Australian Government
Australian Signals Directorate

Australian Cyber Security Centre

Information Security Manual

Published: 10 March 2022

cyber.gov.au

Table of Contents

Using the Information Security Manual

Executive summary

Purpose

The purpose of the *Information Security Manual* (ISM) is to outline a cyber security framework that an organisation can apply, using their risk management framework, to protect their systems and data from cyber threats.

Intended audience

The ISM is intended for Chief Information Security Officers (CISOs), Chief Information Officers, cyber security professionals and information technology managers.

Authority

The ISM represents the considered advice of the Australian Cyber Security Centre (ACSC) within the Australian Signals Directorate (ASD). This advice is provided in accordance with ASD's designated functions under section 7(1)(ca) of the *Intelligence Services Act 2001*.

The ACSC also provides cyber security advice in the form of Australian Communications Security Instructions and other cyber security-related publications. In these cases, device and application-specific advice may take precedence over the advice in the ISM.

Legislation and legal considerations

An organisation is not required as a matter of law to comply with the ISM, unless legislation, or a direction given under legislation or by some other lawful authority, compels them to comply. Furthermore, the ISM does not override any obligations imposed by legislation or law. Finally, if the ISM conflicts with legislation or law, the latter takes precedence.

While the ISM contains examples of when legislation or laws may be relevant for an organisation, there is no comprehensive consideration of such issues. When designing, operating and decommissioning systems, an organisation is encouraged to familiarise themselves with relevant legislation, such as the *Archives Act 1983*, *Privacy Act 1988* and *Telecommunications (Interception and Access) Act 1979*.

Cyber security principles

The purpose of the cyber security principles within the ISM is to provide strategic guidance on how an organisation can protect their systems and data from cyber threats. These cyber security principles are grouped into four key activities: govern, protect, detect and respond. An organisation should be able to demonstrate that the cyber security principles are being adhered to within their organisation.

Cyber security guidelines

The purpose of the cyber security guidelines within the ISM is to provide practical guidance on how an organisation can protect their systems and data from cyber threats. These cyber security guidelines cover governance, physical security, personnel security, and information and communications technology security topics. An organisation should consider the cyber security guidelines that are relevant to each of the systems they operate.

Applying a risk-based approach to cyber security

Using a risk management framework

The risk management framework used by the ISM draws from National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37 Rev. 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*. Broadly, the risk management framework used by the ISM has six steps: define the system, select security controls, implement security controls, assess security controls, authorise the system and monitor the system.

Define the system

Determine the type, value and security objectives for the system based on an assessment of the impact if it were to be compromised.

When embarking upon the design of a system, the type, value and security objectives for the system, based on confidentiality, integrity and availability requirements, should be determined. This will ultimately guide activities, such as selecting and tailoring security controls, to meet those security objectives and determine the level of residual security risk that will be accepted before the system is authorised to operate.

Following the determination of the type and value of a system, along with its security objectives, a description of the system and its characteristics should be documented in the system's system security plan.

Select security controls

Select security controls for the system and tailor them to achieve desired security objectives.

Each cyber security guideline discusses security risks associated with the topics it covers. Paired with these discussions are security controls that the ACSC considers to provide efficient and effective mitigations based on their suitability to achieve the security objectives for a system.

While security risks and security controls are discussed in the cyber security guidelines, and act as a baseline, they should not be considered an exhaustive list for a specific system type or technology. As such, the cyber security guidelines provide an important input into an organisation's risk identification and risk treatment activities however do not represent the full extent of such activities.

While the cyber security guidelines can assist with risk identification and risk treatment activities, an organisation will still need to undertake their own risk analysis and risk evaluation activities due to the unique nature of each system, its operating environment and the organisation's risk tolerances.

Following the selection and tailoring of security controls for a system, they should be recorded along with the details of their planned implementation in the system's system security plan annex. In addition, and as appropriate, security controls should also be recorded in both the system's incident response plan and continuous monitoring plan.

Finally, the selection of security controls for a system, as documented in the system's system security plan annex, should be approved by the system's authorising officer.

Implement security controls

Implement security controls for the system and its operating environment.

Once suitable security controls have been identified for a system, and approved by its authorising officer, they should be implemented. In doing so, the details of their actual implementation, if different from their planned implementation, should be documented in the system's system security plan annex.

Assess security controls

Assess security controls for the system and its operating environment to determine if they have been implemented correctly and are operating as intended.

In conducting a security assessment, it is important that assessors and system owners first agree to the scope, type and extent of assessment activities, which may be documented in a security assessment plan, such that any risks associated with the security assessment can be appropriately managed. To a large extent, the scope of the security assessment will be determined by the type of system and security controls that have been implemented for the system and its operating environment.

For TOP SECRET systems, including sensitive compartmented information systems, security assessments can be undertaken by ASD assessors (or their delegates). While for SECRET and below systems, security assessments can be undertaken by an organisation’s own assessors or Infosec Registered Assessors Program (IRAP) assessors. In all cases, assessors should hold an appropriate security clearance and have an appropriate level of experience and understanding of the type of system they are assessing.

At the conclusion of a security assessment, a security assessment report should be produced outlining the scope of the security assessment, the system’s strengths and weaknesses, security risks associated with the operation of the system, the effectiveness of the implementation of security controls, and any recommended remediation actions. This will assist in performing any initial remediation actions as well as guiding the development of the system’s plan of action and milestones.

Authorise the system

Authorise the system to operate based on the acceptance of the security risks associated with its operation.

Before a system can be granted authorisation to operate, sufficient information should be provided to the authorising officer in order for them to make an informed risk-based decision as to whether the security risks associated with its operation are acceptable or not. This information should take the form of an authorisation package that includes the system’s system security plan, incident response plan, continuous monitoring plan, security assessment report, and plan of action and milestones.

In some cases, the security risks associated with a system’s operation will be acceptable and it will be granted authorisation to operate. However, in other cases the security risks associated with operation of a system may be unacceptable. In such cases, the authorising officer may request further work, and potentially another security assessment, be undertaken by the system owner. In the intervening time, the authorising officer may choose to grant authorisation to operate but with constraints placed on the system’s use. Finally, if the authorising officer deems the security risks to be unacceptable regardless of any potential constraints on the system’s use, they may deny authorisation to operate until such time that sufficient remediation actions, if possible, have been completed to an acceptable standard.

For TOP SECRET systems, and systems that process, store or communicate sensitive compartmented information, the authorising officer is Director-General ASD or their delegate; while for SECRET and below systems, the authorising officer is an organisation’s CISO or their delegate.

For multinational and multi-organisation systems, the authorising officer should be determined by a formal agreement between the parties involved.

For commercial providers providing services to an organisation, the authorising officer is the CISO of the supported organisation or their delegate.

In all cases, the authorising officer should have an appropriate level of seniority and understanding of security risks they are accepting on behalf of their organisation. In cases where an organisation does not have a CISO, the authorising officer could be a Chief Security Officer, a Chief Information Officer or other senior executive within the organisation.

Monitor the system

Monitor the system, and associated cyber threats, security risks and security controls, on an ongoing basis.

Regular monitoring of cyber threats, security risks and security controls associated with a system and its operating environment, as outlined in a continuous monitoring plan, is essential to maintaining its security posture. In doing so, specific events may necessitate additional risk management activities. Such events may include:

- changes in security policies relating to the system
- detection of new or emerging cyber threats to the system or its operating environment
- the discovery that security controls for the system are not as effective as planned
- a major cyber security incident involving the system
- major architectural changes to the system.

Following the implementation or modification of any security controls as a result of risk management activities, another security assessment should be completed. In doing so, the system's authorisation package should be updated. This in turn allows the authorising officer to make an informed risk-based decision as to whether the security risks associated with the system's operation are still acceptable, and whether to grant ongoing authorisation to operate.

Further information

Further information on various risk management frameworks and practices can be found in:

- International Organization for Standardization (ISO) 31000:2018, *Risk management – Guidelines*
- ISO Guide 73:2009, *Risk management – Vocabulary*
- International Electrotechnical Commission 31010:2019, *Risk management – Risk assessment techniques*
- ISO/International Electrotechnical Commission 27005:2018, *Information technology – Security techniques – Information security risk management*
- NIST SP 800-30 Rev. 1, *Guide for Conducting Risk Assessments*
- NIST SP 800-37 Rev. 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*.

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

Cyber Security Principles

The cyber security principles

Purpose of the cyber security principles

The purpose of the cyber security principles is to provide strategic guidance on how an organisation can protect their systems and data from cyber threats. These cyber security principles are grouped into four key activities: govern, protect, detect and respond.

- **Govern:** Identifying and managing security risks.
- **Protect:** Implementing security controls to reduce security risks.
- **Detect:** Detecting and understanding cyber security events to identify cyber security incidents.
- **Respond:** Responding to and recovering from cyber security incidents.

Govern principles

- **G1:** A Chief Information Security Officer provides leadership and oversight of cyber security.
- **G2:** The identity and value of systems, applications and data is determined and documented.
- **G3:** The confidentiality, integrity and availability requirements for systems, applications and data are determined and documented.
- **G4:** Security risk management processes are embedded into organisational risk management frameworks.
- **G5:** Security risks are identified, documented, managed and accepted both before systems and applications are authorised for use, and continuously throughout their operational life.

Protect principles

- **P1:** Systems and applications are designed, deployed, maintained and decommissioned according to their value and their confidentiality, integrity and availability requirements.
- **P2:** Systems and applications are delivered and supported by trusted suppliers.
- **P3:** Systems and applications are configured to reduce their attack surface.
- **P4:** Systems and applications are administered in a secure and accountable manner.
- **P5:** Security vulnerabilities in systems and applications are identified and mitigated in a timely manner.
- **P6:** Only trusted and supported operating systems, applications and computer code can execute on systems.
- **P7:** Data is encrypted at rest and in transit between different systems.
- **P8:** Data communicated between different systems is controlled and inspectable.
- **P9:** Data, applications and configuration settings are backed up in a secure and proven manner on a regular basis.
- **P10:** Only trusted and vetted personnel are granted access to systems, applications and data repositories.
- **P11:** Personnel are granted the minimum access to systems, applications and data repositories required for their duties.

- **P12:** Multiple methods are used to identify and authenticate personnel to systems, applications and data repositories.
- **P13:** Personnel are provided with ongoing cyber security awareness training.
- **P14:** Physical access to systems, supporting infrastructure and facilities is restricted to authorised personnel.

Detect principles

- **D1:** Event logs are collected and analysed in a timely manner to detect cyber security events.
- **D2:** Cyber security events are analysed in a timely manner to identify cyber security incidents.

Respond principles

- **R1:** Cyber security incidents are reported both internally and externally to relevant bodies in a timely manner.
- **R2:** Cyber security incidents are contained, eradicated and recovered from in a timely manner.
- **R3:** Business continuity and disaster recovery plans are enacted when required.

Maturity modelling

When implementing the cyber security principles, an organisation can use the following maturity model to assess the implementation of individual principles, groups of principles or the cyber security principles as a whole. The five levels in the maturity model are:

- **Incomplete:** The cyber security principles are partially implemented or not implemented.
- **Initial:** The cyber security principles are implemented, but in a poor or ad hoc manner.
- **Developing:** The cyber security principles are sufficiently implemented, but on a project-by-project basis.
- **Managing:** The cyber security principles are established as standard business practices and robustly implemented throughout the organisation.
- **Optimising:** A deliberate focus on optimisation and continual improvement exists for the implementation of the cyber security principles throughout the organisation.

Guidelines for Cyber Security Roles

Chief Information Security Officer

Required skills and experience

The role of the Chief Information Security Officer (CISO) requires a combination of technical and soft skills, such as business acumen, leadership, communications and relationship building. Additionally, a CISO must adopt a continuous approach to learning and up-skilling in order to maintain pace with the cyber threat landscape and new technologies. It is expected that a CISO show innovation and imagination in conceiving and delivering cyber security strategies for their organisation.

Providing cyber security leadership and guidance

To provide cyber security leadership and guidance within an organisation, it is important that the organisation appoints a CISO.

Security Control: ISM-0714; Revision: 5; Updated: Oct-20; Applicability: All; Essential Eight: N/A
A CISO is appointed to provide cyber security leadership and guidance for their organisation.

Overseeing the cyber security program

The CISO within an organisation is responsible for overseeing their organisation’s cyber security program and ensuring compliance with cyber security policy, standards, regulations and legislation. They are likely to work with a Chief Security Officer, a Chief Information Officer and other senior executives within their organisation.

Security Control: ISM-1478; Revision: 1; Updated: Oct-20; Applicability: All; Essential Eight: N/A
The CISO oversees their organisation’s cyber security program and ensures their organisation’s compliance with cyber security policy, standards, regulations and legislation.

Security Control: ISM-1617; Revision: 0; Updated: Oct-20; Applicability: All; Essential Eight: N/A
The CISO regularly reviews and updates their organisation’s cyber security program to ensure its relevance in addressing cyber threats and harnessing business and cyber security opportunities.

Security Control: ISM-0724; Revision: 2; Updated: Oct-20; Applicability: All; Essential Eight: N/A
The CISO implements cyber security measurement metrics and key performance indicators for their organisation.

Coordinating cyber security

The CISO is responsible for ensuring the alignment of cyber security and business objectives within their organisation. To achieve this, they should facilitate communication between cyber security and business stakeholders. This includes translating cyber security concepts and language into business concepts and language, as well as ensuring that business teams consult with cyber security teams to determine appropriate security controls when planning new business projects. Additionally, as the CISO is responsible for the development of their organisation’s cyber security program, they are best placed to advise projects on the strategic direction of cyber security within their organisation.

Security Control: ISM-0725; Revision: 3; Updated: Dec-21; Applicability: All; Essential Eight: N/A
The CISO coordinates cyber security and business alignment through a cyber security steering committee or advisory board, comprising of key cyber security and business executives, which meets formally and on a regular basis.

Security Control: ISM-0726; Revision: 2; Updated: Oct-20; Applicability: All; Essential Eight: N/A
The CISO coordinates security risk management activities between cyber security and business teams.

Reporting on cyber security

The CISO is responsible for reporting cyber security matters to their organisation’s senior executive or Board. Reporting should cover:

- the organisation’s security risk profile
- the status of key systems and any outstanding security risks
- any planned cyber security uplift activities
- any recent cyber security incidents
- expected returns on cyber security investments.

Reporting on cyber security matters should be structured by business functions, regions or legal entities and support a consolidated view of an organisation’s security risks.

It is important that the CISO is able to translate security risks into operational risks for their organisation, including financial and legal risks, in order to enable more holistic conversations about their organisation’s risks.

Security Control: ISM-0718; Revision: 3; Updated: Mar-22; Applicability: All; Essential Eight: N/A
The CISO reports directly to their organisation’s senior executive or Board on cyber security matters.

Overseeing incident response activities

To ensure the CISO is able to accurately report to their organisation’s senior executive or Board on cyber security matters, it is important they are fully aware of all cyber security incidents within their organisation.

The CISO is also responsible for overseeing their organisation’s response to cyber security incidents, including how internal teams respond and communicate with each other during an incident. In the event of a major cyber security incident, the CISO should be prepared to step into a crisis management role. They should understand how to bring clarity to the situation and communicate effectively with internal and external stakeholders.

Security Control: ISM-0733; Revision: 2; Updated: Oct-20; Applicability: All; Essential Eight: N/A
The CISO is fully aware of all cyber security incidents within their organisation.

Security Control: ISM-1618; Revision: 0; Updated: Oct-20; Applicability: All; Essential Eight: N/A
The CISO oversees their organisation’s response to cyber security incidents.

Contributing to business continuity and disaster recovery planning

The CISO is responsible for contributing to the development and maintenance of their organisation’s business continuity and disaster recovery plans, with the aim to improve business resilience and ensure the continued operation of critical business processes.

Security Control: ISM-0734; Revision: 3; Updated: Jun-21; Applicability: All; Essential Eight: N/A
The CISO contributes to the development and maintenance of business continuity and disaster recovery plans for their organisation to ensure that business-critical services are supported appropriately in the event of a disaster.

Developing a cyber security communications strategy

To facilitate cyber security cultural change across their organisation, the CISO should act as a thought leader by continually communicating their strategy and vision. A communication strategy can be helpful in achieving this. Communications should be tailored to different parts of their organisation and be topical for the intended audience.

Security Control: ISM-0720; Revision: 1; Updated: Oct-20; Applicability: All; Essential Eight: N/A
The CISO develops and maintains a cyber security communications strategy for their organisation.

Working with suppliers and service providers

The CISO is responsible for ensuring that consistent vendor management processes are applied across their organisation, from discovery through to ongoing management. As supplier and service provider relationships come with additional security risks, the CISO should assist personnel with assessing cyber supply chain risks and understand the security impacts of entering into contracts with suppliers and service providers.

Security Control: ISM-0731; Revision: 2; Updated: Oct-20; Applicability: All; Essential Eight: N/A
The CISO oversees cyber supply chain risk management activities for their organisation.

Receiving and managing a dedicated cyber security budget

Receiving and managing a dedicated cyber security budget will ensure the CISO has sufficient access to funding to support their cyber security program, including cyber security uplift activities and responding to cyber security incidents.

Security Control: ISM-0732; Revision: 2; Updated: Oct-20; Applicability: All; Essential Eight: N/A
The CISO receives and manages a dedicated cyber security budget for their organisation.

Overseeing cyber security personnel

The CISO is responsible for the cyber security workforce within their organisation, including plans to attract, train and retain cyber security personnel. The CISO should also delegate relevant tasks to cyber security managers and other personnel as required and provide them with adequate authority and resources to perform their duties.

Security Control: ISM-0717; Revision: 2; Updated: Oct-20; Applicability: All; Essential Eight: N/A
The CISO oversees the management of cyber security personnel within their organisation.

Overseeing cyber security awareness raising

To ensure personnel are actively contributing to the security culture of their organisation, a cyber security awareness training program should be developed. As the CISO is responsible for cyber security within their organisation, they should oversee the development and operation of the cyber security awareness training program.

Security Control: ISM-0735; Revision: 2; Updated: Oct-20; Applicability: All; Essential Eight: N/A
The CISO oversees the development and operation of their organisation's cyber security awareness training program.

System owners

System ownership and oversight

System owners are responsible for ensuring the secure operation of their systems. However, system owners may delegate the day-to-day management and operation of their systems to system managers.

Security Control: ISM-1071; Revision: 1; Updated: Sep-18; Applicability: All; Essential Eight: N/A
Each system has a designated system owner.

Security Control: ISM-1525; Revision: 1; Updated: Jan-21; Applicability: All; Essential Eight: N/A
System owners register each system with its authorising officer.

Protecting systems and their resources

Broadly, the risk management framework used by the *Information Security Manual* has six steps: define the system, select security controls, implement security controls, assess security controls, authorise the system and monitor the system. System owners are responsible for the implementation of this six step risk management framework for each of their systems.

Security Control: ISM-1633; Revision: 0; Updated: Jan-21; Applicability: All; Essential Eight: N/A
System owners determine the type, value and security objectives for each system based on an assessment of the impact if it were to be compromised.

Security Control: ISM-1634; Revision: 0; Updated: Jan-21; Applicability: All; Essential Eight: N/A
System owners select security controls for each system and tailor them to achieve desired security objectives.

Security Control: ISM-1635; Revision: 1; Updated: Dec-21; Applicability: All; Essential Eight: N/A
System owners implement security controls for each system and its operating environment.

Security Control: ISM-1636; Revision: 0; Updated: Jan-21; Applicability: All; Essential Eight: N/A
System owners ensure security controls for each system and its operating environment are assessed to determine if they have been implemented correctly and are operating as intended.

Security Control: ISM-0027; Revision: 4; Updated: Jan-21; Applicability: All; Essential Eight: N/A
System owners obtain authorisation to operate each system from its authorising officer based on the acceptance of the security risks associated with its operation.

Security Control: ISM-1526; Revision: 1; Updated: Jan-21; Applicability: All; Essential Eight: N/A
System owners monitor each system, and associated cyber threats, security risks and security controls, on an ongoing basis.

Annual reporting of system security status

Annual reporting by system owners on the security status of their systems to their authorising officer can assist the authorising officer in maintaining awareness of the security posture of systems within their organisation.

Security Control: ISM-1587; Revision: 0; Updated: Aug-20; Applicability: All; Essential Eight: N/A
System owners report the security status of each system to its authorising officer at least annually.

Further information

Further information on using the *Information Security Manual*'s six step risk management framework can be found in the applying a risk-based approach to cyber security section of *Using the Information Security Manual*.

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

Guidelines for Cyber Security Incidents

Detecting cyber security incidents

Cyber security events

A cyber security event is an occurrence of a system, service or network state indicating a possible breach of security policy, failure of safeguards or a previously unknown situation that may be relevant to security.

Cyber security incidents

A cyber security incident is an unwanted or unexpected cyber security event, or a series of such events, that have a significant probability of compromising business operations.

Cyber resilience

Cyber resilience is the ability to adapt to disruptions caused by cyber security incidents while maintaining continuous business operations. This includes the ability to detect, manage and recover from cyber security incidents.

Detecting cyber security incidents

One of the core elements of detecting and investigating cyber security incidents is the availability of appropriate data sources. Fortunately, many data sources can be extracted from existing systems without requiring specialised capabilities.

The following are some of the data sources that an organisation can use for detecting and investigating cyber security incidents:

- Domain Name System event logs: Can assist in identifying attempts to resolve malicious domains or Internet Protocol addresses which can indicate an exploitation attempt or successful compromise.
- Email server event logs: Can assist in identifying users targeted with spear-phishing emails. Can also assist in identifying the initial vector of a compromise.
- Gateway event logs: Can assist in identifying anomalous or malicious network traffic which can indicate an exploitation attempt or successful compromise.
- Operating system and application event logs: Can assist in identifying anomalous or malicious activity which can indicate an exploitation attempt or successful compromise.
- Remote access event logs: Can assist in identifying unusual source addresses, times of access and logon/logoff times associated with malicious activity.
- Web proxy event logs: Can assist in identifying Hypertext Transfer Protocol-based vectors and malicious network traffic.

Intrusion detection and prevention policy

Establishing an intrusion detection and prevention policy can increase the likelihood of detecting, and subsequently preventing, malicious activity on networks and hosts. In doing so, an intrusion detection and prevention policy will likely cover the following:

- methods of network-based intrusion detection and prevention used
- methods of host-based intrusion detection and prevention used

- guidelines for reporting and responding to detected intrusions
- resources assigned to intrusion detection and prevention activities.

Security Control: ISM-0576; Revision: 7; Updated: Aug-19; Applicability: All; Essential Eight: N/A
An intrusion detection and prevention policy is developed and implemented.

Trusted insider program

As a trusted insider's system access and knowledge of business processes often makes them harder to detect, establishing a trusted insider program can assist an organisation to detect and respond to trusted insider threats before they occur, or limit damage if they do occur. In doing so, an organisation will likely obtain the most benefit by logging and analysing the following user activities:

- excessive copying or modification of files
- unauthorised or excessive use of removable media
- connecting devices capable of data storage to systems
- unusual system usage outside of normal business hours
- excessive data access or printing compared to their peers
- data transfers to unauthorised cloud services or webmail
- use of unauthorised Virtual Private Networks, file transfer applications or anonymity networks.

Security Control: ISM-1625; Revision: 0; Updated: Nov-20; Applicability: All; Essential Eight: N/A
A trusted insider program is developed and implemented.

Security Control: ISM-1626; Revision: 0; Updated: Nov-20; Applicability: All; Essential Eight: N/A
Legal advice is sought regarding the development and implementation of a trusted insider program.

Access to sufficient data sources and tools

Successful detection of cyber security incidents requires trained cyber security personnel with access to sufficient data sources complemented by tools that support both manual and automated analysis. As such, it is important that during system design and development activities, functionality is added to systems to ensure that sufficient data sources can be captured and provided to cyber security personnel.

Security Control: ISM-0120; Revision: 5; Updated: May-20; Applicability: All; Essential Eight: N/A
Cyber security personnel have access to sufficient data sources and tools to ensure that systems can be monitored for key indicators of compromise.

Further information

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

Further information on establishing and operating a trusted insider program can be found in the Carnegie Mellon University’s Software Engineering Institute’s *Common Sense Guide to Mitigating Insider Threats* publication.

Managing cyber security incidents

Cyber security incident register

Recording cyber security incidents in a register can assist with ensuring that appropriate remediation activities are undertaken. In addition, the types and frequency of cyber security incidents, along with the costs of any remediation activities, can be used as an input to future risk assessment activities.

Security Control: ISM-0125; Revision: 5; Updated: Jun-21; Applicability: All; Essential Eight: N/A
A cyber security incident register is maintained that covers the following:

- *the date the cyber security incident occurred*
- *the date the cyber security incident was discovered*
- *a description of the cyber security incident*
- *any actions taken in response to the cyber security incident*
- *to whom the cyber security incident was reported.*

Handling and containing data spills

When a data spill occurs, an organisation should inform data owners and restrict access to the data. In doing so, affected systems can be powered off, have their network connectivity removed or have additional access controls applied to the data. It should be noted though that powering off systems could destroy data that would be useful for forensic investigations. Furthermore, users should be made aware of appropriate actions to take in the event of a data spill, such as not deleting, copying, printing or emailing the data.

Security Control: ISM-0133; Revision: 2; Updated: Jun-21; Applicability: All; Essential Eight: N/A
When a data spill occurs, data owners are advised and access to the data is restricted.

Handling and containing malicious code infections

Taking immediate remediation steps after the discovery of malicious code can minimise the time and cost spent eradicating and recovering from the infection. As a priority, all infected systems and media should be isolated to prevent the infection from spreading. Once isolated, infected systems and media can be scanned by antivirus software to potentially remove the infection or recover data. It is important to note though, a complete system restoration from a known good backup or rebuild may be the only reliable way to ensure that malicious code can be truly eradicated or data recovered.

Security Control: ISM-0917; Revision: 7; Updated: Oct-19; Applicability: All; Essential Eight: N/A
When malicious code is detected, the following steps are taken to handle the infection:

- *the infected systems are isolated*
- *all previously connected media used in the period leading up to the infection are scanned for signs of infection and isolated if necessary*
- *antivirus software is used to remove the infection from infected systems and media*
- *if the infection cannot be reliably removed, systems are restored from a known good backup or rebuilt.*

Handling and containing intrusions

When an intrusion is detected on a system, an organisation may wish to allow the intrusion to continue for a short period of time in order to fully understand the extent of the compromise and to assist with planning intrusion remediation activities. However, an organisation allowing an intrusion to continue in order to collect data or evidence should first establish with their legal advisors whether such activities would be breaching the *Telecommunications (Interception and Access) Act 1979*.

To increase the likelihood of intrusion remediation activities successfully removing an adversary from their system, an organisation can take preventative measures to ensure the adversary has limited forewarning and awareness of planned intrusion remediation activities. Specifically, using an alternative system to plan and coordinate intrusion remediation activities will prevent alerting the adversary if they have already compromised email, messaging or collaboration services. In addition, conducting intrusion remediation activities in a coordinated manner during the same planned outage will prevent forewarning the adversary, thereby depriving them of sufficient time to establish alternative access points or persistence methods on the system.

Following intrusion remediation activities, an organisation should determine whether the adversary has been successfully removed from the system, including whether or not they have since reacquired access. This can be achieved, in part, by capturing and analysing network traffic for at least seven days following remediation activities.

Security Control: ISM-0137; Revision: 4; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Legal advice is sought before allowing intrusion activity to continue on a system for the purpose of collecting further data or evidence.

Security Control: ISM-1609; Revision: 2; Updated: Dec-21; Applicability: All; Essential Eight: N/A
System owners are consulted before allowing intrusion activity to continue on a system for the purpose of collecting further data or evidence.

Security Control: ISM-1731; Revision: 0; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Planning and coordination of intrusion remediation activities are conducted on a separate system to that which has been compromised.

Security Control: ISM-1732; Revision: 0; Updated: Dec-21; Applicability: All; Essential Eight: N/A
To the extent possible, all intrusion remediation activities are conducted in a coordinated manner during the same planned outage.

Security Control: ISM-1213; Revision: 2; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Following intrusion remediation activities, full network traffic is captured for at least seven days and analysed to determine whether the adversary has been successfully removed from the system.

Integrity of evidence

When gathering evidence following a cyber security incident, it is important that its integrity is maintained. In addition, if the Australian Cyber Security Centre (ACSC) is requested to assist with investigations, no actions which could affect the integrity of evidence should be carried out before the ACSC becomes involved.

Security Control: ISM-0138; Revision: 4; Updated: Aug-20; Applicability: All; Essential Eight: N/A
The integrity of evidence gathered during an investigation is maintained by investigators:

- *recording all of their actions*
- *creating checksums for all evidence*
- *copying evidence onto media for archiving*
- *maintaining a proper chain of custody.*

Further information

Further information on incident response plans can be found in the system-specific security documentation section of the *Guidelines for Security Documentation*.

Further information on handling and managing data spills can be found in the ACSC's *Data Spill Management Guide* publication.

Reporting cyber security incidents

Reporting cyber security incidents

Reporting cyber security incidents, including unplanned outages, to an organisation's Chief Information Security Officer (CISO), or one of their delegates, as soon as possible after they occur or are discovered provides senior management with the opportunity to assess the impact to their organisation and to take remediation actions if necessary. Note, an organisation should also be cognisant of any legislative obligations in regards to reporting cyber security incidents to authorities, customers or the public.

Security Control: ISM-0123; Revision: 3; Updated: Sep-18; Applicability: All; Essential Eight: N/A
Cyber security incidents are reported to an organisation's CISO, or one of their delegates, as soon as possible after they occur or are discovered.

Security Control: ISM-0141; Revision: 5; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Service providers report cyber security incidents to their customer's CISO, or one of their delegates, as soon as possible after they occur or are discovered.

Security Control: ISM-1433; Revision: 3; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Service providers and their customers maintain 24/7 contact details for each other, including additional out-of-band contact details for when normal communication channels fail, in order to report cyber security incidents.

Reporting cyber security incidents to the ACSC

The ACSC uses the cyber security incident reports it receives as the basis for providing assistance to organisations. Cyber security incident reports are also used by the ACSC to identify trends and maintain an accurate threat environment picture. The ACSC utilises this understanding to assist in the development of new and updated cyber security advice, capabilities, and techniques to better prevent and respond to evolving cyber threats. An organisation is recommended to internally coordinate their reporting of cyber security incidents to the ACSC.

The types of cyber security incidents that should be reported to the ACSC include:

- suspicious activities, such as privileged account lockouts and unusual remote access activities
- compromise of sensitive or classified data
- unauthorised access or attempts to access a system
- emails with suspicious attachments or links
- denial-of-service attacks
- ransomware attacks
- suspected tampering of ICT equipment.

Security Control: ISM-0140; Revision: 6; Updated: May-19; Applicability: All; Essential Eight: N/A
Cyber security incidents are reported to the ACSC.

Further information

Further information on reporting cyber security incidents is available from the ACSC.

Guidelines for Outsourcing

Cyber supply chain risk management

Cyber supply chain risk management activities

Cyber supply chain risk management activities should be conducted during the earliest possible stage of procurement processes. In particular, an organisation should consider the security risks that may arise as systems, software and hardware are being designed, built, stored, delivered, installed, operated, maintained and decommissioned. This includes identifying and managing jurisdictional, governance, privacy and security risks associated with the use of suppliers and service providers. For example, outsourced cloud services may be located offshore and subject to lawful and covert data collection without their customers' knowledge. Additionally, use of offshore services introduces jurisdictional risks as foreign countries' laws could change with little warning. Finally, foreign owned service providers operating in Australia may be subject to a foreign government's lawful access to data belonging to their customers.

In managing cyber supply chain risks, it is important that an organisation preferences suppliers and service providers that have demonstrated a commitment to secure-by-design principles, secure programming practices and maintaining the security of their products. In addition, suppliers and service providers should have a strong track record of transparency and maintaining the security of their own systems and cyber supply chains. Also, in some cases, a shared responsibly model which clearly defines the responsibilities of suppliers, service providers and their customers can be highly beneficial.

Security Control: ISM-1631; Revision: 0; Updated: Dec-20; Applicability: All; Essential Eight: N/A
Components and services relevant to the security of systems are identified and understood.

Security Control: ISM-1452; Revision: 3; Updated: Dec-20; Applicability: All; Essential Eight: N/A
Before obtaining components and services relevant to the security of systems, a review of suppliers and service providers (including their country of origin) is performed to assess the potential increase to systems' security risk profile, including by identifying those that are high risk.

Security Control: ISM-1567; Revision: 1; Updated: Dec-20; Applicability: All; Essential Eight: N/A
Suppliers and service providers identified as high risk are not used.

Security Control: ISM-1568; Revision: 2; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Components and services relevant to the security of systems are chosen from suppliers and service providers that have made a commitment to secure-by-design principles, secure programming practices and maintaining the security of their products.

Security Control: ISM-1632; Revision: 1; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Components and services relevant to the security of systems are chosen from suppliers and service providers that have a strong track record of transparency and maintaining the security of their own systems and cyber supply chains.

Security Control: ISM-1569; Revision: 1; Updated: Dec-20; Applicability: All; Essential Eight: N/A
A shared responsibility model is created, documented and shared between suppliers, service providers and their customers in order to articulate the security responsibilities of each party.

Further information

Further information on cyber supply chain risk management can be found in the Australian Cyber Security Centre (ACSC)'s *Cyber Supply Chain Risk Management* and *Identifying Cyber Supply Chain Risks* publications.

Further information on supply chain integrity can be found in National Institute of Standards and Technology Special Publication 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*.

Further information on outsourced goods and services can be found in the Attorney-General's Department's *Protective Security Policy Framework*, *Security governance for contracted goods and service providers* policy.

Managed services and cloud services

Managed services

Managed service providers manage the services of an organisation on their behalf. This may include application services, authentication services, backup services, cloud services, desktop services, enterprise mobility services, gateway services, hosting services, network services, procurement services, security services, support services, and many other business-related services. In doing so, managed service providers may manage services from their customers' premises or their own premises. In considering security risks associated with managed services, an organisation should consider all managed service providers that have access to their facilities, systems or data.

Security Control: ISM-1736; Revision: 0; Updated: Mar-22; Applicability: All; Essential Eight: N/A
A managed service register is maintained and verified on a regular basis.

Security Control: ISM-1737; Revision: 0; Updated: Mar-22; Applicability: All; Essential Eight: N/A
A managed service register contains the following for each managed service:

- *managed service provider's name*
- *purpose for using the managed service*
- *sensitivity or classification of data involved*
- *point of contact for users of the managed service*
- *point of contact for the managed service provider.*

Outsourced cloud services

Outsourcing can be a cost-effective option for providing cloud services, as well as potentially delivering a superior service. However, outsourcing can affect an organisation's security risk profile. Ultimately, an organisation will still need to decide whether a particular outsourced cloud service represents an acceptable security risk and, if appropriate to do so, authorise it for their own use.

Cloud service providers and their cloud services 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, subsequent security assessments should focus on any new cloud services that are being offered as well as any security-related changes that have occurred since the previous security assessment.

Security Control: ISM-1637; Revision: 1; Updated: Mar-22; Applicability: All; Essential Eight: N/A
An outsourced cloud service register is maintained and verified on a regular basis.

Security Control: ISM-1638; Revision: 2; Updated: Mar-22; Applicability: All; Essential Eight: N/A
An outsourced cloud service register contains the following for each outsourced cloud service:

- *cloud service provider's name*
- *cloud service's name*
- *purpose for using the cloud service*
- *sensitivity or classification of data involved*
- *due date for the next security assessment of the cloud service*

- *point of contact for users of the cloud service*
- *point of contact for the cloud service provider.*

Security Control: ISM-1570; Revision: 0; Updated: Jul-20; Applicability: All; Essential Eight: N/A
Cloud service providers and their cloud services undergo a security assessment by an IRAP assessor at least every 24 months.

Security Control: ISM-1529; Revision: 2; Updated: Dec-21; Applicability: S, TS; Essential Eight: N/A
Only community or private clouds are used for outsourced SECRET and TOP SECRET cloud services.

Contractual security requirements

Obligations for protecting data are no different when using a managed service or cloud service than when using an in-house service. As such, contractual arrangements between service providers and their customers should address how security risks will be managed. However, in some cases an organisation may require managed services or cloud services to be used before all security requirements have been implemented by a service provider. In such cases, contractual arrangements should include appropriate timeframes for the implementation of security requirements and break clauses if these are not achieved.

In addition, although data ownership resides with service providers' customers, this can become less clear in some circumstances, such as when legal action is taken and a service provider is asked to provide access to, or data from, their assets. To mitigate the likelihood of data being unavailable or compromised, an organisation can document the types of data and its ownership through contractual arrangements.

Furthermore, an organisation may make the decision to move from their current service provider for strategic, operational or governance reasons. This may involve changing to another service provider, moving to a different service with the same service provider or moving back to an on-premises solution. In many cases, transferring data and functionality between old and new services or systems will be desired. Service providers can assist their customers by ensuring data is as portable as possible and that as much data can be exported as possible. As such, data should be stored in a documented format, preferably an open standard, noting that undocumented or proprietary formats may make it more difficult for an organisation to perform backup, service migration or service decommissioning activities.

Finally, to ensure that an organisation is given sufficient time to download their data or move to another service provider should a service provider cease offering a particular service, a one month notification period should be documented in contractual arrangements.

Security Control: ISM-1395; Revision: 6; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Service providers provide an appropriate level of protection for any data entrusted to them or their services.

Security Control: ISM-0072; Revision: 7; Updated: Jun-21; Applicability: All; Essential Eight: N/A
Security requirements associated with the confidentiality, integrity and availability of data entrusted to a service provider are documented in contractual arrangements.

Security Control: ISM-1571; Revision: 2; Updated: Mar-22; Applicability: All; Essential Eight: N/A
The right to verify compliance with security requirements is documented in contractual arrangements.

Security Control: ISM-1738; Revision: 0; Updated: Mar-22; Applicability: All; Essential Eight: N/A
The right to verify compliance with security requirements documented in contractual arrangements is exercised on a regular and ongoing basis.

Security Control: ISM-1451; Revision: 3; Updated: Jun-21; Applicability: All; Essential Eight: N/A
Types of data and its ownership is documented in contractual arrangements.

Security Control: ISM-1572; Revision: 1; Updated: Jun-21; Applicability: All; Essential Eight: N/A
The regions or availability zones where data will be processed, stored and communicated is documented in contractual arrangements.

Security Control: ISM-1573; Revision: 2; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Access to all logs relating to an organisation's data and services is documented in contractual arrangements.

Security Control: ISM-1574; Revision: 2; Updated: Mar-22; Applicability: All; Essential Eight: N/A
The storage of data in a portable manner that allows for backups, service migration and service decommissioning without any loss of data is documented in contractual arrangements.

Security Control: ISM-1575; Revision: 0; Updated: Jul-20; Applicability: All; Essential Eight: N/A
A minimum notification period of one month for the cessation of any services by a service provider is documented in contractual arrangements.

Access to systems and data by service providers

To perform their contracted duties, service providers may need to access their customers' systems and data. However, without proper security controls in place, this could leave systems and data vulnerable – especially when access occurs from outside of Australian borders. As such, an organisation should ensure that their systems and data are not accessed or administered by service providers unless such requirements, and associated measures to control such requirements, are documented in contractual arrangements. In doing so, it is important that sufficient measures are also in place to detect and record any unauthorised access, such as customer support representatives or platform engineers accessing encryption keys. In such cases, the service provider should immediately report the cyber security incident to their customer and make available all logs pertaining to the unauthorised access.

Security Control: ISM-1073; Revision: 5; Updated: Jun-21; Applicability: All; Essential Eight: N/A
An organisation's systems and data are not accessed or administered by a service provider unless a contractual arrangement exists between the organisation and the service provider to do so.

Security Control: ISM-1576; Revision: 2; Updated: Mar-22; Applicability: All; Essential Eight: N/A
If an organisation's systems or data are accessed or administered by a service provider in an unauthorised manner, the organisation is immediately notified.

Further information

Further information on managed service providers can be found in the ACSC's *How to Manage Your Security When Engaging a Managed Service Provider* and *Questions to ask Managed Service Providers* publications.

Further information on the definition of cloud computing can be found in National Institute of Standards and Technology Special Publication 800-145, *The NIST Definition of Cloud Computing*.

Further information on securing cloud services can be found in the ACSC's *Cloud Computing Security Considerations*, *Cloud Computing Security for Cloud Service Providers* and *Cloud Computing Security for Tenants* publications.

Further information on conducting security assessments of cloud service providers can be found in the ACSC's *Anatomy of a Cloud Assessment and Authorisation* and *Cloud Assessment and Authorisation – Frequently Asked Questions* publications.

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

Further information on the whole-of-government policy for secure cloud computing can be found in the Digital Transformation Agency's *Secure Cloud Strategy* publication.

Guidelines for Security Documentation

Development and maintenance of security documentation

Cyber security strategy

A cyber security strategy sets out an organisation's guiding principles, objectives and priorities for cyber security, typically over a three to five year period. In addition, a cyber security strategy may also cover an organisation's threat environment, cyber security initiatives or investments the organisation plans to make as part of its cyber security program. Without a cyber security strategy, an organisation risks failing to adequately plan for and manage security and business risks within their organisation.

Security Control: ISM-0039; Revision: 5; Updated: Mar-22; Applicability: All; Essential Eight: N/A
A cyber security strategy is developed and implemented.

Approval of security documentation

If security documentation is not reviewed and approved by an appropriate authority, system owners risk failing in their duty to ensure that appropriate security controls have been identified and implemented for systems and their operating environments. In doing so, it is important that a system's security architecture, as outlined within the system security plan and supported by the incident response plan and continuous monitoring plan, is approved by the system's authorising officer prior to the development of the system.

Security Control: ISM-0047; Revision: 4; Updated: May-19; Applicability: All; Essential Eight: N/A
Organisational-level security documentation is approved by the Chief Information Security Officer while system-specific security documentation is approved by the system's authorising officer.

Security Control: ISM-1739; Revision: 0; Updated: Mar-22; Applicability: All; Essential Eight: N/A
A system's security architecture is approved prior to the development of the system.

Maintenance of security documentation

Threat environments are dynamic. If security documentation is not kept up-to-date to reflect the current threat environment, policies, processes and procedures may cease to be effective. In such a situation, resources could be devoted to cyber security initiatives or investments that have reduced effectiveness or are no longer relevant.

Security Control: ISM-0888; Revision: 5; Updated: May-19; Applicability: All; Essential Eight: N/A
Security documentation is reviewed at least annually and includes a 'current as at [date]' or equivalent statement.

Communication of security documentation

It is important that once security documentation has been approved, it is published and communicated to all stakeholders. If security documentation is not communicated to stakeholders they will be unaware of what policies and procedures have been implemented for systems.

Security Control: ISM-1602; Revision: 0; Updated: Aug-20; Applicability: All; Essential Eight: N/A
Security documentation, including notification of subsequent changes, is communicated to all stakeholders.

Further information

Further information on system-specific security documentation, such as a system security plan, incident response plan, continuous monitoring plan, security assessment report and plan of action and milestones, can be found in the following section of these guidelines.

Further information on business continuity and disaster recovery plans can be found in the Chief Information Security Officer section of the *Guidelines for Cyber Security Roles*.

Further information on cyber security communication strategies can be found in the Chief Information Security Officer section of the *Guidelines for Cyber Security Roles*.

Further information on intrusion detection and prevent policy can be found in the detecting cyber security incidents section of the *Guidelines for Cyber Security Incidents*.

Further information on cyber security incident registers can be found in the managing cyber security incidents section of the *Guidelines for Cyber Security Incidents*.

Further information on managed service registers can be found in the managed services and cloud services section of the *Guidelines for Outsourcing*.

