Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Information security manual

Last updated: September 2025

Table of contents

Using the *Information security manual* **1**

Executive summary 1

Applying a risk-based approach to cybersecurity 2

Cybersecurity principles **6**

The cybersecurity principles 6

Guidelines for cybersecurity roles **10**

Board of directors and executive committee 10

Chief information security officer 12

System owners 16

Guidelines for cybersecurity incidents **18**

Managing cybersecurity incidents 18

Responding to cybersecurity incidents 23

Guidelines for procurement and outsourcing **26**

Cyber supply chain risk management 26

Managed services and cloud services 29

Guidelines for cybersecurity documentation **34**

Development and maintenance of cybersecurity documentation 34

System-specific cybersecurity documentation 37

Guidelines for physical security **41**

Facilities and systems 41

IT equipment and media 44

Guidelines for personnel security **46**

Cybersecurity awareness training 46

Access to systems and their resources 49

Guidelines for communications infrastructure **56**

Cabling infrastructure 56

Emanation security 64

Guidelines for communications systems 66

Telephone systems 66

Video conferencing and Internet Protocol telephony 67

Fax machines and multifunction devices 70

Guidelines for enterprise mobility 74

Enterprise mobility 74

Mobile device management 76

Mobile device usage 78

Guidelines for evaluated products 83

Evaluated product procurement 83

Evaluated product usage 85

Guidelines for information technology equipment 87

IT equipment usage 87

IT equipment maintenance and repairs 89

IT equipment sanitisation and destruction 90

IT equipment disposal 93

Guidelines for media 95

Media usage 95

Media sanitisation 98

Media destruction 101

Media disposal 105

Guidelines for system hardening 106

Operating system hardening 106

User application hardening 114

Server application hardening 118

Authentication hardening 125

Virtualisation hardening 134

Guidelines for system management 137

System administration 137

System patching 139

Data backup and restoration 144

Guidelines for system monitoring 147

Event logging and monitoring 147

Guidelines for software development 151

Software development fundamentals 151

Artificial intelligence application development 161

Mobile application development 162

Web application development 162

Guidelines for database systems 165

Database servers 165

Databases 166

Guidelines for email 169

Email usage 169

Email gateways and servers 170

Guidelines for networking 175

Network design and configuration 175

Wireless networks 182

Service continuity for online services 187

Guidelines for cryptography 191

Cryptographic fundamentals 191

ASD-Approved Cryptographic Algorithms 195

ASD-Approved Cryptographic Protocols 202

Transport Layer Security 203

Secure Shell 204

Secure/Multipurpose Internet Mail Extension 206

Internet Protocol Security 206

Guidelines for gateways 209

Gateways 209

Cross Domain Solutions 213

Firewalls 215

Web application firewalls....216
Diodes....216
Web proxies....217
Web content filters....218
Content filtering....219
Peripheral switches....222
Guidelines for data transfers....224
Data transfers....224
Cybersecurity terminology....227
Glossary of abbreviations....227
Glossary of cybersecurity terms....231

Using the *Information security manual*

Executive summary

Purpose

The purpose of the *Information security manual* (ISM) is to outline a cybersecurity framework that an organisation can apply, using their risk management framework, to protect their information technology and operational technology systems from cyberthreats.

Intended audience

The ISM is intended for chief information security officers (CISOs), chief information officers, cybersecurity professionals and information technology managers.

Authority

The ISM represents the considered advice of the Australian Signals Directorate (ASD). This advice is provided in accordance with ASD's designated functions under the *Intelligence Services Act 2001*.

ASD also provides cybersecurity advice in the form of Australian Communications Security Instructions and other cybersecurity-related publications. In these cases, operating system, application and device-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*, *Security of Critical Infrastructure Act 2018* and *Telecommunications (Interception and Access) Act 1979*.

Cybersecurity principles

The purpose of the cybersecurity principles within the ISM is to provide strategic guidance on how an organisation can protect their information technology and operational technology systems from cyberthreats. These cybersecurity principles are grouped into five functions: govern, identify, protect, detect and respond. An organisation should be able to demonstrate that the cybersecurity principles are being adhered to within their organisation.

Cybersecurity guidelines

The purpose of the cybersecurity guidelines within the ISM is to provide practical guidance on how an organisation can protect their information technology and operational technology systems from cyberthreats. An organisation should consider the cybersecurity guidelines that are relevant to each of the systems they operate.

Applying a risk-based approach to cybersecurity

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 controls, implement controls, assess controls, authorise the system and monitor the system.

Define the system

Determine the system boundary, business criticality 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 system boundary, business criticality 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 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 system boundary, business criticality and security objectives for a system, a description of the system and its characteristics should be documented in the system's system security plan.

Select controls

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

Each cybersecurity guideline discusses security risks associated with the topics it covers. Paired with these discussions are controls that ASD considers to provide efficient and effective mitigations based on their suitability to achieve the security objectives for a system. To assist with selecting and tailoring controls for a system, each control is assigned an applicability marking. For example, 'NC' for the protection of non-classified systems (including both government and non-government systems), 'OS' for the protection of OFFICIAL: Sensitive systems, 'P' for the protection of PROTECTED systems, 'S' for the protection of SECRET systems and 'TS' for the protection of TOP SECRET systems.

While security risks and controls are discussed in the cybersecurity guidelines, and act as a baseline, they should not be considered an exhaustive list for a specific system type or technology. As such, the cybersecurity 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 cybersecurity 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 controls for a system, including the identification of any inherited common controls, 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, controls should also be recorded in the system's cybersecurity incident response plan, change and configuration management plan, and continuous monitoring plan.

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

Implement controls

Implement controls for the system and its operating environment.

Once suitable 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 controls

Assess 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 the assessor, system owner and authorising officer 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 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). For non-classified, OFFICIAL: Sensitive, PROTECTED and SECRET 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 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, cybersecurity incident response plan, change and configuration management 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 an ongoing authorisation to operate. However, in other cases the security risks associated with the operation of a system may be unacceptable. In such cases, the authorising officer may request further work 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, such as limiting the system's functionality or specifying an expiration date for authorisation to operate. Finally, if the authorising officer deems the security risks to be unacceptable, regardless of any potential constraints placed 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, including sensitive compartmented information systems, the authorising officer is Director-General ASD (or their delegate). For non-classified, OFFICIAL: Sensitive, PROTECTED and SECRET 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 cyberthreats, security risks and controls, on an ongoing basis.

Real-time monitoring of cyberthreats, security risks and 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 cyberthreats to the system or its operating environment
- the discovery that controls for the system are not as effective as planned
- a major cybersecurity incident involving the system
- major architectural changes to the system.

Following the implementation or modification of any 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. If the security risks are no longer acceptable, the authorising officer may choose to either place constraints on the system's use, such as introducing or amending an expiration date for authorisation to operate, or revoke authorisation to operate altogether.

Further information

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

- International Organization for Standardization (ISO) 31000:2018, *Risk management – Guidelines*
- International Electrotechnical Commission 31010:2019, *Risk management – Risk assessment techniques*
- ISO/International Electrotechnical Commission 27005:2022, *Information security, cybersecurity and privacy protection – Guidance on managing information security risks*
- 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 is available from ASD.

Cybersecurity principles

The cybersecurity principles

Purpose of the cybersecurity principles

The purpose of the cybersecurity principles is to provide strategic guidance on how an organisation can protect their information technology and operational technology systems from cyberthreats. These cybersecurity principles are grouped into six functions:

- **Govern (GOV):** Develop and maintain a strong and resilient cybersecurity culture.
- **Identify (IDE):** Identify assets and associated security risks.
- **Protect (PRO):** Implement and maintain controls to manage security risks.
- **Detect (DET):** Detect and analyse cybersecurity events to identify cybersecurity incidents.
- **Respond (RES):** Respond to cybersecurity incidents.
- **Recover (REC):** Resume normal business operations following cybersecurity incidents.

Govern principles

The govern principles are:

- **GOV-01 – Executive cybersecurity accountability:** The board of directors or executive committee is accountable for cybersecurity.
- **GOV-02 – Executive cybersecurity leadership:** A chief information security officer provides leadership and oversight of cybersecurity activities.
- **GOV-03 – Security risk management:** Security risk management activities for systems (cyber supply chains, infrastructure, operating systems, applications and data) are embedded into organisational risk management frameworks.
- **GOV-04 – Cybersecurity resourcing:** Suitable and sufficient personnel and resources are identified and acquired in support of cybersecurity activities.
- **GOV-05 – Security risk acceptance:** Residual security risks for systems (cyber supply chains, infrastructure, operating systems, applications and data) are accepted before they are authorised for use and continuously monitored and managed throughout their operational life.
- **GOV-06 – Security risk communication:** Residual security risks for systems (cyber supply chains, infrastructure, operating systems, applications and data) are transparently and mutually communicated with stakeholders.
- **GOV-07 – Security risk insights:** Security risk management, and associated cybersecurity activities, are regularly reviewed to identify potential improvements in processes and procedures.

Identify principles

The identify principles are:

- **IDE-01 – Asset identification:** Systems (cyber supply chains, infrastructure, operating systems, applications and data) are identified and documented.
- **IDE-02 – Business criticality identification:** The business criticality of systems (cyber supply chains, infrastructure, operating systems, applications and data) is determined and documented.
- **IDE-03 – Security requirements identification:** The confidentiality, integrity and availability requirements for systems (cyber supply chains, infrastructure, operating systems, applications and data) are determined and documented.
- **IDE-04 – Security risk identification:** Security risks for systems (cyber supply chains, infrastructure, operating systems, applications and data) are identified and documented along with any associated risk management decisions.

Protect principles

The protect principles are:

- **PRO-01 – Secure system lifecycle:** Systems (infrastructure, operating systems and applications) are planned, designed, developed, tested, deployed, maintained and decommissioned according to their business criticality and their confidentiality, integrity and availability requirements.
- **PRO-02 – Secure by design:** Systems (infrastructure, operating systems and applications) are planned, designed, developed, tested, deployed, maintained and decommissioned using Secure by Design and Secure by Default principles and practices.
- **PRO-03 – Trustworthy suppliers:** Systems (infrastructure, operating systems, applications and data) are delivered and supported by trustworthy suppliers.
- **PRO-04 – Attack surface reduction:** Systems (infrastructure, operating systems and applications) are configured to reduce their attack surface.
- **PRO-05 – Secure administration:** Systems (infrastructure, operating systems, applications and data) are administered in a secure and accountable manner.
- **PRO-06 – Vulnerability management:** Vulnerabilities in systems (cyber supply chains, infrastructure, operating systems, applications and data) are identified and mitigated in a timely manner.
- **PRO-07 – Trustworthy software execution:** Only trustworthy and supported operating systems, applications and code can execute on systems.
- **PRO-08 – Data encryption:** Data is encrypted at rest and in transit.
- **PRO-09 – Content filtering:** Data communicated between different security domains is controlled and inspectable.
- **PRO-10 – Regular proven backups:** Operating systems, applications, settings and data are backed up in a secure and proven manner on a regular basis.

- **PRO-11 – Trustworthy personnel:** Only trustworthy personnel are granted access to systems (cyber supply chains, infrastructure, operating systems, applications and data).
- **PRO-12 – Least privilege access:** Personnel and services are granted the minimum access to systems (cyber supply chains, infrastructure, operating systems, applications and data) required to undertake their duties.
- **PRO-13 – Robust access control:** Robust and secure identity, credential and access management is used to control access to systems (cyber supply chains, infrastructure, operating systems, applications and data).
- **PRO-14 – Cybersecurity awareness training:** Personnel are provided with ongoing cybersecurity awareness training tailored to their duties.
- **PRO-15 – Physical access restriction:** Physical access to systems (infrastructure) is restricted to authorised personnel and monitored for unusual activities.

Detect principles

The detect principles are:

- **DET-01 – Centralised event logging:** Security-relevant event logs and all configuration changes are centrally collected and stored securely.
- **DET-02 – Cybersecurity event detection:** Security-relevant event logs and all configuration changes are analysed in a timely manner to detect cybersecurity events.
- **DET-03 – Cybersecurity incident identification:** Cybersecurity events are analysed in a timely manner to identify cybersecurity incidents.

Respond principles

The respond principles are:

- **RES-01 – Cybersecurity incident planning:** Cybersecurity incident response, business continuity and disaster recovery plans support continued business operations during cybersecurity incidents, and the resumption of normal business operations following cybersecurity incidents.
- **RES-02 – Cybersecurity incident reporting:** Cybersecurity incidents, including associated response activities, are reported internally and externally to relevant bodies and stakeholders in a timely manner.
- **RES-03 – Cybersecurity incident response:** Cybersecurity incidents are contained, eradicated and recovered from in a timely manner.
- **RES-04 – Cybersecurity incident insights:** Lessons learnt from cybersecurity incidents are captured, and areas for improvement are identified and actioned in a timely manner.

Recover principles

The recover principles are:

- **REC-01 – Business operations resumption:** Residual security risks for systems (cyber supply chains, infrastructure, operating systems, applications and data) are accepted prior to the resumption of normal business operations following cybersecurity incidents.

Guidelines for cybersecurity roles

Board of directors and executive committee

Embedding cybersecurity

To ensure that cybersecurity is embedded throughout an organisation, it is important that the board of directors or executive committee commits to defining clear roles and responsibilities for cybersecurity, integrating cybersecurity throughout all business functions within their organisation, aligning the cybersecurity strategy for their organisation with the overarching strategic direction and business strategy, and seeking regular briefings or reporting on the cybersecurity posture of their organisation and the threat environment in which it operates.

Control: ISM-1997; Revision: 0; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The board of directors or executive committee defines clear roles and responsibilities for cybersecurity both within the board of directors or executive committee and broadly within their organisation.

Control: ISM-1998; Revision: 0; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The board of directors or executive committee ensures that cybersecurity is integrated throughout all business functions within their organisation.

Control: ISM-1999; Revision: 0; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The board of directors or executive committee ensures the cybersecurity strategy for their organisation is aligned with the overarching strategic direction and business strategy for their organisation.

Control: ISM-2000; Revision: 0; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The board of directors or executive committee seeks regular briefings or reporting on the cybersecurity posture of their organisation, as well as the threat environment in which they operate, from internal and external subject matter experts.

Championing a positive cybersecurity culture

To provide cybersecurity leadership within an organisation, it is important that the board of directors or executive committee champions a positive cybersecurity culture, including through leading by example.

Control: ISM-2001; Revision: 0; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The board of directors or executive committee champions a positive cybersecurity culture within their organisation, including through leading by example.

Building cybersecurity expertise

To assist with embedding cybersecurity throughout an organisation, it is important that the board of directors or executive committee maintains a sufficient level of cybersecurity literacy to fulfil both their fiduciary duties and any legislative or regulatory obligations. In addition, the board of directors or executive committee should maintain awareness of key cybersecurity recruitment activities, retention rates for cybersecurity personnel, and cybersecurity skills and experience gaps for their organisation. Finally, the board of directors or executive committee should support the development of cybersecurity skills and experience for all personnel within their organisation.

Control: ISM-2002; Revision: 0; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The board of directors or executive committee maintains a sufficient level of cybersecurity literacy to fulfil both their fiduciary duties and any legislative or regulatory obligations.

Control: ISM-2003; Revision: 0; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The board of directors or executive committee maintains awareness of key cybersecurity recruitment activities, retention rates for cybersecurity personnel, and cybersecurity skills and experience gaps within their organisation.

Control: ISM-2004; Revision: 0; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The board of directors or executive committee supports the development of cybersecurity skills and experience for all personnel via internal and external cybersecurity awareness raising and training opportunities.

Identifying critical business assets

In order for the board of directors or executive committee to fulfil both their fiduciary duties and any legislative or regulatory obligations, it is important that they understand the business criticality of their organisation's systems, including a basic understanding of what exists, their value, where they reside, who has access, who might seek access, how they are protected, and how that protection is verified.

Control: ISM-2005; Revision: 1; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The board of directors or executive committee understands the business criticality of their organisation's systems, including at least a basic understanding of what exists, their value, where they reside, who has access, who might seek access, how they are protected, and how that protection is verified.

Planning for major cybersecurity incidents

In order for the board of directors or executive committee to fulfil both their fiduciary duties and any legislative or regulatory obligations, it is important that they plan for major cybersecurity incidents, including by participating in exercises, and understand their duties in relation to such cybersecurity incidents.

Control: ISM-2006; Revision: 0; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The board of directors or executive committee plans for major cybersecurity incidents, including by participating in exercises, and understand their duties in relation to such cybersecurity incidents.

Further information

Further information on how the board of directors or executive committee can protect themselves from cyberthreats can be found in the Australian Signals Directorate's (ASD) *Practical cybersecurity tips for business leaders* publication.

Further information on questions the board of directors or executive committee should be asking of their organisation can be found in ASD's *Questions for the board of directors to ask about cybersecurity* and *Ten things to know about data security* publications.

Further information on how the board of directors or executive committee can plan for major cybersecurity incidents can be found in ASD's *Planning for critical vulnerabilities: What the board of directors needs to know* publication.

Further information on cybersecurity considerations for the board of directors or executive committee during mergers, acquisitions and Machinery of Government changes can be found in ASD's *Mergers, acquisitions and Machinery of Government changes* publication.

Further information on cybersecurity responsibilities and duties of the board of directors or executive committee can be found in the United Kingdom's National Cyber Security Centre's Cyber Security Toolkit for Boards.

Chief information security officer

Breadth of responsibilities

The role of the chief information security officer (CISO) within an organisation should extend to information technology and operational technology. However, where appropriate and practical to do so, responsibility for operational technology cybersecurity may be delegated by the CISO.

Within this section, the breadth of responsibilities for information technology and operational technology are collectively referenced under the banner of cybersecurity.

Required skills and experience

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

Providing cybersecurity leadership and guidance

To provide cybersecurity leadership and guidance within an organisation (for information technology and operational technology), it is important that the organisation appoints a CISO.

Control: ISM-0714; Revision: 7; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
A CISO is appointed to provide cybersecurity leadership and guidance for their organisation (covering information technology and operational technology).

Overseeing the cybersecurity program

The CISO within an organisation is responsible for overseeing their organisation's cybersecurity program and ensuring compliance with cybersecurity 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.

Control: ISM-1478; Revision: 2; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The CISO oversees their organisation's cybersecurity program and ensures their organisation's compliance with cybersecurity policy, standards, regulations and legislation.

Control: ISM-1617; Revision: 1; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The CISO regularly reviews and updates their organisation's cybersecurity program to ensure its relevance in addressing cyberthreats and harnessing business and cybersecurity opportunities.

Control: ISM-1966; Revision: 0; Updated: Dec-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The CISO develops, implements, maintains and verifies on a regular basis a register of systems used by their organisation.

Control: ISM-0724; Revision: 3; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The CISO implements cybersecurity measurement metrics and key performance indicators for their organisation.

Coordinating cybersecurity

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

Control: ISM-0725; Revision: 4; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The CISO coordinates cybersecurity and business alignment through a cybersecurity steering committee or advisory board, comprising of key cybersecurity and business executives, which meets formally and on a regular basis.

Control: ISM-0726; Revision: 3; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The CISO coordinates security risk management activities between cybersecurity and business teams.

Reporting on cybersecurity

The CISO is responsible for reporting cybersecurity matters to their organisation's board of directors or executive committee, as well as their organisation's audit, risk and compliance committee (or equivalent). In doing so, it is important that reporting is done directly by the CISO rather than via other senior executives within their organisation. This ensures reporting remains accurate and free of any conflicts of interest.

Reporting should cover:

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

Reporting on cybersecurity 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.

Control: ISM-0718; Revision: 5; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The CISO regularly reports directly to their organisation's board of directors or executive committee on cybersecurity matters.

Control: ISM-1918; Revision: 1; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The CISO regularly reports directly to their organisation's audit, risk and compliance committee (or equivalent) on cybersecurity matters.

Overseeing cybersecurity incident response activities

To ensure the CISO is able to accurately report to their organisation's board of directors or executive committee on cybersecurity matters, it is important they are fully aware of all cybersecurity incidents within their organisation.

The CISO is also responsible for overseeing their organisation's response to cybersecurity incidents, including how internal teams respond and communicate with each other during cybersecurity incidents. In the event of a major cybersecurity 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.

Control: ISM-0733; Revision: 3; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The CISO is fully aware of all cybersecurity incidents within their organisation.

Control: ISM-1618; Revision: 1; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The CISO oversees their organisation's response to cybersecurity incidents.

Contributing to business continuity and disaster recovery planning

The CISO is responsible for contributing to the development, implementation 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.

Control: ISM-0734; Revision: 4; Updated: Sep-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The CISO contributes to the development, implementation 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.

Communicating a cybersecurity vision and strategy

To assist in facilitating cybersecurity cultural change and awareness within their organisation, across their organisation's cyber supply chain and among their organisation's customers, the CISO should act as a cybersecurity leader and regularly communicate the cybersecurity vision and strategy for their organisation. In doing so, a cybersecurity communications strategy can be helpful in achieving this outcome. As part of this, communication styles and content should be tailored to different target audiences.

Control: ISM-0720; Revision: 4; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The CISO oversees the development, implementation and maintenance of a cybersecurity communications strategy to assist in communicating the cybersecurity vision and strategy for their organisation.

Working with suppliers

The CISO is responsible for ensuring that consistent vendor management processes are applied across their organisation, from discovery through to ongoing management. As supplier 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.

Control: ISM-0731; Revision: 2; Updated: Oct-20; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The CISO oversees cyber supply chain risk management activities for their organisation.

Receiving and managing a dedicated cybersecurity budget

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

Control: ISM-0732; Revision: 3; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The CISO receives and manages a dedicated cybersecurity budget for their organisation.

Overseeing cybersecurity personnel

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

Control: ISM-0717; Revision: 3; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The CISO oversees the management of cybersecurity personnel within their organisation.

Control: ISM-2020; Revision: 0; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The CISO ensures sufficient cybersecurity personnel, with the right skills and experience, are acquired to support cybersecurity activities within their organisation.

Overseeing cybersecurity awareness training

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

Control: ISM-0735; Revision: 4; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The CISO oversees the development, implementation and maintenance of their organisation's cybersecurity awareness training program.

Further information

Further information on responding to cybersecurity incidents can be found in the managing cybersecurity incidents section of the *Guidelines for cybersecurity incidents*.

Further information on the development of a cybersecurity strategy can be found in the development and maintenance of cybersecurity documentation section of the *Guidelines for cybersecurity documentation*.

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

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

Further information on cybersecurity awareness training programs can be found in the cybersecurity awareness training section of the *Guidelines for personnel security*.

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. It is recommended that system owners collaborate with their organisation's internal cybersecurity teams or engage external cybersecurity specialists to assist them with their cybersecurity responsibilities.

Control: ISM-1071; Revision: 1; Updated: Sep-18; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Each system has a designated system owner.

Control: ISM-1525; Revision: 1; Updated: Jan-21; Applicable: NC, OS, P, S, TS; Essential 8: 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 controls, implement controls, assess 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.

Control: ISM-1633; Revision: 1; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
System owners, in consultation with each system's authorising officer, determine the system boundary, business criticality and security objectives for each system based on an assessment of the impact if it were to be compromised.

Control: ISM-1203; Revision: 1; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
System owners, in consultation with each system's authorising officer, conduct a threat and risk assessment for each system.

Control: ISM-1634; Revision: 2; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
System owners, in consultation with each system's authorising officer, select controls for each system and tailor them to achieve desired security objectives.

Control: ISM-0009; Revision: 4; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
System owners, in consultation with each system's authorising officer, identify any supplementary controls required based upon the unique nature of each system, its operating environment and the organisation's risk tolerances.

Control: ISM-1635; Revision: 2; Updated: Jun-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
System owners implement controls for each system and its operating environment.

Control: ISM-1636; Revision: 3; Updated: Mar-25; Applicable: NC, OS, P, S; Essential 8: N/A
System owners, in consultation with each system's authorising officer, ensure controls for each non-classified, OFFICIAL: Sensitive, PROTECTED and SECRET system and its operating environment undergo a security assessment by their organisation's own assessors or Infosec Registered Assessor Program (IRAP) assessors to determine if they have been implemented correctly and are operating as intended.

Control: ISM-1967; Revision: 1; Updated: Mar-25; Applicable: TS; Essential 8: N/A
System owners, in consultation with each system's authorising officer, ensure controls for each TOP SECRET system and its operating environment, including each sensitive compartmented information system and its operating environment, undergo a security assessment by ASD assessors (or their delegates) to determine if they have been implemented correctly and are operating as intended.

Control: ISM-0027; Revision: 5; Updated: Dec-24; Applicable: NC, OS, P, S; Essential 8: N/A
System owners obtain authorisation to operate each non-classified, OFFICIAL: Sensitive, PROTECTED and SECRET system from its authorising officer based on the acceptance of the security risks associated with its operation.

Control: ISM-1968; Revision: 0; Updated: Dec-24; Applicable: TS; Essential 8: N/A
System owners obtain authorisation to operate each TOP SECRET system, including each sensitive compartmented information system, from Director-General ASD (or their delegate) based on the acceptance of the security risks associated with its operation.

Control: ISM-1526; Revision: 3; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
System owners monitor each system, and associated cyberthreats, security risks and controls, on an ongoing basis.

Control: ISM-2021; Revision: 0; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
System owners implement and maintain data minimisation practices for each of their systems.

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.

Control: ISM-1587; Revision: 0; Updated: Aug-20; Applicable: NC, OS, P, S, TS; Essential 8: 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 cybersecurity section of *Using the Information security manual*.

Further information on the purpose of IRAP is available from ASD.

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 cybersecurity incidents

Managing cybersecurity incidents

Cybersecurity events

A cybersecurity 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.

Cybersecurity incidents

A cybersecurity incident is an unwanted or unexpected cybersecurity event, or a series of such events, that either has compromised business operations or has a significant probability of compromising business operations.

Cyber resilience

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

Detecting cybersecurity incidents

One of the core elements of detecting and investigating cybersecurity incidents is the availability of appropriate data sources, such as event logs. The following event logs can be used by an organisation to assist with detecting and investigating cybersecurity incidents:

- **Artificial intelligence applications:** May assist in identifying anomalous or malicious code or user behaviour indicating an exploitation attempt or successful compromise.
- **Cross Domain Solutions:** May assist in identifying anomalous or malicious network traffic indicating an exploitation attempt or successful compromise.
- **Databases:** May assist in identifying anomalous or malicious code or user behaviour indicating an exploitation attempt or successful compromise.
- **Domain Name System services:** May assist in identifying attempts to resolve malicious domain names or Internet Protocol addresses indicating an exploitation attempt or successful compromise.
- **Email servers:** May assist in identifying users targeted with phishing emails thereby helping to identify the initial vector of a compromise.
- **Gateways:** May assist in identifying anomalous or malicious network traffic indicating an exploitation attempt or successful compromise.
- **Mobile applications:** May assist in identifying anomalous or malicious code or user behaviour indicating an exploitation attempt or successful compromise.
- **Multifunction devices:** May assist in identifying anomalous or malicious user behaviour indicating a cybersecurity incident.

- **Operating systems:** May assist in identifying anomalous or malicious activity indicating an exploitation attempt or successful compromise.
- **Remote access services:** May assist in identifying unusual locations of access or times of access indicating an exploitation attempt or successful compromise.
- **Security products:** May assist in identifying anomalous or malicious code or network traffic indicating an exploitation attempt or successful compromise.
- **Server applications:** May assist in identifying anomalous or malicious code or user behaviour indicating an exploitation attempt or successful compromise.
- **System access:** May assist in identifying anomalous or malicious user behaviour indicating an exploitation attempt or successful compromise.
- **User applications:** May assist in identifying anomalous or malicious code or user behaviour indicating an exploitation attempt or successful compromise.
- **Web applications:** May assist in identifying anomalous or malicious code or user behaviour indicating an exploitation attempt or successful compromise.
- **Web proxies:** May assist in identifying anomalous or malicious network traffic indicating an exploitation attempt or successful compromise.

Cybersecurity incident management policy

Establishing a cybersecurity incident management policy can increase the likelihood of successfully planning for, detecting and responding to malicious activity on networks and hosts, such as cybersecurity events and cybersecurity incidents. In doing so, a cybersecurity incident management policy will likely cover the following:

- responsibilities for planning for, detecting and responding to cybersecurity incidents
- resources assigned to cybersecurity incident planning, detection and response activities
- guidelines for triaging and responding to cybersecurity events and cybersecurity incidents.

Furthermore, as part of maintaining the cybersecurity incident management policy, it is important that it is, along with its associated cybersecurity incident response plan, exercised at least annually to ensure it remains fit for purpose.

Control: ISM-0576; Revision: 11; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
A cybersecurity incident management policy, and associated cybersecurity incident response plan, is developed, implemented and maintained.

Control: ISM-1784; Revision: 2; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The cybersecurity incident management policy, including the associated cybersecurity incident response plan, is exercised at least annually.

Cybersecurity incident register

Developing, implementing and maintaining a cybersecurity incident register can assist with ensuring that appropriate remediation activities are undertaken in response to cybersecurity incidents. In addition, the

types and frequency of cybersecurity incidents, along with the costs of any remediation activities, can be used as an input to future risk assessment activities.

Control: ISM-0125; Revision: 7; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
A cybersecurity incident register is developed, implemented and maintained.

Control: ISM-1803; Revision: 1; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
A cybersecurity incident register contains the following for each cybersecurity incident:

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

Insider threat mitigation program

As an insider's authorised access to systems and their resources may make them harder to detect when intentionally performing malicious activities, establishing and maintaining an insider threat mitigation program can assist an organisation to detect and respond to 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 data
- 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.

Control: ISM-1625; Revision: 2; Updated: Jun-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
An insider threat mitigation program is developed, implemented and maintained.

Control: ISM-1626; Revision: 1; Updated: Jun-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Legal advice is sought regarding the development and implementation of an insider threat mitigation program.

Access to sufficient data sources and tools

Successful detection of cybersecurity incidents requires trained cybersecurity personnel with access to sufficient data sources, such as event logs, that are complemented by tools that support 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 cybersecurity personnel.

Control: ISM-0120; Revision: 6; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Cybersecurity personnel have access to sufficient data sources and tools to ensure that systems can be monitored for key indicators of compromise.

Reporting cybersecurity incidents

Reporting cybersecurity incidents to the chief information security officer, 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 oversee any cybersecurity incident response activities. Note, an organisation should also be cognisant of any legislative obligations regarding the reporting of cybersecurity incidents to authorities.

Control: ISM-0123; Revision: 5; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: ML2, ML3
Cybersecurity incidents are reported to the chief information security officer, or one of their delegates, as soon as possible after they occur or are discovered.

Reporting cybersecurity incidents to ASD

The Australian Signals Directorate (ASD) uses the cybersecurity incident reports it receives as the basis for providing assistance to organisations. In addition, cybersecurity incident reports are used to identify trends and maintain an accurate threat environment picture. Finally, ASD utilises this understanding to assist in the development of new and updated cybersecurity advice, capabilities, and techniques to better prevent and respond to evolving cyberthreats. Note, under ASD's limited use obligation, information voluntarily provided to ASD about cybersecurity incidents, or potential cybersecurity incidents, cannot be used for regulatory purposes.

An organisation is recommended to internally coordinate their reporting of cybersecurity incidents to ASD. In doing so, the organisation should be cognisant of any legislative obligations regarding the reporting of cybersecurity incidents to ASD.

The types of cybersecurity incidents that should be reported to ASD include:

- suspicious privileged user account lockouts
- suspicious remote access authentication events
- service accounts suspiciously communicating with internet-based infrastructure
- 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 electronic devices.

Control: ISM-0140; Revision: 9; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: ML2, ML3
Cybersecurity incidents are reported to ASD as soon as possible after they occur or are discovered.

Reporting cybersecurity incidents to customers and the public

Reporting cybersecurity incidents to customers and the public in a timely manner after they occur or are discovered is one way that an organisation can demonstrate their commitment to transparency. Note, an organisation should also be cognisant of any legislative obligations regarding the reporting of cybersecurity incidents to customers and the public.

Control: ISM-1880; Revision: 1; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Cybersecurity incidents that involve customer data are reported to customers and the public in a timely manner after they occur or are discovered.

Control: ISM-1881; Revision: 1; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Cybersecurity incidents that do not involve customer data are reported to customers and the public in a timely manner after they occur or are discovered.

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 cybersecurity incident response plans can be found in the system-specific cybersecurity documentation section of the *Guidelines for cybersecurity documentation*.

Further information on preparing for and responding to cybersecurity incidents can be found in ASD's *Cybersecurity incident response planning: Executive guidance* and *Cybersecurity incident response planning: Practitioner guidance* publications.

Further information on understanding, identifying and preventing the insider threat can be found in the Attorney-General's Department's *Countering the Insider Threat: A guide for Australian Government* publication.

Further information on understanding, identifying and preventing the insider threat can also be found in the Australian Security Intelligence Organisation's *Countering the insider threat* brochure and *Countering the insider threat: A security manager's guide* publication.

Further information on understanding, identifying and preventing the insider threat can also be found on the United Kingdom's National Protective Security Authority's Insider Risk Guidance website.

Further information on developing, implementing and maintaining an insider threat mitigation program can be found in the United States' Cybersecurity & Infrastructure Security Agency's *Insider Threat Mitigation Guide*.

Further information on developing, implementing and maintaining an insider threat mitigation program can also be found in Carnegie Mellon University's Software Engineering Institute's *Common Sense Guide to Mitigating Insider Threats, Seventh Edition* publication.

Further information on reporting of cybersecurity incidents by service providers can be found in the managed services and cloud services section of the *Guidelines for procurement and outsourcing*.

Further information on reporting cybercrime incidents and reporting cybersecurity incidents, including ASD's limited use obligation, is available from ASD.

Responding to cybersecurity incidents

Enacting cybersecurity incident response plans

Following a cybersecurity incident being identified, an organisation's cybersecurity incident response plan should be enacted.

Control: ISM-1819; Revision: 3; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: ML2, ML3
Following the identification of a cybersecurity incident, the cybersecurity incident response plan is enacted.

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.

Control: ISM-0133; Revision: 2; Updated: Jun-21; Applicable: NC, OS, P, S, TS; Essential 8: 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 applications 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.

Control: ISM-0917; Revision: 8; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: 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 applications are 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.*

Control: ISM-1969; Revision: 0; Updated: Dec-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Malicious code, when stored or communicated, is treated beforehand to prevent accidental execution.

Control: ISM-1970; Revision: 1; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Malicious code processed for cybersecurity incident response or research purposes is done so in a dedicated analysis environment that is segregated from other systems.

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 malicious actors from their system, an organisation can take preventative measures to ensure malicious actors have limited forewarning and awareness of planned intrusion remediation activities. Specifically, using an alternative system to plan and coordinate intrusion remediation activities will prevent alerting malicious actors 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 malicious actors, 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 malicious actors have 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.

Control: ISM-0137; Revision: 4; Updated: Dec-21; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Legal advice is sought before allowing intrusion activity to continue on a system for the purpose of collecting further data or evidence.

Control: ISM-1609; Revision: 2; Updated: Dec-21; Applicable: NC, OS, P, S, TS; Essential 8: N/A
System owners are consulted before allowing intrusion activity to continue on a system for the purpose of collecting further data or evidence.

Control: ISM-1731; Revision: 0; Updated: Dec-21; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Planning and coordination of intrusion remediation activities are conducted on a separate system to that which has been compromised.

Control: ISM-1732; Revision: 0; Updated: Dec-21; Applicable: NC, OS, P, S, TS; Essential 8: N/A
To the extent possible, all intrusion remediation activities are conducted in a coordinated manner during the same planned outage.

Control: ISM-1213; Revision: 3; Updated: Sep-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Following intrusion remediation activities, full network traffic is captured for at least seven days and analysed to determine whether malicious actors have been successfully removed from the system.

Maintaining the integrity of evidence

When gathering evidence following a cybersecurity incident, it is important that it is gathered in an appropriate manner and that its integrity is maintained. In addition, if ASD is requested to assist with investigations, no actions which could affect the integrity of evidence should be carried out before ASD becomes involved.

Control: ISM-0138; Revision: 5; Updated: Mar-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The integrity of evidence gathered during an investigation is maintained by investigators:

- *recording all of their actions*
- *maintaining a proper chain of custody*
- *following all instructions provided by relevant law enforcement agencies.*

Further information

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

Further information on handling malicious code infections can be found in National Institute of Standards and Technology Special Publication 800-61 Rev. 3, *Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile*.

Guidelines for procurement and 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 of operating systems, applications, information technology (IT) equipment, operational technology (OT) equipment and services. In particular, an organisation should consider the security risks that may arise as systems, and their components, 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, such as software developers, IT equipment manufacturers, OT equipment manufacturers, service providers and other organisations involved in distribution channels. 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 suppliers operating in Australia may be subject to a foreign government's lawful access to data belonging to their customers.

When procuring operating systems, applications, IT equipment, OT equipment and services, it is important for an organisation to choose vendors that have demonstrated a commitment to the security of their products. This will assist not only with reducing the potential number of vulnerabilities, but also increasing the likelihood that timely patches, updates or vendor mitigations will be released to remediate any vulnerabilities that are found. Furthermore, it is important for an organisation to choose suppliers that have demonstrated a commitment to transparency and that have a strong track record of maintaining the security of their own systems. In support of this, suppliers should openly provide evidence of their implementation of such commitments, especially when requested by their customers. Finally, a shared responsibly model which clearly defines the responsibilities of suppliers and their customers can be highly beneficial and should be created and shared between both parties.

Control: ISM-1631; Revision: 4; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Suppliers of operating systems, applications, IT equipment, OT equipment and services associated with systems are identified.

Control: ISM-1452; Revision: 6; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
A supply chain risk assessment is performed for suppliers of operating systems, applications, IT equipment, OT equipment and services in order to assess the impact to a system's security risk profile.

Control: ISM-1567; Revision: 2; Updated: Sep-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Suppliers identified as high risk by a cyber supply chain risk assessment are not used.

Control: ISM-1568; Revision: 7; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Operating systems, applications, IT equipment, OT equipment and services are procured from suppliers that have demonstrated a commitment to the security of their products and services.

Control: ISM-1882; Revision: 3; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Operating systems, applications, IT equipment, OT equipment and services are procured from suppliers that have demonstrated a commitment to transparency for their products and services.

Control: ISM-1632; Revision: 6; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Operating systems, applications, IT equipment, OT equipment and services are procured from suppliers that have a strong track record of maintaining the security of their own systems.

Control: ISM-1569; Revision: 2; Updated: Sep-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
A shared responsibility model is created, documented and shared between suppliers and their customers in order to articulate the security responsibilities of each party.

Supplier relationship management

Developing, implementing and maintaining a supplier relationship management policy can assist an organisation in identifying, prioritising and maintaining strong relationships with suppliers that have demonstrated a commitment to the security of their products and services. In doing so, these suppliers should be recorded on an approved supplier list.

Control: ISM-1785; Revision: 1; Updated: Dec-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
A supplier relationship management policy is developed, implemented and maintained.

Control: ISM-1786; Revision: 1; Updated: Dec-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
An approved supplier list is developed, implemented and maintained.

Sourcing operating systems, applications, IT equipment, OT equipment and services

In sourcing operating systems, applications, IT equipment, OT equipment and services, an organisation should use trustworthy suppliers as part of cyber supply chain risk management assessments and subsequently recorded on their approved supplier list.

