16.2. System Access

Objective

16.2.1. Access to information on systems is controlled in accordance with agency policy and the NZISM.

Context

Scope

16.2.2. This section covers information on accessing systems for all system users.

16.2.3. Additional information on privileged users can be found in Section 16.3 - Privileged User Access and additional information on security clearance, briefing and authorisation requirements can be found in Section 9.2 - Authorisations, Security Clearances and Briefings.

Rationale & Controls

Access control lists

16.2.4.R.01. **Rationale**

A clearly defined process will assist an organisation in the **consistent development** of access control lists for their systems.

16.2.4.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:1930]

Agencies MUST follow a defined process for developing an access control list, such as described in the table below.

Stage	Description
1	Establish groups of all system resources based on similar security objectives.
2	Determine the information owner for each group of resources.
3	Obtain agreement from system owners.
4	Establish groups encompassing all system users based on similar functions or security objectives.
5	Determine the group owner or manager for each group of system users.
6	Determine the degree of access to the resource for each system user group, incorporating the principal of least-privilege access.
7	Decide on the level of access for security administration, based on the internal security policy.
8	Identify any classification, protective markings, and releasability indicators (such as NZEO or compartmented information).

Enforcing authorisations on systems

16.2.5.R.01. **Rationale**

Use of access controls on a system will assist in enforcing the need-to-know principle. How access controls are set up in organisations are becoming increasing important to mitigate threats and minimise attack surfaces.

16.2.5.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:1924]

Agencies MUST have authorisation of system users enforced by access controls.

Protecting compartmented information on systems

16.2.6.R.01. **Rationale**

Compartmented information is particularly sensitive and as such extra measures need to be put in place on systems to restrict access to those with sufficient authorisation, briefings and a demonstrated need-to-know or need- to access.

16.2.6.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:1927]

Agencies MUST restrict access to compartmented information. Such restriction MUST be enforced by the system.

Access from foreign controlled systems and facilities

16.2.7.R.01. **Rationale**

If a New Zealand system is to be accessed overseas it will need to be from at least a facility owned by a country that New Zealand has a multilateral or bilateral agreement with. NZEO systems can be accessed only from facilities under the sole control of the government of New Zealand and by New Zealand citizens.

16.2.7.C.01. **Control System Classifications(s): All Classifications; Compliance: Must Not** [CID:1920]

Agencies MUST NOT allow access to NZEO information from systems and facilities not under the sole control of the government of New Zealand and New Zealand citizens.

16.2.7.C.02. **Control System Classifications(s): All Classifications; Compliance: Should Not** [CID:1921]

Unless a multilateral or bilateral security agreement is in place, agencies SHOULD NOT allow access to classified information from systems and facilities not under the sole control of the government of New Zealand and New Zealand citizens.