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

Further information on authorised Radio Frequency and infrared device registers can be found in the facilities and systems section of the *Guidelines for Physical Security*.

Further information on cable registers can be found in the cabling infrastructure section of the *Guidelines for Communications Infrastructure*.

Further information on floor plan diagrams can be found in the cabling infrastructure section of the *Guidelines for Communications Infrastructure*.

Further information on cable labelling processes and procedures can be found in the cabling infrastructure section of the *Guidelines for Communications Infrastructure*.

Further information on telephone system usage policy can be found in the telephone systems section of the *Guidelines for Communications Systems*.

Further information on denial of service response plans for video conferencing and Internet Protocol telephony services can be found in the video conferencing and Internet Protocol telephony section of the *Guidelines for Communications Systems*.

Further information on fax machine and multifunction device usage policy can be found in the fax machines and multifunction devices section of the *Guidelines for Communications Systems*.

Further information on mobile device management policy can be found in the mobile device management section of the *Guidelines for Enterprise Mobility*.

Further information on mobile device usage policy can be found in the mobile device usage section of the *Guidelines for Enterprise Mobility*.

Further information on mobile device emergency sanitisation processes and procedures can be found in the mobile device usage section of the *Guidelines for Enterprise Mobility*.

Further information on ICT equipment management policy can be found in the ICT equipment usage section of the *Guidelines for ICT Equipment*.

Further information on ICT equipment registers can be found in the ICT equipment usage section of the *Guidelines for ICT Equipment*.

Further information on ICT equipment sanitisation processes and procedures can be found in the ICT equipment sanitisation and destruction section of the *Guidelines for ICT Equipment*.

Further information on ICT equipment destruction processes and procedures can be found in the ICT equipment sanitisation and destruction section of the *Guidelines for ICT Equipment*.

Further information on ICT equipment disposal processes and procedures can be found in the ICT equipment disposal section of the *Guidelines for ICT Equipment*.

Further information on media management policy can be found in the media usage section of the *Guidelines for Media*.

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

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

Further information on media sanitisation processes and procedures can be found in the media sanitisation section of the *Guidelines for Media*.

Further information on media destruction processes and procedures can be found in the media destruction section of the *Guidelines for Media*.

Further information on media disposal processes and procedures can be found in the media disposal section of the *Guidelines for Media*.

Further information on system administration processes and procedures can be found in the system administration section of the *Guidelines for System Management*.

Further information on patch management processes and procedures can be found in the system patching section of the *Guidelines for System Management*.

Further information on software registers can be found in the system patching section of the *Guidelines for System Management*.

Further information on digital preservation policy can be found in the data backup and restoration section of the *Guidelines for System Management*.

Further information on data backup processes and procedures can be found in the data backup and restoration section of the *Guidelines for System Management*.

Further information on data restoration processes and procedures can be found in the data backup and restoration section of the *Guidelines for System Management*.

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

Further information on vulnerability disclosure policy can be found in the application development section of the *Guidelines for Software Development*.

Further information on vulnerability disclosure processes and procedures can be found in the application development section of the *Guidelines for Software Development*.

Further information on database registers can be found in the databases section of the *Guidelines for Database Systems*.

Further information on email usage policy can be found in the email usage section of the *Guidelines for Email*.

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

Further information on web usage policy can be found in the web proxies section of the *Guidelines for Gateways*.

Further information on data transfer processes and procedures can be found in the data transfers section of the *Guidelines for Data Transfers*.

System-specific security documentation

System-specific security documentation

System-specific security documentation, such as a system security plan, incident response plan, continuous monitoring plan, security assessment report, and plan of action and milestones, supports the accurate and consistent application of policies, processes and procedures for systems. As such, it is important that they are developed by personnel with a good understanding of business requirements, technologies being used and cyber security matters.

System-specific security documentation may be presented in a number of formats, including in wikis or other forms of document repositories. Furthermore, depending on the documentation framework used, details common to multiple systems could be consolidated into higher level security documentation.

System security plan

The system security plan provides a description of a system and includes an annex that describes the security controls that have been identified for the system.

There can be many stakeholders involved in developing and maintaining a system security plan. This can include representatives from:

- cyber security teams
- project teams who deliver the capability (including contractors)
- support teams who operate and support the capability
- data owners for data processed, stored or communicated by the system
- users for whom the capability is being developed.

Security Control: ISM-0041; Revision: 4; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Systems have a system security plan that includes a description of the system and an annex that covers both applicable security controls from this document and any additional security controls that have been identified.

Incident response plan

Having an incident response plan ensures that when a cyber security incident occurs, a plan is in place to respond appropriately to the situation. In most situations, the aim of the response will be to prevent the cyber security incident from escalating, restore any impacted system or data, and preserve any evidence.

Security Control: ISM-0043; Revision: 4; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Systems have an incident response plan that covers the following:

- *guidelines on what constitutes a cyber security incident*
- *the types of cyber security incidents likely to be encountered and the expected response to each type*
- *how to report cyber security incidents, internally to an organisation and externally to relevant authorities*
- *other parties which need to be informed in the event of a cyber security incident*
- *the authority, or authorities, responsible for investigating and responding to cyber security incidents*
- *the criteria by which an investigation of a cyber security incident would be requested from a law enforcement agency, the Australian Cyber Security Centre or other relevant authority*
- *the steps necessary to ensure the integrity of evidence relating to a cyber security incident*
- *system contingency measures or a reference to such details if they are located in a separate document.*

Continuous monitoring plan

A continuous monitoring plan can assist an organisation in proactively identifying, prioritising and responding to security vulnerabilities. Measures to monitor and manage security vulnerabilities in systems can also provide an organisation with a wealth of valuable information about their exposure to cyber threats, as well as assisting them to determine security risks associated with the operation of their systems. Undertaking continuous monitoring activities is important as cyber threats and the effectiveness of security controls will change over time.

Three types of continuous monitoring activities are vulnerability assessments, vulnerability scans and penetration tests. A vulnerability assessment typically consists of a review of a system's architecture or an in-depth hands-on assessment while a vulnerability scan involves using software tools to conduct automated checks for known security vulnerabilities. In each case, the goal is to identify as many security vulnerabilities as possible. A penetration test however is designed to exercise real-world scenarios in an attempt to achieve a specific goal, such as compromising critical system components or data. Regardless of the continuous monitoring activities chosen, they should be conducted by suitably skilled personnel independent of the system being assessed. Such personnel can be internal to an organisation or from a third party. This ensures that there is no conflict of interest, perceived or otherwise, and that the activities are undertaken in an objective manner.

Security Control: ISM-1163; Revision: 7; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Systems have a continuous monitoring plan that includes:

- *conducting vulnerability scans for systems at least monthly*
- *conducting vulnerability assessments or penetration tests for systems at least annually*
- *analysing identified security vulnerabilities to determine their potential impact*
- *using a risk-based approach to prioritise the implementation of mitigations based on effectiveness and cost.*

Security assessment report

At the conclusion of a security assessment for a system, a security assessment report should be produced by the assessor. This will assist the system owner in performing any initial remediation actions as well as guiding the development of the system's plan of action and milestones.

Security Control: ISM-1563; Revision: 0; Updated: May-20; Applicability: All; Essential Eight: N/A
At the conclusion of a security assessment for a system, a security assessment report is produced by the assessor and covers:

- *the scope of the security assessment*
- *the system's strengths and weaknesses*
- *security risks associated with the operation of the system*
- *the effectiveness of the implementation of security controls*
- *any recommended remediation actions.*

Plan of action and milestones

At the conclusion of a security assessment for a system, and after the production of a security assessment report by the assessor, a plan of action and milestones should be produced by the system owner. This will assist with tracking any of the system's identified weaknesses and recommended remediation actions identified during the security assessment.

Security Control: ISM-1564; Revision: 0; Updated: May-20; Applicability: All; Essential Eight: N/A
At the conclusion of a security assessment for a system, a plan of action and milestones is produced by the system owner.

Guidelines for Physical Security

Facilities and systems

Physical access to systems

The application of the defence-in-depth principle to the protection of systems is enhanced through the use of successive layers of physical security. The first layer of physical security being the use of a security zone for facilities containing systems.

Deployable platforms should also meet physical security requirements. Notably, physical security certification authorities dealing with deployable platforms may have specific requirements that supersede the security controls in these guidelines. This may include perimeter controls, building standards and manning levels. As such, an organisation implementing deployable platforms should contact their physical security certification authority to seek additional guidance.

Security Control: ISM-0810; Revision: 5; Updated: Dec-21; Applicability: O, P, S, TS; Essential Eight: N/A
Systems are secured in facilities that meet the requirements for a security zone suitable for their sensitivity or classification.

Physical access to servers, network devices and cryptographic equipment

The second layer of physical security is the use of an additional security zone for a server room or communications room. This is then further supplemented by the use of security containers or secure rooms for the protection of servers, network devices and cryptographic equipment.

Security Control: ISM-1053; Revision: 3; Updated: Dec-21; Applicability: O, P, S, TS; Essential Eight: N/A
Servers, network devices and cryptographic equipment are secured in server rooms or communications rooms that meet the requirements for a security zone suitable for their sensitivity or classification.

Security Control: ISM-1530; Revision: 1; Updated: Dec-21; Applicability: O, P, S, TS; Essential Eight: N/A
Servers, network devices and cryptographic equipment are secured in security containers or secure rooms suitable for their sensitivity or classification taking into account the combination of security zones they reside in.

Security Control: ISM-0813; Revision: 4; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Server rooms, communications rooms, security containers and secure rooms are not left in unsecured states.

Security Control: ISM-1074; Revision: 3; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Keys or equivalent access mechanisms to server rooms, communications rooms, security containers and secure rooms are appropriately controlled.

Physical access to network devices in public areas

Unprotected network devices in public areas could lead to accidental or deliberate physical damage resulting in an interruption of services. Alternatively, unauthorised access to network devices may allow an adversary to reset them to factory default settings, thereby removing any security controls, or connect directly to them in order to bypass network access controls. Even if access to network devices is not gained by resetting them to factory default settings, it is highly likely that it will cause an interruption of services.

Physical access to network devices can be restricted through physical security controls, such as using enclosures that prevent access to their console ports and factory reset buttons, mounting them on ceilings or behind walls, or securing them in security containers.

Security Control: ISM-1296; Revision: 3; Updated: Dec-21; Applicability: All; Essential Eight: N/A

Physical security controls are implemented to protect network devices in public areas from physical damage or unauthorised access.

Bringing Radio Frequency and infrared devices into facilities

Radio Frequency (RF) devices, such as mobile devices, wireless keyboards and Bluetooth devices, as well as infrared (IR) devices, can pose a security risk to an organisation, especially when they are capable of recording or transmitting audio or data. In SECRET and TOP SECRET areas, it is important that an organisation understands the security risks associated with the introduction of RF and IR devices and maintain a register of those that have been authorised for use in such environments.

In deciding which RF or IR devices to authorise to be brought into SECRET and TOP SECRET areas, an organisation should consider any mitigating measures already in place, such as whether IR communications would be prevented from travelling outside secured spaces, whether systems of different sensitives or classifications are used in the same spaces, and if any temporary or permanent method of blocking RF or IR transmissions has been applied to the facility.

Security Control: ISM-1543; Revision: 3; Updated: Mar-22; Applicability: S, TS; Essential Eight: N/A
An authorised RF and IR device register is maintained for SECRET and TOP SECRET areas and verified on a regular basis.

Security Control: ISM-0225; Revision: 3; Updated: Sep-21; Applicability: S, TS; Essential Eight: N/A
Unauthorised RF and IR devices are not brought into SECRET and TOP SECRET areas.

Security Control: ISM-0829; Revision: 4; Updated: Mar-19; Applicability: S, TS; Essential Eight: N/A
Security measures are used to detect and respond to unauthorised RF devices in SECRET and TOP SECRET areas.

Preventing observation by unauthorised people

Without sufficient perimeter security, the inside of a facility is often observable by unauthorised people, such as via direct observation or by using equipment with a telephoto lens. Ensuring systems, in particular workstation displays and keyboards, are not visible through windows, such as via the use of blinds, curtains, privacy films or workstation positioning, will assist in reducing this security risk.

Security Control: ISM-0164; Revision: 3; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Unauthorised people are prevented from observing systems, in particular workstation displays and keyboards, within facilities.

Further information

Further information on the certification and accreditation authorities for physical security can be found in the Attorney-General's Department (AGD)'s *Protective Security Policy Framework* (PSPF), *Entity facilities* policy.

Further information on the physical security requirements for specific security zones can be found in AGD's PSPF, *Entity facilities* policy.

Further information on selecting security zones, security containers and secure rooms for the protection of ICT equipment can be found in AGD's PSPF, *Physical security for entity resources* policy.

Further information on emanation security considerations associated with usage of RF devices in SECRET and TOP SECRET areas can be found in the emanation security section of the *Guidelines for Communications Infrastructure*.

ICT equipment and media

Securing ICT equipment and media

ICT equipment and media needs to be secured when not in use. This can be achieved by implementing one of the following approaches:

- securing ICT equipment and media in an appropriate security container or secure room
- using ICT equipment without hard drives and sanitising memory at shut down
- encrypting hard drives of ICT equipment and sanitising memory at shut down
- sanitising memory of ICT equipment at shut down and removing and securing any hard drives.

If none of the above approaches are feasible, an organisation may wish to minimise the potential impact of not securing ICT equipment when not in use. This can be achieved by preventing sensitive or classified data from being stored on hard drives, storing user profiles and documents on network shares, removing temporary user data at logoff, scrubbing virtual memory at shut down, and sanitising memory at shut down. It should be noted though that there is no guarantee that such measures will always work effectively or will not be bypassed due to unexpected circumstances, such as the loss of power. Therefore, hard drives in such cases will retain their sensitivity or classification for the purposes of reuse, reclassification, declassification, sanitisation, destruction and disposal.

Security Control: ISM-0161; Revision: 5; Updated: Mar-19; Applicability: All; Essential Eight: N/A
ICT equipment and media are secured when not in use.

Further information

Further information on the handling of ICT equipment can be found in the ICT equipment usage section of the *Guidelines for ICT Equipment*.

Further information on the handling of media can be found in the media usage section of the *Guidelines for Media*.

Further information on encrypting media can be found in the cryptographic fundamentals section of the *Guidelines for Cryptography*.

Further information on selecting security zones, security containers and secure rooms for the protection of ICT equipment can be found in AGD’s PSPF, *Physical security for entity resources* policy.

Guidelines for Personnel Security

Cyber security awareness training

Providing cyber security awareness training

An organisation should ensure that cyber security awareness training is provided to all personnel in order to assist them in understanding their security responsibilities. Furthermore, the content of cyber security awareness training should be tailored to the needs of specific groups of personnel. For example, personnel with responsibilities beyond that of a normal user will require tailored privileged user training.

Security Control: ISM-0252; Revision: 7; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Cyber security awareness training is undertaken annually by all personnel and covers:

- *the purpose of the cyber security awareness training*
- *security appointments and contacts*
- *authorised use of systems and their resources*
- *protection of systems and their resources*
- *reporting of cyber security incidents and suspected compromises of systems and their resources.*

Security Control: ISM-1565; Revision: 0; Updated: Jun-20; Applicability: All; Essential Eight: N/A
Tailored privileged user training is undertaken annually by all privileged users.

Managing and reporting suspicious changes to banking details or payment requests

Business email compromise, a form of financial fraud, is when an adversary attempts to scam an organisation out of money or assets with the assistance of a compromised email account. An adversary will typically attempt to achieve this via invoice fraud, employee impersonation or company impersonation.

With invoice fraud, an adversary will compromise a vendor’s email account and through it have access to legitimate invoices. The adversary will then edit contact and bank details on invoices and send them to customers with the compromised email account. Customers will then pay the invoices, thinking that they are paying the vendor, but instead be sending money to the adversary’s bank account.

With employee impersonation, an adversary will compromise an organisation’s email account and impersonate an employee via email. This is then used to commit financial fraud in a number of ways. One common method is to impersonate a person in a position of authority, such as a Chief Executive Officer or Chief Financial Officer, and have a false invoice raised. Another method is to request a change to an employee’s banking details. The funds from the false invoice or the employee's salary is then sent to the adversary’s bank account.

With company impersonation, an adversary registers a domain with a name similar to another organisation. The adversary then impersonates that organisation in an email to a vendor and requests a quote for a quantity of expensive assets, such as laptops, and subsequently negotiates for the assets to be delivered to them prior to payment. The assets are then delivered to a location specified by the adversary, with the invoice being sent to the legitimate organisation who never ordered or received the assets.

To mitigate business email compromise, personnel should be educated to look for the following warning signs:

- an unexpected request for a change of banking details
- an urgent payment request, or threats of serious consequences if payment is not made

- unexpected payment requests from a person in a position of authority, particularly if payment requests are unusual from this person
- an email received from a suspicious email address, such as an email address not matching an organisation's name.

In dealing with such situations, personnel should have clear guidance to verify bank account details; think critically before actioning unusual payment requests; and have a process to report threatening demands for immediate action, pressure for secrecy, or requests to circumvent normal business processes and procedures.

Security Control: ISM-1740; Revision: 0; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Personnel dealing with banking details and payment requests are advised of what business email compromise is, how to manage such situations and how to report it.

Reporting suspicious contact via online services

Online services, such as email, internet forums, messaging apps and direct messaging on social media, can be used by an adversary in an attempt to elicit sensitive or classified information from personnel. As such, personnel should be advised of what suspicious contact via online services is and how to report it.

Security Control: ISM-0817; Revision: 4; Updated: Jan-20; Applicability: All; Essential Eight: N/A
Personnel are advised of what suspicious contact via online services is and how to report it.

Posting work information to online services

Personnel should be advised to take special care not to post work information to online services unless authorised to do so, especially in internet forums and on social media. Even information that appears to be benign in isolation could, along with other information, have a considerable security impact. In addition, to ensure that personal opinions of individuals are not misinterpreted, personnel should be advised to maintain separate work and personal accounts for online services, especially when using social media.

Security Control: ISM-0820; Revision: 5; Updated: Jan-20; Applicability: All; Essential Eight: N/A
Personnel are advised to not post work information to unauthorised online services and to report cases where such information is posted.

Security Control: ISM-1146; Revision: 2; Updated: Sep-18; Applicability: All; Essential Eight: N/A
Personnel are advised to maintain separate work and personal accounts for online services.

Posting personal information to online services

Personnel should be advised that any personal information they post to online services, such as social media, could be used by an adversary to develop a detailed understanding of their lifestyle and interests. In turn, this information could be used to build trust in order to elicit sensitive or classified information from them, or influence them to undertake specific actions, such as opening malicious email attachments or visiting malicious websites. Furthermore, posting information on movements and activities may allow an adversary to time attempted financial fraud to align with when a person in a position of authority will be uncontactable, such as attending meetings or travelling. Finally, encouraging personnel to use any available privacy settings for online services can reduce security risks by restricting who can view their information as well as their interactions with such services.

Security Control: ISM-0821; Revision: 3; Updated: Oct-19; Applicability: All; Essential Eight: N/A
Personnel are advised of security risks associated with posting personal information to online services and are encouraged to use any available privacy settings to restrict who can view such information.

Sending and receiving files via online services

When personnel send and receive files via unauthorised online services, such as messaging apps and social media, they often bypass security controls put in place to detect and quarantine malicious code. Advising personnel to send and receive files via authorised online services instead will ensure files are appropriately protected and scanned for malicious code.

Security Control: ISM-0824; Revision: 2; Updated: Sep-18; Applicability: All; Essential Eight: N/A
Personnel are advised not to send or receive files via unauthorised online services.

Further information

Further information on telephone system usage can be found in the telephone systems section of the *Guidelines for Communications Systems*.

Further information on fax machine and multifunction device usage can be found in the fax machines and multifunction devices section of the *Guidelines for Communications Systems*.

Further information on mobile device usage can be found in the mobile device usage section of the *Guidelines for Enterprise Mobility*.

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

Further information on email usage can be found in the email usage section of the *Guidelines for Email*.

Further information on web usage can be found in the web proxies section of the *Guidelines for Gateways*.

Further information on detecting socially engineered messages be found in the Australian Cyber Security Centre (ACSC)'s *Detecting Socially Engineered Messages* publication.

Further information on business email compromise can be found in the ACSC's *Protecting Against Business Email Compromise* publication.

Further information on the use of social media can be found in the ACSC's *Security Tips for Social Media and Messaging Apps* publication.

Further information on the sanitisation of documents before posting them to authorised online services can be found in the ACSC's *An Examination of the Redaction Functionality of Adobe Acrobat Pro DC 2017* publication.

Access to systems and their resources

Security clearances

Where these guidelines refer to security clearances, it applies to Australian security clearances or security clearances from a foreign government which are formally recognised by Australia.

System access requirements

Documenting access requirements for a system and its resources can assist in determining if personnel have the appropriate authorisation, security clearance, briefings and need-to-know to access the system and its resources. Types of users for which access requirements should be documented include unprivileged users, privileged users, foreign nationals and contractors.

Security Control: ISM-0432; Revision: 7; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Access requirements for a system and its resources are documented in its system security plan.

Security Control: ISM-0434; Revision: 7; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Personnel undergo appropriate employment screening and, where necessary, hold an appropriate security clearance before being granted access to a system and its resources.

Security Control: ISM-0435; Revision: 3; Updated: Aug-19; Applicability: All; Essential Eight: N/A
Personnel receive any necessary briefings before being granted access to a system and its resources.

User identification

Having uniquely identifiable users ensures accountability for access to a system and its resources. Furthermore, where a system processes, stores or communicates Australian Eyes Only (AUSTEO), Australian Government Access Only (AGAO) or Releasable To (REL) data, and foreign nationals have access to the system, it is important that the foreign nationals are identified as such.

Security Control: ISM-0414; Revision: 4; Updated: Aug-19; Applicability: All; Essential Eight: N/A
Personnel granted access to a system and its resources are uniquely identifiable.

Security Control: ISM-0415; Revision: 3; Updated: Aug-19; Applicability: All; Essential Eight: N/A
The use of shared user accounts is strictly controlled, and personnel using such accounts are uniquely identifiable.

Security Control: ISM-1583; Revision: 0; Updated: Aug-20; Applicability: All; Essential Eight: N/A
Personnel who are contractors are identified as such.

Security Control: ISM-0420; Revision: 11; Updated: Dec-21; Applicability: S, TS; Essential Eight: N/A
Where a system processes, stores or communicates AUSTEO, AGAO or REL data, personnel who are foreign nationals are identified as such, including by their specific nationality.

Unprivileged access to systems

Personnel seeking access to systems, applications and data repositories should have a genuine business requirement validated by their manager or another appropriate authority.

Finally, to assist with incident response activities, it is important that unprivileged access event logs are centrally stored and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.

Security Control: ISM-0405; Revision: 7; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Requests for unprivileged access to systems, applications and data repositories are validated when first requested.

Security Control: ISM-1566; Revision: 2; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Use of unprivileged access is logged.

Security Control: ISM-1714; Revision: 0; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Unprivileged access event logs are centrally stored and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.

Unprivileged access to systems by foreign nationals

Due to the extra sensitivities associated with AUSTEO, AGAO and REL data, foreign access to such data is strictly controlled.

Security Control: ISM-0409; Revision: 7; Updated: Jun-21; Applicability: S, TS; Essential Eight: N/A
Foreign nationals, including seconded foreign nationals, do not have access to systems that process, store or communicate AUSTEO or REL data unless effective security controls are in place to ensure such data is not accessible to them.

Security Control: ISM-0411; Revision: 6; Updated: Jun-21; Applicability: S, TS; Essential Eight: N/A
Foreign nationals, excluding seconded foreign nationals, do not have access to systems that process, store or communicate AGAO data unless effective security controls are in place to ensure such data is not accessible to them.

Privileged access to systems

Privileged accounts are considered to be those which can alter or circumvent a system's security controls. This can also apply to users who have only limited privileges, such as software developers, but can still bypass security controls. A privileged account often has the ability to modify system configurations, account privileges, event logs and security configurations for applications.

Privileged users, and in some cases privileged service accounts, are often targeted by an adversary as they can potentially give full access to systems. As such, ensuring that privileged accounts do not have the ability to access the internet, email and web services minimises opportunities for these accounts to be compromised.

Finally, to assist with incident response activities, it is important that privileged access event logs and privileged account and group change event logs are centrally stored and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.

Security Control: ISM-1507; Revision: 2; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3
Requests for privileged access to systems and applications are validated when first requested.

Security Control: ISM-1733; Revision: 0; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Requests for privileged access to data repositories are validated when first requested.

Security Control: ISM-1508; Revision: 2; Updated: Sep-21; Applicability: All; Essential Eight: ML3
Privileged access to systems and applications is limited to only what is required for users and services to undertake their duties.

Security Control: ISM-1175; Revision: 4; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3
Privileged user accounts are prevented from accessing the internet, email and web services.

Security Control: ISM-1653; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML3
Privileged service accounts are prevented from accessing the internet, email and web services.

Security Control: ISM-1649; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML3
Just-in-time administration is used for administering systems and applications.

Security Control: ISM-0445; Revision: 6; Updated: Sep-18; Applicability: All; Essential Eight: N/A
Privileged users are assigned a dedicated privileged account to be used solely for tasks requiring privileged access.

Security Control: ISM-1509; Revision: 1; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3
Use of privileged access is logged.

Security Control: ISM-1650; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3
Changes to privileged accounts and groups are logged.

Security Control: ISM-1651; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML3
Privileged access event logs are centrally stored and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.

Security Control: ISM-1652; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML3
Privileged account and group change event logs are centrally stored and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.

Privileged access to systems by foreign nationals

As privileged accounts often have the ability to bypass a system's security controls, it is strongly encouraged that foreign nationals are not given privileged access to systems that process, store or communicate AUSTEO, AGAO or REL data.

Security Control: ISM-0446; Revision: 5; Updated: Jun-21; Applicability: S, TS; Essential Eight: N/A
Foreign nationals, including seconded foreign nationals, do not have privileged access to systems that process, store or communicate AUSTEO or REL data.

Security Control: ISM-0447; Revision: 4; Updated: Jun-21; Applicability: S, TS; Essential Eight: N/A

Foreign nationals, excluding seconded foreign nationals, do not have privileged access to systems that process, store or communicate AGAO data.

Suspension of access to systems

Removing or suspending access to systems, applications and data repositories can prevent them from being accessed when there is no longer a legitimate business requirement for their use, such as when personnel change duties, leave an organisation or are detected undertaking malicious activities.

Security Control: ISM-0430; Revision: 7; Updated: Sep-19; Applicability: All; Essential Eight: N/A
Access to systems, applications and data repositories is removed or suspended on the same day personnel no longer have a legitimate requirement for access.

Security Control: ISM-1591; Revision: 0; Updated: Aug-20; Applicability: All; Essential Eight: N/A
Access to systems, applications and data repositories is removed or suspended as soon as practicable when personnel are detected undertaking malicious activities.

Security Control: ISM-1404; Revision: 3; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Unprivileged access to systems and applications is automatically disabled after 45 days of inactivity.

Security Control: ISM-1648; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3
Privileged access to systems and applications is automatically disabled after 45 days of inactivity.

Security Control: ISM-1716; Revision: 0; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Access to data repositories is automatically disabled after 45 days of inactivity.

Security Control: ISM-1647; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3
Privileged access to systems and applications is automatically disabled after 12 months unless revalidated.

Security Control: ISM-1734; Revision: 0; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Privileged access to data repositories is automatically disabled after 12 months unless revalidated.

Recording authorisation for personnel to access systems

Retaining records of system account requests will assist in maintaining personnel accountability. This is needed to ensure there is a record of all personnel authorised to access a system, their user identification, who provided the authorisation, when the authorisation was granted and when the access was last reviewed.

Security Control: ISM-0407; Revision: 4; Updated: Sep-18; Applicability: All; Essential Eight: N/A
A secure record is maintained for the life of each system covering:

- *all personnel authorised to access the system, and their user identification*
- *who provided authorisation for access*
- *when access was granted*
- *the level of access that was granted*
- *when access, and the level of access, was last reviewed*
- *when the level of access was changed, and to what extent (if applicable)*
- *when access was withdrawn (if applicable).*

Temporary access to systems

Under strict circumstances, temporary access to systems, applications or data repositories may be granted to personnel who lack an appropriate security clearance or briefing. In such circumstances, personnel should have their access controlled in such a way that they only have access to data required for them to undertake their duties.

Security Control: ISM-0441; Revision: 7; Updated: Jun-21; Applicability: All; Essential Eight: N/A
When personnel are granted temporary access to a system, effective security controls are put in place to restrict their access to only data required for them to undertake their duties.

Security Control: ISM-0443; Revision: 3; Updated: Sep-18; Applicability: S, TS; Essential Eight: N/A
Temporary access is not granted to systems that process, store or communicate caveated or sensitive compartmented information.

Emergency access to systems

It is important that an organisation does not lose access to their systems. As such, an organisation should always have a method for gaining access during emergencies. Typically, emergencies would occur when access to systems cannot be gained via normal authentication processes, such as due to misconfigurations of authentication services, misconfigurations of security settings or due to a cyber security incident. In these situations, a break glass account (also known as an emergency access account) can be used to gain access. As break glass accounts generally have the highest level of privileges available for systems, extreme care should be taken to both protect them and to monitor for any signs of compromise or abuse.

When break glass accounts are used, any administrative activities performed will not be directly attributable to an individual, and systems may not generate event logs. As such, additional security controls need to be implemented in order to maintain the system's integrity. In doing so, an organisation should ensure that any administrative activities performed using a break glass account are identified and documented in support of change management processes and procedures. This includes documenting the individual using the break glass account, the reason for using the break glass account and any administrative activities performed using the break glass account.

As the custodian of each break glass account should be the only party who knows the account's credentials, credentials will need to be changed and tested by custodians after any authorised access by another party. Modern password managers that support automated credential changes and testing can assist in reducing the administrative overhead of such activities.

Finally, to assist with incident response activities, it is important that break glass event logs are centrally stored and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.

Security Control: ISM-1610; Revision: 0; Updated: Aug-20; Applicability: All; Essential Eight: N/A
A method of emergency access to systems is documented and tested at least once when initially implemented and each time fundamental information technology infrastructure changes occur.

Security Control: ISM-1611; Revision: 0; Updated: Aug-20; Applicability: All; Essential Eight: N/A
Break glass accounts are only used when normal authentication processes cannot be used.

Security Control: ISM-1612; Revision: 0; Updated: Aug-20; Applicability: All; Essential Eight: N/A
Break glass accounts are only used for specific authorised activities.

Security Control: ISM-1614; Revision: 0; Updated: Aug-20; Applicability: All; Essential Eight: N/A
Break glass account credentials are changed by the account custodian after they are accessed by any other party.

Security Control: ISM-1615; Revision: 0; Updated: Aug-20; Applicability: All; Essential Eight: N/A
Break glass accounts are tested after credentials are changed.

Security Control: ISM-1613; Revision: 1; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Use of break glass accounts is logged.

Security Control: ISM-1715; Revision: 0; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Break glass event logs are centrally stored and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.

Control of Australian systems

Due to extra sensitivities associated with AUSTEO and AGAO data, it is essential that control of systems that process, store or communicate such data are maintained by Australian nationals working for or on behalf of the Australian Government. Furthermore, AUSTEO and AGAO data should only be accessible from systems under the sole control of the Australian Government that are located within facilities authorised by the Australian Government.

Security Control: ISM-0078; Revision: 5; Updated: Jun-21; Applicability: S, TS; Essential Eight: N/A
Systems processing, storing or communicating AUSTEO or AGAO data remain at all times under the control of an Australian national working for or on behalf of the Australian Government.

Security Control: ISM-0854; Revision: 6; Updated: Dec-21; Applicability: S, TS; Essential Eight: N/A
AUSTEO and AGAO data can only be accessed from systems under the sole control of the Australian Government that are located within facilities authorised by the Australian Government.

Further information

Further information on access to government resources, including required security clearances, can be found in the Attorney-General's Department's *Protective Security Policy Framework*, *Access to information* policy.

Further information on access to highly sensitive government resources, including required briefings, can be found in the Government Security Committee's *Australian Government Security Caveat Guidelines*. This publication is available from the Protective Security Policy GovTEAMS community or the Australian Security Intelligence Organisation by email.

Further information on restricting the use of privileged accounts can be found in the ACSC's *Restricting Administrative Privileges* publication.

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

Guidelines for Communications Infrastructure

Cabling infrastructure

Applicability

This section is only applicable to facilities located within Australia. In addition, this section only applies to new cabling infrastructure installations or upgrades.

Shared facilities

In addition to common security controls, this section provides additional security controls for shared facilities, such as a single floor, or part of a floor, within a multi-tenanted building.

Cables and structured cabling systems

For the purposes of this section, a cable is defined as any fibre optic or copper material housed within a protective sheath for the purposes of transmitting data or control signals from one point in a facility to another. Each cable will form part of a structured cabling system and will need to comply with the Australian Standards associated with that system. In addition to network communications and data systems, some common building management structured cabling systems found within facilities are:

- fire control and sensor systems
- security control and surveillance systems
- lighting control systems
- access control systems
- voice and emergency telephony systems
- emergency control alert systems.

Cable sheaths and conduits

A cable's protective sheath is not considered to be a conduit.

Cable connector types

The same cable connector types can be used for all systems within a facility regardless of their sensitivity or classification.

Cabling infrastructure standards

Cabling infrastructure should be installed by an endorsed cable installer to the relevant Australian Standards to ensure personnel safety and system availability.

Security Control: ISM-0181; Revision: 3; Updated: Mar-21; Applicability: All; Essential Eight: N/A
Cabling infrastructure is installed in accordance with relevant Australian Standards, as directed by the Australian Communications and Media Authority.

Use of fibre-optic cables

Fibre-optic cables do not produce, nor are influenced by, electromagnetic emanations; thereby offering the highest degree of protection from electromagnetic emanation effects.

Security Control: ISM-1111; Revision: 3; Updated: Mar-21; Applicability: All; Essential Eight: N/A
Fibre-optic cables are used for cabling infrastructure instead of copper cables.

Cable register

Maintaining and regularly verifying cable registers assists installers and inspectors, with the help of floor plan diagrams, to trace cables for malicious or accidental changes or damage. In doing so, cable registers should track all cabling changes throughout the life of a system.

Security Control: ISM-0211; Revision: 6; Updated: Mar-22; Applicability: All; Essential Eight: N/A
A cable register is maintained and verified on a regular basis.

Security Control: ISM-0208; Revision: 6; Updated: Jun-21; Applicability: All; Essential Eight: N/A
A cable register contains the following for each cable:

- *cable identifier*
- *cable colour*
- *sensitivity/classification*
- *source*
- *destination*
- *location*
- *seal numbers (if applicable).*

Floor plan diagrams

Floor plan diagrams, developed using computer-aided design and drafting software, and using alphanumeric grid referencing, provide an accurate scaled view for each floor and are critical to ensuring that cabling infrastructure components can be easily located by installers and inspectors. In doing so, floor plan diagrams should track all cabling infrastructure changes throughout the life of a system.

Security Control: ISM-1645; Revision: 1; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Floor plan diagrams are maintained and verified on a regular basis.

Security Control: ISM-1646; Revision: 0; Updated: Jun-21; Applicability: All; Essential Eight: N/A
Floor plan diagrams contain the following:

- *cable paths (including ingress and egress points between floors)*
- *cable reticulation system and conduit paths*
- *floor concentration boxes*
- *wall outlet boxes*
- *network cabinets.*

Cable labelling processes and procedures

Well documented cable labelling processes and procedures can make cable verification and fault finding easier.

Security Control: ISM-0206; Revision: 6; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Cable labelling processes, and supporting cable labelling procedures, are developed and implemented.

Labelling cables

Labelling cables with the correct source and destination details minimises the likelihood of cross-patching and aids in fault finding and configuration management.

Security Control: ISM-1096; Revision: 2; Updated: Oct-19; Applicability: All; Essential Eight: N/A
Cables are labelled at each end with sufficient source and destination details to enable the physical identification and inspection of the cable.

Labelling building management cables

All facilities will contain structured cabling systems to support building management and control functions. As Australian Standards require some structured cabling systems to use specified colours, such as red for fire control systems, it is important that all building management cables are appropriately labelled.

Security Control: ISM-1639; Revision: 0; Updated: Mar-21; Applicability: All; Essential Eight: N/A
Building management cables are labelled with their purpose in black writing on a yellow background, with a minimum size of 2.5 cm x 1 cm, and attached at five-metre intervals.

Labelling cables for foreign systems in Australian facilities

Labelling cables for foreign systems in Australian facilities helps prevent unintended cross-patching of Australian and foreign systems.

Security Control: ISM-1640; Revision: 0; Updated: Mar-21; Applicability: All; Essential Eight: N/A
Cables for foreign systems installed in Australian facilities are labelled at inspection points.

Cable colours

The use of designated cable colours can provide an easy way to distinguish SECRET and TOP SECRET systems from other systems. For example, while SECRET and TOP SECRET cables have designated colours, cables for other systems may be any colour except for those reserved for SECRET and TOP SECRET systems. In addition, cable colours for other systems may be the same colour, such as blue.

Security Control: ISM-0926; Revision: 9; Updated: Dec-21; Applicability: O, P; Essential Eight: N/A
OFFICIAL and PROTECTED cables are coloured neither salmon pink nor red.

Security Control: ISM-1718; Revision: 0; Updated: Dec-21; Applicability: S; Essential Eight: N/A
SECRET cables colours are coloured salmon pink.

Security Control: ISM-1719; Revision: 0; Updated: Dec-21; Applicability: TS; Essential Eight: N/A
TOP SECRET cables colours are coloured red.

Cable colour non-conformance

In certain circumstances it may not be possible to use the correct colour for SECRET or TOP SECRET cables. In such cases, an organisation should band such cables with the appropriate colour and ensure that the cable bands are easily visible at inspection points. In doing so, it is important that cable bands are robust enough to stand the test of time. Examples of appropriate cable bands include stick-on coloured labels, colour heat shrink, coloured ferrules or short lengths of banded conduit.

Security Control: ISM-1216; Revision: 3; Updated: Dec-21; Applicability: S, TS; Essential Eight: N/A

SECRET and TOP SECRET cables with non-conformant cable colouring are both banded with the appropriate colour and labelled at inspection points.

Cable inspectability

The ability to inspect cabling infrastructure is necessary to detect illicit tampering or degradation.

Security Control: ISM-1112; Revision: 3; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Cables are inspectable at a minimum of five-metre intervals.

Security Control: ISM-1119; Revision: 2; Updated: Dec-21; Applicability: O, P, S, TS; Essential Eight: N/A
Cables in TOP SECRET areas are fully inspectable for their entire length.

Common cable reticulation systems and conduits

Cables from different cable groups can share common cable reticulation systems and conduits to reduce costs.

Security Control: ISM-0187; Revision: 7; Updated: Dec-21; Applicability: S, TS; Essential Eight: N/A
SECRET and TOP SECRET systems belong exclusively to their own cable groups.

Security Control: ISM-0189; Revision: 4; Updated: Sep-21; Applicability: All; Essential Eight: N/A
Cables only carry a single cable group, unless each cable group belongs to a different subunit.

Security Control: ISM-1114; Revision: 3; Updated: Mar-21; Applicability: All; Essential Eight: N/A
Cable groups sharing a common cable reticulation system have a dividing partition or a visible gap between the cable groups.

Enclosed cable reticulation systems

In shared facilities, cables should be enclosed in a sealed cable reticulation system to prevent access and enhance cable management.

Security Control: ISM-1130; Revision: 4; Updated: Dec-21; Applicability: All; Essential Eight: N/A
In shared facilities, cables are run in an enclosed cable reticulation system.

Covers for enclosed cable reticulation systems

In shared facilities, clear covers on enclosed cable reticulation systems are a convenient method of maintaining inspection requirements. Having clear covers face inwards increases their inspectability.

Security Control: ISM-1164; Revision: 3; Updated: Dec-21; Applicability: All; Essential Eight: N/A
In shared facilities, conduits or the front covers of ducts, cable trays in floors and ceilings, and associated fittings are clear plastic.

Sealing cable reticulation systems and conduits

In shared facilities, Security Construction and Equipment Committee (SCEC) endorsed seals should be used to provide evidence of any tampering or illicit access to TOP SECRET cable reticulation systems. In addition, TOP SECRET conduits should be sealed with a visible smear of conduit glue to prevent access.

Security Control: ISM-0195; Revision: 6; Updated: Dec-21; Applicability: TS; Essential Eight: N/A
In shared facilities, uniquely identifiable SCEC endorsed tamper-evident seals are used to seal all removable covers on TOP SECRET cable reticulation systems.

Security Control: ISM-0194; Revision: 3; Updated: Dec-21; Applicability: TS; Essential Eight: N/A
In shared facilities, a visible smear of conduit glue is used to seal all plastic conduit joints and TOP SECRET conduits connected by threaded lock nuts.

Labelling conduits

Labels for TOP SECRET conduits should be of sufficient size and colour to allow for easy identification.

Security Control: ISM-0201; Revision: 3; Updated: Mar-21; Applicability: TS; Essential Eight: N/A
Labels for TOP SECRET conduits are a minimum size of 2.5 cm x 1 cm, attached at five-metre intervals and marked as 'TS RUN'.

Cables in walls

Cables run correctly in walls allow for neater installations while maintaining separation and inspection requirements.

Security Control: ISM-1115; Revision: 4; Updated: Dec-19; Applicability: All; Essential Eight: N/A
Cables from cable trays to wall outlet boxes are run in flexible or plastic conduit.

Cables in party walls

In shared facilities, TOP SECRET cables are not run in party walls. However, an inner wall can be used to run TOP SECRET cables where sufficient space exists for their inspection.

Security Control: ISM-1133; Revision: 3; Updated: Dec-21; Applicability: TS; Essential Eight: N/A
In shared facilities, TOP SECRET cables are not run in party walls.

Wall penetrations

Penetrating a wall between a TOP SECRET area and a lower classified area requires the integrity of the TOP SECRET area to be maintained. In such scenarios, TOP SECRET cables should be encased in conduit with all gaps between the TOP SECRET conduit and the wall filled with an appropriate sealing compound.

Security Control: ISM-1122; Revision: 2; Updated: Dec-21; Applicability: TS; Essential Eight: N/A
Where wall penetrations exit a TOP SECRET area into a lower classified area, TOP SECRET cables are encased in conduit with all gaps between the TOP SECRET conduit and the wall filled with an appropriate sealing compound.

Wall outlet boxes

Wall outlet boxes are the main method of connecting cabling infrastructure to workstations. They allow the management of cables and the types of connectors allocated to various systems.

Security Control: ISM-1104; Revision: 4; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Wall outlet boxes have connectors on opposite sides of the wall outlet box if the cable group contains cables belonging to different systems.

Security Control: ISM-1105; Revision: 3; Updated: Mar-21; Applicability: All; Essential Eight: N/A
Different cables groups do not share a wall outlet box.

Labelling wall outlet boxes

Clear labelling of wall outlet boxes diminishes the possibility of incorrectly attaching ICT equipment to the wrong wall outlet box. In cases were a wall outbox has a cable group containing cables belonging to different systems, each connector should be individually labelled.

Security Control: ISM-1095; Revision: 5; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Wall outlet boxes denote the systems, cable identifiers and wall outlet box identifier.

Wall outlet box colours

The use of designated wall outlet box colours can provide an easy way to distinguish SECRET and TOP SECRET systems from other systems. For example, while SECRET and TOP SECRET wall outlet boxes have designated colours, wall outlet boxes for other systems may be any colour except for those reserved for SECRET and TOP SECRET systems. In addition, wall outlet box colours for other systems may be the same colour, such as white. Ideally, wall outlet boxes should be the same colour that is used for associated cabling infrastructure.