Furthermore, in order to support system availability, an organisation should aim to identify multiple potential suppliers for critical operating systems, applications, IT equipment, OT equipment and services. This coupled with keeping sufficient spares of critical IT equipment and OT equipment in reserve, can assist in mitigating the impact of cyber supply chain disruptions.

Control: ISM-1787; Revision: 3; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Operating systems, applications, IT equipment, OT equipment and services are sourced from approved suppliers.

Control: ISM-1788; Revision: 3; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Multiple potential suppliers are identified for sourcing critical operating systems, applications, IT equipment, OT equipment and services.

Control: ISM-1789; Revision: 2; Updated: Jun-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Sufficient spares of critical IT equipment and OT equipment are sourced and kept in reserve.

Delivery of operating systems, applications, IT equipment, OT equipment and services

As part of the delivery of operating systems, applications, IT equipment, OT equipment and services, measures should be implemented to protect their integrity, noting that such measures will differ depending on whether delivery relates to digital or physical distribution channels. For example, operating systems and

applications may benefit from delivery via encrypted communication channels while IT equipment and OT equipment may benefit from tracking and tamper-evident packaging. In doing so, such measures are only beneficial if they are assessed as part of acceptance of products and services. In all cases, suppliers should be consulted on how best to confirm the integrity of their products and services.

While ensuring the integrity of operating systems, applications, IT equipment, OT equipment and services is important, so is ensuring their authenticity. For example, a counterfeit product or service securely delivered is still a counterfeit product or service that may not operate as intended or pose a risk to the security of a system. To assist in identifying counterfeit products and services, suppliers should be consulted on how best to confirm the authenticity of their products and services.

Control: ISM-1790; Revision: 2; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Operating systems, applications, IT equipment, OT equipment and services are delivered in a manner that maintains their integrity.

Control: ISM-1791; Revision: 2; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The integrity of operating systems, applications, IT equipment, OT equipment and services are assessed as part of acceptance of products and services.

Control: ISM-1792; Revision: 2; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The authenticity of operating systems, applications, IT equipment, OT equipment and services are assessed as part of acceptance of products and services.

Further information

Further information on cyber supply chain risk management can be found in the following Australian Signals Directorate (ASD) publications:

- *Choosing secure and verifiable technologies: Executive guidance*
- *Choosing secure and verifiable technologies*
- *Cyber supply chain risk management*
- *Identifying cyber supply chain risks*.

Further information on cyber supply chain risk management can also be found in the following publications:

- Canada's Canadian Centre for Cyber Security's *Cyber supply chain: An approach to assessing risk*
- New Zealand's National Cyber Security Centre's *Supply Chain Cyber Security: In Safe Hands*
- United Kingdom's National Cyber Security Centre's *Supply chain security guidance*
- United States' Cybersecurity & Infrastructure Security Agency's *Secure by Demand: Priority Considerations for Operational Technology Owners and Operators when Selecting Digital Products*.

Further information on cyber supply chain risk management can also be found on the United States' Cybersecurity & Infrastructure Security Agency's ICT Supply Chain Resource Library website.

Further information on cyber supply chain integrity can be found in National Institute of Standards and Technology Special Publication 800-161 Rev. 1, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*.

Further information on outsourced products and services can be found in the Department of Home Affairs' *Protective Security Policy Framework*.

Further information on the procurement and use of evaluated operating systems, applications and IT equipment can be found in the evaluated product procurement and evaluated product use sections of the *Guidelines for evaluated products*.

Further information on suppliers that have made a pledge to implement Secure by Design and Secure by Default principles and practices can be found on the United States' Cybersecurity & Infrastructure Security Agency's Secure by Design Pledge website.

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, 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.

Control: ISM-1736; Revision: 1; Updated: Dec-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
A managed service register is developed, implemented, maintained and verified on a regular basis.

Control: ISM-1737; Revision: 1; Updated: Sep-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
A managed service register contains the following for each managed service:

- *managed service provider's name*
- *managed service's name*
- *purpose for using the managed service*
- *sensitivity or classification of data involved*
- *due date for the next security assessment of the managed service*
- *contractual arrangements for the managed service*
- *point of contact for users of the managed service*
- *24/7 contact details for the managed service provider.*

Assessment of managed service providers

Managed service providers will need to undergo regular security assessments against the requirements of the *Information security manual* (ISM) 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 services that are being offered as well as any ISM or security-related system changes that have occurred since the previous security assessment.

Control: ISM-1793; Revision: 1; Updated: Dec-24; Applicable: NC, OS, P, S; Essential 8: N/A
Managed service providers and their non-classified, OFFICIAL: Sensitive, PROTECTED and SECRET managed services undergo an Infosec Registered Assessor Program (IRAP) assessment, using the latest release of the ISM available prior to the beginning of the IRAP assessment (or a subsequent release), at least every 24 months.

Control: ISM-1971; Revision: 0; Updated: Dec-24; Applicable: TS; Essential 8: N/A
Managed service providers and their TOP SECRET managed services, including sensitive compartmented information managed services, undergo a security assessment by ASD assessors (or their delegates), using the latest release of the ISM available prior to the beginning of the security assessment (or a subsequent release), at least every 24 months.

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.

Control: ISM-1637; Revision: 2; Updated: Dec-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
An outsourced cloud service register is developed, implemented, maintained and verified on a regular basis.

Control: ISM-1638; Revision: 3; Updated: Sep-22; Applicable: NC, OS, P, S, TS; Essential 8: 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*
- *contractual arrangements for the cloud service*
- *point of contact for users of the cloud service*
- *24/7 contact details for the cloud service provider.*

Control: ISM-1529; Revision: 2; Updated: Dec-21; Applicable: S, TS; Essential 8: N/A
Only community or private clouds are used for outsourced SECRET and TOP SECRET cloud services.

Assessment of outsourced cloud service providers

Outsourced cloud service providers and their cloud services will need to undergo regular security assessments against the requirements of the ISM 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 ISM or security-related system changes that have occurred since the previous security assessment.

Control: ISM-1570; Revision: 2; Updated: Dec-24; Applicable: NC, OS, P, S; Essential 8: N/A
Outsourced cloud service providers and their non-classified, OFFICIAL: Sensitive, PROTECTED and SECRET

cloud services undergo an IRAP assessment, using the latest release of the ISM available prior to the beginning of the IRAP assessment (or a subsequent release), at least every 24 months.

Control: ISM-1972; Revision: 0; Updated: Dec-24; Applicable: TS; Essential 8: N/A
Outsourced cloud service providers and their TOP SECRET cloud services, including sensitive compartmented information cloud services, undergo a security assessment by ASD assessors (or their delegates), using the latest release of the ISM available prior to the beginning of the security assessment (or a subsequent release), at least every 24 months.

Contractual security requirements with service providers

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 with service providers should address how data entrusted to them, including to any of their subcontractors, will be protected during contractual arrangements and following the completion or termination of such contractual arrangements. 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 with service providers 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 in contractual arrangements with service providers.

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 with service providers.

Control: ISM-1395; Revision: 7; Updated: Dec-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Service providers, including any subcontractors, provide an appropriate level of protection for any data entrusted to them or their services.

Control: ISM-0072; Revision: 9; Updated: Dec-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Security requirements associated with the confidentiality, integrity and availability of data are documented in contractual arrangements with service providers and reviewed on a regular and ongoing basis to ensure they remain fit for purpose.

Control: ISM-1571; Revision: 3; Updated: Dec-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The right to verify compliance with security requirements is documented in contractual arrangements with service providers.

Control: ISM-1738; Revision: 1; Updated: Dec-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The right to verify compliance with security requirements documented in contractual arrangements with service providers is exercised on a regular and ongoing basis.

Control: ISM-1804; Revision: 0; Updated: Dec-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Break clauses associated with failure to meet security requirements are documented in contractual arrangements with service providers.

Control: ISM-0141; Revision: 8; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The requirement for service providers to report cybersecurity incidents to a designated point of contact as soon as possible after they occur or are discovered is documented in contractual arrangements with service providers.

Control: ISM-1794; Revision: 1; Updated: Dec-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
A minimum notification period of one month by service providers for significant changes to their own service provider arrangements is documented in contractual arrangements with service providers.

Control: ISM-1451; Revision: 4; Updated: Dec-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Types of data and its ownership is documented in contractual arrangements with service providers.

Control: ISM-1572; Revision: 3; Updated: Jun-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The regions or availability zones where data will be processed, stored and communicated, as well as a minimum notification period for any configuration changes, is documented in contractual arrangements with service providers.

Control: ISM-1573; Revision: 3; Updated: Dec-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Access to all logs relating to an organisation's data and services is documented in contractual arrangements with service providers.

Control: ISM-1574; Revision: 3; Updated: Dec-22; Applicable: NC, OS, P, S, TS; Essential 8: 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 with service providers.

Control: ISM-1575; Revision: 1; Updated: Dec-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
A minimum notification period of one month for the cessation of any services by a service provider is documented in contractual arrangements with service providers.

Access to systems by service providers

To perform their contracted duties, service providers may need to access their customers' systems. However, without proper controls in place, this could leave systems vulnerable – especially when access occurs from outside of Australian borders. As such, an organisation should ensure that their systems are not accessed or administered by service providers unless such requirements, and associated measures to control such requirements, are documented in contractual arrangements with service providers. 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 cybersecurity incident to their customer and make available all logs pertaining to the unauthorised access.

Control: ISM-1073; Revision: 7; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
An organisation's systems are not accessed or administered by a service provider unless a contractual arrangement exists between the organisation and the service provider to do so.

Control: ISM-1576; Revision: 4; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
If an organisation's systems are accessed or administered by a service provider in an unauthorised manner, the organisation is immediately notified.

Further information

Further information on the use of outsourced cloud services can be found in the service continuity for online services section of the *Guidelines for networking*.

Further information on the use of outsourced gateway services can be found in the gateways section of the *Guidelines for gateways*.

Further information on managed service providers can be found in ASD'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 following ASD publications:

- *Cloud computing security for cloud service providers*
- *Cloud computing security for executives*
- *Cloud computing security for tenants*.

Further information on conducting security assessments of cloud service providers can be found in ASD's *Cloud assessment and authorisation* and *Cloud assessment and authorisation FAQ* publications.

Further information on the purpose of IRAP is available from ASD.

Further information on reporting cybersecurity incidents can be found in the reporting cybersecurity incidents section of the *Guidelines for cybersecurity incidents*.

Guidelines for cybersecurity documentation

Development and maintenance of cybersecurity documentation

Cybersecurity strategy

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

Control: ISM-0039; Revision: 7; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
A cybersecurity strategy is developed, implemented and maintained.

Approval of cybersecurity documentation

If cybersecurity documentation is not reviewed and approved by an appropriate authority, system owners risk failing in their duty to ensure that appropriate 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 cybersecurity incident response plan, change and configuration management plan, and continuous monitoring plan, is approved by the system's authorising officer prior to the development of the system.

Control: ISM-0047; Revision: 5; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Organisational-level cybersecurity documentation is approved by the chief information security officer while system-specific cybersecurity documentation is approved by the system's authorising officer.

Control: ISM-1739; Revision: 0; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
A system's security architecture is approved prior to the development of the system.

Maintenance of cybersecurity documentation

Threat environments are dynamic. If cybersecurity 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 cybersecurity initiatives or investments that have reduced effectiveness or are no longer relevant.

Control: ISM-0888; Revision: 6; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Cybersecurity documentation is reviewed at least annually and includes a 'current as at [date]' or equivalent statement.

Communication of cybersecurity documentation

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

Control: ISM-1602; Revision: 1; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Cybersecurity documentation, including notification of subsequent changes, is communicated to all stakeholders.

Further information

Further information on system-specific cybersecurity documentation, such as a system security plan, cybersecurity incident response plan, change and configuration management 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 system registers can be found in the chief information security officer section of the *Guidelines for cybersecurity roles*.

Further information on business continuity and disaster recovery plans can be found in the chief information security officer section of the *Guidelines for cybersecurity roles*.

Further information on cybersecurity communication strategies can be found in the chief information security officer section of the *Guidelines for cybersecurity roles*.

Further information on cybersecurity incident management policy can be found in the managing cybersecurity incidents section of the *Guidelines for cybersecurity incidents*.

Further information on cybersecurity incident registers can be found in the managing cybersecurity incidents section of the *Guidelines for cybersecurity incidents*.

Further information on supplier relationship management policy can be found in the cyber supply chain risk management section of the *Guidelines for procurement and outsourcing*.

Further information on approved supplier lists can be found in the cyber supply chain risk management section of the *Guidelines for procurement and outsourcing*.

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

Further information on outsourced cloud service registers can be found in the managed services and cloud services section of the *Guidelines for procurement and 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 authorised medical device registers can be found in the facilities and systems section of the *Guidelines for physical security*.

Further information on cybersecurity awareness training registers can be found in the cybersecurity awareness training section of the *Guidelines for personnel security*.

Further information on system usage policy can be found in the access to systems and their resources section of the *Guidelines for personnel 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 information technology (IT) equipment management policy can be found in the IT equipment usage section of the *Guidelines for information technology equipment*.

Further information on networked and non-networked IT equipment registers can be found in the IT equipment usage section of the *Guidelines for information technology equipment*.

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

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

Further information on IT equipment disposal processes and procedures can be found in the IT equipment disposal section of the *Guidelines for information technology 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 software developer cybersecurity knowledge and skills registers can be found in the software development fundamentals section of the *Guidelines for software development*.

Further information on vulnerability disclosure policy can be found in the software development fundamentals section of the *Guidelines for software development*.

Further information on vulnerability disclosure processes and procedures can be found in the software development fundamentals 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 cryptographic key management processes and procedures can be found in the cryptographic fundamentals section of the *Guidelines for cryptography*.

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 cybersecurity documentation

System-specific cybersecurity documentation

System-specific cybersecurity documentation, such as a system security plan, cybersecurity incident response plan, change and configuration management 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 cybersecurity matters.

System-specific cybersecurity 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 cybersecurity documentation.

System security plan

The system security plan provides an overview of the system (covering the system's purpose, the system boundary and how the system is managed) as well as an annex that describes the controls that have been identified and implemented for the system.

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

- cybersecurity 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.

Control: ISM-0041; Revision: 6; Updated: Jun-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Systems have a system security plan that includes an overview of the system (covering the system's purpose, the system boundary and how the system is managed) as well as an annex that covers applicable controls from this document and any additional controls that have been identified and implemented.

Cybersecurity incident response plan

Having a cybersecurity incident response plan ensures that when a cybersecurity 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 cybersecurity incident from escalating, restore any impacted system or data, and preserve any evidence.

Control: ISM-0043; Revision: 6; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Systems have a cybersecurity incident response plan that covers the following:

- *guidelines on what constitutes a cybersecurity incident*
- *the types of cybersecurity incidents likely to be encountered and the expected response to each type*
- *how to report cybersecurity incidents, internally to an organisation and externally to relevant authorities*
- *other parties which need to be informed in the event of a cybersecurity incident*
- *the authority, or authorities, responsible for investigating and responding to cybersecurity incidents*

- *the criteria by which an investigation of a cybersecurity incident would be requested from a law enforcement agency, the Australian Signals Directorate or other relevant authority*
- *the steps necessary to ensure the integrity of evidence relating to a cybersecurity incident*
- *system contingency measures or a reference to such details if they are located in a separate document.*

Change and configuration management plan

Having a change and configuration management plan ensures that changes to the configuration of systems can be made in an accountable manner, with appropriate consultation, consideration and approvals, in order to maintain the security of such systems. Furthermore, change management and configuration management processes and procedures provide an opportunity for the security impact of changes to configuration of systems to be considered and, if necessary, additional risk management activities to be undertaken.

Control: ISM-0912; Revision: 6; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Systems have a change and configuration management plan that includes:

- *the establishment and maintenance of authorised baseline configurations for systems*
- *what constitutes routine and urgent changes to the configuration of systems*
- *how changes to the configuration of systems will be requested, tracked and documented*
- *who needs to be consulted prior to routine and urgent changes to the configuration of systems*
- *who needs to approve routine and urgent changes to the configuration of systems*
- *who needs to be notified of routine and urgent changes to the configuration of systems*
- *what additional change management and configuration management processes and procedures need to be followed before, during and after routine and urgent changes to the configuration of systems.*

Continuous monitoring plan

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

Three types of continuous monitoring activities are vulnerability scans, vulnerability assessments and penetration tests. A vulnerability scan involves using tools to conduct automated checks for known vulnerabilities whereas a vulnerability assessment typically consists of a review of a system's architecture or an in-depth hands-on assessment. In each case, the goal is to identify as many 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.

Control: ISM-1163; Revision: 10; Updated: Sep-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Systems have a continuous monitoring plan that includes:

- *conducting vulnerability scans for systems at least fortnightly*
- *conducting vulnerability assessments and penetration tests for systems prior to deployment, including prior to deployment of significant changes, and at least annually thereafter*
- *analysing identified vulnerabilities to determine their potential impact*
- *implementing mitigations based on risk, 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.

Control: ISM-1563; Revision: 1; Updated: Jun-22; Applicable: NC, OS, P, S, TS; Essential 8: 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 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.

Control: ISM-1564; Revision: 0; Updated: May-20; Applicable: NC, OS, P, S, TS; Essential 8: N/A
At the conclusion of a security assessment for a system, a plan of action and milestones is produced by the system owner.

Further information

To assist with the development of system-specific cybersecurity documentation, a system security plan annex template, and an equivalent cloud controls matrix template, are available from the Australian Signals Directorate's *Information security manual* webpage.

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 generally being the use of a security zone for facilities that contain 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 controls in these guidelines. This may include perimeter controls, building standards and staffing levels. As such, an organisation implementing deployable platforms should contact their physical security certification authority to seek additional guidance.

Control: ISM-1973; Revision: 0; Updated: Dec-24; Applicable: NC; Essential 8: N/A
Non-classified systems are secured in suitably secure facilities.

Control: ISM-0810; Revision: 7; Updated: Dec-24; Applicable: OS, P, S, TS; Essential 8: N/A
Classified systems are secured in facilities that meet the requirements for a security zone suitable for their 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 for the protection of servers, network devices and cryptographic equipment.

Control: ISM-1974; Revision: 0; Updated: Dec-24; Applicable: NC; Essential 8: N/A
Non-classified servers, network devices and cryptographic equipment are secured in suitably secure server rooms or communications rooms.

Control: ISM-1053; Revision: 5; Updated: Dec-24; Applicable: OS, P, S, TS; Essential 8: N/A
Classified 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 classification.

Control: ISM-1975; Revision: 0; Updated: Dec-24; Applicable: NC; Essential 8: N/A
Non-classified servers, network devices and cryptographic equipment are secured in suitably secure security containers.

Control: ISM-1530; Revision: 3; Updated: Dec-24; Applicable: OS, P, S, TS; Essential 8: N/A
Classified servers, network devices and cryptographic equipment are secured in security containers suitable for their classification taking into account the combination of security zones they reside in.

Control: ISM-0813; Revision: 5; Updated: Dec-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Server rooms, communications rooms and security containers are not left in unsecured states.

Control: ISM-1074; Revision: 4; Updated: Dec-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Keys or equivalent access mechanisms to server rooms, communications rooms and security containers 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 malicious actors to reset them to factory default settings, thereby removing any 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 the implementation of physical security, 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.

Control: ISM-1296; Revision: 4; Updated: Jun-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Physical security is 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 develop, implement, maintain and regularly verify 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 sensitivities 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.

Control: ISM-1543; Revision: 4; Updated: Dec-22; Applicable: S, TS; Essential 8: N/A
An authorised RF and IR device register for SECRET and TOP SECRET areas is developed, implemented, maintained and verified on a regular basis.

Control: ISM-0225; Revision: 3; Updated: Sep-21; Applicable: S, TS; Essential 8: N/A
Unauthorised RF and IR devices are not brought into SECRET and TOP SECRET areas.

Control: ISM-0829; Revision: 4; Updated: Mar-19; Applicable: S, TS; Essential 8: N/A
Security measures are used to detect and respond to unauthorised RF devices in SECRET and TOP SECRET areas.

Bringing photographic and video recording devices into facilities

Photographic and video recording devices, such as cameras, video cameras and smart glasses, can pose a security risk to an organisation, especially when they are capable of recording photographs or videos in an inconspicuous manner. In SECRET and TOP SECRET areas, it is important that an organisation understands

the security risks associated with the introduction of photographic and video recording devices and develop, implement, maintain and regularly verify a register of those that have been authorised for use in such environments.

Control: ISM-2069; Revision: 0; Updated: Sep-25; Applicable: S, TS; Essential 8: N/A
An authorised photographic and video recording device register for SECRET and TOP SECRET areas is developed, implemented, maintained and verified on a regular basis.

Control: ISM-2070; Revision: 0; Updated: Sep-25; Applicable: S, TS; Essential 8: N/A
Unauthorised photographic and video recording devices are not brought into SECRET and TOP SECRET areas.

Bringing medical devices into facilities

Medical devices are devices approved by the Therapeutic Goods Administration under the *Therapeutic Goods (Medical Devices) Regulations 2002* for diagnostic or therapeutic purposes. The use of medical devices in SECRET and TOP SECRET areas requires active management, similar to RF devices, as they may contain communications functionality that could compromise the physical security of SECRET or TOP SECRET areas or systems within such areas.

Control: ISM-2007; Revision: 0; Updated: Mar-25; Applicable: S, TS; Essential 8: N/A
An authorised medical device register for SECRET and TOP SECRET areas is developed, implemented, maintained and verified on a regular basis.

Control: ISM-2008; Revision: 0; Updated: Mar-25; Applicable: S, TS; Essential 8: N/A
Medical devices that are authorised to be brought into SECRET and TOP SECRET areas meet, at a minimum, the following criteria:

- *are listed on the Australian Register of Therapeutic Goods*
- *have been prescribed by a legally qualified medical practitioner*
- *have been commercially purchased within Australia*
- *do not have inbuilt cellular connectivity*
- *are capable of operating independently of mobile devices*
- *where possible, have Wi-Fi, Bluetooth and other forms of wireless connectivity disabled when operating within SECRET and TOP SECRET areas.*

Control: ISM-2009; Revision: 0; Updated: Mar-25; Applicable: S, TS; Essential 8: N/A
Unauthorised medical devices are not brought into 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.

Control: ISM-0164; Revision: 3; Updated: Dec-21; Applicable: NC, OS, P, S, TS; Essential 8: 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 Department of Home Affairs' *Protective Security Policy Framework*.

Further information on the physical security requirements for specific security zones can be found in the Department of Home Affairs' *Protective Security Policy Framework*.

Further information on selecting security zones and security containers for the protection of information technology (IT) equipment can be found in the Department of Home Affairs' *Protective Security Policy Framework*.

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*.

Further information on medical devices approved by the Therapeutic Goods Administration for diagnostic or therapeutic purposes can be found on the Australian Register of Therapeutic Goods.

IT equipment and media

Securing IT equipment and media

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

- securing IT equipment and media in an appropriate security container
- using IT equipment without hard drives and sanitising memory at shut down
- encrypting hard drives of IT equipment and sanitising memory at shut down
- sanitising memory of IT 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 IT 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.

Control: ISM-0161; Revision: 6; Updated: Jun-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
IT equipment and media are secured when not in use.

Further information

Further information on the handling of IT equipment can be found in the IT equipment usage section of the *Guidelines for information technology 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 and security containers for the protection of IT equipment can be found in the Department of Home Affairs' *Protective Security Policy Framework*.

Guidelines for personnel security

Cybersecurity awareness training

Providing cybersecurity awareness training

An organisation should ensure that cybersecurity awareness training is provided to all personnel in order to assist them in understanding their security responsibilities and the cyberthreats they may be exposed to in the course of their duties. Furthermore, the content of cybersecurity awareness training should be tailored to the needs of specific groups of personnel, such as general users and different classes of high-risk users. Finally, personnel with privileges beyond that of a normal user, such as software developers and system administrators, will require tailored privileged user training.

Control: ISM-0252; Revision: 8; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Cybersecurity awareness training is undertaken annually by all personnel and covers:

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

Control: ISM-1565; Revision: 0; Updated: Jun-20; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Tailored privileged user training is undertaken annually by all privileged users.

Control: ISM-2022; Revision: 0; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
A cybersecurity awareness training register is developed, implemented and maintained.

Managing and reporting suspicious changes to banking details or payment requests

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

With invoice fraud, malicious actors will compromise a vendor's email account and through it have access to legitimate invoices. Malicious actors 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 malicious actors' bank accounts.

With employee impersonation, malicious actors 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 are then sent to malicious actors' bank accounts.

With company impersonation, malicious actors register a domain with a name similar to another organisation. Malicious actors then impersonate that organisation in an email to a vendor and requests a quote for a quantity of expensive assets, such as laptop computers, and subsequently negotiate for the assets to be delivered to them prior to payment. The assets are then delivered to a location specified by malicious actors, 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.

Control: ISM-1740; Revision: 0; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: 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.

Managing and reporting suspicious requests to disclose or change user account details

Suspicious requests to disclose or change user account details, such as changing mobile phone numbers or email addresses, could indicate a malicious actor attempting to access private user details, facilitate password resets or conduct multi-factor authentication bypass attacks against user accounts.

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

Control: ISM-2071; Revision: 0; Updated: Sep-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Personnel dealing with user account details are advised of what social engineering attacks are, how to manage such situations and how to report them.

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 malicious actors 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.

Control: ISM-0817; Revision: 4; Updated: Jan-20; Applicable: NC, OS, P, S, TS; Essential 8: 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 particular care not to post work information to online services unless authorised to do so, especially for chat services, internet forums, social media and artificial intelligence tools. 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 user accounts for online services, especially when using social media.

Control: ISM-0820; Revision: 5; Updated: Jan-20; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Personnel are advised to not post work information to unauthorised online services and to report cases where such information is posted.

Control: ISM-1146; Revision: 3; Updated: Dec-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Personnel are advised to maintain separate work and personal user 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 malicious actors 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 malicious actors 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.

Control: ISM-0821; Revision: 3; Updated: Oct-19; Applicable: NC, OS, P, S, TS; Essential 8: 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 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.

Control: ISM-0824; Revision: 2; Updated: Sep-18; Applicable: NC, OS, P, S, TS; Essential 8: 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 Signals Directorate's (ASD) *Detecting socially engineered messages* publication.

Further information on business email compromise can be found in ASD's *Protecting against business email compromise* publication.

Further information on the use of social media can be found in ASD's *Security tips for social media and messaging apps* publication.

Further information on reporting cybercrime incidents and reporting cybersecurity incidents, including ASD's limited use obligation, is available from ASD.

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 usage policy

To allow an organisation to be capable of holding personnel accountable for the actions they perform on their systems, it is important that the organisation develops, implements and maintains a system usage policy governing the use of systems and their resources.

Control: ISM-1864; Revision: 0; Updated: Sep-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
A system usage policy is developed, implemented and maintained.

System access requirements

Documenting access requirements for systems and their resources, such as applications and data repositories, can assist in determining if personnel meet the appropriate authorisation, security clearance, briefing and need-to-know requirements for access. Types of users for which access requirements should be documented include unprivileged users, privileged users, foreign nationals and contractors.

Control: ISM-0432; Revision: 8; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Access requirements for systems and their resources are documented in their system security plan.

Control: ISM-0434; Revision: 8; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Personnel undergo appropriate employment screening and, where necessary, hold an appropriate security clearance before being granted access to systems and their resources.

Control: ISM-0435; Revision: 4; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Personnel receive any necessary briefings before being granted access to systems and their resources.

Control: ISM-1865; Revision: 1; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Personnel agree to abide by system usage policies before being granted access to systems and their resources.

User identification

Having uniquely identifiable users ensures accountability for access to systems and their resources. Furthermore, where systems process, store or communicate Australian Eyes Only (AUSTEO), Australian Government Access Only (AGAO) or Releasable To (REL) data, and foreign nationals have access, it is important that the foreign nationals are identified as such.

Control: ISM-0414; Revision: 5; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Personnel granted access to systems and their resources are uniquely identifiable.

Control: ISM-0415; Revision: 3; Updated: Aug-19; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The use of shared user accounts is strictly controlled, and personnel using such accounts are uniquely identifiable.

Control: ISM-1583; Revision: 0; Updated: Aug-20; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Personnel who are contractors are identified as such.

Control: ISM-0420; Revision: 12; Updated: Jun-25; Applicable: S, TS; Essential 8: N/A
Where systems process, store or communicate 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 and their resources should have a genuine business requirement validated by their manager or another appropriate authority.

In addition, centrally logging and analysing unprivileged access events can assist in monitoring the security posture of systems and their resources, detecting malicious behaviour and contributing to investigations following cybersecurity incidents.

Control: ISM-0405; Revision: 8; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Requests for unprivileged access to systems and their resources are validated when first requested.

Control: ISM-1852; Revision: 1; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Unprivileged access to systems and their resources is limited to only what is required for users and services to undertake their duties.

Control: ISM-1566; Revision: 3; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Use of unprivileged access is centrally logged.

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.

Control: ISM-0409; Revision: 8; Updated: Jun-22; Applicable: S, TS; Essential 8: 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 controls are in place to ensure such data is not accessible to them.

Control: ISM-0411; Revision: 7; Updated: Jun-22; Applicable: S, TS; Essential 8: N/A
Foreign nationals, excluding seconded foreign nationals, do not have access to systems that process, store or communicate AGAO data unless effective controls are in place to ensure such data is not accessible to them.

Privileged access to systems

Privileged user accounts are considered those that can alter or circumvent system controls. This also applies to user accounts that may only have limited privileges but still have the ability to bypass some system controls.

Privileged user accounts are often targeted by malicious actors as they can potentially give full access to systems and their resources. As such, ensuring that privileged user accounts are prevented from accessing the internet, email and web services minimises opportunities for these accounts to be compromised. However, if privileged user accounts are explicitly authorised to access online services, they should be strictly limited to only what is required for users and services to undertake their duties.

Finally, centrally logging and analysing privileged access events, as well as privileged user account and security group management events, can assist in monitoring the security posture of systems and their resources, detecting malicious behaviour and contributing to investigations following cybersecurity incidents.

Control: ISM-1507; Revision: 4; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: ML1, ML2, ML3
Requests for privileged access to systems and their resources are validated when first requested.

Control: ISM-1508; Revision: 4; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: ML3
Privileged access to systems and their resources is limited to only what is required for users and services to undertake their duties.

Control: ISM-1175; Revision: 6; Updated: Sep-24; Applicable: NC, OS, P, S, TS; Essential 8: ML1, ML2, ML3
Privileged user accounts (excluding those explicitly authorised to access online services) are prevented from accessing the internet, email and web services.

Control: ISM-1883; Revision: 1; Updated: Sep-24; Applicable: NC, OS, P, S, TS; Essential 8: ML1, ML2, ML3
Privileged user accounts explicitly authorised to access online services are strictly limited to only what is required for users and services to undertake their duties.

Control: ISM-1649; Revision: 1; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: ML3
Just-in-time administration is used for the administration of systems and their resources.

Control: ISM-0445; Revision: 8; Updated: Sep-24; Applicable: NC, OS, P, S, TS; Essential 8: ML1, ML2, ML3
Privileged users are assigned a dedicated privileged user account to be used solely for duties requiring privileged access.

Control: ISM-1263; Revision: 5; Updated: Sep-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Unique privileged user accounts are used for administering individual server applications.

Control: ISM-1509; Revision: 3; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: ML2, ML3
Privileged access events are centrally logged.

Control: ISM-1650; Revision: 3; Updated: Sep-24; Applicable: NC, OS, P, S, TS; Essential 8: ML2, ML3
Privileged user account and security group management events are centrally logged.

Privileged access to systems by foreign nationals

As privileged user accounts often have the ability to bypass system 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.

Control: ISM-0446; Revision: 5; Updated: Jun-21; Applicable: S, TS; Essential 8: N/A
Foreign nationals, including seconded foreign nationals, do not have privileged access to systems that process, store or communicate AUSTEO or REL data.

Control: ISM-0447; Revision: 4; Updated: Jun-21; Applicable: S, TS; Essential 8: 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 and their resources, ideally using an automatic mechanism, 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.

Control: ISM-0430; Revision: 8; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Access to systems and their resources are removed or suspended the same day personnel no longer have a legitimate requirement for access.

Control: ISM-1591; Revision: 1; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Access to systems and their resources are removed or suspended as soon as practicable when personnel are detected undertaking malicious activities.

Control: ISM-1404; Revision: 5; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Unprivileged access to systems and their resources are disabled after 45 days of inactivity.

Control: ISM-1648; Revision: 2; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: ML2, ML3
Privileged access to systems and their resources are disabled after 45 days of inactivity.

Control: ISM-1647; Revision: 2; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: ML2, ML3
Privileged access to systems and their resources are disabled after 12 months unless revalidated.

Recording authorisation for personnel to access systems

Retaining records of account requests for systems and their resources will assist in maintaining personnel accountability. Such records should include each user's user identification, their agreement to abide by system usage policies, who provided the authorisation for their access, when their authorisation was granted and when their access was last reviewed.

Control: ISM-0407; Revision: 6; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
A secure record is maintained for the life of systems and their resources that covers the following for each user:

- *their user identification*
- *their signed agreement to abide by system usage policies*
- *who authorised their access*
- *when their access was granted*
- *the level of access they were granted*
- *when their access, and their level of access, was last reviewed*
- *when their level of access was changed, and to what extent (if applicable)*
- *when their access was withdrawn (if applicable).*

Temporary access to systems

Under strict circumstances, temporary access to systems and their resources 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.

Control: ISM-0441; Revision: 9; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
When personnel are granted temporary access to systems and their resources, effective controls are put in place to restrict their access to only data required for them to undertake their duties.

Control: ISM-0443; Revision: 3; Updated: Sep-18; Applicable: S, TS; Essential 8: 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 systems and their resources. As such, an organisation should always have a method for gaining access during emergencies. Typically, emergencies can occur when access cannot be gained via normal authentication processes, such as due to misconfigurations of authentication services, misconfigurations of security settings or due to a cybersecurity incident. In these situations, break glass accounts (also known as emergency access accounts) can be used to gain access. As break glass accounts have the highest level of privileges available, extreme care should be taken to protect them, as well as monitor them for any signs of compromise or abuse.

When break glass accounts are used, any administrative activities performed will not be directly attributable to individuals, and event logs may not be generated. As such, additional 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 break glass accounts are identified and documented in support of change management processes and procedures. This includes documenting the individuals using break glass accounts, the reasons for using break glass accounts and any administrative activities performed using break glass accounts.

As the custodian of each break glass account should be the only party who knows the break glass 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 can assist in reducing the administrative overhead of such activities.

Finally, centrally logging and analysing break glass account events can assist in monitoring the security posture of systems and their resources, detecting malicious behaviour and contributing to investigations following cybersecurity incidents.

Control: ISM-1610; Revision: 1; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
A method of emergency access to systems and their resources is documented and tested at least once when initially implemented and each time fundamental information technology infrastructure changes occur.

Control: ISM-1611; Revision: 0; Updated: Aug-20; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Break glass accounts are only used when normal authentication processes cannot be used.

Control: ISM-1612; Revision: 0; Updated: Aug-20; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Break glass accounts are only used for specific authorised activities.

Control: ISM-1614; Revision: 0; Updated: Aug-20; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Break glass account credentials are changed by the account custodian after they are accessed by any other party.

Control: ISM-1615; Revision: 0; Updated: Aug-20; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Break glass accounts are tested after credentials are changed.

Control: ISM-1613; Revision: 2; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Use of break glass accounts is centrally logged.

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.

Control: ISM-0078; Revision: 5; Updated: Jun-21; Applicable: S, TS; Essential 8: 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.

Control: ISM-0854; Revision: 6; Updated: Dec-21; Applicable: S, TS; Essential 8: 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 Department of Home Affairs' *Protective Security Policy Framework*.

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 user accounts can be found in ASD's *Restricting administrative privileges* publication.

Further information on administering systems and their resources can be found in the system administration 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*.

Guidelines for communications infrastructure

Cabling infrastructure

Applicability

This section is only applicable to facilities located within Australia.

Shared facilities

In addition to common controls, this section provides additional 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.

Control: ISM-0181; Revision: 3; Updated: Mar-21; Applicable: NC, OS, P, S, TS; Essential 8: 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.

Control: ISM-1111; Revision: 3; Updated: Mar-21; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Fibre-optic cables are used for cabling infrastructure instead of copper cables.

Cable register

Developing, implementing, 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.

Control: ISM-0211; Revision: 7; Updated: Dec-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
A cable register is developed, implemented, maintained and verified on a regular basis.

Control: ISM-0208; Revision: 6; Updated: Jun-21; Applicable: NC, OS, P, S, TS; Essential 8: 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 that are developed using computer-aided design and drafting applications, and use alphanumeric grid referencing, can 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.

Control: ISM-1645; Revision: 2; Updated: Dec-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Floor plan diagrams are developed, implemented, maintained and verified on a regular basis.

Control: ISM-1646; Revision: 0; Updated: Jun-21; Applicable: NC, OS, P, S, TS; Essential 8: 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.

Control: ISM-0206; Revision: 7; Updated: Dec-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Cable labelling processes, and supporting cable labelling procedures, are developed, implemented and maintained.

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.

Control: ISM-1096; Revision: 2; Updated: Oct-19; Applicable: NC, OS, P, S, TS; Essential 8: 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.

Control: ISM-1639; Revision: 0; Updated: Mar-21; Applicable: NC, OS, P, S, TS; Essential 8: 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.

Control: ISM-1640; Revision: 0; Updated: Mar-21; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Cables for foreign systems installed in Australian facilities are labelled at inspection points.

Cable colours

To avoid confusion, it is important that, regardless of the type of cabling involved, a consistent cable colour is used. Furthermore, the use of designated cable colours can provide an easy way to distinguish cables for SECRET and TOP SECRET systems from cables for other systems. For example, while SECRET and TOP SECRET cables have designated cable 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, such as non-classified, OFFICIAL: Sensitive and PROTECTED systems, may use the same colour, such as blue.

Control: ISM-1820; Revision: 0; Updated: Mar-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Cables for individual systems use a consistent colour.

Control: ISM-0926; Revision: 11; Updated: Dec-24; Applicable: NC, OS, P; Essential 8: N/A
Non-classified, OFFICIAL: Sensitive and PROTECTED cables are coloured neither salmon pink nor red.

Control: ISM-1718; Revision: 1; Updated: Mar-23; Applicable: S; Essential 8: N/A
SECRET cables are coloured salmon pink.

Control: ISM-1719; Revision: 1; Updated: Mar-23; Applicable: TS; Essential 8: N/A
TOP SECRET cables 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.

Control: ISM-1216; Revision: 4; Updated: Jun-24; Applicable: S, TS; Essential 8: N/A
SECRET and TOP SECRET cables with non-conformant cable colouring are 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. Note, this does not necessarily mean that cables need to be fully visible all the time. Rather, cable inspectability can still be achieved as long as cables can be viewed and inspected through the easy removal of ceiling, floor or wall panels or manholes.

Control: ISM-1112; Revision: 4; Updated: Dec-24; Applicable: NC, OS, P, S; Essential 8: N/A
Cables in non-TOP SECRET areas are inspectable every five metres or less.

Control: ISM-1119; Revision: 2; Updated: Dec-21; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Cables in TOP SECRET areas are fully inspectable for their entire length.

Common cable bundles and conduits

In some circumstances, cables for different systems can be bundled together or run in a common conduit in order to reduce costs, such as cables for OFFICIAL: Sensitive and PROTECTED systems.

