5.6. Incident Response Plans

Objective

5.6.1. Incident Response Plans (IRP) outline actions to take in response to an information security incident.

Context

Scope

5.6.2. This section relates to the development of IRPs to address information security, and not physical incidents within agencies. Information relating to other mandatory documentation can be found in Section 5.1 - Documentation Fundamentals.

Rationale & Controls

Contents of IRPs

5.6.3.R.01. **Rationale**

The guidance provided on the content of IRPs will ensure that agencies have a baseline to develop an IRP with sufficient flexibility, scope and level of detail to address the majority of information security incidents that could arise.

5.6.3.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:902]

Agencies MUST include, as a minimum, the following content within their IRP:

- broad guidelines on what constitutes an information security incident;
- the minimum level of information security incident response and investigation training for system users and system administrators;
- the authority responsible for initiating investigations of an information security incident;
- the steps necessary to ensure the integrity of evidence supporting an information security incident;
- the steps necessary to ensure that critical systems remain operational;
- when and how to formally report information security incidents; and
- national policy requirements for incident reporting (see Chapter 7 – Information Security Incidents).

5.6.3.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:904]

Agencies SHOULD include the following content within their IRP:

- clear definitions of the types of information security incidents that are likely to be encountered;
- the expected response to each information security incident type;
- the authority within the agency that is responsible for responding to information security incidents;
- the criteria by which the responsible authority would initiate or request formal, police investigations of an information security incident;
- which other agencies or authorities need to be informed in the event of an investigation being undertaken; and
- the details of the system contingency measures or a reference to these details if they are located in a separate document.