16.3. Privileged User Access

Objective

16.3.1. Only trusted personnel are granted privileged access to systems.

Context

Scope

16.3.2. This section covers information relating specifically to personnel that are granted privileged access to systems. Refer also to Section 16.4 – Privileged Access Management.

Privileged access

16.3.3. Within this section, privileged access is, considered to be access which can give a system user:

- the ability to change key system configurations;
- the ability to change control parameters;
- access to audit and security monitoring information;
- the ability to circumvent security measures;
- access to all data, files and accounts used by other system users, including backups and media; or
- special access for troubleshooting the system.

References

16.3.4. Additional information relating to privileged and system accounts, including monitoring, is contained in:

Reference	Title	Publisher	Source
	Restricting administrative privileges	ASD	Restricting Administrative Privileges | Cyber.gov.au

Rationale & Controls

Use of privileged accounts

16.3.5.R.01. **Rationale**

Inappropriate use of any aspect of a system that enables a privileged user to override system or application controls can be a major contributory factor to failures, information security incidents, or system breaches.

16.3.5.R.02. **Rationale**

Privileged access rights allow for system wide changes to be made, as such logging, monitoring and strong change management practice provide greater accountability and auditing capability.

16.3.5.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:1945]

Agencies MUST:

- ensure strong change management practices are implemented;
- ensure that the use of privileged accounts is controlled and accountable;
- ensure that system administrators are assigned, and consistently use, an individual account for the performance of their administration tasks;
- keep privileged accounts to a minimum; and
- allow the use of privileged accounts for administrative work only.

Privileged system access by foreign nationals

16.3.6.R.01.

Rationale

As privileged users may have the ability to bypass controls on a system it is strongly encouraged that foreign nationals are not given privileged access to systems processing particularly sensitive information.

16.3.6.C.01. **Control System Classifications(s): All Classifications; Compliance: Must Not** [CID:1949]

Agencies MUST NOT allow foreign nationals, including seconded foreign nationals, to have privileged access to systems that process, store or communicate NZEO information.

16.3.6.C.02. **Control System Classifications(s): All Classifications; Compliance: Should Not** [CID:1950]

Agencies SHOULD NOT allow foreign nationals, including seconded foreign nationals, to have privileged access to systems that process, store or communicate classified information.

Security clearances for privileged users

16.3.7.R.01. **Rationale**

When frequent data transfers occur between systems of different classifications, having privileged users from the lesser system cleared to the classification of the higher system will assist in any actions that need to be taken resulting from any data spill.

16.3.7.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1953]

Agencies involved in frequent transfers of data from another system to their system with a lesser classification SHOULD ensure at least one privileged user has a security clearance level commensurate the classification of the higher system.