9.2. Authorisations, Security Clearances And Briefings

Objective

9.2.1. Only appropriately authorised, cleared and briefed personnel are allowed access to systems.

Context

Scope

9.2.2. This section covers information relating to the authorisations, security clearances and briefings required by personnel to access systems. Information on the technical implementation of access controls for systems can be found in Section 16.2 - System Access.

Security clearances – New Zealand and foreign

9.2.3. Where this manual refers to security clearances, the reference applies to a National Security Clearance granted by a New Zealand government agency. Foreign nationals may be granted a National Security Clearance if **identified** risks can be mitigated. Refer to PSR Personnel Security for more information.

9.2.4. Such security clearances are required for many roles worldwide by government, commercial and other organisations where there is a requirement for assurance of the ability of an individual and organisation to securely access, manage, and protect confidential, sensitive or classified information. Not all security clearances will grant the same level or types of access.

9.2.5. The process invariably includes background or security checks on the individual, a briefing and then signing documents, in which the individual formally acknowledges the legal requirements to not share such information with unauthorised individuals or organisations. This will include a requirement not to inappropriately remove, store or access classified documents or other sensitive information.

9.2.6. In New Zealand there are two security authorisation processes:

i. for information classified CONFIDENTIAL and above; and
ii. for information classified RESTRICTED and below.

9.2.7. For information classified **CONFIDENTIAL and above** a formal vetting process is required to gain a **National Security Clearance**. Refer to the PSR for more detail of vetting requirements and the process for applying for National Security Clearance.

9.2.8. For information classified **RESTRICTED and below**, the authorisations, security checks and supporting briefings form part of the Agency's recruitment and induction processes for all staff. These authorisations, security checks and briefings are evidenced by a formal record of approval of the authorisation, the requirement for a security check and a signed acknowledgement from the individual staff member. The level of detail for the agency's process will depend on the role, tasks and position of the agency employee.

PSR References

9.2.9. Additional policy and information on granting and maintaining security clearances can be found in:

Reference	Title	Source
PSR Mandatory Requirements	GOV4, INFOSEC1, PERSEC1, PERSEC2, PERSEC3, PERSEC4, PHYSEC1 and PHYSEC2	Home | Protective Security Requirements Security governance (GOV) | Protective Security Requirements Information security (INFOSEC) | Protective Security Requirements Personnel security (PERSEC) | Protective Security Requirements Physical security (PHYSEC) | Protective Security Requirements

Rationale & Controls

Documenting authorisations, security clearance and briefing requirements

9.2.10.R.01. **Rationale**

Ensuring that the requirements for access to a system are documented and agreed upon will assist in determining if system users have appropriate authorisations, security clearances and need-to-know to access the system.

9.2.10.R.02. **Rationale**

Types of system users for which access requirements will need to be documented include general users, privileged users, system administrators, contractors and visitors.

9.2.10.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:1480]

Agencies MUST specify in the System Security Plan (SSP) any authorisations, security clearances and briefings necessary for system access.

Authorisation and system access

9.2.11.R.01. **Rationale**

Personnel seeking access to a system will need to have a genuine business requirement to access the system as verified by their supervisor or manager. Once a requirement to access a system is established, the system user should be given only the privileges that they need to undertake their duties. Providing all system users with privileged access when there is no such requirement can cause significant security vulnerabilities in a system.

9.2.11.C.01. **Control System Classifications(s): Top Secret; Compliance: Must** [CID:1483]

Agencies MUST:

- limit system access on a need-to-know/need-to-access basis;
- provide system users with the least amount of privileges needed to undertake their duties; and
- have any requests for access to a system authorised by the supervisor or manager of the system user.

9.2.11.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1484]

Agencies SHOULD:

- limit system access on a need-to-know/need-to-access basis;
- provide system users with the least amount of privileges needed to undertake their duties;
- have any requests for access to a system authorised by the supervisor or manager of the system user; and
- ensure a formal acknowledgement of the security briefing is obtained and recorded.

Recording authorisation for personnel to access systems

9.2.12.R.01. **Rationale**

In many cases, the requirement to maintain a secure record of all personnel authorised to access a system, their user identification, who provided the authorisation and when the authorisation was granted, can be met by retaining a completed system account request form signed by the supervisor or manager of the system user.

9.2.12.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1487]

Agencies SHOULD:

- maintain a secure record of:
    - all authorised system users;
    - their user identification;
    - why access is required;
    - role and privilege level,
    - who provided the authorisation to access the system;
    - when the authorisation was granted; and
- keep a copy of the acknowledgement signed by the individual granted a clearance; and
- maintain the record, for the life of the system or information to which access is granted, or the length of employment, whichever is the longer.

Security clearance for system access

9.2.13.R.01. **Rationale**

Information classified as CONFIDENTIAL and above requires personnel to have been granted a formal security clearance before access is granted. Refer to the PSR Policy Framework - Personnel Security.

9.2.13.C.01.

Control System Classifications(s): Confidential, Top Secret, Secret; Compliance: Must Not [CID:1490]

System users MUST NOT be granted access to systems or information classified CONFIDENTIAL or above unless vetting procedures have been completed and formal security clearance granted.

9.2.13.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:1491]

All system users MUST:

- hold a security clearance or other authorisation appropriate for the system classification; or
- have been granted access in accordance with the requirements in the PSR for emergency access.

