



Information Security Manual

Published: 10 March 2022

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.

Security Control: ISM-0580; Revision: 6; Updated: Aug-19; Applicability: All; Essential Eight: N/A

An event logging policy is developed and implemented.

Event log details

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

Security 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.

Event logging facility

A centralised event logging facility can be used to 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.

Security Control: ISM-1405; Revision: 2; Updated: Mar-22; Applicability: All; Essential Eight: N/A

A centralised event logging facility is implemented and systems are configured to save event logs to the facility as soon as possible after each event occurs.

Security 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.

Security Control: ISM-0109; Revision: 8; Updated: Mar-22; Applicability: All; Essential Eight: N/A

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

Security Control: ISM-1228; Revision: 3; Updated: Mar-22; Applicability: All; Essential Eight: N/A

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

Event log retention

As event logs are integral to event log monitoring activities, they should be retained for the life of systems, potentially longer. However, the minimum retention period required under the National Archives of Australia's [Administrative Functions Disposal Authority Express Version 2](#) publication is seven years.

Security Control: ISM-0859; Revision: 3; Updated: Jan-20; Applicability: All; Essential Eight: N/A

Event logs are retained for a minimum of 7 years in accordance with the National Archives of Australia's Administrative Functions Disposal Authority Express Version 2 publication.

Security Control: ISM-0991; Revision: 5; Updated: Mar-22; Applicability: All; Essential Eight: N/A

Domain Name System and web proxy event logs are retained for at least 18 months.

Further information

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

Further information on event logging for user activity on systems can be found in the access to systems and their resources section of the [Guidelines for Personnel Security](#).

Further information on event logging for operating systems can be found in the operating system hardening section of the [Guidelines for System Hardening](#).

Further information on event logging for applications can be found in the 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 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 and forwarding can be found in the Australian Cyber Security Centre's [Windows Event Logging and Forwarding](#) publication.