Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Australian Government Information Security Manual

JUNE 2021

Guidelines for Data Transfers

Data transfers

Data transfer process and procedures

Ensuring that a data transfer process, and supporting data transfer procedures, is adhered to will facilitate the consistent application of data transfer-related security controls and the generation of necessary audit records.

Security Control: 0663; Revision: 5; Updated: Aug-19; Applicability: O, P, S, TS
A data transfer process, and supporting data transfer procedures, is developed and implemented.

User responsibilities

When users transfer data to or from a system, they should understand the potential consequences of their actions. This could include spills of data onto a system not authorised to handle the data, or the unintended introduction of malicious code to a system. Accordingly, users should be held accountable for all data transfers that they make.

Security Control: 0661; Revision: 7; Updated: Apr-19; Applicability: O, P, S, TS
Users transferring data to and from a system are held accountable for the data they transfer.

Trusted sources

Trusted sources are people or systems responsible for authorising data exports based on a formal assessment. Trusted sources may include an organisation's Chief Information Security Officer (CISO) and their delegates.

Security Control: 0665; Revision: 5; Updated: Jun-20; Applicability: S, TS
Trusted sources are limited to people and systems that have been authorised as such by an organisation's CISO.

Data transfer approval

Users can prevent cyber security incidents by checking protective markings to ensure that the destination system is appropriate for the data being transferred, performing antivirus scanning on data to be transferred, and following all other procedures as part of the data transfer process.

Security Control: 0664; Revision: 5; Updated: Sep-18; Applicability: S, TS
All data transferred to a system of a lesser sensitivity or classification is reviewed and approved by a trusted source.

Security Control: 0675; Revision: 4; Updated: Jun-20; Applicability: S, TS
A trusted source signs all data authorised for export from a system.

Import of data

Scanning data being imported to a system for malicious and active content reduces the likelihood of the system being infected with malicious code.

Security Control: 0657; Revision: 4; Updated: Sep-18; Applicability: O, P
Data imported to a system is scanned for malicious and active content.

Security Control: 0658; Revision: 4; Updated: Sep-18; Applicability: S, TS
Data imported to a system is scanned for malicious and active content, undergoes data format checks and logging, and is monitored to detect overuse/unusual usage patterns.

Export of data

When data is exported from a system, protective markings should be assessed to determine if the export is permitted. Thorough inspection, the likelihood of data being transferred to a system that is not authorised to handle it, or into the public domain, can be reduced.

Security Control: 1187; Revision: 1; Updated: Sep-18; Applicability: O, P
When exporting data, protective marking checks are undertaken.

Security Control: 0669; Revision: 3; Updated: Sep-18; Applicability: S, TS
When exporting data, the following activities are undertaken:

- *protective marking checks*
- *data format checks and logging*
- *monitoring to detect overuse/unusual usage patterns*
- *limitations on data types and sizes*
- *keyword searches on all textual data.*

Preventing export of particularly important data to foreign systems

In order to reduce the likelihood of spilling Australian Eyes Only (AUSTEO) and Australian Government Access Only (AGAO) data onto foreign systems, it is important that a process, and supporting procedures, is developed to detect AUSTEO and AGAO data and to prevent it from crossing into foreign systems.

Security Control: 1535; Revision: 1; Updated: Aug-19; Applicability: S, TS
A process, and supporting procedures, is developed and implemented to prevent AUSTEO and AGAO data in both textual and non-textual formats from being exported to foreign systems.

Security Control: 0678; Revision: 2; Updated: Sep-18; Applicability: S, TS
When exporting data from an AUSTEO or AGAO system, keyword searches are undertaken on all textual data and any identified data is quarantined until reviewed and approved for release by a trusted source other than the originator.

Monitoring data import and export

It is important to monitor data import and export processes to ensure the confidentiality and integrity of systems and data. This applies to all import and export mechanisms including those which are performed using a gateway, Cross Domain Solution or removable media. Data transfer logs can assist with such activities and may contain information such as who authorised the data transfer, the type of data transferred, where the data was transferred from/to, when the data was transferred, why the data was transferred and how the data was transferred.

Security Control: 1586; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS
Data transfer logs are used to record all data imports and exports from systems.

Security Control: 1294; Revision: 3; Updated: Aug-20; Applicability: O, P
Data transfer logs are partially audited at least monthly.

Security Control: 0660; Revision: 7; Updated: Aug-20; Applicability: S, TS
Data transfer logs are fully audited at least monthly.

Further information

Further information on using removable media for data transfers can be found in the media usage section of the ***Guidelines for Media***.

Further information on data transfers involving a gateway or Cross Domain Solution can be found in the content filtering section of the ***Guidelines for Gateways***.