Information security manual

Guidelines for cybersecurity incidents

Last updated: September 2025

Managing cybersecurity incidents

Cybersecurity events

A cybersecurity event is an occurrence of a system, service or network state indicating a possible breach of security policy, failure of safeguards or a previously unknown situation that may be relevant to security.

Cybersecurity incidents

A cybersecurity incident is an unwanted or unexpected cybersecurity event, or a series of such events, that either has compromised business operations or has a significant probability of compromising business operations.

Cyber resilience

Cyber resilience is the ability to adapt to disruptions caused by cybersecurity incidents while maintaining continuous business operations. This includes the ability to detect, manage and recover from cybersecurity incidents.

Detecting cybersecurity incidents

One of the core elements of detecting and investigating cybersecurity incidents is the availability of appropriate data sources, such as event logs. The following event logs can be used by an organisation to assist with detecting and investigating cybersecurity incidents:

- **Artificial intelligence applications:** May assist in identifying anomalous or malicious code or user behaviour indicating an exploitation attempt or successful compromise.
- **Cross Domain Solutions:** May assist in identifying anomalous or malicious network traffic indicating an exploitation attempt or successful compromise.
- **Databases:** May assist in identifying anomalous or malicious code or user behaviour indicating an exploitation attempt or successful compromise.
- **Domain Name System services:** May assist in identifying attempts to resolve malicious domain names or Internet Protocol addresses indicating an exploitation attempt or successful compromise.

- **Email servers:** May assist in identifying users targeted with phishing emails thereby helping to identify the initial vector of a compromise.
- **Gateways:** May assist in identifying anomalous or malicious network traffic indicating an exploitation attempt or successful compromise.
- **Mobile applications:** May assist in identifying anomalous or malicious code or user behaviour indicating an exploitation attempt or successful compromise.
- **Multifunction devices:** May assist in identifying anomalous or malicious user behaviour indicating a cybersecurity incident.
- **Operating systems:** May assist in identifying anomalous or malicious activity indicating an exploitation attempt or successful compromise.
- **Remote access services:** May assist in identifying unusual locations of access or times of access indicating an exploitation attempt or successful compromise.
- **Security products:** May assist in identifying anomalous or malicious code or network traffic indicating an exploitation attempt or successful compromise.
- **Server applications:** May assist in identifying anomalous or malicious code or user behaviour indicating an exploitation attempt or successful compromise.
- **System access:** May assist in identifying anomalous or malicious user behaviour indicating an exploitation attempt or successful compromise.
- **User applications:** May assist in identifying anomalous or malicious code or user behaviour indicating an exploitation attempt or successful compromise.
- **Web applications:** May assist in identifying anomalous or malicious code or user behaviour indicating an exploitation attempt or successful compromise.
- **Web proxies:** May assist in identifying anomalous or malicious network traffic indicating an exploitation attempt or successful compromise.

Cybersecurity incident management policy

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

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

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

Control: ISM-0576; Revision: 11; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
A cybersecurity incident management policy, and associated cybersecurity incident response plan, is developed, implemented and maintained.

Control: ISM-1784; Revision: 2; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The cybersecurity incident management policy, including the associated cybersecurity incident response plan, is exercised at least annually.

Cybersecurity incident register

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

Control: ISM-0125; Revision: 7; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
A cybersecurity incident register is developed, implemented and maintained.

Control: ISM-1803; Revision: 1; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
A cybersecurity incident register contains the following for each cybersecurity incident:

- *the date the cybersecurity incident occurred*
- *the date the cybersecurity incident was discovered*
- *a description of the cybersecurity incident*
- *any actions taken in response to the cybersecurity incident*
- *to whom the cybersecurity 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 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 user 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.

Access to sufficient data sources and tools

Successful detection of cybersecurity incidents requires trained cybersecurity personnel with access to sufficient data sources, such as event logs, that are complemented by tools that support manual and automated analysis. As such, it is important that during system design and development activities, functionality is added to systems to ensure that sufficient data sources can be captured and provided to cybersecurity personnel.

Control: ISM-0120; Revision: 6; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Cybersecurity personnel have access to sufficient data sources and tools to ensure that systems can be monitored for key indicators of compromise.

