Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Information Security Manual

Last updated: December 2024

Guidelines for Gateways

Gateways

Introduction to gateways

Gateways securely manage data flows between connected networks from different security domains. In doing so, gateways take on the highest sensitivity or classification of connected security domains.

This section describes controls applicable to all types of gateways. Additional sections of these guidelines should also be consulted depending on the types of gateways being deployed and the security domains involved. For example, the Cross Domain Solutions section should be consulted for gateways between different security domains where at least one security domain is classified SECRET or TOP SECRET.

Personnel involved in the planning, design, implementation or assessment of gateways should also refer to the Australian Signals Directorate's (ASD) *Gateway Security Guidance Package*.

Implementing gateways

Gateways are critical for an organisation to reduce the security risks associated with providing external parties with access to their networks. In doing so, it is important that gateways are used not only between an organisation's networks and public network infrastructure, but also between an organisation's networks that belong to different security domains and between an organisation's networks and other organisations' networks that are connected via means other than public network infrastructure.

When implementing gateways between an organisation's networks and public network infrastructure, an organisation should place any services that external parties require access to within a demilitarised zone. This can mitigate security risks for an organisation when hosting such services in an internet-accessible manner.

Finally, in architecting gateways, it is important that they only allow explicitly authorised data flows. In support of this, gateways should inspect and filter data flows at the transport and above network layers. Furthermore, gateways should be capable of performing ingress traffic filtering to detect and prevent Internet Protocol (IP) source address spoofing.

Control: ISM-0628; Revision: 6; Updated: Mar-22; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
Gateways are implemented between networks belonging to different security domains.

Control: ISM-0637; Revision: 6; Updated: Mar-22; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
Gateways implement a demilitarised zone if external parties require access to an organisation's services.

Control: ISM-0631; Revision: 7; Updated: Mar-22; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
Gateways only allow explicitly authorised data flows.

Control: ISM-1192; Revision: 3; Updated: Mar-22; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
Gateways inspect and filter data flows at the transport and above network layers.

Control: ISM-1427; Revision: 3; Updated: Mar-22; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
Gateways perform ingress traffic filtering to detect and prevent IP source address spoofing.

System administrators for gateways

In identifying suitable system administrators for gateways, it is important that individuals comply with any citizenship requirements, undergo appropriate employment screening, and where necessary hold an appropriate security clearance, based on the sensitivity or classification of gateways. For example, all systems administrators for gateways between OFFICIAL: Sensitive and PROTECTED networks will need to hold baseline security clearances.

In addition, when creating privileged user accounts for performing administrative activities, it is important that the principle of least privilege is followed. In turn, this should be supported by the principle of separation of duties. Adhering to these two principles can ensure that system administrators for gateways are not given enough privileges to abuse gateways on their own.

Finally, providing system administrators for gateways with formal training on the operation and management of gateways will ensure that they are fully aware of, and accept, their roles and responsibilities. In doing so, formal training should be conducted through tailored privileged user training.

Control: ISM-1520; Revision: 3; Updated: Sep-23; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
System administrators for gateways undergo appropriate employment screening, and where necessary hold an appropriate security clearance, based on the sensitivity or classification of gateways.

Control: ISM-0613; Revision: 6; Updated: Mar-22; Applicability: S, TS; Essential Eight: N/A
System administrators for gateways that connect to Australian Eyes Only or Releasable To networks are Australian nationals.

Control: ISM-1773; Revision: 0; Updated: Mar-22; Applicability: S, TS; Essential Eight: N/A
System administrators for gateways that connect to Australian Government Access Only networks are Australian nationals or seconded foreign nationals.

Control: ISM-0611; Revision: 5; Updated: Mar-22; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
System administrators for gateways are assigned the minimum privileges required to perform their duties.

Control: ISM-0616; Revision: 5; Updated: Mar-22; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
Separation of duties is implemented in performing administrative activities for gateways.