Control: ISM-0187; Revision: 8; Updated: Mar-23; Applicable: S; Essential 8: N/A
SECRET cables, when bundled together or run in conduit, are run exclusively in their own individual cable bundle or conduit.

Control: ISM-1821; Revision: 0; Updated: Mar-23; Applicable: TS; Essential 8: N/A
TOP SECRET cables, when bundled together or run in conduit, are run exclusively in their own individual cable bundle or conduit.

Common cable reticulation systems

When cable reticulation systems are used for more than one cable bundle or conduit, it is important that there is a dividing partition or visible gap between cable bundles and conduits to facilitate easier cable inspection.

Control: ISM-1114; Revision: 4; Updated: Mar-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Cable bundles or conduits sharing a common cable reticulation system have a dividing partition or visible gap between each cable bundle and conduit.

Enclosed cable reticulation systems

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

Control: ISM-1130; Revision: 4; Updated: Dec-21; Applicable: NC, OS, P, S, TS; Essential 8: 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.

Control: ISM-1164; Revision: 3; Updated: Dec-21; Applicable: NC, OS, P, S, TS; Essential 8: 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, uniquely identifiable Security Construction and Equipment Committee (SCEC)-approved tamper-evident 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.

Control: ISM-0195; Revision: 7; Updated: Jun-22; Applicable: TS; Essential 8: N/A
In shared facilities, uniquely identifiable SCEC-approved tamper-evident seals are used to seal all removable covers on TOP SECRET cable reticulation systems.

Control: ISM-0194; Revision: 3; Updated: Dec-21; Applicable: TS; Essential 8: 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.

Control: ISM-0201; Revision: 3; Updated: Mar-21; Applicable: TS; Essential 8: 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.

Control: ISM-1115; Revision: 4; Updated: Dec-19; Applicable: NC, OS, P, S, TS; Essential 8: 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.

Control: ISM-1133; Revision: 3; Updated: Dec-21; Applicable: TS; Essential 8: 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.

Control: ISM-1122; Revision: 2; Updated: Dec-21; Applicable: TS; Essential 8: 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.

Control: ISM-1105; Revision: 4; Updated: Mar-23; Applicable: S, TS; Essential 8: N/A
SECRET and TOP SECRET wall outlet boxes contain exclusively SECRET or TOP SECRET cables.

Labelling wall outlet boxes

Clear labelling of wall outlet boxes diminishes the possibility of incorrectly attaching information technology (IT) equipment to the wrong wall outlet box. In cases where a wall outbox contains cables for different systems, each connector should be individually labelled.

Control: ISM-1095; Revision: 5; Updated: Dec-21; Applicable: NC, OS, P, S, TS; Essential 8: 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 wall outlet boxes for SECRET and TOP SECRET systems from wall outlet boxes for other systems. For example, while SECRET and TOP SECRET wall outlet boxes have designated wall outlet box 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, such as non-classified, OFFICIAL: Sensitive and PROTECTED systems, may use the same colour, such as blue. Ideally, wall outlet boxes should be the same colour that is used for associated cabling.

Control: ISM-1822; Revision: 0; Updated: Mar-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Wall outlet boxes for individual systems use a consistent colour.

Control: ISM-1107; Revision: 7; Updated: Dec-24; Applicable: NC, OS, P; Essential 8: N/A
Non-classified, OFFICIAL: Sensitive and PROTECTED wall outlet boxes are coloured neither salmon pink nor red.

Control: ISM-1720; Revision: 0; Updated: Dec-21; Applicable: S; Essential 8: N/A
SECRET wall outlet boxes are coloured salmon pink.

Control: ISM-1721; Revision: 0; Updated: Dec-21; Applicable: TS; Essential 8: 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.

Control: ISM-1109; Revision: 3; Updated: Dec-19; Applicable: NC, OS, P, S, TS; Essential 8: 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.

Control: ISM-0218; Revision: 7; Updated: Jun-24; Applicable: TS; Essential 8: N/A
If TOP SECRET fibre-optic fly leads exceeding five metres in length are used to connect wall outlet boxes to IT equipment, they are run in a protective and easily inspected pathway that is clearly labelled at the IT 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.

Control: ISM-1102; Revision: 3; Updated: Dec-21; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Cable reticulation systems leading into cabinets are terminated as close as possible to the cabinet.

Control: ISM-1101; Revision: 3; Updated: Dec-21; Applicable: NC, OS, P, S, TS; Essential 8: 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.

Control: ISM-1103; Revision: 3; Updated: Dec-21; Applicable: NC, OS, P, S, TS; Essential 8: 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.

Control: ISM-1098; Revision: 5; Updated: Mar-23; Applicable: S; Essential 8: N/A
SECRET cables are terminated in an individual cabinet; or for small systems, a cabinet with a division plate between any SECRET cables and non-SECRET cables.

Control: ISM-1100; Revision: 1; Updated: Sep-18; Applicable: TS; Essential 8: N/A
TOP SECRET cables are terminated in an individual TOP SECRET cabinet.

Terminating cables on patch panels

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

Control: ISM-0213; Revision: 4; Updated: Mar-23; Applicable: S, TS; Essential 8: N/A
SECRET and TOP SECRET cables are terminated on their own individual patch panels.

Physical separation of cabinets and patch panels

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

Control: ISM-0216; Revision: 3; Updated: Mar-23; Applicable: TS; Essential 8: N/A
TOP SECRET patch panels are installed in individual TOP SECRET cabinets.

Control: ISM-0217; Revision: 5; Updated: Mar-23; Applicable: TS; Essential 8: N/A
Where spatial constraints demand non-TOP SECRET patch panels be installed 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.*

Control: ISM-1116; Revision: 4; Updated: Mar-23; Applicable: TS; Essential 8: N/A
A visible gap exists between TOP SECRET cabinets and non-TOP SECRET cabinets.

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.

Control: ISM-0198; Revision: 3; Updated: Dec-21; Applicable: TS; Essential 8: 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.

Control: ISM-1123; Revision: 4; Updated: Jun-24; Applicable: TS; Essential 8: N/A
A power distribution board with a feed from an Uninterruptible Power Supply is used to power all TOP SECRET IT equipment.

Further information

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

Further information on SCEC-approved tamper-evident seals can be found on the SCEC's *Security Equipment Evaluated Products List*.

Further information on audio secure rooms can be found in the Department of Home Affairs' *Protective Security Policy Framework*.

Emanation security

Electromagnetic interference/electromagnetic compatibility standards

All IT equipment used by systems will need to meet industry and government standards relating to electromagnetic interference/electromagnetic compatibility.

Control: ISM-0250; Revision: 5; Updated: Jun-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
IT equipment meets industry and government standards relating to electromagnetic interference/electromagnetic compatibility.

Emanation security doctrine

The Australian Signals Directorate (ASD) specifies additional emanation security requirements in Australian Communications Security Instructions that must be complied with. Such requirements supplement these guidelines and, where conflicts occur, take precedence.

Control: ISM-1884; Revision: 0; Updated: Dec-23; Applicable: OS, P, S, TS; Essential 8: N/A
Emanation security doctrine produced by ASD for the management of emanation security matters is complied with.

Emanation security threat assessments

Obtaining advice from ASD on emanation security threats is vital to protecting SECRET and TOP SECRET systems, inside and outside of Australian borders. In particular, this can assist in preventing SECRET and TOP SECRET systems from emanating compromising signals, which if intercepted and analysed, could lead to serious consequences. Note, the implementation of such advice is in addition to, and not a replacement for, industry and government standards relating to electromagnetic interference/electromagnetic compatibility.

In conducting emanation security threat assessments, it is important that they are sought by system owners as early as possible in a system's life cycle as development timeframes and costs will be much greater if changes have to be made to systems once they have been designed and implemented.

On completion of emanation security threat assessments, system owners will receive a TEMPEST requirements statement that contains recommended actions to be taken to reduce emanation security

risks. In doing so, any recommendations not implemented by system owners will need to be accepted by a system's authorising officer.

Control: ISM-1137; Revision: 5; Updated: Dec-23; Applicable: S, TS; Essential 8: N/A
System owners deploying SECRET or TOP SECRET systems within fixed facilities contact ASD for an emanation security threat assessment.

Control: ISM-0249; Revision: 6; Updated: Dec-23; Applicable: S, TS; Essential 8: N/A
System owners deploying SECRET or TOP SECRET systems in mobile platforms, or as a deployable capability, contact ASD for an emanation security threat assessment.

Control: ISM-0246; Revision: 6; Updated: Dec-24; Applicable: S, TS; Essential 8: N/A
When an emanation security threat assessment is required, it is sought as early as possible in a system's life cycle.

Control: ISM-1885; Revision: 1; Updated: Dec-24; Applicable: S, TS; Essential 8: N/A
Recommended actions contained within TEMPEST requirements statements issued for systems are implemented by system owners.

Further information

Further information on ASD's Emanation Security Program, including a list of certified emanation security providers, is available from ASD.

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.

Control: ISM-1078; Revision: 4; Updated: Dec-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
A telephone system usage policy is developed, implemented and maintained.

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 areas where sensitive or classified conversations may occur.

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.

Control: ISM-0229; Revision: 4; Updated: Jun-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Personnel are advised of the permitted sensitivity or classification of information that can be discussed over internal and external telephone systems.

Control: ISM-0230; Revision: 3; Updated: Sep-18; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Personnel are advised of security risks posed by non-secure telephone systems in areas where sensitive or classified conversations can occur.

Control: ISM-0231; Revision: 2; Updated: Dec-21; Applicable: NC, OS, P, S, TS; Essential 8: 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.

Control: ISM-0232; Revision: 3; Updated: Sep-18; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Telephone systems used for sensitive or classified conversations encrypt all traffic that passes over external systems.

Cordless telephone systems

Cordless telephone handsets and headsets typically have minimal transmission security and are susceptible to interception. As such, using cordless telephone handsets and headsets may result in the disclosure of sensitive or classified conversations to malicious actors unless appropriate encryption is used.

Control: ISM-0233; Revision: 4; Updated: Mar-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Cordless telephone handsets and headsets are not used for sensitive or classified conversations unless all communications are encrypted.

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, they may be used.

Control: ISM-0235; Revision: 5; Updated: Dec-24; Applicable: NC, OS, P, S, TS; Essential 8: 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.

Control: ISM-0236; Revision: 5; Updated: Dec-21; Applicable: NC, OS, P, S, TS; Essential 8: 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.

Control: ISM-0931; Revision: 7; Updated: Dec-24; Applicable: NC, OS, P, S, TS; Essential 8: 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 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 network from a different security domain, the gateways section of the *Guidelines for gateways* applies.

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 applications and only runs required services.

Control: ISM-1562; Revision: 0; Updated: Dec-19; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Video conferencing and IP telephony infrastructure is hardened.

Video-aware and voice-aware firewalls and proxies

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

Control: ISM-0546; Revision: 9; Updated: Jun-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
When video conferencing or IP telephony traffic passes through a gateway containing a firewall or proxy, a video-aware or voice-aware firewall or proxy 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.

Control: ISM-0548; Revision: 4; Updated: Dec-21; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Video conferencing and IP telephony calls are established using a secure session initiation protocol.

Control: ISM-0547; Revision: 4; Updated: Dec-21; Applicable: NC, OS, P, S, TS; Essential 8: 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.

Control: ISM-0554; Revision: 1; Updated: Sep-18; Applicable: NC, OS, P, S, TS; Essential 8: N/A
An encrypted and non-replayable two-way authentication scheme is used for call authentication and authorisation.

Control: ISM-0553; Revision: 3; Updated: Sep-18; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Authentication and authorisation is used for all actions on a video conferencing network, including call setup and changing settings.

Control: ISM-0555; Revision: 3; Updated: Dec-19; Applicable: NC, OS, P, S, TS; Essential 8: 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.

Control: ISM-0551; Revision: 7; Updated: Jan-20; Applicable: NC, OS, P, S, TS; Essential 8: 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.*

Control: ISM-1014; Revision: 6; Updated: Dec-21; Applicable: S, TS; Essential 8: 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.

Control: ISM-0549; Revision: 4; Updated: Oct-19; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Video conferencing and IP telephony traffic is separated physically or logically from other data traffic.

Control: ISM-0556; Revision: 5; Updated: Oct-19; Applicable: NC, OS, P, S, TS; Essential 8: 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 malicious actors 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.

Control: ISM-0558; Revision: 6; Updated: Dec-21; Applicable: NC, OS, P, S, TS; Essential 8: 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, malicious actors can email or host malicious

code on a compromised website and use social engineering techniques to convince users into executing the malicious code on their workstation. Such malicious code may then activate microphones or webcams that are attached to the workstation to act as remote listening and recording devices.

Control: ISM-0559; Revision: 6; Updated: Dec-24; Applicable: NC, OS, P; Essential 8: N/A
Microphones (including headsets and USB handsets) and webcams are not used with non-SECRET workstations in SECRET areas.

Control: ISM-1450; Revision: 3; Updated: Dec-24; Applicable: NC, OS, P, S; Essential 8: N/A
Microphones (including headsets and USB handsets) and webcams are not used with non-TOP SECRET workstations in TOP SECRET areas.

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.

Control: ISM-1019; Revision: 9; Updated: Dec-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
A denial of service response plan for video conferencing and IP telephony services is developed, implemented and maintained.

Control: ISM-1805; Revision: 0; Updated: Dec-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
A denial of service response plan for video conferencing and IP telephony services contains the following:

- *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 Signals Directorate'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 Signals Directorate.

Fax machine and multifunction device usage policy

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

Control: ISM-0588; Revision: 4; Updated: Dec-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
A fax machine and MFD usage policy is developed, implemented and maintained.

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. 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 telecommunications infrastructure. In such cases, the fax machine could send the sensitive or classified fax message in the clear causing a data spill.

Control: ISM-1092; Revision: 2; Updated: Sep-18; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Separate fax machines or MFDs are used for sending sensitive or classified fax messages and all other fax messages.

Control: ISM-0241; Revision: 4; Updated: Dec-21; Applicable: NC, OS, P, S, TS; Essential 8: 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.

Control: ISM-1075; Revision: 2; Updated: Dec-21; Applicable: NC, OS, P, S, TS; Essential 8: 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.

Simultaneously connecting multifunction devices to networks and digital telephone systems

When an MFD is simultaneously connected to 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.

Control: ISM-0245; Revision: 5; Updated: Dec-19; Applicable: NC, OS, P, S, TS; Essential 8: 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.

Authenticating to multifunction devices

To prevent users from printing sensitive or classified documents and forgetting to collect them, as well as assisting with the collection of sufficiently detailed event logs, MFDs should implement authentication measures that are of the same strength as used for other devices on the same network they are connected to, such as user workstations. For example, if user access to workstations on a network requires multi-factor authentication, so should user access to MFDs before users can print, scan or copy documents.

Control: ISM-1854; Revision: 0; Updated: Jun-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Users authenticate to MFDs before they can print, scan or copy documents.

Control: ISM-0590; Revision: 8; Updated: Jun-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Authentication measures for MFDs are the same strength as those used for workstations on networks they are connected to.

Scanning and copying documents on multifunction devices

As MFDs residing on networks are often capable of sending scanned documents across networks they are connected to, personnel should be aware that if they scan documents at a level higher sensitivity or classification than that of the network it will cause a data spill. In addition, MFDs used to copy documents above the sensitivity or classification of the network may cause a localised data spill if copies are retained on non-volatile memory within the devices.

Control: ISM-0589; Revision: 7; Updated: Jun-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
MFDs are not used to scan or copy documents above the sensitivity or classification of networks they are connected to.

Logging multifunction device use

Centrally logging and analysing MFD events, including metadata and shadow copies of documents printed, scanned or copied by users, can assist in monitoring the security posture of systems, detecting malicious behaviour and contributing to investigations following cybersecurity incidents.

Control: ISM-1855; Revision: 1; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Use of MFDs for printing, scanning and copying purposes, including the capture of shadow copies of documents, are centrally logged.

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.

Control: ISM-1036; Revision: 3; Updated: Sep-18; Applicable: NC, OS, P, S, TS; Essential 8: 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*.

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

Guidelines for enterprise mobility

Enterprise mobility

Introduction to enterprise mobility

Enterprise mobility generally refers to situations in which personnel work in a mobile manner, such as part of office hot-desking arrangements, when working from home, when travelling or simply when outside the office environment during normal business hours. While enterprise mobility has traditionally been used to refer to the use of mobile devices, such as smartphones, tablets and laptop computers, it is increasingly being applied to the use of desktop computers as part of working from home arrangements.

This section applies to mobile devices and desktop computers that use either a mobile operating system or a desktop operating system.

Privately-owned mobile devices and desktop computers

Allowing privately-owned mobile devices and desktop computers 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*. Furthermore, if an organisation chooses to allow personnel to use privately-owned mobile devices or desktop computers to access their organisation's classified systems or data, they should ensure that it does not present an unacceptable security risk. This can be achieved in part through the enforced separation of classified data from personal data as well as by preventing the storage of any classified data on privately-owned mobile devices and desktop computers.

Control: ISM-1297; Revision: 5; Updated: Sep-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Legal advice is sought prior to allowing privately-owned mobile devices and desktop computers to access systems or data.

Control: ISM-1400; Revision: 9; Updated: Dec-24; Applicable: OS, P; Essential 8: N/A
Personnel accessing OFFICIAL: Sensitive or PROTECTED systems or data using privately-owned mobile devices or desktop computers have enforced separation of classified data from personal data.

Control: ISM-1866; Revision: 0; Updated: Sep-23; Applicable: OS, P; Essential 8: N/A
Personnel accessing OFFICIAL: Sensitive or PROTECTED systems or data using privately-owned mobile devices or desktop computers are prevented from storing classified data on their privately-owned mobile devices and desktop computers.

Control: ISM-0694; Revision: 8; Updated: Sep-23; Applicable: S, TS; Essential 8: N/A
Privately-owned mobile devices and desktop computers do not access SECRET and TOP SECRET systems or data.

Organisation-owned mobile devices and desktop computers

If an organisation chooses to issue personnel with organisation-owned mobile devices or desktop computers to access their organisation's systems or data, they should ensure that it does not present an

unacceptable security risk. This can be achieved in part by enforcing the separation of classified data from any personal data.

Control: ISM-1482; Revision: 8; Updated: Dec-24; Applicable: OS, P, S, TS; Essential 8: N/A
Personnel accessing systems or data using an organisation-owned mobile device or desktop computer have enforced separation of classified data from personal data.

Connecting mobile devices and desktop computers to the internet

When connecting mobile devices and desktop computers to the internet, good practice generally 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 and desktop computers will typically be protected by additional security functionality, such as web content filtering, provided by an organisation's internet gateway. Note, however, in some cases an organisation may accept the security risks associated with allowing direct connections to specific online services, such as web conferencing services and collaboration tools, for performance reasons.

In connecting mobile devices and desktop computers to an organisation's internet gateway, a split tunnel VPN can allow access into the 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.

Control: ISM-0874; Revision: 6; Updated: Sep-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Mobile devices and desktop computers access the internet via a VPN connection to an organisation's internet gateway rather than via a direct connection to the internet.

Control: ISM-0705; Revision: 4; Updated: Dec-21; Applicable: NC, OS, P, S, TS; Essential 8: N/A
When accessing an organisation's network via a VPN connection, split tunnelling is disabled.

Further information

Further information on allowing the use of privately-owned mobile devices and desktop computers by personnel to access their organisation's systems or data can be found in the Australian Signals Directorate's (ASD) *Bring Your Own Device for executives* publication.

Further information and specific guidance on enterprise mobility can be found in ASD's *Risk management of enterprise mobility (including Bring Your Own Device)* publication.

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

Further information on the procurement and use of online services can be found in the managed services and cloud services section of the *Guidelines for procurement and outsourcing*.

Mobile device management

Mobile device management

This section describes the management of mobile devices, such as smartphones and tablets, that use a mobile operating system. Alternatively, guidance for mobile devices that use a desktop operating system 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, implemented and maintained to ensure that mobile devices are sufficiently hardened. In doing so, it is important that Mobile Device Management solutions that have completed a Common Criteria evaluation against the *Protection Profile for Mobile Device Management*, version 4.0 or later, are used to enforce mobile device management policy.

Control: ISM-1533; Revision: 3; Updated: Dec-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
A mobile device management policy is developed, implemented and maintained.

Control: ISM-1195; Revision: 2; Updated: Sep-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Mobile Device Management solutions that have completed a Common Criteria evaluation against the Protection Profile for Mobile Device Management, version 4.0 or later, are used to enforce mobile device management policy.

Approved mobile platforms

In order to ensure an appropriate level of security, mobile devices that access OFFICIAL: Sensitive or PROTECTED systems or data should use mobile platforms that have completed a Common Criteria evaluation against the *Protection Profile for Mobile Device Fundamentals*, version 3.3 or later, and are operated in accordance with the latest version of their associated ASD security configuration guide. Furthermore, to ensure interoperability and maintain trust, mobile devices that access SECRET or TOP SECRET systems or data must use mobile platforms that have been issued an Approval for Use by ASD and are operated in accordance with the latest version of their associated Australian Communications Security Instruction.

Control: ISM-1867; Revision: 1; Updated: Mar-24; Applicable: OS, P; Essential 8: N/A
Mobile devices that access OFFICIAL: Sensitive or PROTECTED systems or data use mobile platforms that have completed a Common Criteria evaluation against the Protection Profile for Mobile Device Fundamentals, version 3.3 or later, and are operated in accordance with the latest version of their associated ASD security configuration guide.

Control: ISM-0687; Revision: 10; Updated: Sep-23; Applicable: S, TS; Essential 8: N/A
Mobile devices that access SECRET or TOP SECRET systems or data use mobile platforms that have been issued an Approval for Use by ASD and are operated in accordance with the latest version of their associated Australian Communications Security Instruction.

Data storage

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

Control: ISM-0869; Revision: 5; Updated: Dec-21; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Mobile devices encrypt their internal storage and any removable media.

Control: ISM-1868; Revision: 0; Updated: Sep-23; Applicable: S, TS; Essential 8: N/A
SECRET and TOP SECRET mobile devices do not use removable media unless approved beforehand by ASD.

Data communications

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

Control: ISM-1085; Revision: 4; Updated: Dec-21; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Mobile devices encrypt all sensitive or classified data communicated over public network infrastructure.

Maintaining mobile device security

Poorly secured mobile devices are more vulnerable to compromise and can provide malicious actors 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 non-approved applications and 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.

Control: ISM-1886; Revision: 0; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Mobile devices are configured to operate in a supervised (or equivalent) mode.

Control: ISM-1887; Revision: 0; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Mobile devices are configured with remote locate and wipe functionality.

Control: ISM-1888; Revision: 0; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Mobile devices are configured with secure lock screens.

Control: ISM-0863; Revision: 5; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Mobile devices prevent personnel from installing non-approved applications once provisioned.

Control: ISM-0864; Revision: 4; Updated: Dec-21; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Mobile devices prevent personnel from disabling or modifying security functionality once provisioned.

Control: ISM-1366; Revision: 2; Updated: Dec-21; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Security updates are applied to mobile devices as soon as they become available.

Further information

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

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

Further information on Common Criteria Protection Profiles for mobile devices can be found in the following United States' National Information Assurance Partnership publications:

- *Protection Profile for Mobile Device Management Version 4.0*

- *Protection Profile for Mobile Device Fundamentals Version 3.3*.

Further information on hardening mobile platforms can be found in the following ASD 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*.

Mobile device usage

Mobile device usage

This section describes the usage of mobile devices that use either a mobile operating system or a desktop operating system.

Mobile device usage policy

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

Control: ISM-1082; Revision: 3; Updated: Dec-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
A mobile device usage policy is developed, implemented and maintained.

Personnel awareness

As mobile devices often have voice and data communication capabilities, personnel should be made aware of the sensitivity or classification of voice and data that mobile devices have been approved to process, store and communicate. In addition, personnel should be made aware of common security practices for mobile device usage.

Control: ISM-1083; Revision: 2; Updated: Sep-18; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Personnel are advised of the sensitivity or classification permitted for voice and data communications when using mobile devices.

Control: ISM-1299; Revision: 4; Updated: Sep-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Personnel are advised to take the following precautions when using mobile devices:

- *never leave mobile devices or removable media unattended, including by placing them in checked-in luggage or leaving them in hotel safes*
- *never store credentials with mobile devices that they grant access to, such as in laptop computer bags*
- *never lend mobile devices or removable media to untrusted people, even if briefly*
- *never allow untrusted people to connect their mobile devices or removable media to your mobile devices, including for charging*
- *never connect mobile devices to designated charging stations or wall outlet charging ports*

- *never use gifted or unauthorised peripherals, chargers or removable media with mobile devices*
- *never use removable media for data transfers or backups that have not been checked for malicious code beforehand*
- *avoid reuse of removable media once used with other parties' systems or mobile devices*
- *avoid connecting mobile devices to open or untrusted Wi-Fi networks*
- *consider disabling any communications capabilities of mobile devices when not in use, such as Wi-Fi, Bluetooth, Near Field Communication and ultra-wideband*
- *consider periodically rebooting mobile devices*
- *consider using a VPN connection to encrypt all cellular and wireless communications*
- *consider using encrypted email or messaging apps for all communications.*

Using 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.

Control: ISM-0240; Revision: 7; Updated: Dec-21; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Paging, Multimedia Message Service, Short Message Service and messaging apps are not used to communicate sensitive or classified data.

Using 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. However, personnel should still consider the location and manner in which they pair non-classified, OFFICIAL: Sensitive and PROTECTED mobile devices with other 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.

Note, however, the Bluetooth protocol provides inadequate protection for the communication of SECRET and TOP SECRET data. As such, Bluetooth functionality is not suitable for use with SECRET and TOP SECRET mobile devices.

Control: ISM-1196; Revision: 4; Updated: Dec-24; Applicable: NC, OS, P; Essential 8: N/A
Non-classified, OFFICIAL: Sensitive and PROTECTED mobile devices are configured to remain undiscoverable to other Bluetooth devices except during Bluetooth pairing.

Control: ISM-1200; Revision: 7; Updated: Dec-24; Applicable: NC, OS, P; Essential 8: N/A
Bluetooth pairing for non-classified, OFFICIAL: Sensitive and PROTECTED mobile devices is performed using Secure Connections, preferably with Numeric Comparison if supported.

Control: ISM-1198; Revision: 4; Updated: Dec-24; Applicable: NC, OS, P; Essential 8: N/A
Bluetooth pairing for non-classified, OFFICIAL: Sensitive and PROTECTED mobile devices is performed in a manner such that connections are only made between intended Bluetooth devices.

Control: ISM-1199; Revision: 5; Updated: Dec-24; Applicable: NC, OS, P; Essential 8: N/A
Bluetooth pairings for non-classified, OFFICIAL: Sensitive and PROTECTED mobile devices are removed when there is no longer a requirement for their use.

Control: ISM-0682; Revision: 5; Updated: Dec-21; Applicable: S, TS; Essential 8: N/A
Bluetooth functionality is not enabled on SECRET and TOP SECRET mobile devices.

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.

Control: ISM-0866; Revision: 6; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Sensitive or classified data is not viewed on mobile devices in public locations unless care is taken to reduce the chance of the screen of a mobile device being observed.

Control: ISM-1145; Revision: 4; Updated: Dec-21; Applicable: S, TS; Essential 8: N/A
Privacy filters are applied to the screens of SECRET and TOP SECRET mobile devices.

Control: ISM-1644; Revision: 1; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Sensitive or classified phone calls and conversations 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.

Control: ISM-0871; Revision: 3; Updated: Apr-19; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Mobile devices are kept under continual direct supervision when being actively used.

Control: ISM-0870; Revision: 3; Updated: Apr-19; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Mobile devices are carried or stored in a secured state when not being actively used.

Control: ISM-1084; Revision: 4; Updated: Dec-21; Applicable: NC, OS, P, S, TS; Essential 8: 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 malicious actors. This may be achieved through the use of a remote wipe capability or a cryptographic key zeroise or sanitisation function if present.

Control: ISM-0701; Revision: 6; Updated: Dec-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Mobile device emergency sanitisation processes, and supporting mobile device emergency sanitisation procedures, are developed, implemented and maintained.

Control: ISM-0702; Revision: 5; Updated: Dec-21; Applicable: S, TS; Essential 8: 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.

Control: ISM-1298; Revision: 2; Updated: Oct-19; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Personnel are advised of privacy and security risks when travelling overseas with mobile devices.

Control: ISM-1554; Revision: 2; Updated: Dec-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
If travelling overseas with mobile devices to high or extreme risk countries, personnel are:

- *issued with newly provisioned user 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.*

Control: ISM-1555; Revision: 3; Updated: Dec-24; Applicable: NC, OS, P, S, TS; Essential 8: 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 data, applications and user accounts*
- *backup all remaining data, applications and settings.*

While travelling overseas with mobile devices

Personnel lose control of mobile devices and removable media any time they are not on their person. In addition, allowing untrusted people to access mobile devices provides an opportunity for them to be tampered with.

Control: ISM-1088; Revision: 6; Updated: Sep-23; Applicable: NC, OS, P, S, TS; Essential 8: 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, including if later returned*
- *lose mobile devices or removable media, including if 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. 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.

Control: ISM-1300; Revision: 6; Updated: Dec-22; Applicable: NC, OS, P, S, TS; Essential 8: 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 credentials that left their possession during their travel*
- *report if significant doubt exists as to the integrity of any mobile devices or removable media.*

Control: ISM-1556; Revision: 3; Updated: Dec-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
If returning from travelling overseas with mobile devices to high or extreme risk countries, personnel take the following additional actions:

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

Further information

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*.

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's Security Equipment Guide-005, *Briefcases for the Carriage of Security Classified Information*. This publication is available from the Protective Security Policy GovTEAMS community or the Australian Security Intelligence Organisation 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*.

Guidelines for evaluated products

Evaluated product procurement

High Assurance evaluations

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 Signals Directorate (ASD) performs evaluations for products used to protect SECRET and TOP SECRET data via its High Assurance Evaluation Program.

Common Criteria evaluations

The Australian Certification Authority within ASD certifies product evaluations conducted by licensed commercial facilities, in accordance with the Common Criteria (i.e. the International Organization for Standardization/International Electrotechnical Commission 15408 series), 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, certified and mutually-recognised in accordance with the Common Criteria and the Common Criteria Recognition Arrangement (CCRA).

Cryptographic evaluations

Some CCRA schemes leverage the Cryptographic Algorithm Validation Program for the evaluation of cryptographic algorithms used by cryptographic modules within evaluated products. In such cases, 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 cyberthreats. PPs can be published by a recognised CCRA scheme or by the CCRA body itself. PPs published by the CCRA body are referred to as collaborative PPs.

ASD recognises all collaborative PPs listed on the Common Criteria website, and will consider national PPs listed on the United States' National Information Assurance Partnership website, in addition to those listed on ASD's AISEP webpage. 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 ASD 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. In addition, PP modules contain additional requirements that are complementary to or extend upon collaborative PPs. For example, a stateful traffic filtering PP module for a firewall evaluated against a network device collaborative PP. Note, when procuring an evaluated product that has completed a PP-based evaluation, it is important to ensure that all applicable PP modules (as well as a software bill of materials assessment if applicable) were included as part of the product's evaluation.

Control: ISM-0280; Revision: 9; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
If procuring an evaluated product, a product that has completed a PP-based evaluation, including against all applicable PP modules (as well as a software bill of materials assessment if applicable), 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 source 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, digital signatures or cryptographic checksums can often be used to ensure the integrity of the product that was delivered.

Control: ISM-0285; Revision: 1; Updated: Sep-18; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Evaluated products are delivered in a manner consistent with any delivery procedures defined in associated evaluation documentation.

Control: ISM-0286; Revision: 8; Updated: Jun-24; Applicable: S, TS; Essential 8: N/A
When procuring high assurance information technology (IT) equipment, ASD is contacted for any equipment-specific delivery procedures.

Further information

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

Further information on the AISEP is available from ASD.

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

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

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.

Using 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 installed, configured, administered 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.

Control: ISM-0289; Revision: 3; Updated: Jun-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Evaluated products are installed, configured, administered and operated in an evaluated configuration and in accordance with vendor guidance.

Control: ISM-0290; Revision: 9; Updated: Jun-24; Applicable: S, TS; Essential 8: N/A
High assurance IT equipment is installed, configured, administered and operated in an evaluated configuration and in accordance with ASD guidance.

Further information

Further information on patching or updating IT 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*.

Further information on the installation, configuration, administration and operation of high assurance IT equipment is available from ASD.

Guidelines for information technology equipment

IT equipment usage

IT equipment management policy

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

Control: ISM-1551; Revision: 2; Updated: Jun-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
An IT equipment management policy is developed, implemented and maintained.

Hardening IT equipment configurations

When IT equipment is deployed in its default state, or with an unapproved configuration, it can lead to an insecure operating environment that may allow malicious actors to gain an initial foothold on networks. Many settings exist within IT equipment to allow them to be configured in an approved secure state in order to minimise this security risk. As such, the Australian Signals Directorate (ASD) and vendors often produce hardening guidance to assist in hardening the configuration of IT equipment. Note, however, in situations where ASD and vendor hardening guidance conflicts, precedence should be given to implementing the most restrictive guidance.

Control: ISM-1913; Revision: 1; Updated: Jun-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Approved configurations for IT equipment are developed, implemented and maintained.

Control: ISM-1858; Revision: 3; Updated: Jun-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
IT equipment is hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur.

IT equipment registers

Developing, implementing, maintaining and regularly verifying registers of authorised IT equipment can assist an organisation in tracking legitimate IT equipment as well as determining whether unauthorised IT equipment, such as workstations, servers and network devices, have been introduced into their organisation. In doing so, an organisation may choose to split their IT equipment register into two by focusing on whether IT equipment is connected to their network or not.

Control: ISM-0336; Revision: 9; Updated: Jun-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
A networked IT equipment register is developed, implemented, maintained and verified on a regular basis.

Control: ISM-1869; Revision: 1; Updated: Jun-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
A non-networked IT equipment register is developed, implemented, maintained and verified on a regular basis.

Labelling IT equipment

Applying protective markings to IT 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 IT 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.

Control: ISM-0294; Revision: 5; Updated: Jun-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
IT equipment, with the exception of high assurance IT equipment, is labelled with protective markings reflecting its sensitivity or classification.

Labelling high assurance IT equipment

High assurance IT 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 IT equipment.

Control: ISM-0296; Revision: 7; Updated: Jun-24; Applicable: S, TS; Essential 8: N/A
ASD's approval is sought before applying labels to external surfaces of high assurance IT equipment.

Classifying IT equipment

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

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

Control: ISM-0293; Revision: 6; Updated: Jun-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
IT equipment is classified based on the highest sensitivity or classification of data that it is approved for processing, storing or communicating.

Handling IT equipment

When IT 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 IT 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 IT equipment and the level of assurance in the cryptographic equipment, applications or libraries being used to encrypt it.

Control: ISM-1599; Revision: 1; Updated: Jun-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
IT equipment is handled in a manner suitable for its sensitivity or classification.

Further information

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

Further information on securing IT equipment when not in use can be found in the IT equipment and media section of the *Guidelines for physical security*.

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

Further information on the protection of IT equipment can be found in the Department of Home Affairs' *Protective Security Policy Framework*.

IT equipment maintenance and repairs

Maintenance and repairs of high assurance IT equipment

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

Control: ISM-1079; Revision: 7; Updated: Jun-24; Applicable: S, TS; Essential 8: N/A
ASD's approval is sought before undertaking any maintenance or repairs to high assurance IT equipment.

On-site maintenance and repairs

Undertaking unauthorised maintenance or repairs to IT equipment could impact its integrity. As such, using appropriately cleared technicians to maintain and repair IT 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 technicians that are not appropriately cleared to maintain or repair IT equipment should be aware of the requirement for cleared personnel to escort the technicians during maintenance and repair activities.

Control: ISM-0305; Revision: 7; Updated: Jun-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Maintenance and repairs of IT equipment is carried out on site by an appropriately cleared technician.

Control: ISM-0307; Revision: 4; Updated: Jun-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
If an appropriately cleared technician is not used to undertake maintenance or repairs of IT equipment, the IT equipment and associated media is sanitised before maintenance or repair work is undertaken.

Control: ISM-0306; Revision: 7; Updated: Jun-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
If an appropriately cleared technician is not used to undertake maintenance or repairs of IT 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 IT equipment*
- *has the authority to direct the technician*
- *is sufficiently familiar with the IT equipment to understand the work being performed.*

Off-site maintenance and repairs

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

Control: ISM-0310; Revision: 8; Updated: Jun-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
IT equipment maintained or repaired off site is done so at facilities approved for handling the sensitivity or classification of the IT equipment.

Inspection of IT equipment following maintenance and repairs

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

Control: ISM-1598; Revision: 2; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Following maintenance or repair activities for IT equipment, the IT equipment is inspected to confirm it retains its approved configuration and that no unauthorised modifications have taken place.

Further information

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

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

IT equipment sanitisation and destruction

IT equipment sanitisation processes and procedures

Developing, implementing and maintaining processes and procedures for IT equipment sanitisation will ensure that an organisation carries out IT equipment sanitisation in an appropriate and consistent manner.

Control: ISM-0313; Revision: 7; Updated: Jun-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
IT equipment sanitisation processes, and supporting IT equipment sanitisation procedures, are developed, implemented and maintained.

IT equipment destruction processes and procedures

Developing, implementing and maintaining processes and procedures for IT equipment destruction will ensure that an organisation carries out IT equipment destruction in an appropriate and consistent manner.

Control: ISM-1741; Revision: 2; Updated: Jun-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
IT equipment destruction processes, and supporting IT equipment destruction procedures, are developed, implemented and maintained.

Sanitising IT equipment

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

Media typically found in IT 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.

Control: ISM-0311; Revision: 7; Updated: Jun-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
IT equipment containing media is sanitised by removing the media from the IT equipment or by sanitising the media in situ.

Control: ISM-1742; Revision: 1; Updated: Jun-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
IT equipment that cannot be sanitised is destroyed.

Sanitising highly sensitive IT equipment

IT 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.

Control: ISM-1218; Revision: 5; Updated: Jun-24; Applicable: S, TS; Essential 8: N/A
IT equipment, including associated media, that is located overseas and has processed, stored or communicated AUSTEO or AGAO data, is sanitised in situ.

Control: ISM-0312; Revision: 7; Updated: Jun-24; Applicable: S, TS; Essential 8: N/A
IT 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 IT equipment

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

Control: ISM-0315; Revision: 9; Updated: Jun-24; Applicable: S, TS; Essential 8: N/A
High assurance IT 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.

Control: ISM-0317; Revision: 3; Updated: Sep-18; Applicable: NC, OS, P, S, TS; Essential 8: N/A
At least three pages of random text with no blank areas are printed on each colour printer cartridge or MFD print drum.

Control: ISM-1219; Revision: 2; Updated: Dec-21; Applicable: NC, OS, P, S, TS; Essential 8: 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.

Control: ISM-1220; Revision: 2; Updated: Dec-21; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Printer and MFD platens are inspected and destroyed if any text or images are retained on the platen.

Control: ISM-1221; Revision: 1; Updated: Sep-18; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Printers and MFDs are checked to ensure no pages are trapped in the paper path due to a paper jam.

Control: ISM-0318; Revision: 3; Updated: Sep-18; Applicable: NC, OS, P, S, TS; Essential 8: N/A
When unable to sanitise printer cartridges or MFD print drums, they are destroyed as per electrostatic memory devices.

Control: ISM-1534; Revision: 0; Updated: Sep-18; Applicable: NC, OS, P, S, TS; Essential 8: 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.

Control: ISM-1076; Revision: 2; Updated: Sep-18; Applicable: NC, OS, P, S, TS; Essential 8: 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.

Control: ISM-1222; Revision: 1; Updated: Sep-18; Applicable: NC, OS, P, S, TS; Essential 8: 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.

Control: ISM-1223; Revision: 6; Updated: Dec-21; Applicable: NC, OS, P, S, TS; Essential 8: 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.

Control: ISM-1225; Revision: 2; Updated: Sep-18; Applicable: NC, OS, P, S, TS; Essential 8: 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.

Control: ISM-1226; Revision: 2; Updated: Sep-18; Applicable: NC, OS, P, S, TS; Essential 8: 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*.

IT equipment disposal

IT equipment disposal processes and procedures

Developing, implementing and maintaining processes and procedures for IT equipment disposal will ensure that an organisation carries out IT equipment disposal in an appropriate and consistent manner.

Control: ISM-1550; Revision: 3; Updated: Jun-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
IT equipment disposal processes, and supporting IT equipment disposal procedures, are developed, implemented and maintained.

Disposal of IT equipment

Before IT equipment can be released into the public domain, it needs to be sanitised, destroyed or declassified. As sanitised, destroyed or declassified IT 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 IT equipment with its prior use will ensure it does not draw undue attention following its disposal.

Control: ISM-1217; Revision: 3; Updated: Jun-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Labels and markings indicating the owner, sensitivity, classification or any other marking that can associate IT equipment with its prior use are removed prior to its disposal.

Control: ISM-0321; Revision: 6; Updated: Jun-24; Applicable: S, TS; Essential 8: N/A
When disposing of IT equipment that has been designed or modified to meet emanation security standards, ASD is contacted for requirements relating to its disposal.

Control: ISM-0316; Revision: 4; Updated: Jun-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Following sanitisation, destruction or declassification, a formal administrative decision is made to release IT 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, implemented and maintained 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.

Control: ISM-1549; Revision: 1; Updated: Dec-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
A media management policy is developed, implemented and maintained.

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.

Control: ISM-1359; Revision: 4; Updated: Dec-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
A removable media usage policy is developed, implemented and maintained.

Removable media register

Developing, implementing, 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.

Control: ISM-1713; Revision: 2; Updated: Dec-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
A removable media register is developed, implemented, 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.

Control: ISM-0332; Revision: 5; Updated: Jun-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Media, with the exception of internally mounted fixed media within information technology 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.

Control: ISM-0323; Revision: 8; Updated: Dec-21; Applicable: NC, OS, P, S, TS; Essential 8: 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.

Control: ISM-0337; Revision: 6; Updated: Dec-21; Applicable: NC, OS, P, S, TS; Essential 8: 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.

Control: ISM-0325; Revision: 6; Updated: Apr-21; Applicable: NC, OS, P, S, TS; Essential 8: 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.

Control: ISM-0330; Revision: 7; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: 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, applications or libraries being used to encrypt it.

Control: ISM-0831; Revision: 5; Updated: Sep-18; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Media is handled in a manner suitable for its sensitivity or classification.

Control: ISM-1059; Revision: 4; Updated: Dec-21; Applicable: NC, OS, P, S, TS; Essential 8: 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.

Control: ISM-1600; Revision: 1; Updated: Apr-21; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Media is sanitised before it is used for the first time.

Control: ISM-1642; Revision: 0; Updated: Apr-21; Applicable: NC, OS, P, S, TS; Essential 8: 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.

Control: ISM-0347; Revision: 5; Updated: Apr-21; Applicable: NC, OS, P, S, TS; Essential 8: 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.

Control: ISM-0947; Revision: 6; Updated: Apr-21; Applicable: NC, OS, P, S, TS; Essential 8: 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 cyber supply chain risk management can be found in the cyber supply chain risk management section of the *Guidelines for procurement and outsourcing*.

Further information on the protection of media can be found in the Department of Home Affairs' *Protective Security Policy Framework*.

Further information on securing media when not in use can be found in the IT 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.

Control: ISM-0348; Revision: 5; Updated: Dec-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Media sanitisation processes, and supporting media sanitisation procedures, are developed, implemented and maintained.

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. In addition to the removal of power, SECRET and TOP SECRET volatile media should be overwritten at least once in its entirety with a random pattern followed by a read back for verification.

Control: ISM-0351; Revision: 6; Updated: Dec-21; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Volatile media is sanitised by removing its power for at least 10 minutes.

Control: ISM-0352; Revision: 4; Updated: Dec-21; Applicable: S, TS; Essential 8: 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.

Control: ISM-0835; Revision: 4; Updated: Dec-21; Applicable: TS; Essential 8: 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, magnetic tape and floppy disks. While non-volatile magnetic tape 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.

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 applications 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 applications 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.

Control: ISM-0354; Revision: 6; Updated: Dec-21; Applicable: NC, OS, P, S, TS; Essential 8: 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.

Control: ISM-1065; Revision: 3; Updated: Dec-21; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The host-protected area and device configuration overlay table are reset prior to the sanitisation of non-volatile magnetic hard drives.

Control: ISM-1067; Revision: 4; Updated: Dec-21; Applicable: NC, OS, P, S, TS; Essential 8: 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.

Control: ISM-0356; Revision: 6; Updated: Dec-21; Applicable: S, TS; Essential 8: 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. Subsequently, the non-volatile EPROM media should be overwritten at least once in its entirety with a random pattern followed by a read back for verification.

Control: ISM-0357; Revision: 5; Updated: Dec-21; Applicable: NC, OS, P, S, TS; Essential 8: 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, followed by a read back for verification, is considered suitable for sanitising non-volatile electrically erasable programmable read-only memory (EEPROM) media.

Control: ISM-0836; Revision: 3; Updated: Dec-21; Applicable: NC, OS, P, S, TS; Essential 8: 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.

Control: ISM-0358; Revision: 6; Updated: Dec-21; Applicable: S, TS; Essential 8: 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 at least twice, and followed by a read back for verification, as this helps to ensure that all memory blocks are overwritten.

Control: ISM-0359; Revision: 4; Updated: Dec-21; Applicable: NC, OS, P, S, TS; Essential 8: 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 potential 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.

Control: ISM-0360; Revision: 6; Updated: Dec-21; Applicable: S, TS; Essential 8: 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, attempts to sanitise media, or verify the sanitisation of media, will be unsuccessful. For example, due to the media being faulty or damaged. In such cases, the media will need to be destroyed prior to its disposal.

Control: ISM-1735; Revision: 1; Updated: Sep-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Media that cannot be successfully sanitised is destroyed prior to its disposal.

Further information

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.

Media destruction

Media destruction processes and procedures

Developing, implementing and maintaining processes and procedures for media destruction will ensure that an organisation carries out media destruction in an appropriate and consistent manner.

Control: ISM-0363; Revision: 4; Updated: Dec-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Media destruction processes, and supporting media destruction procedures, are developed, implemented and maintained.

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.

Control: ISM-0350; Revision: 5; Updated: Dec-21; Applicable: NC, OS, P, S, TS; Essential 8: 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's *Security Equipment Evaluated Products List*, and in the Australian Security Intelligence Organisation's (ASIO) Security Equipment Guide-009, *Optical Media Shredders* and Security Equipment Guide-018, *Destructors*. ASIO's Security Equipment Guides 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 the *NSA/CSS Evaluated Products List for Magnetic Degaussers* and information on common types of magnetic media and their associated magnetic field strengths and orientations.

Control: ISM-1361; Revision: 3; Updated: Jun-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Security Construction and Equipment Committee-approved equipment or ASIO-approved equipment is used when destroying media.

Control: ISM-1160; Revision: 2; Updated: Aug-20; Applicable: NC, OS, P, S, TS; Essential 8: 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.

Control: ISM-1517; Revision: 0; Updated: Sep-18; Applicable: NC, OS, P, S, TS; Essential 8: 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.

Control: ISM-1722; Revision: 1; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Electrostatic memory devices are destroyed using a furnace/incinerator, hammer mill, disintegrator or grinder/sander.

Control: ISM-1723; Revision: 1; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Magnetic floppy disks are destroyed using a furnace/incinerator, hammer mill, disintegrator, degausser or by cutting.

Control: ISM-1724; Revision: 1; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Magnetic hard disks are destroyed using a furnace/incinerator, hammer mill, disintegrator, grinder/sander or degausser.

Control: ISM-1725; Revision: 1; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Magnetic tapes are destroyed using a furnace/incinerator, hammer mill, disintegrator, degausser or by cutting.

Control: ISM-1726; Revision: 1; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Optical disks are destroyed using a furnace/incinerator, hammer mill, disintegrator, grinder/sander or by cutting.

Control: ISM-1727; Revision: 1; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Semiconductor memory is destroyed using a furnace/incinerator, hammer mill or disintegrator.

Control: ISM-0368; Revision: 8; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: 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, if a destruction method is used that results in the generation of media waste particles, such as a hammer mill, disintegrator, grinder/sander or by cutting, it may still need to be stored and handled as classified waste.

Control: ISM-1728; Revision: 0; Updated: Dec-21; Applicable: S; Essential 8: 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.

Control: ISM-1729; Revision: 0; Updated: Dec-21; Applicable: TS; Essential 8: 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.

Control: ISM-0361; Revision: 4; Updated: Dec-21; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Magnetic media is destroyed using a degausser with a suitable magnetic field strength and magnetic orientation.

Control: ISM-0362; Revision: 4; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Product-specific directions provided by degausser manufacturers are followed.

Control: ISM-1641; Revision: 2; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: 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 cleared person.

Control: ISM-0370; Revision: 6; Updated: Sep-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The destruction of media is performed under the supervision of at least one cleared person.

Control: ISM-0371; Revision: 4; Updated: Dec-21; Applicable: NC, OS, P, S, TS; Essential 8: 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 cleared personnel who sign a destruction certificate afterwards.

Control: ISM-0372; Revision: 6; Updated: Sep-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The destruction of media storing accountable material is performed under the supervision of at least two cleared personnel.

Control: ISM-0373; Revision: 4; Updated: Dec-21; Applicable: NC, OS, P, S, TS; Essential 8: 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

While media storing accountable material cannot be outsourced, media storing non-accountable material can be outsourced when using a National Association for Information Destruction AAA certified destruction service with endorsements, as specified in ASIO's Protective Security Circular-167, *External destruction of security classified information*. This publication is available from the Protective Security Policy GovTEAMS community or ASIO by email.

Control: ISM-0839; Revision: 3; Updated: Dec-21; Applicable: OS, P, S, TS; Essential 8: N/A
The destruction of media storing accountable material is not outsourced.

Control: ISM-0840; Revision: 4; Updated: Jun-22; Applicable: OS, P, S; Essential 8: N/A
When outsourcing the destruction of media storing non-accountable material, a National Association for Information Destruction AAA certified destruction service with endorsements, as specified in ASIO's Protective Security Circular-167, is used.

Further information

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

Media disposal

Media disposal processes and procedures

Developing, implementing and maintaining processes and procedures for media disposal will ensure that an organisation carries out media disposal in an appropriate and consistent manner.

Control: ISM-0374; Revision: 4; Updated: Dec-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Media disposal processes, and supporting media disposal procedures, are developed, implemented and maintained.

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.

Control: ISM-0378; Revision: 4; Updated: Dec-21; Applicable: NC, OS, P, S, TS; Essential 8: 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.

Control: ISM-0375; Revision: 6; Updated: Dec-21; Applicable: NC, OS, P, S, TS; Essential 8: 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 and Secure by Default principles and practices, including secure programming practices and either memory-safe programming languages (such as C#, Go, Java, Ruby, Rust and Swift) or less preferably memory-safe programming practices. This will assist not only with reducing the potential number of vulnerabilities in operating systems, but also increasing the likelihood that timely patches, updates or vendor mitigations will be released to remediate any vulnerabilities that are found.

Control: ISM-1743; Revision: 2; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Vendors that have demonstrated a commitment to Secure by Design and Secure by Default principles and practices, including secure programming practices and either memory-safe programming languages or less preferably memory-safe programming practices, are used for operating systems.

Operating system releases and versions

Newer releases of operating systems often introduce improvements in security functionality. This can make it more difficult for malicious actors to craft reliable exploits for vulnerabilities they discover. Using older releases of operating systems, especially those no longer supported by vendors, may expose an organisation to 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.

Control: ISM-1407; Revision: 5; Updated: Dec-22; Applicable: NC, OS, P, S, TS; Essential 8: ML3
The latest release, or the previous release, of operating systems are used.

Control: ISM-1408; Revision: 5; Updated: Dec-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Where supported, 64-bit versions of operating systems are used.

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 malicious actors 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), provided via an automated build process or a golden image, 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 trustworthy 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.

Control: ISM-1406; Revision: 2; Updated: Aug-20; Applicable: NC, OS, P, S, TS; Essential 8: N/A
SOEs are used for workstations and servers.

Control: ISM-1608; Revision: 1; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
SOEs provided by third parties are scanned for malicious code and configurations.

Control: ISM-1588; Revision: 0; Updated: Aug-20; Applicable: NC, OS, P, S, TS; Essential 8: N/A
SOEs are reviewed and updated at least annually.

Hardening operating system configurations

When operating systems are deployed in their default state, or with an unapproved configuration, it can lead to an insecure operating environment that may allow malicious actors to gain an initial foothold on networks. Many settings exist within operating systems to allow them to be configured in an approved secure state in order to minimise this security risk. As such, the Australian Signals Directorate (ASD) and vendors often produce hardening guidance to assist in hardening the configuration of operating systems. Note, however, in situations where ASD and vendor hardening guidance conflicts, precedence should be given to implementing the most restrictive guidance.

Control: ISM-1914; Revision: 0; Updated: Mar-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Approved configurations for operating systems are developed, implemented and maintained.

Control: ISM-1409; Revision: 4; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Operating systems are hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur.

Control: ISM-0383; Revision: 11; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Default user accounts or credentials for operating systems, including for any pre-configured user accounts, are changed, disabled or removed during initial setup.

Control: ISM-0380; Revision: 10; Updated: Dec-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Unneeded user accounts, components, services and functionality of operating systems are disabled or removed.

Control: ISM-0341; Revision: 4; Updated: Dec-21; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Automatic execution features for removable media are disabled.

Control: ISM-1654; Revision: 0; Updated: Sep-21; Applicable: NC, OS, P, S, TS; Essential 8: ML1, ML2, ML3
Internet Explorer 11 is disabled or removed.

Control: ISM-1655; Revision: 0; Updated: Sep-21; Applicable: NC, OS, P, S, TS; Essential 8: ML3
.NET Framework 3.5 (includes .NET 2.0 and 3.0) is disabled or removed.

Control: ISM-1492; Revision: 2; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Operating system exploit protection functionality is enabled.

Control: ISM-1745; Revision: 0; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Early Launch Antimalware, Secure Boot, Trusted Boot and Measured Boot functionality is enabled.

Control: ISM-1584; Revision: 1; Updated: Sep-21; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Unprivileged users are prevented from bypassing, disabling or modifying security functionality of operating systems.

Control: ISM-1491; Revision: 3; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: 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 malicious actors using social engineering in order to convince them to install malicious applications. 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 application repositories or from trustworthy 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 applications.

Control: ISM-1592; Revision: 2; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Unprivileged users do not have the ability to install unapproved applications.

Control: ISM-0382; Revision: 8; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Unprivileged users do not have the ability to uninstall or disable approved applications.

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), 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 files), HTML applications (e.g. .hta files), control panel applets (e.g. .cpl files) 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 malicious actors.

Finally, centrally logging and analysing application control events can assist in monitoring the security posture of systems, detecting malicious behaviour and contributing to investigations following cybersecurity incidents.

Control: ISM-0843; Revision: 9; Updated: Sep-21; Applicable: NC, OS, P, S, TS; Essential 8: ML1, ML2, ML3
Application control is implemented on workstations.

Control: ISM-1490; Revision: 3; Updated: Sep-21; Applicable: NC, OS, P, S, TS; Essential 8: ML2, ML3
Application control is implemented on internet-facing servers.

Control: ISM-1656; Revision: 0; Updated: Sep-21; Applicable: NC, OS, P, S, TS; Essential 8: ML3
Application control is implemented on non-internet-facing servers.

Control: ISM-1870; Revision: 0; Updated: Sep-23; Applicable: NC, OS, P, S, TS; Essential 8: ML1, ML2, ML3
Application control is applied to user profiles and temporary folders used by operating systems, web browsers and email clients.

Control: ISM-1871; Revision: 0; Updated: Sep-23; Applicable: NC, OS, P, S, TS; Essential 8: ML2, ML3
Application control is applied to all locations other than user profiles and temporary folders used by operating systems, web browsers and email clients.

Control: ISM-1657; Revision: 1; Updated: Sep-25; Applicable: NC, OS, P, S, TS; Essential 8: ML1, ML2, ML3
Application control restricts the execution of executables, libraries, scripts, installers, compiled HTML, HTML applications and control panel applets to an organisation-approved set.

Control: ISM-1658; Revision: 0; Updated: Sep-21; Applicable: NC, OS, P, S, TS; Essential 8: ML3
Application control restricts the execution of drivers to an organisation-approved set.

Control: ISM-0955; Revision: 6; Updated: Apr-20; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Application control is implemented using cryptographic hash rules, publisher certificate rules or path rules.

Control: ISM-1471; Revision: 3; Updated: Jun-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
When implementing application control using publisher certificate rules, publisher names and product names are used.

Control: ISM-1392; Revision: 4; Updated: Mar-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
When implementing application control using path rules, only approved users can modify approved files and write to approved folders.

Control: ISM-1746; Revision: 1; Updated: Mar-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
When implementing application control using path rules, only approved users can change file system permissions for approved files and folders.

Control: ISM-1544; Revision: 3; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: ML2, ML3
Microsoft's recommended application blocklist is implemented.

Control: ISM-1659; Revision: 1; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: ML3
Microsoft's vulnerable driver blocklist is implemented.

Control: ISM-1582; Revision: 1; Updated: Sep-21; Applicable: NC, OS, P, S, TS; Essential 8: ML2, ML3
Application control rulesets are validated on an annual or more frequent basis.

Control: ISM-0846; Revision: 8; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
All users (with the exception of local administrator accounts and break glass accounts) cannot disable, bypass or be exempted from application control.

Control: ISM-1660; Revision: 2; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: ML2, ML3
Allowed and blocked application control events are centrally logged.

Command Shell

The Command shell was the first shell developed by Microsoft to assist with the automation of routine system administration tasks, such as running Windows Commands via batch scripts. However, the Command shell can also be used by malicious actors to run Windows Commands on compromised systems. As such, centrally logging and analysing command line process creation events can assist in monitoring the security posture of systems, detecting malicious behaviour and contributing to investigations following cybersecurity incidents.

Control: ISM-1889; Revision: 0; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: ML2, ML3
Command line process creation events are centrally logged.

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 malicious actors.

In order to prevent attacks leveraging 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, centrally logging and analysing PowerShell events can assist in monitoring the security posture of systems, detecting malicious behaviour and contributing to investigations following cybersecurity incidents.

Control: ISM-1621; Revision: 1; Updated: Sep-21; Applicable: NC, OS, P, S, TS; Essential 8: ML3
Windows PowerShell 2.0 is disabled or removed.

Control: ISM-1622; Revision: 0; Updated: Oct-20; Applicable: NC, OS, P, S, TS; Essential 8: ML3
PowerShell is configured to use Constrained Language Mode.

Control: ISM-1623; Revision: 1; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: ML2, ML3
PowerShell module logging, script block logging and transcription events are centrally logged.

Control: ISM-1624; Revision: 0; Updated: Oct-20; Applicable: NC, OS, P, S, TS; Essential 8: N/A
PowerShell script block logs are protected by Protected Event Logging functionality.

Host-based intrusion detection and response solution

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, malicious actors can easily create variants of known malicious code in order to bypass traditional signature-based detection. A Host-based Intrusion Prevention System (HIPS) or Endpoint Detection and Response (EDR) solution 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 either a HIPS or EDR solution is implemented on workstations, critical servers and high-value servers.

Control: ISM-1341; Revision: 3; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
A HIPS or EDR solution is implemented on workstations.

Control: ISM-1034; Revision: 8; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
A HIPS or EDR solution 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 malicious actors 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.

Control: ISM-1416; Revision: 3; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: 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 application

When vendors develop operating systems and applications, they may make coding mistakes that lead to vulnerabilities. Malicious actors can take advantage of this by developing malicious code to exploit any vulnerabilities that have not been detected and remedied by vendors. As significant time and effort is often involved in developing functioning and reliable exploits, malicious actors 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 an antivirus application in place.

Control: ISM-1417; Revision: 5; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
An antivirus application 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

A device access control application, or disabling external communication interfaces, can be used to prevent removable media and mobile devices from being connected to workstations and servers via external communication interfaces. This can assist in preventing the introduction of malicious code or the exfiltration of data by malicious actors.

In addition, malicious actors can connect to locked workstations and servers via external communication interfaces that allow Direct Memory Access (DMA). In doing so, malicious actors 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.

Control: ISM-1418; Revision: 5; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
If there is no business requirement for reading from removable media and devices, such functionality is disabled via the use of a device access control application or by disabling external communication interfaces.

Control: ISM-0343; Revision: 7; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
If there is no business requirement for writing to removable media and devices, such functionality is disabled via the use of a device access control application or by disabling external communication interfaces.

Control: ISM-0345; Revision: 6; Updated: Dec-21; Applicable: NC, OS, P, S, TS; Essential 8: N/A
External communication interfaces that allow DMA are disabled.

Operating system event logging

Centrally logging and analysing security-relevant events, including configuration changes, for operating systems can assist in monitoring the security posture of systems, detecting malicious behaviour and contributing to investigations following cybersecurity incidents.

Typical security-relevant events for operating systems that can be logged include:

- changes to security policies
- failed user logons and account lockouts
- failures, restarts and changes to important processes, services and scheduled tasks
- operating system and application crashes and error messages
- security product-related events
- successful process creations and terminations
- successful user logons and logoffs
- system startups and shutdowns.

Control: ISM-1976; Revision: 0; Updated: Dec-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Security-relevant events for Apple macOS operating systems are centrally logged.

Control: ISM-1977; Revision: 0; Updated: Dec-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Security-relevant events for Linux operating systems are centrally logged.

Control: ISM-0582; Revision: 10; Updated: Dec-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Security-relevant events for Microsoft Windows operating systems are centrally logged.

Further information

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

Further information on vendors that have made a pledge to implement Secure by Design and Secure by Default principles and practices can be found on the United States' Cybersecurity & Infrastructure Security Agency's Secure by Design Pledge website.

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 hardening Microsoft Windows operating systems can be found in ASD's *Hardening Microsoft Windows 10 workstations* and *Hardening Microsoft Windows 11 workstations* publications.

Further information on hardening Microsoft Windows operating systems can also be found in Microsoft's *Windows 11 Security Book* and on the Microsoft Security Baselines Blog website.

Further information on hardening Linux workstations and servers can be found in ASD'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 ASD's *Implementing application control* publication.

Further information on Microsoft's recommended application blocklist and vulnerable driver blocklist are available from Microsoft.

Further information on command line process logging is available from Microsoft.

Further information on the use of PowerShell can be found in ASD's *Securing PowerShell in the enterprise* publication.

Further information on the use of PowerShell by blue teams is available from Microsoft.

Further information on obtaining greater visibility through PowerShell logging is available from Google.

Further information on independent testing of security products' ability to detect or prevent various stages of network intrusions is available from MITRE.

Further information on independent testing of antivirus applications 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*.

Further information on security-relevant events to monitor for Apple macOS, Linux and Microsoft Windows operating systems can be found in the following ASD publications:

- *Hardening Microsoft Windows 10 workstations*
- *Hardening Microsoft Windows 11 workstations*
- *Priority logs for SIEM ingestion: Practitioner guidance*
- *Windows event logging and forwarding*.

User application hardening

User applications

This section is applicable to user applications typically installed on user workstations, such as office productivity suites, web browsers and their extensions, email clients, Portable Document Format (PDF) applications, and security products (e.g. antivirus applications, device access control applications, HIPS and software firewalls). Information on server applications can be found in the server application hardening section of these guidelines.

User application selection

When selecting user applications, it is important that an organisation preferences vendors that have demonstrated a commitment to Secure by Design and Secure by Default principles and practices, including secure programming practices and either memory-safe programming languages (such as C#, Go, Java, Ruby, Rust and Swift) or less preferably memory-safe programming practices. This will assist not only with reducing the potential number of vulnerabilities in user applications, but also increasing the likelihood that timely patches, updates or vendor mitigations will be released to remediate any vulnerabilities that are found.

Control: ISM-0938; Revision: 7; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Vendors that have demonstrated a commitment to Secure by Design and Secure by Default principles and practices, including secure programming practices and either memory-safe programming languages or less preferably memory-safe programming practices, are used for user applications.

User application releases

Newer releases of user applications often introduce improvements in security functionality. This can make it more difficult for malicious actors to craft reliable exploits for vulnerabilities they discover. Using older releases of user applications, especially those no longer supported by vendors, may expose an organisation to vulnerabilities or exploitation techniques that have since been mitigated. This is particularly important for office productivity suites, web browsers and their extensions, email clients, PDF applications, and security products.

Control: ISM-1467; Revision: 4; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The latest release of office productivity suites, web browsers and their extensions, email clients, PDF applications, and security products are used.

Hardening user application configurations

When user applications are deployed in their default state, or with an unapproved configuration, it can lead to an insecure operating environment that may allow malicious actors to gain an initial foothold on

networks. This can be especially risky for office productivity suites, web browsers and their extensions, email clients, PDF applications, and security products as such applications are routinely targeted for exploitation. Many settings exist within such applications to allow them to be configured in an approved secure state in order to minimise this security risk. As such, ASD and vendors often produce hardening guidance to assist in hardening the configuration of these applications. Note, however, in situations where ASD and vendor hardening guidance conflicts, precedence should be given to implementing the most restrictive guidance.

Control: ISM-1915; Revision: 0; Updated: Mar-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Approved configurations for user applications are developed, implemented and maintained.

Control: ISM-1806; Revision: 4; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Default user accounts or credentials for user applications, including for any pre-configured user accounts, are changed, disabled or removed during initial setup.

Control: ISM-1470; Revision: 6; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Unneeded components, services and functionality of office productivity suites, web browsers, email clients, PDF applications and security products are disabled or removed.

Control: ISM-1235; Revision: 5; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Add-ons, extensions and plug-ins for office productivity suites, web browsers, email clients, PDF applications and security products are restricted to an organisation-approved set.

Control: ISM-1667; Revision: 0; Updated: Sep-21; Applicable: NC, OS, P, S, TS; Essential 8: ML2, ML3
Microsoft Office is blocked from creating child processes.

Control: ISM-1668; Revision: 0; Updated: Sep-21; Applicable: NC, OS, P, S, TS; Essential 8: ML2, ML3
Microsoft Office is blocked from creating executable content.

Control: ISM-1669; Revision: 0; Updated: Sep-21; Applicable: NC, OS, P, S, TS; Essential 8: ML2, ML3
Microsoft Office is blocked from injecting code into other processes.

Control: ISM-1542; Revision: 0; Updated: Jan-19; Applicable: NC, OS, P, S, TS; Essential 8: ML2, ML3
Microsoft Office is configured to prevent activation of Object Linking and Embedding packages.

Control: ISM-1859; Revision: 2; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: ML2, ML3
Office productivity suites are hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur.

Control: ISM-1823; Revision: 0; Updated: Mar-23; Applicable: NC, OS, P, S, TS; Essential 8: ML2, ML3
Office productivity suite security settings cannot be changed by users.

Control: ISM-1486; Revision: 1; Updated: Sep-21; Applicable: NC, OS, P, S, TS; Essential 8: ML1, ML2, ML3
Web browsers do not process Java from the internet.

Control: ISM-1485; Revision: 1; Updated: Sep-21; Applicable: NC, OS, P, S, TS; Essential 8: ML1, ML2, ML3
Web browsers do not process web advertisements from the internet.

Control: ISM-1412; Revision: 6; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: ML2, ML3
Web browsers are hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur.

Control: ISM-1585; Revision: 2; Updated: Mar-23; Applicable: NC, OS, P, S, TS; Essential 8: ML1, ML2, ML3
Web browser security settings cannot be changed by users.

Control: ISM-1670; Revision: 1; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: ML2, ML3
PDF applications are blocked from creating child processes.

Control: ISM-1860; Revision: 3; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: ML2, ML3
PDF applications are hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur.

Control: ISM-1824; Revision: 1; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: ML2, ML3
PDF application security settings cannot be changed by users.

Control: ISM-1601; Revision: 1; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Microsoft's attack surface reduction rules are implemented.

Control: ISM-1748; Revision: 1; Updated: Mar-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Email client security settings cannot be changed by users.

Control: ISM-1825; Revision: 0; Updated: Mar-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
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, malicious actors 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.

Control: ISM-1671; Revision: 0; Updated: Sep-21; Applicable: NC, OS, P, S, TS; Essential 8: ML1, ML2, ML3
Microsoft Office macros are disabled for users that do not have a demonstrated business requirement.

Control: ISM-1488; Revision: 1; Updated: Sep-21; Applicable: NC, OS, P, S, TS; Essential 8: ML1, ML2, ML3
Microsoft Office macros in files originating from the internet are blocked.

Control: ISM-1672; Revision: 0; Updated: Sep-21; Applicable: NC, OS, P, S, TS; Essential 8: ML1, ML2, ML3
Microsoft Office macro antivirus scanning is enabled.

Control: ISM-1673; Revision: 0; Updated: Sep-21; Applicable: NC, OS, P, S, TS; Essential 8: ML2, ML3
Microsoft Office macros are blocked from making Win32 API calls.

Control: ISM-1674; Revision: 0; Updated: Sep-21; Applicable: NC, OS, P, S, TS; Essential 8: 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.

Control: ISM-1890; Revision: 0; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: ML3
Microsoft Office macros are checked to ensure they are free of malicious code before being digitally signed or placed within Trusted Locations.

Control: ISM-1487; Revision: 2; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: ML3
Only privileged users responsible for checking that Microsoft Office macros are free of malicious code can write to and modify content within Trusted Locations.

Control: ISM-1675; Revision: 0; Updated: Sep-21; Applicable: NC, OS, P, S, TS; Essential 8: ML3
Microsoft Office macros digitally signed by an untrusted publisher cannot be enabled via the Message Bar or Backstage View.

Control: ISM-1891; Revision: 0; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: ML3
Microsoft Office macros digitally signed by signatures other than V3 signatures cannot be enabled via the Message Bar or Backstage View.

Control: ISM-1676; Revision: 0; Updated: Sep-21; Applicable: NC, OS, P, S, TS; Essential 8: ML3
Microsoft Office's list of trusted publishers is validated on an annual or more frequent basis.

Control: ISM-1489; Revision: 0; Updated: Sep-18; Applicable: NC, OS, P, S, TS; Essential 8: ML1, ML2, ML3
Microsoft Office macro security settings cannot be changed by users.

Further information

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

Further information on vendors that have made a pledge to implement Secure by Design and Secure by Default principles and practices can be found on the United States' Cybersecurity & Infrastructure Security Agency's Secure by Design Pledge website.

Further information on patching or updating user applications can be found in the system patching section of the *Guidelines for system management*.

Further information on the implementation and configuration of security products can be found in the operating system hardening section of these guidelines.

Further information on hardening Microsoft Office can be found in ASD's *Hardening Microsoft 365, Office 2021, Office 2019 and Office 2016* publication.

Further information on hardening Microsoft Office can also be found on the Microsoft Security Baselines Blog website.

Further information on hardening Microsoft Edge can be found on the Microsoft Security Baselines Blog website.

Further information on hardening Google Chrome can be found in Google's *Chrome Browser Enterprise Security Configuration Guide (Windows)*.

Further information on hardening Adobe Reader and Adobe Acrobat can be found in Adobe's *Security Configuration Guide for Acrobat* publication.

Further information on Microsoft's attack surface reduction rules can be found on Microsoft's attack surface reduction rules overview website.

Further information on configuring Microsoft Office macro settings can be found in ASD's *Restricting Microsoft Office macros* publication.

Server application hardening

Server applications

This section is applicable to server applications associated with specific server functionality, such as Microsoft Active Directory services, database management system applications, email server applications and web hosting applications. Information on user applications can be found in the user application hardening section of these guidelines.

Server application selection

When selecting server applications, it is important that an organisation preferences vendors that have demonstrated a commitment to Secure by Design and Secure by Default principles and practices, including secure programming practices and either memory-safe programming languages (such as C#, Go, Java, Ruby, Rust and Swift) or less preferably memory-safe programming practices. This will assist not only with reducing the potential number of vulnerabilities in server applications, but also increasing the likelihood that timely patches, updates or vendor mitigations will be released to remediate any vulnerabilities that are found.

Control: ISM-1826; Revision: 1; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Vendors that have demonstrated a commitment to Secure by Design and Secure by Default principles and practices, including secure programming practices and either memory-safe programming languages or less preferably memory-safe programming practices, are used for server applications.

Server application releases

Newer releases of server applications often introduce improvements in security functionality. This can make it more difficult for malicious actors to craft reliable exploits for vulnerabilities they discover. Using older releases of server applications, especially those no longer supported by vendors, may expose an organisation to vulnerabilities or exploitation techniques that have since been mitigated. This is particularly important for internet-facing server applications, such as web hosting applications.

Control: ISM-1483; Revision: 2; Updated: Mar-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The latest release of internet-facing server applications are used.

Hardening server application configurations

When server applications are deployed in their default state, or with an unapproved configuration, it can lead to an insecure operating environment that may allow malicious actors to gain an initial foothold on networks. This can be especially risky for server applications as such applications are routinely targeted for exploitation. Many settings exist within server applications to allow them to be configured in an approved secure state in order to minimise this security risk. As such, ASD and vendors often produce hardening guidance to assist in hardening the configuration of server applications. Note, however, in situations where ASD and vendor hardening guidance conflicts, precedence should be given to implementing the most restrictive guidance.

Control: ISM-1916; Revision: 0; Updated: Mar-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Approved configurations for server applications are developed, implemented and maintained.

Control: ISM-1246; Revision: 6; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Server applications are hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur.

Control: ISM-1260; Revision: 7; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Default user accounts or credentials for server applications, including for any pre-configured user accounts, are changed, disabled or removed during initial setup.

Control: ISM-1247; Revision: 5; Updated: Dec-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Unneeded user accounts, components, services and functionality of server applications are disabled or removed.

Control: ISM-1245; Revision: 3; Updated: Mar-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
All temporary installation files and logs created during server application installation processes are removed after server applications have been installed.

Restricting privileges for server applications

If a server application operating as a local administrator or root account is compromised by malicious actors, it can present a significant security risk to the underlying server. In addition, server applications by default are often capable of widely accessing their underlying server's file system. Therefore, restricting the ability of server applications to access their underlying server's file system can limit damage should malicious actors compromise the server application.

Control: ISM-1249; Revision: 4; Updated: Dec-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Server applications are configured to run as a separate user account with the minimum privileges needed to perform their functions.

Control: ISM-1250; Revision: 3; Updated: Dec-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The user accounts under which server applications run have limited access to their underlying server's file system.

Microsoft Active Directory services

Due to the critical role that Microsoft Active Directory services perform for domain services, certification services, federated services and identity services within networks, it is crucial that servers performing these services are hardened and access to them is strictly limited, including to their backups. Specifically, this includes servers for Microsoft Active Directory Domain Services (AD DS), Microsoft Active Directory Certificate Services (AD CS), Microsoft Active Directory Federation Services (AD FS) and Microsoft Entra Connect.

In addition, centrally logging and analysing security-relevant events, including configuration changes, for Microsoft Active Directory services can assist in monitoring the security posture of systems, detecting malicious behaviour and contributing to investigations following cybersecurity incidents.

Control: ISM-1926; Revision: 0; Updated: Sep-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Microsoft AD DS domain controllers, Microsoft AD CS CA servers, Microsoft AD FS servers and Microsoft Entra Connect servers are only used for their designed role and no other applications or services are installed, unless they are security related.

Control: ISM-1927; Revision: 0; Updated: Sep-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Access to Microsoft AD DS domain controllers, Microsoft AD CS CA servers, Microsoft AD FS servers and Microsoft Entra Connect servers is limited to privileged users that require access.

Control: ISM-1928; Revision: 0; Updated: Sep-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Backups of Microsoft AD DS domain controllers, Microsoft AD CS CA servers, Microsoft AD FS servers and Microsoft Entra Connect servers are encrypted, stored securely and only accessible to backup administrator accounts.

Control: ISM-1830; Revision: 2; Updated: Sep-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Security-relevant events for Microsoft AD DS domain controllers, Microsoft AD CS CA servers, Microsoft AD FS servers and Microsoft Entra Connect servers are centrally logged.

Microsoft Active Directory Domain Services domain controllers

Microsoft AD DS domain controllers hold sensitive data for systems, such as hashed credentials for all user accounts. As such, particular care should be taken to secure these servers. This can be achieved by hardening their configuration while using dedicated domain administrator user accounts exclusively for their administration. In doing so, technical controls should ensure these dedicated domain administrator user accounts cannot be used to connect to or administer other systems.

Control: ISM-1827; Revision: 0; Updated: Mar-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Microsoft AD DS domain controllers are administered using dedicated domain administrator user accounts that are not used to administer other systems.

Control: ISM-1929; Revision: 0; Updated: Sep-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Lightweight Directory Access Protocol signing is enabled on Microsoft AD DS domain controllers.

Control: ISM-1828; Revision: 0; Updated: Mar-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The Print Spooler service is disabled on Microsoft AD DS domain controllers.

Control: ISM-1829; Revision: 1; Updated: Sep-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Passwords are not stored in Group Policy Preferences.

Control: ISM-1930; Revision: 0; Updated: Sep-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Passwords are prevented from being stored in Group Policy Preferences.

Control: ISM-1931; Revision: 0; Updated: Sep-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
SID Filtering is enabled for domain and forest trusts.

Microsoft Active Directory Domain Services account hardening

Misconfigured user accounts and computer accounts within Microsoft AD DS can pose a significant threat to the security of a system. For example, when malicious actors are able to obtain credentials for a user account, along with associated system access, they may further compromise the system by querying Microsoft AD DS in order to assist with gaining an understanding of the environment, moving laterally through the network and escalating privileges by compromising privileged user accounts. Furthermore, malicious actors with this level of access can become difficult to detect and remove, as they may not need to use exploits for vulnerabilities to achieve their goals. Malicious activities performed by compromised user accounts or computer accounts may also appear very similar to legitimate system activities.

Control: ISM-1832; Revision: 0; Updated: Mar-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Only service accounts and computer accounts are configured with Service Principal Names (SPNs).

Control: ISM-1932; Revision: 0; Updated: Sep-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The number of service accounts configured with an SPN is minimised.

Control: ISM-1933; Revision: 0; Updated: Sep-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Service accounts configured with an SPN do not have DCSync permissions.

Control: ISM-2010; Revision: 0; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Service accounts configured with an SPN use the Advanced Encryption Standard for encryption.

Control: ISM-1834; Revision: 0; Updated: Mar-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Duplicate SPNs do not exist within the domain.

Control: ISM-1833; Revision: 1; Updated: Sep-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
User accounts are provisioned with the minimum privileges required.

Control: ISM-1934; Revision: 0; Updated: Sep-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
User accounts with DCSync permissions are reviewed at least annually, and those without an ongoing requirement for the permissions have them removed.

Control: ISM-1835; Revision: 0; Updated: Mar-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Privileged user accounts are configured as sensitive and cannot be delegated.

Control: ISM-1935; Revision: 0; Updated: Sep-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Computer accounts are not configured for unconstrained delegation.

Control: ISM-1836; Revision: 0; Updated: Mar-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
User accounts require Kerberos pre-authentication.

Control: ISM-1837; Revision: 0; Updated: Mar-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
User accounts are not configured with password never expires or password not required.

Control: ISM-1838; Revision: 0; Updated: Mar-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The UserPassword attribute for user accounts is not used.

Control: ISM-1936; Revision: 0; Updated: Sep-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The sIDHistory attribute for user accounts is not used.

Control: ISM-1937; Revision: 0; Updated: Sep-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
User accounts are checked at least weekly for the presence of the sIDHistory attribute.

Control: ISM-1839; Revision: 0; Updated: Mar-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Account properties accessible by unprivileged users are not used to store passwords.

Control: ISM-1840; Revision: 0; Updated: Mar-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
User account passwords do not use reversible encryption.

Control: ISM-1841; Revision: 0; Updated: Mar-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Unprivileged user accounts cannot add machines to the domain.

Control: ISM-1842; Revision: 1; Updated: Sep-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Dedicated privileged service accounts are used to add machines to the domain.

Control: ISM-1843; Revision: 1; Updated: Sep-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
User accounts with unconstrained delegation are reviewed at least annually, and those without an SPN or demonstrated business requirement are removed.

Control: ISM-1844; Revision: 0; Updated: Mar-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Computer accounts that are not Microsoft AD DS domain controllers are not trusted for delegation to services.

Control: ISM-1938; Revision: 0; Updated: Sep-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The Domain Computers security group does not have write or modify permissions to any Microsoft Active Directory objects.

Microsoft Active Directory Domain Services security group memberships

Microsoft AD DS contains a number of built-in security groups that have elevated permissions or deliberately relaxed security policies. These security groups are often required for a specific purpose, however, overuse or inappropriate use may allow malicious actors to more easily move laterally throughout a network or escalate their privileges. Highly-privileged security groups in particular, such as the Domain Admins and Enterprise Admins security groups, should have their membership limited to the smallest set of possible user accounts to limit malicious actors' opportunities for privilege escalation. In doing so, such highly-privileged security groups should exclude service accounts and computer accounts. In addition, the Domain Computers security group should be excluded from belonging to any privileged or highly-privileged security groups.

Control: ISM-1620; Revision: 1; Updated: Mar-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Privileged user accounts are members of the Protected Users security group.

Control: ISM-1939; Revision: 0; Updated: Sep-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The number of user accounts that are members of the Domain Admins, Enterprise Admins or other highly-privileged security groups is minimised.

Control: ISM-1940; Revision: 0; Updated: Sep-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Service accounts are not members of the Domain Admins, Enterprise Admins or other highly-privileged security groups.

Control: ISM-1941; Revision: 0; Updated: Sep-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Computer accounts are not members of the Domain Admins, Enterprise Admins or other highly-privileged security groups.

Control: ISM-1942; Revision: 0; Updated: Sep-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The Domain Computers security group is not a member of any privileged or highly-privileged security groups.

Control: ISM-1845; Revision: 0; Updated: Mar-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
When a user account is disabled, it is removed from all security group memberships.

Control: ISM-1846; Revision: 0; Updated: Mar-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The Pre-Windows 2000 Compatible Access security group does not contain user accounts.

Microsoft Active Directory Certificate Services

Microsoft AD CS is responsible for the management of Public Key Infrastructure certificates used to secure authentication and communication protocols for systems. As such, particular care should be taken to secure servers that perform this role, such as Certification Authorities (CAs).

Control: ISM-1943; Revision: 0; Updated: Sep-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Strong mapping between certificates and users is enforced.

Control: ISM-1944; Revision: 0; Updated: Sep-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The EDITF_ATTRIBUTESUBJECTALTNAME2 flag is removed from Microsoft AD CS CA configurations.

Control: ISM-1945; Revision: 0; Updated: Sep-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT flag is removed from certificate templates.

Control: ISM-1946; Revision: 0; Updated: Sep-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Unprivileged user accounts do not have write access to certificate templates.

Control: ISM-1947; Revision: 0; Updated: Sep-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Extended Key Usages that enable user authentication are removed.

Control: ISM-1948; Revision: 0; Updated: Sep-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
CA Certificate Manager approval is required for certificate templates that allow a Subject Alternative Name to be supplied.

Microsoft Active Directory Federation Services

Microsoft AD FS is responsible for the sharing of identity and access management rights across security boundaries. As such, particular care should be taken to secure servers that perform this role.

Control: ISM-1949; Revision: 0; Updated: Sep-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Microsoft AD FS servers are administered using a dedicated service account that is not used to administer other systems.

Microsoft Entra Connect

Microsoft Entra Connect is responsible for synchronising identity information between Microsoft AD DS and Microsoft Entra ID services within hybrid on-premises and cloud-based environments. As such, particular care should be taken to secure servers that perform this role.

Control: ISM-1950; Revision: 0; Updated: Sep-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Soft matching between Microsoft AD DS and Microsoft Entra ID is disabled following initial synchronisation activities.

Control: ISM-1951; Revision: 0; Updated: Sep-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Hard match takeover is disabled for Microsoft Entra Connect servers.

Control: ISM-1952; Revision: 0; Updated: Sep-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Privileged user accounts are not synchronised between Microsoft AD DS and Microsoft Entra ID.

Server application event logging

Centrally logging and analysing security-relevant events, including configuration changes, for server applications can assist in monitoring the security posture of systems, detecting malicious behaviour and contributing to investigations following cybersecurity incidents.

Control: ISM-1978; Revision: 0; Updated: Dec-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Security-relevant events for server applications on internet-facing servers are centrally logged.

Control: ISM-1979; Revision: 0; Updated: Dec-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Security-relevant events for server applications on non-internet-facing servers are centrally logged.

Further information

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

Further information on vendors that have made a pledge to implement Secure by Design and Secure by Default principles and practices can be found on the United States' Cybersecurity & Infrastructure Security Agency's Secure by Design Pledge website.

Further information on patching or updating server applications can be found in the system patching section of the *Guidelines for system management*.

Further information on the use of privileged user accounts can be found in the access to systems and their resources section of the *Guidelines for personnel security*.

Further information on administering Microsoft Active Directory services can be found in the system administration section of the *Guidelines for system management*.

Further information on hardening Microsoft Active Directory services can be found in ASD's *Detecting and mitigating Active Directory compromises* publication.

Further information on hardening Microsoft Active Directory services can also be found in Microsoft's *Best practices for securing Active Directory* publication.

Further information on hardening Microsoft Entra Connect can be found in Microsoft's *Prerequisites for Microsoft Entra Connect* 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 security-relevant events to monitor for Microsoft Active Directory can be found in ASD's *Detecting and mitigating Active Directory compromises* and *Priority logs for SIEM ingestion: Practitioner guidance* publications.

Further information on security-relevant events to monitor for Microsoft Active Directory can also be found in Microsoft's *Events to monitor* publication.

Further information on database servers can be found in the database servers section of the *Guidelines for database systems*.

Further information on email servers can be found in the email gateways and servers section of the *Guidelines for email*.

Authentication hardening

User accounts and authentication types

The guidance within this section is equally applicable to all user accounts unless specified otherwise. This includes unprivileged user accounts and privileged user accounts, which includes 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 less preferably via single-factor authentication, such as a username and a passphrase.

Control: ISM-1546; Revision: 0; Updated: Aug-19; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Users are authenticated before they are granted access to a system and its resources.

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.

Control: ISM-1603; Revision: 0; Updated: Aug-20; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Authentication methods susceptible to replay attacks are disabled.

Control: ISM-1055; Revision: 4; Updated: Oct-20; Applicable: NC, OS, P, S, TS; Essential 8: N/A
LAN Manager and NT LAN Manager authentication methods are disabled.

Multi-factor authentication

Multi-factor authentication uses two or more different authentication factors. This may include:

- something users know, such as a memorised secret (i.e. personal identification number, password or passphrase)
- something users have, such as a security key, smart card, passkey, smartphone or one-time password token
- something users are, such as a fingerprint pattern or their facial geometry.

Users of online services, privileged users of systems and users with access to data repositories are more likely to be targeted by malicious actors due to their access. For this reason, it is especially important that multi-factor authentication is used for these user 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 malicious actors' 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 users have should be used with something users know. Alternatively, something users have that is unlocked by something users know or are (often known as passwordless multi-factor authentication) can be used. Furthermore, for increased security, the use of phishing-resistant multi-factor authentication is recommended to protect against real-time phishing attacks.

Finally, centrally logging and analysing multi-factor authentication events can assist in monitoring the security posture of systems, detecting malicious behaviour and contributing to investigations following cybersecurity incidents.

Control: ISM-1504; Revision: 3; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: ML1, ML2, ML3
Multi-factor authentication is used to authenticate users to their organisation's online services that process, store or communicate their organisation's sensitive data.

Control: ISM-1679; Revision: 1; Updated: Sep-23; Applicable: NC, OS, P, S, TS; Essential 8: ML1, ML2, ML3
Multi-factor authentication is used to authenticate users to third-party online services that process, store or communicate their organisation's sensitive data.

Control: ISM-1680; Revision: 1; Updated: Sep-23; Applicable: NC, OS, P, S, TS; Essential 8: ML1, ML2, ML3
Multi-factor authentication (where available) is used to authenticate users to third-party online services that process, store or communicate their organisation's non-sensitive data.

Control: ISM-1892; Revision: 0; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: ML1, ML2, ML3
Multi-factor authentication is used to authenticate users to their organisation's online customer services that process, store or communicate their organisation's sensitive customer data.

Control: ISM-1893; Revision: 0; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: ML1, ML2, ML3
Multi-factor authentication is used to authenticate users to third-party online customer services that process, store or communicate their organisation's sensitive customer data.

Control: ISM-1681; Revision: 3; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: ML1, ML2, ML3
Multi-factor authentication is used to authenticate customers to online customer services that process, store or communicate sensitive customer data.

Control: ISM-1919; Revision: 0; Updated: Jun-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
When multi-factor authentication is used to authenticate users or customers to online services or online customer services, all other authentication protocols that do not support multi-factor authentication are disabled.

Control: ISM-1173; Revision: 4; Updated: Sep-21; Applicable: NC, OS, P, S, TS; Essential 8: ML2, ML3
Multi-factor authentication is used to authenticate privileged users of systems.

Control: ISM-0974; Revision: 6; Updated: Sep-21; Applicable: NC, OS, P, S, TS; Essential 8: ML2, ML3
Multi-factor authentication is used to authenticate unprivileged users of systems.

Control: ISM-1505; Revision: 3; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: ML3
Multi-factor authentication is used to authenticate users of data repositories.

Control: ISM-1401; Revision: 5; Updated: Sep-21; Applicable: NC, OS, P, S, TS; Essential 8: ML1, 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.

Control: ISM-1872; Revision: 1; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: ML2, ML3
Multi-factor authentication used for authenticating users of online services is phishing-resistant.

Control: ISM-1873; Revision: 1; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: ML2
Multi-factor authentication used for authenticating customers of online customer services provides a phishing-resistant option.

Control: ISM-1874; Revision: 1; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: ML3
Multi-factor authentication used for authenticating customers of online customer services is phishing-resistant.

Control: ISM-1682; Revision: 3; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: ML2, ML3
Multi-factor authentication used for authenticating users of systems is phishing-resistant.

Control: ISM-1894; Revision: 0; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: ML3
Multi-factor authentication used for authenticating users of data repositories is phishing-resistant.

Control: ISM-1559; Revision: 3; Updated: Dec-24; Applicable: NC, OS, P; Essential 8: N/A
Memorised secrets used for multi-factor authentication on non-classified, OFFICIAL: Sensitive and PROTECTED systems are a minimum of 6 characters.

Control: ISM-1560; Revision: 2; Updated: Mar-22; Applicable: S; Essential 8: N/A
Memorised secrets used for multi-factor authentication on SECRET systems are a minimum of 8 characters.

Control: ISM-1561; Revision: 2; Updated: Mar-22; Applicable: TS; Essential 8: N/A
Memorised secrets used for multi-factor authentication on TOP SECRET systems are a minimum of 10 characters.

Control: ISM-2011; Revision: 0; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
When phishing-resistant multi-factor authentication is used by user accounts, other non-phishing-resistant multi-factor authentication options are disabled for such user accounts.

Control: ISM-1920; Revision: 0; Updated: Jun-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
When multi-factor authentication is used to authenticate users to online services, online customer services, systems or data repositories – that process, store or communicate their organisation's sensitive data or sensitive customer data – users are prevented from self-enrolling into multi-factor authentication from untrustworthy devices.

Control: ISM-1683; Revision: 2; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: ML2, ML3
Successful and unsuccessful multi-factor authentication events are centrally logged.

Single-factor authentication

A significant threat to the compromise of user accounts is credential cracking tools. When malicious actors gain 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 malicious actors 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 systems, 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 malicious actors 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 password complexity supported by a system will need to be implemented.

Finally, centrally logging and analysing single-factor authentication events can assist in monitoring the security posture of systems, detecting malicious behaviour and contributing to investigations following cybersecurity incidents.

Control: ISM-0417; Revision: 5; Updated: Oct-19; Applicable: NC, OS, P, S, TS; Essential 8: N/A
When systems cannot support multi-factor authentication, single-factor authentication using passphrases is implemented instead.

Control: ISM-0421; Revision: 10; Updated: Dec-24; Applicable: NC, OS, P; Essential 8: N/A
Passphrases used for single-factor authentication on non-classified, OFFICIAL: Sensitive and PROTECTED systems are at least 4 random words with a total minimum length of 15 characters.

Control: ISM-1557; Revision: 2; Updated: Dec-21; Applicable: S; Essential 8: 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.

Control: ISM-0422; Revision: 8; Updated: Dec-21; Applicable: TS; Essential 8: 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.

Control: ISM-1558; Revision: 2; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: 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.

Control: ISM-1895; Revision: 0; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Successful and unsuccessful single-factor authentication events are centrally logged.

Setting credentials for user accounts

Before credentials are set for user accounts, including setting credentials following any reset requests, it is important that users provide sufficient evidence to verify their identity, such as by physically presenting themselves and their pass to a service desk, answering a set of challenge-response questions, or by demonstrating control of a linked mobile device. 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.

Control: ISM-1593; Revision: 1; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Users provide sufficient evidence to verify their identity when requesting new credentials.

Control: ISM-1227; Revision: 5; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Credentials set for user accounts are randomly generated.

Control: ISM-1594; Revision: 1; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: 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.

Control: ISM-1595; Revision: 1; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Credentials provided to users are changed on first use.

Control: ISM-1596; Revision: 2; Updated: Dec-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Credentials, in the form of memorised secrets, are not reused by users across different systems.

Setting credentials for built-in Administrator accounts, break glass accounts, local administrator accounts and service accounts

When built-in Administrator accounts, break glass accounts, local administrator accounts and service accounts use common usernames or weak credentials, it may allow malicious actors that compromise credentials on one workstation or server to easily compromise other workstations and servers. As such, it is critical that credentials for the built-in Administrator account, break glass accounts, local administrator accounts and service accounts in each domain are long, unique, unpredictable and managed.

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 ensures that they are long, unique, unpredictable and managed. This ensures that service account credentials are secure, not misplaced or forgotten, and that they are automatically changed on a regular basis. However, in cases where the use of group Managed Service Accounts is not possible, credentials for service accounts should still be unique, unpredictable and random with a minimum length of 30 characters.

Control: ISM-1953; Revision: 0; Updated: Sep-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Credentials for the built-in Administrator account in each domain are long, unique, unpredictable and managed.

Control: ISM-1685; Revision: 2; Updated: Jun-23; Applicable: NC, OS, P, S, TS; Essential 8: ML2, ML3
Credentials for break glass accounts, local administrator accounts and service accounts are long, unique, unpredictable and managed.

Control: ISM-1795; Revision: 2; Updated: Sep-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Credentials for built-in Administrator accounts, break glass accounts, local administrator accounts and service accounts are a minimum of 30 characters.

Control: ISM-1954; Revision: 0; Updated: Sep-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Credentials for built-in Administrator accounts, break glass accounts, local administrator accounts and service accounts are randomly generated.

Control: ISM-1619; Revision: 0; Updated: Oct-20; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Service accounts are created as group Managed Service Accounts.

Changing credentials

Generally, credentials should not need to be changed on a frequent basis. However, some events may necessitate the requirement for individual user accounts, or groups of user accounts, to change their credentials. This can include credentials being compromised (such as appearing in an online data breach database), being suspected of being compromised (such as when malicious actors gain access to a network), being discovered stored on networks in the clear, being transferred across networks in the clear, when membership of shared user accounts change and if they have not been changed in the past 12 months.

Control: ISM-1590; Revision: 3; Updated: Sep-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Credentials for user accounts are changed if:

- *they are compromised*
- *they are suspected of being compromised*
- *they are discovered stored on networks in the clear*
- *they are discovered being transferred across networks in the clear*
- *membership of a shared user account changes*
- *they have not been changed in the past 12 months.*

Control: ISM-1955; Revision: 0; Updated: Sep-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Credentials for computer accounts are changed if:

- *they are compromised*
- *they are suspected of being compromised*
- *they have not been changed in the past 30 days.*

Control: ISM-1847; Revision: 0; Updated: Mar-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Credentials for the Kerberos Key Distribution Center's service account (KRBTGT) are changed twice, allowing for replication to all Microsoft AD DS domain controllers in-between each change, if:

- *the domain has been directly compromised*
- *the domain is suspected of being compromised*
- *they have not been changed in the past 12 months.*

Control: ISM-1956; Revision: 0; Updated: Sep-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Microsoft AD FS token-signing and encryption certificates are changed twice in quick succession if:

- *they are compromised*
- *they are suspected of being compromised*
- *they have not been changed in the past 12 months.*

Protecting credentials

Obscuring credentials as they are entered into systems can assist in protecting them against screen scrapers and shoulder surfers. In addition, physical credentials, such as written down credentials (e.g. memorised secrets) and dedicated devices that store or generate credentials (e.g. security keys, smart cards and one-time password tokens), when kept together with systems they are used to authenticate to, can increase the likelihood of malicious actors gaining unauthorised access to systems. For example, when smart cards are left on card readers, one-time password tokens are left in laptop computer bags, security keys are left connected to computers or passphrases are written down and stuck to computer monitors. To reduce this security risk, physical credentials should be keep separate from systems they are used to authenticate to, except for when performing authentication activities.

If storing credentials on systems, 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.

When using Microsoft Windows systems, memory integrity, Local Security Authority protection, Credential Guard and Remote Credential Guard functionality, all preferably with a Unified Extensible Firmware Interface (UEFI) lock, can be enabled to provide additional protection for credentials. In addition, malicious actors that have access to systems may attempt to steal cached credentials. To reduce this security risk, cached credentials should be limited to only one previous logon.

Finally, an organisation should regularly scan their systems to detect and remediate any credentials that are being stored in an unprotected manner, such as in the clear in documents, on network file shares or in other data repositories.

Control: ISM-1597; Revision: 0; Updated: Aug-20; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Credentials are obscured as they are entered into systems.

Control: ISM-1980; Revision: 0; Updated: Dec-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Credential hint functionality is not used for systems.

Control: ISM-0418; Revision: 7; Updated: Dec-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Physical credentials are kept separate from systems they are used to authenticate to, except for when performing authentication activities.

Control: ISM-1402; Revision: 6; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Credentials stored on systems are protected by a password manager; a hardware security module; or by salting, hashing and stretching them before storage within a database.

Control: ISM-1957; Revision: 0; Updated: Sep-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Private keys for Microsoft AD CS CA servers are protected by a hardware security module.

Control: ISM-1896; Revision: 0; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: ML3
Memory integrity functionality is enabled.

Control: ISM-1861; Revision: 2; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: ML3
Local Security Authority protection functionality is enabled.

Control: ISM-1686; Revision: 1; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: ML3
Credential Guard functionality is enabled.

Control: ISM-1897; Revision: 0; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: ML3
Remote Credential Guard functionality is enabled.

Control: ISM-1749; Revision: 0; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Cached credentials are limited to one previous logon.

Control: ISM-1875; Revision: 0; Updated: Sep-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Networks are scanned at least monthly to identify any credentials that are being stored in the clear.

User account lockouts

Locking a user account after a specified number of failed logon attempts reduces the likelihood of successful forms of brute-force attacks, such as credential guessing attacks, credential spraying attacks and credential stuffing attacks by malicious actors. 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 user accounts. Implementing multi-factor authentication is also an effective way of reducing the likelihood of successful credential spraying attacks.

Control: ISM-1403; Revision: 4; Updated: Dec-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
User accounts, except for break glass accounts, are locked out after a maximum of five failed logon attempts.

Session termination

Implementing measures to terminate user sessions and restart workstations on a daily basis, outside of business hours and after an appropriate period of inactivity, can assist in system maintenance activities and removing malicious actors that may have compromised a system but failed to gain persistence.

Control: ISM-0853; Revision: 3; Updated: Sep-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
On a daily basis, outside of business hours and after an appropriate period of inactivity, user sessions are terminated and workstations are restarted.

Session locking

Session locking prevents unauthorised access to services which a user has already authenticated to.

Control: ISM-0428; Revision: 10; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Services are configured with a session lock that:

- *activates after a maximum of 15 minutes of user inactivity, a maximum of 12 hours of overall session time or when manually activated by users*
- *blocks access to all session content*
- *requires users to re-authenticate using all authentication factors to unlock the session*
- *denies users the ability to disable the session locking mechanism.*

Screen locking

Screen locking prevents unauthorised access to a system which a user has already authenticated to.

Control: ISM-2012; Revision: 0; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Systems are configured with a screen lock that:

- *activates after a maximum of 15 minutes of user inactivity, or when manually activated by users*
- *conceals all content on the screen*
- *ensures that the screen does not enter a power saving state before the screen lock is activated*
- *requires users to re-authenticate using all authentication factors to unlock the system*
- *denies users the ability to disable the screen locking mechanism.*

Logon banner

Displaying a logon banner to users each time they logon to systems can act as a way of reminding users of their security responsibilities. Logon banners may cover topics such as:

- the sensitivity or classification of the system
- access requirements for the system
- usage policies for the system and its resources
- details of any monitoring activities for the system.

Control: ISM-0408; Revision: 5; Updated: Sep-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Systems have a logon banner that reminds users of their security responsibilities when accessing the system and its resources.

Further information

Further information on implementing multi-factor authentication can be found in ASD'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 how to secure group Managed Service Accounts in Microsoft Windows Server is available from Microsoft.

Further information on changing credentials for the Kerberos Key Distribution Center's service account can be found in Microsoft's *Active Directory accounts* and *Active Directory Forest Recovery - Reset the krbtgt password* publications. A script for changing credentials for this service account is also available from Microsoft.

Further information memory integrity functionality is available from Microsoft.

Further information on Local Security Authority protection functionality is available from Microsoft.

Further information on Credential Guard functionality and Remote Credential Guard functionality is available from Microsoft.

Virtualisation hardening

Hypervisors

This section is applicable to Type 1 hypervisors (those that run on bare metal) and Type 2 hypervisors (those that run on top of a general-purpose operating system). In doing so, Type 1 hypervisors should be treated as operating systems while Type 2 hypervisors should be treated as applications. Note, as Type 1 hypervisors are themselves lightweight operating systems, they can be treated as a combination of a software-based isolation mechanism and an underlying operating system. Conversely, Type 2 hypervisors will run on top of a general-purpose operating system that may be provided by a different vendor to that of the software-based isolation mechanism.

Containerisation

Containers allow for versatile deployment of systems and, in doing so, should be treated the same as any other system. However, 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.

Malicious actors who have compromised a single computing environment, or who legitimately control a single computing environment, might exploit a misconfiguration or 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 controls are implemented when a software-based isolation mechanism is used to share a physical server's hardware.

Control: ISM-1460; Revision: 5; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: 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 demonstrated a commitment to Secure by Design and Secure by Default principles and practices, including secure programming practices and either memory-safe programming languages or less preferably memory-safe programming practices.

Control: ISM-1604; Revision: 0; Updated: Aug-20; Applicable: NC, OS, P, S, TS; Essential 8: 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.

Control: ISM-1605; Revision: 1; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
When using a software-based isolation mechanism to share a physical server's hardware, the underlying operating system is hardened.

Control: ISM-1606; Revision: 2; Updated: Sep-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
When using a software-based isolation mechanism to share a physical server's hardware, patches, updates or vendor mitigations for vulnerabilities are applied to the isolation mechanism and underlying operating system in a timely manner.

Control: ISM-1848; Revision: 0; Updated: Mar-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
When using a software-based isolation mechanism to share a physical server's hardware, the isolation mechanism or underlying operating system is replaced when it is no longer supported by a vendor.

Control: ISM-1607; Revision: 1; Updated: Dec-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
When using a software-based isolation mechanism to share a physical server's hardware, integrity monitoring and centralised event logging is performed for the isolation mechanism and underlying operating system.

Control: ISM-1461; Revision: 5; Updated: Mar-22; Applicable: S, TS; Essential 8: 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 cyber supply chain risk management can be found in the cyber supply chain risk management section of the *Guidelines for procurement and outsourcing*.

Further information on vendors that have made a pledge to implement Secure by Design and Secure by Default principles and practices can be found on the United States' Cybersecurity & Infrastructure Security Agency's Secure by Design Pledge website.

Further information on the use of cloud services can be found in the managed services and cloud services section of the *Guidelines for procurement and 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 networked information technology (IT) equipment
- applying patches, updates or vendor mitigations to applications, drivers, operating systems or firmware
- installing or removing applications, operating systems, network devices or networked IT 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 cybersecurity documentation.

Control: ISM-0042; Revision: 6; Updated: Dec-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
System administration processes, and supporting system administration procedures, are developed, implemented and maintained.

Control: ISM-1211; Revision: 6; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
System administrators perform system administration activities in accordance with the system's change and configuration management plan.

Separate privileged operating environments

One of the greatest threats to the security of networks is the compromise of privileged user 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 user accounts to be compromised by malicious actors.

Using different physical workstations, with one being a dedicated Secure Admin Workstation, is the most secure approach to separating privileged and unprivileged operating environments for system administrators. However, a trusted and hardened virtualisation-based solution may be sufficient for separating privileged and unprivileged operating environments on the same Secure Admin Workstation. In such cases, privileged operating environments should not be virtualised within unprivileged operating environments.

Control: ISM-1898; Revision: 0; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: ML3
Secure Admin Workstations are used in the performance of administrative activities.

Control: ISM-1380; Revision: 5; Updated: Sep-21; Applicable: NC, OS, P, S, TS; Essential 8: ML1, ML2, ML3
Privileged users use separate privileged and unprivileged operating environments.

Control: ISM-1687; Revision: 0; Updated: Sep-21; Applicable: NC, OS, P, S, TS; Essential 8: ML2, ML3
Privileged operating environments are not virtualised within unprivileged operating environments.

Control: ISM-1688; Revision: 1; Updated: Sep-24; Applicable: NC, OS, P, S, TS; Essential 8: ML1, ML2, ML3
Unprivileged user accounts cannot logon to privileged operating environments.

Control: ISM-1689; Revision: 1; Updated: Sep-24; Applicable: NC, OS, P, S, TS; Essential 8: ML1, ML2, ML3
Privileged user accounts (excluding local administrator accounts) cannot logon to unprivileged operating environments.

Control: ISM-1958; Revision: 0; Updated: Sep-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
User accounts with DCSync permissions cannot logon to unprivileged operating environments.

Administrative infrastructure

The security of administrative activities can be improved by segregating administrative infrastructure from the wider network and the internet. In doing so, the use of a jump server (also known as a jump host or jump box) that allows only necessary ports and services to be used 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. In addition, using separate jump servers for the administration of critical servers (such as Microsoft Active Directory Domain Services domain controllers, Microsoft Active Directory Certificate Services Certification Authority servers, Microsoft Active Directory Federation Services servers and Microsoft Entra Connect servers), high-value servers (such as Domain Name System servers, database servers, email servers, file servers and web servers) and regular servers can further assist in protecting these assets.

Control: ISM-1385; Revision: 4; Updated: Jun-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Administrative infrastructure is segregated from the wider network and the internet.

Control: ISM-1750; Revision: 0; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Administrative infrastructure for critical servers, high-value servers and regular servers is segregated from each other.

Control: ISM-1386; Revision: 5; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Network management traffic can only originate from administrative infrastructure.

Control: ISM-1387; Revision: 2; Updated: Sep-21; Applicable: NC, OS, P, S, TS; Essential 8: ML2, ML3
Administrative activities are conducted through jump servers.

Control: ISM-1899; Revision: 0; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Network devices that do not belong to administrative infrastructure cannot initiate connections with administrative infrastructure.

Further information

Further information on system administration can be found in the Australian Signals Directorate's (ASD) *Secure administration* publication.

Further information on change and configuration management plans can be found in the system-specific cybersecurity documentation section of the *Guidelines for cybersecurity documentation*.

Further information on the use of privileged user accounts for system administration activities can be found in the access to systems and their resources section of the *Guidelines for personnel security*.

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.

Control: ISM-1143; Revision: 9; Updated: Dec-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Patch management processes, and supporting patch management procedures, are developed, implemented and maintained.

Control: ISM-0298; Revision: 8; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: 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 develop, implement, maintain and regularly verify software registers for workstations, servers, network devices and networked IT equipment.

Control: ISM-1493; Revision: 6; Updated: Dec-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Software registers for workstations, servers, network devices and networked IT equipment are developed, implemented, maintained and verified on a regular basis.

Control: ISM-1643; Revision: 0; Updated: Jun-21; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Software registers contain versions and patch histories of applications, drivers, operating systems and firmware.

Scanning for unmitigated vulnerabilities

To ensure that patches or updates are being applied to applications, operating systems, drivers and firmware, it is essential that an organisation regularly identifies all assets within their environment using an automated method of asset discovery, such as an asset discovery tool or a vulnerability scanner with equivalent functionality. Following asset discovery, identified assets can be scanned for missing patches or updates using a vulnerability scanner with an up-to-date vulnerability database. Ideally, vulnerability scanning should be conducted in an automated manner and take place at twice the frequency in which patches or updates need to be applied. For example, if patches or updates are to be applied within two weeks of release then vulnerability scanning should be undertaken at least weekly.

Control: ISM-1807; Revision: 0; Updated: Dec-22; Applicable: NC, OS, P, S, TS; Essential 8: ML1, ML2, ML3
An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities.

Control: ISM-1808; Revision: 0; Updated: Dec-22; Applicable: NC, OS, P, S, TS; Essential 8: ML1, ML2, ML3
A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities.

Control: ISM-1698; Revision: 1; Updated: Sep-23; Applicable: NC, OS, P, S, TS; Essential 8: ML1, ML2, ML3
A vulnerability scanner is used at least daily to identify missing patches or updates for vulnerabilities in online services.

Control: ISM-1699; Revision: 2; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: ML1, ML2, ML3
A vulnerability scanner is used at least weekly to identify missing patches or updates for vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF applications, and security products.

Control: ISM-1700; Revision: 3; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: ML2, ML3
A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in applications other than office productivity suites, web browsers and their extensions, email clients, PDF applications, and security products.

Control: ISM-1701; Revision: 1; Updated: Sep-23; Applicable: NC, OS, P, S, TS; Essential 8: ML1, ML2, ML3
A vulnerability scanner is used at least daily to identify missing patches or updates for vulnerabilities in operating systems of internet-facing servers and internet-facing network devices.

Control: ISM-1702; Revision: 2; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: ML1, ML2, ML3
A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in operating systems of workstations, non-internet-facing servers and non-internet-facing network devices.

Control: ISM-1752; Revision: 4; Updated: Jun-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in operating systems of IT equipment other than workstations, servers and network devices.

Control: ISM-1703; Revision: 2; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: ML3
A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in drivers.

Control: ISM-1900; Revision: 0; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: ML3
A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in firmware.

Control: ISM-1921; Revision: 0; Updated: Jun-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The likelihood of system compromise is frequently assessed when working exploits exist for unmitigated vulnerabilities.

Mitigating known vulnerabilities

When patches or updates are released by vendors for vulnerabilities, an organisation should apply them in a timeframe commensurate with the likelihood of attempted exploitation by malicious actors. For example, by prioritising patches or updates for vulnerabilities in online services as well as operating systems of internet-facing servers and internet-facing network devices. This is especially important when vulnerabilities are assessed as critical by vendors or working exploits exist.

If no patches or updates are available for vulnerabilities, mitigation advice from vendors, trustworthy 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 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 IT equipment, ASD will conduct an assessment of the patch or update. Subsequently, if the patch or update is approved for deployment, ASD will provide guidance on the methods and timeframes in which it is to be applied.

Control: ISM-1876; Revision: 0; Updated: Sep-23; Applicable: NC, OS, P, S, TS; Essential 8: ML1, ML2, ML3
Patches, updates or other vendor mitigations for vulnerabilities in online services are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist.

Control: ISM-1690; Revision: 2; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: ML1, ML2, ML3
Patches, updates or other vendor mitigations for vulnerabilities in online services are applied within two weeks of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist.

Control: ISM-1691; Revision: 2; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: ML1, ML2
Patches, updates or other vendor mitigations for vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF applications, and security products are applied within two weeks of release.

Control: ISM-1692; Revision: 2; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: ML3
Patches, updates or other vendor mitigations for vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF applications, and security products are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist.

Control: ISM-1901; Revision: 1; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: ML3
Patches, updates or other vendor mitigations for vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF applications, and security products are applied within two weeks of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist.

Control: ISM-1693; Revision: 3; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: ML2, ML3
Patches, updates or other vendor mitigations for vulnerabilities in applications other than office productivity suites, web browsers and their extensions, email clients, PDF applications, and security products are applied within one month of release.

Control: ISM-1877; Revision: 0; Updated: Sep-23; Applicable: NC, OS, P, S, TS; Essential 8: ML1, ML2, ML3
Patches, updates or other vendor mitigations for vulnerabilities in operating systems of internet-facing servers and internet-facing network devices are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist.

Control: ISM-1694; Revision: 2; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: ML1, ML2, ML3
Patches, updates or other vendor mitigations for vulnerabilities in operating systems of internet-facing servers and internet-facing network devices are applied within two weeks of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist.

Control: ISM-1695; Revision: 2; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: ML1, ML2
Patches, updates or other vendor mitigations for vulnerabilities in operating systems of workstations, non-internet-facing servers and non-internet-facing network devices are applied within one month of release.

Control: ISM-1696; Revision: 1; Updated: Sep-23; Applicable: NC, OS, P, S, TS; Essential 8: ML3
Patches, updates or other vendor mitigations for vulnerabilities in operating systems of workstations, non-internet-facing servers and non-internet-facing network devices are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist.

Control: ISM-1902; Revision: 0; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: ML3
Patches, updates or other vendor mitigations for vulnerabilities in operating systems of workstations, non-internet-facing servers and non-internet-facing network devices are applied within one month of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist.

Control: ISM-1878; Revision: 1; Updated: Jun-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Patches, updates or other vendor mitigations for vulnerabilities in operating systems of IT equipment other than workstations, servers and network devices are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist.

Control: ISM-1751; Revision: 4; Updated: Jun-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Patches, updates or other vendor mitigations for vulnerabilities in operating systems of IT equipment other than workstations, servers and network devices are applied within one month of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist.

Control: ISM-1879; Revision: 1; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: ML3
Patches, updates or other vendor mitigations for vulnerabilities in drivers are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist.

Control: ISM-1697; Revision: 2; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: ML3
Patches, updates or other vendor mitigations for vulnerabilities in drivers are applied within one month of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist.

Control: ISM-1903; Revision: 0; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: ML3
Patches, updates or other vendor mitigations for vulnerabilities in firmware are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist.

Control: ISM-1904; Revision: 0; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: ML3
Patches, updates or other vendor mitigations for vulnerabilities in firmware are applied within one month of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist.

Control: ISM-0300; Revision: 10; Updated: Jun-24; Applicable: S, TS; Essential 8: N/A
Patches, updates or other vendor mitigations for vulnerabilities in high assurance IT equipment are applied only when approved by ASD, and in doing so, using methods and timeframes prescribed by ASD.

Cessation of support

When applications, operating systems, network devices and networked IT equipment reach their cessation date for support, and become legacy IT, an organisation will find it increasingly difficult to protect them against 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 networked IT equipment should be removed or replaced.

In planning for cessation of support, 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 networked IT equipment may cease to receive support immediately after newer versions are released.

Finally, when the immediate removal or replacement of unsupported applications, operating systems, network devices or networked IT equipment is not possible, compensating controls should be implemented until such time that they can be removed or replaced.

Control: ISM-1905; Revision: 0; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: ML1, ML2, ML3
Online services that are no longer supported by vendors are removed.

Control: ISM-1704; Revision: 3; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: ML1, ML2, ML3
Office productivity suites, web browsers and their extensions, email clients, PDF applications, Adobe Flash Player, and security products that are no longer supported by vendors are removed.

Control: ISM-0304; Revision: 8; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: ML3
Applications other than office productivity suites, web browsers and their extensions, email clients, PDF applications, Adobe Flash Player, and security products that are no longer supported by vendors are removed.

Control: ISM-1501; Revision: 1; Updated: Sep-21; Applicable: NC, OS, P, S, TS; Essential 8: ML1, ML2, ML3
Operating systems that are no longer supported by vendors are replaced.

Control: ISM-1753; Revision: 2; Updated: Dec-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Internet-facing network devices that are no longer supported by vendors are replaced.

Control: ISM-1981; Revision: 0; Updated: Dec-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Non-internet-facing network devices that are no longer supported by vendors are replaced.

Control: ISM-1982; Revision: 0; Updated: Dec-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Networked IT equipment that is no longer supported by vendors is replaced.

Control: ISM-1809; Revision: 2; Updated: Dec-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
When applications, operating systems, network devices or networked IT equipment that are no longer supported by vendors cannot be immediately removed or replaced, compensating controls are implemented until such time that they can be removed or replaced.

Further information

Further information on system patching can be found in ASD's *Patching applications and operating systems* publication.

Further information on patching evaluated products can be found in the evaluated product usage section of the *Guidelines for evaluated products*.

Further information on managing risks associated with legacy IT can be found in ASD's *Managing the risks of legacy IT: Executive guidance* and *Managing the risks of legacy IT: Practitioner guidance* publications.

Further information on cessation of support for Microsoft Windows operating systems, including potential compensating controls for use beyond their cessation date for support, can be found in ASD's *End of support for Microsoft Windows and Microsoft Windows Server* publication.

Further information on hardening user applications can be found in the user application hardening section of the *Guidelines for system hardening*.

Further information on hardening server applications can be found in the server application hardening section of the *Guidelines for system hardening*.

Data backup and restoration

Digital preservation policy

Developing, implementing and maintaining a digital preservation policy, as part of digital continuity planning, can assist in ensuring the long-term integrity and availability of data is maintained, especially when taking into account the potential for data degradation and removable media, hardware and software obsolescence.

Control: ISM-1510; Revision: 2; Updated: Dec-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
A digital preservation policy is developed, implemented and maintained.

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.

