Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Australian Government Information Security Manual

MAY 2019

Guidelines for security documentation

Development and maintenance of security documentation

Security documentation

Security documentation supports the accurate and consistent application of security policies 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), Standard Operating Procedures (SOPs) 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 security policies and procedures are in place. Having approval not only assists in the implementation of security policies 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: 3; Updated: Sep-18; 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.

System-specific security documentation

System Security Plan

An SSP describes the system, its system boundary and the security controls that have been implemented. It is developed by selecting relevant security controls from this document based on its classification, functionality and the technologies it is implementing with additional security controls included based on security risks identified during a security risk assessment.

There can be many stakeholders involved in defining a system's 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: 2; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
Systems have a SSP that includes security controls from this document based on its classification, functionality and the technologies it is implementing with additional security controls included based on security risks identified during a security risk assessment.

Standard Operating Procedures

SOPs provide a step-by-step guide to undertaking security related tasks. They provide assurance that tasks can be undertaken in a repeatable manner, even by users without detailed knowledge of a system.

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

Security Control: 0042; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
Systems have SOPs that cover the following:

- *system administration and maintenance activities, such as managing backups and user accounts*
- *software and hardware configuration changes, such as patches, updates and upgrades*
- *the acquisition, support and disposal of assets*
- *the labelling, registering and mustering of assets.*

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 information or services, 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.*

Further information

Further information on detecting, managing and reporting cyber security incidents can be found in the ***Guidelines for cyber security incidents***.