Information security manual

Guidelines for system hardening

Last updated: September 2026

Operating system hardening

Context

This section describes security controls applicable to operating systems used on workstations and servers. Guidance on the use of mobile operating systems is available in the 'Mobile device management' section of the *Guidelines for enterprise mobility*.

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. This includes 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 in not only 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 legacy 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: 6; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
64-bit versions of operating systems are used.

Standard operating environments

Allowing workstations and servers to be set up, configured and maintained outside of centrally managed processes 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 enabling them to be configured in an approved secure state 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. 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-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-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-2127; Revision: 0; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Digital signature verification functionality for drivers is enforced before they are loaded.

Control: ISM-1896; Revision: 0; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: ML3
Memory integrity functionality is enabled.

Control: ISM-2128; Revision: 0; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The ability to install, load or modify kernel-mode code, including drivers, kernel modules and extensions, is limited to privileged users who require such abilities as part of their duties or functions.

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: 4; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Unprivileged human 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 human users' ability to install any application can be exploited by malicious actors using social engineering 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 human users the ability to install approved applications from organisation-managed application repositories or from trustworthy application marketplaces. Furthermore, to prevent unprivileged human users from removing security functionality, or breaking system functionality, unprivileged human users should not have the ability to uninstall or disable approved applications.

Control: ISM-1592; Revision: 3; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Unprivileged human users do not have the ability to install unapproved applications.

Control: ISM-0382; Revision: 9; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Unprivileged human users do not have the ability to uninstall or disable approved applications.

Application control

Application control can be an effective way to both prevent malicious code from executing on workstations and servers and 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 at least annually.

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 cyber security 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: 2; Updated: Jun-26; Applicable: NC, OS, P, S, TS; Essential 8: ML2, ML3
Application control rulesets are validated at least annually.

Control: ISM-0846; Revision: 10; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Users cannot disable or bypass application control, and are not exempted from application control, except when using local administrator accounts or break glass accounts.

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 cyber security 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 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.

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 cyber security 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.

Windows Management Instrumentation

Malicious actors increasingly avoid deploying their own malware and instead live off the land by using management frameworks, such as Windows Management Instrumentation (WMI), that are already present on systems. As these management frameworks are required for legitimate administration activities, blocking them outright is often not feasible. As such, centrally logging and analysing WMI activity, including the creation of permanent event subscriptions, can assist in monitoring the security posture of systems, detecting malicious behaviour and contributing to investigations following cyber security incidents.

Control: ISM-2129; Revision: 0; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
WMI activity, including the creation of permanent event subscriptions, is centrally logged.

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 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: 6; Updated: Jun-26; 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 at least daily*
- *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 cyber security 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 usage, error messages and crashes
- 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 maintenance' 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 Microsoft's attack surface reduction rules can be found on Microsoft's attack surface reduction rules overview website.

Further information on exploit protection functionality within Microsoft Windows is available from Microsoft.

Further information on memory integrity functionality 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 'Security monitoring' section of the *Guidelines for security assurance*.

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

Context

This section describes security controls applicable to user applications typically installed on workstations, such as artificial intelligence (AI) applications, email clients, office productivity suites, Portable Document Format (PDF) applications, security products (e.g. antivirus applications, device access control applications, HIPS and software firewalls) and web browsers, including their extensions. Additional information on cloud-based versions of user applications can be found in the 'Managed services and cloud services' section of the *Guidelines for procurement and outsourcing*. 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. This includes 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 in not only 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. In addition, 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 email clients, office productivity suites, PDF applications, security products and web browsers, including their extensions.

Control: ISM-1467; Revision: 5; Updated: Jun-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The latest release of email clients, office productivity suites, PDF applications, security products and web browsers, including their extensions, 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. Many settings exist within user applications enabling them to be configured in an approved secure state to minimise this security risk. As such, ASD and vendors often produce hardening guidance to assist in hardening the configuration of user applications. 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-2110; Revision: 0; Updated: Jun-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
User applications are hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur.

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: 7; Updated: Jun-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Unneeded user accounts, components, services and functionality of user applications are disabled or removed.

Control: ISM-1235; Revision: 6; Updated: Jun-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Extensions for user applications are restricted to an organisation-approved set.

Control: ISM-2111; Revision: 0; Updated: Jun-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
All temporary installation files created during user application installation processes are removed after user applications have been installed.

Artificial intelligence applications

Allowing AI applications that process classified data to directly access external public data sources, such as by performing web searches, or accessing third-party cloud services or application programming interfaces, could lead to data spills involving classified prompts or responses. For this reason, AI applications processing classified data should not be granted direct access to external public data sources.

Furthermore, allowing AI applications to perform sensitive or high-impact actions without human oversight could result in unintended cyber security incidents. For example, actions that change privileges, that disable security controls, that initiate financial commitments, that transfer data outside the system boundary or that are otherwise irreversible. In such cases, AI applications should show human users the proposed action, target, data being disclosed and expected consequences. Dual approval should be considered for exceptionally consequential actions.

Control: ISM-2112; Revision: 0; Updated: Jun-26; Applicable: OS, P, S, TS; Essential 8: N/A
AI applications that process classified data have their ability to directly access external public data sources disabled.

Control: ISM-2113; Revision: 1; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
AI applications are configured to require human approval before executing sensitive or high-impact actions.

Control: ISM-2114; Revision: 0; Updated: Jun-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Baselines of expected behaviour and performance for AI applications are established and monitored for unexpected deviations.

Email clients

Human users' ability to change the security settings of email clients can be exploited by malicious actors using social engineering. To prevent human users from removing security functionality, or breaking security functionality, human users should not have the ability to change security settings for email clients.

Control: ISM-1748; Revision: 2; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Email client security settings cannot be changed by human users.

Office productivity suites

When office productivity suites, such as Microsoft Office, 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 office productivity suites enabling them to be configured in an approved secure state to minimise this security risk. As such, ASD and vendors often produce hardening guidance to assist in hardening the configuration of office productivity suites. However, in situations where ASD and vendor hardening guidance conflicts, precedence should be given to implementing the most restrictive guidance.

In addition, human users' ability to change the security settings of office productivity suites can be exploited by malicious actors using social engineering. To prevent human users from removing security functionality, or breaking security functionality, human users should not have the ability to change security settings for office productivity suites.

Finally, 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 later to automate repetitive tasks. Macros are powerful tools that can be easily created by human users to improve their productivity. However, malicious actors can also create macros to perform a variety of malicious activities, such as assisting to compromise workstations to exfiltrate or deny access to data. To reduce this security risk, an organisation should disable Microsoft Office macros for human users that do not have a demonstrated business requirement and secure their use for those that do.

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-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-1823; Revision: 1; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: ML2, ML3
Office productivity suite security settings cannot be changed by human users.

Control: ISM-1671; Revision: 1; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: ML1, ML2, ML3
Microsoft Office macros are disabled for human 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: 3; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: ML3
Only privileged human 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: 1; Updated: Jun-26; Applicable: NC, OS, P, S, TS; Essential 8: ML3
Microsoft Office's list of trusted publishers is validated at least annually.

Control: ISM-1489; Revision: 1; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: ML1, ML2, ML3
Microsoft Office macro security settings cannot be changed by human users.

Portable Document Format applications

When PDF applications suites 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 PDF applications enabling them to be configured in an approved secure state to minimise this security risk. As such, ASD and vendors often produce hardening guidance to assist in hardening the configuration of PDF applications. However, in situations where ASD and vendor hardening guidance conflicts, precedence should be given to implementing the most restrictive guidance.

In addition, human users' ability to change the security settings of PDF applications can be exploited by malicious actors using social engineering. To prevent human users from removing security functionality, or breaking security functionality, human users should not have the ability to change the security settings for PDF applications.