Security Control: ISM-1107; Revision: 5; Updated: Dec-21; Applicability: O, P; Essential Eight: N/A
OFFICIAL and PROTECTED wall outlet boxes are coloured neither salmon pink nor red.

Security Control: ISM-1720; Revision: 0; Updated: Dec-21; Applicability: S; Essential Eight: N/A
SECRET wall outlet boxes are coloured salmon pink.

Security Control: ISM-1721; Revision: 0; Updated: Dec-21; Applicability: TS; Essential Eight: N/A
TOP SECRET wall outlet boxes are coloured red.

Wall outlet box covers

Transparent wall outlet box covers allow for inspection of cable cross-patching and tampering.

Security Control: ISM-1109; Revision: 3; Updated: Dec-19; Applicability: All; Essential Eight: N/A
Wall outlet box covers are clear plastic.

Fly lead installation

Keeping the lengths of TOP SECRET fibre-optic fly leads to a minimum prevents clutter around desks, prevents damage, and reduces the chance of cross-patching and tampering. If lengths become excessive, TOP SECRET fibre-optic fly leads should be treated as cabling infrastructure and run in TOP SECRET conduit or fixed infrastructure, such as desk partitioning.

Security Control: ISM-0218; Revision: 6; Updated: Dec-21; Applicability: TS; Essential Eight: N/A
If TOP SECRET fibre-optic fly leads exceeding five metres in length are used to connect wall outlet boxes to ICT equipment, they are run in a protective and easily inspected pathway that is clearly labelled at the ICT equipment end with the wall outlet box's identifier.

Connecting cable reticulation systems to cabinets

Controlling the routing from cable reticulation systems to cabinets can assist in preventing unauthorised modifications and tampering while also providing easy inspection of cables.

Security Control: ISM-1102; Revision: 3; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Cable reticulation systems leading into cabinets are terminated as close as possible to the cabinet.

Security Control: ISM-1101; Revision: 3; Updated: Dec-21; Applicability: O, P, S, TS; Essential Eight: N/A
In TOP SECRET areas, cable reticulation systems leading into cabinets in server rooms or communications rooms are terminated as close as possible to the cabinet.

Security Control: ISM-1103; Revision: 3; Updated: Dec-21; Applicability: O, P, S, TS; Essential Eight: N/A
In TOP SECRET areas, cable reticulation systems leading into cabinets not in server rooms or communications rooms are terminated at the boundary of the cabinet.

Terminating cables in cabinets

Having individual or divided cabinets can assist in preventing accidental or deliberate cross-patching and makes inspection of cables easier.

Security Control: ISM-1098; Revision: 4; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Cables are terminated in individual cabinets; or for small systems, one cabinet with a division plate to delineate cable groups.

Security Control: ISM-1100; Revision: 1; Updated: Sep-18; Applicability: TS; Essential Eight: N/A
TOP SECRET cables are terminated in an individual TOP SECRET cabinet.

Terminating cable groups on patch panels

Terminating cable groups on different patch panels in cabinets can assist in preventing accidental or deliberate cross-patching and makes inspection of cables easier.

Security Control: ISM-0213; Revision: 3; Updated: Mar-21; Applicability: All; Essential Eight: N/A
Different cable groups do not terminate on the same patch panel.

Physical separation of cabinets and patch panels

Physical separation between TOP SECRET systems and systems of lower classifications reduces the chance of cross-patching, thereby the possibility of unauthorised personnel gaining access to TOP SECRET systems.

Security Control: ISM-1116; Revision: 3; Updated: Oct-19; Applicability: O, P, S, TS; Essential Eight: N/A
There is a visible gap between TOP SECRET cabinets and cabinets of lower classifications.

Security Control: ISM-0216; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS; Essential Eight: N/A
TOP SECRET and non-TOP SECRET patch panels are physically separated by installing them in separate cabinets.

Security Control: ISM-0217; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS; Essential Eight: N/A
Where spatial constraints demand patch panels of lower classifications than TOP SECRET be located in the same cabinet as a TOP SECRET patch panel:

- *a physical barrier in the cabinet is provided to separate patch panels*
- *only personnel holding a Positive Vetting security clearance have access to the cabinet*
- *approval from the TOP SECRET system's authorising officer is obtained prior to installation.*

Audio secure rooms

Audio secure rooms are designed to prevent audio conversations from being overheard. The Australian Security Intelligence Organisation should be consulted before any modifications are made to TOP SECRET audio secure rooms.

Security Control: ISM-0198; Revision: 3; Updated: Dec-21; Applicability: TS; Essential Eight: N/A
When penetrating a TOP SECRET audio secure room, the Australian Security Intelligence Organisation is consulted and all directions provided are complied with.

Power reticulation

It is important that TOP SECRET systems have control over the power system to prevent denial of service by deliberate or accidental means.

Security Control: ISM-1123; Revision: 3; Updated: Dec-21; Applicability: TS; Essential Eight: N/A
A power distribution board with a feed from an Uninterruptible Power Supply is used to power all TOP SECRET ICT equipment.

Further information

Australian cabling standards and regulations can be obtained from the Australian Communications and Media Authority.

Further information on endorsed seals for various sealing requirements can be found on the SCEC's *Security Equipment Evaluated Products List*.

Further information on audio secure rooms can be found in the Attorney-General's Department's *Protective Security Policy Framework*, *Physical security for entity resources* policy.

Emanation security

Emanation security threat assessments in Australia

Obtaining advice from the Australian Cyber Security Centre (ACSC) on emanation security controls is vital to protecting SECRET and TOP SECRET systems.

Security Control: ISM-0248; Revision: 6; Updated: Dec-21; Applicability: O, P; Essential Eight: N/A
System owners deploying OFFICIAL or PROTECTED systems with Radio Frequency transmitters that will be co-located with SECRET or TOP SECRET systems contact the ACSC for an emanation security threat assessment and implement any additional installation criteria derived from the threat assessment.

Security Control: ISM-0247; Revision: 4; Updated: Dec-21; Applicability: S, TS; Essential Eight: N/A
System owners deploying SECRET or TOP SECRET systems with Radio Frequency transmitters inside or co-located with their facility contact the ACSC for an emanation security threat assessment and implement any additional installation criteria derived from the threat assessment.

Security Control: ISM-1137; Revision: 3; Updated: Dec-21; Applicability: S, TS; Essential Eight: N/A
System owners deploying SECRET or TOP SECRET systems in shared facilities contact the ACSC for an emanation security threat assessment and implement any additional installation criteria derived from the threat assessment.

Emanation security threat assessments outside Australia

Fixed sites outside Australia, and deployed military platforms, are more vulnerable to emanation security threats. Failing to implement emanation security controls could result in systems or military platforms emanating compromising signals, which if intercepted and analysed, could lead to serious consequences.

Security Control: ISM-0249; Revision: 4; Updated: Dec-21; Applicability: O, P, S, TS; Essential Eight: N/A
System owners deploying systems or military platforms overseas contact the ACSC for an emanation security threat assessment and implement any additional installation criteria derived from the threat assessment.

Early identification of emanation security controls

It is important to identify emanation security controls for systems early in their project life cycle as costs will be much greater if changes have to be made once a system has been designed and deployed.

Security Control: ISM-0246; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS; Essential Eight: N/A
An emanation security threat assessment is sought as early as possible in a project's life cycle as emanation security controls can have significant cost implications.

Electromagnetic interference/electromagnetic compatibility standards

While all ICT equipment may not need certification to emanation security standards, it still needs to meet applicable industry and government standards relating to electromagnetic interference/electromagnetic compatibility.

Security Control: ISM-0250; Revision: 4; Updated: Dec-21; Applicability: All; Essential Eight: N/A
ICT equipment meets industry and government standards relating to electromagnetic interference/electromagnetic compatibility.

Guidelines for Communications Systems

Telephone systems

Telephone system usage policy

All non-secure telephone systems are subject to interception. Personnel accidentally or maliciously communicating sensitive or classified information over a public telephone network can lead to its compromise.

Security Control: ISM-1078; Revision: 3; Updated: Dec-21; Applicability: All; Essential Eight: N/A
A telephone system usage policy is developed and implemented.

Personnel awareness

As there is a potential for unintended disclosure of information when using telephone systems, it is important that personnel are made aware of the sensitivity or classification of conversations that they can be used for. In addition, personnel should also be made aware of the security risks associated with the use of non-secure telephone systems in sensitive or classified areas.

When using cryptographic equipment to enable different levels of conversation for different kinds of connections, providing a visual indication to personnel as to the sensitivity or classification of information that can be discussed over the telephone system can assist in reducing the likelihood of unintended disclosure of information.

Security Control: ISM-0229; Revision: 3; Updated: Sep-18; Applicability: All; Essential Eight: N/A
Personnel are advised of the permitted sensitivity or classification of information that can be discussed over both internal and external telephone systems.

Security Control: ISM-0230; Revision: 3; Updated: Sep-18; Applicability: All; Essential Eight: N/A
Personnel are advised of security risks posed by non-secure telephone systems in areas where sensitive or classified conversations can occur.

Security Control: ISM-0231; Revision: 2; Updated: Dec-21; Applicability: All; Essential Eight: N/A
When using cryptographic equipment to permit different levels of conversation for different kinds of connections, telephone systems give a visual indication of what kind of connection has been made.

Protecting conversations

When sensitive or classified conversations are held using telephone systems, the conversation needs to be appropriately protected through the use of encryption.

Security Control: ISM-0232; Revision: 3; Updated: Sep-18; Applicability: All; Essential Eight: N/A
Telephone systems used for sensitive or classified conversations encrypt all traffic that passes over external systems.

Cordless telephone systems

Cordless telephone systems have minimal transmission security and are susceptible to interception. Using cordless telephone systems can result in disclosure of information to an unauthorised party through interception.

Security Control: ISM-0233; Revision: 3; Updated: Sep-18; Applicability: All; Essential Eight: N/A
Cordless telephone systems are not used for sensitive or classified conversations.

Speakerphones

As speakerphones are designed to pick up and transmit conversations in the vicinity of the device, using speakerphones in TOP SECRET areas presents a number of security risks and they should not be used. However, if personnel are able to reduce security risks through the use of an audio secure room that is secure during any conversations then they may be used.

Security Control: ISM-0235; Revision: 4; Updated: Dec-21; Applicability: O, P, S, TS; Essential Eight: N/A
Speakerphones are not used on telephone systems in TOP SECRET areas unless the telephone system is located in an audio secure room, the room is audio secure during conversations and only personnel involved in conversations are present in the room.

Off-hook audio protection

Using off-hook protection features minimises the chance of background conversations being accidentally coupled into handsets, headsets and speakerphones. Limiting the time an active microphone is open minimises this security risk.

Security Control: ISM-0236; Revision: 5; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Off-hook audio protection features are used on telephone systems in areas where background conversations may exceed the sensitivity or classification that the telephone system is authorised for communicating.

Security Control: ISM-0931; Revision: 6; Updated: Dec-21; Applicability: O, P, S, TS; Essential Eight: N/A
In SECRET and TOP SECRET areas, push-to-talk handsets or push-to-talk headsets are used to meet any off-hook audio protection requirements.

Further information

Further information on encrypting communications can be found in the cryptographic fundamentals section of the *Guidelines for Cryptography*.

Video conferencing and Internet Protocol telephony

Internet Protocol telephony

This section describes the security controls applicable to Internet Protocol (IP) telephony and extends upon the prior telephone systems section.

Video conferencing and Internet Protocol telephony gateways

Where a video conferencing or IP telephony network is connected to another video conferencing or IP telephony network from a different security domain, the gateways section of the *Guidelines for Gateways* applies.

Where an analog telephone network, such as the Public Switched Telephone Network (PSTN), is connected to a data network, the gateways section of the *Guidelines for Gateways* does not apply.

Video conferencing and Internet Protocol telephony infrastructure hardening

Video conferencing and IP telephony infrastructure can be hardened in order to reduce its attack surface. For example, by ensuring that a Session Initiation Protocol server has a fully patched operating system, uses fully patched software and runs only required services.

Security Control: ISM-1562; Revision: 0; Updated: Dec-19; Applicability: All; Essential Eight: N/A
Video conferencing and IP telephony infrastructure is hardened.

Video-aware and voice-aware firewalls

The use of video-aware and voice-aware firewalls provides network security while supporting video and voice traffic. As such, when a requirement exists to implement a firewall in a gateway, and video conferencing or IP telephony traffic passes through the gateway, a video-aware or voice-aware firewall will need to be used. However, this does not require separate firewalls to be deployed for video conferencing, IP telephony and data traffic. In such cases, an organisation is encouraged to implement one firewall that is video-aware and data-aware; voice-aware and data-aware; or video-aware, voice-aware and data-aware depending on their needs.

Security Control: ISM-0546; Revision: 8; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Where a requirement exists to implement a firewall in a gateway, and video conferencing or IP telephony traffic passes through the gateway, a video-aware or voice-aware firewall is used.

Protecting video conferencing and Internet Protocol telephony traffic

Video conferencing and IP telephony traffic can be vulnerable to eavesdropping, denial-of-service, person-in-the-middle and call spoofing attacks. To mitigate this security risk, video conferencing and IP telephony signalling and audio/video data can be protected with the use of Transport Layer Security. This is achieved through the use of the Session Initiation Protocol Secure protocol and the Secure Real-time Transport Protocol.

Security Control: ISM-0548; Revision: 4; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Video conferencing and IP telephony calls are established using a secure session initiation protocol.

Security Control: ISM-0547; Revision: 4; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Video conferencing and IP telephony calls are conducted using a secure real-time transport protocol.

Video conferencing unit and Internet Protocol phone authentication

Blocking unauthorised or unauthenticated devices by default will reduce the likelihood of unauthorised access to a video conferencing or IP telephony network.

Security Control: ISM-0554; Revision: 1; Updated: Sep-18; Applicability: All; Essential Eight: N/A
An encrypted and non-replayable two-way authentication scheme is used for call authentication and authorisation.

Security Control: ISM-0553; Revision: 3; Updated: Sep-18; Applicability: All; Essential Eight: N/A
Authentication and authorisation is used for all actions on a video conferencing network, including call setup and changing settings.

Security Control: ISM-0555; Revision: 3; Updated: Dec-19; Applicability: All; Essential Eight: N/A
Authentication and authorisation is used for all actions on an IP telephony network, including registering a new IP phone, changing phone users, changing settings and accessing voicemail.

Security Control: ISM-0551; Revision: 7; Updated: Jan-20; Applicability: All; Essential Eight: N/A
IP telephony is configured such that:

- *IP phones authenticate themselves to the call controller upon registration*
- *auto-registration is disabled and only authorised devices are allowed to access the network*
- *unauthorised devices are blocked by default*
- *all unused and prohibited functionality is disabled.*

Security Control: ISM-1014; Revision: 6; Updated: Dec-21; Applicability: S, TS; Essential Eight: N/A
Individual logins are implemented for IP phones used for SECRET or TOP SECRET conversations.

Traffic separation

Video conferencing and IP telephony traffic should be physically or logically separated from other data traffic to ensure its availability and quality of service.

Security Control: ISM-0549; Revision: 4; Updated: Oct-19; Applicability: All; Essential Eight: N/A
Video conferencing and IP telephony traffic is separated physically or logically from other data traffic.

Security Control: ISM-0556; Revision: 5; Updated: Oct-19; Applicability: All; Essential Eight: N/A
Workstations are not connected to video conferencing units or IP phones unless the workstation or the device uses Virtual Local Area Networks or similar mechanisms to maintain separation between video conferencing, IP telephony and other data traffic.

Internet Protocol phones in public areas

IP phones in public areas may give an adversary the opportunity to access data networks or poorly protected voicemail and directory services. As such, any services accessible to IP phones in public areas should be restricted.

Security Control: ISM-0558; Revision: 6; Updated: Dec-21; Applicability: All; Essential Eight: N/A
IP phones used in public areas do not have the ability to access data networks, voicemail and directory services.

Microphones and webcams

Microphones (including headsets and Universal Serial Bus [USB] handsets) and webcams can pose a security risk in SECRET and TOP SECRET areas. Specifically, an adversary can email or host a malicious application on a compromised website and use social engineering techniques to convince users into installing the application on their workstation. Such malicious applications may then activate microphones or webcams that are attached to the workstation to act as remote listening and recording devices.

Security Control: ISM-0559; Revision: 5; Updated: Dec-21; Applicability: O, P; Essential Eight: N/A
Microphones (including headsets and USB handsets) and webcams are not used with non-SECRET workstations in SECRET areas.

Security Control: ISM-1450; Revision: 2; Updated: Dec-21; Applicability: O, P, S; Essential Eight: N/A
Microphones (including headsets and USB handsets) and webcams are not used with non-TOP SECRET workstations in TOP SECRET areas.

Developing a denial of service response plan

Video conferencing and IP telephony services may be a critical service for an organisation. In such cases, a denial of service response plan will assist in responding to denial-of-service attacks against these services.

Security Control: ISM-1019; Revision: 8; Updated: Dec-21; Applicability: All; Essential Eight: N/A
A denial of service response plan is developed and implemented for video conferencing and IP telephony services that includes:

- *how to identify signs of a denial-of-service attack*
- *how to identify the source of a denial-of-service attack*
- *how capabilities can be maintained during a denial-of-service attack*
- *what actions can be taken to respond to a denial-of-service attack.*

Further information

Further information on gateways can be found in the gateways section of the *Guidelines for Gateways*.

Further information on firewalls can be found in the firewalls section of the *Guidelines for Gateways*.

Further information on the use of web conferencing solutions can be found in the Australian Cyber Security Centre's *Web Conferencing Security* publication.

Fax machines and multifunction devices

Using cryptographic equipment with fax machines and multifunction devices

Further information on processes and procedures for sending classified fax messages using High Assurance Cryptographic Equipment can be requested from the Australian Cyber Security Centre.

Fax machine and multifunction device usage policy

As fax machines and multifunction devices (MFDs) are a potential source of cyber security incidents, it is important that an organisation develops a policy governing their use.

Security Control: ISM-0588; Revision: 3; Updated: Aug-19; Applicability: All; Essential Eight: N/A
A fax machine and MFD usage policy is developed and implemented.

Sending fax messages

Once a fax machine or MFD has been connected to cryptographic equipment, and used to send a sensitive or classified fax message, it can no longer be trusted when connected directly to unsecured telecommunications infrastructure, such as the PSTN. For example, if a fax machine fails to send a sensitive or classified fax message the device will continue attempting to send the fax message even if it has been disconnected from cryptographic equipment and re-connected directly to the PSTN. In such cases, the fax machine could send the sensitive or classified fax message in the clear causing a data spill.

Security Control: ISM-1092; Revision: 2; Updated: Sep-18; Applicability: All; Essential Eight: N/A
Separate fax machines or MFDs are used for sending sensitive or classified fax messages and all other fax messages.

Security Control: ISM-0241; Revision: 4; Updated: Dec-21; Applicability: All; Essential Eight: N/A
When sending fax messages, the fax message is encrypted to an appropriate level to be communicated over unsecured telecommunications infrastructure.

Receiving fax messages

While the communications path between fax machines and MFDs may be appropriately protected, personnel should still be aware of who has a need to know of the information being communicated. It is therefore important that fax messages are collected from the receiving fax machine or MFD as soon as possible. Furthermore, if an expected fax message is not received it may indicate that there was a problem with the original transmission or the fax message has been taken by an unauthorised person.

Security Control: ISM-1075; Revision: 2; Updated: Dec-21; Applicability: All; Essential Eight: N/A
The sender of a fax message makes arrangements for the receiver to collect the fax message as soon as possible after it is sent and for the receiver to notify the sender if the fax message does not arrive in an agreed amount of time.

Connecting multifunction devices to networks

As networked MFDs are considered to be devices that reside on networks, they should have security controls of a similar strength to other devices on networks.

Security Control: ISM-0590; Revision: 6; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Security controls for MFDs connected to networks are of a similar strength to those for other devices on networks.

Connecting multifunction devices to both networks and digital telephone systems

When an MFD is connected to both a network and a digital telephone system, the MFD can act as a bridge between the two. The digital telephone system therefore needs to operate at the same sensitivity or classification as the network.

Security Control: ISM-0245; Revision: 5; Updated: Dec-19; Applicability: All; Essential Eight: N/A
A direct connection from an MFD to a digital telephone system is not enabled unless the digital telephone system is authorised to operate at the same sensitivity or classification as the network to which the MFD is connected.

Copying documents on multifunction devices

As networked MFDs are capable of sending scanned or copied documents across connected networks, personnel should be aware that if they scan or copy documents at a level higher than that of networks that devices are connected to it will cause a data spill.

Security Control: ISM-0589; Revision: 6; Updated: Mar-22; Applicability: All; Essential Eight: N/A
MFDs connected to networks are not used to copy documents above the sensitivity or classification of connected networks.

Observing fax machine and multifunction device use

Placing fax machines and MFDs in public areas can help reduce the likelihood of any suspicious use going unnoticed.

Security Control: ISM-1036; Revision: 3; Updated: Sep-18; Applicability: All; Essential Eight: N/A
Fax machines and MFDs are located in areas where their use can be observed.

Further information

Further information on encrypting communications can be found in the cryptographic fundamentals section of the *Guidelines for Cryptography*.

Guidelines for Enterprise Mobility

Mobile device management

Types of mobile devices

These guidelines describe the use and protection of mobile devices, such as smartphones, tablets and laptops. Further guidance for laptops is available in the *Guidelines for System Hardening* and the *Guidelines for System Management*.

Mobile device management policy

Since mobile devices routinely leave the office environment, and the protection it affords, it is important that a mobile device management policy is developed and implemented to ensure that they are sufficiently hardened.

Security Control: ISM-1533; Revision: 2; Updated: Aug-19; Applicability: All; Essential Eight: N/A
A mobile device management policy is developed and implemented.

Security Control: ISM-1195; Revision: 1; Updated: Sep-18; Applicability: All; Essential Eight: N/A
A Mobile Device Management solution is used to ensure mobile device management policy is applied to all mobile devices.

Approval for use

Due to the requirement for the provision of keying material, all mobile devices that process, store or communicate SECRET or TOP SECRET data need to be approved for use by the Australian Cyber Security Centre (ACSC) before keying material will be issued.

Security Control: ISM-0687; Revision: 8; Updated: Dec-21; Applicability: S, TS; Essential Eight: N/A
Mobile devices do not process, store or communicate SECRET or TOP SECRET data until approved for use by the ACSC.

Privately-owned mobile devices

Allowing privately-owned mobile devices to access an organisation’s systems or data can increase liability risk. As such, an organisation should seek legal advice to ascertain whether this scenario affects compliance with relevant legislation, such as the *Privacy Act 1988* and the *Archives Act 1983*, and also consider whether the increased liability risks are acceptable to the organisation.

If an organisation chooses to allow personnel to use a privately-owned mobile device to access their organisation’s systems or data, they should ensure that it does not present an unacceptable security risk. This can be achieved by encouraging the use of an ACSC-approved platform, with a security configuration in accordance with ACSC guidance, along with enforced separation of work data from any personal data.

Security Control: ISM-1297; Revision: 4; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Legal advice is sought prior to allowing privately-owned mobile devices to access systems or data.

Security Control: ISM-1400; Revision: 6; Updated: Dec-21; Applicability: O, P; Essential Eight: N/A
Personnel accessing OFFICIAL and PROTECTED systems or data using a privately-owned mobile device use an ACSC-approved platform, a security configuration in accordance with ACSC guidance and have enforced separation of work data from any personal data.

Security Control: ISM-0694; Revision: 7; Updated: Dec-21; Applicability: S, TS; Essential Eight: N/A
Privately-owned mobile devices do not access SECRET and TOP SECRET systems or data.

Organisation-owned mobile devices

If an organisation chooses to issue personnel with an organisation-owned mobile device to access their organisation's systems or data, they should ensure that it does not present an unacceptable security risk. This can be achieved by using an ACSC-approved platform with a security configuration in accordance with ACSC guidance.

Security Control: ISM-1482; Revision: 5; Updated: Dec-21; Applicability: O, P, S, TS; Essential Eight: N/A
Personnel accessing systems or data using an organisation-owned mobile device use an ACSC-approved platform with a security configuration in accordance with ACSC guidance.

Storage encryption

Encrypting the internal storage, and any removable media, for mobile devices will prevent an adversary from gaining easy access to any sensitive or classified data stored on them if they are lost or stolen.

Security Control: ISM-0869; Revision: 5; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Mobile devices encrypt their internal storage and any removable media.

Communications encryption

If appropriate encryption is not available to protect data in transit, mobile devices communicating sensitive or classified data will present a security risk.

Security Control: ISM-1085; Revision: 4; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Mobile devices encrypt all sensitive or classified data communicated over public network infrastructure.

Bluetooth functionality

To mitigate security risks associated with pairing mobile devices with other Bluetooth devices, Bluetooth version 4.1 introduced the Secure Connections functionality for Bluetooth Classic, while Bluetooth version 4.2 introduced the Secure Connections functionality for Bluetooth Low Energy. This functionality uses keys generated using Elliptic Curve Diffie-Hellman cryptography, thereby offering greater security compared to previous key exchange protocols. In addition, personnel should consider the location and manner in which they pair Bluetooth devices, such as by avoiding pairing devices in public locations, and remove all Bluetooth pairings when there is no longer a requirement for their use.

Finally, the Bluetooth protocol provides inadequate protection for SECRET and TOP SECRET data to be communicated between mobile devices and other Bluetooth devices. As such, Bluetooth functionality is not suitable for use with SECRET and TOP SECRET mobile devices.

Security Control: ISM-1196; Revision: 1; Updated: Sep-18; Applicability: O, P; Essential Eight: N/A
Mobile devices are configured to remain undiscoverable to other Bluetooth devices except during Bluetooth pairing.

Security Control: ISM-1200; Revision: 4; Updated: Dec-21; Applicability: O, P; Essential Eight: N/A
Bluetooth pairing is performed using Secure Connections, preferably with Numeric Comparison if supported.

Security Control: ISM-1198; Revision: 1; Updated: Sep-18; Applicability: O, P; Essential Eight: N/A
Bluetooth pairing is performed in a manner such that connections are only made between intended Bluetooth devices.

Security Control: ISM-1199; Revision: 2; Updated: Dec-21; Applicability: O, P; Essential Eight: N/A
Bluetooth pairings are removed when there is no longer a requirement for their use.

Security Control: ISM-0682; Revision: 5; Updated: Dec-21; Applicability: S, TS; Essential Eight: N/A
Bluetooth functionality is not enabled on SECRET and TOP SECRET mobile devices.

Maintaining mobile device security

Poorly secured mobile devices are more vulnerable to compromise, and provide an adversary with a potential access point into any connected systems. Although an organisation may initially provide secure mobile devices, their security posture may degrade over time if personnel are capable of installing or uninstalling non-approved applications, or disabling or modifying security functionality. Furthermore, it is important that security updates are applied to mobile devices as soon as they become available in order to maintain their security posture.

Security Control: ISM-0863; Revision: 4; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Mobile devices prevent personnel from installing or uninstalling non-approved applications once provisioned.

Security Control: ISM-0864; Revision: 4; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Mobile devices prevent personnel from disabling or modifying security functionality once provisioned.

Security Control: ISM-1366; Revision: 2; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Security updates are applied to mobile devices as soon as they become available.

Connecting mobile devices to the internet

When connecting mobile devices to the internet, best practice involves establishing a Virtual Private Network (VPN) connection to an organisation’s internet gateway rather than a direct connection to the internet. In doing so, mobile devices will be protected by additional security functionality, such as web content filtering, provided by an organisation’s internet gateway.

A split tunnel VPN can allow access into an organisation’s network from other networks, such as the internet. If split tunnelling is not disabled there is an increased security risk that the VPN connection will be susceptible to intrusions from other networks. An organisation can refer to the relevant ACSC security configuration guidance for mobile devices on how to mitigate this security risk.

Security Control: ISM-0874; Revision: 5; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Mobile devices access the internet via a VPN connection to an organisation’s internet gateway rather than via a direct connection to the internet.

Security Control: ISM-0705; Revision: 4; Updated: Dec-21; Applicability: All; Essential Eight: N/A
When accessing an organisation’s network via a VPN connection, split tunnelling is disabled.

Further information

Further information on hardening operating systems for laptops can be found in the operating system hardening section of the *Guidelines for System Hardening*.

Further information on hardening applications for laptops can be found in the application hardening section of the *Guidelines for System Hardening*.

Further information on patching or updating operating systems and applications for laptops can be found in the system patching section of the *Guidelines for System Management*.

Further information on allowing the use of privately-owned mobile devices by personnel to access their organisation’s systems and data can be found in the ACSC’s *Bring Your Own Device for Executives* publication.

Further information and specific guidance on enterprise mobility can be found in the ACSC’s *Risk Management of Enterprise Mobility Including Bring Your Own Device (BYOD)* publication.

Further information on ACSC-approved platforms can be found in the following ACSC publications:

- *Security Configuration Guide – Apple iOS 14 Devices*
- *Security Configuration Guide – Samsung Galaxy S10, S20 and Note 20 Devices*

- *Security Configuration Guide – Viasat Mobile Dynamic Defense*.

Further information on encrypting mobile devices and their communications can be found in the cryptographic fundamentals section of the *Guidelines for Cryptography*.

Further information on Bluetooth security can be found in National Institute of Standards and Technology Special Publication 800-121 Rev. 2, *Guide to Bluetooth Security*.

Mobile device usage

Mobile device usage policy

Since mobile devices routinely leave the office environment, and the protection it affords, it is important that an organisation develops a mobile device usage policy governing their use.

Security Control: ISM-1082; Revision: 2; Updated: Aug-19; Applicability: All; Essential Eight: N/A
A mobile device usage policy is developed and implemented.

Personnel awareness

Mobile devices can have both a voice and data communications component. In such cases, personnel should know the sensitivity or classification of voice and data that mobile devices have been approved to process, store and communicate.

Security Control: ISM-1083; Revision: 2; Updated: Sep-18; Applicability: All; Essential Eight: N/A
Personnel are advised of the sensitivity or classification permitted for voice and data communications when using mobile devices.

Paging, message services and messaging apps

As paging, messaging services and many messaging apps do not sufficiently encrypt data in transit, they cannot be relied upon for the communication of sensitive or classified data.

Security Control: ISM-0240; Revision: 7; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Paging, Multimedia Message Service, Short Message Service and messaging apps are not used to communicate sensitive or classified data.

Using mobile devices in public spaces

Personnel should be aware of the environment in which they use mobile devices to view or communicate sensitive or classified data. In particular, personnel should take care to ensure that sensitive or classified data is not observed by other parties in public areas, such as on public transport, in transit lounges and at coffee shops. In some cases, privacy filters can be applied to the screen of a mobile device to prevent onlookers from reading content off its screen.

In addition, personnel should maintain awareness of the environments from which they conduct sensitive or classified phone calls and the potential for their conversations to be overheard.

Security Control: ISM-0866; Revision: 5; Updated: Jun-21; Applicability: All; Essential Eight: N/A
Sensitive or classified data is not viewed or communicated in public locations unless care is taken to reduce the chance of the screen of a mobile device being observed.

Security Control: ISM-1145; Revision: 4; Updated: Dec-21; Applicability: S, TS; Essential Eight: N/A
Privacy filters are applied to the screens of SECRET and TOP SECRET mobile devices.

Security Control: ISM-1644; Revision: 0; Updated: Jun-21; Applicability: All; Essential Eight: N/A
Sensitive or classified phone calls are not conducted in public locations unless care is taken to reduce the chance of conversations being overheard.

Maintaining control of mobile devices

As mobile devices are portable in nature, and can be easily lost or stolen, it is strongly advised that personnel maintain continual direct supervision of them when they are being actively used and carry or store them in a secured state when they are not being activity used. Note, while mobile devices may be encrypted, the effectiveness of encryption might be reduced if they are lost or stolen while in sleep mode or powered on with a locked screen.

Security Control: ISM-0871; Revision: 3; Updated: Apr-19; Applicability: All; Essential Eight: N/A
Mobile devices are kept under continual direct supervision when being actively used.

Security Control: ISM-0870; Revision: 3; Updated: Apr-19; Applicability: All; Essential Eight: N/A
Mobile devices are carried or stored in a secured state when not being actively used.

Security Control: ISM-1084; Revision: 4; Updated: Dec-21; Applicability: All; Essential Eight: N/A
If unable to carry or store mobile devices in a secured state, they are physically transferred in a security briefcase or an approved multi-use satchel, pouch or transit bag.

Mobile device emergency sanitisation processes and procedures

The sanitisation of mobile devices in emergency situations can assist in reducing the potential for compromise of data by an adversary. This may be achieved through the use of a remote wipe capability or a cryptographic key zeroise or sanitisation function if present.

Security Control: ISM-0701; Revision: 5; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Mobile device emergency sanitisation processes, and supporting mobile device emergency sanitisation procedures, are developed and implemented.

Security Control: ISM-0702; Revision: 5; Updated: Dec-21; Applicability: S, TS; Essential Eight: N/A
If a cryptographic zeroise or sanitise function is provided for cryptographic keys on a SECRET or TOP SECRET mobile device, the function is used as part of mobile device emergency sanitisation processes and procedures.

Before travelling overseas with mobile devices

Personnel travelling overseas with mobile devices face additional security risks compared to travelling domestically, especially when travelling to high or extreme risk countries. As such, appropriate precautions should be taken. Personnel should also be aware that when they leave Australian borders they also leave behind any expectations of privacy.

Security Control: ISM-1298; Revision: 2; Updated: Oct-19; Applicability: All; Essential Eight: N/A
Personnel are advised of privacy and security risks when travelling overseas with mobile devices.

Security Control: ISM-1554; Revision: 1; Updated: Dec-21; Applicability: All; Essential Eight: N/A
If travelling overseas with mobile devices to high or extreme risk countries, personnel are:

- *issued with newly provisioned accounts, mobile devices and removable media from a pool of dedicated travel devices which are used solely for work-related activities*
- *advised on how to apply and inspect tamper seals to key areas of mobile devices*
- *advised to avoid taking any personal mobile devices, especially if rooted or jailbroken.*

Security Control: ISM-1555; Revision: 1; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Before travelling overseas with mobile devices, personnel take the following actions:

- *record all details of the mobile devices being taken, such as product types, serial numbers and International Mobile Equipment Identity numbers*
- *update all operating systems and applications*

- *remove all non-essential accounts, applications and data*
- *apply security configuration settings, such as lock screens*
- *configure remote locate and wipe functionality*
- *enable encryption, including for any removable media*
- *backup all important data and configuration settings.*

While travelling overseas with mobile devices

Personnel lose control of mobile devices and removable media any time they are not on their person. This includes when placing mobile devices and removable media in checked-in luggage or leaving them in hotel rooms (including hotel room safes). In addition, allowing untrusted people to access mobile devices provides an opportunity for them to be tampered with.

Security Control: ISM-1299; Revision: 3; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Personnel take the following precautions when travelling overseas with mobile devices:

- *never leaving mobile devices or removable media unattended for any period of time, including by placing them in checked-in luggage or leaving them in hotel safes*
- *never storing credentials with mobile devices that they grant access to, such as in laptop bags*
- *never lending mobile devices or removable media to untrusted people, even if briefly*
- *never allowing untrusted people to connect their mobile devices or removable media, including for charging*
- *never using designated charging stations, wall outlet charging ports or chargers supplied by untrusted people*
- *avoiding connecting mobile devices to open or untrusted Wi-Fi networks*
- *using a VPN connection to encrypt all mobile device communications*
- *using encrypted messaging apps for communications instead of using foreign telecommunication networks*
- *disabling any communications capabilities of mobile devices when not in use, such as cellular data, wireless, Bluetooth and Near Field Communication*
- *avoiding reuse of removable media once used with other parties' systems or mobile devices*
- *ensuring any removable media used for data transfers are thoroughly checked for malicious code beforehand*
- *never using any gifted mobile devices, especially removable media, when travelling or upon returning from travelling.*

Security Control: ISM-1088; Revision: 5; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Personnel report the potential compromise of mobile devices, removable media or credentials to their organisation as soon as possible, especially if they:

- *provide credentials to foreign government officials*
- *decrypt mobile devices for foreign government officials*
- *have mobile devices taken out of sight by foreign government officials*
- *have mobile devices or removable media stolen that are later returned*
- *lose mobile devices or removable media that are later found*
- *observe unusual behaviour of mobile devices.*

After travelling overseas with mobile devices

Following overseas travel with mobile devices, personnel should take appropriate precautions to ensure that they do not pose an undue security risk to their organisation's systems and data. In most cases, sanitising and resetting mobile devices, including all removable media, will be sufficient. However, upon returning from high or extreme risk countries, additional precautions will likely be needed.

Security Control: ISM-1300; Revision: 5; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Upon returning from travelling overseas with mobile devices, personnel take the following actions:

- *sanitise and reset mobile devices, including all removable media*
- *decommission any physical credentials that left their possession during their travel*
- *report if significant doubt exists as to the integrity of any mobile devices or removable media.*

Security Control: ISM-1556; Revision: 1; Updated: Dec-21; Applicability: All; Essential Eight: N/A
If returning from travelling overseas with mobile devices to high or extreme risk countries, personnel take the following additional actions:

- *reset user credentials used with mobile devices, including those used for remote access to their organisation's systems*
- *monitor accounts for any indicators of compromise, such as failed logon attempts.*

Further information

Further information on usage of mobile devices in SECRET and TOP SECRET areas can be found in the facilities and systems section of the *Guidelines for Physical Security*.

Further information on security briefcases can be found in the Australian Security Intelligence Organisation (ASIO)'s Security Equipment Guide-005, *Briefcases for the Carriage of Security Classified Information*. ASIO's Security Equipment Guide-005 is available from the Protective Security Policy GovTEAMS community or ASIO by email.

Further information on approved multi-use satchels, pouches and transit bags can be found on the Security Construction and Equipment Committee's *Security Equipment Evaluated Products List*.

Further information on travelling overseas with mobile devices can be found in the ACSC's *Travelling Overseas with Electronic Devices* publication.

Guidelines for Evaluated Products

Evaluated product acquisition

Evaluated products

An evaluated product provides a level of assurance in its security functionality that an unevaluated product does not. To assist in providing this assurance, the Australian Cyber Security Centre (ACSC) performs product evaluations through the following programs:

- Enterprise Mobility Evaluation Program: For enterprise mobility products used to protect sensitive or classified data.
- High Assurance Evaluation Program: For products used to protect SECRET and TOP SECRET data.

The Australian Certification Authority within the ACSC also certifies product evaluations conducted by licensed commercial facilities, in accordance with the Common Criteria, as part of the Australian Information Security Evaluation Program (AISEP).

For an organisation seeking to procure evaluated products, the Common Criteria's *Certified Products List* contains a list of products that have been evaluated and certified in accordance with the Common Criteria. Alternatively, the ACSC can be contacted for information on both products that are in-evaluation as well as those that have completed evaluation via the Enterprise Mobility Evaluation Program or the High Assurance Evaluation Program.

Cryptographic evaluations

The Common Criteria leverages the Cryptographic Algorithm Validation Program for the evaluation of cryptographic algorithms used by cryptographic modules within evaluated products. All cryptographic evaluations are performed by Cryptographic and Security Testing laboratories that are accredited by the United States' National Voluntary Laboratory Accreditation Program to International Organization for Standardization/International Electrotechnical Commission 17025:2017, *General requirements for the competence of testing and calibration laboratories*.

Protection Profiles

A Protection Profile (PP) is a technology-specific document that defines the security functionality that must be included in a Common Criteria evaluated product to mitigate specific cyber threats. PPs can be published by a recognised Common Criteria Recognition Arrangement (CCRA) scheme or by the CCRA body itself. PPs published by the CCRA body are referred to as collaborative PPs.

The ACSC recognises all PPs listed on the Common Criteria website in addition to those listed on the ACSC's website. Where a PP does not exist, an evaluation based on an Evaluation Assurance Level (EAL) may be accepted. Such evaluations are capped at EAL2+ as this represents the best balance between completion time and meaningful security assurance gains.

Evaluation documentation

An organisation choosing to use Common Criteria evaluated products can determine their suitability by reviewing their evaluation documentation. This includes the security target and certification report.

Products that are undergoing a Common Criteria evaluation will not have published evaluation documentation. However, documentation can be obtained from the ACSC if a product is being evaluated through the AISEP. For a product that is in evaluation through a foreign scheme, the product's vendor can be contacted directly for further information.

Evaluated product selection

A Common Criteria evaluation is traditionally conducted at a specified EAL. However, evaluations against a PP exist outside of this scale. Notably, while products evaluated against a PP will fulfil the Common Criteria EAL requirements, the EAL number will not be published.

Security Control: ISM-0280; Revision: 7; Updated: Sep-19; Applicability: All; Essential Eight: N/A
If procuring an evaluated product, a product that has completed a PP-based evaluation is selected in preference to one that has completed an EAL-based evaluation.

Delivery of evaluated products

It is important that an organisation ensures that products they purchase are the actual products that are delivered. In the case of evaluated products, if the product delivered differs from an evaluated version then the assurance gained from the evaluation may not necessarily apply.

Packaging and delivery practices can vary greatly from product to product. For most evaluated products, standard commercial packaging and delivery practices are likely to be sufficient. However, in some cases more secure packaging and delivery practices, including tamper-evident seals and secure transportation, may be required. In the case of the digital delivery of evaluated products, vendor-supplied checksums can often be used to ensure the integrity of software that was delivered.

Security Control: ISM-0285; Revision: 1; Updated: Sep-18; Applicability: All; Essential Eight: N/A
Evaluated products are delivered in a manner consistent with any delivery procedures defined in associated evaluation documentation.

Security Control: ISM-0286; Revision: 6; Updated: Dec-21; Applicability: S, TS; Essential Eight: N/A
When procuring high assurance ICT equipment, the ACSC is contacted for any equipment-specific delivery procedures.

Further information

Further information on the High Assurance Evaluation Program is available from the ACSC.

Further information on the AISEP is available from the ACSC.

Further information on Common Criteria evaluated products can be found on the Common Criteria's *Certified Products List*.

Evaluated product usage

Evaluated configuration

An evaluated product is considered to be operating in an evaluated configuration if:

- functionality that it uses was in the scope of the evaluation and it is implemented in the specified manner
- only product updates that have been assessed through maintenance and re-evaluation activities (known as assurance continuity) have been applied
- the environment complies with assumptions or organisational security policies stated in the evaluation documentation.

Unevaluated configuration

An evaluated product is considered to be operating in an unevaluated configuration when it does not meet the requirements of the evaluated configuration and guidance provided in its certification report.

Patching evaluated products

In the majority of cases, the latest patched version of an evaluated product will be more secure than an older unpatched version. While the application of patches will not normally place an evaluated product into an unevaluated configuration, some vendors may include new functionality which has not been evaluated with their patches. In such cases, an organisation should use their judgement to determine whether this deviation from the evaluated configuration constitutes additional security risk or not.

Installation and configuration of evaluated products

Product evaluation provides assurance that a product's security functionality will work as expected when operating in a clearly defined configuration. The scope of the evaluation specifies the security functionality that can be used and how a product is to be configured and operated. Using an evaluated product in an unevaluated configuration could result in the introduction of security risks that were not considered as part of the product's evaluation.

Security Control: ISM-0289; Revision: 2; Updated: Sep-18; Applicability: All; Essential Eight: N/A
Evaluated products are installed, configured, administered and operated in accordance with vendor guidance and evaluation documentation.

Security Control: ISM-0290; Revision: 6; Updated: Dec-21; Applicability: S, TS; Essential Eight: N/A
High assurance ICT equipment is installed, configured, administered and operated in accordance with guidance produced by the ACSC.

