Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Australian Government Information Security Manual

SEPTEMBER 2019

Guidelines for Security Documentation

Development and maintenance of security documentation

Security documentation

Security documentation supports the accurate and consistent application of policies, processes and procedures. It is important that security documentation is developed by personnel with a good understanding of security matters, the technologies being used and the business requirements of the organisation and system owners.

The System Security Plan (SSP) and Incident Response Plan (IRP) form a documentation suite for a system, it is essential that they are logically connected and consistent. Furthermore, it is important that security documentation for systems are logically connected to organisational-level security documentation such as a cyber security strategy.

Security documentation may be presented in a number of formats including dynamic content such as wikis, intranets or other forms of document repositories.

Security Control: 0039; Revision: 4; Updated: May-19; Applicability: O, P, S, TS; Priority: Must
A cyber security strategy is developed and implemented for the organisation.

Approval of security documentation

If security documentation is not approved, personnel will have difficulty ensuring appropriate policies, processes and procedures are in place. Having approval not only assists in the implementation of policies, processes and procedures, it also ensures personnel are aware of cyber security issues and security risks. As such, it is important that once security documentation has been approved it is published and communicated to all personnel.

Security Control: 0047; Revision: 4; Updated: May-19; Applicability: O, P, S, TS; Priority: Should
Organisational-level security documentation is approved by the Chief Information Security Officer while system-specific security documentation is approved by the system's authorising officer.

Maintenance of security documentation

Threat environments are dynamic. If security documentation is not kept up-to-date to reflect the current threat environment, security controls and processes may cease to be effective. In such a situation, resources could be devoted to areas that have reduced effectiveness or are no longer relevant.

Security Control: 0888; Revision: 5; Updated: May-19; Applicability: O, P, S, TS; Priority: Should
Security documentation is reviewed at least annually and includes a 'current as at [date]' or equivalent statement.

Further information

Further information on intrusion detection and prevent policy can be found in the ***Guidelines for Cyber Security Incidents***.

Further information on cyber security incident registers can be found in the ***Guidelines for Cyber Security Incidents***.

Further information on ICT equipment and media registers can be found in the ***Guidelines for Physical Security***.

Further information on authorised Radio Frequency devices for SECRET and TOP SECRET area registers can be found in the ***Guidelines for Physical Security***.

Further information on cable registers can be found in the ***Guidelines for Communications Infrastructure***.

Further information on cable labelling process and procedures can be found in the ***Guidelines for Communications Infrastructure***.

Further information on telephone systems usage policy can be found in the ***Guidelines for Communications Systems***.

Further information on fax machine and multifunction device usage policy can be found in the ***Guidelines for Communications Systems***.

Further information on mobile device management policy and mobile device usage policy, as well as mobile device emergency sanitisation process and procedures, can be found in the ***Guidelines for Enterprise Mobility***.

Further information on ICT equipment management policy, as well as ICT equipment sanitisation and disposal processes and procedures, can be found in the ***Guidelines for ICT Equipment Management***.

Further information on media management policy and removable media usage policy, as well as media sanitisation, destruction and disposal processes and procedures, can be found in the ***Guidelines for Media Management***.

Further information on system administration process and procedures can be found in the ***Guidelines for System Management***.

Further information on patch management process and procedures can be found in the ***Guidelines for System Management***.

Further information on software registers can be found in the ***Guidelines for System Management***.

Further information on change management process and procedures can be found in the ***Guidelines for System Management***.

Further information on digital preservation policy, as well as data backup and restoration processes and procedures, can be found in the ***Guidelines for System Management***.

Further information on event logging policy, as well as event log auditing process and procedures, can be found in the ***Guidelines for System Monitoring***.

Further information vulnerability management policy can be found in the ***Guidelines for System Monitoring***.

Further information on database registers can be found in the ***Guidelines for Database Systems Management***.

Further information on email usage policy can be found in the ***Guidelines for Email Management***.

Further information on network device registers can be found in the ***Guidelines for Network Management***.

Further information on web usage policy can be found in the ***Guidelines for Gateway Management***.

Further information on data transfer process and procedures can be found in the ***Guidelines for Data Transfers and Content Filtering***.

System-specific security documentation

System Security Plan

The SSP provides a description of a system and includes an annex that describes the security controls that have been identified and implemented for the system.

There can be many stakeholders involved in defining a SSP. This can include representatives from:

- cyber security teams within the organisation
- project teams who deliver the capability (including contractors)
- support teams who operate and support the capability
- owners of information to be processed, stored or communicated by the system
- users for whom the capability is being developed.

Depending on the documentation framework used, some details common to multiple systems could be consolidated in a higher-level SSP.

Security Control: 0041; Revision: 3; Updated: Aug-19; Applicability: O, P, S, TS; Priority: Must
Systems have a SSP that includes a description of the system and an annex that covers both security controls from this document (based on the system's classification, functionality and technologies) and any additional security controls that have been identified for the system.

Incident Response Plan

Having an IRP ensures that when a cyber security incident occurs, a plan is in place to respond appropriately to the situation. In most situations, the aim of the response will be to prevent the cyber security incident from escalating, restore any impacted system or information, and preserve any evidence.

Depending on the documentation framework used, some details common to multiple systems could be consolidated into a higher-level IRP.

Security Control: 0043; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
Systems have an IRP that covers the following:

- *guidelines on what constitutes a cyber security incident*
- *the types of incidents likely to be encountered and the expected response to each type*
- *how to report cyber security incidents, internally to the organisation and externally to the Australian Cyber Security Centre (ACSC)*
- *other parties which need to be informed in the event of a cyber security incident*
- *the authority, or authorities, responsible for investigating and responding to cyber security incidents*
- *the criteria by which an investigation of a cyber security incident would be requested from a law enforcement agency, the ACSC or other relevant authority*
- *the steps necessary to ensure the integrity of evidence relating to a cyber security incident*
- *system contingency measures or a reference to such details if they are located in a separate document.*