Control: ISM-1547; Revision: 2; Updated: Dec-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Data backup processes, and supporting data backup procedures, are developed, implemented and maintained.

Control: ISM-1548; Revision: 2; Updated: Dec-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Data restoration processes, and supporting data restoration procedures, are developed, implemented and maintained.

Performing and retaining backups

To mitigate the security risk of losing system availability or data as part of a ransomware attack, or other form of destructive attack, backups of data, applications and settings should be performed and retained in accordance with an organisation's business criticality and business continuity requirements. In doing so, backups of all data, applications and settings should be synchronised to enable restoration to a common point in time. Furthermore, it is essential that all backups are retained in a secure and resilient manner. This will ensure that should a system fall victim to a ransomware attack, or other form of destructive attack, data will not be lost and, if necessary, systems can be quickly restored.

Control: ISM-1511; Revision: 4; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: ML1, ML2, ML3
Backups of data, applications and settings are performed and retained in accordance with business criticality and business continuity requirements.

Control: ISM-1810; Revision: 1; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: ML1, ML2, ML3
Backups of data, applications and settings are synchronised to enable restoration to a common point in time.

Control: ISM-1811; Revision: 1; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: ML1, ML2, ML3
Backups of data, applications and settings are retained in a secure and resilient manner.

Backup access

To mitigate the security risk of unauthorised access to backups, an organisation should ensure that access to backups is controlled through the use of appropriate access controls.

Control: ISM-1812; Revision: 1; Updated: Sep-24; Applicable: NC, OS, P, S, TS; Essential 8: ML1, ML2, ML3
Unprivileged user accounts cannot access backups belonging to other user accounts.

Control: ISM-1813; Revision: 1; Updated: Sep-24; Applicable: NC, OS, P, S, TS; Essential 8: ML3
Unprivileged user accounts cannot access their own backups.

Control: ISM-1705; Revision: 2; Updated: Sep-24; Applicable: NC, OS, P, S, TS; Essential 8: ML2, ML3
Privileged user accounts (excluding backup administrator accounts) cannot access backups belonging to other user accounts.

Control: ISM-1706; Revision: 2; Updated: Sep-24; Applicable: NC, OS, P, S, TS; Essential 8: ML3
Privileged user accounts (excluding backup administrator accounts) cannot access their own backups.

Backup modification and deletion

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 during their retention period.

Control: ISM-1814; Revision: 1; Updated: Sep-24; Applicable: NC, OS, P, S, TS; Essential 8: ML1, ML2, ML3
Unprivileged user accounts are prevented from modifying and deleting backups.

Control: ISM-1707; Revision: 2; Updated: Sep-24; Applicable: NC, OS, P, S, TS; Essential 8: ML2, ML3
Privileged user accounts (excluding backup administrator accounts) are prevented from modifying and deleting backups.

Control: ISM-1708; Revision: 2; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: ML3
Backup administrator accounts are prevented from modifying and deleting backups during their retention period.

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 data, applications and settings from backups to a common point in time is tested in a coordinated manner as part of disaster recovery exercises.

Control: ISM-1515; Revision: 4; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: ML1, ML2, ML3
Restoration of data, applications and settings from backups to a common point in time is tested as part of disaster recovery exercises.

Further information

Further information on digital preservation planning and data retention is available from the National Archives of Australia.

Further information on the collection and retention of personal information can be found in the Office of the Australian Information Commissioner's *Australian Privacy Principles* and the associated *Australian Privacy Principles guidelines*.

Further information on business continuity and disaster recovery planning can be found in the chief information security officer section of the *Guidelines for cybersecurity roles*.

Guidelines for system monitoring

Event logging and monitoring

Event logging and monitoring activities

These guidelines are intended for security-relevant event logs. They are not intended for non-security-relevant event logs, such as operating system and application performance-related event logs.

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.

Control: ISM-0580; Revision: 7; Updated: Dec-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
An event logging policy is developed, implemented and maintained.

Centralised event logging facility

A centralised event logging facility can be used to capture, protect and manage event logs from multiple sources in a coordinated manner. This may be achieved by using a Security Information and Event Management (SIEM) platform, a Security Orchestration, Automation and Response (SOAR) platform, or both. Furthermore, in support of a centralised event logging facility, it is important that an accurate and consistent time source is used to assist with identifying connections between events.

Control: ISM-1405; Revision: 4; Updated: Dec-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
A centralised event logging facility is implemented.

Control: ISM-1983; Revision: 0; Updated: Dec-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Event logs sent to a centralised event logging facility are done so as soon as possible after they occur.

Control: ISM-1984; Revision: 0; Updated: Dec-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Event logs sent to a centralised event logging facility are encrypted in transit.

Control: ISM-1985; Revision: 0; Updated: Dec-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Event logs are protected from unauthorised access.

Control: ISM-1815; Revision: 1; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: ML2, ML3
Event logs are protected from unauthorised modification and deletion.

Control: ISM-0988; Revision: 7; Updated: Sep-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
An accurate and consistent time source is used for event logging.

Event log details

For each event logged, sufficient detail needs to be recorded in order for event logs to be useful. In doing so, event logs should be captured and stored in a consistent and structured format.

Control: ISM-0585; Revision: 6; Updated: Jun-24; Applicable: NC, OS, P, S, TS; Essential 8: 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 information technology equipment involved are recorded.

Control: ISM-1959; Revision: 0; Updated: Sep-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
To the extent possible, event logs are captured and stored in a consistent and structured format.

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 cybersecurity events, thereby, leading to the identification of cybersecurity incidents.

Control: ISM-1986; Revision: 1; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Event logs from critical servers are analysed in a timely manner to detect cybersecurity events.

Control: ISM-1906; Revision: 1; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: ML2, ML3
Event logs from internet-facing servers are analysed in a timely manner to detect cybersecurity events.

Control: ISM-1907; Revision: 1; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: ML3
Event logs from non-internet-facing servers are analysed in a timely manner to detect cybersecurity events.

Control: ISM-0109; Revision: 10; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: ML3
Event logs from workstations are analysed in a timely manner to detect cybersecurity events.

Control: ISM-1987; Revision: 1; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Event logs from security products are analysed in a timely manner to detect cybersecurity events.

Control: ISM-1960; Revision: 1; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Event logs from internet-facing network devices are analysed in a timely manner to detect cybersecurity events.

Control: ISM-1961; Revision: 1; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Event logs from non-internet-facing network devices are analysed in a timely manner to detect cybersecurity events.

Control: ISM-1228; Revision: 4; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: ML2, ML3
Cybersecurity events are analysed in a timely manner to identify cybersecurity incidents.

Event log retention

The retention of event logs is integral to system monitoring, hunt and cybersecurity incident response activities. As such, event logs should be retained for a suitable period of time to facilitate these activities.

Control: ISM-1988; Revision: 0; Updated: Dec-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Event logs are retained in a searchable manner for at least 12 months.

Control: ISM-1989; Revision: 0; Updated: Dec-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Event logs are retained as per minimum retention requirements for various classes of records as set out by the National Archives of Australia's Administrative Functions Disposal Authority Express (AFDA Express) Version 2 publication.

Further information

Further information on logging intrusion activity can be found in the managing cybersecurity incidents section of the *Guidelines for cybersecurity incidents*.

Further information on event logging for application-based security products can be found in the operating system hardening section of the *Guidelines for system hardening*.

Further information on event logging for artificial intelligence applications can be found in the software development fundamentals section of the *Guidelines for software development*.

Further information on event logging for Cross Domain Solutions can be found in the Cross Domain Solutions section of the *Guidelines for gateways*.

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 for mobile applications can be found in the software development fundamentals section of the *Guidelines for software development*.

Further information on event logging for multifunction devices can be found in the fax machines and multifunction devices section of the *Guidelines for communications systems*.

Further information on event logging for network-based security products can be found in the network design and configuration section of the *Guidelines for networking*.

Further information on event logging for operating systems can be found in the operating system hardening and authentication hardening sections of the *Guidelines for system hardening*.

Further information on event logging for server applications can be found in the server application hardening section of the *Guidelines for system hardening*.

Further information on event logging for system access can be found in the access to systems and their resources section of the *Guidelines for personnel security*.

Further information on event logging for user applications can be found in the user application hardening section of the *Guidelines for system hardening*.

Further information on event logging for web applications can be found in the software development section of the *Guidelines for software development*.

Further information on event logging for web proxies can be found in the web proxies section of the *Guidelines for gateways*.

Further information on event logging can be found in the following Australian Signals Directorate publications:

- *Best practices for event logging and threat detection*
- *Detecting and mitigating Active Directory compromises*
- *Hardening Microsoft Windows 10 workstations*

- *Hardening Microsoft Windows 11 workstations*
- *Priority logs for SIEM ingestion: Practitioner guidance*
- *Windows event logging and forwarding*.

Further information on SIEM and SOAR platforms can be found in the Australian Signals Directorate's *Implementing SIEM and SOAR platforms: Executive guidance* and *Implementing SIEM and SOAR platforms: Practitioner guidance* publications.

Further information on prioritising the collection and storage of event logs can be found in the United States' Cybersecurity & Infrastructure Security Agency's *Guidance for Implementing M-21-31: Improving the Federal Government's Investigative and Remediation Capabilities* publication.

Further information on the National Archives of Australia's requirements for event log retention can be found in their *AFDA Express Version 2 – Technology & Information Management* publication.

Guidelines for software development

Software development fundamentals

Introduction to software development

This section applies to software development activities for traditional applications (including user applications and server applications), artificial intelligence applications, mobile applications and web applications. Additional sections of these guidelines should also be consulted depending on the type of software development being undertaken. For example, the web application development section should be consulted for additional controls applicable to web applications.

Development, testing, staging and production environments

Segregating development, testing, staging and production environments, and their associated data, can minimise the likelihood of faulty or malicious 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.

Control: ISM-0400; Revision: 6; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Development, testing, staging and production environments are segregated.

Control: ISM-1419; Revision: 1; Updated: Sep-18; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Development and modification of software only takes place in development environments.

Control: ISM-1420; Revision: 5; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Data from production environments is not used in non-production environments unless the non-production environment is secured to at least the same level as the production environment.

Authoritative source for software

Software developers need to ensure that they are using a secure authoritative source for software as part of their development environment, as doing so can reduce the security risks related to unauthorised access to source code, source code tampering and other possible cyber supply chain attacks on software artefacts. In doing so, the authoritative source for software should be able to provide sufficient access control and event logging for access to, and modification of, any source code and software artefacts.

Control: ISM-2023; Revision: 0; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
An authoritative source for software is established and maintained.

Control: ISM-2024; Revision: 0; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The authoritative source for software is used for all software development activities.

Control: ISM-1422; Revision: 3; Updated: Sep-18; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Unauthorised access to the authoritative source for software is prevented.

Control: ISM-1816; Revision: 0; Updated: Dec-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Unauthorised modification of the authoritative source for software is prevented.

Issue tracking

To providing visibility into source code changes, and support traceability, software developers should be able to link all changes, including security updates, change or feature updates, or bug fixes to a request or decision that is documented within an issue tracking solution.

Control: ISM-2025; Revision: 0; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
An issue tracking solution is used to link software development tasks to security issues and decisions, change or feature requests, programming issues, or bug fixes.

Software artefacts

Software artefacts can include compiled code (such as libraries and executables), configuration files and any other file consumed by the software development process. Software artefacts, both internally and externally developed, could include malicious code or specifically crafted vulnerabilities designed to be exploited at a later stage. To assist in preventing the introduction of malicious software artefacts into an authoritative source for software, all software artefacts should be scanned for malicious code, undergo security testing or both before being stored in the authoritative source for software.

Control: ISM-2026; Revision: 0; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
All software artefacts are scanned for malicious code before being imported into the authoritative source for software, including all compiled code, third-party libraries and software components.

Control: ISM-2027; Revision: 0; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
All software artefacts are verified by a digital signature, or a secure hash provided over a secure channel, before being imported into the authoritative source for software.

Control: ISM-2028; Revision: 0; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
All imported or referenced third-party software artefacts are tested using static application security testing (SAST), dynamic application security testing (DAST) and software composition analysis (SCA) before being imported into the authoritative source for software and periodically throughout the software development life cycle.

Control: ISM-2029; Revision: 1; Updated: Sep-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The authoritative source for software restricts the use and import of third-party libraries and software components to trustworthy sources.

Control: ISM-2030; Revision: 0; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Scanning is used during commits to identify plain text or encoded secrets and keys, which are then blocked from being stored in the authoritative source for software.

Build solution

The build process for software can unintentionally allow vulnerabilities in software to make it into production environments. This security risk can be reduced by ensuring the build solution uses all available security features and that all automated tested is completed as part of the build process.

Control: ISM-2031; Revision: 0; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Compilers, interpreters and build tools (including pipelines) that provide security features to improve executable file security are implemented and such security features are used.

Control: ISM-2032; Revision: 0; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The build solution ensures that all automated testing is completed without warnings, alerts or errors before building software artefacts.

Secure software development

The use of Secure by Design principles and practices, including secure programming practices and either memory-safe programming languages (such as C#, Go, Java, Ruby, Rust and Swift) or less preferably memory-safe programming practices, along with threat modelling and mitigation of common security risks, is an important part of secure software development. In addition, providing mechanisms to assist in determining the authenticity and integrity of software, while configuring it in a secure manner, can assist with cyber supply chain security activities.

As part of secure software development, software should be designed and built to be Secure by Default, that is, the software is secure 'out of the box' with little to no additional setup or configuration required to achieve an adequate level of security. Importantly, all built-in security measures, such as multi-factor authentication and event logging, are included in the base product at no extra cost to consumers.

Control: ISM-2033; Revision: 0; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
All software security requirements are documented, stored securely and maintained throughout the software development life cycle.

Control: ISM-2034; Revision: 0; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Security design decisions are documented and reviewed throughout the software development cycle.

Control: ISM-2035; Revision: 0; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Security roles, responsibilities and knowledge requirements required to support the software development life cycle are identified and documented.

Control: ISM-2036; Revision: 0; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Security responsibilities for software developers are identified and documented.

Control: ISM-2037; Revision: 0; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Software developers that lack sufficient cybersecurity knowledge and skills required for their projects or tasks undertake suitable training on secure software development and programming practices.

Control: ISM-2038; Revision: 0; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
A software developer cybersecurity knowledge and skills register is implemented and maintained.

Control: ISM-0401; Revision: 8; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Secure by Design principles and practices are followed throughout the software development life cycle.

Control: ISM-1238; Revision: 6; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Threat modelling is used in support of the software development life cycle.

Control: ISM-2039; Revision: 0; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The software threat model is reviewed throughout the software development life cycle to ensure it reflects the as-built software and any changes to the threat environment.

Control: ISM-2040; Revision: 0; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Secure programming practices for the chosen programming language are used for software development.

Control: ISM-2041; Revision: 0; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Memory-safe programming languages, or less preferably memory-safe programming practices, are used for software development.

Control: ISM-2042; Revision: 0; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Secure by Default principles and practices are followed throughout the software development life cycle, including by ensuring that all built-in security measures are included and enabled in the base product at no extra cost to consumers.

Control: ISM-1780; Revision: 1; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
SecDevOps practices are used for software development.

Control: ISM-2043; Revision: 0; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Software is architected and structured to support readability and maintainability.

Control: ISM-1796; Revision: 1; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Files containing executable content are digitally signed by a certificate with a verifiable chain of trust as part of software development.

Control: ISM-1797; Revision: 1; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Installers, patches and updates are digitally signed or provided with cryptographic checksums as part of software development.

Control: ISM-2044; Revision: 0; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Software has no default credentials; however, if credentials are required, they are created on first install by the installing organisation.

Control: ISM-2045; Revision: 0; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Application backwards compatibility does not compromise any security measures or features.

Control: ISM-2046; Revision: 0; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Where software allows user impersonation, sensitive data is not logged and appropriate permissions are set.

Control: ISM-2047; Revision: 0; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Where software allows an authentication factor to be reset, the user is notified of the reset through a secondary channel.

Control: ISM-2048; Revision: 0; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Where software supports multiple user roles, non-administrative users are prevented from altering their profile permissions or privileges.

Control: ISM-2049; Revision: 0; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
When user permissions or credentials are changed, software forces all impacted users to re-authenticate.

Control: ISM-2050; Revision: 0; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
When digital signatures are processed by software, they are validated against a certificate trust chain and checked for revocation using a Certificate Revocation List or with the Online Certificate Status Protocol.

Control: ISM-2051; Revision: 0; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Software generates sufficient event logs to support the detection of cybersecurity events.

Control: ISM-2052; Revision: 0; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Event logs produced by software ensure that any sensitive data is protected.

Control: ISM-1798; Revision: 2; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Secure configuration guidance, in the form of a hardening guide or loosening guide, is produced and made available to consumers as part of software development.

Control: ISM-2053; Revision: 0; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
End of life procedures for software, covering how to remove the software and how to archive or destroy any user accounts and data, are produced and made available to consumers.

Software bill of materials

A software bill of materials is a list of open source and commercial software components used in software development. This can assist software developers in ensuring they are not using software components with known vulnerabilities. It can also assist in providing greater cyber supply chain transparency for consumers of software by allowing for easier identification and management of security risks associated with individual software components used by software.

Control: ISM-2054; Revision: 0; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
If a software bill of materials is available for imported third-party software components, it is used during software development to ensure such software components have no known vulnerabilities.

Control: ISM-1730; Revision: 0; Updated: Dec-21; Applicable: NC, OS, P, S, TS; Essential 8: N/A
A software bill of materials is produced and made available to consumers of software.

Software build provenance

A software build provenance is a manifest that describes the software components used in the build process, the set of commands executed during the build process, any relevant environmental context for the build process and the materials that were generated by the build process. A software build provenance assists in providing greater cyber supply chain transparency for consumers by allowing for the build process to be verified and, if needed, recreated.

Control: ISM-2055; Revision: 0; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
If a software build provenance is available for imported third-party software components, it is used during software development to ensure such software components are built to an appropriate standard.

Control: ISM-2056; Revision: 0; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
A software build provenance is produced and made available to consumers of software.

Network application programming interfaces

Network application programming interfaces (APIs) can facilitate the exchange of data between computing devices. As such, common security risks associated with their use should be mitigated during their development, especially for network APIs that are accessible over the internet. In particular, this includes mitigating poorly secured network APIs that facilitate unauthorised modification of data or access to data not authorised for release into the public domain. In such cases, ensuring authentication and authorisation of clients is performed when clients call network APIs can assist in mitigating unauthorised modification of, or access to, data. Finally, centrally logging and analysing network API use can assist in detecting malicious behaviour and contributing to investigations following cybersecurity incidents.

Control: ISM-1818; Revision: 2; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Authentication and authorisation of clients is performed when clients call network APIs that facilitate modification of data and are accessible over the internet.

Control: ISM-2013; Revision: 0; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Authentication and authorisation of clients is performed when clients call network APIs that facilitate modification of data but are not accessible over the internet.

Control: ISM-1817; Revision: 2; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Authentication and authorisation of clients is performed when clients call network APIs that facilitate access to data not authorised for release into the public domain and are accessible over the internet.

Control: ISM-2014; Revision: 0; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Authentication and authorisation of clients is performed when clients call network APIs that facilitate access to data not authorised for release into the public domain but are not accessible over the internet.

Control: ISM-1910; Revision: 1; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Network API calls that facilitate modification of data, or access to data not authorised for release into the public domain, and are accessible over the internet, are centrally logged.

Control: ISM-2015; Revision: 0; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Network API calls that facilitate modification of data, or access to data not authorised for release into the public domain, but are not accessible over the internet, are centrally logged.

Software input handling

Many vulnerabilities in software are caused by a lack of secure input handling. As such, it is essential that software does 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.

Control: ISM-1240; Revision: 5; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Validation and sanitisation are performed on all input received over the internet by software.

Control: ISM-2016; Revision: 1; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Validation and sanitisation are performed on all input received over a local network by software.

Control: ISM-2057; Revision: 0; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
All input validation rules are documented, matched in code and tested with both positive and negative unit testing or integration testing.

Control: ISM-2058; Revision: 0; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Data sources and serialised data inputs are validated before being deserialised.

Control: ISM-2059; Revision: 0; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
File uploads or input are restricted to specific file types, with malicious content scanning occurring prior to file access, file execution or file storage.

Software interaction with databases

Structured Query Language (SQL) injection attacks, facilitated by the use of dynamically generated queries, are a significant threat to the confidentiality, integrity and availability of database contents. Specifically, SQL injection attacks can allow malicious actors 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 software fail, they may display detailed error information about the structure of databases. This can be used by malicious actors to further tailor their SQL injection attacks.

Finally, centrally logging and analysing all queries to databases from software that are initiated by users can assist in monitoring the security posture of databases, detecting malicious behaviour and contributing to investigations following cybersecurity incidents.

Control: ISM-1275; Revision: 2; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
All queries to databases from software are filtered for legitimate content and correct syntax.

Control: ISM-1276; Revision: 5; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Parameterised queries or stored procedures, instead of dynamically generated queries, are used by software for database interactions.

Control: ISM-1278; Revision: 5; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Software is designed or configured to provide as little error information as possible about the structure of databases.

Control: ISM-1536; Revision: 3; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
All queries to databases from software that are initiated by users, and any resulting crash or error messages, are centrally logged.

Software security testing

Software security testing can assist software developers in identifying vulnerabilities in their software. In doing so, testing should be designed to be repeatable and scalable while ensuring vulnerabilities in software are identified and remediated as early as possible. Such software security testing should include SAST, DAST and SCA in order to achieve comprehensive test coverage. As part of software security testing, software developers may also wish to replicate testing within typical consumer environments. Furthermore, software developers may choose to use independent testing to assist with removing any potential for bias that might occur when they test their own software. Finally, software needs to be comprehensively tested for vulnerabilities during development, prior to all releases and periodically in order to attempt to identify any previously unidentified vulnerabilities.

Control: ISM-0402; Revision: 9; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Software is comprehensively tested for vulnerabilities, using SAST, DAST and SCA prior to its initial release, any subsequent releases and periodically in order to attempt to identify any previously unidentified vulnerabilities.

Control: ISM-2060; Revision: 0; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Code reviews are utilised to ensure software meets Secure by Design principles and practices as well as secure programming practices.

Control: ISM-2061; Revision: 0; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Software developer-supported security-focused peer reviews are conducted on all critical and security-focused software components.

Control: ISM-2062; Revision: 0; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Unit testing and integration testing, covering both positive and negative use cases, are used to ensure code quality and security.

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 vulnerabilities in a coordinated manner. Furthermore, following the verification and resolution of reported vulnerabilities, it can assist an organisation in notifying their customers of 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 vulnerabilities disclosed by 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 vulnerabilities
- actions, and associated timeframes, upon notification of vulnerabilities
- expectations regarding the public disclosure of vulnerabilities
- any recognition or reward for finders of vulnerabilities.

Finally, the Australian Signals Directorate (ASD) encourages security researchers and other members of the public to responsibly report vulnerabilities directly to an organisation. However, ASD 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, vulnerabilities can be reported to ASD as an independent coordinator. Note, under ASD's limited use obligation, information voluntarily provided to ASD about vulnerabilities cannot be used for regulatory purposes.

Control: ISM-1616; Revision: 0; Updated: Aug-20; Applicable: NC, OS, P, S, TS; Essential 8: N/A
A vulnerability disclosure program is implemented to assist with the secure development and maintenance of products and services.

Control: ISM-1755; Revision: 1; Updated: Dec-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
A vulnerability disclosure policy is developed, implemented and maintained.

Control: ISM-1756; Revision: 1; Updated: Dec-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Vulnerability disclosure processes, and supporting vulnerability disclosure procedures, are developed, implemented and maintained.

Control: ISM-1717; Revision: 3; Updated: Sep-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
A 'security.txt' file is hosted for each of an organisation's internet-facing website domains to assist in the responsible disclosure of vulnerabilities in the organisation's products and services.

Reporting and resolving vulnerabilities

Following the identification of vulnerabilities in software, either via internal software security testing or external security researchers, it is important that they are publicly disclosed in a responsible and timely manner. This allows users of impacted software to determine their risk exposure as part of their own cyber supply chain risk management activities. In doing so, such vulnerabilities should be resolved in a timely manner. In support of this, root cause analysis should be performed and, to the greatest extent possible, entire vulnerability classes should be remediated.

If vulnerabilities cannot be resolved in a timely manner via patches or updates, advice should be provided on how, to the greatest extent possible, the likelihood of vulnerabilities being exploited can be reduced, the impact of vulnerabilities being exploited can be reduced or both.

Control: ISM-1908; Revision: 2; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Vulnerabilities identified in software are publicly disclosed in a responsible and timely manner, including with Common Weakness Enumeration and Common Platform Enumeration information.

Control: ISM-1754; Revision: 4; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Vulnerabilities identified in software are resolved in a timely manner.

Control: ISM-1909; Revision: 1; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
In resolving vulnerabilities, root cause analysis is performed and, to the greatest extent possible, entire vulnerability classes are remediated.

Software event logging

Centrally logging and analysing security-relevant software crashes and error messages can assist in monitoring the security posture of software, detecting malicious behaviour and contributing to investigations following cybersecurity incidents.

Control: ISM-1911; Revision: 2; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Security-relevant software crashes and error messages are centrally logged.

Further information

Further information on a secure software development framework can be found in National Institute of Standards and Technology Special Publication 800-218, *Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities*.

Further information on Secure by Design and Secure by Default principles and practices can be found in the following publications:

- ASD's *Secure by Design foundations*
- ASD's *IoT Secure by Design guidance for manufacturers*
- United Kingdom's National Cyber Security Centre's *Secure development and deployment guidance*

- United Kingdom's Central Digital and Data Office's *Secure by Design Principles* and *Secure by Design Activities*
- United States' Cybersecurity & Infrastructure Security Agency's *Safe Software Deployment: How Software Manufacturers Can Ensure Reliability for Customers*
- United States' Cybersecurity & Infrastructure Security Agency's *Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software*.

Further information on secure programming practices is available from the Carnegie Mellon University's Software Engineering Institute.

Further information on the need for memory-safe programming languages can be found the following publications:

- United States' Cybersecurity & Infrastructure Security Agency's *The Case for Memory Safe Roadmaps: Why Both C-Suite Executives and Technical Experts Need to Take Memory Safe Coding Seriously*
- United States' Cybersecurity & Infrastructure Security Agency's *Exploring Memory Safety in Critical Open Source Projects*
- United States' National Security Agency's *Software Memory Safety*
- United States' National Security Agency and Cybersecurity & Infrastructure Security Agency's *Memory Safe Languages: Reducing Vulnerabilities in Modern Software Development*.

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 software bill of materials can also be found in the United States' Cybersecurity & Infrastructure Security Agency's *A Shared Vision of Software Bill of Materials (SBOM) for Cybersecurity* publication.

Further information on strong authentication can be found in the authentication hardening section of the *Guidelines for system hardening*.

Further information on software security testing can be found on the Open Worldwide Application Security Project's (OWASP) DevSecOps Guidelines and Source Code Analysis Tools websites.

Further information on implementing a vulnerability disclosure program can be found in the following publications:

- Google's *Starting a Vulnerability Disclosure Program*
- Carnegie Mellon University's Software Engineering Institute'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 developing a vulnerability disclosure policy is available from the disclose.io project to assist an organisation with their implementation.

Further information on recommended contents for a 'security.txt' file is available to assist an organisation with their implementation.

Further information on reporting vulnerabilities to ASD as an independent coordinator, including ASD's limited use obligation, is available from ASD.

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

Artificial intelligence application development

Introduction to artificial intelligence application development

This section describes the controls applicable to artificial intelligence application development and extends upon the prior software development fundamentals section.

Secure artificial intelligence application development

OWASP provides comprehensive resources for software developers that should be followed when developing artificial intelligence applications. In addition, artificial intelligence applications should be designed to reduce their attack surface with artificial intelligence models being stored in a file formats that does not allow arbitrary code execution.

Control: ISM-1923; Revision: 0; Updated: Jun-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The OWASP Top 10 for Large Language Model Applications are mitigated in the development of large language model applications.

Control: ISM-1924; Revision: 1; Updated: Sep-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Generative artificial intelligence applications evaluate user prompts to detect and mitigate adversarial inputs or suffixes designed to elicit unintended behaviour or assist in the generation of sensitive or harmful content.

Control: ISM-2072; Revision: 0; Updated: Sep-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Artificial intelligence models are stored in a file format that does not allow arbitrary code execution.

Further information

Further information on large language model application security risks can be found in the *OWASP Top 10 for Large Language Model Applications version 2025* publication.

Further information on artificial intelligence security risks can be found in ASD's *An introduction to artificial intelligence* and *Engaging with artificial intelligence* publications.

Further information on artificial intelligence security risks can also be found in the following publications:

- MITRE's *Adversarial Threat Landscape for Artificial-Intelligence Systems*
- National Institute of Standards and Technology AI 100-2 E2023, *Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations*

- United Kingdom's National Cyber Security Centre and United States' Cybersecurity & Infrastructure Security Agency's *Guidelines for secure AI system development*
- United States' National Security Agency's *AI Data Security: Best Practices for Securing Data Used to Train & Operate AI Systems*
- United States' National Security Agency's *Deploying AI Systems Securely: Best Practices for Deploying Secure and Resilient AI Systems*.

Mobile application development

Introduction to mobile application development

This section describes the controls applicable to mobile application development and extends upon the prior software development fundamentals section.

Secure mobile application development

OWASP provides comprehensive resources for software developers that should be followed when developing mobile applications.

Control: ISM-1922; Revision: 0; Updated: Jun-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The OWASP Mobile Application Security Verification Standard is used in the development of mobile applications.

Further information

Further information on mobile application security can be found in the *OWASP Mobile Application Security Verification Standard version 2.1.0* publication.

Web application development

Introduction to web application development

This section describes the controls applicable to web application development and extends upon the prior software development fundamentals section.

Secure web application design and development

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. In addition, OWASP provides comprehensive resources for software developers that should be followed when developing web applications.

Control: ISM-1239; Revision: 4; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Robust web application frameworks are used in the development of web applications.

Control: ISM-0971; Revision: 8; Updated: Mar-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The OWASP Application Security Verification Standard is used in the development of web applications.

Control: ISM-1849; Revision: 0; Updated: Mar-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The OWASP Top 10 Proactive Controls are used in the development of web applications.

Control: ISM-1850; Revision: 0; Updated: Mar-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The OWASP Top 10 are mitigated in the development of web applications.

Control: ISM-2063; Revision: 0; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
If supported, web application session cookies set the HttpOnly flag, Secure flag and the SameSite flag by default.

Control: ISM-2064; Revision: 0; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Web application session cookies contain only digitally signed opaque bearer tokens.

Control: ISM-2065; Revision: 0; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Web application session cookies using opaque bearer tokens that are not digitally signed use non-sequential random identifiers with a minimum of 128 bits of entropy, preferably 256 bits of entropy.

Control: ISM-2066; Revision: 0; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Web application sessions are centrally managed server side.

Control: ISM-2067; Revision: 0; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Web applications that support Single Sign On equally support Single Logout.

Web security policy response headers

Web security policy response header measures, such as Content-Security-Policy, Hypertext Transfer Protocol Strict Transport Security and X-Frame-Options, can be applied by web browsers to help protect themselves. This is achieved by web server software specifying security policy in response headers which web browsers then apply.

Control: ISM-1424; Revision: 5; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Content-Security-Policy, Hypertext Transfer Protocol Strict Transport Security and X-Frame-Options are specified by web server software via security policy in response headers.

Web application interactions

Hypertext Transfer Protocol Secure (HTTPS) is the Hypertext Transfer Protocol secured by Transport Layer Security (TLS) encryption. The use of HTTPS for web applications ensures that interactions with web applications are confidential and that the integrity of such interactions are also maintained.

Control: ISM-1552; Revision: 0; Updated: Oct-19; Applicable: NC, OS, P, S, TS; Essential 8: N/A
All web application content is offered exclusively using HTTPS.

Web application programming interfaces

Web APIs can facilitate the exchange of data between computing devices. As such, common security risks associated with their use should be mitigated during their development.

Control: ISM-1851; Revision: 0; Updated: Mar-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The OWASP API Security Top 10 are mitigated in the development of web APIs.

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 '<', '>' and '&'.

Control: ISM-1241; Revision: 4; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Output encoding is performed on all output produced by web applications.

Further information

Further information on web application security can be found in the *OWASP Application Security Verification Standard 5.0.0* and *OWASP Top 10 Proactive Controls 2024* publications.

Further information on web application security risks can be found in the *OWASP Top 10 2021* publication.

Further information on implementing HTTPS can be found in ASD'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 API security can be found in the *OWASP API Security Top 10 2023* publication.

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 compromised by malicious actors. This security risk can be mitigated by ensuring that database servers are functionally separated from web servers.

Control: ISM-1269; Revision: 3; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: 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 malicious actors. As such, it is important that all data communicated between database servers and web servers is encrypted.

Control: ISM-1277; Revision: 4; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: 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 compromised by malicious actors. 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.

Control: ISM-1270; Revision: 3; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Database servers are placed on a different network segment to user workstations.

Control: ISM-1271; Revision: 3; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Network access controls are implemented to restrict database server communications to strictly defined network resources that require access to the database server.

Control: ISM-1272; Revision: 2; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
If only local access to a database is required, networking functionality of database management system applications are disabled or directed to listen solely to the localhost interface.

Segregation of development, testing, staging and production database servers

Using database servers across different environments, such as development, testing, staging and production environments, could result in accidental damage to their integrity or exposure of their hosted database contents.

Control: ISM-1273; Revision: 4; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Database servers for development, testing, staging and production environments are segregated.

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*.

Further information on database management system applications can be found in the server application hardening section of the *Guidelines for system hardening*.

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. As such, it is important that a database register is developed, implemented, maintained and verified on a regular basis.

Control: ISM-1243; Revision: 6; Updated: Dec-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
A database register is developed, implemented, 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.

Control: ISM-1256; Revision: 3; Updated: Sep-18; Applicable: NC, OS, P, S, TS; Essential 8: 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 malicious actors 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.

Control: ISM-0393; Revision: 8; Updated: Jun-21; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Databases and their contents are classified based on the sensitivity or classification of data that they contain.

Control: ISM-1255; Revision: 4; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Database users' ability to access, insert, modify and remove database contents is restricted based on their work duties.

Control: ISM-1268; Revision: 2; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The need-to-know principle is enforced for database contents through the application of minimum privileges, database views, database roles and data tokenisation.

Segregation of development, testing, staging and production databases

Using database contents from production environments in non-production environments, such as development, testing or staging environments, could result in inadequate protection being applied to the database contents.

Control: ISM-1274; Revision: 7; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Database contents from production environments are not used in non-production environments unless the non-production environment is secured to at least the same level as the production environment.

Database event logging

Centrally logging and analysing security-relevant events, including configuration changes, for databases can assist in monitoring the security posture of databases, detecting malicious behaviour and contributing to investigations following cybersecurity incidents.

Control: ISM-1537; Revision: 5; Updated: Sep-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Security-relevant events for databases are centrally logged, including:

- *access or modification of particularly important content*
- *addition of new users, especially privileged users*
- *changes to user roles or privileges*
- *attempts to elevate user privileges*
- *queries containing comments*
- *queries containing multiple embedded queries*
- *database and query alerts or failures*
- *database structure changes*
- *database administrator actions*
- *use of executable commands*
- *database logons and logoffs.*

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, implements and maintains an email usage policy governing its use.

Control: ISM-0264; Revision: 4; Updated: Dec-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
An email usage policy is developed, implemented and maintained.

Webmail services

When users access non-approved webmail services, they often bypass 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.

Control: ISM-0267; Revision: 7; Updated: Mar-19; Applicable: NC, OS, P, S, TS; Essential 8: 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.

Control: ISM-0270; Revision: 6; Updated: Jun-21; Applicable: NC, OS, P, S, TS; Essential 8: 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.

Control: ISM-0271; Revision: 3; Updated: Mar-19; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Protective marking tools do not automatically insert protective markings into emails.

Control: ISM-0272; Revision: 4; Updated: Mar-19; Applicable: NC, OS, P, S, TS; Essential 8: 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.

Control: ISM-1089; Revision: 5; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: 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.

Control: ISM-0565; Revision: 4; Updated: Mar-19; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Email servers are configured to block, log and report emails with inappropriate protective markings.

Control: ISM-1023; Revision: 6; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: 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.

Control: ISM-0269; Revision: 5; Updated: Mar-22; Applicable: S, TS; Essential 8: 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 Department of Home Affairs' *Protective Security Policy Framework*.

Email gateways and servers

Centralised email gateways

When routing emails via centralised email gateways it will be easier 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.

Control: ISM-0569; Revision: 5; Updated: Jun-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Emails are routed via centralised email gateways.

Control: ISM-0571; Revision: 7; Updated: Jun-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
When users send or receive emails, an authenticated and encrypted channel is used to route emails via their organisation's centralised email gateways.

Email gateway maintenance activities

As backup and alternative email gateways are often poorly maintained in terms of patches and email content filtering, malicious actors 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.

Control: ISM-0570; Revision: 4; Updated: Sep-18; Applicable: NC, OS, P, S, TS; Essential 8: 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.

Control: ISM-0567; Revision: 5; Updated: Sep-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Email servers only relay emails destined for or originating from their domains (including subdomains).

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. 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.

In support of MTA-STS implementations, TLS Reporting provides 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.

Control: ISM-0572; Revision: 4; Updated: Sep-21; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Opportunistic TLS encryption is enabled on email servers that make incoming or outgoing email connections over public network infrastructure.

Control: ISM-1589; Revision: 3; Updated: Jun-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
MTA-STS is enabled to prevent the unencrypted transfer of emails between email servers.

Sender Policy Framework

SPF aids in the detection of spoofed emails by specifying a list of hosts or Internet Protocol (IP) addresses that are allowed to send emails on behalf of a specified domain or subdomain. If an email server is not in the SPF record for a domain or subdomain, SPF verification will not pass. In specifying SPF records, domain

owners should ensure that they delegate the minimum necessary set of hosts or IP addresses necessary for sending emails. In addition, extra care should be taken when delegating to hosts or IP addresses not under an organisation's control.

Control: ISM-0574; Revision: 7; Updated: Jun-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
SPF is used to specify authorised email servers (or lack thereof) for an organisation's domains (including subdomains).

Control: ISM-1183; Revision: 3; Updated: Jun-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
A hard fail SPF record is used when specifying authorised email servers (or lack thereof) for an organisation's domains (including subdomains).

Control: ISM-1151; Revision: 3; Updated: Oct-19; Applicable: NC, OS, P, S, TS; Essential 8: N/A
SPF is used to verify the authenticity of incoming emails.

DomainKeys Identified Mail

DKIM enables the detection of spoofed email contents. This is achieved by DKIM records specifying the public key used to verify the digital signature in an email. Specifically, if the signed digest in an email header does not match the signed contents of the email, verification will not pass.

Control: ISM-0861; Revision: 3; Updated: Sep-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
DKIM signing is enabled on emails originating from an organisation's domains (including subdomains).

Control: ISM-1026; Revision: 6; Updated: Jun-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
DKIM signatures on incoming emails are verified.

Control: ISM-1027; Revision: 5; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Email distribution list applications 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 as a result of domain alignment, SPF and DKIM checks. For emails that do not pass DMARC 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 malicious actors to spoof their organisation's domains.

Control: ISM-1540; Revision: 3; Updated: Jun-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
DMARC records are configured for an organisation's domains (including subdomains) such that emails are rejected if they do not pass DMARC checks.