Control: ISM-0612; Revision: 5; Updated: Mar-22; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
System administrators for gateways are formally trained on the operation and management of gateways.

System administration of gateways

In performing administrative activities for gateways, it is important that they are conducted via a secure path isolated from all connected networks. In doing so, this will minimise threats should a connected network be compromised by malicious actors. Furthermore, where gateways exist between networks belonging to different security domains, any shared components should be managed by system administrators for the higher security domain, alternatively, it may be more appropriate to use system administrators from a mutually agreed upon third party.

Control: ISM-1774; Revision: 0; Updated: Mar-22; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
Gateways are managed via a secure path isolated from all connected networks.

Control: ISM-0629; Revision: 5; Updated: Dec-23; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
For gateways between networks belonging to different security domains, any shared components are managed by system administrators for the higher security domain or by system administrators from a mutually agreed upon third party.

Authenticating to networks accessed via gateways

Ensuring users and information technology (IT) equipment are authenticated to other networks accessed via gateways can reduce the likelihood of unauthorised access.

Control: ISM-0619; Revision: 6; Updated: Mar-22; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
Users authenticate to other networks accessed via gateways.

Control: ISM-0622; Revision: 7; Updated: Jun-24; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
IT equipment authenticates to other networks accessed via gateways.

Border Gateway Protocol route security

Resource Public Key Infrastructure (RPKI) uses asymmetric cryptography to authenticate routing data on the internet. This allows an organisation, particularly a telecommunications carrier or cloud service provider, to verify routing data they receive, transmit and process in order to determine routing calculations for internet traffic. By using RPKI, an organisation may reduce Border Gateway Protocol-related cyber threats, such as some types of denial-of-service attacks, accidental or deliberate rerouting of internet traffic, and opportunities for the undermining of IP address-based reputational services. RPKI Route Origin Authorization (ROA) records, which describe routes in terms of network/prefix and Autonomous Systems from which they are expected to originate, should be configured for the public IP addresses controlled by, or used by, an organisation. ROA records should also be configured for the unannounced IP address space controlled by an organisation.

Control: ISM-1783; Revision: 0; Updated: Jun-22; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
Public IP addresses controlled by, or used by, an organisation are signed by valid ROA records.

Gateway event logging

Centrally logging and analysing security-relevant events for gateways can assist in monitoring the security posture of gateways, detecting malicious behaviour and contributing to investigations following cyber security incidents.

Control: ISM-0634; Revision: 11; Updated: Sep-24; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
Security-relevant events for gateways are centrally logged, including:

- *data packets and data flows permitted through gateways*
- *data packets and data flows attempting to leave gateways*
- *real-time alerts for attempted intrusions.*

Assessment of gateways

Testing of gateways following configuration changes, and at regular intervals no more than six months apart, assists with validating that gateways conform to expected security configurations. In addition, gateways will need to undergo regular security assessments by an Infosec Registered Assessor Program (IRAP) assessor to determine their security

posture and security risks associated with their use. Following an initial security assessment by an IRAP assessor, subsequent security assessments should focus on any new services that are being offered as well as any security-related changes that have occurred since the previous security assessment.

Control: ISM-1037; Revision: 6; Updated: Jun-22; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
Gateways undergo testing following configuration changes, and at regular intervals no more than six months apart, to validate they conform to expected security configurations.

Control: ISM-0100; Revision: 11; Updated: Jun-22; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
Gateways undergo a security assessment by an IRAP assessor at least every 24 months.

Further information

Further information on cyber supply chain risk management can be found in the cyber supply chain risk management section of the *Guidelines for Procurement and Outsourcing*.

Further information on the procurement of outsourced services can be found in the managed services and cloud services section of the *Guidelines for Procurement and Outsourcing*.

Further information on designing, configuring and managing networks can be found in the network design and configuration section of the *Guidelines for Networking*.

Further information on privileged access to systems can be found in the access to systems and their resources section of the *Guidelines for Personnel Security*.

Further information on cyber security awareness training can be found in the cyber security awareness training section of the *Guidelines for Personnel Security*.

Further information on authenticating users can be found in the authentication hardening section of the *Guidelines for System Hardening*.

Further information on authenticating IT equipment can be found in the network design and configuration section of the *Guidelines for Networking*.

Further information on RPKI and ROA records is available from the Asia Pacific Network Information Centre.

Further information on event logging can be found in the event logging and monitoring section of the *Guidelines for System Monitoring*.

Further information on the purpose of IRAP, and a list of current IRAP assessors, is available from ASD.

Cross Domain Solutions

Introduction to Cross Domain Solutions

A Cross Domain Solution (CDS) is a system comprised of security-enforcing functions tailored to mitigate specific security risks associated with accessing or transferring data between different security domains. CDSs may be an integrated appliance or, more commonly, be composed of discrete technologies or sub-systems, with each sub-system consisting of hardware or software components.

This section describes the controls applicable to CDSs and extends upon the prior gateways section. Additional sections of these guidelines should also be consulted depending on the types of CDSs being deployed.

Personnel involved in the planning, design, implementation or assessment of CDSs should also refer to ASD's *Introduction to Cross Domain Solutions* and *Fundamentals of Cross Domain Solutions* publications.

Types of Cross Domain Solutions

This section defines two types of CDSs, Transfer CDSs and Access CDSs. These definitions are closely aligned with how CDSs are described and sold by vendors. Note, however, vendors may also offer combined Access and Transfer CDSs.

In defining the functionality of different types of CDSs, Transfer CDSs facilitate the transfer of data in one direction (unidirectional) or multiple directions (bi-directional) between different security domains. In comparison, Access CDSs provide users with access to multiple security domains from a single device. However, while Access CDSs allow interaction with different security domains, they do not allow users to move data between the different security domains.

Implementing Cross Domain Solutions

As there are significant security risks associated with connecting SECRET or TOP SECRET networks to other networks in different security domains, CDSs will need to be implemented.

Control: ISM-0626; Revision: 6; Updated: Mar-22; Applicability: S, TS; Essential Eight: N/A
CDSs are implemented between SECRET or TOP SECRET networks and any other networks belonging to different security domains.

Consultation on Cross Domain Solutions

As CDSs can be complex to implement and manage securely, it is critical that when an organisation is planning, designing, implementing or introducing additional connectivity to CDSs that ASD is consulted and any directions provided by ASD are complied with.

Control: ISM-0597; Revision: 8; Updated: Sep-23; Applicability: S, TS; Essential Eight: N/A
When planning, designing, implementing or introducing additional connectivity to CDSs, ASD is consulted and any directions provided by ASD are complied with.

Separation of data flows

To ensure that data flows are appropriately controlled within CDSs, it is important that isolated upward and downward network paths are implemented. This, in turn, should be supported by independent security-enforcing functions and protocol breaks at each network layer.

Control: ISM-0635; Revision: 7; Updated: Mar-22; Applicability: S, TS; Essential Eight: N/A
CDSs implement isolated upward and downward network paths.

Control: ISM-1522; Revision: 3; Updated: Mar-22; Applicability: S, TS; Essential Eight: N/A
CDSs implement independent security-enforcing functions for upward and downward network paths.

Control: ISM-1521; Revision: 3; Updated: Mar-22; Applicability: S, TS; Essential Eight: N/A
CDSs implement protocol breaks at each network layer.

Cross Domain Solution event logging

CDSs should have comprehensive event logging capabilities to ensure accountability of users for all activities they undertake. Furthermore, effective event logging and monitoring practices can increase the likelihood that operational failures will be detected.

In addition, centrally logging and analysing security-relevant events for CDSs can assist in monitoring the security posture of CDSs, detecting malicious behaviour and contributing to investigations following cyber security incidents.

Control: ISM-0670; Revision: 7; Updated: Sep-24; Applicability: S, TS; Essential Eight: N/A
Security-relevant events for CDSs are centrally logged.

