for review and comments. The report may include:

- Recommended actions to prevent further attack
- Information that is needed quickly and the way to get the information
- Additional tools used or needed to aid in the detection and eradication process
- Sufficiency in respect of preparation and response
- Adequacy in communication
- Practical difficulties
- Damage of incident, which may include:
    - manpower costs required to deal with the incident
    - monetary cost
    - cost of operation disruption
    - value of data, software and hardware lost or damaged, including sensitive data disclosed
    - legal liability of entrusted confidential data
    - public embarrassment or loss of goodwill
- Other experiences learnt

The finalized report will provide a reference that can be used to assist in handling similar incidents. The finalized report should be kept for at least 3 years.

References

The following documents were consulted during the preparation of this document:

Office of the Government Chief Information Officer, Government of Hong Kong (2012), *Information Security Incident Handling Guidelines (G54)*

National Institute of Standard and Technology, U.S. Department of Commerce (2012), *Computer Security Incident Handling Guide - NIST Special Publication 800-61 Revision 2*