Information Security Manual

Last updated: June 2024

Guidelines for Data Transfers

Data transfers

Performing data transfers

This section describes controls applicable to manual data transfers and data transfers using gateways or Cross Domain Solutions (CDSs). For data transfers using gateways or CDSs, the content filtering section of the *Guidelines for Gateways* is also applicable.

Data transfer processes and procedures

Ensuring that data transfer processes and procedures are developed, implemented and maintained can facilitate consistent data transfers. In addition, in order to reduce the likelihood of Australian Eyes Only (AUSTEO), Australian Government Access Only (AGAO) and Releasable To (REL) data crossing into unsuitable foreign systems, it is important that additional processes and procedures are developed, implemented and maintained to prevent this from occurring. Note, depending on protective markings applied to REL data, it may be suitable for export to some foreign systems but not to others.

Control: ISM-0663; Revision: 7; Updated: Dec-22; Applicability: All; Essential Eight: N/A
Data transfer processes, and supporting data transfer procedures, are developed, implemented and maintained.

Control: ISM-1535; Revision: 6; Updated: Jun-24; Applicability: S, TS; Essential Eight: N/A
Processes, and supporting procedures, are developed, implemented and maintained to prevent AUSTEO, AGAO and REL data in textual and non-textual formats from being exported to unsuitable foreign systems.

User responsibilities

When users transfer data to or from systems, they should understand the potential consequences of their actions. This could include transferring data onto systems not authorised to handle the data, or the unintended introduction of malicious code to systems. As such, users should be held accountable for all data transfers that they perform.

Control: ISM-0661; Revision: 8; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Users transferring data to and from systems are held accountable for data transfers they perform.

Manual import of data

When manually importing data to systems, such as via the use of removable media, the data should be scanned for malicious and active content to reduce the likelihood of causing a malicious code infection. In cases where security

checks fail, data should be quarantined until it can be reviewed and subsequently approved or not approved for release.

Control: ISM-0657; Revision: 6; Updated: Mar-22; Applicability: All; Essential Eight: N/A
When manually importing data to systems, the data is scanned for malicious and active content.

Control: ISM-1778; Revision: 0; Updated: Mar-22; Applicability: All; Essential Eight: N/A
When manually importing data to systems, all data that fails security checks is quarantined until reviewed and subsequently approved or not approved for release.

Authorising export of data

Data exported from SECRET and TOP SECRET systems should be reviewed and authorised by a trusted source beforehand, such as the Chief Information Security Officer or one of their delegates. In doing so, all data authorised for export should be digitally signed by the trusted source.

Control: ISM-0664; Revision: 7; Updated: Mar-22; Applicability: S, TS; Essential Eight: N/A
Data exported from SECRET and TOP SECRET systems is reviewed and authorised by a trusted source beforehand.

Control: ISM-0675; Revision: 6; Updated: Mar-22; Applicability: S, TS; Essential Eight: N/A
Data authorised for export from SECRET and TOP SECRET systems is digitally signed by a trusted source.

Control: ISM-0665; Revision: 7; Updated: Jun-23; Applicability: S, TS; Essential Eight: N/A
Trusted sources for SECRET and TOP SECRET systems are limited to people and services that have been authorised as such by the Chief Information Security Officer.

Manual export of data

When manually exporting data from systems, such as via the use of removable media, the data should be checked for unsuitable protective markings to reduce the likelihood of causing a data spill. In addition, data manually exported from SECRET and TOP SECRET systems will require additional assurances, for example, by validating digital signatures and checking for keywords within all textual data. Finally, in cases where security checks fail, data should be quarantined until it can be reviewed and subsequently approved or not approved for release.

Control: ISM-1187; Revision: 3; Updated: Mar-22; Applicability: All; Essential Eight: N/A
When manually exporting data from systems, the data is checked for unsuitable protective markings.

Control: ISM-0669; Revision: 6; Updated: Dec-22; Applicability: S, TS; Essential Eight: N/A
When manually exporting data from SECRET and TOP SECRET systems, digital signatures are validated and keyword checks are performed within all textual data.

Control: ISM-1779; Revision: 0; Updated: Mar-22; Applicability: All; Essential Eight: N/A
When manually exporting data from systems, all data that fails security checks is quarantined until reviewed and subsequently approved or not approved for release.

Monitoring data import and export

To ensure the ongoing confidentiality and integrity of systems, applications and data, it is important to log all data transfers. This applies to all forms of data transfers, such as those performed using removable media, gateways or CDSs. Ideally, data transfer logs should contain information on who authorised the data transfer, what data was transferred, where the data was transferred from or to, when the data was transferred, why the data was transferred, and how the data was transferred. Monitoring of such activities, via periodic verification of data transfer logs, can

assist in identifying abuse of data transfer privileges and any unusual usage patterns that may indicate attempts by malicious actors to surreptitiously import malicious code or exfiltrate data from SECRET and TOP SECRET systems.

Control: ISM-1586; Revision: 0; Updated: Aug-20; Applicability: All; Essential Eight: N/A
Data transfer logs are used to record all data imports and exports from systems.

Control: ISM-1294; Revision: 5; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Data transfer logs for systems are partially verified at least monthly.

Control: ISM-0660; Revision: 9; Updated: Mar-22; Applicability: S, TS; Essential Eight: N/A
Data transfer logs for SECRET and TOP SECRET systems are fully verified at least monthly.

Further information

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

Further information on data transfers using gateways or CDSs can be found in the content filtering section of the *Guidelines for Gateways*.

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

For more information, or to report a cyber security incident, contact us:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

Australian Government

Australian Signals Directorate