Control: ISM-1523; Revision: 1; Updated: Mar-22; Applicability: S, TS; Essential Eight: N/A
A sample of security-relevant events relating to data transfer policies are taken at least every three months and assessed against security policies for CDSs to identify any operational failures.

User training

To assist in preventing cyber security incidents, it is important that users know how to use CDSs securely. This can be achieved by training users on the secure use of CDSs before access is granted.

Control: ISM-0610; Revision: 8; Updated: Mar-22; Applicability: S, TS; Essential Eight: N/A
Users are trained on the secure use of CDSs before access is granted.

Further information

Further information on cyber supply chain risk management can be found in the cyber supply chain risk management section of the *Guidelines for Procurement and Outsourcing*.

Further information on evaluated products can be found in the evaluated product procurement section of the *Guidelines for Evaluated Products*.

Further information on designing, configuring and managing networks can be found in the network design and configuration section of the *Guidelines for Networking*.

Further information on event logging can be found in the event logging and monitoring section of the *Guidelines for System Monitoring*.

Further information on cyber security awareness training can be found in the cyber security awareness training section of the *Guidelines for Personnel Security*.

Firewalls

Using firewalls

When implementing gateways between an organisation's networks and public network infrastructure, an organisation should implement firewalls to protect themselves from intrusions that may originate from the public network infrastructure. In addition, when an organisation's networks connect to another organisation's networks, both organisations should implement independent firewalls to protect themselves from intrusions that may originate from each other's networks. Note, this requirement may not be necessary in cases where shared network infrastructure is used only as a transport medium and encryption is applied to all network traffic.

Control: ISM-1528; Revision: 3; Updated: Mar-22; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
Evaluated firewalls are used between an organisation's networks and public network infrastructure.

Control: ISM-0639; Revision: 9; Updated: Mar-22; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
Evaluated firewalls are used between networks belonging to different security domains.

Further information

Further information on cyber supply chain risk management can be found in the cyber supply chain risk management section of the *Guidelines for Procurement and Outsourcing*.

Further information on evaluated products can be found in the evaluated product procurement section of the *Guidelines for Evaluated Products*.

Diodes

Using diodes

Diodes enforce one-way data flows, thereby, making it more difficult for malicious actors to use the same network path to launch an intrusion and exfiltrate data afterwards. As such, diodes should be used for controlling the data flow of unidirectional gateways.

Control: ISM-0643; Revision: 7; Updated: Mar-22; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
Evaluated diodes are used for controlling the data flow of unidirectional gateways between an organisation's networks and public network infrastructure.

Control: ISM-0645; Revision: 7; Updated: Mar-22; Applicability: S, TS; Essential Eight: N/A
Evaluated diodes used for controlling the data flow of unidirectional gateways between SECRET or TOP SECRET networks and public network infrastructure complete a high assurance evaluation.

Control: ISM-1157; Revision: 5; Updated: Mar-22; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
Evaluated diodes are used for controlling the data flow of unidirectional gateways between networks.

Control: ISM-1158; Revision: 6; Updated: Mar-22; Applicability: S, TS; Essential Eight: N/A
Evaluated diodes used for controlling the data flow of unidirectional gateways between SECRET or TOP SECRET networks and any other networks complete a high assurance evaluation.

Further information

Further information on cyber supply chain risk management can be found in the cyber supply chain risk management section of the *Guidelines for Procurement and Outsourcing*.

Further information on evaluated products can be found in the evaluated product procurement section of the *Guidelines for Evaluated Products*.

Web proxies

Web usage policy

As there are many security risks associated with the use of web services, it is important that an organisation develops, implements and maintains a web usage policy governing its use.

Control: ISM-0258; Revision: 4; Updated: Dec-22; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
A web usage policy is developed, implemented and maintained.

Using web proxies

Web proxies are a key component in enforcing web usage policies and preventing cyber security incidents.