Reporting cybersecurity incidents

Reporting cybersecurity 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 cybersecurity incident response activities. Note, an organisation should also be cognisant of any legislative obligations regarding the reporting of cybersecurity incidents to authorities.

Control: ISM-0123; Revision: 5; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: ML2, ML3
Cybersecurity 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 cybersecurity incidents to ASD

The Australian Signals Directorate (ASD) uses the cybersecurity incident reports it receives as the basis for providing assistance to organisations. In addition, cybersecurity 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 cybersecurity advice, capabilities, and techniques to better prevent and respond to evolving cyberthreats. Note, under ASD's limited use obligation, information voluntarily provided to ASD about cybersecurity incidents, or potential cybersecurity incidents, cannot be used for regulatory purposes.

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

The types of cybersecurity 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: 9; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: ML2, ML3
Cybersecurity incidents are reported to ASD as soon as possible after they occur or are discovered.

Reporting cybersecurity incidents to customers and the public

Reporting cybersecurity 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. Note, an organisation should also be cognisant of any legislative obligations regarding the reporting of cybersecurity incidents to customers and the public.

Control: ISM-1880; Revision: 1; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Cybersecurity 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: 1; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Cybersecurity 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 event logging and monitoring section of the *Guidelines for system monitoring*.

Further information on cybersecurity incident response plans can be found in the system-specific cybersecurity documentation section of the *Guidelines for cybersecurity documentation*.

Further information on preparing for and responding to cybersecurity incidents can be found in ASD's *Cybersecurity incident response planning: Executive guidance* and *Cybersecurity 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 cybersecurity 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 cybersecurity incidents, including ASD's limited use obligation, is available from ASD.

Responding to cybersecurity incidents

Enacting cybersecurity incident response plans

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

Control: ISM-1819; Revision: 3; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: ML2, ML3
Following the identification of a cybersecurity incident, the cybersecurity 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. It should be noted though that powering off systems could destroy data that would be useful for forensic investigations. Furthermore, 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: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Malicious code processed for cybersecurity incident response or research purposes is done so in a dedicated analysis environment that is segregated from other systems.

Handling and containing intrusions

When an intrusion is detected on a system, an organisation may wish to allow the intrusion to continue for a short period of time in order to fully understand the extent of the compromise and 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 be breaching the *Telecommunications (Interception and Access) Act 1979*.

To increase the likelihood of intrusion remediation activities successfully removing malicious actors from their system, an organisation can take preventative measures to ensure malicious actors have limited forewarning and awareness of planned intrusion remediation activities. Specifically, using an alternative system to plan and coordinate intrusion remediation activities will prevent alerting malicious actors if they have already compromised email, messaging or collaboration services. In addition, conducting intrusion remediation activities in a coordinated manner during the same planned outage will prevent forewarning malicious actors, thereby depriving them of sufficient time to establish alternative access points or persistence methods on the system.

Following intrusion remediation activities, an organisation should determine whether malicious actors have been successfully removed from the system, including whether or not they have since reacquired access. This can be achieved, in part, by capturing and analysing network traffic for at least seven days following remediation activities.

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: 0; Updated: Dec-21; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Planning and coordination of intrusion remediation activities are conducted on a separate system to that which has been compromised.

Control: ISM-1732; Revision: 0; Updated: Dec-21; Applicable: NC, OS, P, S, TS; Essential 8: N/A
To the extent possible, all intrusion remediation activities are conducted in a coordinated manner during the same planned outage.

Control: ISM-1213; Revision: 3; Updated: Sep-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Following intrusion remediation activities, full network traffic is captured for at least seven days and analysed to determine whether malicious actors have been successfully removed from the system.

Maintaining the integrity of evidence

When gathering evidence following a cybersecurity 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 which could affect the integrity of evidence should be carried out before ASD becomes involved.

Control: ISM-0138; Revision: 5; Updated: Mar-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The integrity of evidence gathered during an investigation is maintained by investigators:

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

Further information

Further information on cybersecurity incident response plans can be found in the system-specific cybersecurity documentation section of the *Guidelines for cybersecurity 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