Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Australian Government Information Security Manual

NOVEMBER 2018

Guidelines for data transfers and content filtering

Data transfers

Data transfer procedures

Ensuring that correct procedures are adhered to facilitates the appropriate and consistent application of security controls as well as the generation of necessary audit records.

Security Control: 0663; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
Data transfers are performed in accordance with approved procedures.

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 systems 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: 6; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
Users transferring data to and from a system are held accountable through policies and procedures for the data they transfer.

Trusted sources

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

Security Control: 0665; Revision: 3; Updated: Sep-18; Applicability: S, TS; Priority: Must
Trusted sources are a strictly limited number of personnel that have been identified using a security risk assessment and have been authorised as such by an organisation's CISO.

Security Control: 0675; Revision: 3; Updated: Sep-18; Applicability: S, TS; Priority: Must
A trusted source makes an informed decision to sign all data authorised for export from a security domain.

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 for data transfers.

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

Import of data

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

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

Security Control: 0658; Revision: 4; Updated: Sep-18; Applicability: S, TS; Priority: Must
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 between systems, the classification should be assessed to determine if the export is permitted. Thorough inspection, including protective marking checks, can reduce the likelihood of data being transferred to a system that is not authorised to handle it or into the public domain.

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

Security Control: 0669; Revision: 3; Updated: Sep-18; Applicability: S, TS; Priority: Must
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 procedures are developed to detect AUSTEO and AGAO data and to prevent it from crossing into foreign systems.

Security Control: 1535; Revision: 0; Updated: Sep-18; Applicability: S, TS; Priority: Must
Procedures are developed 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; Priority: Must
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 Cross Domain Solutions (CDS), gateways and removable media.

Security Control: 0667; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
Data exported from each security domain, including through a gateway, is only permitted once the classification has been assessed including a protective marking check.

Security Control: 0660; Revision: 5; Updated: Sep-18; Applicability: S, TS; Priority: Must
When importing data to each security domain, by any means including through a gateway, the complete data transfer logs are audited at least monthly.

Security Control: 0673; Revision: 5; Updated: Sep-18; Applicability: S, TS; Priority: Must
When exporting data out of each security domain, by any means including through a gateway, the complete data transfer logs are audited at least monthly.

Security Control: 1294; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
When importing content to a security domain, including through a gateway, monthly audits of the imported content are performed.

Security Control: 1295; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
When exporting content out of a security domain, including through a gateway, monthly audits of the exported content are performed.

Further information

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

Further information on data transfers via gateways or security domains can be found in the ***Content filtering*** section of these guidelines.

Content filtering

Content filtering techniques

Content filters reduce the likelihood of unauthorised or malicious content transiting a security domain boundary by assessing data based on defined security policies. The following techniques can assist with assessing the suitability of data to transit a security domain boundary.

Technique	Purpose
Antivirus scan	Scans the data for viruses and other malicious code.
Automated dynamic analysis	Analyses email and web content in a sandbox before delivering it to users.
Data format check	Inspects data to ensure that it conforms to expected and permitted formats.
Data range check	Checks the data in each field to ensure that it falls within the expected and permitted ranges.
Data type check	Inspects each file header to determine the actual file type.

File extension check	Inspects the file name extension to determine the purported file type.
Keyword search	Searches data for keywords or 'dirty words' that could indicate the presence of inappropriate or undesirable material.
Metadata check	Inspects files for metadata that should be removed prior to release.
Protective marking check	Validates the protective marking of the data to ensure that it is correct.
Manual inspection	The manual inspection of data for suspicious content that an automated system could miss, which is particularly important for the transfer of multimedia or content rich files.
Verification against file specification	Verifies that the file conforms to the defined file specification and can be effectively processed by subsequent content filters.

Content filtering

Implementing an effective content filter which cannot be bypassed reduces the likelihood of malicious content successfully passing into a security domain. Content filtering is only effective when suitable components are selected and appropriately configured with consideration of an organisation's business processes and threat environment.

When content filters are protecting classified environments as a component of a CDS, their assurance requirements necessitate rigorous security testing.

Security Control: 0659; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
When importing data into a security domain, by any means including a CDS, the data is filtered by a content filter designed for that purpose.

Security Control: 1524; Revision: 0; Updated: Sep-18; Applicability: S, TS; Priority: Should
Content filters deployed in CDS are subject to rigorous security assessment to ensure they mitigate content-based threats and cannot be bypassed.

Active, malicious and suspicious content

Many files are executable and are potentially harmful if executed by a user. Many file type specifications allow active content to be embedded in the file, which increases the attack surface. The definition of suspicious content will depend on the system's security risk profile and what is considered to be normal system behaviour.

Security Control: 0651; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
All suspicious, malicious and active content is blocked from entering a security domain.

Security Control: 0652; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
Any data identified by a content filtering process as suspicious is blocked until reviewed and approved for transfer by a trusted source other than the originator.

Automated dynamic analysis

Analysing email and web content in a sandbox is a highly effective strategy to detect suspicious behaviour including network traffic, new or modified files, or other configuration changes.

Security Control: 1389; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
Email and web content entering a security domain is automatically run in a dynamic malware analysis sandbox to detect suspicious behaviour.

Content validation

Content validation aims to ensure that the content received conforms to an approved standard. Content validation can be an effective means of identifying malformed content, allowing organisations to block potentially malicious content. Content validation operates on a whitelisting principle, blocking all content except for that which is explicitly permitted.

Examples of content validation include:

- ensuring numeric fields only contain numeric numbers
- ensuring content falls within acceptable length boundaries
- ensuring Extensible Markup Language (XML) documents are compared to a strictly defined XML schema.

Security Control: 1284; Revision: 1; Updated: Sep-18; Applicability: O, P; Priority: Should
Content validation is performed on all data passing through a content filter with content which fails content validation blocked.

Security Control: 1285; Revision: 1; Updated: Sep-18; Applicability: S, TS; Priority: Must
Content validation is performed on all data passing through a content filter with content which fails content validation blocked.

Content conversion and transformation

Content conversion or transformation can be an effective method to render potentially malicious content harmless by separating the presentation format from the data. By converting a file to another format, the exploit, active content and/or payload can be removed or disrupted.

Examples of content conversion and transformation to mitigate the threat of content exploitation include:

- converting a Microsoft Word document to a Portable Document Format (PDF) file
- converting a Microsoft PowerPoint presentation to a series of Joint Photographic Experts Group (JPEG) images
- converting a Microsoft Excel spreadsheet to a comma-separated values file
- converting a PDF document to a plain text file.

Some file types, such as XML, will not benefit from conversion. Applying the conversion process to any attachments or files contained within other files (e.g. archive files or encoded files embedded in XML) can increase the effectiveness of a content filter.

Security Control: 1286; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
Content conversion is performed for all ingress or egress data transiting a security domain boundary.

Content sanitisation

Sanitisation is the process of attempting to make potentially malicious content safe to use by removing or altering active content while leaving the original content as intact as possible. Sanitisation is not as secure a method of content filtering as conversion, though many techniques may be combined. Inspecting and filtering extraneous application and

protocol data, including metadata, where possible will assist in mitigating the threat of content exploitation. Examples include:

- removal of document property information in Microsoft Office documents
- removal or renaming of JavaScript sections from PDF files
- removal of metadata, such as Exchangeable image file format (Exif) information from within JPEG files.

Security Control: 1287; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
Content sanitisation is performed on suitable file types if content conversion is not appropriate for data transiting a security domain boundary.

Antivirus scanning

Antivirus scanning is used to prevent, detect and remove malicious code that includes computer viruses, worms, Trojans, spyware and adware.

Security Control: 1288; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
Antivirus scanning, using multiple different scanning engines, is performed on all content.

Archive and container files

Archive and container files can be used to bypass content filtering processes if the content filter does not handle the file type and embedded content correctly. Ensuring the content filtering process recognises archived and container files will ensure the embedded files they contain are subject to the same content filtering measures as un-archived files.

Archive files can be constructed in a manner which can pose a denial of service security risk due to processor, memory or disk space exhaustion. To limit the likelihood of such an attack, content filters can specify resource constraints/quotas while extracting these files. If these constraints are exceeded the inspection is terminated, the content blocked and a security administrator alerted.

Security Control: 1289; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
The contents from archive/container files are extracted and subjected to content filter checks.

Security Control: 1290; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
Controlled inspection of archive/container files is performed to ensure that content filter performance or availability is not adversely affected.

Security Control: 1291; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
Files that cannot be inspected are blocked and generate an alert or notification.

Whitelisting permitted content

Creating and enforcing a whitelist of allowed content is a strong content filtering method. Only allowing content that satisfies a business requirement can reduce the attack surface of the system. As a simple example, an email content filter might only allow Microsoft Office documents and PDF files.

Security Control: 0649; Revision: 3; Updated: Sep-18; Applicability: O, P; Priority: Should
A whitelist of permitted content types is created and enforced based on business requirements and the results of a security risk assessment.

Security Control: 0650; Revision: 3; Updated: Sep-18; Applicability: S, TS; Priority: Must
A whitelist of permitted content types is created and enforced based on business requirements and the results of a security risk assessment.

Data integrity

Ensuring the authenticity and integrity of content reaching a security domain is a key component in ensuring its trustworthiness. It is also essential that content that has been authorised for release from a security domain is not modified (e.g. by the addition or substitution of information). If content passing through a filter contains a form of integrity protection, such as a digital signature, the content filter needs to verify the content's integrity before allowing it through. If the content fails these integrity checks it may have been spoofed or tampered with and should be dropped.

Examples of data integrity checks include:

- an email server or content filter verifying an email protected by DomainKeys Identified Mail (DKIM)
- a web service verifying the XML digital signature contained within a Simple Object Access Protocol (SOAP) request
- validating a file against a separately supplied hash
- checking that data to be exported from a security domain has been digitally signed by a release authority.

Security Control: 1292; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
The integrity of content is verified where applicable and blocked if verification fails.

Security Control: 0677; Revision: 4; Updated: Sep-18; Applicability: S, TS; Priority: Must
If data is signed, the signature is validated before the data is exported.

Encrypted data

Encryption can be used to bypass content filtering if encrypted content cannot be subject to the same checks performed on unencrypted content. Organisations should consider the need to decrypt content, depending on the security domain they are communicating with and depending on whether the need-to-know principle needs to be enforced.

Choosing not to decrypt content poses a security risk that malicious code's encrypted communications and data could move between security domains. In addition, encryption could mask information at a higher classification being allowed to pass to a security domain of lower classification, which could result in a data spill.

Where a business need to preserve the confidentiality of encrypted data exists, an organisation may consider a dedicated system to allow encrypted content through external, boundary or perimeter controls to be decrypted in an appropriately secure environment, in which case the content should be subject to all applicable content filtering controls after it has been decrypted.

Security Control: 1293; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
All encrypted content, traffic and data is decrypted and inspected to allow content filtering.