Australian Government
Australian Signals Directorate

Information security manual

Guidelines for system monitoring

Last updated: September 2025

Event logging and monitoring

Event logging and monitoring activities

These guidelines are intended for security-relevant event logs. They are not intended for non-security-relevant event logs, such as operating system and application performance-related event logs.

Event logging policy

By developing an event logging policy, taking into consideration any shared responsibilities between service providers and their customers, an organisation can improve their chances of detecting malicious behaviour on their systems. In doing so, an event logging policy should cover details of events to be logged, event logging facilities to be used, how event logs will be monitored and how long to retain event logs.

Control: ISM-0580; Revision: 7; Updated: Dec-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
An event logging policy is developed, implemented and maintained.

Centralised event logging facility

A centralised event logging facility can be used to capture, protect and manage event logs from multiple sources in a coordinated manner. This may be achieved by using a Security Information and Event Management (SIEM) platform, a Security Orchestration, Automation and Response (SOAR) platform, or both. Furthermore, in support of a centralised event logging facility, it is important that an accurate and consistent time source is used to assist with identifying connections between events.

Control: ISM-1405; Revision: 4; Updated: Dec-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
A centralised event logging facility is implemented.

Control: ISM-1983; Revision: 0; Updated: Dec-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Event logs sent to a centralised event logging facility are done so as soon as possible after they occur.

Control: ISM-1984; Revision: 0; Updated: Dec-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Event logs sent to a centralised event logging facility are encrypted in transit.

Control: ISM-1985; Revision: 0; Updated: Dec-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Event logs are protected from unauthorised access.

Control: ISM-1815; Revision: 1; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: ML2, ML3
Event logs are protected from unauthorised modification and deletion.

Control: ISM-0988; Revision: 7; Updated: Sep-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
An accurate and consistent time source is used for event logging.

Event log details

For each event logged, sufficient detail needs to be recorded in order for event logs to be useful. In doing so, event logs should be captured and stored in a consistent and structured format.

Control: ISM-0585; Revision: 6; Updated: Jun-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
For each event logged, the date and time of the event, the relevant user or process, the relevant filename, the event description, and the information technology equipment involved are recorded.

Control: ISM-1959; Revision: 0; Updated: Sep-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
To the extent possible, event logs are captured and stored in a consistent and structured format.

Event log monitoring

Event log monitoring is critical to maintaining the security posture of systems. Notably, such activities involve analysing event logs in a timely manner to detect cybersecurity events, thereby, leading to the identification of cybersecurity incidents.

Control: ISM-1986; Revision: 1; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Event logs from critical servers are analysed in a timely manner to detect cybersecurity events.

Control: ISM-1906; Revision: 1; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: ML2, ML3
Event logs from internet-facing servers are analysed in a timely manner to detect cybersecurity events.

Control: ISM-1907; Revision: 1; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: ML3
Event logs from non-internet-facing servers are analysed in a timely manner to detect cybersecurity events.

Control: ISM-0109; Revision: 10; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: ML3
Event logs from workstations are analysed in a timely manner to detect cybersecurity events.

Control: ISM-1987; Revision: 1; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Event logs from security products are analysed in a timely manner to detect cybersecurity events.

Control: ISM-1960; Revision: 1; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Event logs from internet-facing network devices are analysed in a timely manner to detect cybersecurity events.

Control: ISM-1961; Revision: 1; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Event logs from non-internet-facing network devices are analysed in a timely manner to detect cybersecurity events.

Control: ISM-1228; Revision: 4; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: ML2, ML3
Cybersecurity events are analysed in a timely manner to identify cybersecurity incidents.

Event log retention

The retention of event logs is integral to system monitoring, hunt and cybersecurity incident response activities. As such, event logs should be retained for a suitable period of time to facilitate these activities.

Control: ISM-1988; Revision: 0; Updated: Dec-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Event logs are retained in a searchable manner for at least 12 months.

Control: ISM-1989; Revision: 0; Updated: Dec-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Event logs are retained as per minimum retention requirements for various classes of records as set out by the National Archives of Australia's Administrative Functions Disposal Authority Express (AFDA Express) Version 2 publication.

Further information

Further information on logging intrusion activity can be found in the managing cybersecurity incidents section of the *Guidelines for cybersecurity incidents*.

Further information on event logging for application-based security products can be found in the operating system hardening section of the *Guidelines for system hardening*.

Further information on event logging for artificial intelligence applications can be found in the software development fundamentals section of the *Guidelines for software development*.

Further information on event logging for Cross Domain Solutions can be found in the Cross Domain Solutions section of the *Guidelines for gateways*.

Further information on event logging for databases can be found in the databases section of the *Guidelines for database systems*.

Further information on event logging for gateways can be found in the gateways section of the *Guidelines for gateways*.

Further information on event logging for mobile applications can be found in the software development fundamentals section of the *Guidelines for software development*.

Further information on event logging for multifunction devices can be found in the fax machines and multifunction devices section of the *Guidelines for communications systems*.

Further information on event logging for network-based security products can be found in the network design and configuration section of the *Guidelines for networking*.

Further information on event logging for operating systems can be found in the operating system hardening and authentication hardening sections of the *Guidelines for system hardening*.

Further information on event logging for server applications can be found in the server application hardening section of the *Guidelines for system hardening*.

Further information on event logging for system access can be found in the access to systems and their resources section of the *Guidelines for personnel security*.

Further information on event logging for user applications can be found in the user application hardening section of the *Guidelines for system hardening*.

Further information on event logging for web applications can be found in the software development section of the *Guidelines for software development*.

Further information on event logging for web proxies can be found in the web proxies section of the *Guidelines for gateways*.

Further information on event logging can be found in the following Australian Signals Directorate publications:

- *Best practices for event logging and threat detection*
- *Detecting and mitigating Active Directory compromises*
- *Hardening Microsoft Windows 10 workstations*
- *Hardening Microsoft Windows 11 workstations*
- *Priority logs for SIEM ingestion: Practitioner guidance*
- *Windows event logging and forwarding*.

Further information on SIEM and SOAR platforms can be found in the Australian Signals Directorate's *Implementing SIEM and SOAR platforms: Executive guidance* and *Implementing SIEM and SOAR platforms: Practitioner guidance* publications.

Further information on prioritising the collection and storage of event logs can be found in the United States' Cybersecurity & Infrastructure Security Agency's *Guidance for Implementing M-21-31: Improving the Federal Government's Investigative and Remediation Capabilities* publication.

Further information on the National Archives of Australia's requirements for event log retention can be found in their *AFDA Express Version 2 – Technology & Information Management* publication.

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

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre