5.2. Information Security Policies

Objective

5.2.1. Information security policies (SecPol) set the strategic direction for information security.

Context

Scope

5.2.2. This section relates to the development of Information Security Policies and any supporting plans. Information relating to other mandatory documentation can be found in Section 5.1 - Documentation Fundamentals.

Rationale & Controls

The Information Security Policy (SecPol)

5.2.3.R.01. **Rationale**

To provide consistency in approach and documentation, agencies should consider the following when developing their SecPol:

- policy objectives;
- how the policy objectives will be achieved;
- the guidelines and legal framework under which the policy will operate;
- stakeholders;
- education and training;
- what resourcing will be available to support the implementation of the policy;
- what performance measures will be established to ensure that the policy is being implemented effectively; and
- a review cycle.

5.2.3.R.02. **Rationale**

In developing the contents of the SecPol, agencies may also consult any agency-specific directives that are applicable to information security within their agency.

5.2.3.R.03. **Rationale**

Agencies should also avoid outlining controls for systems within their SecPol. The controls for a system will be determined by this manual and based on the scope of the system, along with any additional controls as determined by the SRMP, and documented within the SSP.

5.2.3.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:780]

The Information Security Policy (SecPol) SHOULD document the information security guidelines, standards and responsibilities of an agency.

5.2.3.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:781]

The Information Security Policy (SecPol) SHOULD include topics such as:

- accreditation processes;
- personnel responsibilities;
- configuration control;
- access control;
- networking and connections with other systems;
- physical security and media control;
- emergency procedures and information security incident management;
- vulnerability disclosure;
- change management; and
- information security awareness and training.