7.3. Managing Information Security Incidents

Objective

7.3.1. Organisations have processes implemented for incident identification, management and analysis of information security incidents, including selection of appropriate remedies which will assist in preventing or reducing the impact of future information security incidents.

Context

Scope

7.3.2. This section covers information relating primarily to managing information security incidents. The management of physical and personnel security incidents is considered to be out of scope unless it directly impacts on the protection of systems (e.g. the breaching of physical protection for a server room).

7.3.3. It is important to note that, in most cases, information systems are likely to be affected.

References

7.3.4. Additional information relating to the management of ICT evidence is contained in:

Reference	Title	Publisher	Source
ISO/IEC 27037:2012	**Information Technology – Security Techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence.**	ISO	https://www.iso.org/standard/44381.html
HB 171:2003	**Guidelines for the Management of Information Technology Evidence**	Standards Australia	https://www.saiglobal.com/PDFTemp/Previews/OSH/as/misc/handbook/HB171.PDF [PDF, 350 KB]
	Incident Response	NCSC	Incidents | National Cyber Security Centre (ncsc.govt.nz)

Rationale & Controls

Information security incident management documentation

7.3.5.R.01. **Rationale**

Ensuring responsibilities and procedures for information security incidents are documented in relevant Information Security Documentation will ensure that when an information security incident does occur, agency personnel can respond in an appropriate manner. In addition, ensuring that system users are aware of reporting procedures will assist in identifying any information security incidents that an ITSM, or system owner fail to notice.

7.3.5.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:1260]

Agencies MUST detail information security incident responsibilities and procedures for each system in the relevant Information Security Documents.

7.3.5.R.02. **Rationale**

Alternative communications efforts should be established to avoid using potentially compromised infrastructure to communicate during an incident.

Recording information security incidents

7.3.6.R.01. **Rationale**

The purpose of recording information security incidents is to highlight the nature and frequency of information security incidents so that corrective action can be taken. This information can subsequently be used as an input to security risk assessments of systems.

7.3.6.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1264]

Agencies SHOULD ensure that **all** information security incidents are recorded in a register.

7.3.6.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1266]

Agencies SHOULD use their incidents register as a reference for future security risk assessments.

Handling data spills or data breach

7.3.7.R.01. **Rationale**

A data spill or data breach is defined as the unauthorised or unintentional release, transmission or transfer of data. If there is a possibility that sensitive or classified information may be compromised as a result of an information security incident, agencies need to be able to respond in a timely fashion to limit damage and contain the incident.

For example, Data Loss Prevention (DLP) techniques and tools such as network activity monitoring, endpoint DLP tools, data classification can aid in detecting and preventing data spills or data breaches.

7.3.7.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:1271]

Agencies MUST implement procedures and processes to detect data spills or data breach.

7.3.7.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:1273]

When a data spill occurs agencies MUST assume that data at the highest classification held on or processed by the system, has been compromised.

7.3.7.C.03. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:1274]

Agency SOPs MUST include procedure for:

- all personnel with access to systems;
- notification to the ITSM of any data spillage or breaches; and
- notification to the ITSM of access to any data which they are not authorised to access.

7.3.7.C.04. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:1275]

Agencies MUST document procedures for dealing with data spills or data breaches in their IRP.

7.3.7.C.05. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:1276]

Agencies MUST treat any data spill or data breach as an information security incident and follow the IRP to deal with it.

7.3.7.C.06. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:1277]

When a data spill or data breach occurs agencies MUST report the details to the Privacy Commissioner and information owner in accordance with the Privacy Act 2020.

Containing data spills

7.3.8.R.01. **Rationale**

The spillage of classified information onto a system not accredited to handle the information is considered a serious information security incident. It may be a critical information security incident if personal information or particularly sensitive information is spilled. Refer to Section 7.2 – Reporting Information Security Incidents.

7.3.8.R.02. **Rationale**

Isolation may include disconnection from other systems and any external connections. In some cases system isolation may not be possible for architectural or operational reasons.

7.3.8.R.03. **Rationale**

Segregation may be achieved by isolation, enforcing separation of key elements of a virtual system, removing network connectivity to the relevant

device or applying access controls to prevent or limit access.

7.3.8.R.04. **Rationale**

It is important to note that powering off a system can destroy information that may be useful in forensics analysis or other investigative work. In large, inter-connected systems, powering off a system may not be feasible.

7.3.8.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:1283]

When classified information is introduced onto a system not accredited to handle the information, the following actions MUST be followed:

1. Immediately seek the advice of an ITSM;
2. Segregate or isolate the affected system and/or data spill;
3. Personnel MUST NOT delete the higher classified information unless specifically authorised by an ITSM.

7.3.8.C.02. **Control System Classifications(s): All Classifications; Compliance: Must Not** [CID:1284]

When classified information is introduced onto a system not accredited to handle the information, personnel MUST NOT copy, view, print or email the information.

7.3.8.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1285]

When a data spill or data breach involving classified or sensitive information or contamination of classified systems occurs and systems cannot be segregated, or isolated agencies SHOULD immediately contact the NCSC for further advice.

Handling malicious code infection

7.3.9.R.01. **Rationale**

Malicious code or malware is defined as software that attempts to compromise the confidentiality, integrity or availability of a system. This guidance for handling malicious code infections assists organisations have the procedures and processes in place to manage potential infections, further spread and similar future infections. Important details include:

- the infection date/time of the machine;
- any observed effects and source details;
- the possibility that system records and logs could be compromised; and
- the period of infection.

7.3.9.R.02. **Rationale**

Positive detection of malicious code will require the below steps to occur:

- Isolation of infected systems to prevent further spread. Check connected systems and media for infections and isolate as required;
- Removal of the malicious code should be performed with appropriate malware removal tools;
- Eradication and recovery in some cases would require restoring systems with original media.

7.3.9.R.03. **Rationale**

Agencies should be aware that some malicious code infections such as rootkits, employ persistence mechanisms. This will require specialist assistance or advice to detect and eradicate .

7.3.9.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1290]

Agencies SHOULD follow the steps described below when malicious code is detected:

- isolate the infected system;
- decide whether to request assistance from NCSC;
- if such assistance is requested and agreed to, delay any further action until advised by NCSC;
- check connected systems and media including backups for malicious code;
- isolate all infected systems and media to prevent reinfection;
- change all passwords and key material stored or potentially accessed from compromised systems, including any websites with password controlled access;
- advise system users of any relevant aspects of the compromise, including a recommendation to change all passwords on compromised systems;
- revoke all session tokens associated with user and/or device;
- use up-to-date anti-malware software to remove the malware from the systems or media;
- monitor network traffic for malicious activity;
- record and report the information security incident and perform any other activities specified in the IRP; and
- in certain scenarios rebuilding and reinitialising the system and/or user profile may be required.

Allowing continued attacks

7.3.10.R.01. **Rationale**

Agencies allowing an attacker to continue an attack against a system in order to seek further information or evidence will need to establish with their business owner(s) and legal advisor(s) whether the actions are breaching any business service level agreements or contractual obligations.

7.3.10.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:1294]

Agencies considering allowing an attacker to continue some actions under controlled conditions for the purpose of seeking further information or evidence MUST seek legal advice.

Integrity of evidence

7.3.11.R.01. **Rationale**

While gathering evidence it is important to maintain the integrity of the information and the chain of evidence. Even though in most cases an investigation does not directly lead to a police prosecution, it is important that the integrity of evidence such as manual logs, automatic audit trails and intrusion detection tool outputs be protected. This may also include a record of activities taken by the agency to contain the incident.

7.3.11.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1297]

Agencies SHOULD:

- transfer a copy of raw audit trails and other relevant data onto media for secure archiving, as well as securing manual log records for retention; and
- ensure that all personnel involved in the investigation maintain a record of actions undertaken to support the investigation.

Seeking assistance

7.3.12.R.01. **Rationale**

After detecting an information security incident, organisations need to preserve the evidence prior to taking any remediation steps. For example, snapshots including memory of virtual machines. This greatly increases NCSC's ability to provide assistance.

7.3.12.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1300]

Agencies SHOULD ensure that any requests for NCSC assistance are made as soon as possible after the information security incident is detected and that no actions which could affect the integrity of the evidence are carried out prior to NCSC's involvement.