Control: ISM-1799; Revision: 0; Updated: Sep-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Incoming emails are rejected if they do not pass DMARC 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.

Control: ISM-1234; Revision: 5; Updated: Dec-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Email content filtering is implemented to filter potentially harmful content in email bodies and attachments.

Blocking suspicious emails

Blocking specific types of suspicious emails, such as where the email source address uses an internal domain, or internal subdomain, reduces the likelihood of phishing emails entering an organisation's network.

Control: ISM-1502; Revision: 2; Updated: Sep-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Emails arriving via an external connection where the email source address uses an internal domain, or internal subdomain, 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.

Control: ISM-1024; Revision: 5; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: 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 Signals Directorate's (ASD) *Implementing certificates, TLS, HTTPS and opportunistic TLS* publication.

Further information on implementing SPF, DKIM and DMARC can be found in ASD'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 ASD'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 ASD'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 Version 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 cybersecurity incidents. As such, network documentation should include high-level network diagrams showing all connections into networks; logical network diagrams showing all critical servers, high-value servers, network devices and network security appliances; and device settings for all critical servers, high-value servers, network devices and network security appliances. Finally, as network documentation could be used by malicious actors to assist in compromising networks, it is important that it is appropriately protected.

Control: ISM-0518; Revision: 6; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Network documentation is developed, implemented and maintained.

Control: ISM-0516; Revision: 5; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: 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.

Control: ISM-1912; Revision: 0; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Network documentation includes device settings for all critical servers, high-value servers, network devices and network security appliances.

Control: ISM-1178; Revision: 3; Updated: Sep-18; Applicable: NC, OS, P, S, TS; Essential 8: 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 controls in preventing malicious actors 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.

Control: ISM-1181; Revision: 5; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Networks are segregated into multiple network zones according to the criticality of servers, services and data.

Control: ISM-1577; Revision: 1; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: 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 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 controls.

Control: ISM-1532; Revision: 3; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
VLANs are not used to separate network traffic between an organisation's networks and public network infrastructure.

Control: ISM-0529; Revision: 6; Updated: Dec-21; Applicable: NC, OS, P, S, TS; Essential 8: N/A
VLANs are not used to separate network traffic between networks belonging to different security domains.

Control: ISM-0530; Revision: 6; Updated: Dec-21; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Network devices managing VLANs are administered from the most trusted security domain.

Control: ISM-0535; Revision: 6; Updated: Dec-21; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Network devices managing VLANs belonging to different security domains do not share VLAN trunks.

Control: ISM-1364; Revision: 3; Updated: Dec-21; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Network devices managing VLANs terminate VLANs belonging to different security domains on separate physical network interfaces.

Functional separation between networked devices and the internet

Implementing functional separation between networked devices and the internet reduces the exposure of such devices to attacks originating from the internet.

Control: ISM-2068; Revision: 0; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Internet connectivity for networked devices is strictly limited to those that require access.

Networked management interfaces

To assist in reducing the attack surface of networks, IT equipment residing on networks (such as servers) or constituting the makeup of network infrastructure (such as network devices) should not directly expose their networked management interfaces to the internet. In situations where this is not possible, such as for some cloud services and web applications, additional compensating controls will need to be implemented in order to protect weak or vulnerable networked management interfaces from being exploited by malicious actors to remotely compromise networks. Ideally, IT equipment on networks, or constituting the makeup of network infrastructure, should be managed via administrative infrastructure segregated from the wider network and the internet.

Control: ISM-1863; Revision: 1; Updated: Jun-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Networked management interfaces for IT equipment are not directly exposed to the internet.

Functional separation between servers

Implementing functional separation between servers reduces the likelihood that a server compromised by malicious actors will pose an increased security risk to other servers.

Control: ISM-0385; Revision: 6; Updated: Sep-18; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Servers maintain effective functional separation with other servers allowing them to operate independently.

Control: ISM-1479; Revision: 1; Updated: Jun-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Servers minimise communications with other servers at the network and file system level.

Network encryption

While physical security can provide a degree of protection against unauthorised physical access to network infrastructure, unauthorised access to unencrypted data can still be gained via other means, such as compromised network devices. For this reason, it is important that all data communicated over network infrastructure is encrypted, even within appropriately secure areas. Note, however, some protocols do not have encrypted equivalents. In such situations, where practical and feasible, an organisation should consider transitioning to the use of alternative protocols that support encryption.

Control: ISM-1781; Revision: 0; Updated: Jun-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
All data communicated over network infrastructure is encrypted.

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 malicious actors.

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 malicious actors 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.

Control: ISM-0521; Revision: 6; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
IPv6 functionality is disabled in dual-stack network devices unless it is being used.

Control: ISM-1186; Revision: 4; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
IPv6 capable network security appliances are used on IPv6 and dual-stack networks.

Control: ISM-1428; Revision: 2; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Unless explicitly required, IPv6 tunnelling is disabled on all network devices.

Control: ISM-1429; Revision: 3; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
IPv6 tunnelling is blocked by network security appliances at externally-connected network boundaries.

Control: ISM-1430; Revision: 3; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: 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 malicious actors have reduced opportunities to physically connect unauthorised network devices, or networked information technology (IT) equipment, to networks, they also have reduced opportunities to compromise such 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.

Control: ISM-0520; Revision: 9; Updated: Dec-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Network access controls are implemented on networks to prevent the connection of unauthorised network devices and networked IT equipment.

Control: ISM-1182; Revision: 5; Updated: Sep-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Network access controls are implemented to limit the flow of network traffic within and between network segments to only that required for business purposes.

Network management traffic

Implementing security measures specifically for network management traffic provides another layer of defence should malicious actors find an opportunity to connect to networks. In addition, this also makes it more difficult for malicious actors to enumerate networks.

Control: ISM-1006; Revision: 6; Updated: Sep-18; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Security measures are implemented to prevent unauthorised access to network management traffic.

Using the Server Message Block protocol

The Server Message Block (SMB) protocol is used to share files and printers across networks. Unfortunately, a number of weaknesses exist in SMB version 1 that can be used by malicious actors to gain access to resources on networks, including Microsoft Active Directory Domain Services domain controllers.

Control: ISM-1962; Revision: 0; Updated: Sep-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
SMB version 1 is not used on networks.

Using the 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.

Control: ISM-1311; Revision: 3; Updated: Dec-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
SNMP version 1 and SNMP version 2 are not used on networks.

Control: ISM-1312; Revision: 3; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: 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.

Control: ISM-1028; Revision: 8; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
A NIDS or NIPS is deployed in gateways between an organisation's networks and other networks they do not manage.

Control: ISM-1030; Revision: 8; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: 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.

Blocking anonymity network traffic

Inbound network connections from anonymity networks, such as the Tor network, can be used by malicious actors for reconnaissance and malicious code 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 malicious code for command and control or data exfiltration purposes and should be blocked.

Control: ISM-1627; Revision: 1; Updated: Sep-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Inbound network connections from anonymity networks are blocked.

Control: ISM-1628; Revision: 0; Updated: Nov-20; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Outbound network connections to anonymity networks are blocked.

Encrypted Domain Name System Services

Domain Name System (DNS) is a hierarchical naming system built on a distributed database for resources connected to the internet. In performing this service, DNS maps human-readable domain names to their associated IP addresses. Unfortunately, malicious actors can surveil standard DNS requests for the purpose of intelligence gathering. As such, it is important that DNS traffic is encrypted by clients and servers wherever supported, such as via DNS over Hypertext Transfer Protocol Secure or DNS over Transport Layer Security.

Control: ISM-2017; Revision: 0; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
DNS traffic is encrypted by clients and servers wherever supported.

Protective Domain Name System Services

A protective DNS service can be an effective way of blocking requests made by an organisation's users, or malicious actors on an organisation's network, to known malicious domain names – either as part of an initial compromise or subsequent command and control activities. DNS event logs captured by a protective DNS service can also be useful for investigating any exploitation attempt or successful compromise of a network by malicious actors.

In selecting a protective DNS service, many commercial offerings exist. In addition, the Australian Signals Directorate (ASD) offers a free protective DNS service for Australia's most critical systems.

Control: ISM-1782; Revision: 1; Updated: Dec-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
A protective DNS service is used to block access to known malicious domain names.

Flashing network devices with trusted firmware before first use

Flashing network devices with trusted firmware, obtained from vendors via trusted means, before network devices are used for the first time can assist in reducing cyber supply chain risks, such as the introduction of malicious firmware resulting from a cyber supply chain interdiction attack or a compromised vendor development environment or source code repository.

Control: ISM-1800; Revision: 0; Updated: Sep-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Network devices are flashed with trusted firmware before they are used for the first time.

Default user accounts and credentials for network devices

Network devices can come pre-configured with default user accounts and credentials. For example, wireless access points with a user account named 'admin' and a password of 'admin'. Ensuring default user accounts or credentials are changed, disabled or removed during initial setup can assist in reducing the likelihood of network devices being exploited by malicious actors.

Control: ISM-1304; Revision: 7; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Default user accounts or credentials for network devices, including for any pre-configured user accounts, are changed, disabled or removed during initial setup.

Disabling unused physical ports on network devices

Disabling unused physical ports on network devices reduces the opportunity for malicious actors to connect to networks if they can gain physical access to network devices.

Control: ISM-0534; Revision: 2; Updated: Sep-18; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Unused physical ports on network devices are disabled.

Regularly restarting network devices

Implementing measures to restart network devices on at least a monthly basis can assist in maintaining network device performance as well as removing malicious actors that may have compromised a network device but failed to gain persistence.

Control: ISM-1801; Revision: 0; Updated: Sep-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Network devices are restarted on at least a monthly basis.

Network device event logging

Centrally logging and analysing security-relevant events, including configuration changes, for network devices, especially internet-facing network devices, can assist in monitoring the security posture of systems, detecting malicious behaviour and contributing to investigations following cybersecurity incidents.

Control: ISM-1963; Revision: 0; Updated: Sep-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Security-relevant events for internet-facing network devices are centrally logged.

Control: ISM-1964; Revision: 0; Updated: Sep-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Security-relevant events for non-internet-facing network devices are centrally logged.

Further information

Further information on secure network design can be found in ASD's *Foundations for modern defensible architecture* publication.

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 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 ASD's *Implementing network segmentation and segregation* publication.

Further information on network security zones can be found in Canada's Canadian Centre for Cyber Security's *Baseline security requirements for network security zones (version 2.0)* 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 blocking anonymity network traffic can be found in ASD's *Defending against the malicious use of the Tor network* publication.

Further information on DNS services can be found in ASD's *Domain Name System security for domain owners* and *Domain Name System security for domain resolvers* publications.

Further information on implementing encrypted DNS can be can be found in the United States' National Security Agency's *Adopting Encrypted DNS in Enterprise Environments* publication and the Cybersecurity & Infrastructure Security Agency's *Encrypted DNS Implementation Guidance* publication.

Further information on selecting a protective DNS service can be found in the United States' National Security Agency and Cybersecurity & Infrastructure Security Agency's *Selecting a Protective DNS Service* publication.

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

Further information on network device hardening, particularly for edge devices, can be found in the following publications:

- ASD's *Mitigation strategies for edge devices: Executive guidance*
- ASD's *Mitigation strategies for edge devices: Practitioner guidance*

- Canada's Canadian Centre for Cyber Security's *Security considerations for edge devices*
- United Kingdom's National Cyber Security Centre's *Guidance on digital forensics and protective monitoring specifications for producers of network devices and appliances*.

Further information on network device hardening can also be found in the United States' National Security Agency's *Network Infrastructure Security Guide* 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 event logging for network devices can also be found in ASD's *Priority logs for SIEM ingestion: Practitioner guidance* publication.

Wireless networks

Wireless networks

This section describes the 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.

Control: ISM-1314; Revision: 2; Updated: Sep-21; Applicable: NC, OS, P, S, TS; Essential 8: 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 malicious actors allowing them to target organisation networks in order to steal data or disrupt services.

Control: ISM-0536; Revision: 7; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: 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.

Control: ISM-1315; Revision: 2; Updated: Sep-18; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The administrative interface on wireless access points is disabled for wireless network connections.

Default settings

Some wireless access points come pre-configured with weak default settings. As such, it is important to harden the settings of wireless access points prior to their deployment in networks. In addition, some wireless access points come with default Service Set Identifiers (SSIDs). As default SSIDs are often documented on the internet, it is important to change default SSIDs of wireless access points.

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, malicious actors 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 malicious wireless access point instead. In doing so, malicious actors could steal authentication credentials in order to gain access to the legitimate wireless network.

Control: ISM-1710; Revision: 2; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Settings for wireless access points are hardened.

Control: ISM-1316; Revision: 3; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Default SSIDs of wireless access points are changed.

Control: ISM-1317; Revision: 3; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: 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.

Control: ISM-1318; Revision: 3; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
SSID broadcasting is not disabled on wireless access points.

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, malicious actors 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.

Control: ISM-1320; Revision: 2; Updated: Sep-18; Applicable: NC, OS, P, S, TS; Essential 8: 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, malicious actors 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.

Control: ISM-1319; Revision: 2; Updated: Sep-18; Applicable: NC, OS, P, S, TS; Essential 8: 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 ensures no cryptographic 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).

Control: ISM-1332; Revision: 3; Updated: Sep-21; Applicable: NC, OS, P, S, TS; Essential 8: 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 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 sourcing 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.

Control: ISM-1321; Revision: 2; Updated: Sep-21; Applicable: NC, OS, P, S, TS; Essential 8: N/A
802.1X authentication with EAP-TLS, using X.509 certificates, is used for mutual authentication; with all other EAP methods disabled on supplicants and authentication servers.

Control: ISM-1711; Revision: 0; Updated: Sep-21; Applicable: NC, OS, P, S, TS; Essential 8: 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.

Control: ISM-1322; Revision: 4; Updated: Sep-21; Applicable: NC, OS, P, S, TS; Essential 8: 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 malicious actors have 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.

Control: ISM-1324; Revision: 4; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Certificates are generated using an evaluated certificate authority or hardware security module.

Control: ISM-1323; Revision: 4; Updated: Jun-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Certificates are required for devices and users accessing wireless networks.

Control: ISM-1327; Revision: 3; Updated: Jun-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Certificates are protected by logical and physical access controls, encryption, and user authentication.

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).

Control: ISM-1330; Revision: 1; Updated: Sep-18; Applicable: NC, OS, P, S, TS; Essential 8: 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.

Control: ISM-1712; Revision: 1; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: 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.

Control: ISM-1454; Revision: 2; Updated: Sep-21; Applicable: NC, OS, P, S, TS; Essential 8: 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, such as using 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.

Control: ISM-1334; Revision: 2; Updated: Sep-18; Applicable: NC, OS, P, S, TS; Essential 8: 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.

Control: ISM-1335; Revision: 1; Updated: Sep-18; Applicable: NC, OS, P, S, TS; Essential 8: 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.

Control: ISM-1338; Revision: 2; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: 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.

Control: ISM-1013; Revision: 6; Updated: Dec-21; Applicable: S, TS; Essential 8: 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 testing and certification programs is available from the Wi-Fi Alliance.

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

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

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

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 cloud service providers. An organisation can attempt to 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 a genuine spike in demand. In cases of denial-of-service attacks, 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.

Control: ISM-1437; Revision: 5; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Cloud service providers are used for hosting online services.

Capacity and 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 availability. In support of this, an organisation and their cloud service providers should discuss the ability for resources to dynamically scale in response to a genuine spike in demand, including any authorised activities that can be undertaken to verify measures implemented to support such requirements, especially where a requirement for high availability exists. For example, an organisation and their cloud service providers may 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 and availability 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.

Control: ISM-1579; Revision: 2; Updated: Jun-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Cloud service providers' ability to dynamically scale resources in response to a genuine spike in demand is discussed and verified as part of capacity and availability planning for online services.

Control: ISM-1580; Revision: 1; Updated: Dec-21; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Where a high availability requirement exists for online services, the services are architected to automatically transition between availability zones.

Control: ISM-1581; Revision: 3; Updated: Jun-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Continuous real-time monitoring of the capacity and 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 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 attack mitigations.

In using CDNs, care should be taken with their configuration to ensure that the IP addresses of an organisation's web servers (referred to as origin servers) are not identifiable by malicious actors, as knowledge of origin server IP addresses could allow for protections provided by CDNs to be bypassed. Additionally, appropriate controls should be applied to only allow communication between origin servers, CDNs and authorised management networks.

Control: ISM-1438; Revision: 2; Updated: Dec-21; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Where a high availability requirement exists for website hosting, CDNs that cache websites are used.

Control: ISM-1439; Revision: 3; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: 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 attack mitigation 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, malicious actors 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 all processing resources, or hijacking online services in an attempt to redirect legitimate users away from those services to other services that malicious actors control.

As an organisation often cannot avoid being targeted by denial-of-service attacks, they should discuss with their cloud service providers any denial-of-service attack detection and monitoring services that may be available for their use. For example, reporting dashboards that provide out-of-band and real-time alerts based on organisation-defined notification thresholds. Furthermore, an organisation should discuss with their cloud service providers what mitigation strategies they can implement to prepare for, and reduce the impact of, being targeted by a denial-of-service attack. Finally, with the express consent of their cloud service providers, an organisation may seek to test the effectiveness of any denial-of-service attack mitigation strategies that have been implemented.

Overall, preparing for denial-of-service attacks before they occur, such as by identifying critical online services and implementing preventative denial-of-service attack mitigation strategies, is by far the best approach as it is very difficult to respond to denial-of-service attacks once they begin and efforts at that stage are unlikely to be effective.

Control: ISM-1431; Revision: 5; Updated: Jun-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Denial-of-service attack mitigation strategies are discussed with cloud service providers, specifically:

- *their capacity to withstand denial-of-service attacks*
- *costs likely to be incurred as a result of denial-of-service attacks*
- *availability monitoring and thresholds for notification of denial-of-service attacks*
- *thresholds for turning off any online services or functionality 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.*

Control: ISM-1436; Revision: 3; Updated: Jun-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Critical online services are segregated from other online services that are more likely to be targeted as part of denial-of-service attacks.

Control: ISM-1432; Revision: 3; Updated: Jun-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Domain names for online services are protected via registrar locking and confirming that domain registration details are correct.

Further information

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

Further information on the use of cloud service providers can be found in the managed services and cloud services section of the *Guidelines for procurement and outsourcing*.

Further information on business continuity and disaster recovery planning can be found in the chief information security officer section of the *Guidelines for cybersecurity roles*.

Further information on mitigating denial-of-service attacks can be found in ASD'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 information technology (IT) 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 malicious actors.

International standards for cryptographic modules

International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 19790:2025, *Information security, cybersecurity and privacy protection – Security requirements for cryptographic modules*, and ISO/IEC 24759:2025, *Information security, cybersecurity and privacy protection –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) 800-140, *FIPS 140-3 Derived Test Requirements (DTR): CMVP Validation Authority Updates to ISO/IEC 24759* are United States standards based upon earlier versions of ISO/IEC 19790 and ISO/IEC 24759.

Communications security doctrine

The Australian Signals Directorate (ASD) specifies additional communications security requirements in Australian Communications Security Instructions and ASD Broadcasts that must be complied with when operating High Assurance Cryptographic Equipment (HACE). Such requirements supplement these guidelines and, where conflicts occur, take precedence.

Control: ISM-0499; Revision: 12; Updated: Jun-25; Applicable: S, TS; Essential 8: N/A
Communications security doctrine and policy produced by ASD for the management and operation of HACE is complied with.

Approved High Assurance Cryptographic Equipment

In order to ensure interoperability and maintain trust, all HACE must be issued an Approval for Use by ASD and be operated in accordance with the latest version of their associated Australian Communications Security Instructions.

Control: ISM-1802; Revision: 1; Updated: Sep-23; Applicable: S, TS; Essential 8: N/A
HACE are issued an Approval for Use by ASD and operated in accordance with the latest version of their associated Australian Communications Security Instructions.

Cryptographic key management processes and procedures

Well documented cryptographic key management processes and procedures can assist with the secure use and management of cryptographic keys and associated hardware and software. In doing so, cryptographic key management processes and procedures should cover cryptographic key generation, registration, distribution, installation, usage, protection, storage, access, recovery and destruction.

Control: ISM-0507; Revision: 5; Updated: Dec-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Cryptographic key management processes, and supporting cryptographic key management procedures, are developed, implemented and maintained.

Encrypting data at rest

When encryption is applied to data at rest it provides an additional layer of defence against unauthorised access by malicious actors. 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. When selecting cryptographic equipment, applications or libraries for this purpose, the level of assurance required will depend on the sensitivity or classification of the data.

Control: ISM-1080; Revision: 5; Updated: Jun-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
An ASD-Approved Cryptographic Algorithm (AACA) or high assurance cryptographic algorithm is used when encrypting media.

Control: ISM-0459; Revision: 4; Updated: Dec-21; Applicable: NC, OS, P, S, TS; Essential 8: 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 data in transit

When data is communicated over network infrastructure, encryption should be used to protect the data from unauthorised access or manipulation. When selecting cryptographic equipment, applications or libraries for this purpose, the level of assurance required will depend on the sensitivity or classification of the data and the environment in which it is being applied.

Control: ISM-0469; Revision: 6; Updated: Jun-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
An ASD-Approved Cryptographic Protocol (AACP) or high assurance cryptographic protocol is used to protect data when communicated over network infrastructure.

Cryptographic implementation assurance

Securely implementing cryptographic algorithms and protocols is a difficult task that requires expertise and diligence. In doing so, suppliers, and their cyber supply chains, need to carry out their duties competently and honestly as small flaws in cryptographic equipment, applications or libraries can be catastrophic and difficult to detect. Therefore, to provide a degree of cryptographic implementation assurance, cryptographic equipment, applications and libraries should be assessed by one of the following processes, listed in order of preference:

- a Common Criteria evaluation against an ASD-endorsed Protection Profile
- a FIPS 140-3 cryptographic evaluation via the United States and Canada's Cryptographic Module Validation Program
- a cryptographic evaluation via the United States and Canada's Cryptographic Algorithm Validation Program
- a Common Criteria evaluation against an Evaluation Assurance Level
- an independent security review by a reputable process or body.

Note, when a suitable Common Criteria evaluated product does not exist, an alternate product capable of securely implementing AACAs and AACPs may be used. However, cyber supply chain security risks still need to be considered to ensure the product does not present a high risk. For example, an organisation should still follow robust and secure procurement processes by selecting a product from a supplier with:

- a history of undertaking Common Criteria evaluations for their other products
- a demonstrated commitment to the security of their products, including by adopting Secure by Design principles and practices, responsively resolving known vulnerabilities, and providing clear end of life advice for consumers
- a demonstrated commitment to transparency for their products
- a strong track record of maintaining the security of their own systems
- sufficient information on how to securely configure their products.

Control: ISM-0457; Revision: 11; Updated: Sep-25; Applicable: OS, P; Essential 8: N/A
Cryptographic equipment, applications or libraries that have completed a Common Criteria evaluation against an ASD-endorsed Protection Profile are used when encrypting media that contains OFFICIAL: Sensitive or PROTECTED data.

Control: ISM-0460; Revision: 13; Updated: Sep-23; Applicable: S, TS; Essential 8: N/A
HACE is used when encrypting media that contains SECRET or TOP SECRET data.

Control: ISM-0465; Revision: 11; Updated: Sep-25; Applicable: OS, P; Essential 8: N/A
Cryptographic equipment, applications or libraries that have completed a Common Criteria evaluation against an ASD-endorsed Protection Profile are used to protect OFFICIAL: Sensitive or PROTECTED data when communicated over insufficiently secure networks, outside of appropriately secure areas or via public network infrastructure.

Control: ISM-0467; Revision: 12; Updated: Sep-23; Applicable: S, TS; Essential 8: 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.

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, applications and libraries provide a means of data recovery.

Control: ISM-0455; Revision: 5; Updated: Sep-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Where practical, cryptographic equipment, applications and libraries provide a means of data recovery to allow for circumstances where the encryption key is unavailable due to loss, damage or failure.

Handling encrypted IT equipment and media

When a user authenticates to the encryption functionality of IT equipment or media, encrypted data is made available. At such a time, the IT 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 IT equipment or media can be considered to be protected by the encryption functionality again.

Control: ISM-0462; Revision: 8; Updated: Jun-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
When a user authenticates to the encryption functionality of IT 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.

Control: ISM-0501; Revision: 6; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Keyed cryptographic equipment is transported based on the sensitivity or classification of its keying material.

Reporting cryptographic-related cybersecurity 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 cybersecurity incident should be reported to the chief information security officer, or one of their delegates, as soon as possible after it occurs, and all keying material should be changed.

Control: ISM-0142; Revision: 5; Updated: Jun-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The compromise or suspected compromise of cryptographic equipment or associated keying material is reported to the chief information security officer, or one of their delegates, as soon as possible after it occurs.

Control: ISM-1091; Revision: 6; Updated: Dec-21; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Keying material is changed when compromised or suspected of being compromised.

Further information

Further information on cryptographic key management practices can be found in ASD's *Managing cryptographic keys and secrets* publication.

Further information on cryptographic key management practices for HACE is available from ASD.

Further information on general cryptographic key management practices can be found in NIST SP 800-57 Part 1 Rev. 5, *Recommendation for Key Management: Part 1 – General*.

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

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

Further information on 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 evaluation of the implementation of cryptographic algorithms, including testing requirements, is available as part of the Cryptographic Algorithm Validation Program which is jointly operated by NIST and the Canadian Centre for Cyber Security.

Further information on the protection of IT equipment and media can be found in the Department of Home Affairs' *Protective Security Policy Framework*.

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 ASD.

ASD-Approved Cryptographic Algorithms

There is no guarantee of a cryptographic algorithm's resistance to currently unknown attacks. However, the cryptographic 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 cryptographic algorithms listed in this section is limited to cases where they are implemented in accordance with these guidelines.

The approved asymmetric cryptographic algorithms are:

- Diffie-Hellman (DH) for agreeing on encryption session keys
- Elliptic Curve Diffie-Hellman (ECDH) for agreeing on encryption session keys
- Elliptic Curve Digital Signature Algorithm (ECDSA) for digital signatures

- Module-Lattice-Based Digital Signature Algorithm (ML-DSA) for digital signatures
- Module-Lattice-Based Key Encapsulation Mechanism (ML-KEM) for encapsulating encryption session keys (and similar keys)
- Rivest-Shamir-Adleman (RSA) for digital signatures and transporting encryption session keys (and similar keys).

The only approved hashing algorithm for general purpose use is Secure Hashing Algorithm 2 (SHA-2). However, Secure Hashing Algorithm 3 (SHA-3), including its extendable-output functions (XOFs), is approved exclusively for use within ML-DSA and ML-KEM.

The only approved symmetric cryptographic algorithm is Advanced Encryption Standard (AES).

Where there is a range of key sizes for a cryptographic algorithm, some key sizes are not approved as they are insecure against current attacks or do not provide an adequate safety margin against possible future attacks. For example, advances in integer factorisation methods have rendered some RSA moduli sizes vulnerable and could render other RSA moduli vulnerable in the future.

The minimum targets used for the effective security strength of cryptographic algorithms listed within this section are:

- 112 bits for non-classified data
- 112 bits for OFFICIAL: Sensitive data
- 112 bits for PROTECTED data
- 128 bits for SECRET data
- 192 bits for TOP SECRET data.

Note, certain key sizes and parameters, such as specific elliptic curves, are preferred in order to promote interoperability with the United States' National Security Agency's *Commercial National Security Algorithm Suite 2.0*.

Using ASD-Approved Cryptographic Algorithms

If cryptographic equipment, applications or libraries implement unapproved cryptographic algorithms, it is possible that these cryptographic 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 cryptographic algorithms (preferred) or by advising users not to use the unapproved cryptographic algorithms via usage policies.

Control: ISM-0471; Revision: 9; Updated: Sep-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Only AACAs or high assurance cryptographic algorithms are used by cryptographic equipment, applications and libraries.

Asymmetric cryptographic algorithms

ECDH is vulnerable to different types of attacks than DH. Consequently, ECDH offers more effective security per bit increase in key size than DH. This leads to smaller data requirements, which in turn means that the

elliptic curve variants have become de facto global standards. For reduced data cost, and to promote interoperability, ECDH should be used in preference to DH where possible.

Control: ISM-0994; Revision: 7; Updated: Mar-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
ECDH is used in preference to DH.

Using Diffie-Hellman

A modulus of 2048 bits for correctly implemented DH provides 112 bits of effective security strength, with larger modulus sizes providing more bits of effective security strength. However, taking into account projected technological advances in quantum computing, DH will not be approved beyond 2030.

When DH in a prime field is used, the prime modulus impacts the security of the cryptographic 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.

Control: ISM-0472; Revision: 7; Updated: Dec-24; Applicable: NC, OS, P; Essential 8: N/A
When using DH for agreeing on encryption session keys, a modulus of at least 2048 bits is used, preferably 3072 bits.

Control: ISM-1759; Revision: 0; Updated: Mar-22; Applicable: S, TS; Essential 8: N/A
When using DH for agreeing on encryption session keys, a modulus of at least 3072 bits is used, preferably 3072 bits.

Control: ISM-1629; Revision: 1; Updated: Dec-21; Applicable: NC, OS, P, S, TS; Essential 8: 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 Elliptic Curve Cryptography

The curve used within an elliptic curve cryptographic algorithm impacts the security of the cryptographic algorithm. As such, only suitable curves from NIST SP 800-186 should be used.

Control: ISM-1446; Revision: 3; Updated: Mar-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
When using elliptic curve cryptography, a suitable curve from NIST SP 800-186 is used.

Using Elliptic Curve Diffie-Hellman

When identifying a suitable curve from NIST SP 800-186, a base point order and key size of at least 224 bits for correctly implemented ECDH provides 112 bits of effective security strength, with larger key sizes providing more bits of effective security strength. However, taking into account projected technological advances in quantum computing, ECDH will not be approved beyond 2030.

Note, security of a curve selected from another source cannot be assumed to have the same security using base point order and key size alone.

Control: ISM-0474; Revision: 7; Updated: Dec-24; Applicable: NC, OS, P; Essential 8: 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.

Control: ISM-1761; Revision: 0; Updated: Mar-22; Applicable: S; Essential 8: 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.

Control: ISM-1762; Revision: 0; Updated: Mar-22; Applicable: TS; Essential 8: 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 identifying a suitable curve from NIST SP 800-186, a base point order and key size of 224 bits for correctly implemented ECDSA provides 112 bits of effective security strength, with larger key sizes providing more bits of effective security strength. However, taking into account projected technological advances in quantum computing, ECDSA will not be approved beyond 2030.

Note, security of a curve selected from another source cannot be assumed to have the same security using base point order and key size alone.

Control: ISM-0475; Revision: 7; Updated: Dec-24; Applicable: NC, OS, P; Essential 8: 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.

Control: ISM-1763; Revision: 0; Updated: Mar-22; Applicable: S; Essential 8: 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.

Control: ISM-1764; Revision: 0; Updated: Mar-22; Applicable: TS; Essential 8: N/A
When using ECDSA for digital signatures, NIST P-384 or P-521 curves are used, preferably the NIST P-384 curve.

Using post-quantum cryptographic algorithms

Post-quantum cryptographic algorithms are more complex than their traditional counterparts. To reduce the risk that vulnerabilities are introduced via implementation errors, approval is given to specific post-quantum cryptographic standards and their constituent post-quantum cryptographic algorithms.

Control: ISM-1990; Revision: 0; Updated: Dec-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
When using ML-DSA and ML-KEM, as per FIPS 204 and FIPS 203 respectively, adherence to pre-requisite FIPS publications is preferred.

Using the Module-Lattice-Based Digital Signature Algorithm

The effective security strength of ML-DSA has a complex dependency on numerous parameters with different effective security strengths targeted by different standardised parameter sets. The ML-DSA standard contains three different parameter sets: ML-DSA-44, ML-DSA-65 and ML-DSA-87. The use of ML-DSA-65 and ML-DSA-87 are approved. However, for interoperability and maintainability reasons, ML-DSA-65 will not be approved beyond 2030.

When using ML-DSA for digital signing, it may either be hedged or deterministic. Notably, the hedged variant provides effective protection from certain side-channel attacks which apply to the deterministic variant. For this reason, the hedged variant should be used whenever possible. The deterministic variant

should not be used unless the nature of the digital signing platform renders the creation of random data infeasible, which is a mandatory step for the hedged variant.

When using ML-DSA for digital signing, signing a message first involves hashing the message using SHAKE128 or SHAKE256. In environments where the message being hashed is large, and the digital signing platform lacks hardware support for SHAKE128 and SHAKE256, pre-hashed variants of ML-DSA might be used to reduce computational overheads. In such cases, pre-hashed variants of ML-DSA take as their input a hash of the message as computed by an alternative, and less computationally expensive, hashing algorithm. In such cases, care should be taken to ensure that an appropriate alternative hashing algorithm is being used, such as a SHA-2 hashing algorithm. In such cases, the hash used should be twice as long as the desired effective security strength. In practice, this requires the use of at least SHA-384 for the pre-hashed variant of ML-DSA-65 and at the use of at least SHA-512 for the pre-hashed variant of ML-DSA-87.

Control: ISM-1991; Revision: 0; Updated: Dec-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
When using ML-DSA for digital signatures, ML-DSA-65 or ML-DSA-87 is used, preferably ML-DSA-87.

Control: ISM-1992; Revision: 0; Updated: Dec-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
When using ML-DSA for digital signatures, the hedged variant is used whenever possible.

Control: ISM-1993; Revision: 0; Updated: Dec-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Pre-hashed variants of ML-DSA-65 and ML-DSA-87 are only used when the performance of default variants is unacceptable.

Control: ISM-1994; Revision: 0; Updated: Dec-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
When the pre-hashed variants of ML-DSA-65 and ML-DSA-87 are used, at least SHA-384 and SHA-512 respectively are used for pre-hashing.

Using the Module-Lattice-Based Key Encapsulation Mechanism

The effective security strength of ML-KEM has a complex dependency on numerous parameters with different effective security strengths targeted by different standardised parameter sets. The ML-KEM standard contains three different parameter sets: ML-KEM-512, ML-KEM-768 and ML-KEM-1024. The use of ML-KEM-768 and ML-KEM-1024 are approved. However, for interoperability and maintainability reasons, ML-KEM-768 will not be approved beyond 2030.

Control: ISM-1995; Revision: 0; Updated: Dec-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
When using ML-KEM for encapsulating encryption session keys (and similar keys), ML-KEM-768 or ML-KEM-1024 is used, preferably ML-KEM-1024.

Using Rivest-Shamir-Adleman

A modulus of 2048 bits for correctly implemented RSA provides 112 bits of effective security strength, with larger modulus sizes providing more bits of effective security strength. However, taking into account projected technological advances in quantum computing, RSA will not be approved beyond 2030.

Control: ISM-0476; Revision: 8; Updated: Dec-24; Applicable: NC, OS, P; Essential 8: N/A
When using RSA for digital signatures, and transporting encryption session keys (and similar keys), a modulus of at least 2048 bits is used, preferably 3072 bits.

Control: ISM-1765; Revision: 1; Updated: Dec-24; Applicable: S, TS; Essential 8: N/A
When using RSA for digital signatures, and transporting encryption session keys (and similar keys), a modulus of at least 3072 bits is used, preferably 3072 bits.

Control: ISM-0477; Revision: 9; Updated: Dec-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
When using RSA for digital signatures, and for transporting encryption session keys (and similar keys), a different key pair is used for digital signatures and transporting encryption session keys.

Using Secure Hashing Algorithms

For most purposes, a hashing algorithm with an output size of 224 bits provides 112 bits of effective security strength, with larger output sizes providing more bits of effective security strength. However, for interoperability and maintainability reasons, SHA-224 and SHA-256 will not be approved beyond 2030.

Only SHA-2 hashing algorithms are approved for general purpose use. SHA-3 and XOF approval (i.e. SHA3-256, SHA3-512, SHAKE128 and SHAKE256) is restricted to use within internal steps of ML-DSA and ML-KEM.

Control: ISM-1766; Revision: 1; Updated: Dec-24; Applicable: NC, OS, P; Essential 8: N/A
When using SHA-2 for hashing, an output size of at least 224 bits is used, preferably SHA-384 or SHA-512.

Control: ISM-1767; Revision: 1; Updated: Dec-24; Applicable: S; Essential 8: N/A
When using SHA-2 for hashing, an output size of at least 256 bits is used, preferably SHA-384 or SHA-512.

Control: ISM-1768; Revision: 1; Updated: Dec-24; Applicable: TS; Essential 8: N/A
When using SHA-2 for hashing, an output size of at least 384 bits is used, preferably SHA-384 or SHA-512.

Using symmetric cryptographic algorithms

When using AES, a key size of 128 bits provides 128 bits of effective security strength, with larger key sizes providing more bits of effective security strength. However, for interoperability and maintainability reasons, AES-128 and AES-192 will not be approved beyond 2030.

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, malicious actors 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 cryptographic algorithm.

Control: ISM-1769; Revision: 1; Updated: Dec-24; Applicable: NC, OS, P, S; Essential 8: N/A
When using AES for encryption, AES-128, AES-192 or AES-256 is used, preferably AES-256.

Control: ISM-1770; Revision: 0; Updated: Mar-22; Applicable: TS; Essential 8: N/A
When using AES for encryption, AES-192 or AES-256 is used, preferably AES-256.

Control: ISM-0479; Revision: 5; Updated: Dec-21; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Symmetric cryptographic algorithms are not used in Electronic Codebook Mode.

Transitioning to post-quantum cryptography

The consensus model for quantum computing allows for different types of quantum attacks against traditional cryptography. While the direct impact of these quantum attacks varies across different cryptographic algorithms, there is a stark difference in impact between asymmetric cryptographic algorithms and symmetric cryptographic algorithms.

One known quantum attack (using Shor's algorithm) effectively defeats all traditional cryptography that relies upon asymmetric cryptographic algorithms such as DH, ECDH, ECDSA or RSA. The efficiency of this is such that it is infeasible to securely use these AACAs in the presence of a cryptographically relevant quantum computer (CRQC). While a CRQC does not currently exist, the trajectory of technological advances in quantum computing means that these AACAs will need to be phased out in favour of alternative AACAs that offer greater protection. As such, the development or procurement of new cryptographic equipment, applications and libraries, which are intended to be used beyond 2030, should be undertaken with the goal of supporting ASD-approved post-quantum cryptographic algorithms by 2030.

The impact of quantum attacks on hashing algorithms and symmetric cryptographic algorithms, such as SHA-2 and AES, is unlikely to be felt for some time. However, for interoperability reasons, the design and provision of new cryptographic equipment, applications and libraries, which are intended to be used beyond 2030, should support SHA-384, SHA-512 and AES-256.

Control: ISM-2073; Revision: 0; Updated: Sep-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
A post-quantum cryptography transition plan is developed, implemented and maintained.

Control: ISM-1917; Revision: 3; Updated: Sep-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The development and procurement of new cryptographic equipment, applications and libraries ensures support for the use of ML-DSA-87, ML-KEM-1024, SHA-384, SHA-512 and AES-256 by no later than 2030.

Post-quantum traditional hybrid schemes

A post-quantum traditional hybrid scheme is a multi-algorithm scheme where at least one cryptographic algorithm is a post-quantum cryptographic algorithm (e.g. ML-KEM) and at least one cryptographic algorithm is a traditional cryptographic algorithm (e.g. RSA). Generally, such schemes have the advantage of the security offered by the traditional cryptographic algorithm in the event that the post-quantum cryptographic algorithm is vulnerable to an implementation flaw or new attack. This advantage comes at the cost of increased complexity, making maintenance, analysis and secure implementation more difficult, as well as having greater computational and bandwidth overheads.

