Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Australian Government Information Security Manual

JUNE 2021

Guidelines for System Monitoring

Event logging and auditing

Event logging policy

By developing an event logging policy, taking into consideration any shared responsibilities between organisations and their service providers, an organisation can improve their chances of detecting malicious behaviour on systems and networks. Such an event logging policy would cover events to be logged, logging facilities to be used, event log retention periods and how event logs will be protected.

Security Control: 0580; Revision: 6; Updated: Aug-19; Applicability: O, P, S, TS
An event logging policy is developed and implemented.

Centralised logging facility

A centralised logging facility can be used to correlate event logs from multiple sources. This functionality may be provided by a Security Information and Event Management solution.

Security Control: 1405; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
A centralised logging facility is implemented and systems are configured to save event logs to the centralised logging facility as soon as possible after each event occurs.

Security Control: 0988; Revision: 5; Updated: Sep-18; Applicability: O, P, S, TS
An accurate time source is established and used consistently across systems and network devices to assist with the correlation of events.

Events to be logged

The following list of events can assist in monitoring the security posture of systems, detecting malicious behaviour and contributing to investigations following cyber security incidents.

Security Control: 0584; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
For any system requiring authentication, logon, failed logon and logoff events are logged.

Security Control: 0582; Revision: 6; Updated: Aug-20; Applicability: O, P, S, TS
The following events are logged for operating systems:

- *access to important data and processes*
- *application crashes and any error messages*

- *attempts to use special privileges*
- *changes to accounts*
- *changes to security policy*
- *changes to system configurations*
- *Domain Name System (DNS) and Hypertext Transfer Protocol requests*
- *failed attempts to access data and system resources*
- *service failures and restarts*
- *system startup and shutdown*
- *transfer of data to and from external media*
- *user or group management*
- *use of special privileges.*

Security Control: 1536; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS
The following events are logged for web applications:

- *attempted access that is denied*
- *crashes and any error messages*
- *search queries initiated by users.*

Security Control: 1537; Revision: 1; Updated: Jun-21; Applicability: O, P, S, TS
The following events are logged for databases:

- *access to particularly important data*
- *addition of new users, especially privileged users*
- *any query containing comments*
- *any query containing multiple embedded queries*
- *any query or database alerts or failures*
- *attempts to elevate privileges*
- *attempted access that is successful or unsuccessful*
- *changes to the database structure*
- *changes to user roles or database permissions*
- *database administrator actions*
- *database logons and logoffs*
- *modifications to data*
- *use of executable commands.*

Event log details

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

Security Control: 0585; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS

For each event logged, the date and time of the event, the relevant user or process, the event description, and the ICT equipment involved are recorded.

Event log protection

Effective event log protection and storage, from the time they are created to the time they are destroyed, ensures the integrity, availability and non-repudiation of captured event logs.

Security Control: 0586; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS
Event logs are protected from unauthorised access, modification and deletion.

Event log retention

Since event logs can contribute to investigations following cyber security incidents, they should ideally be retained for the life of a system, and potentially longer. However, the minimum retention requirement for these records under the National Archives of Australia's ***Administrative Functions Disposal Authority Express Version 2*** publication is seven years.

Security Control: 0859; Revision: 3; Updated: Jan-20; Applicability: O, P, S, TS
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: 0991; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS
DNS and proxy logs are retained for at least 18 months.

Event log auditing process and procedures

Auditing of event logs is an integral part of maintaining the security posture of systems. Such activities can help detect and attribute any violations of security policy, including cyber security incidents.

Security Control: 0109; Revision: 6; Updated: Aug-19; Applicability: O, P, S, TS
An event log auditing process, and supporting event log auditing procedures, is developed and implemented covering the scope and schedule of audits, what constitutes a violation of security policy, and actions to be taken when violations are detected, including reporting requirements.

Security Control: 1228; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
Events are correlated across event logs to prioritise audits and focus investigations.

Further information

Further information on event logging associated with a cyber security incident can be found in the ***Guidelines for Cyber Security Incidents***.

Further information on event logging and forwarding can be found in the Australian Cyber Security Centre's ***Windows Event Logging and Forwarding*** publication at https://www.cyber.gov.au/acsc/view-all-content/publications/windows-event-logging-and-forwarding.

Further information on retaining event logs can be found in the National Archives of Australia's ***Administrative Functions Disposal Authority Express Version 2*** publication at https://www.naa.gov.au/information-management/records-authorities/types-records-authorities/afda-express-version-2-functions.