21.1. Data Transfers

Objective

21.1.1. Data transfers between systems are controlled and accountable.

Context

Scope

21.1.2. This section covers the fundamental requirements of data transfers between systems and applies equally to data transfers using removal media and to data transfers via gateways.

21.1.3. Additional requirements for data transfers using removal media can be found in the Section 13.3 – Media Usage and additional requirements for data transfers via gateways can be found in the Section 20.2 – Data Import and Export.

21.1.4. Transfers from a classified system where strong information security controls exist to a system of lower classification where controls may not be as robust, can lead to data spills, information loss and privacy breaches. It is important that appropriate levels of oversight and accountability are in place to minimise or prevent the undesirable loss or leakage of information.

PSR references

21.1.5. Relevant PSR requirements can be found at:

Reference	Title	Source
PSR Mandatory Requirements	GOV2, GOV6, INFOSEC1, INFOSEC2, INFOSEC3, INFOSEC4, PERSEC1, PERSEC2, PERSEC3 and PERSEC4	Home | Protective Security Requirements Security governance (GOV) | Protective Security Requirements Information security (INFOSEC) | Protective Security Requirements Personnel security (PERSEC) | Protective Security Requirements

Rationale & Controls

User responsibilities

21.1.6.R.01. **Rationale**

When users transfer data to and from systems they need to be aware of the potential consequences of their actions. This could include data spills of classified information onto systems not accredited to handle the classification of the data or the unintended introduction of malicious code. Accordingly agencies will need to hold personnel accountable for all data transfers that they make.

21.1.6.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4138]

Agencies MUST establish a policy and train staff in the processes for data transfers between systems and the authorisations required before transfers can take place.

21.1.6.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4141]

Agencies MUST ensure that system users transferring data to and from a system are held accountable for the data they transfer.

Data transfer processes and procedures

21.1.7.R.01. **Rationale**

Personnel can assist in preventing information security incidents by checking protective markings (classifications, endorsements and releasability)

checks to ensure that the destination system is appropriate for the protection of the data being transferred, performing antivirus checks on data to be transferred to and from a system, and following all processes and procedures for the transfer of data.

21.1.7.C.01. **Control System Classifications(s): Confidential, Top Secret, Secret; Compliance: Must** [CID:4147]

Agencies MUST ensure that data transfers are performed in accordance with processes and procedures approved by the Accreditation Authority.

21.1.7.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4148]

Agencies SHOULD ensure that data transfers are performed in accordance with processes and procedures approved by the Accreditation Authority.

Data transfer authorisation

21.1.8.R.01. **Rationale**

Using a trusted source to approve transfers from a classified system to another system of a lesser classification or where a releasability endorsement is applied to the data to be transferred, ensures appropriate oversight and reporting of the activity.

21.1.8.C.01. **Control System Classifications(s): Secret, Confidential, Top Secret; Compliance: Must** [CID:4151]

Agencies MUST ensure that all data transferred to a system of a lesser classification or a less secure system, is approved by a trusted source.

Trusted sources

21.1.9.R.01. **Rationale**

Trusted sources are designated personnel who have the delegated authority to assess and approve the transfer or release of data or documents. Trusted sources may include security personnel within the agency such as the CISO and the ITSM.

21.1.9.C.01. **Control System Classifications(s): Top Secret, Secret, Confidential; Compliance: Must** [CID:4156]

Trusted sources MUST be:

- a strictly limited list derived from business requirements and the result of a security risk assessment;
- where necessary an appropriate security clearance is held; and
- approved by the Accreditation Authority.

Import of data

21.1.10.R.01. **Rationale**

Scanning imported data for active or malicious content reduces the security risk of a system or network being infected, thus allowing the continued confidentiality, integrity and availability of the system or network.

21.1.10.R.02. **Rationale**

Format checks provide a method to prevent known malicious formats from entering the system or network. Keeping and regularly auditing these logs allow for the system or network to be checked for any unusual activity or usage.

21.1.10.R.03. **Rationale**

Personnel reporting unexpected events through the agency's incident management process provide an early opportunity to contain malware, limit damage and correct errors.

21.1.10.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4165]

Agencies importing data to a system MUST ensure that the data is scanned for malicious and active content.

21.1.10.C.02. **Control System Classifications(s): Top Secret, Confidential, Secret; Compliance: Must** [CID:4168]

Agencies importing data to a system MUST implement the following controls:

- scanning for malicious and active content;
- data format checks;
- identify unexpected attachments or embedded objects;
- log each event; and
- monitoring to detect overuse/unusual usage patterns.

Export of highly formatted textual data

21.1.11.R.01.

Rationale

When highly formatted textual data with no free text fields is to be transferred between systems, the checking requirements are lessened because the format of the information is strongly defined.

21.1.11.C.01. **Control System Classifications(s): Confidential, Secret, Top Secret; Compliance: Must** [CID:4239]

When agencies export formatted textual data with no free text fields and all fields have a predefined set of permitted formats and data values, agencies MUST implement the following controls:

- protective marking checks;
- data validation and format checks;
- size limits;
- keyword checks;
- identify unexpected attachments or embedded objects;
- log each event; and
- monitoring to detect overuse/unusual usage patterns.

Export of other data

21.1.12.R.01. **Rationale**

Textual data that it is not highly formatted can be difficult to check in an automated manner. Agencies will need to implement measures to ensure that classified information is not accidentally being transferred to another system not accredited for that classification or transferred into the public domain.

21.1.12.C.01. **Control System Classifications(s): Confidential, Top Secret, Secret; Compliance: Must** [CID:4245]

When agencies export data, other than highly formatted textual data, agencies MUST implement the following controls:

- protective marking checks;
- data validation and format checks;
- limitations on data types;
- size limits;
- keyword checks;
- identify unexpected attachments or embedded objects;
- log each event; and
- monitoring to detect overuse/unusual usage patterns.

Preventing export of NZEO data to foreign systems

21.1.13.R.01. **Rationale**

In order to reduce the security risk of spilling data with an endorsement onto foreign systems, it is important that procedures are developed to detect NZEO marked data and to prevent it from crossing into foreign systems or being exposed to foreign nationals.

21.1.13.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4249]

Agencies MUST:

- ensure that keyword searches are performed on all textual data;
- ensure that any identified data is quarantined until reviewed and approved for release by a trusted source other than the originator; and
- develop procedures to prevent NZEO information in both textual and non-textual formats from being exported.