Use of high assurance ICT equipment in unevaluated configurations

Given the value of data being protected by high assurance ICT equipment, it should always be operated in an evaluated configuration.

Security Control: ISM-0292; Revision: 6; Updated: Dec-21; Applicability: S, TS; Essential Eight: N/A
High assurance ICT equipment is always operated in an evaluated configuration.

Further information

Further information on patching or updating ICT equipment can be found in the system patching section of the *Guidelines for System Management*.

Further information on the installation, configuration, administration and operation of Common Criteria products is available from vendors and can be found in evaluation documentation on the Common Criteria's *Certified Products List*.

For information on the installation, configuration, administration and operation of high assurance ICT equipment is available from the ACSC.

Guidelines for ICT Equipment

ICT equipment usage

ICT equipment management policy

Since ICT equipment is capable of processing, storing or communicating sensitive or classified data, it is important that an ICT equipment management policy is developed and implemented to ensure that ICT equipment, and the data it processes, stores or communicates, is protected in an appropriate manner.

Security Control: ISM-1551; Revision: 0; Updated: Aug-19; Applicability: All; Essential Eight: N/A
An ICT equipment management policy is developed and implemented.

ICT equipment register

Maintaining and regularly verifying a register of authorised ICT equipment can assist an organisation in tracking legitimate ICT equipment as well as determining whether unauthorised ICT equipment, such as workstations, servers and network devices, have been introduced into their organisation.

Security Control: ISM-0336; Revision: 6; Updated: Mar-22; Applicability: All; Essential Eight: N/A
An ICT equipment register is maintained and verified on a regular basis.

Labelling ICT equipment

Applying protective markings to ICT equipment assists to reduce the likelihood that a user will accidentally input data into it that it is not approved for processing, storing or communicating.

While text-based protective markings are typically used for labelling ICT equipment, there may be circumstances where colour-based protective markings or other marking schemes need to be used instead. In such cases, the marking scheme will need to be documented and personnel will need to be trained in its use.

Security Control: ISM-0294; Revision: 4; Updated: Sep-18; Applicability: All; Essential Eight: N/A
ICT equipment, with the exception of high assurance ICT equipment, is labelled with protective markings reflecting its sensitivity or classification.

Labelling high assurance ICT equipment

High assurance ICT equipment often has tamper-evident seals placed on its external surfaces. To assist users in noticing changes to these seals, and to prevent functionality being degraded, an organisation should limit the use of labels on high assurance ICT equipment.

Security Control: ISM-0296; Revision: 5; Updated: Dec-21; Applicability: S, TS; Essential Eight: N/A
The Australian Cyber Security Centre (ACSC)'s approval is sought before applying labels to external surfaces of high assurance ICT equipment.

Classifying ICT equipment

The purpose of classifying ICT equipment is to acknowledge the sensitivity or classification of data that it is approved for processing, storing or communicating.

Classifying ICT equipment also assists in ensuring that the appropriate sanitisation, destruction and disposal processes are followed at the end of its life.

Security Control: ISM-0293; Revision: 5; Updated: Jun-21; Applicability: All; Essential Eight: N/A

ICT equipment is classified based on the highest sensitivity or classification of data that it is approved for processing, storing or communicating.

Handling ICT equipment

When ICT equipment displays, processes, stores or communicates sensitive or classified data, it will need to be handled as per the sensitivity or classification of that data. However, applying encryption to media within the ICT equipment may change the manner in which it needs to be handled. Any change in handling needs to be based on the original sensitivity or classification of data residing on media within the ICT equipment and the level of assurance in the cryptographic equipment or software being used to encrypt it.

Security Control: ISM-1599; Revision: 0; Updated: Aug-20; Applicability: All; Essential Eight: N/A
ICT equipment is handled in a manner suitable for its sensitivity or classification.

Further information

Further information on securing ICT equipment when not in use can be found in the ICT equipment and media section of the *Guidelines for Physical Security*.

Further information on encrypting media within ICT equipment can be found in the cryptographic fundamentals section of the *Guidelines for Cryptography*.

Further information on the protection of ICT equipment can be found in the Attorney-General’s Department’s *Protective Security Policy Framework*, *Physical security for entity resources* policy.

ICT equipment maintenance and repairs

Maintenance and repairs of high assurance ICT equipment

Due to the nature of high assurance ICT equipment, it is important that that ACSC’s approval is sought before any maintenance or repairs are undertaken.

Security Control: ISM-1079; Revision: 5; Updated: Dec-21; Applicability: S, TS; Essential Eight: N/A
The ACSC’s approval is sought before undertaking any maintenance or repairs to high assurance ICT equipment.

On-site maintenance and repairs

Undertaking unauthorised maintenance or repairs to ICT equipment could impact its integrity. As such, using appropriately cleared technicians to maintain and repair ICT equipment on site is considered the most secure approach. This ensures that if data is disclosed during the course of maintenance or repairs, the technicians are aware of the requirements to protect such data.

An organisation choosing to use uncleared technicians to maintain or repair ICT equipment should be aware of the requirement for cleared personnel to escort uncleared technicians during maintenance or repair activities.

Security Control: ISM-0305; Revision: 6; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Maintenance and repairs of ICT equipment is carried out on site by an appropriately cleared technician.

Security Control: ISM-0307; Revision: 2; Updated: Sep-18; Applicability: All; Essential Eight: N/A
If an uncleared technician is used to undertake maintenance or repairs of ICT equipment, the ICT equipment and associated media is sanitised before maintenance or repair work is undertaken.

Security Control: ISM-0306; Revision: 5; Updated: Jun-21; Applicability: All; Essential Eight: N/A
If an uncleared technician is used to undertake maintenance or repairs of ICT equipment, the technician is escorted by someone who:

- *is appropriately cleared and briefed*

- *takes due care to ensure that data is not disclosed*
- *takes all responsible measures to ensure the integrity of the ICT equipment*
- *has the authority to direct the technician*
- *is sufficiently familiar with the ICT equipment to understand the work being performed.*

Off-site maintenance and repairs

An organisation choosing to have ICT equipment maintained or repaired off site should do so at facilities approved for handling the sensitivity or classification of the ICT equipment. However, an organisation may be able to sanitise the ICT equipment prior to transport, and subsequent maintenance or repair activities, to change how it needs to be handled.

Security Control: ISM-0310; Revision: 7; Updated: Mar-22; Applicability: All; Essential Eight: N/A
ICT equipment maintained or repaired off site is done so at facilities approved for handling the sensitivity or classification of the ICT equipment.

Inspection of ICT equipment following maintenance and repairs

Following the maintenance or repair of ICT equipment, it is important that the ICT equipment is inspected to ensure that it retains its approved software configuration and that no unauthorised modifications have been made by technicians.

Security Control: ISM-1598; Revision: 0; Updated: Aug-20; Applicability: All; Essential Eight: N/A
Following maintenance or repair activities for ICT equipment, the ICT equipment is inspected to confirm it retains its approved software configuration and that no unauthorised modifications have taken place.

Further information

Further information on the sanitisation of media can be found in the media sanitisation section of the *Guidelines for Media*.

ICT equipment sanitisation and destruction

ICT equipment sanitisation processes and procedures

Documenting processes and procedures for ICT equipment sanitisation will ensure that an organisation carries out ICT equipment sanitisation in an appropriate and consistent manner.

Security Control: ISM-0313; Revision: 5; Updated: Dec-21; Applicability: All; Essential Eight: N/A
ICT equipment sanitisation processes, and supporting ICT equipment sanitisation procedures, are developed and implemented.

ICT equipment destruction processes and procedures

Documenting processes and procedures for ICT equipment destruction will ensure that an organisation carries out ICT equipment destruction in an appropriate and consistent manner.

Security Control: ISM-1741; Revision: 0; Updated: Mar-22; Applicability: All; Essential Eight: N/A
ICT equipment destruction processes, and supporting ICT equipment destruction procedures, are developed and implemented.

Sanitising ICT equipment

When sanitising ICT equipment, any media within the ICT equipment should be removed or sanitised. Once any media has been removed or sanitised, ICT equipment can be considered sanitised. However, if media cannot be removed or sanitised, the ICT equipment should be destroyed as per media destruction requirements.

Media typically found in ICT equipment includes:

- electrostatic memory devices, such as laser printer cartridges used in multifunction devices (MFDs)
- non-volatile magnetic memory, such as hard disks
- non-volatile semiconductor memory, such as flash cards and solid state drives
- volatile memory, such as random-access memory sticks.

Security Control: ISM-0311; Revision: 6; Updated: Mar-22; Applicability: All; Essential Eight: N/A
ICT equipment containing media is sanitised by removing the media from the ICT equipment or by sanitising the media in situ.

Security Control: ISM-1742; Revision: 0; Updated: Mar-22; Applicability: All; Essential Eight: N/A
ICT equipment that cannot be sanitised is destroyed.

Sanitising highly sensitive ICT equipment

ICT equipment located overseas that has processed, stored or communicated Australian Eyes Only (AUSTEO) or Australian Government Access Only (AGAO) data can have more severe consequences for Australian interests if not sanitised appropriately.

Security Control: ISM-1218; Revision: 4; Updated: Dec-21; Applicability: S, TS; Essential Eight: N/A
ICT equipment, including associated media, that is located overseas and has processed, stored or communicated AUSTEO or AGAO data, is sanitised in situ.

Security Control: ISM-0312; Revision: 6; Updated: Dec-21; Applicability: S, TS; Essential Eight: N/A
ICT equipment, including associated media, that is located overseas and has processed, stored or communicated AUSTEO or AGAO data that cannot be sanitised in situ, is returned to Australia for destruction.

Destroying high assurance ICT equipment

Due to the nature of high assurance ICT equipment, and many of the protective mechanisms it employs, sanitisation alone is not sufficient prior to its disposal. As such, all high assurance ICT equipment should be destroyed prior to its disposal.

Security Control: ISM-0315; Revision: 8; Updated: Mar-22; Applicability: S, TS; Essential Eight: N/A
High assurance ICT equipment is destroyed prior to its disposal.

Sanitising printers and multifunction devices

When sanitising printers and MFDs, the printer cartridge or MFD print drum should be sanitised in addition to the removal or sanitisation of any media. This can be achieved by printing random text with no blank areas on each colour printer cartridge or MFD print drum. In addition, image transfer rollers and platens can become imprinted with text and images over time and should be destroyed if any text or images have been retained. Finally, any paper jammed in the paper path should be removed.

When printer cartridges and MFD print drums cannot be sanitised due to a hardware failure, or when they are empty, there is no other option available but to destroy them. Printer ribbons cannot be sanitised and should be destroyed.

Security Control: ISM-0317; Revision: 3; Updated: Sep-18; Applicability: All; Essential Eight: N/A

At least three pages of random text with no blank areas are printed on each colour printer cartridge or MFD print drum.

Security Control: ISM-1219; Revision: 2; Updated: Dec-21; Applicability: All; Essential Eight: N/A
MFD print drums and image transfer rollers are inspected and destroyed if there is remnant toner which cannot be removed or a print is visible on the image transfer roller.

Security Control: ISM-1220; Revision: 2; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Printer and MFD platens are inspected and destroyed if any text or images are retained on the platen.

Security Control: ISM-1221; Revision: 1; Updated: Sep-18; Applicability: All; Essential Eight: N/A
Printers and MFDs are checked to ensure no pages are trapped in the paper path due to a paper jam.

Security Control: ISM-0318; Revision: 3; Updated: Sep-18; Applicability: All; Essential Eight: N/A
When unable to sanitise printer cartridges or MFD print drums, they are destroyed as per electrostatic memory devices.

Security Control: ISM-1534; Revision: 0; Updated: Sep-18; Applicability: All; Essential Eight: N/A
Printer ribbons in printers and MFDs are removed and destroyed.

Sanitising televisions and computer monitors

All types of televisions and computer monitors are capable of retaining data if mitigating measures are not taken during their lifetime. Cathode Ray Tube monitors and plasma screens can be affected by burn-in while Liquid Crystal Display and Organic Light Emitting Diode screens can be affected by image persistence.

Televisions and computer monitors can be visually inspected by turning up the brightness and contrast to their maximum level to determine if any data has been burnt into or persists on the screen. If burn-in or image persistence is removed by this activity, televisions and computer monitors can be considered sanitised. However, if burn-in or persistence is not removed through these measures, televisions and computer monitors cannot be sanitised and should be destroyed.

If televisions or computer monitors cannot be powered on, such as due to a faulty power supply, they cannot be sanitised and should be destroyed.

Security Control: ISM-1076; Revision: 2; Updated: Sep-18; Applicability: All; Essential Eight: N/A
Televisions and computer monitors with minor burn-in or image persistence are sanitised by displaying a solid white image on the screen for an extended period of time.

Security Control: ISM-1222; Revision: 1; Updated: Sep-18; Applicability: All; Essential Eight: N/A
Televisions and computer monitors that cannot be sanitised are destroyed.

Sanitising network devices

As network devices can store network configuration data or credentials in their memory, the memory should be sanitised prior to the disposal of the network devices. The correct method to sanitise network devices will depend on their configuration and the type of memory they use. As such, device-specific guidance provided in evaluation documentation, or vendor sanitisation guidance, should be consulted to determine the most appropriate method to sanitise memory in network devices.

Security Control: ISM-1223; Revision: 6; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Memory in network devices is sanitised using the following processes, in order of preference:

- *following device-specific guidance provided in evaluation documentation*
- *following vendor sanitisation guidance*
- *loading a dummy configuration file, performing a factory reset and then reinstalling firmware.*

Sanitising fax machines

As fax machines can store pages that are ready for transmission in their memory, the memory should be sanitised prior to the disposal of the fax machines. This can be achieved by removing the paper tray, transmitting a fax message with a minimum length of four pages, then re-installing the paper tray and allowing a fax summary page to be printed. In addition, any paper that becomes trapped in the paper path should be removed prior to disposal.

Security Control: ISM-1225; Revision: 2; Updated: Sep-18; Applicability: All; Essential Eight: N/A
The paper tray of the fax machine is removed, and a fax message with a minimum length of four pages is transmitted, before the paper tray is re-installed to allow a fax summary page to be printed.

Security Control: ISM-1226; Revision: 2; Updated: Sep-18; Applicability: All; Essential Eight: N/A
Fax machines are checked to ensure no pages are trapped in the paper path due to a paper jam.

Further information

Further information on the sanitisation of media can be found in the media sanitisation section of the *Guidelines for Media*.

Further information on the destruction of media can be found in the media destruction section of the *Guidelines for Media*.

Further information on the sanitisation of network devices is available from vendors and can be found in evaluation documentation on the Common Criteria's *Certified Products List*.

ICT equipment disposal

ICT equipment disposal processes and procedures

Documenting processes and procedures for ICT equipment disposal will ensure that an organisation carries out ICT equipment disposal in an appropriate and consistent manner.

Security Control: ISM-1550; Revision: 1; Updated: Dec-21; Applicability: All; Essential Eight: N/A
ICT equipment disposal processes, and supporting ICT equipment disposal procedures, are developed and implemented.

Disposal of ICT equipment

Before ICT equipment can be released into the public domain, it needs to be sanitised, destroyed or declassified. As sanitised, destroyed or declassified ICT equipment still presents a security risk, albeit very minor, an appropriate authority needs to formally authorise its release into the public domain. Furthermore, as part of disposal processes, removing labels and markings indicating the owner, sensitivity, classification or any other marking that can associate ICT equipment with its prior use will ensure it does not draw undue attention following its disposal.

Security Control: ISM-1217; Revision: 2; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Labels and markings indicating the owner, sensitivity, classification or any other marking that can associate ICT equipment with its prior use are removed prior to its disposal.

Security Control: ISM-0321; Revision: 4; Updated: Dec-21; Applicability: S, TS; Essential Eight: N/A
When disposing of ICT equipment that has been designed or modified to meet emanation security standards, the ACSC is contacted for requirements relating to its disposal.

Security Control: ISM-0316; Revision: 3; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Following sanitisation, destruction or declassification, a formal administrative decision is made to release ICT equipment, or its waste, into the public domain.

Guidelines for Media

Media usage

Media management policy

Since media is capable of storing sensitive or classified data, it is important that a media management policy is developed and implemented to ensure that all types of media, and the data it stores, is protected in an appropriate manner. In many cases, an organisation's media management policy will be closely tied to their removable media usage policy.

Security Control: ISM-1549; Revision: 0; Updated: Aug-19; Applicability: All; Essential Eight: N/A
A media management policy is developed and implemented.

Removable media usage policy

Establishing a removable media usage policy can decrease the likelihood and consequence of data spills, data loss and data theft. In doing so, a removable media usage policy will likely cover the following:

- permitted types and uses of removable media
- registration and labelling of removable media
- handling and protection of removable media
- reporting of lost or stolen removable media
- sanitisation or destruction of removable media at the end of its life.

Security Control: ISM-1359; Revision: 3; Updated: Aug-19; Applicability: All; Essential Eight: N/A
A removable media usage policy is developed and implemented.

Removable media register

Maintaining and regularly verifying a register of removable media can assist an organisation in tracking and accounting for authorised removable media as well as identifying any non-authorised removal media in use within their organisation.

Security Control: ISM-1713; Revision: 1; Updated: Mar-22; Applicability: All; Essential Eight: N/A
A removable media register is maintained and verified on a regular basis.

Labelling media

Labelling media helps personnel to identify its sensitivity or classification and ensure that appropriate measures are applied to its storage, handling and use.

While text-based protective markings are typically used for labelling media, there may be circumstances where colour-based protective markings or other marking schemes need to be used instead. In such cases, the marking scheme will need to be documented and personnel will need to be trained in its use.

Security Control: ISM-0332; Revision: 4; Updated: Sep-18; Applicability: All; Essential Eight: N/A
Media, with the exception of internally mounted fixed media within ICT equipment, is labelled with protective markings reflecting its sensitivity or classification.

Classifying media

Media that is not correctly classified could be stored and handled inappropriately, accessed by personnel who do not have an appropriate security clearance or used with systems it is not authorised to be used with.

Security Control: ISM-0323; Revision: 8; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Media is classified to the highest sensitivity or classification of data it stores, unless the media has been classified to a higher sensitivity or classification.

Security Control: ISM-0337; Revision: 6; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Media is only used with systems that are authorised to process, store or communicate its sensitivity or classification.

Reclassifying media

Some activities may necessitate or allow for a change to the sensitivity or classification of media. For example, when media is connected to a system that lacks a mechanism through which read-only access can be ensured, when media is sanitised or destroyed, or when data stored on media is subject to a sensitivity or classification change.

Security Control: ISM-0325; Revision: 6; Updated: Apr-21; Applicability: All; Essential Eight: N/A
Any media connected to a system with a higher sensitivity or classification than the media is reclassified to the higher sensitivity or classification, unless the media is read-only or the system has a mechanism through which read-only access can be ensured.

Security Control: ISM-0330; Revision: 7; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Before reclassifying media to a lower sensitivity or classification, the media is sanitised or destroyed, and a formal administrative decision is made to reclassify it.

Handling media

As media can be easily misplaced or stolen, measures should be put in place to protect data stored on it. In some cases, applying encryption to media may change the manner in which it needs to be handled. Any change in handling needs to be based on the original sensitivity or classification of the media and the level of assurance in the cryptographic equipment or software being used to encrypt it.

Security Control: ISM-0831; Revision: 5; Updated: Sep-18; Applicability: All; Essential Eight: N/A
Media is handled in a manner suitable for its sensitivity or classification.

Security Control: ISM-1059; Revision: 4; Updated: Dec-21; Applicability: All; Essential Eight: N/A
All data stored on media is encrypted.

Sanitising media before first use

Sanitising media before first use can assist in reducing cyber supply chain risks, such as new media containing malicious code. In addition, sanitising media before first use in a different security domain can prevent potential data spills from occurring.

Security Control: ISM-1600; Revision: 1; Updated: Apr-21; Applicability: All; Essential Eight: N/A
Media is sanitised before it is used for the first time.

Security Control: ISM-1642; Revision: 0; Updated: Apr-21; Applicability: All; Essential Eight: N/A
Media is sanitised before it is reused in a different security domain.

Using media for data transfers

An organisation transferring data between systems belonging to different security domains is strongly encouraged to use write-once media. When done properly, such as using non-rewritable compact discs that have been finalised, this will ensure that data from the destination system cannot be accidently transferred, or maliciously exfiltrated, onto the media used for the data transfer and then onto another system, such as the original source system. Alternatively, if suitable write-once media is not used, the destination system should have a mechanism through which read-only access can be ensured, such as via a read-only device or hardware write-blocker. However, the use of read-only mechanisms is not immune to failure or compromise, therefore, rewritable media should still be sanitised following each data transfer.

It is important to note that for most non-volatile flash memory media, it will be possible to sanitise and reclassify it following a data transfer in order to allow it to be connected to other systems again. This is not possible for SECRET and TOP SECRET non-volatile flash memory media as it cannot be reclassified following sanitisation.

Security Control: ISM-0347; Revision: 5; Updated: Apr-21; Applicability: All; Essential Eight: N/A
When transferring data manually between two systems belonging to different security domains, write-once media is used unless the destination system has a mechanism through which read-only access can be ensured.

Security Control: ISM-0947; Revision: 6; Updated: Apr-21; Applicability: All; Essential Eight: N/A
When transferring data manually between two systems belonging to different security domains, rewritable media is sanitised after each data transfer.

Further information

Further information on the protection of media can be found in the Attorney-General's Department's *Protective Security Policy Framework*, *Physical security for entity resources* policy.

Further information on securing media when not in use can be found in the ICT equipment and media section of the *Guidelines for Physical Security*.

Further information on encrypting media can be found in the cryptographic fundamentals section of the *Guidelines for Cryptography*.

Further information on using media to transfer data between systems can be found in the data transfers section of the *Guidelines for Data Transfers*.

Media sanitisation

Hybrid hard drives

When sanitising hybrid hard drives, separate the non-volatile magnetic media from the circuit board containing non-volatile flash memory media and sanitise each separately.

Solid state drives

When sanitising solid state drives, the method for sanitising non-volatile flash memory media applies.

Media sanitisation processes and procedures

Using approved methods to sanitise media provides a level of assurance that, to the extent possible, no data will be left following sanitisation. The methods described in these guidelines are designed not only to prevent common data recovery practices but also to protect from those that could emerge in the future.

Security Control: ISM-0348; Revision: 4; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Media sanitisation processes, and supporting media sanitisation procedures, are developed and implemented.

Volatile media sanitisation

When sanitising volatile media, the specified time to wait following the removal of power is based on applying a safety factor to the time recommended by research into preventing the recovery of data. If read back cannot be achieved following the overwriting of volatile media, or data persists, it will need to be destroyed.

Security Control: ISM-0351; Revision: 6; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Volatile media is sanitised by removing its power for at least 10 minutes.

Security Control: ISM-0352; Revision: 4; Updated: Dec-21; Applicability: S, TS; Essential Eight: N/A
SECRET and TOP SECRET volatile media is sanitised by overwriting it at least once in its entirety with a random pattern followed by a read back for verification.

Treatment of volatile media following sanitisation

Research suggests that short-term remanence effects are likely in volatile media. For example, up to minutes at normal room temperatures and up to hours in extremely cold temperatures. Furthermore, some volatile media can suffer from long-term remanence effects resulting from physical changes due to the continuous storage of static data for extended periods of time. It is for these reasons that under certain circumstances TOP SECRET volatile media retains its classification following sanitisation.

Typical circumstances preventing the reclassification of TOP SECRET volatile media include a static cryptographic key being stored in the same memory location during every boot of a device, or a static image being displayed on a device and stored in volatile media for a period of months.

Security Control: ISM-0835; Revision: 4; Updated: Dec-21; Applicability: TS; Essential Eight: N/A
Following sanitisation, TOP SECRET volatile media retains its classification if it stored static data for an extended period of time, or had data repeatedly stored on or written to the same memory location for an extended period of time.

Non-volatile magnetic media sanitisation

Non-volatile magnetic media encompasses non-volatile magnetic hard drives, tape drives and floppy disks. While non-volatile magnetic tape drives and floppy disks can be sanitised by overwriting them at least once (or three times if pre-2001 or under 15 GB) in their entirety with a random pattern followed by a read back for verification, additional considerations apply to non-volatile magnetic hard drives due to their use of a host-protected area, device configuration overlay table and growth defects table.

Both the host-protected area and device configuration overlay table of non-volatile magnetic hard drives are normally not visible to a computer's Unified Extensible Firmware Interface or operating system. Therefore, any sanitisation of the readable sectors of non-volatile magnetic hard drives will leave any data contained in sectors listed in the host-protected area and device configuration overlay table untouched. Some sanitisation programs include the ability to reset non-volatile magnetic hard drives to their default state, thereby removing any host-protected areas or device configuration overlays. This allows the sanitisation program to see the entire contents of non-volatile magnetic hard drives during subsequent sanitisation processes.

Modern non-volatile magnetic hard drives automatically reallocate space for bad sectors at a hardware level. These bad sectors are maintained in what is known as the growth defects table or 'g-list'. If data was stored in a sector that was subsequently added to the growth defects table, sanitising the non-volatile magnetic hard drive will not overwrite such data. While these sectors may be considered bad by non-volatile magnetic hard drives, quite often this is due to the sectors no longer meeting expected performance norms and not due to an inability to read or write to them. The Advanced Technology Attachment (ATA) secure erase command was built into the firmware of post-2001 non-volatile magnetic hard drives and is able to access sectors that have been added to the growth defects table.

Modern non-volatile magnetic hard drives also contain a primary defects table or 'p-list'. The primary defects table contains a list of bad sectors found during post-production processes. No data is ever stored in sectors listed in the primary defects table as they are marked as inaccessible before non-volatile magnetic hard drives are used for the first time.

Security Control: ISM-0354; Revision: 6; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Non-volatile magnetic media is sanitised by overwriting it at least once (or three times if pre-2001 or under 15 GB) in its entirety with a random pattern followed by a read back for verification.

Security Control: ISM-1065; Revision: 3; Updated: Dec-21; Applicability: All; Essential Eight: N/A
The host-protected area and device configuration overlay table are reset prior to the sanitisation of non-volatile magnetic hard drives.

Security Control: ISM-1067; Revision: 4; Updated: Dec-21; Applicability: All; Essential Eight: N/A
The ATA secure erase command is used, in addition to block overwriting software, to ensure the growth defects table of non-volatile magnetic hard drives is overwritten.

Treatment of non-volatile magnetic media following sanitisation

Due to concerns with the sanitisation processes for non-volatile magnetic media, SECRET and TOP SECRET non-volatile magnetic media retains its classification following sanitisation.

Security Control: ISM-0356; Revision: 6; Updated: Dec-21; Applicability: S, TS; Essential Eight: N/A
Following sanitisation, SECRET and TOP SECRET non-volatile magnetic media retains its classification.

Non-volatile erasable programmable read-only memory media sanitisation

When sanitising non-volatile erasable programmable read-only memory (EPROM), three times the manufacturer’s specification for ultraviolet erasure time should be applied to provide additional certainty in sanitisation processes.

Security Control: ISM-0357; Revision: 5; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Non-volatile EPROM media is sanitised by applying three times the manufacturer’s specified ultraviolet erasure time and then overwriting it at least once in its entirety with a random pattern followed by a read back for verification.

Non-volatile electrically erasable programmable read-only memory media sanitisation

A single overwrite with a random pattern is considered suitable for sanitising non-volatile electrically erasable programmable read-only memory (EEPROM) media.

Security Control: ISM-0836; Revision: 3; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Non-volatile EEPROM media is sanitised by overwriting it at least once in its entirety with a random pattern followed by a read back for verification.

Treatment of non-volatile erasable and electrically erasable programmable read-only memory media following sanitisation

As little research has been conducted into the recovery of data from non-volatile EPROM and EEPROM media, SECRET and TOP SECRET EPROM and EEPROM media retains its classification following sanitisation.

Security Control: ISM-0358; Revision: 6; Updated: Dec-21; Applicability: S, TS; Essential Eight: N/A
Following sanitisation, SECRET and TOP SECRET non-volatile EPROM and EEPROM media retains its classification.

Non-volatile flash memory media sanitisation

For non-volatile flash memory media, a technique known as wear levelling ensures that writes are distributed evenly across each memory block. This feature necessitates non-volatile flash memory media being overwritten with a random pattern twice as this helps to ensure that all memory blocks are overwritten.

Security Control: ISM-0359; Revision: 4; Updated: Dec-21; Applicability: All; Essential Eight: N/A

Non-volatile flash memory media is sanitised by overwriting it at least twice in its entirety with a random pattern followed by a read back for verification.

Treatment of non-volatile flash memory media following sanitisation

Due to the use of wear levelling in non-volatile flash memory media, and the potentially for bad memory blocks, it is possible that not all memory blocks will be overwritten during sanitisation processes. For this reason, SECRET and TOP SECRET non-volatile flash memory media retains its classification following sanitisation.

Security Control: ISM-0360; Revision: 6; Updated: Dec-21; Applicability: S, TS; Essential Eight: N/A
Following sanitisation, SECRET and TOP SECRET non-volatile flash memory media retains its classification.

Media that cannot be successfully sanitised

In some cases, sanitisation processes will be unsuccessful due to faulty or damaged media. In such cases, the faulty or damage media will need to be destroyed prior to its disposal.

Security Control: ISM-1735; Revision: 0; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Faulty or damaged media that cannot be successfully sanitised is destroyed prior to its disposal.

Further information

Further information on recoverability of data from volatile media can be found in the *Data Remanence in Semiconductor Devices* paper.

Further information on the random-access memory testing tool MemTest86 can be obtained from PassMark Software.

Further information on the graphics card random-access memory testing tools MemtestG80 and MemtestCL can be obtained from their GitHub projects.

Further information on HDDerase is available from the Center for Memory and Recording Research at the University of California San Diego. HDDerase is capable of calling the ATA secure erase command as well as resetting the host-protected area and device configuration overlay table on non-volatile magnetic media.

Further information on reliably erasing data from solid state drives can be found in the *Reliably Erasing Data From Flash-Based Solid State Drives* paper.

Media destruction

Media destruction processes and procedures

Documenting processes and procedures for media destruction will ensure that an organisation carries out media destruction in an appropriate and consistent manner.

Security Control: ISM-0363; Revision: 3; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Media destruction processes, and supporting media destruction procedures, are developed and implemented.

Media that cannot be sanitised

Some media types are incapable of being sanitised. As such, they will need to be destroyed prior to their disposal.

Security Control: ISM-0350; Revision: 5; Updated: Dec-21; Applicability: All; Essential Eight: N/A
The following media types are destroyed prior to their disposal:

- *microfiche and microfilm*
- *optical discs*

- *programmable read-only memory*
- *read-only memory*
- *other types of media that cannot be sanitised.*

Media destruction equipment

When physically destroying media, using approved equipment can provide a level of assurance that the data it stores is actually destroyed.

Approved equipment includes destruction equipment listed on the Security Construction and Equipment Committee (SCEC)'s *Security Equipment Evaluated Products List*, and in the Australian Security Intelligence Organisation (ASIO)'s Security Equipment Guide (SEG)-009, *Optical Media Shredders* and SEG-018, *Destructors*. ASIO's SEG-009 and SEG-018 are available from the Protective Security Policy GovTEAMS community or ASIO by email.

If using degaussers to destroy media, the United States' National Security Agency maintains an *Evaluated Products List for Magnetic Degaussers* and information on common types of magnetic media and their associated magnetic field strengths and orientations.

Security Control: ISM-1361; Revision: 2; Updated: Mar-22; Applicability: All; Essential Eight: N/A
SCEC or ASIO-approved equipment is used when destroying media.

Security Control: ISM-1160; Revision: 2; Updated: Aug-20; Applicability: All; Essential Eight: N/A
If using degaussers to destroy media, degaussers evaluated by the United States' National Security Agency are used.

Media destruction methods

The destruction methods identified below are designed to ensure that recovery of data is impossible or impractical.

Security Control: ISM-1517; Revision: 0; Updated: Sep-18; Applicability: All; Essential Eight: N/A
Equipment that is capable of reducing microform to a fine powder, with resultant particles not showing more than five consecutive characters per particle upon microscopic inspection, is used to destroy microfiche and microfilm.

Security Control: ISM-1722; Revision: 1; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Electrostatic memory devices are destroyed using a furnace/incinerator, hammer mill, disintegrator or grinder/sander.

Security Control: ISM-1723; Revision: 1; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Magnetic floppy disks are destroyed using a furnace/incinerator, hammer mill, disintegrator, degausser or by cutting.

Security Control: ISM-1724; Revision: 1; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Magnetic hard disks are destroyed using a furnace/incinerator, hammer mill, disintegrator, grinder/sander or degausser.

Security Control: ISM-1725; Revision: 1; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Magnetic tapes are destroyed using a furnace/incinerator, hammer mill, disintegrator, degausser or by cutting.

Security Control: ISM-1726; Revision: 1; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Optical disks are destroyed using a furnace/incinerator, hammer mill, disintegrator, grinder/sander or by cutting.

Security Control: ISM-1727; Revision: 1; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Semiconductor memory is destroyed using a furnace/incinerator, hammer mill or disintegrator.

Security Control: ISM-0368; Revision: 8; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Media destroyed using a hammer mill, disintegrator, grinder/sander or by cutting results in media waste particles no larger than 9 mm.

Treatment of media waste particles

Following the destruction of SECRET and TOP SECRET media, normal accounting and verification processes and procedures do not apply. However, depending on the destruction method used, and the resulting media waste particle size, it may still need to be stored and handled as classified waste.

Security Control: ISM-1728; Revision: 0; Updated: Dec-21; Applicability: S; Essential Eight: N/A
The resulting media waste particles from the destruction of SECRET media is stored and handled as OFFICIAL if less than or equal to 3 mm, PROTECTED if greater than 3 mm and less than or equal to 6 mm, or SECRET if greater than 6 mm and less than or equal to 9 mm.

Security Control: ISM-1729; Revision: 0; Updated: Dec-21; Applicability: TS; Essential Eight: N/A
The resulting media waste particles from the destruction of TOP SECRET media is stored and handled as OFFICIAL if less than or equal to 3 mm, or SECRET if greater than 3 mm and less than or equal to 9 mm.

Degaussing magnetic media

Degaussing magnetic media changes its magnetic properties, thereby, permanently corrupting data. When degaussing magnetic media, care needs to be taken as a degausser of insufficient magnetic field strength will not be effective. In addition, since 2006 perpendicular magnetic media has progressively replaced longitudinal magnetic media. As some older degaussers are only capable of destroying longitudinal magnetic media, care needs to be taken to ensure that a degausser with a suitable magnetic orientation is also used. Furthermore, to ensure that degaussers are being used in the correct manner to effectively destroy magnetic media, product-specific directions provided by degausser manufacturers should be followed. Finally, to provide an additional level of assurance following the use of a degausser, magnetic media should be physically damaged by deforming any internal platters.

Security Control: ISM-0361; Revision: 4; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Magnetic media is destroyed using a degausser with a suitable magnetic field strength and magnetic orientation.

Security Control: ISM-0362; Revision: 4; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Product-specific directions provided by degausser manufacturers are followed.

Security Control: ISM-1641; Revision: 2; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Following the use of a degausser, magnetic media is physically damaged by deforming any internal platters.

Supervision of destruction

To verify that media is appropriately destroyed, destruction processes need to be supervised by at least one person cleared to the sensitivity or classification of the media being destroyed.

Security Control: ISM-0370; Revision: 5; Updated: Dec-21; Applicability: All; Essential Eight: N/A
The destruction of media is performed under the supervision of at least one person cleared to its sensitivity or classification.

Security Control: ISM-0371; Revision: 4; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Personnel supervising the destruction of media supervise its handling to the point of destruction and ensure that the destruction is completed successfully.

Supervision of accountable material destruction

The successful destruction of media storing accountable material is more important than for other media. As such, its destruction should be supervised by at least two personnel who sign a destruction certificate afterwards.

Security Control: ISM-0372; Revision: 5; Updated: Dec-21; Applicability: O, P, S, TS; Essential Eight: N/A
The destruction of media storing accountable material is performed under the supervision of at least two personnel cleared to its sensitivity or classification.

Security Control: ISM-0373; Revision: 4; Updated: Dec-21; Applicability: O, P, S, TS; Essential Eight: N/A
Personnel supervising the destruction of media storing accountable material supervise its handling to the point of destruction, ensure that the destruction is completed successfully and sign a destruction certificate afterwards.

Outsourcing media destruction

National Association for Information Destruction AAA certified destruction services with endorsements can be used for the outsourced destruction of media, as specified in ASIO's Protective Security Circular (PSC)-167, *External destruction of security classified information*. ASIO's PSC-167 is available from the Protective Security Policy GovTEAMS community or ASIO by email.

Security Control: ISM-0840; Revision: 3; Updated: Sep-18; Applicability: O, P, S; Essential Eight: N/A
When outsourcing the destruction of media to an external destruction service, a National Association for Information Destruction AAA certified destruction service with endorsements, as specified in ASIO's PSC-167, is used.

Security Control: ISM-0839; Revision: 3; Updated: Dec-21; Applicability: O, P, S, TS; Essential Eight: N/A
The destruction of media storing accountable material is not outsourced.

Media disposal

Media disposal processes and procedures

Documenting processes and procedures for media disposal will ensure that an organisation carries out media disposal in an appropriate and consistent manner.

Security Control: ISM-0374; Revision: 3; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Media disposal processes, and supporting media disposal procedures, are developed and implemented.

Disposal of media

Before media can be released into the public domain, it needs to be sanitised, destroyed or declassified. As sanitised, destroyed or declassified media still presents a security risk, albeit very minor, an appropriate authority needs to formally authorise its release into the public domain. Furthermore, as part of disposal processes, removing labels and markings indicating the owner, sensitivity, classification or any other marking that can associate media with its prior use will ensure it does not draw undue attention following its disposal.

Security Control: ISM-0378; Revision: 4; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Labels and markings indicating the owner, sensitivity, classification or any other marking that can associate media with its prior use are removed prior to its disposal.

Security Control: ISM-0375; Revision: 6; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Following sanitisation, destruction or declassification, a formal administrative decision is made to release media, or its waste, into the public domain.

Guidelines for System Hardening

Operating system hardening

Operating system selection

When selecting operating systems, it is important that an organisation preferences vendors that have demonstrated a commitment to secure-by-design principles, secure programming practices and maintaining the security of their products. This will assist not only with reducing the potential number of security vulnerabilities in operating systems, but also increasing the likelihood that timely patches, updates or vendor mitigations will be released to remediate any security vulnerabilities that are found.

Security Control: ISM-1743; Revision: 0; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Operating systems are chosen from vendors that have made a commitment to secure-by-design principles, secure programming practices and maintaining the security of their products.

Operating system releases and versions

Newer releases of operating systems often introduce improvements in security functionality. This can make it more difficult for an adversary to craft reliable exploits for security vulnerabilities they discover. Using older releases of operating systems, especially those no longer supported by vendors, may expose an organisation to security vulnerabilities or exploitation techniques that have since been mitigated. In addition, 64-bit versions of operating systems support additional security functionality that 32-bit versions do not.

Security Control: ISM-1407; Revision: 4; Updated: Sep-21; Applicability: All; Essential Eight: ML3
The latest release, or the previous release, of operating systems are used for workstations, servers and network devices.

Security Control: ISM-1744; Revision: 0; Updated: Mar-22; Applicability: All; Essential Eight: N/A
The latest release, or the previous release, of operating systems are used for other ICT equipment.

Security Control: ISM-1408; Revision: 4; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Where supported, 64-bit versions of operating systems are used for workstations, servers, network devices and other ICT equipment.

Standard Operating Environments

Allowing users to setup, configure and maintain their own workstations and servers can result in an inconsistent operating environment. Such operating environments may assist an adversary in gaining an initial foothold on networks due to the higher likelihood of poorly configured or maintained workstations and servers. Conversely, a Standard Operating Environment (SOE) is designed to facilitate a standardised and consistent operating environment within an organisation.

When SOEs are obtained from third parties, such as service providers, there are additional cyber supply chain risks that should be considered, such as the accidental or deliberate inclusion of malicious code or configurations. To reduce the likelihood of such occurrences, an organisation should endeavour to obtain their SOEs from trusted third parties while also scanning them for malicious code and configurations.

As operating environments naturally change over time, such as patches or updates are applied, configurations are changed, and applications are added or removed, it is essential that SOEs are reviewed and updated at least annually to ensure that an up-to-date baseline is maintained.

Security Control: ISM-1406; Revision: 2; Updated: Aug-20; Applicability: All; Essential Eight: N/A
SOEs are used for workstations and servers.

Security Control: ISM-1608; Revision: 1; Updated: Mar-22; Applicability: All; Essential Eight: N/A
SOEs provided by third parties are scanned for malicious code and configurations.

Security Control: ISM-1588; Revision: 0; Updated: Aug-20; Applicability: All; Essential Eight: N/A
SOEs are reviewed and updated at least annually.

Hardening operating system configurations

When operating systems are deployed in their default state it can lead to an insecure operating environment that may allow an adversary to gain an initial foothold on networks. Many configuration settings exist within operating systems to allow them to be configured in a secure state in order to minimise this security risk. As such, the Australian Cyber Security Centre (ACSC) and vendors often produce guidance to assist in hardening the configuration of operating systems. Note, however, in situations where ACSC and vendor guidance conflicts, preference should be given to implementing ACSC hardening guidance.

Security Control: ISM-1409; Revision: 1; Updated: Sep-18; Applicability: All; Essential Eight: N/A
ACSC and vendor guidance is implemented to assist in hardening the configuration of operating systems.

Security Control: ISM-0380; Revision: 9; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Unneeded accounts, components, services and functionality of operating systems are disabled or removed.

Security Control: ISM-0383; Revision: 7; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Default credentials for pre-configured accounts are changed.

Security Control: ISM-0341; Revision: 4; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Automatic execution features for removable media are disabled.

Security Control: ISM-1654; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML3
Internet Explorer 11 is disabled or removed.

Security Control: ISM-1655; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML3
.NET Framework 3.5 (includes .NET 2.0 and 3.0) is disabled or removed.

Security Control: ISM-1492; Revision: 2; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Operating system exploit protection functionality is enabled.

Security Control: ISM-1745; Revision: 0; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Early Launch Antimalware, Secure Boot, Trusted Boot and Measured Boot functionality is enabled.

Security Control: ISM-1584; Revision: 1; Updated: Sep-21; Applicability: All; Essential Eight: N/A
Unprivileged users are prevented from bypassing, disabling or modifying security functionality of operating systems.

Security Control: ISM-1491; Revision: 3; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Unprivileged users are prevented from running script execution engines, including:

- *Windows Script Host (cscript.exe and wscript.exe)*
- *PowerShell (powershell.exe, powershell_ise.exe and pwsh.exe)*
- *Command Prompt (cmd.exe)*
- *Windows Management Instrumentation (wmic.exe)*
- *Microsoft Hypertext Markup Language (HTML) Application Host (mshta.exe).*

Application management

Unprivileged users' ability to install any application can be exploited by an adversary using social engineering in order to convince them to install a malicious application. One way to mitigate this security risk, while also removing burden from system administrators, is to allow unprivileged users the ability to install approved applications from organisation-managed software repositories or from trusted application marketplaces. Furthermore, to prevent unprivileged users from removing security functionality, or breaking system functionality, unprivileged users should not have the ability to uninstall or disable approved software.

Security Control: ISM-1592; Revision: 1; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Unprivileged users do not have the ability to install unapproved software.

Security Control: ISM-0382; Revision: 7; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Unprivileged users do not have the ability to uninstall or disable approved software.

