21.2. Data Import and Export

Objective

21.2.1. Data is transferred through gateways in a controlled and accountable manner.

Context

Scope

21.2.2. This section covers the specific requirements relating to the movement of data between systems via gateways. Fundamental requirements of data transfers between systems can be found in Section 20.1 – Data Transfers. These fundamental requirements apply to gateways.

Rationale & Controls

User responsibilities

21.2.3.R.01. **Rationale**

When users transfer data to or from a system they need to be aware of the potential consequences of their actions. This could include data spills of sensitive or classified data onto systems not accredited to handle the data, or the unintended introduction of malicious code to a system. Accordingly, users need to be held accountable for all data transfers they make.

21.2.3.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4264]

Users transferring data to and from a system MUST be held accountable for the data they transfer.

Data Transfer authorisation

21.2.4.R.01. **Rationale**

Users can help prevent information security incidents by:

- checking protective markings to ensure that the destination system is appropriate for the data being transferred;
- performing antivirus checks on data to be transferred to and from a system;
- following the processes and procedures for the transfer of data.

21.2.4.C.01. **Control System Classifications(s): Secret, Confidential, Top Secret; Compliance: Must** [CID:4269]

All data transferred to a system of a lesser sensitivity or classification MUST be approved by a trusted source.

Trusted sources

21.2.5.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.

21.2.5.C.01. **Control System Classifications(s): Confidential, Secret, Top Secret; Compliance: Must** [CID:4277]

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 through gateways

21.2.6.R.01. **Rationale**

In order to ensure the continued functioning of systems it is important to constantly analyse data being imported. Converting data from one format

into another can effectively destroy most malicious active content.

21.2.6.C.01. **Control System Classifications(s): Secret, Confidential, Top Secret; Compliance: Must** [CID:4280]

When agencies import data to a system through gateways, the data MUST be filtered by a product specifically designed for that purpose, including filtering malicious and active content.

21.2.6.C.02. **Control System Classifications(s): Confidential, Top Secret, Secret; Compliance: Must** [CID:4281]

When agencies import data to a system through gateways, full or partial audits of the event logs MUST be performed at least monthly.

21.2.6.C.03. **Control System Classifications(s): Confidential, Secret, Top Secret; Compliance: Should** [CID:4282]

Agencies SHOULD convert data being imported at gateways into an alternative format before entering the network.

Export of data through gateways

21.2.7.R.01. **Rationale**

In order to ensure the continued integrity and confidentiality of data on an agency network, data MUST pass through a series of checks before it is exported onto systems of a lesser classification.

21.2.7.R.02. **Rationale**

Filtering content based on protective markings is an adequate method to protect the confidentiality of lesser classified material.

21.2.7.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4286]

Agencies SHOULD restrict the export of data to a system of a lesser classification by filtering data using at least protective marking checks.

Export of highly formatted textual data through gateways

21.2.8.R.01. **Rationale**

The security risks of releasing higher classified data are partially reduced when the data is restricted to highly formatted textual data. In such cases the data is less likely to contain hidden data and have classified content. Such data can be automatically scanned through a series of checks to detect classified content. Risk is further reduced when there is a gateway filter that blocks (rejects) the export of data classified above the classification of the network outside of the gateway, and logs are regularly reviewed to detect if there has been unusual usage or overuse.

21.2.8.C.01. **Control System Classifications(s): Top Secret, Confidential, Secret; Compliance: Must** [CID:4289]

When the export of highly formatted textual data occurs through gateways agencies MUST implement:

- checks for protective markings;
- data filtering performed by a product specifically designed for that purpose;
- data range and data type checks; and
- full or partial audits of the event logs performed at least monthly.

Export of other data through gateways

21.2.9.R.01. **Rationale**

Textual data which is not highly formatted can contain hidden data as well as having a higher classification due to the aggregated content. Risk is somewhat reduced by running additional automated checks on non-formatted data being exported, in addition to those checks for highly formatted textual data. Where a classification cannot be automatically determined, a human trusted source should make that determination.

21.2.9.C.01. **Control System Classifications(s): Confidential, Secret, Top Secret; Compliance: Must** [CID:4292]

When agencies export data, other than highly formatted textual data, through gateways, agencies MUST implement data filtering performed by a product specifically designed for that purpose.

21.2.9.C.02. **Control System Classifications(s): Top Secret, Confidential, Secret; Compliance: Must** [CID:4293]

When agencies do not perform audits of the complete data transfer logs at least monthly they MUST perform randomly timed audits of random subsets of the data transfer logs on a weekly basis.

21.2.9.C.03. **Control System Classifications(s): Top Secret, Secret, Confidential; Compliance: Should** [CID:4294]

Where the classification cannot be determined automatically, a human trusted source SHOULD assess the classification of the data.

21.2.9.C.04. **Control System Classifications(s): Top Secret, Confidential, Secret; Compliance: Should** [CID:4295]

When the export of other data occurs through gateways agencies SHOULD perform audits of the complete data transfer logs at least monthly.

Preventing export of NZEO data to foreign systems

21.2.10.R.01. **Rationale**

NZEO networks are particularly sensitive and further security measures need to be put in place when connecting them to other networks.

21.2.10.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4301]

To prevent the export of NZEO data to foreign systems, agencies MUST implement NZEO data filtering performed by a product specifically designed or configured for that purpose.

21.2.10.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4303]

Agencies MUST undertake checks of protective markings and keywords before permitting data export.

Requirement to sign exported data

21.2.11.R.01. **Rationale**

Digitally signing data being exported, demonstrates authenticity and improves assurance that the data has not been altered in transit.

21.2.11.C.01. **Control System Classifications(s): Secret, Top Secret, Confidential; Compliance: Must** [CID:4308]

A trusted source MUST sign the data to be exported if the data is to be communicated over a network to which untrusted personnel or systems have access.

21.2.11.C.02. **Control System Classifications(s): Secret, Confidential; Compliance: Must** [CID:4309]

Agencies MUST ensure that the gateway verifies authority to release prior to the release of the data to be exported.

21.2.11.C.03. **Control System Classifications(s): Confidential, Top Secret, Secret; Compliance: Should** [CID:4310]

Agencies SHOULD use a product evaluated to at least an EAL4 assurance level for the purpose of data signing and signature confirmation.