3.5. System Users

Objective

3.5.1. System users comply with information security policies and procedures within their agency.

Context

Scope

3.5.2. This section covers the role that system users undertake with respect to information security.

Types of system users

3.5.3. This section covers responsibilities for all system users i.e. users with general access (general users), and users with privileged access (privileged users).

Rationale & Controls

Responsibilities of system users

3.5.4.R.01. **Rationale**

If agencies fail to develop and maintain a security culture where system users are complying with relevant security policies and procedures for the systems they are using, there is an increased security risk of a system user unwittingly assisting with an attack against a system.

3.5.4.R.02. **Rationale**

Security policies, procedures and mechanisms aim to cover all situations that may arise within an agency. However there may be legitimate reasons for a system user to bypass security policies, procedures or mechanisms. If this is the case, the system user MUST seek formal authorisations from the CISO or the ITSM (if this authority has been specifically delegated to the ITSM) before any actions are undertaken.

3.5.4.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:466]

All system users MUST comply with the relevant security policies and procedures for the systems they use.

3.5.4.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:467]

All system users MUST:

- protect account authenticators at the same classification of the system it secures;
- not share authenticators for accounts without approval;
- be responsible for all actions under their accounts; and
- use their access to only perform authorised tasks and functions.

3.5.4.C.03. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:468]

System users that need to bypass security policies, procedures or mechanisms for any reason MUST seek formal authorisation from the CISO or the ITSM if this authority has been specifically delegated to the ITSM.