System access briefings

9.2.14.R.01. **Rationale**

Some systems process endorsed or compartmented information. As such, unique briefings may exist that system users need to receive before being granted access to the system. All system users will require a briefing on their responsibilities on access to and use of the system to which they have been granted access to avoid inadvertent errors and security breaches. Specialised system training may also be required.

9.2.14.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:1494]

All system users MUST have received any necessary briefings before being granted access to compartmented or endorsed information or systems.

Access by foreign nationals to NZEO systems

9.2.15.R.01. **Rationale**

NZEO information is restricted to New Zealand nationals.

9.2.15.C.01. **Control System Classifications(s): All Classifications; Compliance: Must Not** [CID:1497]

Where systems process, store or communicate unprotected NZEO information, agencies MUST NOT allow foreign nationals, including seconded foreign nationals, to have access to the system.

9.2.15.C.02. **Control System Classifications(s): All Classifications; Compliance: Must Not** [CID:1498]

Where agencies protect NZEO information on a system by implementing controls to ensure that NZEO information is not passed to, or made accessible to, foreign nationals, agencies MUST NOT allow foreign nationals, including seconded foreign nationals, to have access to the system.

Access by foreign nationals to New Zealand systems

9.2.16.R.01. **Rationale**

When information from foreign nations is entrusted to the New Zealand Government, care needs to be taken to ensure that foreign nationals do not have access to such information unless it has also been released to their country.

9.2.16.C.01. **Control System Classifications(s): All Classifications; Compliance: Must Not** [CID:1501]

Where systems process, store or communicate classified information with nationality releasability markings, agencies MUST NOT allow foreign nationals, including seconded foreign nationals, to have access to such information that is not marked as releasable to their nation.

Granting limited higher access

9.2.17.R.01. **Rationale**

Under exceptional circumstances, temporary access to systems classified RESTRICTED and below may be granted.

9.2.17.C.01. **Control System Classifications(s): Confidential, Top Secret, Secret; Compliance: Must Not** [CID:1504]

Agencies MUST NOT permit limited higher access for systems and information classified CONFIDENTIAL or above.

9.2.17.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:1505]

Agencies granting **limited** higher access to information or systems MUST ensure that:

- the requirement to grant limited higher access is temporary in nature and is an exception rather than the norm;
- an ITSM has recommended the limited higher access;
- a cessation date for limited higher access has been set;
- the access period does not exceed two months;

- the limited higher access is granted on an occasional NOT non-ongoing basis;
- the system user is not granted privileged access to the system;
- the system user's access is formally documented; and
- the system user's access is approved by the CISO.

Controlling limited higher access

9.2.18.R.01. **Rationale**

When personnel are granted access to a system under the provisions of limited higher access they need to be closely supervised or have their access controlled such that they have access only to that information they require to undertake their duties.

9.2.18.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:1508]

Agencies granting **limited** higher access to a system MUST ensure that:

- the approval for access is formally acknowledged and recorded; and either
  - effective controls are in place to restrict access **only** to classified information that is necessary to undertake the system user's duties; or
  - the system user is continually supervised by another system user who has the appropriate security clearances to access the system.

Granting emergency access

9.2.19.R.01. **Rationale**

Emergency access to a system may be granted where there is an immediate and critical need to access information for which personnel do not have the appropriate security clearances. Such access will need to be granted by the agency head or their delegate and be formally documented.

9.2.19.R.02. **Rationale**

It is important that appropriate debriefs take place at the conclusion of any emergency in order to manage the ongoing security of information and systems and to identify "lessons learned".

9.2.19.C.01. **Control System Classifications(s): Confidential, Top Secret, Secret; Compliance: Must Not** [CID:1512]

Emergency access MUST NOT be granted unless personnel have a security clearance to at least CONFIDENTIAL level.

9.2.19.C.02. **Control System Classifications(s): Confidential, Secret, Top Secret; Compliance: Must Not** [CID:1513]

Emergency access MUST NOT be used on reassignment of duties while awaiting completion of full security clearance procedures.

9.2.19.C.03. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:1514]

Agencies granting emergency access to a system MUST ensure that:

- the requirements to grant emergency access is due to an immediate and critical need to access classified information and there is insufficient time to complete clearance procedures;
- the agency head or their delegate has approved the emergency access;
- the system user's access is formally documented;
- the system user's access is reported to the CISO;
- appropriate briefs and debriefs for the information and system are conducted;
- access is limited to information and systems necessary to deal with the particular emergency and is governed by strict application of the "need to know" principle;
- emergency access is limited to ONE security clearance level higher than the clearance currently held; and
- the security clearance process is completed as soon as possible.

9.2.19.C.04. **Control System Classifications(s): Secret, Top Secret, Confidential; Compliance: Must** [CID:1515]

Personnel granted emergency access MUST be debriefed at the conclusion of the emergency.

Accessing endorsed or compartmented information

9.2.20.R.01. **Rationale**

Limited higher access to systems processing, storing or communicating endorsed or compartmented information is not permitted.

9.2.20.C.01. **Control System Classifications(s): All Classifications; Compliance: Must Not** [CID:1518]

Agencies MUST NOT grant limited higher access to systems that process, store or communicate endorsed or compartmented information.