5.5. Standard Operating Procedures

Objective

5.5.1. Standard Operating Procedures (SOPs) ensure security procedures are followed in an appropriate and repeatable manner.

Context

Scope

5.5.2. This section relates to the development of security related SOPs. Information relating to other mandatory documentation can be found in Section 5.1 - Documentation Fundamentals.

Rationale & Controls

Development of SOPs

5.5.3.R.01. **Rationale**

In order to ensure that personnel undertake their duties in an appropriate manner, with a minimum of confusion, it is important that the roles of ITSMs, system administrators and system users are covered by SOPs. Furthermore, taking steps to ensure that SOPs are consistent with SSPs will reduce the potential for confusion resulting from conflicts in policy and procedures.

5.5.3.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:844]

Agencies SHOULD develop SOPs for each of the following roles:

- ITSM;
- system administrator; and
- system user.

ITSM SOPs

5.5.4.R.01. **Rationale**

The ITSM SOPs are intended to cover the management and leadership of information security functions within the agency.

5.5.4.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:849]

The following procedures SHOULD be documented in the ITSMs SOPs.

Topic	Procedures to be included
Access control	Authorising access rights to applications and data.
Asset Musters	Labelling, registering and mustering assets, including media.
Audit logs	Reviewing system audit trails and manual logs, particularly for privileged users.
Configuration control	Approving and releasing changes to the system software or configurations.
Information security incidents	Detecting, reporting and managing potential information security incidents.
	Establishing the cause of any information security incident, whether accidental or deliberate.
	Actions to be taken to recover and minimise the exposure from an information security incident.
	Additional actions to prevent reoccurrence.
Data transfers	Managing the review of media containing classified information that is to be transferred off-site.
	Managing the review of incoming media for malware or unapproved software.
IT equipment	Managing the disposal & destruction of unserviceable IT equipment and media.
System Patching	Advising and recommending system patches, updates and version changes based on security notices and related advisories.
System integrity audit	Reviewing system user accounts, system parameters and access controls to ensure that the system is secure.
	Checking the integrity of system software.
	Testing access controls.
System maintenance	Managing the ongoing security and functionality of system software, including: maintaining awareness of current software vulnerabilities, testing and applying software patches/updates/signatures, and applying appropriate hardening techniques.
User account management	Authorising new system users.

System Administrator SOPs

5.5.5.R.01. **Rationale**

The system administrator SOPs focus on the administrative activities related to system operations.

5.5.5.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:865]

The following procedures SHOULD be documented in the system administrator's SOPs.

Topic	Procedures to be included
Access control	Implementing access rights to applications and data.
Configuration control	Implementing changes to the system software or configurations.
System backup and recovery	Backing up data, including audit logs.
	Securing backup tapes.
	Recovering from system failures.
User account management	Adding and removing system users.
	Setting system user privileges.
	Cleaning up directories and files when a system user departs or changes roles.
Incident response	Detecting, reporting and managing potential information security incidents.
	Establishing the cause of any information security incident, whether accidental or deliberate.
	Actions to be taken to recover and minimise the exposure from information security incident.
	Additional actions to prevent reoccurrence.

System User SOPs

5.5.6.R.01. **Rationale**

The system user SOPs focus on day to day activities that system users need to be made aware of, and comply with, when using systems.

5.5.6.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:884]

The following procedures SHOULD be documented in the system user's SOPs.

Topic	Procedures to be included
Acceptable Use	Acceptable uses of the system(s).
End of day	How to secure systems at the end of the day.
Information security incidents	What to do in the case of a suspected or actual information security incident.
Media control	Procedures for handling and using media.
Passwords	Choosing and protecting passwords.
Temporary absence	How to secure systems when temporarily absent.

Agreement to abide by SOPs

5.5.7.R.01. **Rationale**

When SOPs are produced the intended audience should be made aware of their existence and acknowledge that they have read, understood and agree to abide by their contents.

5.5.7.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:889]

ITSMs, system administrators and system users SHOULD sign a statement that they have read and agree to abide by their respective SOPs.