9.1. Information Security Awareness and Training

Objective

9.1.1. A security culture is fostered through induction training and ongoing security education tailored to roles, responsibilities, changing threat environment and sensitivity of information, systems and operations.

Context

Scope

9.1.2. This section covers information relating specifically to information security awareness and training.

PSR references

9.1.3. Relevant PSR requirements can be found at:

Reference	Source
PSR Mandatory Requirements	Home | Protective Security Requirements Security governance (GOV) | Protective Security Requirements Information security (INFOSEC) | Protective Security Requirements Personnel security (PERSEC) | Protective Security Requirements

Rationale & Controls

Information security awareness and training responsibility

9.1.4.R.01. **Rationale**

Agency management is responsible for ensuring that an appropriate information security awareness and a training program is provided for all personnel. Without management support, security personnel might not have sufficient resources to facilitate awareness and training for other personnel.

9.1.4.R.02. **Rationale**

Awareness and knowledge degrades over time without ongoing refresher training and updates. Providing ongoing information security awareness and training will assist in keeping personnel aware of issues and their responsibilities.

9.1.4.R.03. **Rationale**

Methods that can be used to continually promote awareness include logon banners, system access forms and departmental bulletins and memoranda.

9.1.4.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:1449]

Agency management MUST ensure that all personnel who have access to a system have sufficient training and ongoing information security awareness.

Information security awareness and training

9.1.5.R.01. **Rationale**

Information security awareness and training programs are designed to help system users:

- become familiar with their roles and responsibilities;
- understand any legislative or regulatory mandates and requirements;
- understand any national or agency policy mandates and requirements;
- understand and support security requirements;
- assist in maintaining security; and

- learn how to fulfil their security responsibilities.

9.1.5.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:1452]

Agencies MUST provide ongoing information security awareness and a training programme for personnel on topics such as responsibilities, legislation and regulation, consequences of non-compliance with information security policies and procedures, and potential security risks and counter-measures.

9.1.5.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:1453]

Agencies MUST provide information security awareness training as part of their employee induction programmes.

Degree and content of information security awareness and training

9.1.6.R.01. **Rationale**

The detail, content and coverage of information security awareness and training will depend on the objectives of the organisation. Personnel with responsibilities beyond that of a general user should have tailored training to meet their needs.

9.1.6.R.02. **Rationale**

As part of the guidance provided to system users, there should be sufficient emphasis placed on the activities that are NOT allowed on systems. The minimum list of content will also ensure that personnel are sufficiently exposed to issues that could cause an information security incident through lack of awareness or through lack of knowledge.

9.1.6.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1457]

Agencies SHOULD align the detail, content and coverage of information security awareness and training programmes to system user responsibilities.

9.1.6.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1458]

Agencies SHOULD ensure that information security awareness and training includes information on:

- the purpose of the training or awareness program;
- any legislative or regulatory mandates and requirements;
- any national or agency policy mandates and requirements;
- agency security appointments and contacts;
- the legitimate use of system accounts, software and classified information;
- the security of accounts, including shared passwords;
- authorisation requirements for applications, databases and data;
- the security risks associated with non-agency systems, particularly the Internet;
- reporting any suspected compromises or anomalies;
- reporting requirements for information security incidents, suspected compromises or anomalies;
- classifying, marking, controlling, storing and sanitising media;
- protecting workstations from unauthorised access;
- informing the support section when access to a system is no longer needed;
- observing rules and regulations governing the secure operation and authorised use of systems; and
- supporting documentation such as SOPs and user guides.

9.1.6.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1459]

Agencies SHOULD ensure that information security awareness and training includes advice to system users not to attempt to:

- tamper with the system;
- bypass, strain or test information security mechanisms;
- introduce or use unauthorised IT equipment or software on a system;
- replace items such as keyboards, pointing devices and other peripherals with personal equipment;
- assume the roles and privileges of others;
- attempt to gain access to classified information for which they have no authorisation; or
- relocate equipment without proper authorisation.

System familiarisation training

9.1.7.R.01. **Rationale**

A TOP SECRET system needs increased awareness by personnel. Ensuring familiarisation with information security policies and procedures, the secure operation of the system and basic information security training, will provide them with specific knowledge relating to these types of systems.

9.1.7.C.01. **Control System Classifications(s): Top Secret; Compliance: Must** [CID:1462]

Agencies MUST provide all system users with familiarisation training on the information security policies and procedures and the secure operation

of the system before being granted unsupervised access to the system.

Disclosure of information while on courses

9.1.8.R.01. **Rationale**

Government personnel attending courses with non-government personnel may not be aware of the consequences of disclosing information relating to the security of their agency's systems. Raising awareness of such consequences in personnel will assist in preventing disclosures that could lead to a targeted attack being launched against an agency's systems.

9.1.8.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1465]

Agencies SHOULD advise personnel attending courses along with non-government personnel not to disclose any details that could be used to compromise agency security.