Control: ISM-0260; Revision: 3; Updated: Mar-22; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
All web access, including that by internal servers, is conducted through web proxies.

Web proxy event logging

Centrally logging and analysing web proxy events can assist in monitoring the security posture of networks, detecting malicious behaviour and contributing to investigations following cyber security incidents.

Control: ISM-0261; Revision: 6; Updated: Dec-23; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
The following details are centrally logged for websites accessed via web proxies:

- *web address*
- *date and time*
- *user*
- *amount of data uploaded and downloaded*
- *internal and external IP addresses.*

Further information

Further information on cyber supply chain risk management can be found in the cyber supply chain risk management section of the *Guidelines for Procurement and Outsourcing*.

Further information on event logging can be found in the event logging and monitoring section of the *Guidelines for System Monitoring*.

Web content filters

Using web content filters

Effective web content filters can greatly reduce the likelihood of malicious code, or other inappropriate content, being accessed by users. Furthermore, web content filters can disrupt or prevent malicious actors from communicating with their malicious code if they manage to deploy it on an organisation's networks.

Control: ISM-0963; Revision: 7; Updated: Dec-22; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
Web content filtering is implemented to filter potentially harmful web-based content.

Control: ISM-0961; Revision: 8; Updated: Mar-22; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
Client-side active content is restricted by web content filters to an organisation-approved list of domain names.

Control: ISM-1237; Revision: 2; Updated: Mar-22; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
Web content filtering is applied to outbound web traffic where appropriate.

Transport Layer Security filtering

As encrypted Hypertext Transfer Protocol Secure connections can bypass traditional web content filtering techniques, an organisation should implement Transport Layer Security (TLS) inspection. Note, an organisation may choose to allow some web traffic, such as that for internet banking, to go uninspected to protect the privacy of users.

Control: ISM-0263; Revision: 8; Updated: Mar-22; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
TLS traffic communicated through gateways is decrypted and inspected.

Allowing and blocking access to domain names

Defining an organisation-approved list of domain names, and blocking all others, removes one of the most common data exfiltration paths used by malicious actors. In doing so, even a relatively permissive list of allowed domain names, such as the entire Australian top-level domain ('*.au') or the top 1,000 websites from the Alexa website ranking, offers better security than relying solely on a list of malicious domain names.

Furthermore, in cases where an organisation chooses to implement a relatively permissive list of allowed domain names, or list of website categories, security risks can be further mitigated by blocking dynamic domain names, or domain names that can be registered anonymously for free, as these are often used by malicious actors due to their lack of attribution. Finally, as users rarely have a requirement to access websites via their IP addresses instead of their domain names, the presence of such activities could indicate malicious code attempting to communicate with malicious actors' command and control infrastructure and should be blocked.

Control: ISM-0958; Revision: 8; Updated: Mar-22; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
An organisation-approved list of domain names, or list of website categories, is implemented for all Hypertext Transfer Protocol and Hypertext Transfer Protocol Secure traffic communicated through gateways.

Control: ISM-1236; Revision: 2; Updated: Mar-22; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
Malicious domain names, dynamic domain names and domain names that can be registered anonymously for free are blocked by web content filters.

Control: ISM-1171; Revision: 2; Updated: Mar-22; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
Attempts to access websites through their IP addresses instead of their domain names are blocked by web content filters.

Further information

Further information on cyber supply chain risk management can be found in the cyber supply chain risk management section of the *Guidelines for Procurement and Outsourcing*.

Further information on content filtering techniques can be found in the content filtering section of these guidelines.

Further information and examples of client-side JavaScript controls are available from the NoScript project.

Content filtering

Content filtering techniques

The following content filtering techniques should be considered as part of an organisation's content filtering implementation for gateways and CDSs:

- **Antivirus scans:** Scans files for viruses and other malicious code.
- **Automated dynamic analysis:** Analyses executable files run in a sandbox to detect suspicious behaviour.
- **File extension checks:** Checks file extensions to determine purported file types.
- **File format checks:** Checks files conform to defined file format specifications.

- **File type checks:** Checks file headers to determine actual file types.
- **Keyword checks:** Checks files for keywords that could indicate undesirable content.
- **Metadata checks:** Checks files for metadata that should be removed.
- **Protective marking checks:** Checks files for protective markings that may indicate undesirable content.
- **Manual inspections:** Involves the manual inspection of files for suspicious or undesirable content that an automated system may miss, which is particularly important for multimedia and content rich files.

Performing content filtering

Content filters perform an important function within gateways and CDSs by reducing the likelihood of unauthorised content or malicious code from entering or exiting networks. In performing content filtering checks, some content will be readily identifiable as malicious, or cannot be inspected, while other content, such as active content, may be deemed suspicious depending on what is considered normal behaviour for content passing through gateways and CDSs within an organisation. Finally, when content filters are used by CDSs, their assurance requirements necessitate rigorous security testing to ensure they perform as expected and cannot be bypassed.

Control: ISM-0659; Revision: 6; Updated: Mar-22; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
Files imported or exported via gateways or CDSs undergo content filtering checks.

Control: ISM-0651; Revision: 5; Updated: Mar-22; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
Files identified by content filtering checks as malicious, or that cannot be inspected, are blocked.

Control: ISM-0652; Revision: 3; Updated: Mar-22; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
Files identified by content filtering checks as suspicious are quarantined until reviewed and subsequently approved or not approved for release.

Control: ISM-1524; Revision: 2; Updated: Mar-22; Applicability: S, TS; Essential Eight: N/A
Content filters used by CDSs undergo rigorous security testing to ensure they perform as expected and cannot be bypassed.

Encrypted files

As encryption can be used to bypass content filtering checks, this poses a security risk in that malicious code could enter networks, or data could be exfiltrated from networks, undetected. In addition, encrypted files could mask data at a higher classification than that authorised to pass through gateways or CDSs, which could result in a data spill. As such, encrypted files should be decrypted in order to undergo content filtering checks.

Note, where a requirement to preserve the confidentiality of encrypted files exists, an organisation may consider a dedicated system to allow encrypted files to be decrypted in an appropriately secure environment before being subjected to all applicable content filtering checks.

Control: ISM-1293; Revision: 2; Updated: Mar-22; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
Encrypted files imported or exported via gateways or CDSs are decrypted in order to undergo content filtering checks.

Archive files

Archive files can be used to bypass content filtering checks if content filters do not handle such files correctly. Ensuring content filters recognise archive files will ensure the embedded files they contain are subject to the same content filtering checks as un-archived files.

Archive files can be constructed in a manner which can result in a denial of service to content filters due to processor, memory or disk space exhaustion. To limit the likelihood of such situations, content filters can specify resource constraints while unpacking archive files. If these constraints are exceeded, content filtering checks should be terminated.

Control: ISM-1289; Revision: 2; Updated: Mar-22; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
Archive files imported or exported via gateways or CDSs are unpacked in order to undergo content filtering checks.

Control: ISM-1290; Revision: 2; Updated: Mar-22; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
Archive files are unpacked in a controlled manner to ensure content filter performance or availability is not adversely affected.

Antivirus scanning

Antivirus scanning can be used to detect malicious files. In doing so, multiple different scanning engines should be used to increase the likelihood of identifying any malicious files.

Control: ISM-1288; Revision: 2; Updated: Mar-22; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
Files imported or exported via gateways or CDSs undergo antivirus scanning using multiple different scanning engines.

Automated dynamic analysis

Analysing executable files in a sandbox can be an effective method to detect suspicious behaviour upon file execution, such as network traffic, creation or modification of files, or system configuration changes.

Control: ISM-1389; Revision: 2; Updated: Mar-22; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
Executable files imported via gateways or CDSs are automatically executed in a sandbox to detect any suspicious behaviour.

