



Information Security Manual

Published: 22 June 2023

Guidelines for System Monitoring

Event logging and monitoring

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; **Applicability:** All; **Essential Eight:** N/A

An event logging policy is developed, implemented and maintained.

Event log details

For each event logged, sufficient detail needs to be recorded in order for the event log to be useful.

Control: ISM-0585; **Revision:** 5; **Updated:** Mar-22; **Applicability:** All; **Essential Eight:** 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 ICT equipment involved are recorded.

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 solution. Furthermore, in support of a centralised event logging facility, it is important that an accurate time source is established and used consistently across systems to assist with identifying connections between events.

Control: ISM-1405; **Revision:** 3; **Updated:** Dec-22; **Applicability:** All; **Essential Eight:** ML3

A centralised event logging facility is implemented and event logs are sent to the facility as soon as possible after they occur.

Control: ISM-1815; **Revision:** 0; **Updated:** Dec-22; **Applicability:** All; **Essential Eight:** ML3

Event logs stored within a centralised event logging facility are protected from unauthorised modification and deletion.

Control: ISM-0988; **Revision:** 6; **Updated:** Mar-22; **Applicability:** All; **Essential Eight:** N/A

An accurate time source is established and used consistently across systems to assist with identifying connections between events.

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 cyber security events, thereby, leading to the identification of cyber security incidents.

Control: ISM-0109; Revision: 8; Updated: Mar-22; Applicability: All; Essential Eight: ML3

Event logs are analysed in a timely manner to detect cyber security events.

Control: ISM-1228; Revision: 3; Updated: Mar-22; Applicability: All; Essential Eight: ML3

Cyber security events are analysed in a timely manner to identify cyber security incidents.

Event log retention

The retention of event logs is integral to system monitoring, hunt and incident response activities. As such, event logs for Cross Domain Solutions, databases, Domain Name System services, email servers, gateways, multifunction devices, operating systems, remote access services, security services, server applications, system access, user applications, web applications and web proxies should be retained for a suitable period of time to facilitate these activities.

Control: ISM-0859; Revision: 4; Updated: Mar-23; Applicability: All; Essential Eight: N/A

Event logs, excluding those for Domain Name System services and web proxies, are retained for at least seven years.

Control: ISM-0991; Revision: 6; Updated: Mar-23; Applicability: All; Essential Eight: N/A

Event logs for Domain Name System services and web proxies are retained for at least 18 months.

Further information

Further information on logging intrusion activity can be found in the managing cyber security incidents section of the [Guidelines for Cyber Security Incidents](#).

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 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 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 application-based security services can be found in the operating system hardening section of the [Guidelines for System Hardening](#).

Further information on event logging for network-based security services can be found in the network design and configuration section of the [Guidelines for Networking](#).

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 web application 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 and forwarding can be found in the Australian Cyber Security Centre's [Windows Event Logging and Forwarding](#) publication.