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: 2; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: ML2, ML3
PDF application security settings cannot be changed by human users.

Security products

Human users' ability to change the security settings of security products can be exploited by malicious actors using social engineering. To prevent human users from removing security functionality, or breaking security functionality, human users should not have the ability to change security settings for security products.

Control: ISM-1825; Revision: 1; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Security product security settings cannot be changed by human users.

Web browsers

When web browsers 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 web browsers enabling them to be configured in an approved secure state to minimise this security risk. As such, ASD and vendors often produce hardening guidance to assist in hardening the configuration of web browsers. However, in situations where ASD and vendor hardening guidance conflicts, precedence should be given to implementing the most restrictive guidance.

In addition, human users' ability to change the security settings of web browsers can be exploited by malicious actors using social engineering. To prevent human users from removing security functionality, or breaking security functionality, human users should not have the ability to change the security settings for web browsers.

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: 3; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: ML1, ML2, ML3
Web browser security settings cannot be changed by human 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 maintenance' section of the *Guidelines for system management*.

Further information on the use of AI agents can be found in ASD's *Careful adoption of agentic AI services* publication.

Further information on hardening AI applications can be found in the United States' National Security Agency's *Deploying AI Systems Securely: Best Practices for Deploying Secure and Resilient AI Systems* publication.

Further information on hardening Microsoft Office can be found in ASD's *Hardening Microsoft 365, Office 2021, Office 2019 and Office 2016* and *Restricting Microsoft Office macros* publications.

Further information on hardening Microsoft Office can also be found on the Microsoft Security Baselines Blog website.

Further information on hardening Adobe Reader and Adobe Acrobat can be found in Adobe's *Security Configuration Guide for Acrobat* publication.

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 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)*.

Server application hardening

Context

This section describes security controls 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. This includes 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 in not only 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. In addition, 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.

Control: ISM-1483; Revision: 3; Updated: Jun-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The latest release of internet-facing server applications is 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. Many settings exist within server applications enabling them to be configured in an approved secure state to minimise this security risk. As such, ASD and vendors often produce hardening guidance to

assist in hardening the configuration of server applications. 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-2115; Revision: 0; Updated: Jun-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Extensions for server applications are restricted to an organisation-approved set.

Control: ISM-1245; Revision: 4; Updated: Jun-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
All temporary installation files 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 cyber security incidents.

Control: ISM-1926; Revision: 1; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Microsoft AD DS domain controllers, Microsoft AD CS 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: 1; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Access to Microsoft AD DS domain controllers, Microsoft AD CS servers, Microsoft AD FS servers and Microsoft Entra Connect servers is limited to privileged users that require access.

Control: ISM-1928; Revision: 2; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Backups of Microsoft AD DS domain controllers, Microsoft AD CS servers, Microsoft AD FS servers and Microsoft Entra Connect servers are encrypted using ASD-approved cryptography, stored securely and only accessible to backup administrator accounts.

Control: ISM-1830; Revision: 3; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Security-relevant events for Microsoft AD DS domain controllers, Microsoft AD CS servers, Microsoft AD FS servers and Microsoft Entra Connect servers are centrally logged.

Microsoft Active Directory Domain Services

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 security 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 obtain credentials for a user account, along with associated system access, they may further compromise the system by querying Microsoft AD DS to assist in 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: 1; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
User accounts with DCSync permissions are reviewed at least every six months, 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-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 several 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, 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: 1; Updated: Jun-26; 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: 1; Updated: Jun-26; 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: 1; Updated: Jun-26; 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: 1; Updated: Jun-26; 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, and presents significant opportunities for privilege escalation and persistence by malicious actors. As such, particular care should be taken to secure

servers that perform this role. For example, in addition to baseline configuration hardening, web-based enrolment interfaces should be disabled or hardened against authentication-relay attacks, certificate templates should be periodically audited, and certificate enrolment activity should be centrally logged.

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 certification authority 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: 1; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Certificate manager approval is required for certificate templates that allow a Subject Alternative Name to be supplied.

Control: ISM-2130; Revision: 0; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Web-based enrolment interfaces for Microsoft AD CS servers are disabled unless required, and where enabled, are configured to require HTTPS and Extended Protection for Authentication.

Control: ISM-2131; Revision: 0; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Certificate templates are reviewed at least every three months to identify and remediate misconfigurations that could enable privilege escalation or unauthorised certificate enrolment.

Control: ISM-2132; Revision: 0; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Certificate enrolment events, including successful and unsuccessful requests and changes to certificate templates or Microsoft AD CS configurations, are centrally logged.

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 cyber security 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 maintenance' section of the *Guidelines for system management*.

Further information on the use of privileged user accounts can be found in the 'Identity and access management' section of the *Guidelines for system access*.

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 'Security monitoring' section of the *Guidelines for security assurance*.

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*.

Virtualisation hardening

Context

This section describes security controls 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. 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.

Furthermore, containers enable versatile deployment of systems and, in doing so, should be treated the same as any other system. However, security controls in a containerised environment may take a different form when compared to other types of systems. For example, patching the operating system of a workstation may be performed differently to ensuring that a patched image is used for a container, however, the principle is the same. In general, the same security risks that apply to non-containerised systems will likely apply to containerised systems.

Functional separation between operating environments

Physical computing resources can be shared among multiple operating environments via software-based isolation mechanisms. In doing so, an operating environment only has access to the virtual resources provided via the software-based isolation mechanism. In some cases, multiple layers of virtualisation, known as nested virtualisation, can exist. This is particularly prevalent with cloud services.

Examples of software-based isolation include:

- an operating system installed in a virtual machine where the isolation mechanism is a hypervisor, such as an Infrastructure as a Service offering
- an application that uses the shared kernel of the underlying operating system of the physical computing resource where the isolation mechanism is an application container or application sandbox, such as a Platform as a Service offering
- a containerised service hosted in a cloud environment, such as a Platform as a Service offering.

The logical separation of data within a single application, such as a Software as a Service offering, is not considered the same as multiple operating environments.

Malicious actors who have compromised a single operating environment, or who legitimately control a single operating environment, might exploit a misconfiguration or vulnerability in an underlying software-based isolation mechanism. This can lead to the compromise of other operating environments that share the same software-based isolation mechanism or the compromise of the underlying operating system of

the physical computing resource. As such, it is important that additional security controls be implemented when using a software-based isolation mechanism that consumes shared physical computing resources.

Control: ISM-1460; Revision: 6; Updated: Jun-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
When using a software-based isolation mechanism that consumes shared physical computing resources, 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: 1; Updated: Jun-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
When using a software-based isolation mechanism that consumes shared physical computing resources, 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: 2; Updated: Jun-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
When using a software-based isolation mechanism that consumes shared physical computing resources, the underlying operating system is hardened.

Control: ISM-1606; Revision: 3; Updated: Jun-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
When using a software-based isolation mechanism that consumes shared physical computing resources, 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: 1; Updated: Jun-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
When using a software-based isolation mechanism that consumes shared physical computing resources, the isolation mechanism or underlying operating system is replaced when it is no longer supported by a vendor.

Control: ISM-1607; Revision: 2; Updated: Jun-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
When using a software-based isolation mechanism that consumes shared physical resources, integrity monitoring and centralised event logging is performed for the isolation mechanism and underlying operating system.

Control: ISM-1461; Revision: 6; Updated: Jun-26; Applicable: S, TS; Essential 8: N/A
When using a software-based isolation mechanism that consumes shared physical computing resources for SECRET or TOP SECRET operating environments, the physical server and all operating 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 maintenance' section of the *Guidelines for system management*.

Further information on event logging can be found in the 'Security monitoring' section of the *Guidelines for security assurance*.

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*.

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

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