Allowing specific content types

Creating and enforcing an organisation-approved list of allowed file types, can reduce the attack surface of networks. For example, a content filter in an email gateway might only allow Microsoft Office files and Portable Document Format (PDF) files.

Control: ISM-0649; Revision: 8; Updated: Mar-22; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
Files imported or exported via gateways or CDSs are filtered for allowed file types.

Content validation

Content validation, such as file format checks, aims to ensure that files conform to defined file format specifications. In performing content validation, any malformed content may indicate the presence of unauthorised content or malicious code, such as that designed to exploit known vulnerabilities in operating systems or applications.

Control: ISM-1284; Revision: 3; Updated: Mar-22; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
Files imported or exported via gateways or CDSs undergo content validation.

Content checking

Content checking, such as keyword checks, metadata checks and protective marking checks, aims to ensure that files do not contain any content that could cause a data spill or facilitate unauthorised export of data from systems.

Control: ISM-1965; Revision: 0; Updated: Sep-24; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
Files imported or exported via gateways or CDSs undergo content checking.

Content conversion

Content conversion can be an effective method to render malicious code harmless by converting one file type to another file type. Note, however, some file types will not benefit from content conversion. Examples of content conversion include:

- converting Microsoft Word documents to PDF files
- converting Microsoft PowerPoint presentations to image files
- converting Microsoft Excel spreadsheets to comma-separated values files
- converting PDF documents to plain text files.

Control: ISM-1286; Revision: 2; Updated: Mar-22; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
Files imported or exported via gateways or CDSs undergo content conversion.

Content sanitisation

Content sanitisation is the process of rendering files safe by removing or altering active content while leaving the original content as intact as possible, such as by removing macros from Microsoft Office files or removing JavaScript sections from PDF files.

Control: ISM-1287; Revision: 2; Updated: Mar-22; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
Files imported or exported via gateways or CDSs undergo content sanitisation.

Validating file integrity

If files passing through gateways or CDSs contain a form of integrity protection, such as a digital signature or cryptographic checksum, content filters should verify their integrity. In doing so, the failure of any integrity checks may indicate that files have been tampered with.

Control: ISM-0677; Revision: 7; Updated: Mar-23; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
Files imported or exported via gateways or CDSs that have a digital signature or cryptographic checksum are validated.

Further information

Further information on cyber supply chain risk management can be found in the cyber supply chain risk management section of the *Guidelines for Procurement and Outsourcing*.

Further information on performing data transfers can be found in the data transfers section of the *Guidelines for Data Transfers*.

Peripheral switches

Using peripheral switches

When accessing different systems through peripheral switches, it is important that sufficient assurance is obtained in their operation to ensure that data does not pass between connected systems. As such, the level of assurance needed

in peripheral switches is determined by the difference in sensitivity or classification of systems they are connected to. Note, there is no requirement for evaluated peripheral switches to be used when all connected systems belong to the same security domain.

Control: ISM-0591; Revision: 8; Updated: Mar-22; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
Evaluated peripheral switches are used when sharing peripherals between systems.

Control: ISM-1457; Revision: 4; Updated: Mar-22; Applicability: S, TS; Essential Eight: N/A
Evaluated peripheral switches used for sharing peripherals between SECRET and TOP SECRET systems, or between SECRET or TOP SECRET systems belonging to different security domains, preferably complete a high assurance evaluation.

Control: ISM-1480; Revision: 2; Updated: Mar-22; Applicability: S, TS; Essential Eight: N/A
Evaluated peripheral switches used for sharing peripherals between SECRET or TOP SECRET systems and any non-SECRET or TOP SECRET systems complete a high assurance evaluation.

Further information

Further information on cyber supply chain risk management can be found in the cyber supply chain risk management section of the *Guidelines for Procurement and Outsourcing*.

Further information on evaluated products can be found in the evaluated product procurement section of the *Guidelines for Evaluated Products*.

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