Application control

Application control can be an effective way to not only prevent malicious code from executing on workstations and servers, but also to ensure only approved applications can execute. When developing application control rulesets, determining approved executables (e.g. .exe and .com files), software libraries (e.g. .dll and.ocx files), scripts (e.g. .ps1, .bat, .cmd, .vbs and .js files), installers (e.g. .msi, .msp and .mst files), compiled HTML (e.g. .chm), HTML applications (e.g. .hta), control panel applets (e.g. .cpl) and drivers based on business requirements is a more secure method than simply approving those already residing on a workstation or server. Furthermore, it is preferable that an organisation defines their own application control rulesets, rather than relying on those from application control vendors, and validate them on an annual or more frequent basis.

In implementing application control, an organisation should use a reliable method, or combination of methods, such as cryptographic hash rules, publisher certificate rules or path rules. Depending on the method chosen, further hardening may be required to ensure that application control mechanisms and application control rulesets cannot be bypassed by an adversary.

Finally, to assist with incident response activities, it is important that application control event logs are centrally stored and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.

Security Control: ISM-0843; Revision: 9; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3
Application control is implemented on workstations.

Security Control: ISM-1490; Revision: 3; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3
Application control is implemented on internet-facing servers.

Security Control: ISM-1656; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML3
Application control is implemented on non-internet-facing servers.

Security Control: ISM-1657; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3
Application control restricts the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets to an organisation-approved set.

Security Control: ISM-1658; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML3
Application control restricts the execution of drivers to an organisation-approved set.

Security Control: ISM-0955; Revision: 6; Updated: Apr-20; Applicability: All; Essential Eight: N/A
Application control is implemented using cryptographic hash rules, publisher certificate rules or path rules.

Security Control: ISM-1582; Revision: 1; Updated: Sep-21; Applicability: All; Essential Eight: ML3
Application control rulesets are validated on an annual or more frequent basis.

Security Control: ISM-1471; Revision: 2; Updated: Apr-20; Applicability: All; Essential Eight: N/A
When implementing application control using publisher certificate rules, both publisher names and product names are used.

Security Control: ISM-1392; Revision: 3; Updated: Mar-22; Applicability: All; Essential Eight: N/A

When implementing application control using path rules, only approved users can write to and modify content within approved folders and files.

Security Control: ISM-1746; Revision: 0; Updated: Mar-22; Applicability: All; Essential Eight: N/A
When implementing application control using path rules, only approved users can change file system permissions for approved folders and files.

Security Control: ISM-1544; Revision: 2; Updated: Sep-21; Applicability: All; Essential Eight: ML3
Microsoft's 'recommended block rules' are implemented.

Security Control: ISM-1659; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML3
Microsoft's 'recommended driver block rules' are implemented.

Security Control: ISM-0846; Revision: 8; Updated: Mar-22; Applicability: All; Essential Eight: N/A
All users (with the exception of local administrator accounts and break glass accounts) cannot disable, bypass or be exempted from application control.

Security Control: ISM-1660; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3
Allowed and blocked executions on workstations are logged.

Security Control: ISM-1661; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3
Allowed and blocked executions on internet-facing servers are logged.

Security Control: ISM-1662; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML3
Allowed and blocked executions on non-internet facing servers are logged.

Security Control: ISM-1663; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML3
Application control event logs are centrally stored and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.

PowerShell

PowerShell is a powerful scripting language developed by Microsoft and, due to its ubiquity and ease with which it can be used to fully control operating systems, is an important part of system administrator toolkits. However, PowerShell can also be a dangerous exploitation tool in the hands of an adversary.

In order to prevent attacks leveraging security vulnerabilities in earlier PowerShell versions, Windows PowerShell 2.0 should be disabled or removed from operating systems. Additionally, PowerShell's language mode should be set to Constrained Language Mode to achieve a balance between security and functionality.

Finally, logging and transcription functionality available in PowerShell can provide invaluable information for incident responders. As such, it is important that PowerShell event logs are centrally stored and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.

Security Control: ISM-1621; Revision: 1; Updated: Sep-21; Applicability: All; Essential Eight: ML3
Windows PowerShell 2.0 is disabled or removed.

Security Control: ISM-1622; Revision: 0; Updated: Oct-20; Applicability: All; Essential Eight: ML3
PowerShell is configured to use Constrained Language Mode.

Security Control: ISM-1623; Revision: 0; Updated: Oct-20; Applicability: All; Essential Eight: N/A
PowerShell is configured to use module logging, script block logging and transcription functionality.

Security Control: ISM-1624; Revision: 0; Updated: Oct-20; Applicability: All; Essential Eight: N/A
PowerShell script block logs are protected by Protected Event Logging functionality.

Security Control: ISM-1664; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3
Blocked PowerShell script executions are logged.

Security Control: ISM-1665; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML3

PowerShell event logs are centrally stored and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.

Host-based Intrusion Prevention System

Many security products rely on signatures to detect malicious code. This approach is only effective when malicious code has already been profiled and signatures are available from security vendors. Unfortunately, an adversary can easily create variants of known malicious code in order to bypass traditional signature-based detection. A Host-based Intrusion Prevention System (HIPS) can use behaviour-based detection to assist in identifying and blocking anomalous behaviour as well as detecting malicious code that has yet to be identified by security vendors. As such, it is important that a HIPS is implemented on workstations, critical servers and high-value servers.

Security Control: ISM-1341; Revision: 2; Updated: Sep-18; Applicability: All; Essential Eight: N/A
A HIPS is implemented on workstations.

Security Control: ISM-1034; Revision: 7; Updated: Mar-22; Applicability: All; Essential Eight: N/A
A HIPS is implemented on critical servers and high-value servers.

Software firewall

Traditional network firewalls often fail to prevent the propagation of malicious code on networks, or an adversary from exfiltrating data from networks, as they only control which ports or protocols can be used between different network segments. Many forms of malicious code are designed specifically to take advantage of this by using common protocols, such as Hypertext Transfer Protocol, Hypertext Transfer Protocol Secure, Simple Mail Transfer Protocol or Domain Name System. Software firewalls are more effective than traditional network firewalls as they can control which applications and services can communicate to and from workstations and servers. As such, a software firewall should be implemented on workstations and servers to restrict inbound and outbound network connections to an organisation-approved set of applications and services.

Security Control: ISM-1416; Revision: 3; Updated: Mar-22; Applicability: All; Essential Eight: N/A
A software firewall is implemented on workstations and servers to restrict inbound and outbound network connections to an organisation-approved set of applications and services.

Antivirus software

When vendors develop software they may make coding mistakes that lead to security vulnerabilities. An adversary can take advantage of this by developing malicious code to exploit any security vulnerabilities that have not been detected and remedied by vendors. As significant time and effort is often involved in developing functioning and reliable exploits, an adversary will often attempt to reuse their exploits as much as possible. While exploits may have been previously identified by security vendors, they often remain viable against an organisation that does not have antivirus software in place.

Security Control: ISM-1417; Revision: 4; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Antivirus software is implemented on workstations and servers with:

- *signature-based detection functionality enabled and set to a high level*
- *heuristic-based detection functionality enabled and set to a high level*
- *reputation rating functionality enabled*
- *ransomware protection functionality enabled*
- *detection signatures configured to update on at least a daily basis*
- *regular scanning configured for all fixed disks and removable media.*

Device access control software

Device access control software can be used to prevent removable media and mobile devices from being connecting to workstations and servers via external communication interfaces. This can assist in preventing the introduction of malicious code or the exfiltration of data by an adversary.

In addition, an adversary can connect to locked workstations and servers via external communication interfaces that allow Direct Memory Access (DMA). In doing so, the adversary can gain access to encryption keys in memory or write malicious code to memory. The best defence against this security risk is to disable access to external communication interfaces that allow DMA, such as FireWire, ExpressCard and Thunderbolt.

Security Control: ISM-1418; Revision: 4; Updated: Mar-22; Applicability: All; Essential Eight: N/A
If there is no business requirement for reading from removable media and devices, such functionality is disabled via the use of device access control software or by disabling external communication interfaces.

Security Control: ISM-0343; Revision: 6; Updated: Mar-22; Applicability: All; Essential Eight: N/A
If there is no business requirement for writing to removable media and devices, such functionality is disabled via the use of device access control software or by disabling external communication interfaces.

Security Control: ISM-0345; Revision: 6; Updated: Dec-21; Applicability: All; Essential Eight: N/A
External communication interfaces that allow DMA are disabled.

Operating system event logging

Certain operating system events can assist in monitoring the security posture of operating systems, detecting malicious behaviour and contributing to investigations following cyber security incidents. In doing so, operating system event logs should be centrally stored and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.

Security Control: ISM-0582; Revision: 7; Updated: Mar-22; Applicability: All; Essential Eight: N/A
The following events are logged for operating systems:

- *application and operating system crashes and error messages*
- *changes to security policies and system configurations*
- *successful user logons and logoffs, failed user logons and account lockouts*
- *failures, restarts and changes to important processes and services*
- *requests to access internet resources*
- *security product-related events*
- *system startups and shutdowns.*

Security Control: ISM-1747; Revision: 0; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Operating system event logs are centrally stored and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.

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 Outsourcing*.

Further information on patching or updating operating systems can be found in the system patching section of the *Guidelines for System Management*.

Further information on end of support for Microsoft Windows operating systems can be found in the ACSC's *End of Support for Microsoft Windows 10* and *End of Support for Microsoft Windows Server 2008 and Windows Server 2008 R2* publications.

Further information on securely configuring Microsoft Windows operating systems can be found in the ACSC's *Hardening Microsoft Windows 10 version 21H1 Workstations* publication.

Further information on securely configuring Linux workstations and servers can be found in the ACSC's *Hardening Linux Workstations and Servers* publication.

Further information on exploit protection functionality within Microsoft Windows is available from Microsoft.

Further information on implementing application control can be found in the ACSC's *Implementing Application Control* publication.

Further information on Microsoft's 'recommended block rules' and 'recommended driver block rules' are available from Microsoft.

Further information on the use of PowerShell can be found in the ACSC's *Securing PowerShell in the Enterprise* publication.

Further information on the use of PowerShell by blue teams is available from Microsoft while further information on obtaining greater visibility through PowerShell logging is available from FireEye.

Further information on independent testing of security products' ability to detect or prevent various stages of network intrusions is available from The MITRE Corporation.

Further information on independent testing of antivirus software is available from AV-Comparatives and AV-TEST.

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

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

Application hardening

Application selection

When selecting applications, it is important that an organisation preferences vendors that have demonstrated a commitment to secure-by-design principles, secure programming practices and maintaining the security of their products. This will assist not only with reducing the potential number of security vulnerabilities in applications, but also increasing the likelihood that timely patches, updates or vendor mitigations will be released to remediate any security vulnerabilities that are found.

Security Control: ISM-0938; Revision: 5; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Applications are chosen from vendors that have made a commitment to secure-by-design principles, secure programming practices and maintaining the security of their products.

Application releases

Newer releases of applications often introduce improvements in security functionality. This can make it more difficult for an adversary to craft reliable exploits for security vulnerabilities they discover. Using older releases of applications, especially those no longer supported by vendors, may expose an organisation to security vulnerabilities or exploitation techniques that have since been mitigated. This is particularly important for office productivity suites, web browsers and their extensions, email clients, Portable Document Format (PDF) software, and security products, as well as web server applications and other internet-accessible server applications.

Security Control: ISM-1467; Revision: 3; Updated: Mar-22; Applicability: All; Essential Eight: N/A
The latest release of office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are used.

Security Control: ISM-1483; Revision: 1; Updated: Mar-22; Applicability: All; Essential Eight: N/A
The latest release of web server applications, and other internet-accessible server applications, are used.

Hardening application configurations

When applications are deployed in their default state it can lead to an insecure operating environment that may allow an adversary to gain an initial foothold on networks. This can be especially risky for office productivity suites, web browsers, email clients, PDF software and security products as such applications are routinely targeted for exploitation. Many configuration settings exist within such applications to allow them to be configured in a secure state in order to minimise this security risk. As such, the ACSC and vendors often produce guidance to assist in hardening the configuration of such applications. Note, however, in situations where ACSC and vendor guidance conflicts, preference should be given to implementing ACSC hardening guidance.

Security Control: ISM-1412; Revision: 3; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3
ACSC or vendor hardening guidance for web browsers, Microsoft Office and PDF software is implemented.

Security Control: ISM-1470; Revision: 5; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Unneeded components, services and functionality of office productivity suites, web browsers, email clients, PDF software and security products are disabled or removed.

Security Control: ISM-1235; Revision: 4; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Add-ons, extensions and plug-ins for office productivity suites, web browsers, email clients, PDF software and security products are restricted to an organisation-approved set.

Security Control: ISM-1486; Revision: 1; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3
Web browsers do not process Java from the internet.

Security Control: ISM-1485; Revision: 1; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3
Web browsers do not process web advertisements from the internet.

Security Control: ISM-1666; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML2
Internet Explorer 11 does not process content from the internet.

Security Control: ISM-1667; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3
Microsoft Office is blocked from creating child processes.

Security Control: ISM-1668; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3
Microsoft Office is blocked from creating executable content.

Security Control: ISM-1669; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3
Microsoft Office is blocked from injecting code into other processes.

Security Control: ISM-1542; Revision: 0; Updated: Jan-19; Applicability: All; Essential Eight: ML2, ML3
Microsoft Office is configured to prevent activation of Object Linking and Embedding packages.

Security Control: ISM-1670; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3
PDF software is blocked from creating child processes.

Security Control: ISM-1601; Revision: 1; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Microsoft's Attack Surface Reduction rules are implemented.

Security Control: ISM-1585; Revision: 1; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3
Web browser, Microsoft Office and PDF software security settings cannot be changed by users.

Security Control: ISM-1748; Revision: 0; Updated: Mar-22; Applicability: All; Essential Eight: N/A

Office productivity suite, email client and security product security settings cannot be changed by users.

Microsoft Office macros

Microsoft Office files can contain embedded code, known as a macro, written in the Visual Basic for Applications programming language. A macro can contain a series of commands that can be coded or recorded and replayed at a later time to automate repetitive tasks. Macros are powerful tools that can be easily created by users to greatly improve their productivity. However, an adversary can also create macros to perform a variety of malicious activities, such as assisting to compromise workstations in order to exfiltrate or deny access to data. To reduce this security risk, an organisation should disable Microsoft Office macros for users that do not have a demonstrated business requirement and secure their use for the remaining users that do.

Finally, to assist with incident response activities, it is important that Microsoft Office macro event logs are centrally stored and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.

Security Control: ISM-1671; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3
Microsoft Office macros are disabled for users that do not have a demonstrated business requirement.

Security Control: ISM-1488; Revision: 1; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3
Microsoft Office macros in files originating from the internet are blocked.

Security Control: ISM-1672; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3
Microsoft Office macro antivirus scanning is enabled.

Security Control: ISM-1673; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3
Microsoft Office macros are blocked from making Win32 API calls.

Security Control: ISM-1674; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML3
Only Microsoft Office macros running from within a sandboxed environment, a Trusted Location or that are digitally signed by a trusted publisher are allowed to execute.

Security Control: ISM-1487; Revision: 1; Updated: Sep-21; Applicability: All; Essential Eight: ML3
Only privileged users responsible for validating that Microsoft Office macros are free of malicious code can write to and modify content within Trusted Locations.

Security Control: ISM-1675; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML3
Microsoft Office macros digitally signed by an untrusted publisher cannot be enabled via the Message Bar or Backstage View.

Security Control: ISM-1676; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML3
Microsoft Office's list of trusted publishers is validated on an annual or more frequent basis.

Security Control: ISM-1489; Revision: 0; Updated: Sep-18; Applicability: All; Essential Eight: ML2, ML3
Microsoft Office macro security settings cannot be changed by users.

Security Control: ISM-1677; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3
Allowed and blocked Microsoft Office macro executions are logged.

Security Control: ISM-1678; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML3
Microsoft Office macro event logs are centrally stored and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.

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 Outsourcing*.

Further information on patching or updating applications can be found in the system patching section of the *Guidelines for System Management*.

Further information on securely configuring Microsoft Office can be found in the ACSC’s *Hardening Microsoft 365, Office 2021, Office 2019 and Office 2016* publication.

Further information on configuring Microsoft Office macro settings can be found in the ACSC’s *Microsoft Office Macro Security* publication.

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

Authentication hardening

Account and authentication types

The guidance within this section is equally applicable to all account types. This includes unprivileged accounts, privileged accounts, break glass accounts and service accounts. In addition, the guidance is equally applicable to interactive authentication and non-interactive authentication.

Authenticating to systems

Before access to a system and its resources is granted to a user, it is essential that they are authenticated. This can be achieved via multi-factor authentication, such as a username along with a passphrase and security key, or via single-factor authentication, such as a username and a passphrase.

Security Control: ISM-1546; Revision: 0; Updated: Aug-19; Applicability: All; Essential Eight: N/A
Users are authenticated before they are granted access to a system and its resources.

Multi-factor authentication

Multi-factor authentication uses two or more authentication factors. This may include:

- something a user knows, such as a memorised secret (i.e. personal identification number, password or passphrase)
- something a user has, such as a security key, smart card, smartphone or physical one-time password token
- something a user is, such as a fingerprint pattern or their facial geometry.

Note, however, that if a memorised secret is written down, or stored in a document on a system, this becomes something that a user has rather than something a user knows.

Privileged users, users of remote access solutions and users with access to important data repositories are more likely to be targeted by an adversary due to their access. For this reason, it is especially important that multi-factor authentication is used for these accounts. In addition, multi-factor authentication is vital to any administrative activities as it can limit the consequences of a compromise by preventing or slowing an adversary’s ability to gain unrestricted access to assets. In this regard, multi-factor authentication can be implemented as part of jump server authentication where assets being administered do not support multi-factor authentication themselves.

When implementing multi-factor authentication, several different authentication factors can be implemented. Unfortunately, some authentication factors, such as biometrics or codes sent via Short Message Service, Voice over Internet Protocol or email, are more susceptible to compromise than others. For this reason, authentication factors that involve something a user has should be used as part of multi-factor authentication. Furthermore, for increased security, the use of verifier impersonation resistant authentication factors are recommended to protect against real-time phishing attacks.

Finally, to assist with incident response activities, it is important that multi-factor authentication event logs are centrally stored and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.

Security Control: ISM-0974; Revision: 6; Updated: Sep-21; Applicability: All; Essential Eight: N/A
Multi-factor authentication is used to authenticate unprivileged users of systems.

Security Control: ISM-1173; Revision: 4; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3
Multi-factor authentication is used to authenticate privileged users of systems.

Security Control: ISM-1504; Revision: 1; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3
Multi-factor authentication is used by an organisation's users if they authenticate to their organisation's internet-facing services.

Security Control: ISM-1679; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3
Multi-factor authentication is used by an organisation's users if they authenticate to third-party internet-facing services that process, store or communicate their organisation's sensitive data.

Security Control: ISM-1680; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3
Multi-factor authentication (where available) is used by an organisation's users if they authenticate to third-party internet-facing services that process, store or communicate their organisation's non-sensitive data.

Security Control: ISM-1681; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3
Multi-factor authentication is enabled by default for non-organisational users (but users can choose to opt out) if they authenticate to an organisation's internet-facing services.

Security Control: ISM-1505; Revision: 1; Updated: Sep-21; Applicability: All; Essential Eight: ML3
Multi-factor authentication is used to authenticate users accessing important data repositories.

Security Control: ISM-1401; Revision: 5; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3
Multi-factor authentication uses either: something users have and something users know, or something users have that is unlocked by something users know or are.

Security Control: ISM-1682; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML3
Multi-factor authentication is verifier impersonation resistant.

Security Control: ISM-1559; Revision: 2; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Memorised secrets used for multi-factor authentication are a minimum of 6 characters, unless more stringent requirements apply.

Security Control: ISM-1560; Revision: 2; Updated: Mar-22; Applicability: S; Essential Eight: N/A
Memorised secrets used for multi-factor authentication on SECRET systems are a minimum of 8 characters.

Security Control: ISM-1561; Revision: 2; Updated: Mar-22; Applicability: TS; Essential Eight: N/A
Memorised secrets used for multi-factor authentication on TOP SECRET systems are a minimum of 10 characters.

Security Control: ISM-1683; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3
Successful and unsuccessful multi-factor authentications are logged.

Security Control: ISM-1684; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML3
Multi-factor authentication event logs are centrally stored and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.

Single-factor authentication

A significant threat to the compromise of accounts is credential cracking tools. When an adversary gains access to a list of usernames and hashed credentials from a system they can attempt to recover username and credential pairs by comparing the hashes of known credentials with the hashed credentials they have gained access to. By finding a match an adversary will know the credential associated with a given username.

In order to reduce this security risk, an organisation should implement multi-factor authentication. Note, while single-factor authentication is no longer considered suitable for protecting sensitive or classified data, it may not be possible to implement multi-factor authentication on some systems. In such cases, an organisation will need to increase the time on average it takes an adversary to compromise a credential by continuing to increase its length over time. Such increases in length can be balanced against useability through the use of passphrases rather than passwords. In cases where systems do not support passphrases, and as an absolute last resort, the strongest password length and complexity supported by a system will need to be implemented.

Security Control: ISM-0417; Revision: 5; Updated: Oct-19; Applicability: All; Essential Eight: N/A
When systems cannot support multi-factor authentication, single-factor authentication using passphrases is implemented instead.

Security Control: ISM-0421; Revision: 8; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Passphrases used for single-factor authentication are at least 4 random words with a total minimum length of 14 characters, unless more stringent requirements apply.

Security Control: ISM-1557; Revision: 2; Updated: Dec-21; Applicability: S; Essential Eight: N/A
Passphrases used for single-factor authentication on SECRET systems are at least 5 random words with a total minimum length of 17 characters.

Security Control: ISM-0422; Revision: 8; Updated: Dec-21; Applicability: TS; Essential Eight: N/A
Passphrases used for single-factor authentication on TOP SECRET systems are at least 6 random words with a total minimum length of 20 characters.

Security Control: ISM-1558; Revision: 2; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Passphrases used for single-factor authentication are not a list of categorised words; do not form a real sentence in a natural language; and are not constructed from song lyrics, movies, literature or any other publicly available material.

Security Control: ISM-1596; Revision: 1; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Passphrases are not reused for single-factor authentication across different systems.

Setting credentials for user accounts

Before new credentials are issued for user accounts, it is important that users' provide sufficient evidence to verify their identity, such as by users physically presenting themselves and their pass to a service desk or by answering a set of challenge-response questions. Following the verification of user identity, credentials should be randomly generated and provided to users via a secure communications channel or, if not possible, split into two parts with one part provided to users and the other part provided to supervisors. Subsequently, users should reset their credentials on first use to ensure that they are not known by other parties.

Security Control: ISM-1593; Revision: 1; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Users provide sufficient evidence to verify their identity when requesting new credentials.

Security Control: ISM-1227; Revision: 5; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Credentials set for user accounts are randomly generated.

Security Control: ISM-1594; Revision: 1; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Credentials are provided to users via a secure communications channel or, if not possible, split into two parts with one part provided to users and the other part provided to supervisors.

Security Control: ISM-1595; Revision: 1; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Credentials provided to users are changed on first use.

Setting credentials for service accounts

To provide additional security and credential management functionality for service accounts, Microsoft introduced group Managed Service Accounts to Microsoft Windows Server. In doing so, service accounts that are created as group

Managed Service Accounts do not require manual credential management by system administrators, as the operating system automatically manages the credentials. This ensures that service account credentials are not misplaced or forgotten, and that they are automatically changed on a regular basis.

Security Control: ISM-1619; Revision: 0; Updated: Oct-20; Applicability: All; Essential Eight: N/A
Service accounts are created as group Managed Service Accounts.

Account lockouts

Locking an account after a specified number of failed logon attempts reduces the likelihood of successful credential spraying attacks by an adversary. However, care should be taken as implementing account lockout functionality can increase the likelihood of a denial of service. Alternatively, some systems can be configured to automatically slowdown repeated failed logon attempts (known as rate limiting) rather than locking accounts. Implementing multi-factor authentication is also an effective way of reducing the likelihood of successful credential spraying attacks.

Security Control: ISM-1403; Revision: 2; Updated: Oct-19; Applicability: All; Essential Eight: N/A
Accounts are locked out after a maximum of five failed logon attempts.

Insecure authentication methods

Authentication methods need to resist theft, interception, duplication, forgery, unauthorised access and unauthorised modification. For example, Local Area Network (LAN) Manager and NT LAN Manager authentication methods use weak hashing algorithms. As such, credentials used as part of LAN Manager authentication and NT LAN Manager authentication (i.e. NTLMv1, NTLMv2 and NTLM2) can easily be compromised. Instead, an organisation should use Kerberos for authentication within Microsoft Windows environments and ensure all privileged accounts are members of the Protected Users security group.

Security Control: ISM-1603; Revision: 0; Updated: Aug-20; Applicability: All; Essential Eight: N/A
Authentication methods susceptible to replay attacks are disabled.

Security Control: ISM-1055; Revision: 4; Updated: Oct-20; Applicability: All; Essential Eight: N/A
LAN Manager and NT LAN Manager authentication methods are disabled.

Security Control: ISM-1620; Revision: 0; Updated: Oct-20; Applicability: All; Essential Eight: N/A
Privileged accounts are members of the Protected Users security group.

Protecting credentials

When local administrator accounts use common usernames and credentials, it can allow an adversary that compromises credentials on one workstation or server to easily compromise other workstations and servers. As such, it is critical that credentials for local administrator accounts and service accounts are unique, unpredictable and managed.

Storing physical credentials with a system, such as security keys, smart cards, one-time password tokens and written down memorised secrets, increases the likelihood of an adversary gaining access to the system. For example, when passphrases are written down and stuck to a computer monitor, smart cards are left on desks or security keys are left in laptop bags. Furthermore, obscuring credentials as they are entered into systems can assist in protecting them against screen scrapers and shoulder surfers.

If storing credentials on a system, sufficient protection should be implemented to prevent them from being compromised. For example, credentials can be stored in a password manager or hardware security module, while credentials stored in a database should be hashed, salted and stretched. In addition, Windows Defender Credential Guard and Windows Defender Remote Credential Guard can be enabled to provide additional protection for credentials.

When using Microsoft Windows systems, cached credentials are stored in the Security Accounts Manager database and can allow a user to logon to a workstation they have previously logged onto even if the domain is not available. Whilst this functionality may be desirable from an availability perspective, this functionality can be abused by an adversary who can retrieve these cached credentials. To reduce this security risk, cached credentials should be limited to only one previous logon.

Security Control: ISM-1685; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3
Credentials for local administrator accounts and service accounts are unique, unpredictable and managed.

Security Control: ISM-0418; Revision: 5; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Physical credentials are stored separately from systems to which they grant access.

Security Control: ISM-1597; Revision: 0; Updated: Aug-20; Applicability: All; Essential Eight: N/A
Credentials are obscured as they are entered into systems.

Security Control: ISM-1402; Revision: 6; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Credentials stored on systems are protected by a password manager; a hardware security module; or by hashing, salting and stretching them before storage within a database.

Security Control: ISM-1686; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML3
Windows Defender Credential Guard and Windows Defender Remote Credential Guard are enabled.

Security Control: ISM-1749; Revision: 0; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Cached credentials are limited to one previous logon.

Security Control: ISM-1590; Revision: 1; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Credentials are changed if:

- *they are directly compromised*
- *they are suspected of being compromised*
- *they appear in an online data breach database*
- *they are discovered stored on networks in the clear*
- *they are discovered being transferred across networks in the clear*
- *membership of a shared account changes*
- *they have not been changed in the past 12 months.*

Session termination

Implementing measures to automatically terminate user sessions and reboot workstations outside of business hours, after an appropriate period of inactivity, can assist in both system maintenance activities as well as removing an adversary that may have compromised a system but failed to gain persistence.

Security Control: ISM-0853; Revision: 2; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Outside of business hours, after an appropriate period of inactivity, user sessions are automatically terminated and workstations are rebooted.

Session and screen locking

Session and screen locking prevents unauthorised access to a system which a user has already authenticated to.

Security Control: ISM-0428; Revision: 8; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Systems are configured with a session or screen lock that:

- *activates after a maximum of 15 minutes of user inactivity, or if manually activated by users*

- *conceals all session content on the screen*
- *ensures that the screen does not enter a power saving state before the session or screen lock is activated*
- *requires users to reauthenticate to unlock the session*
- *denies users the ability to disable the session or screen locking mechanism.*

Logon banner

Displaying a logon banner to users before access is granted to a system reminds them of their security responsibilities. Logon banners may cover topics such as:

- the sensitivity or classification of the system
- access to the system being restricted to authorised users
- acceptable usage and security policies for the system
- an agreement to abide by acceptable usage and security policies for the system
- legal ramifications of violating acceptable usage and security policies for the system
- details of any monitoring activities for the system.

Security Control: ISM-0408; Revision: 4; Updated: Sep-18; Applicability: All; Essential Eight: N/A
Systems have a logon banner that requires users to acknowledge and accept their security responsibilities before access is granted.

Security Control: ISM-0979; Revision: 4; Updated: Sep-18; Applicability: All; Essential Eight: N/A
Legal advice is sought on the exact wording of logon banners.

Further information

Further information on implementing multi-factor authentication can be found in the ACSC's *Implementing Multi-Factor Authentication* publication.

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

Further information on randomly generating passphrases (preferably using five dice rolls and a long word list) is available from the Electronic Frontier Foundation while a random dice roller is available from RANDOM.ORG.

Further information on mitigating the use of stolen credentials can be found in the ACSC's *Mitigating the Use of Stolen Credentials* publication.

Further information on mitigating the use of stolen credentials can also be found in Microsoft's *Mitigating Pass-the-Hash (PtH) Attacks and Other Credential Theft Techniques, Version 1 and 2* publication.

Virtualisation hardening

Containerisation

Containers allow for versatile deployment of systems and, in doing so, should be treated the same as any other system. However, security controls in a containerised environment may take a different form when compared to other types of systems. For example, patching the operating system of a workstation may be performed differently to ensuring that a patched image is used for a container, however, the principle is the same. In general, the same security risks that apply to non-containerised systems will likely apply to containerised systems.

Functional separation between computing environments

Physical servers often use a software-based isolation mechanism to share their hardware among multiple computing environments. In doing so, a computing environment could consist of an entire operating system installed in a virtual machine where the isolation mechanism is a hypervisor, such as cloud services providing Infrastructure as a Service, or alternatively, a computing environment could consist of an application which uses the shared kernel of the underlying operating system of the physical server where the isolation mechanism is an application container or application sandbox, such as cloud services providing Platform as a Service. Note, however, the logical separation of data within a single application, such as cloud services providing Software as a Service, is not considered to be the same as multiple computing environments.

An adversary who has compromised a single computing environment, or who legitimately controls a single computing environment, might exploit a misconfiguration or security vulnerability in the isolation mechanism to compromise other computing environments on the same physical server or compromise the underlying operating system of the physical server. As such, it is important that additional security controls are implemented when a software-based isolation mechanism is used to share a physical server's hardware.

Security Control: ISM-1460; Revision: 3; Updated: Mar-22; Applicability: All; Essential Eight: N/A
When using a software-based isolation mechanism to share a physical server's hardware, the isolation mechanism is from a vendor that has made a commitment to secure-by-design principles, secure programming practices and maintaining the security of their products.

Security Control: ISM-1604; Revision: 0; Updated: Aug-20; Applicability: All; Essential Eight: N/A
When using a software-based isolation mechanism to share a physical server's hardware, the configuration of the isolation mechanism is hardened by removing unneeded functionality and restricting access to the administrative interface used to manage the isolation mechanism.

Security Control: ISM-1605; Revision: 1; Updated: Mar-22; Applicability: All; Essential Eight: N/A
When using a software-based isolation mechanism to share a physical server's hardware, the underlying operating system is hardened.

Security Control: ISM-1606; Revision: 1; Updated: Mar-22; Applicability: All; Essential Eight: N/A
When using a software-based isolation mechanism to share a physical server's hardware, patches, updates or vendor mitigations for security vulnerabilities are applied to the isolation mechanism and underlying operating system in a timely manner.

Security Control: ISM-1607; Revision: 0; Updated: Aug-20; Applicability: All; Essential Eight: N/A
When using a software-based isolation mechanism to share a physical server's hardware, integrity and log monitoring are performed for the isolation mechanism and underlying operating system in a timely manner.

Security Control: ISM-1461; Revision: 5; Updated: Mar-22; Applicability: S, TS; Essential Eight: N/A
When using a software-based isolation mechanism to share a physical server's hardware for SECRET or TOP SECRET computing environments, the physical server and all computing environments are of the same classification and belong to the same security domain.

Further information

Further information on container security can be found in National Institute of Standards and Technology Special Publication 800-190, *Application Container Security Guide*.

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

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

Further information on hardening operating systems can be found in the operating system hardening section of these guidelines.

Further information on patching or updating operating systems and applications can be found in the system patching section of the *Guidelines for System Management*.

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

Further information on hypervisor security can be found in National Institute of Standards and Technology Special Publication 800-125A Rev. 1, *Security Recommendations for Server-based Hypervisor Platforms*.

Guidelines for System Management

System administration

System administration of cloud services

System administration of cloud services brings unique challenges when compared to system administration of on-premises assets. Notably, responsibility for system administration of cloud services is often shared between service providers and their customers. As the system administration processes and procedures implemented by service providers are often opaque to their customers, customers should consider a service provider's control plane to operate within a different security domain.

System administration processes and procedures

A key component of system administration is ensuring that administrative activities are undertaken in a repeatable and accountable manner using system administration processes and procedures. In doing so, requirements for administrative activities may cover:

- configuring applications, operating systems, network devices or other ICT equipment
- applying patches, updates or vendor mitigations to applications, drivers, operating systems or firmware
- installing or removing applications, operating systems, network devices or other ICT equipment
- implementing system changes or enhancements
- resolving problems identified by users.

Furthermore, in support of change management processes and procedures, system administrators should document requirements for administrative activities, consider potential security impacts, obtain any necessary approvals, notify users of any disruptions or outages, and maintain system and security documentation.

Security Control: ISM-0042; Revision: 5; Updated: Dec-21; Applicability: All; Essential Eight: N/A
System administration processes, and supporting system administration procedures, are developed and implemented.

Security Control: ISM-1211; Revision: 5; Updated: Mar-22; Applicability: All; Essential Eight: N/A
System administrators document requirements for administrative activities, consider potential security impacts, obtain any necessary approvals, notify users of any disruptions or outages, and maintain system and security documentation.

Separate privileged operating environments

One of the greatest threats to the security of networks is the compromise of privileged accounts. Providing a separate privileged operating environment for system administrators, in addition to their unprivileged operating environment, makes it much harder for administrative activities and privileged accounts to be compromised by an adversary.

Using different physical workstations is the most secure approach to separating privileged and unprivileged operating environments for system administrators. However, a virtualisation-based solution may be sufficient for separating privileged and unprivileged operating environments. In such cases, privileged operating environments should not be virtualised within unprivileged operating environments.

Security Control: ISM-1380; Revision: 5; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3
Privileged users use separate privileged and unprivileged operating environments.

Security Control: ISM-1687; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3
Privileged operating environments are not virtualised within unprivileged operating environments.

Security Control: ISM-1688; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3
Unprivileged accounts cannot logon to privileged operating environments.

Security Control: ISM-1689; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3
Privileged accounts (excluding local administrator accounts) cannot logon to unprivileged operating environments.

Administrative infrastructure

The security of administrative activities can be improved by segregating administrative infrastructure from the wider network. In doing so, the use of a jump server (also known as a jump host or jump box) can be an effective way of simplifying and securing administrative activities. Specifically, a jump server can provide filtering of network management traffic while also acting as a focal point to perform multi-factor authentication; store and manage administrative tools; and perform logging, monitoring and alerting activities. Finally, using separate jump servers for the administration of critical servers, high-value servers and regular servers can further assist in protecting these assets.

Security Control: ISM-1385; Revision: 3; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Administrative infrastructure is segregated from the wider network.

Security Control: ISM-1750; Revision: 0; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Administrative infrastructure for critical servers, high-value servers and regular servers is segregated from each other.

Security Control: ISM-1386; Revision: 5; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Network management traffic can only originate from administrative infrastructure.

Security Control: ISM-1387; Revision: 2; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3
Administrative activities are conducted through jump servers.

Security Control: ISM-1381; Revision: 3; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Only privileged operating environments can communicate with jump servers.

Security Control: ISM-1388; Revision: 2; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Only jump servers can communicate with assets requiring administrative activities to be performed.

Further information

Further information on system administration can be found in the Australian Cyber Security Centre (ACSC)'s *Secure Administration* publication.

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

Further information on multi-factor authentication can be found in the authentication hardening section of the *Guidelines for System Hardening*.

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

Further information on network segmentation and segregation can be found in the network design and configuration section of the *Guidelines for Networking*.

System patching

Patch management processes and procedures

Applying patches or updates is critical to ensuring the ongoing security of applications, drivers, operating systems and firmware. In doing so, it is important that patches or updates are applied consistently and in a secure manner. For example, by using a centralised and managed approach that maintains the integrity of patches or updates, and confirms that they have been applied successfully.

Security Control: ISM-1143; Revision: 8; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Patch management processes, and supporting patch management procedures, are developed and implemented.

Security Control: ISM-0298; Revision: 8; Updated: Mar-22; Applicability: All; Essential Eight: N/A
A centralised and managed approach that maintains the integrity of patches or updates, and confirms that they have been applied successfully, is used to patch or update applications, operating systems, drivers and firmware.

Software register

To assist with monitoring information sources for details of relevant patches or updates, an organisation should maintain and regularly verify software registers for workstations, servers, network devices and other ICT equipment.

Security Control: ISM-1493; Revision: 3; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Software registers are maintained for workstations, servers, network devices and other ICT equipment and verified on a regular basis.

Security Control: ISM-1643; Revision: 0; Updated: Jun-21; Applicability: All; Essential Eight: N/A
Software registers contain versions and patch histories of applications, drivers, operating systems and firmware.

When to patch security vulnerabilities

When patches or updates are released by vendors for security vulnerabilities, an organisation should apply them in a timeframe commensurate with the likelihood of attempted exploitation by an adversary. For example, by prioritising patches or updates for security vulnerabilities in internet-facing services and their operating systems, especially when exploitation code exists or active exploitation is occurring.

If no patches or updates are available for security vulnerabilities, mitigation advice from vendors, trusted authorities or security researchers may provide some protection until patches or updates are made available. Such mitigation advice may be published in conjunction with, or soon after, announcements made relating to security vulnerabilities. Mitigation advice may cover how to disable or block access to vulnerable functionality, how to reconfigure vulnerable functionality, or how to detect attempted or successful exploitation of vulnerable functionality.

If a patch or update is released for high assurance ICT equipment, the ACSC will conduct an assessment of the patch or update. Subsequently, if the patch or update is approved for deployment, the ACSC will provide guidance on the methods and timeframes in which it is to be applied.

Security Control: ISM-1690; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3
Patches, updates or vendor mitigations for security vulnerabilities in internet-facing services are applied within two weeks of release, or within 48 hours if an exploit exists.

Security Control: ISM-1691; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3
Patches, updates or vendor mitigations for security vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within two weeks of release.

Security Control: ISM-1692; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML3
Patches, updates or vendor mitigations for security vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within 48 hours if an exploit exists.

Security Control: ISM-1693; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3
Patches, updates or vendor mitigations for security vulnerabilities in other applications are applied within one month.

Security Control: ISM-1694; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3
Patches, updates or vendor mitigations for security vulnerabilities in operating systems of internet-facing services are applied within two weeks of release, or within 48 hours if an exploit exists.

Security Control: ISM-1695; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3
Patches, updates or vendor mitigations for security vulnerabilities in operating systems of workstations, servers and network devices are applied within two weeks of release.

Security Control: ISM-1696; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML3
Patches, updates or vendor mitigations for security vulnerabilities in operating systems of workstations, servers and network devices are applied within 48 hours if an exploit exists.

Security Control: ISM-1751; Revision: 0; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Patches, updates or vendor mitigations for security vulnerabilities in operating systems of other ICT equipment are applied within two weeks of release, or within 48 hours if an exploit exists.

Security Control: ISM-1697; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: N/A
Patches, updates or vendor mitigations for security vulnerabilities in drivers and firmware are applied within two weeks of release, or within 48 hours if an exploit exists.

Security Control: ISM-0300; Revision: 8; Updated: Mar-22; Applicability: S, TS; Essential Eight: N/A
Patches, updates or vendor mitigations for security vulnerabilities in high assurance ICT equipment are applied only when approved by the ACSC, and in doing so, using methods and timeframes prescribed by the ACSC.

Scanning for missing patches or updates

To ensure that patches or updates have been applied to applications, operating systems, drivers and firmware, it is essential that an organisation scan for missing patches or updates on a regular basis using a vulnerability scanner, preferably in an automated manner. Ideally, vulnerability scanning should take place at half the frequency in which patches or updates need to be applied. For example, if patches or updates are applied fortnightly then vulnerability scanning should be undertaken weekly.

Security Control: ISM-1698; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3
A vulnerability scanner is used at least daily to identify missing patches or updates for security vulnerabilities in internet-facing services.

Security Control: ISM-1699; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3
A vulnerability scanner is used at least weekly to identify missing patches or updates for security vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products.

Security Control: ISM-1700; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3
A vulnerability scanner is used at least fortnightly to identify missing patches or updates for security vulnerabilities in other applications.

Security Control: ISM-1701; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3
A vulnerability scanner is used at least daily to identify missing patches for security vulnerabilities in operating systems of internet-facing services.

Security Control: ISM-1702; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3
A vulnerability scanner is used at least weekly to identify missing patches for security vulnerabilities in operating systems of workstations, servers and network devices.

Security Control: ISM-1752; Revision: 0; Updated: Mar-22; Applicability: All; Essential Eight: N/A
A vulnerability scanner is used at least weekly to identify missing patches for security vulnerabilities in operating systems of other ICT equipment.

Security Control: ISM-1703; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: N/A
A vulnerability scanner is used at least weekly to identify missing patches for security vulnerabilities in drivers and firmware.

Cessation of support

When applications, operating systems, network devices and other ICT equipment reach their cessation date for support, an organisation will find it increasingly difficult to protect them against security vulnerabilities as patches, updates and other forms of support will no longer be made available by vendors. As such, unsupported applications, operating systems, network devices and other ICT equipment should be removed or replaced. In planning for such activities, it is important to note that while vendors generally advise the cessation date for support of operating systems well in advance, some applications, network devices and other ICT equipment may cease to receive support immediately after newer versions are released.

Security Control: ISM-1704; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3
Internet-facing services, office productivity suites, web browsers and their extensions, email clients, PDF software, Adobe Flash Player, and security products that are no longer supported by vendors are removed.

Security Control: ISM-0304; Revision: 6; Updated: Sep-21; Applicability: All; Essential Eight: ML3
Applications that are no longer supported by vendors are removed.

Security Control: ISM-1501; Revision: 1; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3
Operating systems that are no longer supported by vendors are replaced.

Security Control: ISM-1753; Revision: 0; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Network devices and other ICT equipment that are no longer supported by vendors are replaced.

Further information

Further information on system patching can be found in the ACSC's *Assessing Security Vulnerabilities and Applying Patches* publication.

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

Data backup and restoration

Digital preservation policy

Developing and implementing a digital preservation policy, as part of digital continuity planning, can assist in ensuring the long term integrity and availability of important data is maintained, especially when taking into account the potential for data degradation and removable media, hardware and software obsolesce.

Security Control: ISM-1510; Revision: 1; Updated: Aug-19; Applicability: All; Essential Eight: N/A
A digital preservation policy is developed and implemented.

Data backup and restoration processes and procedures

Having data backup and restoration processes and procedures is an important part of business continuity and disaster recovery planning. Such activities will also form an integral part of an overarching digital preservation policy.

Security Control: ISM-1547; Revision: 1; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Data backup processes, and supporting data backup procedures, are developed and implemented.

Security Control: ISM-1548; Revision: 1; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Data restoration processes, and supporting data restoration procedures, are developed and implemented.

Performing and retaining backups

When performing backups, all important data, software and configuration settings should be captured in a coordinated and resilient manner on a regular basis in accordance with business continuity requirements. This will ensure that should a system fall victim to a ransomware attack, important data will not be lost and, if necessary, systems can be quickly restored.

Security Control: ISM-1511; Revision: 2; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3
Backups of important data, software and configuration settings are performed and retained in a coordinated and resilient manner in accordance with business continuity requirements.

Backup access and modification

To mitigate the security risk of backups being accidentally or maliciously modified or deleted, an organisation should ensure that backups are sufficiently protected from unauthorised modification and deletion through the use of appropriate access controls.

Security Control: ISM-1705; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3
Unprivileged accounts, and privileged accounts (excluding backup administrators) cannot access other account's backups.

Security Control: ISM-1706; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML3
Unprivileged accounts, and privileged accounts (excluding backup administrators) cannot access their own account's backups.

Security Control: ISM-1707; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3
Unprivileged accounts, and privileged accounts (excluding backup administrators), are prevented from modifying or deleting backups.

Security Control: ISM-1708; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML3
Backup administrators (excluding backup break glass accounts), are prevented from modifying or deleting backups.

Testing restoration of backups

To ensure that backups can be restored when the need arises, and that any dependencies can be identified and managed beforehand, it is important that the restoration of systems, software and important data from backups is tested in a coordinated manner as part of disaster recovery exercises.

Security Control: ISM-1515; Revision: 2; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3
Restoration of systems, software and important data from backups is tested in a coordinated manner as part of disaster recovery exercises.

Further information

Further information on preserving digital information is available from the National Archives of Australia.

Further information on business continuity and disaster recovery planning can be found in the Chief Information Security Officer section of the *Guidelines for Cyber Security Roles*.

Guidelines for System Monitoring

Event logging and monitoring

Event logging policy

By developing an event logging policy, taking into consideration any shared responsibilities between service providers and their customers, an organisation can improve their chances of detecting malicious behaviour on their systems. In doing so, an event logging policy should cover details of events to be logged, event logging facilities to be used, how event logs will be monitored and how long to retain event logs.

Security Control: ISM-0580; Revision: 6; Updated: Aug-19; Applicability: All; Essential Eight: N/A
An event logging policy is developed and implemented.

Event log details

For each event logged, sufficient detail needs to be recorded in order for the event log to be useful.

Security Control: ISM-0585; Revision: 5; Updated: Mar-22; Applicability: All; Essential Eight: N/A
For each event logged, the date and time of the event, the relevant user or process, the relevant filename, the event description, and the ICT equipment involved are recorded.

Event logging facility

A centralised event logging facility can be used to manage event logs from multiple sources in a coordinated manner. This may be achieved by using a Security Information and Event Management solution. Furthermore, in support of a centralised event logging facility, it is important that an accurate time source is established and used consistently across systems to assist with identifying connections between events.

Security Control: ISM-1405; Revision: 2; Updated: Mar-22; Applicability: All; Essential Eight: N/A
A centralised event logging facility is implemented and systems are configured to save event logs to the facility as soon as possible after each event occurs.

Security Control: ISM-0988; Revision: 6; Updated: Mar-22; Applicability: All; Essential Eight: N/A
An accurate time source is established and used consistently across systems to assist with identifying connections between events.

Event log monitoring

Event log monitoring is critical to maintaining the security posture of systems. Notably, such activities involve analysing event logs in a timely manner to detect cyber security events, thereby, leading to the identification of cyber security incidents.

Security Control: ISM-0109; Revision: 8; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Event logs are analysed in a timely manner to detect cyber security events.

Security Control: ISM-1228; Revision: 3; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Cyber security events are analysed in a timely manner to identify cyber security incidents.

Event log retention

As event logs are integral to event log monitoring activities, they should be retained for the life of systems, potentially longer. However, the minimum retention period required under the National Archives of Australia's *Administrative Functions Disposal Authority Express Version 2* publication is seven years.

Security Control: ISM-0859; Revision: 3; Updated: Jan-20; Applicability: All; Essential Eight: N/A
Event logs are retained for a minimum of 7 years in accordance with the National Archives of Australia's Administrative Functions Disposal Authority Express Version 2 publication.

Security Control: ISM-0991; Revision: 5; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Domain Name System and web proxy event logs are retained for at least 18 months.

Further information

Further information on logging intrusion activity can be found in the detecting cyber security incidents section of the *Guidelines for Cyber Security Incidents*.

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

Further information on event logging for operating systems can be found in the operating system hardening section of the *Guidelines for System Hardening*.

Further information on event logging for applications can be found in the application hardening section of the *Guidelines for System Hardening*.

Further information on event logging for web applications can be found in the web application development section of the *Guidelines for Software Development*.

Further information on event logging for databases can be found in the databases section of the *Guidelines for Database Systems*.

Further information on event logging for gateways can be found in the gateways section of the *Guidelines for Gateways*.

Further information on event logging and forwarding can be found in the Australian Cyber Security Centre's *Windows Event Logging and Forwarding* publication.

Guidelines for Software Development

Application development

Types of application development

These guidelines are applicable to both traditional application development and mobile application development.

Development, testing and production environments

Segregating development, testing and production environments, and associated data, can limit the spread of malicious code and minimises the likelihood of faulty code being introduced into a production environment. Furthermore, protecting the authoritative source for software is critical to preventing malicious code being surreptitiously introduced into software.

Security Control: ISM-0400; Revision: 5; Updated: Aug-20; Applicability: All; Essential Eight: N/A
Development, testing and production environments are segregated.

Security Control: ISM-1419; Revision: 1; Updated: Sep-18; Applicability: All; Essential Eight: N/A
Development and modification of software only takes place in development environments.

Security Control: ISM-1420; Revision: 4; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Data from production environments is not used in a development or testing environment unless the environment is secured to the same level as the production environment.

Security Control: ISM-1422; Revision: 3; Updated: Sep-18; Applicability: All; Essential Eight: N/A
Unauthorised access to the authoritative source for software is prevented.

Secure software design and development

Secure-by-design principles and secure programming practices, supported by threat modelling, are an important part of application development as they can assist with the identification and mitigation of at risk software components and risky programming practices.

Security Control: ISM-0401; Revision: 5; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Secure-by-design principles and secure programming practices are used as part of application development.

Security Control: ISM-1238; Revision: 4; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Threat modelling is used in support of application development.

Software bill of materials

A software bill of materials is a list of open source and commercial software components used in application development. This can assist in providing greater cyber supply chain transparency for consumers by allowing for easier identification and management of security risks associated with individual software components used by applications.

Security Control: ISM-1730; Revision: 0; Updated: Dec-21; Applicability: All; Essential Eight: N/A
A software bill of materials is produced and made available to consumers of software.

Application testing and maintenance

Application testing and maintenance activities can lessen the likelihood of security vulnerabilities in applications being introduced into a production environment. Robust application testing can be performed using both static testing, such as code analysis, as well as dynamic testing, such as input validation and fuzzing. Vulnerability scanning tools can also assist in the detection of known security vulnerabilities, such as out-of-date or vulnerable software components. Using an independent party for application testing will remove any bias that can occur when a software developer tests their own applications.

Security Control: ISM-0402; Revision: 4; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Applications are robustly tested for security vulnerabilities by software developers, as well as independent parties, prior to their initial release and following any maintenance activities.

Security Control: ISM-1754; Revision: 0; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Security vulnerabilities identified in applications are resolved by software developers.

Vulnerability disclosure program

Implementing a vulnerability disclosure program, based on responsible disclosure, can assist an organisation to improve the security of their products and services as it provides a way for security researchers and other members of the public to responsibly notify them of security vulnerabilities in a coordinated manner. Furthermore, following the verification and resolution of reported security vulnerabilities, it can assist an organisation in notifying their customers of security vulnerabilities that have been discovered in their products and services, and any patches, updates or vendor mitigations that should be applied.

A vulnerability disclosure program should include processes and procedures for receiving, verifying, resolving and reporting security vulnerabilities disclosed by both internal and external parties. In support of this, a vulnerability disclosure policy should be made publicly available that covers:

- the purpose of the vulnerability disclosure program
- types of security research that are and are not allowed
- how to report any security vulnerabilities
- actions, and associated timeframes, upon notification of security vulnerabilities
- expectations regarding the public disclosure of security vulnerabilities
- any recognition or reward for finders of security vulnerabilities.

Finally, the Australian Cyber Security Centre (ACSC) encourages security researchers and other members of the public to responsibility report security vulnerabilities directly to an organisation. However, the ACSC recognises that this is not always practical, initial attempts at communication may be unsuccessful or the person making the report may not wish to do so directly. In such cases, security vulnerabilities can be reported to the ACSC as an independent coordinator.

Security Control: ISM-1616; Revision: 0; Updated: Aug-20; Applicability: All; Essential Eight: N/A
A vulnerability disclosure program is implemented to assist with the secure development and maintenance of products and services.

Security Control: ISM-1755; Revision: 0; Updated: Mar-22; Applicability: All; Essential Eight: N/A
A vulnerability disclosure policy is developed and implemented.

Security Control: ISM-1756; Revision: 0; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Vulnerability disclosure processes, and supporting vulnerability disclosure procedures, are developed and implemented.

Security Control: ISM-1717; Revision: 1; Updated: Mar-22; Applicability: All; Essential Eight: N/A
A 'security.txt' file is hosted for all internet-facing organisational domains to assist in the responsible disclosure of security vulnerabilities in an organisation's products and services.

Further information

Further information on a secure development life cycle model, known as *The Trustworthy Computing Security Development Lifecycle*, is available from Microsoft.

Further information on secure programming practices is available from the Carnegie Mellon University's Software Engineering Institute.

Further information on cyber supply chain transparency, and recommended content for a software bill of materials, can be found in the United States' National Telecommunications and Information Administration's *The Minimum Elements For a Software Bill of Materials (SBOM)* publication.

Further information on implementing a vulnerability disclosure program can be found in:

- Google's *Starting a Vulnerability Disclosure Program*
- European Union Agency for Cybersecurity's *Good Practice Guide on Vulnerability Disclosure*
- Netherland's National Cyber Security Centre's *Coordinated Vulnerability Disclosure: The Guideline*
- Carnegie Mellon University's *The CERT Guide to Coordinated Vulnerability Disclosure*
- International Organization for Standardization/International Electrotechnical Commission 29147:2018, *Information technology – Security techniques – Vulnerability disclosure*
- International Organization for Standardization/International Electrotechnical Commission 30111:2019, *Information technology – Security techniques – Vulnerability handling processes*.

Further information on recommended contents for a 'security.txt' file is available to assist an organisation with their implementation.

Further information on reporting security vulnerabilities to the ACSC as an independent coordinator is available from the ACSC.

Web application development

Open Web Application Security Project

The Open Web Application Security Project (OWASP) provides comprehensive resources for software developers that should be followed when developing web applications.

Security Control: ISM-0971; Revision: 7; Updated: Apr-19; Applicability: All; Essential Eight: N/A
The OWASP Application Security Verification Standard is followed when developing web applications.

Web application frameworks

Web application frameworks can be leveraged by software developers to enhance the security of web applications while decreasing development time. These resources can assist in securely implementing complex software functions, such as session management, input handling and cryptographic operations.

Security Control: ISM-1239; Revision: 4; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Robust web application frameworks are used in the development of web applications.

Web application interactions

Hypertext Transfer Protocol Secure (HTTPS) is the Hypertext Transfer Protocol secure by Transport Layer Security (TLS) encryption. The use of HTTPS for web applications ensures that not only are interactions with web applications confidential, but the integrity of interactions are also maintained.

Security Control: ISM-1552; Revision: 0; Updated: Oct-19; Applicability: All; Essential Eight: N/A
All web application content is offered exclusively using HTTPS.

Web application input handling

Most web application security vulnerabilities are caused by a lack of secure input handling. As such, it is essential that web applications do not trust any input, such as website addresses and their parameters, Hypertext Markup Language (HTML) form data, cookie values, or request headers, without performing validation or sanitisation. Examples of validation and sanitisation include ensuring a telephone form field contains only numerals, ensuring data used in a Structured Query Language query is sanitised properly and ensuring Unicode input is handled appropriately.

Security Control: ISM-1240; Revision: 3; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Validation or sanitisation is performed on all input handled by web applications.

Web application output encoding

The likelihood of cross-site scripting and other content injection attacks can be reduced through the use of output encoding. In particular, output encoding is useful when external data sources, which may not be subject to the same level of input filtering, are output to users. The most common example of output encoding is the conversion of potentially dangerous HTML characters into their encoded equivalents, such as '<', '>' and '&' into '&lt;', '&gt;' and '&amp;'.

Security Control: ISM-1241; Revision: 4; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Output encoding is performed on all output produced by web applications.

Web browser-based security controls

Web browser-based security controls, such as Content-Security-Policy, Hypertext Transfer Protocol Strict Transport Security (HSTS) and X-Frame-Options, can be used by web applications to help protect themselves and their users. This is achieved via setting security policy in response headers from web applications which web browsers then apply. Note, since the security controls are applied via response headers, they can be applied to legacy or proprietary web applications where changes to their source code may be impractical.

Security Control: ISM-1424; Revision: 4; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Web applications implement Content-Security-Policy, HSTS and X-Frame-Options via security policy in response headers.

Web application event logging

Certain web application events can assist in monitoring the security posture of web applications, detecting malicious behaviour and contributing to investigations following cyber security incidents. In doing so, web application event logs should be centrally stored and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.

Security Control: ISM-1536; Revision: 1; Updated: Mar-22; Applicability: All; Essential Eight: N/A
The following events are logged for web applications: attempted access that is denied, crashes and error messages, and search queries initiated by users.

Security Control: ISM-1757; Revision: 0; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Web application event logs are centrally stored and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.

Further information

Further information on web application security can be found in the OWASP *Application Security Verification Standard* publication.

Further information on implementing HTTPS can be found in the ACSC's *Implementing Certificates, TLS, HTTPS and Opportunistic TLS* publication.

Further information on using TLS in HTTPS can be found in the Transport Layer Security section of the *Guidelines for Cryptography*.

Further information on web application security can be found in the ACSC's *Protecting Web Applications and Users* and *Securing Content Management Systems* publications.

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

Guidelines for Database Systems

Database servers

Functional separation between database servers and web servers

Due to the higher threat environment that web servers are typically exposed to, hosting database servers and web servers within the same operating environment increases the likelihood of database servers being compromise by an adversary. This security risk can be mitigated by ensuring that database servers are functionally separated from web servers.

Security Control: ISM-1269; Revision: 3; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Database servers and web servers are functionally separated.

Communications between database servers and web servers

Data communicated between database servers and web servers, especially over the internet, is susceptible to capture by an adversary. As such, it is important that all data communicated between database servers and web servers is encrypted.

Security Control: ISM-1277; Revision: 4; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Data communicated between database servers and web servers is encrypted.

Network environment

Placing database servers on the same network segment as user workstations can increase the likelihood of database servers being compromise by an adversary. Additionally, in cases where databases will only be accessed from their own database server, allowing remote access to the database server poses an unnecessary security risk.

Security Control: ISM-1270; Revision: 3; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Database servers are placed on a different network segment to user workstations.

Security Control: ISM-1271; Revision: 2; Updated: Jan-20; Applicability: All; Essential Eight: N/A
Network access controls are implemented to restrict database server communications to strictly defined network resources, such as web servers, application servers and storage area networks.

Security Control: ISM-1272; Revision: 1; Updated: Sep-18; Applicability: All; Essential Eight: N/A
If only local access to a database is required, networking functionality of database management system (DBMS) software is disabled or directed to listen solely to the localhost interface.

Separation of development, testing and production database servers

Using production database servers for development and testing activities could result in accidental damage to their integrity or contents.

Security Control: ISM-1273; Revision: 3; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Development and testing environments do not use the same database servers as production environments.

Further information

Further information on the functional separation of computing environments can be found in the virtualisation hardening section of the *Guidelines for System Hardening*.

Further information on encrypting communications can be found in the cryptographic fundamentals section of the *Guidelines for Cryptography*.

Further information on network segmentation and segregation can be found in the network design and configuration section of the *Guidelines for Networking*.

Database management system software

Temporary installation files and logs

DBMS software will often leave behind temporary installation files and logs during the installation process in case a database administrator needs to troubleshoot a failed installation. These files, which can include credentials, could be valuable to an adversary.

Security Control: ISM-1245; Revision: 2; Updated: Sep-18; Applicability: All; Essential Eight: N/A
All temporary installation files and logs are removed after DBMS software has been installed.

Hardening and configuration

Poorly configured DBMS software could provide an opportunity for an adversary to gain unauthorised access to database contents. To assist an organisation in deploying DBMS software, vendors often provide guidance on how to securely configure their products.

Security Control: ISM-1246; Revision: 2; Updated: Sep-18; Applicability: All; Essential Eight: N/A
DBMS software is configured according to vendor guidance.

Security Control: ISM-1247; Revision: 3; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Unneeded accounts, components, services and functionality of DBMS software are disabled or removed.

Restricting privileges

If DBMS software operating as a local administrator or root account is compromised by an adversary, it can present a significant security risk to the underlying database server. In addition, DBMS software is often capable of accessing files that it has read access to on the database server. For example, an adversary performing a Structured Query Language (SQL) injection attack could use the command *LOAD DATA LOCAL INFILE 'etc/passwd' INTO TABLE Users;* or *SELECT LOAD_FILE('/etc/passwd');* to access the contents of a Linux password file. Disabling the ability of the DBMS software to read local files from its database server will prevent such SQL injection attacks from succeeding.

Security Control: ISM-1249; Revision: 2; Updated: Sep-18; Applicability: All; Essential Eight: N/A
DBMS software is configured to run as a separate account with the minimum privileges needed to perform its functions.

Security Control: ISM-1250; Revision: 1; Updated: Sep-18; Applicability: All; Essential Eight: N/A
The account under which DBMS software runs has limited access to non-essential areas of the database server's file system.

Security Control: ISM-1251; Revision: 3; Updated: Mar-22; Applicability: All; Essential Eight: N/A
The ability of DBMS software to read local files from its database server is disabled.

Database administrator accounts

DBMS software often comes pre-configured with default database administrator accounts and credentials that are listed in vendor documentation. These default database administrator accounts should be disabled, renamed or have their credentials changed.

When sharing database administrator accounts for the performance of administrative activities, any actions undertaken will not be attributable to an individual database administrator. This can hinder investigations relating to an attempted or successful intrusion. Furthermore, database administrator accounts shared across different databases can exacerbate any compromise of a database administrator account by an adversary.

When creating new database administrator accounts, accounts are often allocated all privileges available to system administrators. However, most database administrators will only require a subset of all available privileges to undertake their duties.

Security Control: ISM-1260; Revision: 3; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Default database administrator accounts are disabled, renamed or have their credentials changed.

Security Control: ISM-1262; Revision: 1; Updated: Sep-18; Applicability: All; Essential Eight: N/A
Database administrators have unique and identifiable accounts.

Security Control: ISM-1261; Revision: 2; Updated: Sep-18; Applicability: All; Essential Eight: N/A
Database administrator accounts are not shared across different databases.

Security Control: ISM-1263; Revision: 3; Updated: Sep-21; Applicability: All; Essential Eight: N/A
Database administrator accounts are used exclusively for administrative activities, with standard database accounts used for general purpose interactions with databases.

Security Control: ISM-1264; Revision: 1; Updated: Sep-18; Applicability: All; Essential Eight: N/A
Database administrator access is restricted to defined roles rather than accounts with default administrative permissions or all permissions.

Further information

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

Databases

Database register

Without knowledge of all the databases in an organisation, and their contents, an organisation will be unable to appropriately protect their assets.

Security Control: ISM-1243; Revision: 5; Updated: Mar-22; Applicability: All; Essential Eight: N/A
A database register is maintained and verified on a regular basis.

Protecting databases

Databases can be protected from unauthorised copying, and subsequent offline analysis, by applying file-based access controls to database files.

Security Control: ISM-1256; Revision: 3; Updated: Sep-18; Applicability: All; Essential Eight: N/A
File-based access controls are applied to database files.

Protecting database contents

Database administrators and database users should know the sensitivity or classification associated with databases and their contents. In cases where all of a database's contents are the same sensitivity or classification, an organisation should classify the entire database at this level and protect it as such. Alternatively, in cases where a database's contents are of varying sensitivities or classifications, and database users have varying levels of access to the database's contents, an organisation should protect the database's contents at a more granular level.

Restricting database users' ability to access, insert, modify or remove database contents, based on their work duties, ensures that the likelihood of unauthorised access, modification or deletion of database contents is reduced.

Furthermore, where concerns exist that the aggregation of separate pieces of content from within a database could lead to an adversary determining more sensitive or classified content, the need-to-know principle can be enforced through the use of minimum privileges, database views and database roles. Alternatively, the content of concern could be separated by implementing multiple databases, each with restricted data sets.

Security Control: ISM-0393; Revision: 8; Updated: Jun-21; Applicability: All; Essential Eight: N/A
Databases and their contents are classified based on the sensitivity or classification of data that they contain.

Security Control: ISM-1255; Revision: 4; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Database users' ability to access, insert, modify and remove database contents is restricted based on their work duties.

Security Control: ISM-1268; Revision: 1; Updated: Sep-18; Applicability: All; Essential Eight: N/A
The need-to-know principle is enforced for database contents through the application of minimum privileges, database views and database roles.

Separation of development, testing and production databases

Using database contents from production environments in development or testing environments could result in inadequate protection being applied to the database contents.

Security Control: ISM-1274; Revision: 6; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Database contents from production environments are not used in development or testing environments unless the environment is secured to the same level as the production environment.

Web application interaction with databases

SQL injection attacks are a significant threat to the confidentiality, integrity and availability of database contents. Specifically, SQL injection attacks can allow an adversary to steal database contents, modify database contents, delete an entire database or even in some circumstances gain control of the underlying database server. Furthermore, when database queries from web applications fail they may display detailed error information about the structure of databases. This can be used by an adversary to further tailor SQL injection attacks.

Security Control: ISM-1275; Revision: 1; Updated: Sep-18; Applicability: All; Essential Eight: N/A
All queries to databases from web applications are filtered for legitimate content and correct syntax.

Security Control: ISM-1276; Revision: 2; Updated: Sep-18; Applicability: All; Essential Eight: N/A
Parameterised queries or stored procedures are used for database interaction instead of dynamically generated queries.

Security Control: ISM-1278; Revision: 3; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Web applications are designed to provide as little error information as possible about the structure of databases.

Database event logging

Certain database events can assist in monitoring the security posture of databases, detecting malicious behaviour and contributing to investigations following cyber security incidents. In doing so, database event logs should be centrally stored and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.

Security Control: ISM-1537; Revision: 2; Updated: Mar-22; Applicability: All; Essential Eight: N/A
The following events are logged for databases:

- *access or modification of particularly important content*
- *addition of new users, especially privileged users*
- *changes to user roles or database permissions*
- *attempts to elevate privileges*

- *any query containing comments*
- *any query containing multiple embedded queries*
- *any query or database alerts or failures*
- *changes to the database structure*
- *database administrator actions*
- *use of executable commands*
- *database logons and logoffs.*

Security Control: ISM-1758; Revision: 0; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Database event logs are centrally stored and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.

Further information

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

Guidelines for Email

Email usage

Email usage policy

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

Security Control: ISM-0264; Revision: 3; Updated: Aug-19; Applicability: All; Essential Eight: N/A
An email usage policy is developed and implemented.

Webmail services

When users access non-approved webmail services, they often bypass security controls that have been implemented by an organisation, such as email content filtering. To mitigate this security risk, access to non-approved webmail services should be blocked.

Security Control: ISM-0267; Revision: 7; Updated: Mar-19; Applicability: All; Essential Eight: N/A
Access to non-approved webmail services is blocked.

Protective markings for emails

Implementing protective markings for emails helps to prevent data spills, such as unauthorised data being released into the public domain. In doing so, it is important that protective markings reflect the highest sensitivity or classification of the subject, body and attachments of emails.

Security Control: ISM-0270; Revision: 6; Updated: Jun-21; Applicability: All; Essential Eight: N/A
Protective markings are applied to emails and reflect the highest sensitivity or classification of the subject, body and attachments.

Protective marking tools

Requiring user involvement in the protective marking of emails ensures a conscious decision is made by users, thereby lessening the chance of incorrect protective markings being applied to emails. In addition, allowing users to select only protective markings for which a system is authorised to process, store or communicate lessens the chance of users inadvertently over-classifying emails.

Email content filters may only check the most recent protective marking applied to emails. Therefore, when users are responding to or forwarding emails, requiring protective markings which are at least as high as that of emails that are received will help email content filters prevent emails being sent to systems that are not authorised to handle their original sensitivity or classification.

Security Control: ISM-0271; Revision: 3; Updated: Mar-19; Applicability: All; Essential Eight: N/A
Protective marking tools do not automatically insert protective markings into emails.

Security Control: ISM-0272; Revision: 4; Updated: Mar-19; Applicability: All; Essential Eight: N/A
Protective marking tools do not allow users to select protective markings that a system has not been authorised to process, store or communicate.

Security Control: ISM-1089; Revision: 5; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Protective marking tools do not allow users replying to or forwarding emails to select protective markings lower than previously used.

Handling emails with inappropriate, invalid or missing protective markings

It is important that email servers are configured to block emails with inappropriate protective markings. For example, blocking inbound and outbound emails with protective markings higher than the sensitivity or classification of the receiving system, as this will prevent a data spill from occurring. In doing so, it is important to inform the intended recipients of blocked inbound emails, and the senders of blocked outbound emails, that this has occurred.

If emails are received with invalid or missing protective markings they may still be passed to their intended recipients. However, the recipients will have an obligation to determine appropriate protective markings if emails are to be responded to, forwarded or printed. If unsure, original senders of emails should be contacted to provide guidance on appropriate protective markings.

Security Control: ISM-0565; Revision: 4; Updated: Mar-19; Applicability: All; Essential Eight: N/A
Email servers are configured to block, log and report emails with inappropriate protective markings.

Security Control: ISM-1023; Revision: 6; Updated: Mar-22; Applicability: All; Essential Eight: N/A
The intended recipients of blocked inbound emails, and the senders of blocked outbound emails, are notified.

Email distribution lists

In some cases, the membership and nationality of members of email distribution lists will be unknown. As such, emails containing Australian Eyes Only, Australian Government Access Only or Releasable To data that are sent to email distribution lists could accidentally cause a data spill.

Security Control: ISM-0269; Revision: 5; Updated: Mar-22; Applicability: S, TS; Essential Eight: N/A
Emails containing Australian Eyes Only, Australian Government Access Only or Releasable To data are not sent to email distribution lists unless the nationality of all members of email distribution lists can be confirmed.

Further information

Further information on the Australian Government’s email protective marking standard can be found in the Attorney-General’s Department’s *Protective Security Policy Framework*, *Sensitive and classified information* policy.

Email gateways and servers

Centralised email gateways

By failing to route emails via a centralised email gateway, it will be difficult for an organisation to deploy Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), Domain-based Message Authentication, Reporting and Conformance (DMARC) and protective marking checks.

Security Control: ISM-0569; Revision: 4; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Emails are routed via a centralised email gateway.

Security Control: ISM-0571; Revision: 6; Updated: Mar-22; Applicability: All; Essential Eight: N/A
When users send or receive emails, an authenticated and encrypted channel is used to route emails via their organisation’s centralised email gateway.

Email gateway maintenance activities

As backup and alternative email gateways are often poorly maintained in terms of patches and email content filtering, an adversary will often seek to exploit this when sending malicious emails to an organisation. As such, it is important that backup and alternative email gateways are maintained at the same standard as an organisation’s primary email gateway.

Security Control: ISM-0570; Revision: 4; Updated: Sep-18; Applicability: All; Essential Eight: N/A
Where backup or alternative email gateways are in place, they are maintained at the same standard as the primary email gateway.

Open relay email servers

An open relay email server (or open mail relay) is an email server that is configured to allow anyone on the internet to send emails through it. Such configurations are highly undesirable as spammers and worms can exploit them.

Security Control: ISM-0567; Revision: 4; Updated: Mar-19; Applicability: All; Essential Eight: N/A
Email servers only relay emails destined for or originating from their domains.

Email server transport encryption

Emails can be intercepted anywhere between originating email servers and destination email servers. Implementing opportunistic Transport Layer Security (TLS) encryption can mitigate this security risk while ensuring email servers remain compatible with each other. However, opportunistic TLS encryption is susceptible to downgrade attacks. To mitigate this security risk, Mail Transfer Agent Strict Transport Security (MTA-STS) allows domain owners to indicate that email transfers should only occur if satisfactory TLS encryption is negotiated beforehand.

Implementing MTA-STS reduces the opportunity for downgrade attacks during email transfers, and provides visibility of when they are attempted. TLS reporting supports the implementation of MTA-STS by providing a mechanism for a domain owner to publish a location where reports can be submitted regarding the success or failure of attempts to initiate encrypted connections when sending emails to a specified domain.

Security Control: ISM-0572; Revision: 4; Updated: Sep-21; Applicability: All; Essential Eight: N/A
Opportunistic TLS encryption is enabled on email servers that make incoming or outgoing email connections over public network infrastructure.

Security Control: ISM-1589; Revision: 1; Updated: Sep-21; Applicability: All; Essential Eight: N/A
MTA-STS is enabled to prevent the transfer of unencrypted emails between complying servers.

Sender Policy Framework

SPF aids in the detection of spoofed emails by specifying a list of domains that are allowed to send emails. If an email server is not in the SPF record for a domain, SPF verification will fail. In specifying SPF records, domain owners should ensure that they delegate the minimum necessary set of hosts or Internet Protocol addresses necessary for sending emails. In addition, extra care should be taken when delegating to hosts or Internet Protocol addresses not under an organisation’s control.

Security Control: ISM-0574; Revision: 5; Updated: Mar-22; Applicability: All; Essential Eight: N/A
SPF is used to specify authorised email servers (or lack thereof) for all domains.

Security Control: ISM-1183; Revision: 1; Updated: Sep-18; Applicability: All; Essential Eight: N/A
A hard fail SPF record is used when specifying email servers.

Security Control: ISM-1151; Revision: 3; Updated: Oct-19; Applicability: All; Essential Eight: N/A
SPF is used to verify the authenticity of incoming emails.

Security Control: ISM-1152; Revision: 3; Updated: Mar-19; Applicability: All; Essential Eight: N/A
Incoming emails that fail SPF checks are blocked or marked in a manner that is visible to the recipients.

DomainKeys Identified Mail

DKIM enables the detection of spoofed email contents. This is achieved by DKIM records specifying the public key used to sign email contents. Specifically, if the signed digest in an email header does not match the signed contents of the email, verification will fail.

Security Control: ISM-0861; Revision: 2; Updated: Mar-19; Applicability: All; Essential Eight: N/A
DKIM signing is enabled on emails originating from an organisation's domains.

Security Control: ISM-1026; Revision: 5; Updated: Jan-20; Applicability: All; Essential Eight: N/A
DKIM signatures on received emails are verified.

Security Control: ISM-1027; Revision: 4; Updated: Sep-18; Applicability: All; Essential Eight: N/A
Email distribution list software used by external senders is configured such that it does not break the validity of the sender's DKIM signature.

Domain-based Message Authentication, Reporting and Conformance

DMARC enables a domain owner to specify what action receiving email servers should take if they receive emails that fail SPF or DKIM checks. This includes 'reject' (emails are rejected), 'quarantine' (emails are marked as spam) or 'none' (no action is taken).

DMARC also provides a reporting feature which enables a domain owner to receive reports on the actions taken by receiving email servers. While this feature does not mitigate malicious emails sent to the domain owner's organisation, it can give the domain owner some visibility of attempts by an adversary to spoof their organisation's domains.

Security Control: ISM-1540; Revision: 1; Updated: Oct-19; Applicability: All; Essential Eight: N/A
DMARC records are configured for all domains such that emails are rejected if they fail SPF or DKIM checks.

Email content filtering

Content filtering performed on email bodies and attachments provides a defence-in-depth approach to preventing malicious code being introduced into networks.

Security Control: ISM-1234; Revision: 4; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Email content filtering is implemented for email bodies and attachments.

Blocking suspicious emails

Blocking specific types of suspicious emails, such as where the source address uses an internal domain name, reduces the likelihood of phishing emails entering an organisation's network.

Security Control: ISM-1502; Revision: 1; Updated: Mar-19; Applicability: All; Essential Eight: N/A
Emails arriving via an external connection where the source address uses an internal domain name are blocked at the email gateway.

Notifications of undeliverable emails

Notifications of undeliverable emails are commonly sent by receiving email servers when emails cannot be delivered, usually because destination addresses are invalid. Due to the common spamming practice of spoofing sender addresses, this often results in a large number of notifications of undeliverable emails being sent to innocent third parties. Sending notifications of undeliverable emails only to senders that can be verified via SPF, or other trusted means, avoids contributing to this problem while allowing legitimate senders to be notified.

Security Control: ISM-1024; Revision: 5; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Notifications of undeliverable emails are only sent to senders that can be verified via SPF or other trusted means.

Further information

Further information on implementing opportunistic TLS encryption for email servers can be found in the Australian Cyber Security Centre (ACSC)'s *Implementing Certificates, TLS, HTTPS and Opportunistic TLS* publication.

Further information on implementing SPF, DKIM and DMARC can be found in the ACSC's *How to Combat Fake Emails* publication.

Further information on engaging the services of email service providers for marketing or filtering purposes can be found in the ACSC's *Marketing and Filtering Email Service Providers* publication.

Further information on email content filtering can be found in the content filtering section of the *Guidelines for Gateways*.

Further information on email content filtering can be found in the ACSC's *Malicious Email Mitigation Strategies* publication.

Further information on email security can be found in the following National Institute of Standards and Technology (NIST) publications:

- NIST Special Publication (SP) 800-45 Rev. 2, *Guidelines on Electronic Mail Security*
- NIST SP 800-177 Rev. 1, *Trustworthy Email*
- NIST SP 1800-6, *Domain Name System-Based Electronic Mail Security*.

Guidelines for Networking

Network design and configuration

Network documentation

It is important that network documentation is developed and accurately depicts the current state of networks, as this can assist in troubleshooting network problems as well as responding to and recovering from cyber security incidents. As such, network documentation should include, at a minimum, high-level network diagrams showing all connections into networks and logical network diagrams showing all critical servers, high-value servers, network devices and network security appliances. Finally, as network documentation could be used by an adversary to assist in compromising networks, it is important that it is appropriately protected.

Security Control: ISM-0516; Revision: 5; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Network documentation includes high-level network diagrams showing all connections into networks and logical network diagrams showing all critical servers, high-value servers, network devices and network security appliances.

Security Control: ISM-0518; Revision: 4; Updated: Sep-18; Applicability: All; Essential Eight: N/A
Network documentation is updated as network configuration changes are made and includes a 'current as at [date]' or equivalent statement.

Security Control: ISM-1178; Revision: 3; Updated: Sep-18; Applicability: All; Essential Eight: N/A
Network documentation provided to a third party, or published in public tender documentation, only contains details necessary for other parties to undertake contractual services.

Network segmentation and segregation

Network segmentation and segregation is one of the most effective security controls in preventing an adversary from easily propagating throughout networks once initial access has been gained. To achieve this, networks can be segregated into multiple network zones in order to protect servers, services and data. For example, administrative infrastructure used for managing critical servers, high-value servers and regular servers should be segregated from each other. In addition, all administrative infrastructure should be segregated from other assets on networks.

Security Control: ISM-1181; Revision: 5; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Networks are segregated into multiple network zones according to the criticality of servers, services and data.

Security Control: ISM-1577; Revision: 1; Updated: Mar-22; Applicability: All; Essential Eight: N/A
An organisation's networks are segregated from their service providers' networks.

Using Virtual Local Area Networks

Virtual Local Area Networks (VLANs) can be used to implement network segmentation and segregation as long as networks belong to the same security domain. In such cases, if a data spill occurs the impact will be less than if a data spill occurred between two networks of different classifications or between an organisation's network and public network infrastructure. Should an organisation choose to risk manage implementing VLANs between networks belonging to different security domains, such as at the same classification, additional security controls for network devices will apply, such as not sharing VLAN trunks and terminating VLANs on separate physical network interfaces.

For the purposes of this topic, Multiprotocol Label Switching is considered to be equivalent to VLANs and is subject to the same security controls.

Security Control: ISM-1532; Revision: 3; Updated: Mar-22; Applicability: All; Essential Eight: N/A
VLANs are not used to separate network traffic between an organisation's networks and public network infrastructure.

Security Control: ISM-0529; Revision: 6; Updated: Dec-21; Applicability: All; Essential Eight: N/A
VLANs are not used to separate network traffic between networks belonging to different security domains.

Security Control: ISM-0530; Revision: 6; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Network devices managing VLANs are administered from the most trusted security domain.

Security Control: ISM-0535; Revision: 6; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Network devices managing VLANs belonging to different security domains do not share VLAN trunks.

Security Control: ISM-1364; Revision: 3; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Network devices managing VLANs terminate VLANs belonging to different security domains on separate physical network interfaces.

Using Internet Protocol version 6

The use of Internet Protocol version 6 (IPv6) can introduce additional security risks to networks. As such, an organisation exclusively using Internet Protocol version 4 (IPv4) should disable IPv6. This will assist in minimising the attack surface of networks and ensure that IPv6 cannot be exploited by an adversary.

To aid in the transition from IPv4 to IPv6, numerous tunnelling protocols have been developed to allow interoperability between IPv4 and IPv6. Disabling IPv6 tunnelling protocols on networks that do not require such functionality will prevent an adversary from bypassing traditional network defences by encapsulating IPv6 data inside IPv4 packets.

Stateless Address Autoconfiguration is a method of stateless Internet Protocol (IP) address configuration in IPv6 networks. Notably, it reduces the ability of an organisation to maintain effective logs of IP address assignments on networks. For this reason, stateless IP addressing should be avoided.

Security Control: ISM-0521; Revision: 6; Updated: Mar-22; Applicability: All; Essential Eight: N/A
IPv6 functionality is disabled in dual-stack network devices unless it is being used.

Security Control: ISM-1186; Revision: 4; Updated: Mar-22; Applicability: All; Essential Eight: N/A
IPv6 capable network security appliances are used on IPv6 and dual-stack networks.

Security Control: ISM-1428; Revision: 2; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Unless explicitly required, IPv6 tunnelling is disabled on all network devices.

Security Control: ISM-1429; Revision: 3; Updated: Mar-22; Applicability: All; Essential Eight: N/A
IPv6 tunnelling is blocked by network security appliances at externally-connected network boundaries.

Security Control: ISM-1430; Revision: 3; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Dynamically assigned IPv6 addresses are configured with Dynamic Host Configuration Protocol version 6 in a stateful manner with lease data stored in a centralised event logging facility.

Network access controls

If an adversary has reduced opportunities to physically connect unauthorised network devices to networks, they also have reduced opportunities to compromise networks. Network access controls can not only prevent unauthorised physical access to networks, but also prevent personnel from carelessly bridging networks by connecting one network to another network. Furthermore, network access controls can also be useful for limiting the flow of network traffic between network segments.

Security Control: ISM-0520; Revision: 6; Updated: Sep-18; Applicability: All; Essential Eight: N/A
Network access controls are implemented on networks to prevent the connection of unauthorised network devices.

Security Control: ISM-1182; Revision: 4; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Network access controls are implemented to limit network traffic within and between network segments to only those required for business purposes.

Default accounts for network devices

Network devices can come pre-configured with default credentials. For example, wireless access points with an account named ‘admin’ and a password of ‘admin’. Ensuring default accounts are disabled, renamed or have their credentials changed can assist in reducing the likelihood of their exploitation by an adversary.

Security Control: ISM-1304; Revision: 3; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Default accounts for network devices are disabled, renamed or have their credentials changed.

Disabling unused physical ports on network devices

Disabling unused physical ports on network devices reduces the opportunity for an adversary to connect to networks if they can gain physical access to network devices.

Security Control: ISM-0534; Revision: 2; Updated: Sep-18; Applicability: All; Essential Eight: N/A
Unused physical ports on network devices are disabled.

Functional separation between servers

Implementing functional separation between servers reduces the likelihood that a server compromised by an adversary will pose an increased security risk to other servers.

Security Control: ISM-0385; Revision: 6; Updated: Sep-18; Applicability: All; Essential Eight: N/A
Servers maintain effective functional separation with other servers allowing them to operate independently.

Security Control: ISM-1479; Revision: 0; Updated: Sep-18; Applicability: All; Essential Eight: N/A
Servers minimise communications with other servers at both the network and file system level.

Network management traffic

Implementing security measures specifically for network management traffic provides another layer of defence should an adversary find an opportunity to connect to networks. In addition, this also makes it more difficult for an adversary to enumerate networks.

Security Control: ISM-1006; Revision: 6; Updated: Sep-18; Applicability: All; Essential Eight: N/A
Security measures are implemented to prevent unauthorised access to network management traffic.

Use of Simple Network Management Protocol

The Simple Network Management Protocol (SNMP) can be used to monitor the status of network devices. The first two iterations of SNMP were inherently insecure as they used trivial authentication methods. Furthermore, changing all default SNMP community strings on network devices, and limiting their access to read-only, is strongly encouraged.

Security Control: ISM-1311; Revision: 2; Updated: Sep-18; Applicability: All; Essential Eight: N/A
SNMP version 1 and 2 are not used on networks.

Security Control: ISM-1312; Revision: 3; Updated: Mar-22; Applicability: All; Essential Eight: N/A
All default SNMP community strings on network devices are changed and write access is disabled.

Using Network-based Intrusion Detection and Prevention Systems

A Network-based Intrusion Detection System (NIDS) or Network-based Intrusion Prevention System (NIPS) can be an effective way of identifying and responding to network intrusions. In addition, generating event logs and alerts for network traffic that contravenes any rule in a firewall ruleset can help identify suspicious or malicious network traffic entering networks due to a failure of, or configuration change to, firewalls.

Security Control: ISM-1028; Revision: 8; Updated: Mar-22; Applicability: All; Essential Eight: N/A

A NIDS or NIPS is deployed in gateways between an organisation's networks and other networks they do not manage.

Security Control: ISM-1030; Revision: 8; Updated: Mar-22; Applicability: All; Essential Eight: N/A
A NIDS or NIPS is located immediately inside the outermost firewall for gateways and configured to generate event logs and alerts for network traffic that contravenes any rule in a firewall ruleset.

Security Control: ISM-1185; Revision: 4; Updated: Mar-22; Applicability: All; Essential Eight: N/A
When deploying a NIDS or NIPS in non-internet gateways, it is configured for anomaly-based detection rather than signature-based detection.

Blocking anonymity network traffic

Inbound network connections from anonymity networks, such as the Tor network, to an organisation's internet-facing services can be used by an adversary for reconnaissance and malware delivery purposes with minimal risk of detection and attribution. As such, this network traffic should be blocked. However, an organisation might choose to support anonymous connections to their websites to cater for individuals who want to remain anonymous for privacy reasons. In such cases, it is suggested that network traffic from anonymity networks be logged and monitored instead. Additionally, outbound network connections to anonymity networks can be used by malware for command and control or data exfiltration purposes and should be blocked.

Security Control: ISM-1627; Revision: 0; Updated: Nov-20; Applicability: All; Essential Eight: N/A
Inbound network connections from anonymity networks to internet-facing services are blocked.

Security Control: ISM-1628; Revision: 0; Updated: Nov-20; Applicability: All; Essential Eight: N/A
Outbound network connections to anonymity networks are blocked.

Further information

Further information on wireless networks can be found in the wireless networks section of these guidelines.

Further information on gateways can be found in the gateways section of the *Guidelines for Gateways*.

Further information on network segmentation and segregation can be found in the Australian Cyber Security Centre (ACSC)'s *Implementing Network Segmentation and Segregation* publication.

Further information on implementing network segmentation and segregation for system administration purposes can be found in the system administration section of the *Guidelines for System Management*.

Further information on functional separation of servers using virtualisation can be found in the virtualisation hardening section of the *Guidelines for System Hardening*.

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

Further information on blocking anonymity network traffic can be found in the ACSC's *Defending Against the Malicious Use of the Tor Network* publication.

Further information on Domain Name System services can be found in the ACSC's *Domain Name System Security for Domain Owners* and *Domain Name System Security for Domain Resolvers* publications.

Further information on network design and configuration can be found in the United States' National Security Agency's *Network Infrastructure Security Guidance* publication.

Wireless networks

Wireless networks

This section describes the security controls applicable to wireless networks and extends upon the prior network design and configuration section.

Choosing wireless devices

Using wireless devices, such as wireless access points, wireless adapters and wireless network cards, which have been certified against a Wi-Fi Alliance certification program, provides an organisation with the assurance that they conform to wireless standards and are guaranteed to be interoperable with other wireless devices on wireless networks.

Security Control: ISM-1314; Revision: 2; Updated: Sep-21; Applicability: All; Essential Eight: N/A
All wireless devices are Wi-Fi Alliance certified.

Public wireless networks

When an organisation provides a public wireless network for general public use, connecting the public wireless network to, or sharing infrastructure with, any other organisation networks can create an entry point for an adversary allowing them to target organisation networks in order to steal data or disrupt services.

Security Control: ISM-0536; Revision: 7; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Public wireless networks provided for general public use are segregated from all other organisation networks.

Administrative interfaces for wireless access points

Administrative interfaces allow users to modify the configuration and security settings of wireless access points. Often, by default, wireless access points allow users to access administrative interfaces over fixed network connections or wireless network connections. To assist in reducing the attack surface for wireless access points, the administrative interface should be disabled for wireless network connections.

Security Control: ISM-1315; Revision: 2; Updated: Sep-18; Applicability: All; Essential Eight: N/A
The administrative interface on wireless access points is disabled for wireless network connections.

Default settings

Some wireless access points come with default Service Set Identifiers (SSIDs) or weak default configuration settings. As default SSIDs are often documented on the internet, along with default accounts and credentials, it is important to change default SSIDs of wireless access points along with default credentials and weak configuration settings.

When changing default SSIDs, it is important that new SSIDs do not bring undue attention to an organisation’s wireless networks. In doing so, SSIDs of wireless networks should not be readily associated with an organisation, the location of their premises or the functionality of wireless networks.

A method commonly recommended to lower the profile of wireless networks is disabling SSID broadcasting. While this ensures that the existence of wireless networks are not broadcast overtly using beacon frames, SSIDs are still broadcast in probe requests, probe responses, association requests and re-association requests. As such, it is easy to determine SSIDs of wireless networks by capturing these requests and responses. By disabling SSID broadcasting, an organisation will make it more difficult for users to connect to wireless networks. Furthermore, an adversary could configure a malicious wireless access point to broadcast the same SSID as a hidden SSID used by a legitimate wireless network, thereby fooling users or devices into automatically connecting to the adversary’s malicious wireless access point instead. In doing so, the adversary could steal authentication credentials in order to gain access to the legitimate wireless network.

Security Control: ISM-1316; Revision: 3; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Default SSIDs of wireless access points are changed.

Security Control: ISM-1317; Revision: 3; Updated: Mar-22; Applicability: All; Essential Eight: N/A
SSIDs of non-public wireless networks are not readily associated with an organisation, the location of their premises or the functionality of wireless networks.

Security Control: ISM-1318; Revision: 3; Updated: Mar-22; Applicability: All; Essential Eight: N/A
SSID broadcasting is not disabled on wireless access points.

Security Control: ISM-1709; Revision: 1; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Default accounts and credentials of wireless access points are changed.

Security Control: ISM-1710; Revision: 1; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Configuration settings for wireless access points are hardened.

Media Access Control address filtering

Devices that connect to wireless networks generally have a unique Media Access Control (MAC) address. Using MAC address filtering can prevent rogue devices from connecting to wireless networks. However, an adversary may be able to determine MAC addresses of legitimate devices and use this information to gain access to wireless networks. As such, MAC address filtering introduces management overhead without any tangible security benefit.

Security Control: ISM-1320; Revision: 2; Updated: Sep-18; Applicability: All; Essential Eight: N/A
MAC address filtering is not used to restrict which devices can connect to wireless networks.

Static addressing

Assigning static IP addresses for devices accessing wireless networks can prevent rogue devices connecting to wireless networks from being assigned routable IP addresses. However, an adversary may be able to determine IP addresses of legitimate devices and use this information to gain access to wireless networks. As such, configuring devices to use static IP addresses introduces management overhead without any tangible security benefit.

Security Control: ISM-1319; Revision: 2; Updated: Sep-18; Applicability: All; Essential Eight: N/A
Static addressing is not used for assigning IP addresses on wireless networks.

Confidentiality and integrity of wireless network traffic

As wireless networks are often capable of being accessed from outside the perimeter of secured spaces, all wireless network traffic requires suitable cryptographic protection. For this purpose it is recommended that Wi-Fi Protected Access 3 (WPA3) be used as it provides equivalent or greater security than its predecessor Wi-Fi Protected Access 2 (WPA2). WPA3 has also prohibited the use of various outdated and insecure cipher suites.

WPA3-Enterprise supports three enterprise modes of operation: enterprise only mode, transition mode and 192-bit mode. Preference is given to WPA3-Enterprise 192-bit mode as this mode incorporates changes that satisfy the United States' Commercial National Security Algorithm Suite requirements and ensures no algorithms with known weaknesses are used. However, if any other WPA3-Enterprise modes are used then Authentication and Key Management suite 00-0F-AC:1 should be disabled (if this option is available).

Security Control: ISM-1332; Revision: 3; Updated: Sep-21; Applicability: All; Essential Eight: N/A
WPA3-Enterprise 192-bit mode is used to protect the confidentiality and integrity of all wireless network traffic.

802.1X authentication

WPA3-Enterprise uses 802.1X authentication which requires the use of an Extensible Authentication Protocol (EAP). A number of EAP methods supported by both WPA2 and WPA3 are available.

Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) is considered one of the most secure EAP methods and is widely supported. It uses a Public Key Infrastructure to secure communications between devices and a Remote Access Dial-In User Service (RADIUS) server through the use of X.509 certificates. While EAP-TLS provides strong mutual authentication, it requires an organisation to have established a Public Key Infrastructure. This involves deploying their own certificate authority and issuing certificates, or purchasing certificates from a commercial certificate authority, for every device that accesses their wireless networks. While this introduces additional costs and management overheads, the security advantages are significant.

Security Control: ISM-1321; Revision: 2; Updated: Sep-21; Applicability: All; Essential Eight: N/A
802.1X authentication with EAP-TLS, using X.509 certificates, is used for mutual authentication; with all other EAP methods disabled on supplications and authentication servers.

Security Control: ISM-1711; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: N/A
User identity confidentiality is used if available with EAP-TLS implementations.

Evaluation of 802.1X authentication implementation

The security of 802.1X authentication is dependent on four main elements and how they interact with each other. These four elements include supplicants, authenticators, wireless access points and authentication servers. To provide assurance that these elements have been implemented correctly, they should have completed an evaluation.

Security Control: ISM-1322; Revision: 4; Updated: Sep-21; Applicability: All; Essential Eight: N/A
Evaluated supplicants, authenticators, wireless access points and authentication servers are used in wireless networks.

Generating and issuing certificates for authentication

When issuing certificates to devices in order to access wireless networks, an organisation should be aware that certificates could be stolen by malicious code. Once compromised, certificates could be used on other devices to gain unauthorised access to wireless networks. An organisation should also be aware that in only issuing certificates to devices, any actions taken by users will only be attributable to specific devices.

When issuing certificates to users in order to access wireless networks, it can be in the form of certificates that are stored on devices or certificates that are stored on smart cards. While issuing certificates on smart cards provides increased security, it comes at a higher cost. However, users are more likely to notice missing smart cards and alert their security team, who are then able to revoke their credentials, which can minimise the time an adversary has access to wireless networks. In addition, to reduce the likelihood of stolen smart cards from being used to gain unauthorised access to wireless networks, multi-factor authentication can be implemented through the use of personal identification numbers on smart cards. This is particularly important when smart cards grant users any form of administrative access.

Security Control: ISM-1324; Revision: 4; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Certificates are generated using an evaluated certificate authority or hardware security module.

Security Control: ISM-1323; Revision: 3; Updated: Sep-21; Applicability: All; Essential Eight: N/A
Certificates are required for both devices and users accessing wireless networks.

Security Control: ISM-1327; Revision: 2; Updated: Sep-21; Applicability: All; Essential Eight: N/A
Certificates are protected by encryption, user authentication, and both logical and physical access controls.

Caching 802.1X authentication outcomes

When 802.1X authentication is used, a shared secret key known as the Pairwise Master Key (PMK) is generated upon successful authentication of devices. This PMK is then capable of being cached to assist with fast roaming between wireless access points. When devices roam away from wireless access points they have authenticated to, they will not need to perform a full re-authentication should they roam back while the cached PMK remains valid. To further assist with roaming, wireless access points can be configured to pre-authenticate devices to neighbouring wireless access points that devices might roam to. Although requiring full authentication for devices each time they roam between wireless access points is ideal, an organisation can choose to use PMK caching and pre-authentication if they have a business requirement for fast roaming. If PMK caching is used, the PMK caching period should not be set to greater than 1440 minutes (24 hours).

Security Control: ISM-1330; Revision: 1; Updated: Sep-18; Applicability: All; Essential Eight: N/A
The PMK caching period is not set to greater than 1440 minutes (24 hours).

Fast Basic Service Set Transition

The WPA3 standard specifies support for Fast Basic Service Set Transition (FT) (802.11r). FT is a feature designed to improve user mobility and combat lag introduced by the need to authenticate to each wireless access point. However, FT requires authenticators to request and send keys to other authenticators within a security domain. If any of these keys are intercepted, all security properties are lost. Therefore, it is imperative that communications are appropriately secured. As such, FT should be disabled unless it can be confirmed that authenticator-to-authenticator communications are secured by a suitable ASD-Approved Cryptographic Protocol that provides confidentiality, integrity and mutual authentication.

Security Control: ISM-1712; Revision: 1; Updated: Mar-22; Applicability: All; Essential Eight: N/A
The use of FT (802.11r) is disabled unless authenticator-to-authenticator communications are secured by an ASD-Approved Cryptographic Protocol.

Remote Authentication Dial-In User Service authentication

Separate to the 802.1X authentication process is the RADIUS authentication process that occurs between authenticators and a RADIUS server. RADIUS is what is known as an authentication, authorisation and accounting protocol, and is intended to mediate network access. However, RADIUS is not secure enough to be used without protection. To protect credentials communicated between authenticators and a RADIUS server, communications should be encapsulated with an additional layer of encryption, such as RADIUS over Internet Protocol Security or RADIUS over Transport Layer Security.

Security Control: ISM-1454; Revision: 2; Updated: Sep-21; Applicability: All; Essential Eight: N/A
Communications between authenticators and a RADIUS server are encapsulated with an additional layer of encryption using RADIUS over Internet Protocol Security or RADIUS over Transport Layer Security.

Interference between wireless networks

When wireless networks are deployed in close proximity, there is the potential for interference to impact their availability, especially when operating on commonly used 802.11b/g (2.4 GHz) default channels of 1 and 11. Sufficiently separating wireless networks through the use of frequency separation can help reduce this security risk. This can be achieved by using wireless networks that are configured to operate on channels that minimise overlapping frequencies or by using both 802.11b/g (2.4 GHz) channels and 802.11n (5 GHz) channels. It is important to note though, if implementing a mix of 2.4 GHz and 5 GHz channels, not all devices may be compatible with 802.11n and able to connect to 5 GHz channels.

Security Control: ISM-1334; Revision: 2; Updated: Sep-18; Applicability: All; Essential Eight: N/A
Wireless networks implement sufficient frequency separation from other wireless networks.

Protecting management frames on wireless networks

An effective denial-of-service attack can be performed by exploiting unprotected management frames using inexpensive commercial hardware. The 802.11 standard provides no protection for management frames and therefore does not protect against spoofing or denial-of-service attacks. However, the 802.11w amendment specifically addresses the protection of management frames on wireless networks and should be enabled for WPA2. Note, in WPA3 this feature is built into the standard.

Security Control: ISM-1335; Revision: 1; Updated: Sep-18; Applicability: All; Essential Eight: N/A
Wireless access points enable the use of the 802.11w amendment to protect management frames.

Wireless network footprint

Instead of deploying a small number of wireless access points that broadcast on high power, a greater number of wireless access points that use less broadcast power can be deployed to achieve the desired footprint for wireless networks. This has the benefit of providing service continuity should wireless access points become unserviceable. In such cases, the output power of nearby wireless access points can be increased to cover the footprint gap until the unserviceable wireless access points can be replaced.

In addition to minimising the output power of wireless access points to reduce the footprint of wireless networks, the use of Radio Frequency (RF) shielding can be used for an organisation's facilities. While expensive, this will limit wireless communications to areas under the control of an organisation. RF shielding on an organisation's facilities also has the added benefit of preventing the jamming of wireless networks from outside of the facilities in which wireless networks are operating.

Security Control: ISM-1338; Revision: 2; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Instead of deploying a small number of wireless access points that broadcast on high power, a greater number of wireless access points that use less broadcast power are deployed to achieve the desired footprint for wireless networks.

Security Control: ISM-1013; Revision: 6; Updated: Dec-21; Applicability: S, TS; Essential Eight: N/A
The effective range of wireless communications outside an organisation's area of control is limited by implementing RF shielding on facilities in which SECRET or TOP SECRET wireless networks are used.

Further information

Further information on Wi-Fi technologies and associated certification programs are available from the Wi-Fi Alliance.

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

Further information on encrypting wireless network communications can be found in the cryptographic fundamentals section of the *Guidelines for Cryptography*.

Further information on the United States' Commercial National Security Algorithm Suite is available from the United States' National Security Agency.

Service continuity for online services

Cloud-based hosting of online services

Using cloud service providers can allow an organisation to build highly resilient online services due to the increased computing resources, bandwidth and multiple separate physical sites made available by the cloud server providers. An organisation can achieve the same results using their own infrastructure. However, doing so may require significant upfront costs and may still result in a limited capability to scale dynamically to meet increased demand. In case of a denial-of-service attack, cloud-based hosting can also provide segregation from self-hosted or other cloud-hosted services ensuring that other systems, such as email, are not affected.

Security Control: ISM-1437; Revision: 5; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Cloud service providers are used for hosting online services.

Location policies for online services

When using cloud service providers, an organisation will need to consider whether they should lock their data to specific regions or availability zones. In choosing to do so, an organisation will have an expectation that their data will not be relocated to different regions or availability zones by cloud service providers.

Security Control: ISM-1578; Revision: 2; Updated: Mar-22; Applicability: All; Essential Eight: N/A
An organisation is notified by cloud service providers of any change to configured regions or availability zones for online services.

Availability planning and monitoring for online services

It is important that connectivity between an organisation and their cloud service providers meets requirements for bandwidth, latency and reliability. In support of this, an organisation and their cloud service providers should discuss any specific network requirements, performance characteristics or planned responses to availability failures, especially when a requirement for high availability exists. Furthermore, an organisation and their cloud service providers should discuss whether dedicated communication links or connections over the internet will be used and whether any secondary communications links will provide sufficient capacity to maintain operational requirements should the primary communication link become unavailable.

Furthermore, capacity monitoring should be performed in order to manage workloads and monitor the health of online services. This can be achieved through continuous real-time monitoring of metrics, such as latency, jitter, packet loss, throughput and availability. In addition, feedback should be provided to cloud service providers when performance does not meet service level agreement targets. To assist with this, anomaly detection can be performed through network telemetry that is integrated into security monitoring tools.

Security Control: ISM-1579; Revision: 1; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Cloud service providers' ability to dynamically scale resources due to a genuine spike in demand or a denial-of-service attack is tested as part of capacity planning processes for online services.

Security Control: ISM-1580; Revision: 1; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Where a high availability requirement exists for online services, the services are architected to automatically transition between availability zones.

Security Control: ISM-1441; Revision: 3; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Where a requirement for high availability exists for online services, a denial of service mitigation service is used.

Security Control: ISM-1581; Revision: 2; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Continuous real-time monitoring of the availability of online services is performed.

Using content delivery networks

Similar to cloud-based hosting, the use of content delivery networks (CDNs) can allow an organisation to create highly resilient online services by leveraging the large bandwidth, geographically dispersed hosting locations, traffic scrubbing and other security controls offered by CDNs.

The use of CDNs is particularly effective when serving static bandwidth intensive media, such as images, sound or video files. However, the services offered by CDNs can include more than basic content hosting, such as web response caching, load balancing, web application security and denial of service mitigations.

Care should be taken when configuring the use of CDNs to ensure that the IP addresses of an organisation's web servers are not identifiable by an adversary, as this could allow for protections to be bypassed. Additionally, appropriate security controls should be applied to only allow communication between an organisation's web servers, CDNs and authorised management networks.

Security Control: ISM-1438; Revision: 2; Updated: Dec-21; Applicability: All; Essential Eight: N/A

Where a high availability requirement exists for website hosting, CDNs that cache websites are used.

Security Control: ISM-1439; Revision: 3; Updated: Mar-22; Applicability: All; Essential Eight: N/A
If using CDNs, disclosing the IP addresses of web servers under an organisation's control (referred to as origin servers) is avoided and access to the origin servers is restricted to the CDNs and authorised management networks.

Denial of service strategies

Denial-of-service attacks are designed to disrupt or degrade online services, such as website, email and Domain Name System services. To achieve this goal, an adversary may use a number of methods to deny access to legitimate users of online services. This includes using multiple computers to direct a large volume of unwanted network traffic at online services in an attempt to consume all available network bandwidth, using multiple computers to direct tailored network traffic at online services in an attempt to consume the processing resources of online services, or hijacking online services in an attempt to redirect legitimate users away from those services to other services that the adversary controls.

Although an organisation cannot avoid being targeted by denial-of-service attacks, there are a number of measures they can implement to prepare for and potentially reduce the impact if targeted. This includes engaging with their cloud service providers to identify the denial of service detection technologies that may be available for their use. For example, real-time capacity reporting dashboards that provide out-of-band and real-time alerts based on organisation-defined thresholds can assist with the rapid identification of denial-of-service attacks.

Finally, not all online services offered by an organisation may be business critical. Understanding what online services can be disabled or offered with reduced functionality during denial-of-service attacks can help an organisation reduce or eliminate the impact on essential services. Overall, preparing for denial-of-service attacks before they occur is by far the best strategy as it is very difficult to respond once they begin and efforts at this stage are unlikely to be effective.

Security Control: ISM-1431; Revision: 4; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Denial-of-service attack mitigation strategies are discussed with cloud service providers, specifically:

- *their capacity to withstand denial-of-service attacks*
- *any costs likely to be incurred as a result of denial-of-service attacks*
- *thresholds for notification of denial-of-service attacks*
- *thresholds for turning off online services during denial-of-service attacks*
- *pre-approved actions that can be undertaken during denial-of-service attacks*
- *any arrangements with upstream service providers to block malicious network traffic as far upstream as possible.*

Security Control: ISM-1458; Revision: 2; Updated: Dec-21; Applicability: All; Essential Eight: N/A
The functionality and quality of online services, how to maintain such functionality, and what functionality can be lived without during a denial-of-service attack, are determined and documented.

Domain name registrar locking

The use of domain name registrar locking can prevent a denial of service caused by unauthorised modification of a domain's registration details or unauthorised deletion or transfer of a domain.

Security Control: ISM-1432; Revision: 2; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Domain names for online services are protected via registrar locking and confirming domain registration details are correct.

Monitoring with real-time alerting for online services

An organisation should perform automated monitoring of online services with real-time alerting to ensure that a denial-of-service attack is detected and responded to as soon as possible.

Security Control: ISM-1435; Revision: 2; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Availability monitoring with real-time alerting is implemented for online services to detect denial-of-service attacks and measure their impact.

Segregation of critical online services

Denial-of-service attacks are typically focused on highly visible online services, such as an organisation's core website, in order to have a publicly noticeable impact. By segregating online services, such as using one internet connection for email and internet access, and a separate internet connection for web hosting services, the impact of a denial-of-service attack can be limited.

Security Control: ISM-1436; Revision: 2; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Critical online services are segregated from other online services that are more likely to be targeted.

Preparing for service continuity

An organisation's full-featured website may have higher processing or resource demands due to database integration or the presence of high-resolution images and videos. These additional resource requirements may make the website more susceptible to denial-of-service attacks. As such, depending on the nature of a denial-of-service attack, replacing the full-featured website with a minimal impact static version can help provide a level of service which would otherwise not be possible.

Security Control: ISM-1518; Revision: 1; Updated: Dec-21; Applicability: All; Essential Eight: N/A
A static version of a website is pre-prepared that requires minimal processing and bandwidth in order to facilitate at least a basic level of service when under a denial-of-service attack.

Further information

Further information on business continuity and disaster recovery planning can be found in the Chief Information Security Officer section of the *Guidelines for Cyber Security Roles*.

Further information on mitigating denial-of-service attacks can be found in the ACSC's *Preparing for and Responding to Denial-of-Service Attacks* publication.

Guidelines for Cryptography

Cryptographic fundamentals

Purpose of cryptography

The purpose of cryptography is to provide confidentiality, integrity, authentication and non-repudiation of data. In doing so, confidentiality protects data by making it unreadable to all but authorised entities, integrity protects data from accidental or deliberate manipulation by entities, authentication ensures that an entity is who they claim to be, and non-repudiation provides proof that an entity performed a particular action.

Using encryption

Encryption of data at rest can be used to protect sensitive or classified data stored on ICT equipment and media. In addition, encryption of data in transit can be used to protect sensitive or classified data communicated over public network infrastructure. However, when an organisation uses encryption for data at rest, or data in transit, they are not reducing the sensitivity or classification of the data, they are simply reducing the immediate consequences of the data being accessed by an adversary.

International standards for cryptographic modules

International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 19790:2012, *Information technology – Security techniques – Security requirements for cryptographic modules*, and ISO/IEC 24759:2017, *Information technology – Security techniques – Test requirements for cryptographic modules*, are international standards for the design and validation of hardware and software cryptographic modules.

Federal Information Processing Standard (FIPS) 140-3, *Security Requirements for Cryptographic Modules* and National Institute of Standards and Technology (NIST) Special Publication (SP) 180-140, *FIPS 140-3 Derived Test Requirements (DTR): CMVP Validation Authority Updates to ISO/IEC 24759* are United States standards based upon ISO/IEC 19790:2012 and ISO/IEC 24759:2017.

High assurance cryptography

The Australian Cyber Security Centre (ACSC) may specify additional requirements in Australian Communications Security Instructions and other cyber security-related publications for High Assurance Cryptographic Equipment (HACE). Such requirements supplement these guidelines and, where conflicts occur, take precedence.

Furthermore, due to the sensitive nature of HACE, areas in which HACE are used are separated from other areas and designated as cryptographic controlled areas.

Security Control: ISM-0499; Revision: 9; Updated: Jun-21; Applicability: S, TS; Essential Eight: N/A
All communications security and equipment-specific doctrine produced by the ACSC for the management and use of HACE is complied with.

Security Control: ISM-0506; Revision: 4; Updated: Mar-22; Applicability: S, TS; Essential Eight: N/A
Areas in which HACE are used are separated from other areas and designated as cryptographic controlled areas.

Encrypting data at rest

When encryption is applied to data at rest it provides an additional layer of defence against unauthorised access by an adversary. In doing so, it is important that full disk encryption is used as it provides a greater level of protection than file-based encryption. This is due to the fact that while file-based encryption may encrypt individual files, there is the possibility that unencrypted copies of files may be left in temporary locations used by an operating system.

Security Control: ISM-0457; Revision: 9; Updated: Mar-22; Applicability: O, P; Essential Eight: N/A
Cryptographic equipment or software that has completed a Common Criteria evaluation against a Protection Profile is used when encrypting media that contains OFFICIAL: Sensitive or PROTECTED data.

Security Control: ISM-0460; Revision: 11; Updated: Dec-21; Applicability: S, TS; Essential Eight: N/A
HACE is used when encrypting media that contains SECRET or TOP SECRET data.

Security Control: ISM-0459; Revision: 4; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Full disk encryption, or partial encryption where access controls will only allow writing to the encrypted partition, is implemented when encrypting data at rest.

Encrypting highly sensitive data at rest

Due to the sensitivities associated with Australian Eyes Only (AUSTEO) and Australian Government Access Only (AGAO) data, it needs to be encrypted when at rest.

Security Control: ISM-1080; Revision: 4; Updated: Mar-22; Applicability: S, TS; Essential Eight: N/A
An ASD-Approved Cryptographic Algorithm (AACA) or high assurance cryptographic algorithm is used to encrypt AUSTEO and AGAO data when at rest on a system.

Encrypting data in transit

Where insufficient security exists for the protection of data communicated in the clear over network infrastructure, encryption should be used to protect the data from unauthorised access or manipulation. For example, when sensitive or classified data is communicated over networks not authorised to communicate the data in the clear, when sensitive or classified data is communicated outside of appropriately secure areas, or when sensitive or classified data is communicated over public network infrastructure.

Security Control: ISM-0465; Revision: 9; Updated: Mar-22; Applicability: O, P; Essential Eight: N/A
Cryptographic equipment or software that has completed a Common Criteria evaluation against a Protection Profile is used to protect OFFICIAL: Sensitive or PROTECTED data when communicated over insufficiently secure networks, outside of appropriately secure areas or via public network infrastructure.

Security Control: ISM-0467; Revision: 10; Updated: Dec-21; Applicability: S, TS; Essential Eight: N/A
HACE is used to protect SECRET and TOP SECRET data when communicated over insufficiently secure networks, outside of appropriately secure areas or via public network infrastructure.

Encrypting highly sensitive data in transit

Due to the sensitivities associated with AUSTEO and AGAO data, it needs to be encrypted when communicated over network infrastructure.

Security Control: ISM-0469; Revision: 5; Updated: Mar-22; Applicability: S, TS; Essential Eight: N/A
An ASD-Approved Cryptographic Protocol (AACP) or high assurance cryptographic protocol is used to protect AUSTEO and AGAO data when communicated over network infrastructure.

Data recovery

To ensure that access to encrypted data is not lost due to the loss, damage or failure of an encryption key, it is important that where practical cryptographic equipment and software provides a means of data recovery.

Security Control: ISM-0455; Revision: 3; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Where practical, cryptographic equipment and software provides a means of data recovery to allow for circumstances where the encryption key is unavailable due to loss, damage or failure.

Handling encrypted ICT equipment and media

When a user authenticates to the encryption functionality of ICT equipment or media, encrypted data is made available. At such a time, the ICT equipment or media should be handled according to its original sensitivity or classification. Once the user deauthenticates from the encryption functionality, such as shutting down a device or activating a lock screen, the ICT equipment or media can be considered to be protected by the encryption functionality again.

Security Control: ISM-0462; Revision: 7; Updated: Mar-22; Applicability: All; Essential Eight: N/A
When a user authenticates to the encryption functionality of ICT equipment or media, it is treated in accordance with its original sensitivity or classification until the user deauthenticates from the encryption functionality.

Transporting cryptographic equipment

Transporting cryptographic equipment in a keyed state may expose its keying material to potential compromise. Therefore, if cryptographic equipment is transported in a keyed state it should be done based on the sensitivity or classification of its keying material.

Security Control: ISM-0501; Revision: 6; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Keyed cryptographic equipment is transported based on the sensitivity or classification of its keying material.

Reporting cryptographic-related cyber security incidents

If cryptographic equipment or associated keying material is compromised, or suspected of being compromised, then the confidentiality and integrity of previous and future communications may also be compromised. In such cases, the cyber security incident should be reported to an organisation's Chief Information Security Officer, or one of their delegates, as soon as possible after it occurs and all keying material should be changed.

Security Control: ISM-0142; Revision: 4; Updated: Dec-21; Applicability: All; Essential Eight: N/A
The compromise or suspected compromise of cryptographic equipment or associated keying material is reported to an organisation's Chief Information Security Officer, or one of their delegates, as soon as possible after it occurs.

Security Control: ISM-1091; Revision: 6; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Keying material is changed when compromised or suspected of being compromised.

Further information

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

Further information on the evaluation of cryptographic modules, including testing requirements, is available as part of the Cryptographic Module Validation Program which is jointly operated by NIST and the Canadian Centre for Cyber Security.

Further information on the protection of ICT equipment and media can be found in the Attorney-General's Department's *Protective Security Policy Framework*, *Physical security for entity resources* policy.

ASD-Approved Cryptographic Algorithms

High assurance cryptographic algorithms

High assurance cryptographic algorithms, which are not covered in this section, can be used for the protection of SECRET and TOP SECRET data if they are suitably implemented in HACE. Further information on high assurance cryptographic algorithms can be obtained from the ACSC.

ASD-Approved Cryptographic Algorithms

There is no guarantee of an algorithm's resistance to currently unknown attacks. However, the algorithms listed in this section have been extensively scrutinised by industry and academic communities in a practical and theoretical setting. Approval for the use of the algorithms listed in this section is limited to cases where they are implemented in accordance with these guidelines.

The approved asymmetric/public key algorithms are:

- Diffie-Hellman (DH) for agreeing on encryption session keys
- Digital Signature Algorithm (DSA) for digital signatures
- Elliptic Curve Diffie-Hellman (ECDH) for key exchange
- Elliptic Curve Digital Signature Algorithm (ECDSA) for digital signatures
- Rivest-Shamir-Adleman (RSA) for digital signatures and passing encryption session keys or similar keys.

The only approved hashing algorithm is Secure Hashing Algorithm 2 (SHA-2).

The only approved symmetric encryption algorithm is Advanced Encryption Standard (AES).

Where there is a range of key sizes for an algorithm, some of the smaller key sizes are not approved as they do not provide an adequate safety margin against possible future attacks. For example, advances in integer factorisation methods could render smaller RSA moduli vulnerable.

The targets used for the effective security strength of algorithms listed within this section are 112 bits for PROTECTED and below data, 128 bits for SECRET data and 192 bits for TOP SECRET data. However, some key sizes and curves are preferred in order to ensure interoperability with the United States' Commercial National Security Algorithm Suite.

Using ASD-Approved Cryptographic Algorithms

If cryptographic equipment or software implements unapproved algorithms, it is possible that these algorithms could be used without a user's knowledge. In combination with an assumed level of security confidence, this can represent a security risk. As such, an organisation can ensure that only AACAs or high assurance cryptographic algorithms can be used by disabling all unapproved algorithms (preferred) or by advising users not to use the unapproved algorithms via usage policies.

Security Control: ISM-0471; Revision: 7; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Only AACAs or high assurance cryptographic algorithms are used by cryptographic equipment and software.

Asymmetric/public key algorithms

DH and DSA are vulnerable to different types of attacks than ECDH and ECDSA. As a result, ECDH and ECDSA offer more effective security per bit increase. This leads to smaller data requirements which in turn means that elliptic curve variants have become de facto global standards. For reduced data cost, and to promote interoperability, ECDH and ECDSA should be used where possible.

Security Control: ISM-0994; Revision: 6; Updated: Dec-21; Applicability: All; Essential Eight: N/A
ECDH and ECDSA are used in preference to DH and DSA.

Using Diffie-Hellman

A modulus of 2048 bits for correctly implemented DH provides 112 bits of effective security strength. Taking into account projected technological advances, it is assessed that 112 bits of effective security strength will remain secure until 2030.

When DH in a prime field is used, the prime modulus impacts the security of the algorithm. The security considerations when creating such a prime modulus can be found in NIST SP 800-56A Rev. 3, along with a collection of commonly used secure moduli.

Security Control: ISM-0472; Revision: 6; Updated: Mar-22; Applicability: O, P; Essential Eight: N/A
When using DH for agreeing on encryption session keys, a modulus of at least 2048 bits is used, preferably 3072 bits.

Security Control: ISM-1759; Revision: 0; Updated: Mar-22; Applicability: S, TS; Essential Eight: N/A
When using DH for agreeing on encryption session keys, a modulus of at least 3072 bits is used, preferably 3072 bits.

Security Control: ISM-1629; Revision: 1; Updated: Dec-21; Applicability: All; Essential Eight: N/A
When using DH for agreeing on encryption session keys, a modulus and associated parameters are selected according to NIST SP 800-56A Rev. 3.

Using the Digital Signature Algorithm

A modulus of 2048 bits for correctly implemented DSA provides 112 bits of effective security strength. Taking into account projected technological advances, it is assessed that 112 bits of effective security strength will remain secure until 2030.

Security Control: ISM-0473; Revision: 5; Updated: Dec-20; Applicability: O, P; Essential Eight: N/A
When using DSA for digital signatures, a modulus of at least 2048 bits is used.

Security Control: ISM-1630; Revision: 2; Updated: Mar-22; Applicability: O, P; Essential Eight: N/A
When using DSA for digital signatures, a modulus and associated parameters are generated according to FIPS 186-4.

Security Control: ISM-1760; Revision: 0; Updated: Mar-22; Applicability: S, TS; Essential Eight: N/A
DSA is not used for digital signatures.

Using Elliptic Curve Cryptography

The curve used within an elliptic curve algorithm impacts the security of the algorithm. As such, only suitable curves from FIPS 186-4 should be used.

Security Control: ISM-1446; Revision: 2; Updated: Dec-21; Applicability: All; Essential Eight: N/A
When using elliptic curve cryptography, a curve from FIPS 186-4 is used.

Using Elliptic Curve Diffie-Hellman

When using a curve from FIPS 186-4, a base point order and key size of at least 224 bits for correctly implemented ECDH provides 112 bits of effective security strength. Security of a curve selected from another source cannot be assumed to have the same security using base point order and key size alone.

Security Control: ISM-0474; Revision: 6; Updated: Mar-22; Applicability: O, P; Essential Eight: N/A
When using ECDH for agreeing on encryption session keys, a base point order and key size of at least 224 bits is used, preferably the NIST P-384 curve.

Security Control: ISM-1761; Revision: 0; Updated: Mar-22; Applicability: S; Essential Eight: N/A
When using ECDH for agreeing on encryption session keys, NIST P-256, P-384 or P-521 curves are used, preferably the NIST P-384 curve.

Security Control: ISM-1762; Revision: 0; Updated: Mar-22; Applicability: TS; Essential Eight: N/A
When using ECDH for agreeing on encryption session keys, NIST P-384 or P-521 curves are used, preferably the NIST P-384 curve.

Using the Elliptic Curve Digital Signature Algorithm

When using a curve from FIPS 186-4, a base point order and key size of 224 bits for correctly implemented ECDSA provides 112 bits of effective security strength. Security of a curve selected from another source cannot be assumed to have the same security using base point order and key size alone.

Security Control: ISM-0475; Revision: 6; Updated: Mar-22; Applicability: O, P; Essential Eight: N/A
When using ECDSA for digital signatures, a base point order and key size of at least 224 bits is used, preferably the P-384 curve.

Security Control: ISM-1763; Revision: 0; Updated: Mar-22; Applicability: S; Essential Eight: N/A
When using ECDSA for digital signatures, NIST P-256, P-384 or P-521 curves are used, preferably the NIST P-384 curve.

Security Control: ISM-1764; Revision: 0; Updated: Mar-22; Applicability: TS; Essential Eight: N/A
When using ECDSA for digital signatures, NIST P-384 or P-521 curves are used, preferably the NIST P-384 curve.

Using Rivest-Shamir-Adleman

A modulus of 2048 bits for correctly implemented RSA provides 112 bits of effective security strength. Taking into account projected technological advances, it is assessed that 112 bits of effective security strength will remain secure until 2030.

Security Control: ISM-0476; Revision: 7; Updated: Mar-22; Applicability: O, P; Essential Eight: N/A
When using RSA for digital signatures, and passing encryption session keys or similar keys, a modulus of at least 2048 bits is used, preferably 3072 bits.

Security Control: ISM-1765; Revision: 0; Updated: Mar-22; Applicability: S, TS; Essential Eight: N/A
When using RSA for digital signatures, and passing encryption session keys or similar keys, a modulus of at least 3072 bits is used, preferably 3072 bits.

Security Control: ISM-0477; Revision: 8; Updated: Mar-22; Applicability: All; Essential Eight: N/A
When using RSA for digital signatures, and for passing encryption session keys or similar keys, a different key pair is used for digital signatures and passing encrypted session keys.

Using hashing algorithms

For most purposes, a hashing algorithm with an output size of 224 bits provides 112 bits of effective security strength. Similarly, a hashing algorithm with an output size of 256 bits provides 128 bits of effective security strength, and an output size of 384 bits provides 192 bits of effective security strength. Only hashing algorithms from the SHA-2 family are approved for use.

Security Control: ISM-1766; Revision: 0; Updated: Mar-22; Applicability: O, P; Essential Eight: N/A
When using SHA-2 for hashing, an output size of at least 224 bits is used, preferably SHA-384.

Security Control: ISM-1767; Revision: 0; Updated: Mar-22; Applicability: S; Essential Eight: N/A
When using SHA-2 for hashing, an output size of at least 256 bits is used, preferably SHA-384.

Security Control: ISM-1768; Revision: 0; Updated: Mar-22; Applicability: TS; Essential Eight: N/A
When using SHA-2 for hashing, an output size of at least 384 bits is used, preferably SHA-384.

Using symmetric encryption algorithms

The use of Electronic Codebook Mode with block ciphers allows repeated patterns in plaintext to appear as repeated patterns in ciphertext. Most plaintext, including written language and formatted files, contains significant repeated patterns. As such, an adversary can use this to deduce possible meanings of ciphertext. The use of other modes, such as Cipher Block Chaining, Cipher Feedback, Galois/Counter Mode or Output Feedback, can prevent such attacks, although each has different properties which can make them inappropriate for certain use cases. AES is the only approved symmetric encryption algorithm.

Security Control: ISM-1769; Revision: 0; Updated: Mar-22; Applicability: O, P, S; Essential Eight: N/A
When using AES for encryption, AES-128, AES-192 or AES-256 is used, preferably AES-256.

Security Control: ISM-1770; Revision: 0; Updated: Mar-22; Applicability: TS; Essential Eight: N/A
When using AES for encryption, AES-192 or AES-256 is used, preferably AES-256.

Security Control: ISM-0479; Revision: 5; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Symmetric cryptographic algorithms are not used in Electronic Codebook Mode.

Further information

Further information on the United States' Commercial National Security Algorithm Suite is available from the United States' National Security Agency.

ASD-Approved Cryptographic Protocols

High assurance cryptographic protocols

High assurance cryptographic protocols, which are not covered in this section, can be used for the protection of SECRET and TOP SECRET data if they are suitably implemented in HACE. Further information on high assurance cryptographic protocols can be obtained from the ACSC.

ASD-Approved Cryptographic Protocols

There is no guarantee of a protocol's resistance to currently unknown attacks. However, the protocols listed in this section have been extensively scrutinised by industry and academic communities in a practical and theoretical setting. Approval for the use of the protocols listed in this section is limited to cases where they are implemented in accordance with these guidelines.

The AACPs are:

- Transport Layer Security (TLS)
- Secure Shell (SSH)
- Secure/Multipurpose Internet Mail Extension (S/MIME)
- OpenPGP Message Format
- Internet Protocol Security (IPsec)
- Wi-Fi Protected Access 2
- Wi-Fi Protected Access 3.

Using ASD-Approved Cryptographic Protocols

If cryptographic equipment or software implements unapproved protocols, it is possible that these protocols could be used without a user's knowledge. In combination with an assumed level of security confidence, this can represent a security risk. As such, an organisation can ensure that only AACPs or high assurance cryptographic protocols can be used by disabling unapproved protocols (preferred) or by advising users not to use unapproved protocols via usage policies.

Security Control: ISM-0481; Revision: 6; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Only AACPs or high assurance cryptographic protocols are used by cryptographic equipment and software.

Further information

Further information on AACPs can be found in the following sections of these guidelines.

Further information on the use of Wi-Fi Protected Access 2 and Wi-Fi Protected Access 3 can be found in the wireless networks section of the *Guidelines for Networking*.

Transport Layer Security

Using Transport Layer Security

When using ICT equipment or software that implements TLS, security controls for using AACAs and AACPs in the ASD-Approved Cryptographic Algorithms and ASD-Approved Cryptographic Protocols sections of these guidelines will also need to be consulted.

Configuring Transport Layer Security

The terms Secure Sockets Layer and TLS have traditionally been used interchangeably. However, Secure Sockets Layer and earlier versions of TLS are no longer considered suitable for use as an AACP. As such, an organisation implementing TLS should implement TLS version 1.3. In addition, a number of security risks exist when TLS is configured in an insecure manner. To mitigate these security risks, TLS should be configured as per the configuration settings below.

Security Control: ISM-1139; Revision: 6; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Only the latest version of TLS is used for TLS connections.

Security Control: ISM-1369; Revision: 3; Updated: Mar-22; Applicability: All; Essential Eight: N/A
AES-GCM is used for encryption of TLS connections.

Security Control: ISM-1370; Revision: 3; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Only server-initiated secure renegotiation is used for TLS connections.

Security Control: ISM-1372; Revision: 3; Updated: Mar-22; Applicability: All; Essential Eight: N/A
DH or ECDH is used for key establishment of TLS connections.

Security Control: ISM-1448; Revision: 2; Updated: Mar-22; Applicability: All; Essential Eight: N/A
When using DH or ECDH for key establishment of TLS connections, the ephemeral variant is used.

Security Control: ISM-1373; Revision: 2; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Anonymous DH is not used for TLS connections.

Security Control: ISM-1374; Revision: 3; Updated: Mar-22; Applicability: All; Essential Eight: N/A
SHA-2-based certificates are used for TLS connections.

Security Control: ISM-1375; Revision: 4; Updated: Mar-22; Applicability: All; Essential Eight: N/A
SHA-2 is used for the Hash-based Message Authentication Code (HMAC) and pseudorandom function (PRF) for TLS connections.

Security Control: ISM-1553; Revision: 1; Updated: Mar-22; Applicability: All; Essential Eight: N/A
TLS compression is disabled for TLS connections.

Security Control: ISM-1453; Revision: 1; Updated: Sep-18; Applicability: All; Essential Eight: N/A
Perfect Forward Secrecy (PFS) is used for TLS connections.

Further information

Further information on implementing TLS can be found in in the ACSC’s *Implementing Certificates, TLS, HTTPS and Opportunistic TLS* publication.

Further information on TLS filtering in gateways can be found in the web content filters section of the *Guidelines for Gateways*.

Secure Shell

Using Secure Shell

When using ICT equipment or software that implements SSH, security controls for using AACAs and AACPs in the ASD-Approved Cryptographic Algorithms and ASD-Approved Cryptographic Protocols sections of these guidelines will also need to be consulted.

Configuring Secure Shell

SSH version 1 was found to have a number of security vulnerabilities, and was subsequently replaced by SSH version 2. As such, an organisation implementing SSH should disable the use of SSH version 1. In addition, a number of security risks exist when SSH is configured in an insecure manner. To mitigate these security risks, SSH should be configured as per the configuration settings below.

The configuration settings below are based on OpenSSH. An organisation using other implementations of SSH should adapt these settings to suit their SSH implementation.

Security Control: ISM-1506; Revision: 1; Updated: Mar-22; Applicability: All; Essential Eight: N/A
The use of SSH version 1 is disabled for SSH connections.

Security Control: ISM-0484; Revision: 6; Updated: Dec-21; Applicability: All; Essential Eight: N/A
The SSH daemon is configured to:

- *only listen on the required interfaces (ListenAddress xxx.xxx.xxx.xxx)*
- *have a suitable login banner (Banner x)*
- *have a login authentication timeout of no more than 60 seconds (LoginGraceTime 60)*
- *disable host-based authentication (HostbasedAuthentication no)*
- *disable rhosts-based authentication (IgnoreRhosts yes)*
- *disable the ability to login directly as root (PermitRootLogin no)*
- *disable empty passwords (PermitEmptyPasswords no)*
- *disable connection forwarding (AllowTCPForwarding no)*
- *disable gateway ports (GatewayPorts no)*
- *disable X11 forwarding (X11Forwarding no).*

Authentication mechanisms

As public key-based authentication schemes offer stronger authentication than passphrase-based authentication schemes, due to being much less susceptible to brute-force attacks, they should be used for SSH connections. Furthermore, in order to protect SSH private keys, access to such keys should be protected via the use of passphrases or key encryption keys.

Security Control: ISM-0485; Revision: 3; Updated: Sep-18; Applicability: All; Essential Eight: N/A
Public key-based authentication is used for SSH connections.

Security Control: ISM-1449; Revision: 1; Updated: Sep-18; Applicability: All; Essential Eight: N/A
SSH private keys are protected with a passphrase or a key encryption key.

Automated remote access

If using logins without a passphrase for automated purposes, a number of security risks may arise, specifically:

- if access from unknown Internet Protocol (IP) addresses is not restricted, an adversary could automatically authenticate to systems without needing to know any passphrases
- if port forwarding is not disabled, or it is not configured securely, access may be gained to forwarded ports, thereby, creating a communication channel between an adversary and a host
- if agent credential forwarding is enabled, an adversary could connect to the stored authentication credentials and use them to connect to other trusted hosts, or even intranet hosts if port forwarding has been allowed as well
- if X11 display remoting is not disabled, an adversary could gain control of displays as well as keyboard and mouse control functions
- if console access is allowed, every user who logs into the console could run programs that are normally restricted to authenticated users.

To assist in mitigating these security risks, it is essential that the 'forced command' option is used to specify what command is executed and parameter checking is enabled.

Security Control: ISM-0487; Revision: 4; Updated: Mar-22; Applicability: All; Essential Eight: N/A
When using logins without a passphrase for SSH connections, the following are disabled:

- *access from IP addresses that do not require access*
- *port forwarding*
- *agent credential forwarding*
- *X11 display remoting*
- *console access.*

Security Control: ISM-0488; Revision: 4; Updated: Mar-22; Applicability: All; Essential Eight: N/A
If using remote access without the use of a passphrase for SSH connections, the 'forced command' option is used to specify what command is executed and parameter checking is enabled.

SSH-agent

SSH-agent and similar key caching programs manage private keys stored on workstations and servers. Specifically, when an SSH-agent launches, it requests a user's passphrase to unlock the user's private key. Subsequent access to remote systems is then performed by the SSH-agent and does not require the user to re-enter their passphrase. Screen locks and expiring key caches can be used to ensure that a user's private key is not left unlocked for a long period of time.

Security Control: ISM-0489; Revision: 5; Updated: Mar-22; Applicability: All; Essential Eight: N/A
When SSH-agent or similar key caching programs are used, it is limited to workstations and servers with screen locks and key caches that are set to expire within four hours of inactivity.

Further information

Further information on configuring OpenSSH is available from the OpenSSH project.

Secure/Multipurpose Internet Mail Extension

Using Secure/Multipurpose Internet Mail Extension

When using ICT equipment or software that implements S/MIME, security controls for using AACAs and AACPs in the ASD-Approved Cryptographic Algorithms and ASD-Approved Cryptographic Protocols sections of these guidelines will also need to be consulted.

Configuring Secure/Multipurpose Internet Mail Extension

S/MIME version 2.0 required the use of weaker cryptography than approved for use in these guidelines. As such, S/MIME version 3.0 was the first version to be approved for use as an AACP.

Security Control: ISM-0490; Revision: 4; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Versions of S/MIME earlier than S/MIME version 3.0 are not used for S/MIME connections.

Internet Protocol Security

Using Internet Protocol Security

When using ICT equipment or software that implements IPsec, security controls for using AACAs and AACPs in the ASD-Approved Cryptographic Algorithms and ASD-Approved Cryptographic Protocols sections of these guidelines will also need to be consulted.

Mode of operation

IPsec can be operated in tunnel mode or transport mode. The tunnel mode of operation is preferred as it provides full encapsulation of IP packets while the transport mode of operation only encapsulates the payload of IP packets.

Security Control: ISM-0494; Revision: 3; Updated: Sep-18; Applicability: All; Essential Eight: N/A
Tunnel mode is used for IPsec connections; however, if using transport mode, an IP tunnel is used.

Protocol selection

IPsec contains two major protocols, the Authentication Header (AH) protocol and the Encapsulating Security Payload (ESP) protocol. In order to provide a secure Virtual Private Network style connection, both authentication and encryption are needed. While the AH and ESP protocols can both provide authentication, for the IP packet and the payload respectively, only the ESP protocol can provide encryption.

As the combined use of the AH protocol and the ESP protocol is not supported by Internet Key Exchange (IKE) version 2, the ESP protocol should be used for authentication and encryption of IPsec connections.

Security Control: ISM-0496; Revision: 5; Updated: Mar-22; Applicability: All; Essential Eight: N/A
The ESP protocol is used for authentication and encryption of IPsec connections.

Key exchange

There are several methods for establishing shared keying material for IPsec connections, including manual keying and the IKE protocol. As the IKE protocol addresses a number of security risks associated with manual keying, it is the preferred method for key establishment. Note, as IKE version 1 has been deprecated, IKE version 2 should be used.

Security Control: ISM-1233; Revision: 2; Updated: Mar-22; Applicability: All; Essential Eight: N/A
IKE version 2 is used for key exchange when establishing IPsec connections.

Encryption algorithms

The only approved encryption algorithm for IPsec connections is AES. IKE version 2 supports the use of AES with Cipher Block Chaining, Counter Mode, Counter with Cipher Block Chaining Message Authentication Code, and Galois/Counter Mode. Note, however, supported modes may vary between different cryptographic equipment and software.

Security Control: ISM-1771; Revision: 0; Updated: Mar-22; Applicability: All; Essential Eight: N/A
AES is used for encrypting IPsec connections, preferably ENCR_AES_GCM_16.

Pseudorandom function algorithms

IKE version 2 requires the use of a PRF in order to generate random data for cryptographic operations. The approved algorithms that can be used for PRF are HMAC-SHA256, HMAC-SHA384 and HMAC-SHA512.

Security Control: ISM-1772; Revision: 0; Updated: Mar-22; Applicability: All; Essential Eight: N/A
PRF_HMAC_SHA2_256, PRF_HMAC_SHA2_384 or PRF_HMAC_SHA2_512 is used for IPsec connections, preferably PRF_HMAC_SHA2_512.

Integrity algorithms

The approved integrity algorithms for IPsec connections are HMAC-SHA256, HMAC-SHA384 and HMAC-SHA512. However, if using AES with Galois/Counter Mode as the encryption algorithm, it can also be used for authentication purposes. In such cases, the integrity algorithm should be configured as NONE.

Security Control: ISM-0998; Revision: 5; Updated: Mar-22; Applicability: All; Essential Eight: N/A
AUTH_HMAC_SHA2_256_128, AUTH_HMAC_SHA2_384_192, AUTH_HMAC_SHA2_512_256 or NONE (only with AES-GCM) is used for authenticating IPsec connections, preferably NONE.

Diffie-Hellman groups

A sufficiently large DH modulus provides greater security for key exchanges when establishing IPsec connections.

Security Control: ISM-0999; Revision: 6; Updated: Mar-22; Applicability: All; Essential Eight: N/A
DH or ECDH is used for key establishment of IPsec connections, preferably 384-bit random ECP group, 3072-bit MODP Group or 4096-bit MODP Group.

Security association lifetimes

Using a security association lifetime of less than four hours (14400 seconds) can provide a balance between security and usability.

Security Control: ISM-0498; Revision: 4; Updated: Mar-22; Applicability: All; Essential Eight: N/A
A security association lifetime of less than four hours (14400 seconds) is used for IPsec connections.

Perfect Forward Secrecy

Using PFS reduces the impact of the compromise of a security association.

Security Control: ISM-1000; Revision: 4; Updated: Sep-18; Applicability: All; Essential Eight: N/A
PFS is used for IPsec connections.

Guidelines for Gateways

Gateways

Introduction to gateways

This section describes security controls applicable to all types of gateways. In applying these security controls, gateways take on the highest sensitivity or classification of connected security domains.

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.

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.

Security Control: ISM-0628; Revision: 6; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Gateways are implemented between networks belonging to different security domains.

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

Security Control: ISM-0631; Revision: 7; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Gateways only allow explicitly authorised data flows.

Security Control: ISM-1192; Revision: 3; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Gateways inspect and filter data flows at the transport and above network layers.

Security Control: ISM-1427; Revision: 3; Updated: Mar-22; Applicability: All; 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 and PROTECTED networks will need to hold baseline security clearances.

In addition, when creating privileged 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.

Security Control: ISM-1520; Revision: 2; Updated: Mar-22; Applicability: All; 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.

Security 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.

Security 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.

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

Security Control: ISM-0616; Revision: 5; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Separation of duties is implemented in performing administrative activities for gateways.

Security Control: ISM-0612; Revision: 5; Updated: Mar-22; Applicability: All; 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 connected networks be compromised by an adversary. 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 third party.

Security Control: ISM-1774; Revision: 0; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Gateways are managed via a secure path isolated from all connected networks.

Security Control: ISM-0629; Revision: 4; Updated: Mar-22; Applicability: All; 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 third party.

Authenticating to networks accessed via gateways

Ensuring users and ICT equipment are authenticated to other networks accessed via gateways can reduce the likelihood of unauthorised access.

Security Control: ISM-0619; Revision: 6; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Users authenticate to other networks accessed via gateways.

Security Control: ISM-0622; Revision: 6; Updated: Mar-22; Applicability: All; Essential Eight: N/A
ICT equipment authenticates to other networks accessed via gateways.

Gateway event logging and alerting

Gateway event logs can assist in monitoring the security posture of networks, detecting malicious behaviour and contributing to investigations following cyber security incidents. In doing so, gateway event logs should be centrally stored and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.

Security Control: ISM-0634; Revision: 8; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Gateways are configured to:

- *log network traffic permitted through gateways*
- *log network traffic attempting to leave gateways*
- *provide real-time alerts for attempted intrusions and unusual usage patterns.*

Security Control: ISM-1775; Revision: 0; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Gateway event logs are centrally stored and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.

Gateway testing

Testing security controls for gateways assists with understanding their security posture. In doing so, testing should be conducted at irregular intervals to reduce the likelihood that an adversary could exploit testing activities or cease operations during such times to avoid detection.

Security Control: ISM-1037; Revision: 5; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Gateways are subject to rigorous testing following configuration changes, and at irregular intervals no more than six months apart, to determine the effectiveness of security controls.

Further information

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 ICT equipment 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*.

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 security 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 the Australian Cyber Security Centre (ACSC)'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.

Security 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 the ACSC is consulted and any directions provided by the ACSC are complied with.

Security Control: ISM-0597; Revision: 7; Updated: Mar-22; Applicability: S, TS; Essential Eight: N/A
When planning, designing, implementing or introducing additional connectivity to CDSs, the ACSC is consulted and any directions provided by the ACSC 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.

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

Security 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.

Security 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 and unauthorised activities will be detected. In doing so, CDS event logs should be centrally stored and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.

Security Control: ISM-0670; Revision: 5; Updated: Mar-22; Applicability: S, TS; Essential Eight: N/A
All security-relevant events generated by CDSs are logged.

Security Control: ISM-1776; Revision: 0; Updated: Mar-22; Applicability: All; Essential Eight: N/A
CDS event logs are centrally stored and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.

Security 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 3 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.

Security 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 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.

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

Security Control: ISM-0639; Revision: 9; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Evaluated firewalls are used between networks belonging to different security domains.

Further information

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

Diodes

Using diodes

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

Security Control: ISM-0643; Revision: 7; Updated: Mar-22; Applicability: All; 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.

Security 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.

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

Security 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.

Data volume monitoring

Monitoring the volume of data transferred across diodes can assist in ensuring that they conform to expectations. Such activities can also alert an organisation to potentially malicious activity if the volume of data being transferred suddenly changes.

Security Control: ISM-0648; Revision: 4; Updated: Mar-22; Applicability: All; Essential Eight: N/A
The volume of data transferred across diodes is monitored.

Further information

Further information on evaluated products can be found in the evaluated product acquisition 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 a web usage policy governing its use.

Security Control: ISM-0258; Revision: 3; Updated: Aug-19; Applicability: All; Essential Eight: N/A
A web usage policy is developed and implemented.

Using web proxies

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

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

Web proxy event logging

Web proxy event logs can assist in monitoring the security posture of networks, detecting malicious behaviour and contributing to investigations following cyber security incidents. In doing so, web proxy event logs should be centrally stored and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.

Security Control: ISM-0261; Revision: 5; Updated: Mar-22; Applicability: All; Essential Eight: N/A
The following details are logged for websites accessed via web proxies:

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

Security Control: ISM-1777; Revision: 0; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Web proxy event logs are centrally stored and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.

Further information

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 an adversary from communicating with their malicious code if they manage to deploy it on an organisation's networks.

Security Control: ISM-0963; Revision: 6; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Web content filters are used to filter potentially harmful web-based content.

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

Security Control: ISM-1237; Revision: 2; Updated: Mar-22; Applicability: All; 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.

Security Control: ISM-0263; Revision: 8; Updated: Mar-22; Applicability: All; 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 an adversary. In doing so, even a relatively permissive list of allowed domain names, such as the entire Australian subdomain (‘*.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 an adversary 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 an adversary’s command and control infrastructure and should be blocked.

Security Control: ISM-0958; Revision: 8; Updated: Mar-22; Applicability: All; 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.

Security Control: ISM-1236; Revision: 2; Updated: Mar-22; Applicability: All; 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.

Security Control: ISM-1171; Revision: 2; Updated: Mar-22; Applicability: All; 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 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.

Security Control: ISM-0659; Revision: 6; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Files imported or exported via gateways or CDSs undergo content filtering checks.

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

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

Security 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.

Security Control: ISM-1293; Revision: 2; Updated: Mar-22; Applicability: All; 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.

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

Security Control: ISM-1290; Revision: 2; Updated: Mar-22; Applicability: All; 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.

Security Control: ISM-1288; Revision: 2; Updated: Mar-22; Applicability: All; 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 communications, creation or modification of files, or system configuration changes.

Security Control: ISM-1389; Revision: 2; Updated: Mar-22; Applicability: All; 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 documents and Portable Document Format (PDF) files.

Security Control: ISM-0649; Revision: 8; Updated: Mar-22; Applicability: All; 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 security vulnerabilities in operating systems or applications.

Security Control: ISM-1284; Revision: 3; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Files imported or exported via gateways or CDSs undergo content validation.

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.

Security Control: ISM-1286; Revision: 2; Updated: Mar-22; Applicability: All; 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 documents or removing JavaScript sections from PDF files.

Security Control: ISM-1287; Revision: 2; Updated: Mar-22; Applicability: All; 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 checksum, content filters should verify their integrity. In doing so, the failure of any integrity checks may indicate that files have been tampered with.

Security Control: ISM-0677; Revision: 6; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Files imported or exported via gateways or CDSs that have a digital signature or checksum are validated.

Further information

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.

Security Control: ISM-0591; Revision: 8; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Evaluated peripheral switches are used when sharing peripherals between systems.

Security 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.

Security 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 evaluated products can be found in the evaluated product acquisition section of the *Guidelines for Evaluated Products*.

Guidelines for Data Transfers

Data transfers

Performing data transfers

This section describes security controls applicable to both 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 and implemented 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 and implemented 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.

Security Control: ISM-0663; Revision: 6; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Data transfer processes, and supporting data transfer procedures, are developed and implemented.

Security Control: ISM-1535; Revision: 4; Updated: Mar-22; Applicability: S, TS; Essential Eight: N/A
Processes, and supporting procedures, are developed and implemented to prevent AUSTEO, AGAO and REL data in both 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.

Security 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 addition, data manually imported to SECRET and TOP SECRET systems will require additional assurances that it does not contain malicious code, for example, by undergoing data formatting checks. Finally, in cases where security checks fail, data should be quarantined until it can be reviewed and subsequently approved or not approved for release.

Security 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.

Security Control: ISM-0658; Revision: 6; Updated: Mar-22; Applicability: S, TS; Essential Eight: N/A
When manually importing data to SECRET and TOP SECRET systems, the data undergoes data formatting checks.

Security 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 an organisation's 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.

Security 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.

Security 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.

Security Control: ISM-0665; Revision: 6; Updated: Dec-21; 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 an organisation's 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 undergoing data formatting checks, data type and sizes checks, signature checks, and keyword checks 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.

Security 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.

Security Control: ISM-0669; Revision: 5; Updated: Mar-22; Applicability: S, TS; Essential Eight: N/A
When manually exporting data from SECRET and TOP SECRET systems, the data undergoes data formatting checks, data type and size checks, signature checks, and keyword checks within all textual data.

Security 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 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 an adversary to surreptitiously import malicious code or exfiltrate data from SECRET and TOP SECRET systems.

Security 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.

Security 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.

Security 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*.

Cyber Security Terminology

Glossary of abbreviations

Abbreviation	Meaning
AACA	ASD-Approved Cryptographic Algorithm
AACP	ASD-Approved Cryptographic Protocol
ACSC	Australian Cyber Security Centre
AES	Advanced Encryption Standard
AGAO	Australian Government Access Only
AGD	Attorney-General's Department
AH	Authentication Header
AISEP	Australian Information Security Evaluation Program
ASD	Australian Signals Directorate
ASIO	Australian Security Intelligence Organisation
ATA	Advanced Technology Attachment
AUSTEO	Australian Eyes Only
CCRA	Common Criteria Recognition Arrangement
CDN	content delivery network
CDS	Cross Domain Solution
CISO	Chief Information Security Officer
DBMS	database management system
DH	Diffie-Hellman
DKIM	DomainKeys Identified Mail

DMA	Direct Memory Access
DMARC	Domain-based Message Authentication, Reporting and Conformance
DSA	Digital Signature Algorithm
EAL	Evaluation Assurance Level
EAP	Extensible Authentication Protocol
EAP-TLS	Extensible Authentication Protocol-Transport Layer Security
ECDSA	Elliptic Curve Digital Signature Algorithm
ECDH	Elliptic Curve Diffie-Hellman
EEPROM	electrically erasable programmable read-only memory
EPROM	erasable programmable read-only memory
ESP	Encapsulating Security Payload
FIPS	Federal Information Processing Standard
FT	Fast Basic Service Set Transition
HACE	High Assurance Cryptographic Equipment
HIPS	Host-based Intrusion Prevention System
HMAC	Hashed Message Authentication Code
HSTS	Hypertext Transfer Protocol Strict Transport Security
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICT	Information and Communications Technology
IEC	International Electrotechnical Commission

IKE	Internet Key Exchange
IP	Internet Protocol
IPsec	Internet Protocol Security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IR	infrared
IRAP	Infosec Registered Assessors Program
ISM	Information Security Manual
ISO	International Organization for Standardization
LAN	Local Area Network
MAC	Media Access Control
MFD	multifunction device
MTA-STS	Mail Transfer Agent Strict Transport Security
NAA	National Archives of Australia
NIDS	Network-based Intrusion Detection System
NIPS	Network-based Intrusion Prevention System
NIST	National Institute of Standards and Technology
OWASP	Open Web Application Security Project
PDF	Portable Document Format
PFS	Perfect Forward Secrecy
PMK	Pairwise Master Key
PP	Protection Profile
PRF	pseudorandom function

PSC	Protective Security Circular
PSPF	Protective Security Policy Framework
PSTN	Public Switched Telephone Network
RADIUS	Remote Access Dial-In User Service
REL	Releasable To
RF	Radio Frequency
RSA	Rivest-Sharmir-Adleman
SCEC	Security Construction and Equipment Committee
SEG	Security Equipment Guide
SHA-2	Secure Hashing Algorithm 2
S/MIME	Secure/Multipurpose Internet Mail Extension
SNMP	Simple Network Management Protocol
SOE	Standard Operating Environment
SQL	Structured Query Language
SP	Special Publication
SPF	Sender Policy Framework
SSH	Secure Shell
SSID	Service Set Identifier
SSL	Secure Sockets Layer
TLS	Transport Layer Security
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
VPN	Virtual Private Network

WPA2	Wi-Fi Protected Access 2
WPA3	Wi-Fi Protected Access 3

Glossary of cyber security terms

Term	Meaning
access control	The process of granting or denying requests for access to systems, applications and data. Can also refer to the process of granting or denying requests for access to facilities.
Access Cross Domain Solution	A system permitting access to multiple security domains from a single client device.
accountable material	Accountable material requires the strictest control over its access and movement. Accountable material includes TOP SECRET data, some types of caveated data and any data designated as accountable material by its originator.
aggregation (of data)	A term used to describe compilations of data that may require a higher level of protection than their component parts.
application control	An approach in which only an explicitly defined set of trusted applications are allowed to execute on systems.
asset	Anything of value, such as ICT equipment, software or data.
attack surface	The amount of ICT equipment and software used in a system. The greater the attack surface the greater the chances of an adversary finding an exploitable security vulnerability.
Australian Information Security Evaluation Program	A program under which evaluations are performed by impartial bodies against the Common Criteria. The results of these evaluations are then certified by the Australian Certification Authority within the Australian Cyber Security Centre.
Australian Eyes Only data	Data not to be passed to, or accessed by, foreign nationals.

Australian Government Access Only data	Data not to be passed to, or accessed by, foreign nationals, with the exception of seconded foreign nationals.
authentication	Verifying the identity of a user, process or device as a prerequisite to allowing access to resources in a system.
Authentication Header	A protocol used in Internet Protocol Security (IPsec) that provides data integrity and data origin authenticity but not confidentiality.
authorising officer	An executive with the authority to formally accept the security risks associated with the operation of a system and to authorise it to operate.
availability	The assurance that systems and data are accessible and useable by authorised entities when required.
biometrics	Measurable physical characteristics used to identify or verify an individual.
cascaded connections	Cascaded connections occur when one network is connected to another, which is then connected to another, and so on.
caveat	A marking that indicates that the data has special requirements in addition to those indicated by its classification. This term covers codewords, source codewords, releasability indicators and special-handling caveats.
certification report	An artefact of Common Criteria evaluations that outlines the outcomes of a product’s evaluation.
Chief Information Security Officer	A senior executive who is responsible for coordinating communication between security and business functions as well as overseeing the application of security controls and associated security risk management processes.
classification	The categorisation of systems and data according to the expected impact if it was to be compromised.
classified data	Data that would cause damage, serious damage or exceptionally grave damage to the national interest, an organisation or an individual if compromised (i.e. data assessed as PROTECTED, SECRET or TOP SECRET).

coercivity	A property of magnetic material, used as a measure of the amount of coercive force required to reduce the magnetic induction to zero from its remnant state.
Commercial Grade Cryptographic Equipment	A subset of ICT equipment which contains cryptographic components.
Common Criteria	An international standard for product evaluations.
Common Criteria Recognition Arrangement	An international agreement which facilitates the mutual recognition of Common Criteria evaluations by certificate producing schemes.
communications security	The security controls applied to protect telecommunications from unauthorised interception and exploitation, as well as ensure the authenticity of such telecommunications.
conduit	A tube, duct or pipe used to protect cables.
confidentiality	The assurance that data is disclosed only to authorised entities.
connection forwarding	The use of network address translation to allow a port on a node inside a network to be accessed from outside the network. Alternatively, using a Secure Shell server to forward a Transmission Control Protocol connection to an arbitrary port on the local host.
content filter	A filter that examines content to assess conformance against a security policy.
continuous monitoring plan	A document that describes the plan for the continuous monitoring and assurance in the effectiveness of security controls for a system.
control plane	The administrative interface that allows for the management and orchestration of a system's infrastructure and applications.
critical server	A server that provides critical network or security services. For example, a domain controller or authentication server.
Cross Domain Solution	A system capable of implementing comprehensive data flow security policies with a high level of trust between two or more differing security domains.

cryptographic algorithm	An algorithm used to perform cryptographic functions, such as encryption, integrity, authentication, digital signatures or key establishment.
cryptographic equipment	A generic term for commercial cryptographic equipment and High Assurance Cryptographic Equipment.
cryptographic hash	An algorithm (the hash function) which takes as input a string of any length (the message) and generates a fixed length string (the message digest or fingerprint) as output. The algorithm is designed to make it computationally infeasible to find any input which maps to a given digest, or to find two different messages that map to the same digest.
cryptographic protocol	An agreed standard for secure communication between two or more entities to provide confidentiality, integrity, authentication and non-repudiation of data.
cryptographic software	Software designed to perform cryptographic functions.
cryptographic system	A related set of hardware or software used for cryptographic communication, processing or storage and the administrative framework in which it operates.
cyber resilience	The ability to adapt to disruptions caused by cyber security incidents while maintaining continuous business operations. This includes the ability to detect, manage and recover from cyber security incidents.
cyber security	Measures used to protect the confidentiality, integrity and availability of systems and data.
cyber security event	An occurrence of a system, service or network state indicating a possible breach of security policy, failure of safeguards or a previously unknown situation that may be relevant to security.
cyber security incident	An unwanted or unexpected cyber security event, or a series of such events, that have a significant probability of compromising business operations.
cyber threat	Any circumstance or event with the potential to harm systems or data.
data at rest	Data that resides on media or a system.

data in transit	Data that is being communicated across a communication medium.
data security	Measures used to protect the confidentiality, integrity and availability of data.
data spill	The accidental or deliberate exposure of data into an uncontrolled or unauthorised environment, or to people without a need-to-know.
declassification	A process whereby requirements for the protection of data are removed and an administrative decision is made to formally authorise its release into the public domain.
degausser	An electrical device or permanent magnet assembly which generates a coercive magnetic force for the purpose of degaussing magnetic storage devices.
degaussing	A process for reducing the magnetisation of a magnetic storage device to zero by applying a reverse (coercive) magnetic force, rendering any previously stored data unreadable.
demilitarised zone	A small network with one or more servers that is kept separate from the core network, typically on the outside of the firewall or as a separate network protected by the firewall. Demilitarised zones usually provide data to less trusted networks, such as the internet.
denial-of-service attack	An attempt by an adversary to prevent legitimate access to online services (typically a website), for example, by consuming the amount of available bandwidth or the processing capacity of the server hosting the online service.
device access control software	Software that can be used on a system to restrict access to communications ports. Device access control software can block all access to a communications port or allow access based on device types, manufacturer’s identification or even unique device identifiers.
digital preservation	The coordinated and ongoing set of processes and activities that ensure long-term, error-free storage of digital information, with means for retrieval and interpretation, for the entire time span the information is required.

digital signature	A cryptographic process that allows the proof of the source (with non-repudiation) and the verification of the integrity of that data.
diode	A device that allows data to flow in only one direction.
distributed-denial-of-service attack	A distributed form of denial-of-service attack.
dual-stack network device	ICT equipment that implements both Internet Protocol version 4 and Internet Protocol version 6 protocol stacks.
emanation security	The counter-measures employed to reduce sensitive or classified emanations from a facility and its systems to an acceptable level. Emanations can be in the form of Radio Frequency energy, sound waves or optical signals.
Encapsulating Security Payload	A protocol used for encryption and authentication in IPsec.
Enterprise Mobility Evaluation Program	The investigation, analysis, verification and validation of enterprise mobility solutions used to protect up to PROTECTED data.
escort	A person who ensures that when maintenance or repairs are undertaken to ICT equipment that uncleared personnel are not exposed to data they are not authorised to access.
event	In the context of system logs, an event constitutes an evident change to the normal behaviour of a network, system or user.
facility	A physical space where business is performed. For example, a facility can be a building, a floor of a building or a designated space on the floor of a building.
fax machine	A device that allows copies of documents to be sent over a telephone network.
firewall	A network device that filters incoming and outgoing network data based on a series of rules.
firmware	Software embedded in ICT equipment.
fly lead	A lead that connects ICT equipment to the fixed infrastructure of a facility. For example, the lead that connects a workstation to a network wall socket.

foreign national	A person who is not an Australian citizen.
foreign system	A system that is not managed by, or on behalf of, the Australian Government.
fuzzing	Fuzzing (or fuzz testing) is a method used to discover errors or potential security vulnerabilities in software.
gateway	Gateways securely manage data flows between connected networks from different security domains.
hardware	A generic term for ICT equipment.
Hash-based Message Authentication Code Algorithms	A cryptographic construction that can be used to compute Message Authentication Codes using a hash function and a secret key.
High Assurance Cryptographic Equipment	Cryptographic equipment that has been designed and authorised for the protection of SECRET and TOP SECRET data.
High Assurance Evaluation Program	The rigorous investigation, analysis, verification and validation of products used to protect SECRET and TOP SECRET data.
high assurance ICT equipment	ICT equipment that has been designed and authorised for the protection of SECRET and TOP SECRET data.
high-value server	A server that provide important network services or contains important data repositories. For example, a Domain Name System server, database server, email server, file server or web server.
Host-based Intrusion Detection System	Software, resident on a system, which monitors system activities for malicious or unwanted behaviour.
Host-based Intrusion Prevention System	Software, resident on a system, which monitors system activities for malicious or unwanted behaviour and can react in real-time to block or prevent those activities.
hybrid hard drive	Non-volatile magnetic media that uses a cache to increase read/write speeds and reduce boot times. The cache is normally non-volatile flash memory media.
ICT equipment	Any device that can process, store or communicate data, such as computers, multifunction devices, network

	devices, smartphones, digital cameras, electronic storage media and other radio devices.
incident response plan	A document that describes the plan for responding to cyber security incidents.
Infosec Registered Assessors Program	An initiative of the Australian Cyber Security Centre designed to register suitably qualified individuals to carry out security assessments for systems.
infrared device	Devices such as mice, keyboards and pointing devices that have an infrared communications capability.
integrity	The assurance that data has been created, amended or deleted only by authorised individuals.
interactive authentication	Authentication that involves the interaction of a person with a system.
Internet Protocol Security	A suite of protocols for secure communications through authentication or encryption of Internet Protocol (IP) packets as well as including protocols for cryptographic key establishment.
Internet Protocol telephony	The transport of telephone calls over IP networks.
Internet Protocol version 6	A protocol used for communicating over packet switched networks. Version 6 is the successor to version 4 which is widely used on the internet.
Intrusion Detection System	An automated system used to identify an infringement of security policy. IDS can be host-based or network-based.
jump server	A computer which is used to manage important or critical resources in a separate security domain. Also known as a jump host or jump box.
keying material	Cryptographic keys generated or used by cryptographic equipment or software.
key management	The use and management of cryptographic keys and associated hardware and software. It includes their generation, registration, distribution, installation, usage, protection, storage, access, recovery and destruction.

lockable commercial cabinet	A cabinet that is commercially available, of robust construction and is fitted with a commercial lock.
logging facility	A facility that includes software which generates events and their associated details, the transmission (if necessary) of event logs, and how they are stored.
malicious code	Any software that attempts to subvert the confidentiality, integrity or availability of a system.
malicious code infection	The occurrence of malicious code infecting a system.
media	A generic term for hardware, often portable in nature, which is used to store data.
media destruction	The process of physically damaging media with the intent of making data stored on it inaccessible. To destroy media effectively, only the actual material in which data is stored needs to be destroyed.
media disposal	The process of relinquishing control of media when it is no longer required.
media sanitisation	The process of erasing or overwriting data stored on media so that it cannot be retrieved or reconstructed.
metadata	Descriptive data about the content and context used to identify data.
mobile device	A portable computing or communications device. For example, smartphones, tablets and laptops.
multifunction device	ICT equipment that combines printing, scanning, copying, faxing or voice messaging functionality in the one device. These devices are often designed to connect to computer and telephone networks simultaneously.
need-to-know	The principle of restricting an individual’s access to only the data they require to fulfil the duties of their role.
network access control	Security policies used to control access to a network and actions on a network. This can include authentication checks and authorisation controls.
network device	ICT equipment designed to facilitate the communication of data. For example, routers, switches and wireless access points.

network infrastructure	The infrastructure used to carry data between workstations and servers or other network devices.
network management traffic	Network traffic generated by system administrators over a network in order to control workstations and servers. This includes standard management protocols and other network traffic that contains data relating to the management of the network.
non-interactive authentication	Authentication between systems or services that does not involve the interaction of a person.
non-repudiation	Providing proof that a user performed an action, and in doing so preventing a user from denying that they did so.
non-volatile flash memory media	A specific type of electrically erasable programmable read-only memory.
non-volatile media	A type of media which retains its data when power is removed.
off-hook audio protection	A method of mitigating the possibility of an active handset inadvertently allowing background discussions to be heard by a remote party. This can be achieved through the use of a hold feature, mute feature, push-to-talk handset or equivalent.
online services	Services such as social media, online collaboration tools, web browsing, instant messaging, IP telephony, video conferencing, file sharing websites and peer-to-peer applications.
OpenPGP Message Format	An open-source implementation of Pretty Good Privacy, a widely available cryptographic toolkit.
passphrase	A sequence of words used for authentication.
passphrase complexity	The use of at least three of the following character sets in passphrases: lower-case alphabetical characters (a-z), upper-case alphabetical characters (A-Z), numeric characters (0-9) or special characters.
password	A sequence of characters used for authentication.

patch	A piece of software designed to remedy security vulnerabilities, or improve the usability or performance of software and ICT equipment.
patch cable	A metallic (copper) or fibre-optic cable used for routing signals between two components in an enclosed container or rack.
patch panel	A group of sockets or connectors that allow manual configuration changes, generally by means of connecting patch cables.
penetration test	A penetration test is designed to exercise real-world scenarios in an attempt to achieve a specific goal, such as compromising critical systems or data.
Perfect Forward Secrecy	Additional security for security associations ensuring that if one security association is compromised subsequent security associations will not be compromised.
peripheral switch	A device used to share a set of peripherals between multiple computers. For example, a keyboard, video monitor and mouse.
plan of action and milestones	A document that describes security vulnerabilities in a system and the plans for their rectification.
position of trust	A position that involves duties that require a higher level of assurance than that provided by normal employment screening. In some cases additional screening may be required. Positions of trust can include, but are not limited to, an organisation’s Chief Information Security Officer and their delegates, system administrators or privileged users.
privileged accounts	Privileged accounts include privileged user accounts and privileged service accounts.
privileged operating environments	Privileged operating environments are those used exclusively for administrative activities.
privileged user	A user who can alter or circumvent a system’s security controls. This can also apply to users who could have only limited privileges, such as software developers, who can still bypass security controls. A privileged user can have the capability to modify system configurations,

	account privileges, event logs and security configurations for applications.
product	A generic term used to describe software or hardware.
PROTECTED area	An area that has been authorised to process, store or communicate PROTECTED data. Such areas are not necessarily tied to a specific level of security zone.
Protection Profile	A document that stipulates the security functionality that must be included in Common Criteria evaluation to meet a range of defined threats. Protection Profiles also define the activities to be taken to assess the security function of an evaluated product.
protective marking	An administrative label assigned to data that not only shows the value of the data but also defines the level of protection to be provided.
public data	Data that has been formally authorised for release into the public domain.
public network infrastructure	Network infrastructure that an organisation has no control over, such as the internet.
Public Switched Telephone Network	Public network infrastructure used for voice communications.
push-to-talk handsets	Handsets that have a button which is pressed by the user before audio can be communicated, thus providing off-hook audio protection.
quality of service	The ability to provide different priorities to different applications, users or data flows, or to guarantee a certain level of performance to a data flow.
Radio Frequency transmitter	A device designed to transmit electromagnetic radiation as part of a radio communication system.
reclassification	An administrative decision to change the security controls used to protect data based on a reassessment of the potential impact of its unauthorised disclosure. The lowering of the security controls for media containing sensitive or classified data often requires sanitisation or destruction processes to be undertaken prior to a formal decision to lower the security controls protecting the data.

Releasable To data	Data not to be passed to, or accessed by, foreign nationals beyond those belonging to specific nations which the data has been authorised for release to.
remote access	Access to a system that originates from outside an organisation’s network and enters the network through a gateway, including over the internet.
removable media	Storage media that can be easily removed from a system and is designed for removal, such as Universal Serial Bus flash drives and optical media.
seconded foreign national	A representative of a foreign government on exchange or long-term posting.
SECRET area	An area that has been authorised to process, store or communicate SECRET data. Such areas are not necessarily tied to a specific level of security zone.
secured space	An area certified to the physical security requirements for a Security Zone Two to Security Zone Five area, as defined in the Attorney-General’s Department’s *Protective Security Policy Framework*, *Entity facilities* policy, to allow for the processing or storage of sensitive or classified data.
Secure/Multipurpose Internet Mail Extension	A protocol which allows the encryption and signing of email messages.
Secure Shell	A network protocol that can be used to securely log into, execute commands on, and transfer files between remote workstations and servers.
security assessment	An activity undertaken to assess security controls for a system and its environment to determine if they have been implemented correctly and are operating as intended.
security assessment report	A document that describes that outcomes of a security assessment and contributes to the development of a plan of action and milestones.
security association	A collection of connection-specific parameters used for IPsec connections.
security association lifetime	The duration a security association is valid for.

Security Construction and Equipment Committee	An Australian Government interdepartmental committee responsible for the evaluation and endorsement of security equipment and services. The committee is chaired by the Australian Security Intelligence Organisation.
security documentation	An organisation's cyber security strategy; system-specific security documentation; and any supporting diagrams, plans, policies, processes, procedures and registers.
security domain	A system or collection of systems operating under a consistent security policy that defines the classification, releasability and special handling caveats for data processed within the domain.
security posture	The level of security risk to which a system is exposed. A system with a strong security posture is exposed to a low level of security risk while a system with a weak security posture is exposed to a high level of security risk.
security risk	Any event that could result in the compromise, loss of integrity or unavailability of data or resources, or deliberate harm to people measured in terms of its likelihood and consequences.
security risk appetite	Statements that communicate the expectations of an organisation's senior management about their security risk tolerance. These criteria help an organisation identify security risks, prepare appropriate treatments and provide a benchmark against which the success of mitigations can be measured.
security risk management	The process of identifying, assessing and taking steps to reduce security risks to an acceptable level.
security target	An artefact of Common Criteria evaluations that specifies conformance claims, threats and assumptions, security objectives, and security requirements for an evaluated product.
security vulnerability	A weakness in a system's security requirements, design, implementation or operation that could be accidentally triggered or intentionally exploited and result in a violation of the system's security policy.
sensitive data	Data that would cause limited damage to the national interest, an organisation or an individual if compromised.

server	A computer that provides services to users or other systems. For example, a file server, email server or database server.
shared facility	Where an organisation’s facility resides within a larger facility that is shared with one or more different organisations.
shared responsibility model	A framework that describes the management and operational responsibilities between different parties for a system. Where responsibilities relating to specific security controls are shared between multiple parties, enough detail is documented to provide clear demarcation between the parties.
softphone	An application that allows a workstation to act as a phone using a built-in or externally-connected microphone and speaker.
software	An element of a system including, but not limited to, an application or operating system.
solid state drive	Non-volatile media that uses non-volatile flash memory media to retain its data when power is removed and, unlike non-volatile magnetic media, contains no moving parts.
split tunnelling	Functionality that allows personnel to access both public network infrastructure and a Virtual Private Network connection at the same time, such as an organisation’s system and the internet.
Standard Operating Environment	A standardised build of an operating system and associated software that can be used for servers, workstations, laptops and mobile devices.
Standard Operating Procedure	Instructions for following a defined set of activities in a specific manner. For example, an approved data transfer process.
system	A related set of hardware and software used for the processing, storage or communication of data and the governance framework in which it operates.
system owner	The executive responsible for a system.

system classification	The classification of a system is the highest classification of data which the system is authorised to store, process or communicate.
system security plan	A document that describes a system and its associated security controls.
system-specific security documentation	A system’s system security plan, incident response plan, continuous monitoring plan, security assessment report, and plan of action and milestones.
telemetry	The automatic measurement and transmission of data collected from remote sources. Such data is often used within systems to measure the use, performance and health of one or more functions or devices that make up the system.
telephone	A device that is used for point-to-point communication over a distance. This includes digital and IP telephony.
telephone system	A system designed primarily for the transmission of voice communications.
TOP SECRET area	An area that has been authorised to process, store or communicate TOP SECRET data. Such areas are not necessarily tied to a specific level of security zone.
Transfer Cross Domain Solution	A system that facilitates the transfer of data, in one or multiple directions (low to high or high to low), between different security domains.
transport mode	An IPsec mode that provides a secure connection between two endpoints by encapsulating an IP payload.
trusted source	A person or system formally identified as being capable of reliably producing data meeting certain defined parameters, such as a maximum data classification and reliably reviewing data produced by others to confirm compliance with certain defined parameters.
tunnel mode	An IPsec mode that provides a secure connection between two endpoints by encapsulating an entire IP packet.
unprivileged accounts	Unprivileged accounts include unprivileged user accounts and unprivileged service accounts.

unprivileged operating environments	Unprivileged operating environments are those used for non-administrative activities, such as reading emails and browsing the web.
unsecured space	An area not been certified to the physical security requirements for a Security Zone Two to Security Zone Five area, as defined in the Attorney-General's Department's *Protective Security Policy Framework*, *Entity facilities* policy, to allow for the processing or storage of sensitive or classified data.
user	An individual that is authorised to access a system.
validation	Confirmation (through the provision of strong, sound, objective evidence) that requirements for a specific intended use or application have been fulfilled.
verification	Confirmation, through the provision of objective evidence, that specified requirements have been fulfilled.
Virtual Local Area Network	Network devices and other ICT equipment grouped logically based on resources, security or business requirements instead of their physical location.
Virtual Private Network	A network that maintains privacy through a tunnelling protocol and security procedures. Virtual Private Networks may use encryption to protect network traffic.
virtualisation	Simulation of a hardware platform, operating system, application, storage device or network resource.
volatile media	A type of media, such as random-access memory, which gradually loses its data when power is removed.
vulnerability assessment	A vulnerability assessment can consist of a documentation-based review of a system's design, an in-depth hands-on assessment or automated scanning with software tools. In each case, the goal is to identify as many security vulnerabilities as possible.
wear levelling	A technique used in non-volatile flash memory media to prolong the life of the media. As data can be written to and erased from memory blocks a finite number of times, wear-levelling helps to distribute writes evenly across each memory block, thereby decreasing wear and increasing its lifetime.

Wi-Fi Protected Access	A protocol designed for communicating data over wireless networks.
Wi-Fi Protected Access 2	A protocol designed to replace the Wi-Fi Protected Access protocol for communicating data over wireless networks.
Wi-Fi Protected Access 3	A protocol designed to replace the WPA2 protocol for communicating data over wireless networks.
wireless access point	A device which enables communications between wireless clients. It is typically also the device which connects wired and wireless networks.
wireless communications	The transmission of data over a communications path using electromagnetic waves rather than a wired medium.
wireless network	A network based on the 802.11 standards.
workstation	A stand-alone or networked single-user computer.
X11 Forwarding	X11, also known as the X Window System, is a basic method of video display used in a variety of operating systems. X11 Forwarding allows the video display from one device to be shown on another device.