The use of post-quantum traditional hybrid schemes is not recommended, however, it is not prohibited. If such schemes are to be used, at least one of the post-quantum or traditional cryptographic algorithms, or both, should be an AACA. It is important to note though, that in the presence of a CRQC, the security of such schemes are reduced to that provided by the post-quantum cryptographic algorithm. As such, there is no practical value in the use of such schemes in the presence of a CRQC. An organisation choosing to implement a post-quantum traditional hybrid scheme should also keep in mind the eventual additional cost of transitioning to a pure post-quantum scheme in the future.

Control: ISM-1996; Revision: 0; Updated: Dec-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
When a post-quantum traditional hybrid scheme is used, either the post-quantum cryptographic algorithm, the traditional cryptographic algorithm or both are AACAs.

Further information

Further information on post-quantum traditional hybrid schemes can be found in the United Kingdom's National Cyber Security Centre's *Next steps in preparing for post-quantum cryptography* guidance.

Further information on how to combine the different components of a post-quantum traditional hybrid scheme used for key encapsulation can be found in NIST SP 800-56C Rev. 2, *Recommendation for Key-*

Derivation Methods in Key-Establishment Schemes. Note, this publication does not pertain to post-quantum traditional hybrid schemes used for digital signatures.

Further information on planning for the transition to post-quantum cryptography can be found in ASD's *Planning for post-quantum cryptography* publication.

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 ASD.

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, applications or libraries implement 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.

Control: ISM-0481; Revision: 8; Updated: Sep-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Only AACPs or high assurance cryptographic protocols are used by cryptographic equipment, applications and libraries.

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 IT equipment or applications that implement TLS, 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 TLS version 1.2 and earlier are no longer considered suitable for use as an AACP. As such, an organisation implementing TLS should use only the latest version of TLS (i.e. 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 clients and servers should be configured to enforce secure settings at the time of the TLS handshake. In situations where this is not possible, such as for some multi-tenancy environments (e.g. content delivery networks), additional controls will need to be implemented. For example, by further restricting the permitted TLS configuration within Layer 7 authorisation logic.

Control: ISM-1139; Revision: 6; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Only the latest version of TLS is used for TLS connections.

Control: ISM-1369; Revision: 3; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
AES-GCM is used for encryption of TLS connections.

Control: ISM-1370; Revision: 3; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Only server-initiated secure renegotiation is used for TLS connections.

Control: ISM-1372; Revision: 3; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
DH or ECDH is used for key establishment of TLS connections.

Control: ISM-1448; Revision: 2; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
When using DH or ECDH for key establishment of TLS connections, the ephemeral variant is used.

Control: ISM-1373; Revision: 2; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Anonymous DH is not used for TLS connections.

Control: ISM-1374; Revision: 3; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
SHA-2-based certificates are used for TLS connections.

Control: ISM-1375; Revision: 4; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
SHA-2 is used for the Hash-based Message Authentication Code (HMAC) and pseudorandom function (PRF) for TLS connections.

Control: ISM-1553; Revision: 1; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
TLS compression is disabled for TLS connections.

Control: ISM-1453; Revision: 1; Updated: Sep-18; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Perfect Forward Secrecy (PFS) is used for TLS connections.

Further information

Further information on implementing TLS can be found in ASD'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 IT equipment or applications that implement SSH, 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 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 settings below.

The settings below are based on OpenSSH. An organisation using other implementations of SSH should adapt these settings to suit their SSH implementation.

Control: ISM-1506; Revision: 1; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The use of SSH version 1 is disabled for SSH connections.

Control: ISM-0484; Revision: 6; Updated: Dec-21; Applicable: NC, OS, P, S, TS; Essential 8: 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.

Control: ISM-0485; Revision: 3; Updated: Sep-18; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Public key-based authentication is used for SSH connections.

Control: ISM-1449; Revision: 1; Updated: Sep-18; Applicable: NC, OS, P, S, TS; Essential 8: 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, malicious actors 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 malicious actors and a host
- if agent credential forwarding is enabled, malicious actors 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 forwarding is not disabled, malicious actors 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 applications 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.

Control: ISM-0487; Revision: 5; Updated: Sep-24; Applicable: NC, OS, P, S, TS; Essential 8: 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 forwarding*
- *console access.*

Control: ISM-0488; Revision: 4; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: 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 applications 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.

Control: ISM-0489; Revision: 6; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
When SSH-agent or similar key caching applications 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 IT equipment or applications that implement S/MIME, 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.

Control: ISM-0490; Revision: 4; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: 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 IT equipment or applications that implement IPsec, 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.

Control: ISM-0494; Revision: 3; Updated: Sep-18; Applicable: NC, OS, P, S, TS; Essential 8: 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, authentication and encryption are needed. While the AH and ESP protocols can 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.

Control: ISM-0496; Revision: 5; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: 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.

Control: ISM-1233; Revision: 2; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: 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, applications and libraries.

Control: ISM-1771; Revision: 0; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
AES is used for encrypting IPsec connections, preferably ENCR_AES_GCM_16.

Pseudorandom function

IKE version 2 requires the use of a PRF in order to generate random data for cryptographic operations. The approved hashing algorithms that can be used for the PRF are HMAC-SHA256, HMAC-SHA384 and HMAC-SHA512. Note, for interoperability and maintainability reasons, HMAC-SHA256 will not be approved beyond 2030.

Control: ISM-1772; Revision: 0; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: 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. Note, for interoperability and maintainability reasons, HMAC-SHA256 will not be approved beyond 2030.

Control: ISM-0998; Revision: 5; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: 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. Note, taking into account projected technological advances in quantum computing, DH and ECDH will not be approved beyond 2030.

Control: ISM-0999; Revision: 6; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: 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) for IKE version 2 can provide a balance between security and usability.

Control: ISM-0498; Revision: 4; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: 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.

Control: ISM-1000; Revision: 4; Updated: Sep-18; Applicable: NC, OS, P, S, TS; Essential 8: N/A
PFS is used for IPsec connections.

Guidelines for gateways

Gateways

Introduction to gateways

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

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

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

Implementing gateways

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

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

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

Control: ISM-0628; Revision: 6; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Gateways are implemented between networks belonging to different security domains.

Control: ISM-0637; Revision: 6; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Gateways implement a demilitarised zone if external parties require access to an organisation's services.

Control: ISM-0631; Revision: 7; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Gateways only allow explicitly authorised data flows.

Control: ISM-1192; Revision: 3; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Gateways inspect and filter data flows at the transport and above network layers.

Control: ISM-1427; Revision: 3; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Gateways perform ingress traffic filtering to detect and prevent IP source address spoofing.

System administrators for gateways

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

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

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

Control: ISM-1520; Revision: 3; Updated: Sep-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
System administrators for gateways undergo appropriate employment screening, and where necessary hold an appropriate security clearance, based on the sensitivity or classification of gateways.

Control: ISM-0613; Revision: 6; Updated: Mar-22; Applicable: S, TS; Essential 8: N/A
System administrators for gateways that connect to Australian Eyes Only or Releasable To networks are Australian nationals.

Control: ISM-1773; Revision: 0; Updated: Mar-22; Applicable: S, TS; Essential 8: N/A
System administrators for gateways that connect to Australian Government Access Only networks are Australian nationals or seconded foreign nationals.

Control: ISM-0611; Revision: 5; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
System administrators for gateways are assigned the minimum privileges required to perform their duties.

Control: ISM-0616; Revision: 5; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Separation of duties is implemented in performing administrative activities for gateways.

Control: ISM-0612; Revision: 5; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
System administrators for gateways are formally trained on the operation and management of gateways.

System administration of gateways

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

Control: ISM-1774; Revision: 0; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Gateways are managed via a secure path isolated from all connected networks.

Control: ISM-0629; Revision: 5; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
For gateways between networks belonging to different security domains, any shared components are

managed by system administrators for the higher security domain or by system administrators from a mutually agreed upon third party.

Authenticating to networks accessed via gateways

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

Control: ISM-0619; Revision: 6; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Users authenticate to other networks accessed via gateways.

Control: ISM-0622; Revision: 7; Updated: Jun-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
IT equipment authenticates to other networks accessed via gateways.

Border Gateway Protocol routing security

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

Route Origin Validation (ROV) is a mechanism that enables the validation of ROA covered IP addresses received via BGP. For increased BGP security, ROV should be implemented with all routing data received from transit providers being filtered. In doing so, any routes received that are invalid, or have multiple transit providers where one them does not implement ROV, should be rejected or deprioritised. In cases where an organisation chooses to deprioritise invalid routes to meet specific operational requirements, as opposed to rejecting them, such decisions should be regularly reviewed noting valid routes should always be prioritised over those that are not.

Finally, an organisation should consider the inclusion of routing security measures as part of procurement and contract requirements to ensure such functionality is available for their use.

Control: ISM-1783; Revision: 0; Updated: Jun-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Public IP addresses controlled by, or used by, an organisation are signed by valid ROA records.

Control: ISM-2018; Revision: 0; Updated: Mar-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Routes for RPKI-registered IP addresses that are advertised from invalid Autonomous Systems, or that are longer than allowed, are rejected or deprioritised by routers that exchange routes via BGP.

Gateway event logging

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

Control: ISM-0634; Revision: 11; Updated: Sep-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Security-relevant events for gateways are centrally logged, including:

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

Assessment of gateways

Testing of gateways following configuration changes, and at regular intervals no more than six months apart, assists with validating that gateways conform to expected security configurations. In addition, gateways will need to undergo regular security assessments by an Infosec Registered Assessor Program (IRAP) assessor, or an ASD assessor (or their delegate), 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 services that are being offered as well as any security-related changes that have occurred since the previous security assessment.

Control: ISM-1037; Revision: 6; Updated: Jun-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Gateways undergo testing following configuration changes, and at regular intervals no more than six months apart, to validate they conform to expected security configurations.

Control: ISM-0100; Revision: 12; Updated: Mar-25; Applicable: NC, OS, P, S; Essential 8: N/A
Non-classified, OFFICIAL: Sensitive, PROTECTED and SECRET gateways undergo an IRAP assessment, using the latest release of the ISM available prior to the beginning of the IRAP assessment (or a subsequent release), at least every 24 months.

Control: ISM-2019; Revision: 0; Updated: Mar-25; Applicable: TS; Essential 8: N/A
TOP SECRET gateways undergo a security assessment by ASD assessors (or their delegates), using the latest release of the ISM available prior to the beginning of the assessment (or a subsequent release), at least every 24 months.

Further information

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

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

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

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

Further information on cybersecurity awareness training can be found in the cybersecurity awareness training section of the *Guidelines for personnel security*.

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

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

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

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

Further information on event logging for network devices in gateways can also be found in ASD's *Priority logs for SIEM ingestion: Practitioner guidance* publication.

Further information on the purpose of IRAP is available from ASD.

Cross Domain Solutions

Introduction to Cross Domain Solutions

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

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

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

Types of Cross Domain Solutions

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

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

Implementing Cross Domain Solutions

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

Control: ISM-0626; Revision: 6; Updated: Mar-22; Applicable: S, TS; Essential 8: N/A
CDSs are implemented between SECRET or TOP SECRET networks and any other networks belonging to different security domains.

Consultation on Cross Domain Solutions

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

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

Separation of data flows

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

Control: ISM-0635; Revision: 7; Updated: Mar-22; Applicable: S, TS; Essential 8: N/A
CDSs implement isolated upward and downward network paths.

Control: ISM-1522; Revision: 3; Updated: Mar-22; Applicable: S, TS; Essential 8: N/A
CDSs implement independent security-enforcing functions for upward and downward network paths.

Control: ISM-1521; Revision: 3; Updated: Mar-22; Applicable: S, TS; Essential 8: N/A
CDSs implement protocol breaks at each network layer.

Cross Domain Solution event logging

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

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

Control: ISM-0670; Revision: 7; Updated: Sep-24; Applicable: S, TS; Essential 8: N/A
Security-relevant events for CDSs are centrally logged.

Control: ISM-1523; Revision: 1; Updated: Mar-22; Applicable: S, TS; Essential 8: N/A
A sample of security-relevant events relating to data transfer policies are taken at least every three months and assessed against security policies for CDSs to identify any operational failures.

User training

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

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

Further information

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

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

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

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

Further information on event logging for network devices in Cross Domain Solutions can also be found in ASD's *Priority logs for SIEM ingestion: Practitioner guidance* publication.

Further information on cybersecurity awareness training can be found in the cybersecurity awareness training section of the *Guidelines for personnel security*.

Firewalls

Using firewalls

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

Control: ISM-1528; Revision: 3; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Evaluated firewalls are used between an organisation's networks and public network infrastructure.

Control: ISM-0639; Revision: 9; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Evaluated firewalls are used between networks belonging to different security domains.

Further information

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

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

Web application firewalls

Using web application firewalls

When using a web application firewall (WAF), care should be taken with their configuration to ensure that the IP addresses of an organisation's web servers (referred to as origin servers) are not identifiable by malicious actors, as knowledge of origin server IP addresses could allow for protections provided by a WAF to be bypassed. Additionally, appropriate controls should be applied to only allow communication between origin servers, the WAF and authorised management networks.

Control: ISM-1862; Revision: 0; Updated: Jun-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
If using a WAF, 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 WAF and authorised management networks.

Further information

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

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

Diodes

Using diodes

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

Control: ISM-0643; Revision: 7; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Evaluated diodes are used for controlling the data flow of unidirectional gateways between an organisation's networks and public network infrastructure.

Control: ISM-0645; Revision: 7; Updated: Mar-22; Applicable: S, TS; Essential 8: N/A
Evaluated diodes used for controlling the data flow of unidirectional gateways between SECRET or TOP SECRET networks and public network infrastructure complete a high assurance evaluation.

Control: ISM-1157; Revision: 5; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Evaluated diodes are used for controlling the data flow of unidirectional gateways between networks.

Control: ISM-1158; Revision: 6; Updated: Mar-22; Applicable: S, TS; Essential 8: N/A
Evaluated diodes used for controlling the data flow of unidirectional gateways between SECRET or TOP SECRET networks and any other networks complete a high assurance evaluation.

Further information

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

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

Web proxies

Web usage policy

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

Control: ISM-0258; Revision: 4; Updated: Dec-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
A web usage policy is developed, implemented and maintained.

Using web proxies

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

Control: ISM-0260; Revision: 3; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
All web access, including that by internal servers, is conducted through web proxies.

Web proxy event logging

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

Control: ISM-0261; Revision: 6; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The following details are centrally logged for websites accessed via web proxies:

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

Further information

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

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

Web content filters

Using web content filters

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

Control: ISM-0963; Revision: 7; Updated: Dec-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Web content filtering is implemented to filter potentially harmful web-based content.

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

Control: ISM-1237; Revision: 2; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Web content filtering is applied to outbound web traffic where appropriate.

Transport Layer Security filtering

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

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

Allowing and blocking access to domain names

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

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

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

Control: ISM-1236; Revision: 2; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Malicious domain names, dynamic domain names and domain names that can be registered anonymously for free are blocked by web content filters.

Control: ISM-1171; Revision: 2; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Attempts to access websites through their IP addresses instead of their domain names are blocked by web content filters.

Further information

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

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

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

Content filtering

Content filtering techniques

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

- **Antivirus scans:** Scans files for viruses and other malicious code.
- **Automated dynamic analysis:** Analyses executable files run in a sandbox to detect suspicious behaviour.
- **File extension checks:** Checks file extensions to determine purported file types.
- **File format checks:** Checks files conform to defined file format specifications.
- **File type checks:** Checks file headers to determine actual file types.
- **Keyword checks:** Checks files for keywords that could indicate undesirable content.
- **Metadata checks:** Checks files for metadata that should be removed.
- **Protective marking checks:** Checks files for protective markings that may indicate undesirable content.
- **Manual inspections:** Involves the manual inspection of files for suspicious or undesirable content that an automated system may miss, which is particularly important for multimedia and content rich files.

Performing content filtering

Content filters perform an important function within gateways and CDSs by reducing the likelihood of unauthorised content or malicious code from entering or exiting networks. In performing content filtering checks, some content will be readily identifiable as malicious, or cannot be inspected, while other content,

such as active content, may be deemed suspicious depending on what is considered normal behaviour for content passing through gateways and CDSs within an organisation. Finally, when content filters are used by CDSs, their assurance requirements necessitate rigorous security testing to ensure they perform as expected and cannot be bypassed.

Control: ISM-0659; Revision: 6; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Files imported or exported via gateways or CDSs undergo content filtering checks.

Control: ISM-0651; Revision: 5; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Files identified by content filtering checks as malicious, or that cannot be inspected, are blocked.

Control: ISM-0652; Revision: 3; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Files identified by content filtering checks as suspicious are quarantined until reviewed and subsequently approved or not approved for release.

Control: ISM-1524; Revision: 2; Updated: Mar-22; Applicable: S, TS; Essential 8: N/A
Content filters used by CDSs undergo rigorous security testing to ensure they perform as expected and cannot be bypassed.

Encrypted files

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

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

Control: ISM-1293; Revision: 2; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Encrypted files imported or exported via gateways or CDSs are decrypted in order to undergo content filtering checks.

Archive files

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

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

Control: ISM-1289; Revision: 2; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Archive files imported or exported via gateways or CDSs are unpacked in order to undergo content filtering checks.

Control: ISM-1290; Revision: 2; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Archive files are unpacked in a controlled manner to ensure content filter performance or availability is not adversely affected.

Antivirus scanning

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

Control: ISM-1288; Revision: 2; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Files imported or exported via gateways or CDSs undergo antivirus scanning using multiple different scanning engines.

Automated dynamic analysis

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

Control: ISM-1389; Revision: 2; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Executable files imported via gateways or CDSs are automatically executed in a sandbox to detect any suspicious behaviour.

Allowing specific content types

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

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

Content validation

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

Control: ISM-1284; Revision: 3; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Files imported or exported via gateways or CDSs undergo content validation.

Content checking

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

Control: ISM-1965; Revision: 0; Updated: Sep-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Files imported or exported via gateways or CDSs undergo content checking.

Content conversion

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

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

Control: ISM-1286; Revision: 2; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Files imported or exported via gateways or CDSs undergo content conversion.

Content sanitisation

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

Control: ISM-1287; Revision: 2; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Files imported or exported via gateways or CDSs undergo content sanitisation.

Validating file integrity

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

Control: ISM-0677; Revision: 7; Updated: Mar-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Files imported or exported via gateways or CDSs that have a digital signature or cryptographic checksum are validated.

Further information

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

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

Peripheral switches

Using peripheral switches

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

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

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

Control: ISM-1457; Revision: 4; Updated: Mar-22; Applicable: S, TS; Essential 8: N/A
Evaluated peripheral switches used for sharing peripherals between SECRET and TOP SECRET systems, or between SECRET or TOP SECRET systems belonging to different security domains, preferably complete a high assurance evaluation.

Control: ISM-1480; Revision: 2; Updated: Mar-22; Applicable: S, TS; Essential 8: N/A
Evaluated peripheral switches used for sharing peripherals between SECRET or TOP SECRET systems and any non-SECRET or TOP SECRET systems complete a high assurance evaluation.

Further information

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

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

Guidelines for data transfers

Data transfers

Performing data transfers

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

Data transfer processes and procedures

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

Control: ISM-0663; Revision: 7; Updated: Dec-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Data transfer processes, and supporting data transfer procedures, are developed, implemented and maintained.

Control: ISM-1535; Revision: 6; Updated: Jun-24; Applicable: S, TS; Essential 8: N/A
Processes, and supporting procedures, are developed, implemented and maintained to prevent AUSTEO, AGAO and REL data in textual and non-textual formats from being exported to unsuitable foreign systems.

User responsibilities

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

Control: ISM-0661; Revision: 8; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Users transferring data to and from systems are held accountable for data transfers they perform.

Manual import of data

When manually importing data to systems, such as via the use of removable media, the data should be scanned for malicious and active content to reduce the likelihood of causing a malicious code infection. In cases where security checks fail, data should be quarantined until it can be reviewed and subsequently approved or not approved for release.

Control: ISM-0657; Revision: 6; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
When manually importing data to systems, the data is scanned for malicious and active content.

Control: ISM-1778; Revision: 0; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: 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 trustworthy source beforehand, such as the chief information security officer or one of their delegates. In doing so, all data authorised for export should be digitally signed by the trustworthy source.

Control: ISM-0664; Revision: 8; Updated: Sep-25; Applicable: S, TS; Essential 8: N/A
Data exported from SECRET and TOP SECRET systems is reviewed and authorised by a trustworthy source beforehand.

Control: ISM-0675; Revision: 7; Updated: Sep-25; Applicable: S, TS; Essential 8: N/A
Data authorised for export from SECRET and TOP SECRET systems is digitally signed by a trustworthy source.

Control: ISM-0665; Revision: 8; Updated: Sep-25; Applicable: S, TS; Essential 8: N/A
Trustworthy sources for SECRET and TOP SECRET systems are limited to people and services that have been verified and authorised as such by the chief information security officer.

Manual export of data

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

Control: ISM-1187; Revision: 3; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
When manually exporting data from systems, the data is checked for unsuitable protective markings.

Control: ISM-0669; Revision: 6; Updated: Dec-22; Applicable: S, TS; Essential 8: N/A
When manually exporting data from SECRET and TOP SECRET systems, digital signatures are validated and keyword checks are performed within all textual data.

Control: ISM-1779; Revision: 0; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: 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, it is important to log all data transfers. This applies to all forms of data transfers, such as those performed using removable media, gateways or CDSs. Ideally, data transfer logs should contain information on who authorised the data transfer, what data was transferred, where the data was transferred from or to, when the data was transferred, why the data was transferred, and how the data was transferred. Monitoring of such activities, via periodic verification of data transfer logs, can assist in identifying abuse of data transfer privileges and any unusual usage patterns that may indicate attempts by malicious actors to surreptitiously import malicious code or exfiltrate data from SECRET and TOP SECRET systems.

Control: ISM-1586; Revision: 0; Updated: Aug-20; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Data transfer logs are used to record all data imports and exports from systems.

Control: ISM-1294; Revision: 5; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Data transfer logs for systems are partially verified at least monthly.

Control: ISM-0660; Revision: 9; Updated: Mar-22; Applicable: S, TS; Essential 8: 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*.

Cybersecurity terminology

Glossary of abbreviations

Abbreviation	Meaning
AACA	ASD-Approved Cryptographic Algorithm
AACP	ASD-Approved Cryptographic Protocol
AD CS	Active Directory Certificate Services
AD DS	Active Directory Domain Services
AD FS	Active Directory Federation Services
AES	Advanced Encryption Standard
AGAO	Australian Government Access Only
AH	Authentication Header
AISEP	Australian Information Security Evaluation Program
API	application programming interface
ASD	Australian Signals Directorate
ASIO	Australian Security Intelligence Organisation
ATA	Advanced Technology Attachment
AUSTEO	Australian Eyes Only
BGP	Border Gateway Protocol
CA	Certification Authority
CCRA	Common Criteria Recognition Arrangement
CDN	content delivery network
CDS	Cross Domain Solution
CISO	chief information security officer

CRQC	cryptographically relevant quantum computer
DAST	dynamic application security testing
DH	Diffie-Hellman
DKIM	DomainKeys Identified Mail
DMA	Direct Memory Access
DMARC	Domain-based Message Authentication, Reporting and Conformance
DNS	Domain Name System
EAL	Evaluation Assurance Level
EAP	Extensible Authentication Protocol
EAP-TLS	Extensible Authentication Protocol-Transport Layer Security
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EDR	Endpoint Detection and Response
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
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure

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
IT	information technology
LAN	Local Area Network
MAC	Media Access Control
MFD	multifunction device
ML-DSA	Module-Lattice-Based Digital Signature Algorithm
ML-KEM	Module-Lattice-Based Key Encapsulation Mechanism
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
OT	operational technology
OWASP	Open Worldwide Application Security Project
PDF	Portable Document Format

PFS	Perfect Forward Secrecy
PMK	Pairwise Master Key
PP	Protection Profile
PRF	pseudorandom function
RADIUS	Remote Access Dial-In User Service
REL	Releasable To
RF	radio frequency
ROA	Route Origin Authorization
ROV	Route Origin Verification
RPKI	Resource Public Key Infrastructure
RSA	Rivest-Sharmir-Adleman
SAST	static application security testing
SCA	software composition analysis
SCEC	Security Construction and Equipment Committee
SHA-2	Secure Hashing Algorithm 2
SHA-3	Secure Hashing Algorithm 3
SIEM	Security Information and Event Management
S/MIME	Secure/Multipurpose Internet Mail Extension
SMB	Server Message Block
SNMP	Simple Network Management Protocol
SOAR	Security Orchestration, Automation and Response
SOE	Standard Operating Environment
SP	Special Publication
SPF	Sender Policy Framework

SPN	Service Principal Name
SQL	Structured Query Language
SSH	Secure Shell
SSID	Service Set Identifier
TLS	Transport Layer Security
UEFI	Unified Extensible Firmware Interface
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAF	web application firewall
WPA2	Wi-Fi Protected Access 2
WPA3	Wi-Fi Protected Access 3
XOF	extendable-output function

Glossary of cybersecurity terms

Term	Meaning
access control	The process of granting or denying requests for access to systems. 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.
application control	An approach in which only an explicitly defined set of trusted applications are allowed to execute on systems.

assets	In the context of technology, an overarching term used to refer to operating systems, applications, IT equipment, OT equipment, services and data. Such assets may also be referred to as technology assets.
asymmetric cryptographic algorithms	Cryptographic algorithms where two different keys are used, commonly a private and a public key. Asymmetric cryptographic algorithms are also known as public key cryptographic algorithms.
attack surface	The operating systems, applications, IT equipment, OT equipment and services used by a system. The greater the attack surface the greater the chances of malicious actors finding an exploitable vulnerability.
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.
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 Signals Directorate (ASD).
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 are accessible and useable by authorised entities when required.
biometrics	Measurable physical characteristics used to identify or verify an individual.
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.
change and configuration management plan	A document that describes the management of changes to the configuration of systems.

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 controls and associated security risk management processes.
classification	The categorisation of systems according to the expected impact if it was to be compromised.
classified data	Data that would cause limited through to exceptionally grave damage to Australia's national interests, the Australian Government generally or to an individual Commonwealth entity if compromised (i.e. data assessed as OFFICIAL: Sensitive, PROTECTED, SECRET or TOP SECRET).
commercial cryptographic equipment	A subset of IT 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 controls applied to protect telecommunications from unauthorised interception and exploitation, as well as ensure the authenticity of such telecommunications.
computer accounts	Accounts used to identify computers that belong to a domain, also known as machine accounts. Computer accounts provide a means for authenticating and auditing computer access to networks and domain resources.
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 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, Microsoft Active Directory Domain Services domain controllers, Microsoft Active Directory Certificate Services Certification Authority servers, Microsoft Active Directory Federation Services servers and Microsoft Entra Connect servers.
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 application	An application designed to perform cryptographic functions.
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 module	The set of hardware and software that implements approved cryptographic functions (including key generation) that are contained within the cryptographic boundary of the module.
cryptographic protocol	An agreed standard for secure communication between two or more entities to provide confidentiality, integrity, authentication and non-repudiation of data.
cryptographic system	A related set of hardware, software and supporting infrastructure used for cryptographic communication, processing or storage and the administrative framework in which it operates. Cryptographic systems may be based upon traditional cryptography, post-quantum cryptography or a combination of both.
cryptographically relevant quantum computer	A quantum computer that is capable of successfully executing attacks against traditional cryptographic systems.
customer	A person that an organisation has dealings with, typically via the consumption of goods or services. A customer does not necessarily need to purchase goods or services from the organisation.

cyber resilience	The ability to adapt to disruptions caused by cybersecurity incidents while maintaining continuous business operations. This includes the ability to detect, manage and recover from cybersecurity incidents.
cybersecurity	Measures used to protect the confidentiality, integrity and availability of information technology (IT) and operational technology (OT) systems.
cybersecurity documentation	An organisation's cybersecurity strategy; system-specific cybersecurity documentation; and any supporting diagrams, plans, policies, processes, procedures and registers.
cybersecurity 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.
cybersecurity incident	An unwanted or unexpected cybersecurity event, or a series of such events, that either has compromised business operations or has a significant probability of compromising business operations.
cybersecurity incident response plan	A document that describes the plan for responding to cybersecurity incidents.
cyberthreat	Any circumstance or event with the potential to harm systems.
data at rest	Data that resides on media or a system.
data in transit	Data that is being communicated across a communication medium.
data repository	A location in which data is stored, managed and made available to users.
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.
decommission	The process of removing something from operational service.
degausser	An electrical device or permanent magnet assembly which generates a 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 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 malicious actors 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 application	An application that can be used to prevent removable media and mobile devices from being connected to workstations and servers via external communication interfaces.
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	IT equipment that implements Internet Protocol version 4 and Internet Protocol version 6 protocol stacks.
elliptic curve cryptography	A group of asymmetric cryptographic algorithms underpinned by the mathematics of elliptic curves.
emanation security	The countermeasures 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.
event	In the context of system logs, an event constitutes an evident change to the normal behaviour of a network, system or user.
extendable-output function	A function that uses a hash function to output a digest of a user-chosen length. This is different to a hash function which outputs a digest of a fixed length.

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 IT equipment or OT equipment.
fly lead	A lead that connects IT 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.
gateway	Gateways securely manage data flows between connected networks from different security domains.
hardware	A generic term for IT equipment and OT equipment.
hardware security module	A physical computing device that safeguards cryptographic keys and provides cryptographic processing. A hardware security module is or contains a cryptographic module. Hardware security modules are commonly deployed in Public Key Infrastructure, digital identity solutions and payment systems.
Hash-based Message Authentication Code	A cryptographic function 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 authorised by ASD for the protection of SECRET and TOP SECRET data.
High Assurance Evaluation Program	The rigorous investigation, analysis, verification and validation of products by ASD to protect SECRET and TOP SECRET data.
high assurance IT equipment	IT equipment that has been designed and authorised for the protection of SECRET and TOP SECRET data.
high-value server	A server that provides important network services or contains data repositories. For example, Domain Name System servers, database servers, email servers, file servers and web servers.
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.

information technology	Hardware, software and supporting infrastructure used for the processing, storage or communication of data.
Infosec Registered Assessors Program	An initiative of ASD 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.
insider	Any person that has, or had, authorised logical or physical access to a system and its resources.
insider threat	An insider that performs, or attempts to perform, damaging activities (either intentionally or unintentionally) to a system or its resources. Some organisations may choose to exclude unintentional damage to systems and their resources (often referred to as negligent or accidental damage) from their definition of insider threat in order to focus on insiders with malicious intent (often referred to as malicious insiders).
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 malicious or unwanted activities. An Intrusion Detection System can be host-based or network-based.
Intrusion Prevention System	An automated system used to identify malicious or unwanted activities and react in real-time to block or prevent such activities. An Intrusion Prevention System can be host-based or network-based.
IRAP assessment	A security assessment conducted by an IRAP assessor against the requirements of the *Information security manual*.
IT equipment	Any device that can process, store or communicate data within IT environments, such as computers, multifunction devices, network devices, smartphones, electronic storage media and smart devices.

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.
key encapsulation mechanism	A form of asymmetric cryptography that carries out two functions. Specifically, generating an encryption session key and then securely transporting it to the receiver.
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.
keying material	Cryptographic keys generated or used by cryptographic equipment, applications or libraries.
logging facility	A facility that collects and stores event logs.
malicious actors	Individuals, groups or organisations that conduct malicious activities, such as cyber espionage, cyberattacks or cyber-enabled crime.
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.
medical device	Devices approved by the Therapeutic Goods Administration under the *Therapeutic Goods (Medical Devices) Regulations 2002* for diagnostic or therapeutic purposes.
memory-safe programming languages	Programming languages that prevent the introduction of vulnerabilities related to memory use. Examples of memory-safe programming languages include C#, Go, Java, Ruby, Rust and Swift. Examples of non-memory-safe programming languages include Assembly and C/C++.
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 laptop computers.
multi-factor authentication	Authentication using two or more different authentication factors. This may include something users know, something users have or something users are.
multifunction device	IT 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	IT 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 directly accessible over the internet, including those located behind a perimeter firewall. Such services may also be referred to as internet-facing services.

OpenPGP Message Format	An open-source implementation of Pretty Good Privacy, a widely available cryptographic toolkit.
operating system	Software that provides the interface through which users access a system. Operating systems also facilitate access to user applications, server applications, mobile applications and web applications.
operational technology	Systems that detect or cause a direct change to the physical environment through the monitoring or control of devices, processes and events. Operational technology is predominantly used to describe industrial control systems which include supervisory control and data acquisition systems and distributed control systems.
OT equipment	Any device that can process, store or communicate data or signals within OT environments, such as programmable logic controllers and remote terminal units.
passphrase	A sequence of words used for authentication.
password	A sequence of characters used for authentication.
password complexity	The use of different character sets, such as lower-case alphabetical characters (a-z), upper-case alphabetical characters (A-Z), numeric characters (0-9) and special characters.
passwordless authentication	Authentication that does not involve the use of something users know. Passwordless authentication may be single-factor or multi-factor, with the later often referred to as passwordless multi-factor authentication.
passwordless multi-factor authentication	Multi-factor authentication using something users have that is unlocked by something users know or are. Note, while a memorised secret may be used as part of passwordless multi-factor authentication (e.g. to unlock access to a cryptographic private key stored on a device) it is not the primary authentication factor, hence the use of the passwordless terminology.
patch	A piece of software designed to remedy vulnerabilities or improve the usability or performance of operating systems, applications, IT equipment or OT 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.
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 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, chief information security officers and their delegates, system administrators and privileged users.
post-quantum cryptography	Asymmetric cryptography designed to remain secure in the presence of a cryptographically relevant quantum computer.
post-quantum traditional hybrid scheme	An asymmetric cryptographic scheme that incorporates at least two different components based on different mathematically hard problems. Generally, post-quantum traditional hybrid schemes are used to combine post-quantum cryptography and traditional cryptography such that defeating the scheme requires defeating each component.
privileged operating environments	Privileged operating environments are those used for activities that require a degree of privileged access, such as system administration activities.
privileged user accounts	User accounts that have the capability to modify system configurations, account privileges, event logs or security configurations. This also applies to user accounts that may only have limited privileges but still have the ability to bypass some system controls. A privileged user account may belong to a person or a service.
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 a 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.
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 controls used to protect data based on a reassessment of the potential impact of its unauthorised disclosure. The lowering of the 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 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.

Secure Admin Workstation	A hardened workstation, or virtualised privileged operating environment, used specifically in the performance of administrative activities.
Secure by Default	A software development principle whereby products and services are configured for maximum security by default.
Secure by Demand	When a customer requests that their suppliers provide evidence of their commitment to security and transparency for their products and services.
Secure by Design	A software development principle whereby security is designed into every stage of a product or service's development.
secure channel	A path for transferring data between two entities that ensures confidentiality and integrity, as well as mutual authentication, between the two entities.
Secure Shell	A network protocol that can be used to securely log into, execute commands on, and transfer files between remote workstations and servers.
Secure/Multipurpose Internet Mail Extension	A protocol which allows the encryption and signing of email messages.
secured space	An area certified to the physical security requirements for a Security Zone Two to Security Zone Five area, as defined in the Department of Home Affairs' *Protective Security Policy Framework*.
security assessment	An activity undertaken to assess 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 the 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 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.
sensitive data	Data that would cause damage to 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.
service accounts	User accounts that are used to perform automated tasks without manual intervention, such as machine to machine communications. Service accounts will typically be configured to disallow interactive logins.
shared facility	A facility shared by multiple tenants. For example, a single floor, or part of a floor, within a multi-tenanted building.
shared responsibility model	A framework that describes the management and operational responsibilities between different parties for a system. Where responsibilities relating to specific controls are shared between multiple parties, enough detail is documented to provide clear demarcation between the parties.
software	An element of a system including, but not limited to, an operating system or application.
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 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 applications that can be used for servers, workstations and mobile devices.
supplier	Organisations, such as software developers, IT equipment manufacturers, OT equipment manufacturers, service providers and data brokers, that provide products and services. Suppliers can also include other organisations involved in distribution channels.
symmetric cryptographic algorithms	Cryptographic algorithms that use the same key for encryption and decryption. Block ciphers and stream ciphers are common types of symmetric cryptographic algorithms.
system	The cyber supply chain, infrastructure, operating systems and applications supporting the processing, storage or communication of data, including the governance framework in which they operate.
system administrator	A system administration role performed by a privileged user that holds a position of trust.
system classification	The classification of a system is the highest classification of data which the system is authorised to store, process or communicate.
system owner	The executive responsible for a system.
system security plan	A document that describes a system and its associated controls.
system-specific cybersecurity documentation	A system's system security plan, cybersecurity incident response plan, change and configuration management 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.

traditional cryptography	Common well studied and understood cryptographic algorithms that existed before the threat of a cryptographically relevant quantum computer existed.
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.
trustworthy 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.
trustworthy supplier	A supplier that has been verified as trustworthy as part of a cyber supply chain risk management assessment and subsequently recorded on an organisation's approved supplier list.
tunnel mode	An IPsec mode that provides a secure connection between two endpoints by encapsulating an entire IP packet.
unprivileged user accounts	User accounts that do not have the capability to modify system configurations, account privileges, event logs or security configurations. An unprivileged user account may belong to a person or a service.
unprivileged operating environments	Unprivileged operating environments are those used for activities that do not require privileged access, such as reading emails and browsing the web.
unsecured space	An area not certified to the physical security requirements for a Security Zone Two to Security Zone Five area, as defined in the Department of Home Affairs' *Protective Security Policy Framework*.
untrusted device	Any IT equipment that an organisation does not trust. For example, unknown IT equipment (which might belong to malicious actors), or an uncontrolled personal mobile device of an employee.
user	An individual that works for an organisation and is authorised to access a system.
user accounts	User accounts include privileged user accounts and unprivileged user accounts.
validation	Confirmation that stakeholder requirements for the intended use of operating systems, applications, IT equipment or OT equipment have been met.

verification	Confirmation that design or compliance requirements for operating systems, applications, IT equipment or OT equipment have been met.
Virtual Local Area Network	Network devices and networked IT equipment grouped logically based on resources, security or business requirements instead of their physical location.
virtual patching	A security measure designed to prevent known exploitation attempts against known vulnerabilities in web applications, typically via the use of a network-based intrusion prevention system or a web application firewall.
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 hardware or software resources.
volatile media	A type of media, such as random-access memory, which gradually loses its data when power is removed.
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.
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 tools. In each case, the goal is to identify as many 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.

Disclaimer

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

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

Copyright

© Commonwealth of Australia 2025

With the exception of the Coat of Arms and where otherwise stated, all material presented in this publication is provided under a Creative Commons Attribution 4.0 International license (https://creativecommons.org/licenses/by/4.0/).

For the avoidance of doubt, this means this license only applies to material as set out in this document.

The details of the relevant license conditions are available on the Creative Commons website as is the full legal code for the CC BY 4.0 license (https://creativecommons.org/licenses/by/4.0/legalcode.en).

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the Department of the Prime Minister and Cabinet website (https://www.pmc.gov.au/resources/commonwealth-coat-arms-information-and-guidelines).

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre