Information security manual

Guidelines for cyber security incidents

Last updated: September 2026

Managing cyber security incidents

Cyber security incident management policy

Establishing a cyber security incident management policy can increase the likelihood of successfully planning for, detecting and responding to malicious activity on networks and hosts, such as cyber security events and cyber security incidents. In doing so, a cyber security incident management policy will likely cover the following:

- responsibilities for planning for, detecting and responding to cyber security incidents
- resources assigned to cyber security incident planning, detection and response activities
- guidelines for triaging and responding to cyber security events and cyber security incidents.

Furthermore, as part of maintaining the cyber security incident management policy, it is important that it, along with its associated cyber security incident response plan, is exercised at least annually to ensure it remains fit for purpose.

Control: ISM-0576; Revision: 10; Updated: Sep-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
A cyber security incident management policy, and associated cyber security incident response plan, is developed, implemented and maintained.

Control: ISM-1784; Revision: 1; Updated: Sep-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The cyber security incident management policy, including the associated cyber security incident response plan, is exercised at least annually.

Cyber security incident register

Developing, implementing and maintaining a cyber security incident register can assist in ensuring that appropriate remediation activities are undertaken in response to cyber security incidents. In addition, the types and frequency of cyber security incidents, along with the costs of any remediation activities, can be used as input to future risk assessment activities.

Control: ISM-0125; Revision: 6; Updated: Dec-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
A cyber security incident register is developed, implemented and maintained.

Control: ISM-1803; Revision: 0; Updated: Dec-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
A cyber security incident register contains the following for each cyber security incident:

- *the date the cyber security incident occurred*
- *the date the cyber security incident was discovered*
- *a description of the cyber security incident*
- *any actions taken in response to the cyber security incident*
- *to whom the cyber security incident was reported.*

Insider threat mitigation program

As an insider's authorised access to systems and their resources may make them harder to detect when intentionally performing malicious activities, establishing and maintaining an insider threat mitigation program can assist an organisation to detect and respond to indicators of potential insider threats before they occur, or limit damage if they do occur. In doing so, an organisation will likely obtain the most benefit by logging and analysing the following activities:

- excessive copying or modification of data
- unauthorised or excessive use of removable media
- connecting devices capable of data storage to systems
- unusual system usage outside of normal business hours
- excessive data access or printing compared to their peers
- data transfers to unauthorised cloud services or webmail
- use of unauthorised virtual private networks, file transfer applications or anonymity networks.

Control: ISM-1625; Revision: 2; Updated: Jun-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
An insider threat mitigation program is developed, implemented and maintained.

Control: ISM-1626; Revision: 1; Updated: Jun-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Legal advice is sought regarding the development and implementation of an insider threat mitigation program.

Reporting cyber security incidents

Reporting cyber security incidents to the chief information security officer, or one of their delegates, as soon as possible after they occur or are discovered provides senior management with the opportunity to assess the impact to their organisation and to oversee any cyber security incident response activities. In addition, an organisation should be cognisant of any legislative obligations regarding the reporting of cyber security incidents to authorities.

Control: ISM-0123; Revision: 4; Updated: Jun-23; Applicable: NC, OS, P, S, TS; Essential 8: ML2, ML3
Cyber security incidents are reported to the chief information security officer, or one of their delegates, as soon as possible after they occur or are discovered.

Reporting cyber security incidents to ASD

The Australian Signals Directorate (ASD) uses the cyber security incident reports it receives as the basis for assisting organisations. In addition, cyber security incident reports are used to identify trends and maintain an accurate threat environment picture. Finally, ASD utilises this understanding to assist in the development of new and updated cyber security advice, capabilities and techniques to better prevent and respond to evolving cyber threats. Under ASD's limited use obligation, any information voluntarily provided to ASD about cyber security incidents, or potential cyber security incidents, cannot be used for regulatory purposes.

An organisation is recommended to coordinate their reporting of cyber security incidents to ASD. In doing so, the organisation should be cognisant of any legislative obligations regarding the reporting of cyber security incidents to ASD.

The types of cyber security incidents that should be reported to ASD include:

- suspicious privileged user account lockouts
- suspicious remote access authentication events
- service accounts suspiciously communicating with internet-based infrastructure
- compromise of sensitive or classified data
- unauthorised access or attempts to access a system
- emails with suspicious attachments or links
- denial-of-service attacks
- ransomware attacks
- suspected tampering of electronic devices.

Control: ISM-0140; Revision: 8; Updated: Sep-23; Applicable: NC, OS, P, S, TS; Essential 8: ML2, ML3
Cyber security incidents are reported to ASD as soon as possible after they occur or are discovered.

Reporting cyber security incidents to customers and the public

Reporting cyber security incidents to customers and the public in a timely manner after they occur or are discovered is one way that an organisation can demonstrate their commitment to transparency. In addition, an organisation should be cognisant of any legislative obligations regarding the reporting of cyber security incidents to customers and the public.

Control: ISM-1880; Revision: 0; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Cyber security incidents that involve customer data are reported to customers and the public in a timely manner after they occur or are discovered.

Control: ISM-1881; Revision: 0; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Cyber security incidents that do not involve customer data are reported to customers and the public in a timely manner after they occur or are discovered.

Further information

Further information on event logging can be found in the 'Security monitoring' section of the *Guidelines for security assurance*.

Further information on cyber security incident response plans can be found in the 'System-specific cyber security documentation' section of the *Guidelines for cyber security documentation*.

Further information on preparing for and responding to cyber security incidents can be found in ASD's *Cyber security incident response planning: Executive guidance* and *Cyber security incident response planning: Practitioner guidance* publications.

Further information on understanding, identifying and preventing the insider threat can be found in the Attorney-General's Department's *Countering the Insider Threat: A guide for Australian Government* publication.

Further information on understanding, identifying and preventing the insider threat can also be found in the Australian Security Intelligence Organisation's *Countering the insider threat* brochure and *Countering the insider threat: A security manager's guide* publication.

Further information on understanding, identifying and preventing the insider threat can also be found on the United Kingdom's National Protective Security Authority's Insider Risk Guidance website.

Further information on developing, implementing and maintaining an insider threat mitigation program can be found in the United States' Cybersecurity & Infrastructure Security Agency's *Insider Threat Mitigation Guide*.

Further information on developing, implementing and maintaining an insider threat mitigation program can also be found in Carnegie Mellon University's Software Engineering Institute's *Common Sense Guide to Mitigating Insider Threats, Seventh Edition* publication.

Further information on reporting of cyber security incidents by service providers can be found in the 'Managed services and cloud services' section of the *Guidelines for procurement and outsourcing*.

Further information on reporting cybercrime incidents and reporting cyber security incidents, including ASD's limited use obligation, is available from ASD.

Responding to cyber security incidents

Enacting cyber security incident response plans

Following a cyber security incident being identified, an organisation's cyber security incident response plan should be enacted.

Control: ISM-1819; Revision: 2; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: ML2, ML3
Following the identification of a cyber security incident, the cyber security incident response plan is enacted.

Handling and containing data spills

When a data spill occurs, an organisation should inform data owners and restrict access to the data. In doing so, affected systems can be powered off, have their network connectivity removed or have additional access controls applied to the data. However, powering off systems could destroy data that would be useful

for forensic investigations. Furthermore, human users should be made aware of appropriate actions to take in the event of a data spill, such as not deleting, copying, printing or emailing the data.

Control: ISM-0133; Revision: 2; Updated: Jun-21; Applicable: NC, OS, P, S, TS; Essential 8: N/A
When a data spill occurs, data owners are advised and access to the data is restricted.

Handling and containing malicious code infections

Taking immediate remediation steps after the discovery of malicious code can minimise the time and cost spent eradicating and recovering from the infection. As a priority, all infected systems and media should be isolated to prevent the infection from spreading. Once isolated, infected systems and media can be scanned by antivirus applications to potentially remove the infection or recover data. It is important to note though, a complete system restoration from a known good backup or rebuild may be the only reliable way to ensure that malicious code can be truly eradicated.

Control: ISM-0917; Revision: 8; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
When malicious code is detected, the following steps are taken to handle the infection:

- *the infected systems are isolated*
- *all previously connected media used in the period leading up to the infection are scanned for signs of infection and isolated if necessary*
- *antivirus applications are used to remove the infection from infected systems and media*
- *if the infection cannot be reliably removed, systems are restored from a known good backup or rebuilt.*

Control: ISM-1969; Revision: 0; Updated: Dec-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Malicious code, when stored or communicated, is treated beforehand to prevent accidental execution.

Control: ISM-1970; Revision: 1; Updated: Jun-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Malicious code processing for cyber security incident response or research purposes is conducted in a dedicated analysis environment segregated from other systems.

Handling and containing intrusions

When an intrusion is detected on a system, an organisation may, in limited circumstances, choose to allow the intrusion to continue for a short period to better understand the extent of the compromise or to assist with planning intrusion remediation activities. However, an organisation allowing an intrusion to continue in order to collect data or evidence should first establish with their legal advisors whether such activities would breach the *Telecommunications (Interception and Access) Act 1979*.

To increase the likelihood of eradicating malicious actors from a system, an organisation can take preventative measures to ensure malicious actors have limited awareness of planned intrusion remediation activities. Specifically, using trusted systems separate from a compromised system to plan and coordinate intrusion remediation activities prevents alerting malicious actors if they have already compromised communication or collaboration services. In addition, coordinating and sequencing intrusion remediation activities can reduce opportunities for re-compromise of the system while balancing operational risk and business continuity requirements.

Finally, following intrusion remediation activities, an organisation should determine whether malicious actors have been eradicated from the system and have not re-established access. Enhanced monitoring should be conducted until there is sufficient evidence-based confidence that this has been achieved.

In determining whether sufficient evidence-based confidence has been achieved, an organisation should consider the scope and quality of its digital forensic investigations, including whether:

- the initial access vector and full extent of the compromise have been identified
- persistence mechanisms, malicious infrastructure and unauthorised access paths have been identified and remediated
- the affected system has been rebuilt, restored from known-good backups or otherwise verified as trustworthy
- compromised accounts, credentials, certificates, keys and trust relationships have been remediated
- threat hunting has identified no continuing or renewed indicators of malicious activity.

Control: ISM-0137; Revision: 4; Updated: Dec-21; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Legal advice is sought before allowing intrusion activity to continue on a system for the purpose of collecting further data or evidence.

Control: ISM-1609; Revision: 2; Updated: Dec-21; Applicable: NC, OS, P, S, TS; Essential 8: N/A
System owners are consulted before allowing intrusion activity to continue on a system for the purpose of collecting further data or evidence.

Control: ISM-1731; Revision: 1; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Planning and coordination of intrusion remediation activities are conducted using trusted systems separate from a compromised system.

Control: ISM-1732; Revision: 1; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Intrusion remediation activities are coordinated and sequenced to minimise opportunities for re-compromise of a system while balancing operational risk and business continuity requirements.

Control: ISM-1213; Revision: 4; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Following intrusion remediation activities, enhanced monitoring is conducted until there is sufficient evidence-based confidence that malicious actors have been eradicated from a system and have not re-established access.

Maintaining the integrity of evidence

When gathering evidence following a cyber security incident, it is important that it is gathered in an appropriate manner and that its integrity is maintained. In addition, if ASD is requested to assist with investigations, no actions that could affect the integrity of evidence should be carried out before ASD becomes involved.

Control: ISM-0138; Revision: 6; Updated: Jun-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The integrity of evidence gathered during an investigation is maintained by investigators:

- *recording all their actions*
- *maintaining a proper chain of custody*
- *following all instructions provided by relevant law enforcement agencies.*

Further information

Further information on cyber security incident response plans can be found in the 'System-specific cyber security documentation' section of the *Guidelines for cyber security documentation*.

Further information on handling malicious code infections can be found in National Institute of Standards and Technology Special Publication 800-61 Rev. 3, *Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile*.

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

Copyright

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the Department of the Prime Minister and Cabinet website (https://www.pmc.gov.au/resources/commonwealth-coat-arms-information-and-guidelines).

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre