Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

# Information Security Manual

**Published:** 22 June 2023

# 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, use of memory-safe programming languages where possible (such as C#, Go, Java, Ruby, Rust and Swift), secure programming practices, and maintaining the security of their products. This will assist not only with reducing the potential number of security vulnerabilities in operating systems, but also increasing the likelihood that timely patches, updates or vendor mitigations will be released to remediate any security vulnerabilities that are found.

***Control: ISM-1743; Revision: 1; Updated: Mar-23; Applicability: All; Essential Eight: N/A***
*Operating systems are chosen from vendors that have demonstrated a commitment to secure-by-design and secure-by-default principles, use of memory-safe programming languages where possible, secure programming practices, and maintaining the security of their products.*

### Operating system releases and versions

Newer releases of operating systems often introduce improvements in security functionality. This can make it more difficult for an adversary to craft reliable exploits for security vulnerabilities they discover. Using older releases of operating systems, especially those no longer supported by vendors, may expose an organisation to security vulnerabilities or exploitation techniques that have since been mitigated. In addition, 64-bit versions of operating systems support additional security functionality that 32-bit versions do not.

***Control: ISM-1407; Revision: 5; Updated: Dec-22; Applicability: All; Essential Eight: ML3***
*The latest release, or the previous release, of operating systems are used.*

***Control: ISM-1408; Revision: 5; Updated: Dec-22; Applicability: All; Essential Eight: 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 an adversary in gaining an initial foothold on networks due to the higher likelihood of poorly configured or maintained workstations and servers. Conversely, a Standard Operating Environment (SOE), 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 trusted third parties while also scanning them for malicious code and configurations.

As operating environments naturally change over time, such as patches or updates are applied, configurations are changed, and applications are added or removed, it is essential that SOEs are reviewed and updated at least annually to ensure that an up-to-date baseline is maintained.

***Control: ISM-1406; Revision: 2; Updated: Aug-20; Applicability: All; Essential Eight: N/A***
*SOEs are used for workstations and servers.*

***Control: ISM-1608; Revision: 1; Updated: Mar-22; Applicability: All; Essential Eight: N/A***
*SOEs provided by third parties are scanned for malicious code and configurations.*

***Control: ISM-1588; Revision: 0; Updated: Aug-20; Applicability: All; Essential Eight: N/A***
*SOEs are reviewed and updated at least annually.*

## Hardening operating system configurations

When operating systems are deployed in their default state it can lead to an insecure operating environment that may allow an adversary to gain an initial foothold on networks. Many configuration settings exist within operating systems to allow them to be configured in a secure state in order to minimise this security risk. As such, the Australian Cyber Security Centre (ACSC) and vendors often produce hardening guidance to assist in hardening the configuration of operating systems. Note, however, in situations where ACSC and vendor hardening guidance conflicts, preference should be given to implementing ACSC hardening guidance.

***Control: ISM-1409; Revision: 2; Updated: Jun-23; Applicability: All; Essential Eight: N/A***
*ACSC and vendor hardening guidance for operating systems is implemented.*

***Control: ISM-0380; Revision: 9; Updated: Mar-22; Applicability: All; Essential Eight: N/A***
*Unneeded accounts, components, services and functionality of operating systems are disabled or removed.*

***Control: ISM-0383; Revision: 8; Updated: Dec-22; Applicability: All; Essential Eight: N/A***
*Default accounts or credentials for operating systems, including for any pre-configured accounts, are changed.*

***Control: ISM-0341; Revision: 4; Updated: Dec-21; Applicability: All; Essential Eight: N/A***
*Automatic execution features for removable media are disabled.*

***Control: ISM-1654; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML3***
*Internet Explorer 11 is disabled or removed.*

***Control: ISM-1655; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML3***
*.NET Framework 3.5 (includes .NET 2.0 and 3.0) is disabled or removed.*

***Control: ISM-1492; Revision: 2; Updated: Mar-22; Applicability: All; Essential Eight: N/A***
*Operating system exploit protection functionality is enabled.*

***Control: ISM-1745; Revision: 0; Updated: Mar-22; Applicability: All; Essential Eight: N/A***
*Early Launch Antimalware, Secure Boot, Trusted Boot and Measured Boot functionality is enabled.*

***Control: ISM-1584; Revision: 1; Updated: Sep-21; Applicability: All; Essential Eight: N/A***
*Unprivileged users are prevented from bypassing, disabling or modifying security functionality of operating systems.*

***Control: ISM-1491; Revision: 3; Updated: Mar-22; Applicability: All; Essential Eight: N/A***
*Unprivileged users are prevented from running script execution engines, including:*

- *Windows Script Host (cscript.exe and wscript.exe)*
- *PowerShell (powershell.exe, powershell_ise.exe and pwsh.exe)*

- *Command Prompt (cmd.exe)*
- *Windows Management Instrumentation (wmic.exe)*
- *Microsoft Hypertext Markup Language (HTML) Application Host (mshta.exe).*

## Application management

Unprivileged users' ability to install any application can be exploited by an adversary using social engineering in order to convince them to install a malicious application. One way to mitigate this security risk, while also removing burden from system administrators, is to allow unprivileged users the ability to install approved applications from organisation-managed software repositories or from trusted application marketplaces. Furthermore, to prevent unprivileged users from removing security functionality, or breaking system functionality, unprivileged users should not have the ability to uninstall or disable approved software.

***Control: ISM-1592; Revision: 1; Updated: Mar-22; Applicability: All; Essential Eight: N/A***
*Unprivileged users do not have the ability to install unapproved software.*

***Control: ISM-0382; Revision: 7; Updated: Mar-22; Applicability: All; Essential Eight: N/A***
*Unprivileged users do not have the ability to uninstall or disable approved software.*

## Application control

Application control can be an effective way to not only prevent malicious code from executing on workstations and servers, but also to ensure only approved applications can execute. When developing application control rulesets, determining approved executables (e.g. .exe and .com files), software libraries (e.g. .dll and.ocx files), scripts (e.g. .ps1, .bat, .cmd, .vbs and .js files), installers (e.g. .msi, .msp and .mst files), compiled HTML (e.g. .chm 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 an adversary.

Finally, application control event logs can assist in monitoring the security posture of systems, detecting malicious behaviour and contributing to investigations following cyber security incidents. To facilitate such activities, application control event logs should be captured and stored centrally.

***Control: ISM-0843; Revision: 9; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3***
*Application control is implemented on workstations.*

***Control: ISM-1490; Revision: 3; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3***
*Application control is implemented on internet-facing servers.*

***Control: ISM-1656; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML3***
*Application control is implemented on non-internet-facing servers.*

***Control: ISM-1657; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3***
*Application control restricts the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets to an organisation-approved set.*

***Control: ISM-1658; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML3***
*Application control restricts the execution of drivers to an organisation-approved set.*

***Control: ISM-0955; Revision: 6; Updated: Apr-20; Applicability: All; Essential Eight: N/A***

*Application control is implemented using cryptographic hash rules, publisher certificate rules or path rules.*

***Control: ISM-1582; Revision: 1; Updated: Sep-21; Applicability: All; Essential Eight: ML3***
*Application control rulesets are validated on an annual or more frequent basis.*

***Control: ISM-1471; Revision: 2; Updated: Apr-20; Applicability: All; Essential Eight: N/A***
*When implementing application control using publisher certificate rules, both publisher names and product names are used.*

***Control: ISM-1392; Revision: 4; Updated: Mar-23; Applicability: All; Essential Eight: 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; Applicability: All; Essential Eight: 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: 2; Updated: Sep-21; Applicability: All; Essential Eight: ML3***
*Microsoft's 'recommended block rules' are implemented.*

***Control: ISM-1659; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML3***
*Microsoft's 'recommended driver block rules' are implemented.*

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

***Control: ISM-1660; Revision: 1; Updated: Dec-22; Applicability: All; Essential Eight: ML2, ML3***
*Allowed and blocked execution events on workstations are logged.*

***Control: ISM-1661; Revision: 1; Updated: Dec-22; Applicability: All; Essential Eight: ML2, ML3***
*Allowed and blocked execution events on internet-facing servers are logged.*

***Control: ISM-1662; Revision: 1; Updated: Dec-22; Applicability: All; Essential Eight: ML3***
*Allowed and blocked execution events on non-internet-facing servers are logged.*

***Control: ISM-1663; Revision: 1; Updated: Dec-22; Applicability: All; Essential Eight: ML3***
*Application control event logs are stored centrally.*

## PowerShell

PowerShell is a powerful scripting language developed by Microsoft and, due to its ubiquity and ease with which it can be used to fully control operating systems, is an important part of system administrator toolkits. However, PowerShell can also be a dangerous exploitation tool in the hands of an adversary.

In order to prevent attacks leveraging security vulnerabilities in earlier PowerShell versions, Windows PowerShell 2.0 should be disabled or removed from operating systems. Additionally, PowerShell's language mode should be set to Constrained Language Mode to achieve a balance between security and functionality.

Finally, PowerShell event logs can assist in monitoring the security posture of systems, detecting malicious behaviour and contributing to investigations following cyber security incidents. To facilitate such activities, PowerShell event logs should be captured and stored centrally.

***Control: ISM-1621; Revision: 1; Updated: Sep-21; Applicability: All; Essential Eight: ML3***
*Windows PowerShell 2.0 is disabled or removed.*

***Control: ISM-1622; Revision: 0; Updated: Oct-20; Applicability: All; Essential Eight: ML3***
*PowerShell is configured to use Constrained Language Mode.*

***Control: ISM-1623; Revision: 0; Updated: Oct-20; Applicability: All; Essential Eight: N/A***

*PowerShell is configured to use module logging, script block logging and transcription functionality.*

***Control: ISM-1624; Revision: 0; Updated: Oct-20; Applicability: All; Essential Eight: N/A***
*PowerShell script block logs are protected by Protected Event Logging functionality.*

***Control: ISM-1664; Revision: 1; Updated: Dec-22; Applicability: All; Essential Eight: ML2, ML3***
*Blocked PowerShell script execution events are logged.*

***Control: ISM-1665; Revision: 1; Updated: Dec-22; Applicability: All; Essential Eight: ML3***
*PowerShell event logs are stored centrally.*

### Host-based Intrusion Prevention System

Many security products rely on signatures to detect malicious code. This approach is only effective when malicious code has already been profiled and signatures are available from security vendors. Unfortunately, an adversary can easily create variants of known malicious code in order to bypass traditional signature-based detection. A Host-based Intrusion Prevention System (HIPS) can use behaviour-based detection to assist in identifying and blocking anomalous behaviour as well as detecting malicious code that has yet to be identified by security vendors. As such, it is important that a HIPS is implemented on workstations, critical servers and high-value servers.

***Control: ISM-1341; Revision: 2; Updated: Sep-18; Applicability: All; Essential Eight: N/A***
*A HIPS is implemented on workstations.*

***Control: ISM-1034; Revision: 7; Updated: Mar-22; Applicability: All; Essential Eight: N/A***
*A HIPS is implemented on critical servers and high-value servers.*

### Software firewall

Traditional network firewalls often fail to prevent the propagation of malicious code on networks, or an adversary from exfiltrating data from networks, as they only control which ports or protocols can be used between different network segments. Many forms of malicious code are designed specifically to take advantage of this by using common protocols, such as Hypertext Transfer Protocol, Hypertext Transfer Protocol Secure, Simple Mail Transfer Protocol or Domain Name System. Software firewalls are more effective than traditional network firewalls as they can control which applications and services can communicate to and from workstations and servers. As such, a software firewall should be implemented on workstations and servers to restrict inbound and outbound network connections to an organisation-approved set of applications and services.

***Control: ISM-1416; Revision: 3; Updated: Mar-22; Applicability: All; Essential Eight: N/A***
*A software firewall is implemented on workstations and servers to restrict inbound and outbound network connections to an organisation-approved set of applications and services.*

### Antivirus software

When vendors develop software they may make coding mistakes that lead to security vulnerabilities. An adversary can take advantage of this by developing malicious code to exploit any security vulnerabilities that have not been detected and remedied by vendors. As significant time and effort is often involved in developing functioning and reliable exploits, an adversary will often attempt to reuse their exploits as much as possible. While exploits may have been previously identified by security vendors, they often remain viable against an organisation that does not have antivirus software in place.

***Control: ISM-1417; Revision: 4; Updated: Mar-22; Applicability: All; Essential Eight: N/A***
*Antivirus software is implemented on workstations and servers with:*

- *signature-based detection functionality enabled and set to a high level*
- *heuristic-based detection functionality enabled and set to a high level*

- *reputation rating functionality enabled*
- *ransomware protection functionality enabled*
- *detection signatures configured to update on at least a daily basis*
- *regular scanning configured for all fixed disks and removable media.*

## Device access control software

Device access control software can be used to prevent removable media and mobile devices from being 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 an adversary.

In addition, an adversary can connect to locked workstations and servers via external communication interfaces that allow Direct Memory Access (DMA). In doing so, the adversary can gain access to encryption keys in memory or write malicious code to memory. The best defence against this security risk is to disable access to external communication interfaces that allow DMA, such as FireWire, ExpressCard and Thunderbolt.

***Control: ISM-1418; Revision: 4; Updated: Mar-22; Applicability: All; Essential Eight: N/A***
*If there is no business requirement for reading from removable media and devices, such functionality is disabled via the use of device access control software or by disabling external communication interfaces.*

***Control: ISM-0343; Revision: 6; Updated: Mar-22; Applicability: All; Essential Eight: N/A***
*If there is no business requirement for writing to removable media and devices, such functionality is disabled via the use of device access control software or by disabling external communication interfaces.*

***Control: ISM-0345; Revision: 6; Updated: Dec-21; Applicability: All; Essential Eight: N/A***
*External communication interfaces that allow DMA are disabled.*

## Operating system event logging

Operating system events can assist in monitoring the security posture of systems, detecting malicious behaviour and contributing to investigations following cyber security incidents. To facilitate such activities, operating system event logs should be captured and stored centrally.

***Control: ISM-0582; Revision: 7; Updated: Mar-22; Applicability: All; Essential Eight: N/A***
*The following events are logged for operating systems:*

- *application and operating system crashes and error messages*
- *changes to security policies and system configurations*
- *successful user logons and logoffs, failed user logons and account lockouts*
- *failures, restarts and changes to important processes and services*
- *requests to access internet resources*
- *security product-related events*
- *system startups and shutdowns.*

***Control: ISM-1747; Revision: 1; Updated: Dec-22; Applicability: All; Essential Eight: N/A***
*Operating system event logs are stored centrally.*

## 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 patching or updating operating systems can be found in the system patching section of the *Guidelines for System Management*.

Further information on securely configuring Microsoft Windows operating systems can be found in the ACSC's *Hardening Microsoft Windows 10 version 21H1 Workstations* publication.

Further information on securely configuring Linux workstations and servers can be found in the ACSC's *Hardening Linux Workstations and Servers* publication.

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

Further information on implementing application control can be found in the ACSC's *Implementing Application Control* publication.

Further information on Microsoft's 'recommended block rules' and 'recommended driver block rules' are available from Microsoft.

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

Further information on the use of PowerShell by blue teams is available from Microsoft while further information on obtaining greater visibility through PowerShell logging is available from Mandiant.

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

Further information on independent testing of antivirus software is available from AV-Comparatives and AV-TEST.

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

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

## User application hardening

### User applications

This section is applicable to applications typically installed on user workstations, such as office productivity suites, web browsers and their extensions, email clients, Portable Document Format (PDF) software, and security products (e.g. antivirus software, device access control software, 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, use of memory-safe programming languages where possible (such as C#, Go, Java, Ruby, Rust and Swift), secure programming practices, and maintaining the security of their products. This will assist not only with reducing the potential number of security vulnerabilities in user applications, but also increasing the likelihood that timely patches, updates or vendor mitigations will be released to remediate any security vulnerabilities that are found.

***Control: ISM-0938; Revision: 6; Updated: Mar-23; Applicability: All; Essential Eight: N/A***
*User applications are chosen from vendors that have demonstrated a commitment to secure-by-design and secure-by-default principles, use of memory-safe programming languages where possible, secure programming practices, and maintaining the security of their products.*

## User application releases

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

***Control: ISM-1467; Revision: 3; Updated: Mar-22; Applicability: All; Essential Eight: N/A***
*The latest release of office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are used.*

## Hardening user application configurations

When user applications are deployed in their default state it can lead to an insecure operating environment that may allow an adversary to gain an initial foothold on networks. This can be especially risky for office productivity suites, web browsers and their extensions, email clients, PDF software, and security products as such applications are routinely targeted for exploitation. Many configuration settings exist within such applications to allow them to be configured in a secure state in order to minimise this security risk. As such, the ACSC and vendors often produce hardening guidance to assist in hardening the configuration of these applications. Note, however, in situations where ACSC and vendor hardening guidance conflicts, preference should be given to implementing ACSC hardening guidance.

***Control: ISM-1806; Revision: 1; Updated: Mar-23; Applicability: All; Essential Eight: N/A***
*Default accounts or credentials for user applications, including for any pre-configured accounts, are changed.*

***Control: ISM-1470; Revision: 5; Updated: Mar-22; Applicability: All; Essential Eight: N/A***
*Unneeded components, services and functionality of office productivity suites, web browsers, email clients, PDF software and security products are disabled or removed.*

***Control: ISM-1235; Revision: 4; Updated: Mar-22; Applicability: All; Essential Eight: N/A***
*Add-ons, extensions and plug-ins for office productivity suites, web browsers, email clients, PDF software and security products are restricted to an organisation-approved set.*

***Control: ISM-1667; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3***
*Microsoft Office is blocked from creating child processes.*

***Control: ISM-1668; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3***
*Microsoft Office is blocked from creating executable content.*

***Control: ISM-1669; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3***
*Microsoft Office is blocked from injecting code into other processes.*

***Control: ISM-1542; Revision: 0; Updated: Jan-19; Applicability: All; Essential Eight: ML2, ML3***
*Microsoft Office is configured to prevent activation of Object Linking and Embedding packages.*

***Control: ISM-1859; Revision: 0; Updated: Jun-23; Applicability: All; Essential Eight: ML2, ML3***
*ACSC or vendor hardening guidance for office productivity suites is implemented.*

***Control: ISM-1823; Revision: 0; Updated: Mar-23; Applicability: All; Essential Eight: ML2, ML3***
*Office productivity suite security settings cannot be changed by users.*

***Control: ISM-1486; Revision: 1; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3***
*Web browsers do not process Java from the internet.*

***Control: ISM-1485; Revision: 1; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3***
*Web browsers do not process web advertisements from the internet.*

***Control: ISM-1666; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML2***

*Internet Explorer 11 does not process content from the internet.*

***Control: ISM-1412; Revision: 4; Updated: Jun-23; Applicability: All; Essential Eight: ML2, ML3***
*ACSC or vendor hardening guidance for web browsers is implemented.*

***Control: ISM-1585; Revision: 2; Updated: Mar-23; Applicability: All; Essential Eight: ML2, ML3***
*Web browser security settings cannot be changed by users.*

***Control: ISM-1670; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3***
*PDF software is blocked from creating child processes.*

***Control: ISM-1860; Revision: 0; Updated: Jun-23; Applicability: All; Essential Eight: ML2, ML3***
*ACSC or vendor hardening guidance for PDF software is implemented.*

***Control: ISM-1824; Revision: 0; Updated: Mar-23; Applicability: All; Essential Eight: ML2, ML3***
*PDF software security settings cannot be changed by users.*

***Control: ISM-1601; Revision: 1; Updated: Mar-22; Applicability: All; Essential Eight: N/A***
*Microsoft's Attack Surface Reduction rules are implemented.*

***Control: ISM-1748; Revision: 1; Updated: Mar-23; Applicability: All; Essential Eight: N/A***
*Email client security settings cannot be changed by users.*

***Control: ISM-1825; Revision: 0; Updated: Mar-23; Applicability: All; Essential Eight: 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, an adversary can also create macros to perform a variety of malicious activities, such as assisting to compromise workstations in order to exfiltrate or deny access to data. To reduce this security risk, an organisation should disable Microsoft Office macros for users that do not have a demonstrated business requirement and secure their use for the remaining users that do.

Finally, Microsoft Office macro event logs can assist in monitoring the security posture of systems, detecting malicious behaviour and contributing to investigations following cyber security incidents. To facilitate such activities, Microsoft Office macro event logs should be captured and stored centrally.

***Control: ISM-1671; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3***
*Microsoft Office macros are disabled for users that do not have a demonstrated business requirement.*

***Control: ISM-1488; Revision: 1; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3***
*Microsoft Office macros in files originating from the internet are blocked.*

***Control: ISM-1672; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3***
*Microsoft Office macro antivirus scanning is enabled.*

***Control: ISM-1673; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3***
*Microsoft Office macros are blocked from making Win32 API calls.*

***Control: ISM-1674; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML3***
*Only Microsoft Office macros running from within a sandboxed environment, a Trusted Location or that are digitally signed by a trusted publisher are allowed to execute.*

***Control: ISM-1487; Revision: 1; Updated: Sep-21; Applicability: All; Essential Eight: ML3***
*Only privileged users responsible for validating that Microsoft Office macros are free of malicious code can write to and modify content within Trusted Locations.*

***Control: ISM-1675; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML3***
*Microsoft Office macros digitally signed by an untrusted publisher cannot be enabled via the Message Bar or Backstage View.*

***Control: ISM-1676; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML3***
*Microsoft Office's list of trusted publishers is validated on an annual or more frequent basis.*

***Control: ISM-1489; Revision: 0; Updated: Sep-18; Applicability: All; Essential Eight: ML2, ML3***
*Microsoft Office macro security settings cannot be changed by users.*

***Control: ISM-1677; Revision: 1; Updated: Dec-22; Applicability: All; Essential Eight: ML2, ML3***
*Allowed and blocked Microsoft Office macro execution events are logged.*

***Control: ISM-1678; Revision: 1; Updated: Dec-22; Applicability: All; Essential Eight: ML3***
*Microsoft Office macro event logs are stored centrally.*

### 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 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 securely configuring Microsoft Office can be found in the ACSC's *Hardening Microsoft 365, Office 2021, Office 2019 and Office 2016* publication.

Further information on securely configuring the Microsoft Edge web browser can be found in the ACSC's *Hardening Microsoft Windows 10 version 21H1 Workstations* publication.

Further information on configuring Microsoft Office macro settings can be found in the ACSC's *Microsoft Office Macro Security* publication.

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

## Server application hardening

### Server applications

This section is applicable to applications associated with specific server functionality, such as Microsoft Active Directory Domain Services (AD DS), database management system software, email server software and web hosting software. 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, use of memory-safe programming languages where possible (such as C#, Go, Java, Ruby, Rust and Swift), secure programming practices, and maintaining the security of their products. This will assist not only with reducing the potential number of security vulnerabilities in server applications, but also increasing the likelihood that timely patches, updates or vendor mitigations will be released to remediate any security vulnerabilities that are found.

***Control: ISM-1826; Revision: 0; Updated: Mar-23; Applicability: All; Essential Eight: N/A***

*Server applications are chosen from vendors that have demonstrated a commitment to secure-by-design and secure-by-default principles, use of memory-safe programming languages where possible, secure programming practices, and maintaining the security of their products.*

### Server application releases

Newer releases of server applications often introduce improvements in security functionality. This can make it more difficult for an adversary to craft reliable exploits for security vulnerabilities they discover. Using older releases of server applications, especially those no longer supported by vendors, may expose an organisation to security vulnerabilities or exploitation techniques that have since been mitigated. This is particularly important for internet-facing server applications, such as web hosting software.

***Control: ISM-1483; Revision: 2; Updated: Mar-23; Applicability: All; Essential Eight: 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 it can lead to an insecure operating environment that may allow an adversary to gain an initial foothold on networks. This can be especially risky for server applications as such applications are routinely targeted for exploitation. Many configuration settings exist within server applications to allow them to be configured in a secure state in order to minimise this security risk. As such, the ACSC and vendors often produce hardening guidance to assist in hardening the configuration of server applications. Note, however, in situations where ACSC and vendor hardening guidance conflicts, preference should be given to implementing ACSC hardening guidance.

***Control: ISM-1246; Revision: 4; Updated: Jun-23; Applicability: All; Essential Eight: N/A***
*ACSC and vendor hardening guidance for server applications is implemented.*

***Control: ISM-1260; Revision: 4; Updated: Mar-23; Applicability: All; Essential Eight: N/A***
*Default accounts or credentials for server applications, including for any pre-configured accounts, are changed.*

***Control: ISM-1247; Revision: 4; Updated: Mar-23; Applicability: All; Essential Eight: N/A***
*Unneeded accounts, components, services and functionality of server applications are disabled or removed.*

***Control: ISM-1245; Revision: 3; Updated: Mar-23; Applicability: All; Essential Eight: 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 an adversary, 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 an adversary compromise the server application.

***Control: ISM-1249; Revision: 3; Updated: Mar-23; Applicability: All; Essential Eight: N/A***
*Server applications are configured to run as a separate account with the minimum privileges needed to perform their functions.*

***Control: ISM-1250; Revision: 2; Updated: Mar-23; Applicability: All; Essential Eight: N/A***
*The accounts under which server applications run have limited access to their underlying server’s file system.*

### 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.

Finally, security-related events for Microsoft AD DS can assist in monitoring the security posture of systems, detecting malicious behaviour and contributing to investigations following cyber security incidents. To facilitate such activities, Microsoft AD DS event logs should be captured and stored centrally.

***Control: ISM-1827; Revision: 0; Updated: Mar-23; Applicability: All; Essential Eight: 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-1828; Revision: 0; Updated: Mar-23; Applicability: All; Essential Eight: N/A***
*The Print Spooler service is disabled on Microsoft AD DS domain controllers.*

***Control: ISM-1829; Revision: 0; Updated: Mar-23; Applicability: All; Essential Eight: N/A***
*Passwords and cpasswords are not used in Group Policy Preferences.*

***Control: ISM-1830; Revision: 0; Updated: Mar-23; Applicability: All; Essential Eight: N/A***
*Security-related events for Microsoft AD DS are logged.*

***Control: ISM-1831; Revision: 0; Updated: Mar-23; Applicability: All; Essential Eight: N/A***
*Microsoft AD DS event logs are stored centrally.*

## Microsoft Active Directory Domain Services account hardening

Misconfigured user accounts within Microsoft AD DS can pose a significant threat to the security of a system. For example, when an adversary is 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 accounts. Furthermore, an adversary with this level of access can become difficult to detect and remove, as they may not need to use exploits for security vulnerabilities to achieve their goals. Malicious activities performed by compromised user accounts may also appear very similar to legitimate system activities.

***Control: ISM-1832; Revision: 0; Updated: Mar-23; Applicability: All; Essential Eight: N/A***
*Only service accounts and computer accounts are configured with Service Principal Names (SPNs).*

***Control: ISM-1833; Revision: 0; Updated: Mar-23; Applicability: All; Essential Eight: N/A***
*Service accounts are provisioned with the minimum privileges required and are not members of the domain administrators group or similar highly privileged groups.*

***Control: ISM-1834; Revision: 0; Updated: Mar-23; Applicability: All; Essential Eight: N/A***
*Duplicate SPNs do not exist within the domain.*

***Control: ISM-1835; Revision: 0; Updated: Mar-23; Applicability: All; Essential Eight: N/A***
*Privileged user accounts are configured as sensitive and cannot be delegated.*

***Control: ISM-1836; Revision: 0; Updated: Mar-23; Applicability: All; Essential Eight: N/A***
*User accounts require Kerberos pre-authentication.*

***Control: ISM-1837; Revision: 0; Updated: Mar-23; Applicability: All; Essential Eight: N/A***
*User accounts are not configured with password never expires or password not required.*

***Control: ISM-1838; Revision: 0; Updated: Mar-23; Applicability: All; Essential Eight: N/A***
*The UserPassword attribute for user accounts is not used.*

***Control: ISM-1839; Revision: 0; Updated: Mar-23; Applicability: All; Essential Eight: N/A***
*Account properties accessible by unprivileged users are not used to store passwords.*

***Control: ISM-1840; Revision: 0; Updated: Mar-23; Applicability: All; Essential Eight: N/A***
*User account passwords do not use reversible encryption.*

***Control: ISM-1841; Revision: 0; Updated: Mar-23; Applicability: All; Essential Eight: N/A***
*Unprivileged user accounts cannot add machines to the domain.*

***Control: ISM-1842; Revision: 0; Updated: Mar-23; Applicability: All; Essential Eight: N/A***
*Dedicated service accounts are used to add machines to the domain.*

***Control: ISM-1843; Revision: 0; Updated: Mar-23; Applicability: All; Essential Eight: N/A***
*User accounts with unconstrained delegation are reviewed at least annually, and those without an associated Kerberos SPN or demonstrated business requirement are removed.*

***Control: ISM-1844; Revision: 0; Updated: Mar-23; Applicability: All; Essential Eight: N/A***
*Computer accounts that are not Microsoft AD DS domain controllers are not trusted for delegation to services.*

## 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 an adversary to more easily move laterally throughout a network, or escalate their privileges. Privileged security groups in particular should be limited to the smallest set of possible users to limit an adversary's opportunities for privilege escalation.

***Control: ISM-1620; Revision: 1; Updated: Mar-23; Applicability: All; Essential Eight: N/A***
*Privileged user accounts are members of the Protected Users security group.*

***Control: ISM-1845; Revision: 0; Updated: Mar-23; Applicability: All; Essential Eight: N/A***
*When a user account is disabled, it is removed from all security group memberships.*

***Control: ISM-1846; Revision: 0; Updated: Mar-23; Applicability: All; Essential Eight: N/A***
*The Pre-Windows 2000 Compatible Access security group does not contain user accounts.*

## 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 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 accounts can be found in the access to systems and their resources section of the *Guidelines for Personnel Security*.

Further information on securely configuring Microsoft AD DS can be found in Microsoft's *Best Practices for Securing Active Directory* publication.

Further information on recommended security-related events to monitor for Microsoft AD DS can be found in Microsoft's *Events to monitor* 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 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

### Account and authentication types

The guidance within this section is equally applicable to all account types unless specified otherwise. This includes unprivileged accounts, privileged accounts, break glass accounts and service accounts. In addition, the guidance is equally applicable to interactive authentication and non-interactive authentication.

### Authenticating to systems

Before access to a system and its resources is granted to a user, it is essential that they are authenticated. This can be achieved via multi-factor authentication, such as a username along with a passphrase and security key, or via single-factor authentication, such as a username and a passphrase.

***Control: ISM-1546; Revision: 0; Updated: Aug-19; Applicability: All; Essential Eight: N/A***
*Users are authenticated before they are granted access to a system and its resources.*

### 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; Applicability: All; Essential Eight: N/A***
*Authentication methods susceptible to replay attacks are disabled.*

***Control: ISM-1055; Revision: 4; Updated: Oct-20; Applicability: All; Essential Eight: 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, smartphone or one-time password token
- something users are, such as a fingerprint pattern or their facial geometry.

Note, however, that if a memorised secret is written down, or stored in a document on a system, this becomes something that users have rather than something users know.

Privileged users, users of remote access solutions and users with access to important data repositories are more likely to be targeted by an adversary due to their access. For this reason, it is especially important that multi-factor authentication is used for these accounts. In addition, multi-factor authentication is vital to any administrative activities as it can limit the consequences of a compromise by preventing or slowing an adversary’s ability to gain unrestricted access to assets. In this regard, multi-factor authentication can be implemented as part of jump server authentication where assets being administered do not support multi-factor authentication themselves.

When implementing multi-factor authentication, several different authentication factors can be implemented. Unfortunately, some authentication factors, such as biometrics or codes sent via Short Message Service, Voice over Internet Protocol or email, are more susceptible to compromise than others. For this reason, authentication factors that involve something 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, multi-factor authentication event logs can assist in monitoring the security posture of systems, detecting malicious behaviour and contributing to investigations following cyber security incidents. To facilitate such activities, multi-factor authentication event logs should be captured and stored centrally.

***Control: ISM-0974; Revision: 6; Updated: Sep-21; Applicability: All; Essential Eight: N/A***
*Multi-factor authentication is used to authenticate unprivileged users of systems.*

***Control: ISM-1173; Revision: 4; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3***
*Multi-factor authentication is used to authenticate privileged users of systems.*

***Control: ISM-1504; Revision: 1; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3***
*Multi-factor authentication is used by an organisation's users if they authenticate to their organisation's internet-facing services.*

***Control: ISM-1679; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3***
*Multi-factor authentication is used by an organisation's users if they authenticate to third-party internet-facing services that process, store or communicate their organisation's sensitive data.*

***Control: ISM-1680; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3***
*Multi-factor authentication (where available) is used by an organisation's users if they authenticate to third-party internet-facing services that process, store or communicate their organisation's non-sensitive data.*

***Control: ISM-1681; Revision: 1; Updated: Jun-23; Applicability: All; Essential Eight: ML2, ML3***
*Multi-factor authentication is enabled by default for an organisation's non-organisational users (but users can choose to opt out) if they authenticate to the organisation's internet-facing services.*

***Control: ISM-1505; Revision: 1; Updated: Sep-21; Applicability: All; Essential Eight: ML3***
*Multi-factor authentication is used to authenticate users accessing important data repositories.*

***Control: ISM-1401; Revision: 5; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3***
*Multi-factor authentication uses either: something users have and something users know, or something users have that is unlocked by something users know or are.*

***Control: ISM-1682; Revision: 1; Updated: Mar-23; Applicability: All; Essential Eight: ML3***
*Multi-factor authentication is phishing-resistant.*

***Control: ISM-1559; Revision: 2; Updated: Mar-22; Applicability: All; Essential Eight: N/A***
*Memorised secrets used for multi-factor authentication are a minimum of 6 characters, unless more stringent requirements apply.*

***Control: ISM-1560; Revision: 2; Updated: Mar-22; Applicability: S; Essential Eight: N/A***
*Memorised secrets used for multi-factor authentication on SECRET systems are a minimum of 8 characters.*

***Control: ISM-1561; Revision: 2; Updated: Mar-22; Applicability: TS; Essential Eight: N/A***
*Memorised secrets used for multi-factor authentication on TOP SECRET systems are a minimum of 10 characters.*

***Control: ISM-1683; Revision: 1; Updated: Dec-22; Applicability: All; Essential Eight: ML2, ML3***
*Successful and unsuccessful multi-factor authentication events are logged.*

***Control: ISM-1684; Revision: 1; Updated: Dec-22; Applicability: All; Essential Eight: ML3***
*Multi-factor authentication event logs are stored centrally.*

## Single-factor authentication

A significant threat to the compromise of accounts is credential cracking tools. When an adversary gains access to a list of usernames and hashed credentials from a system they can attempt to recover username and credential pairs by comparing the hashes of known credentials with the hashed credentials they have gained access to. By finding a match an adversary will know the credential associated with a given username.

In order to reduce this security risk, an organisation should implement multi-factor authentication. Note, while single-factor authentication is no longer considered suitable for protecting sensitive or classified data, it may not be possible to implement multi-factor authentication on some systems. In such cases, an organisation will need to increase the time on average it takes an adversary to compromise a credential by continuing to increase its length over time. Such increases in length can be balanced against useability through the use of passphrases rather than passwords. In cases where systems do not support passphrases, and as an absolute last resort, the strongest password length and complexity supported by a system will need to be implemented.

***Control: ISM-0417; Revision: 5; Updated: Oct-19; Applicability: All; Essential Eight: N/A***
*When systems cannot support multi-factor authentication, single-factor authentication using passphrases is implemented instead.*

***Control: ISM-0421; Revision: 8; Updated: Dec-21; Applicability: All; Essential Eight: N/A***
*Passphrases used for single-factor authentication are at least 4 random words with a total minimum length of 14 characters, unless more stringent requirements apply.*

***Control: ISM-1557; Revision: 2; Updated: Dec-21; Applicability: S; Essential Eight: N/A***
*Passphrases used for single-factor authentication on SECRET systems are at least 5 random words with a total minimum length of 17 characters.*

***Control: ISM-0422; Revision: 8; Updated: Dec-21; Applicability: TS; Essential Eight: N/A***
*Passphrases used for single-factor authentication on TOP SECRET systems are at least 6 random words with a total minimum length of 20 characters.*

***Control: ISM-1558; Revision: 2; Updated: Mar-22; Applicability: All; Essential Eight: N/A***
*Passphrases used for single-factor authentication are not a list of categorised words; do not form a real sentence in a natural language; and are not constructed from song lyrics, movies, literature or any other publicly available material.*

## Setting credentials for user accounts

Before new credentials are issued for user accounts, it is important that users' provide sufficient evidence to verify their identity, such as by users physically presenting themselves and their pass to a service desk or by answering a set of challenge-response questions. Following the verification of user identity, credentials should be randomly generated and provided to users via a secure communications channel or, if not possible, split into two parts with one part provided to users and the other part provided to supervisors. Subsequently, users should reset their credentials on first use to ensure that they are not known by other parties.

***Control: ISM-1593; Revision: 1; Updated: Mar-22; Applicability: All; Essential Eight: N/A***
*Users provide sufficient evidence to verify their identity when requesting new credentials.*

***Control: ISM-1227; Revision: 5; Updated: Mar-22; Applicability: All; Essential Eight: N/A***
*Credentials set for user accounts are randomly generated.*

***Control: ISM-1594; Revision: 1; Updated: Mar-22; Applicability: All; Essential Eight: N/A***
*Credentials are provided to users via a secure communications channel or, if not possible, split into two parts with one part provided to users and the other part provided to supervisors.*

***Control: ISM-1595; Revision: 1; Updated: Mar-22; Applicability: All; Essential Eight: N/A***
*Credentials provided to users are changed on first use.*

***Control: ISM-1596; Revision: 2; Updated: Dec-22; Applicability: All; Essential Eight: N/A***
*Credentials, in the form of memorised secrets, are not reused by users across different systems.*

## Setting credentials for break glass accounts, local administrator accounts and service accounts

When break glass accounts, local administrator accounts and service accounts use common usernames or weak credentials, it may allow an adversary that compromises credentials on one workstation or server to easily compromise other workstations and servers. As such, it is critical that credentials for break glass accounts, local administrator accounts and service accounts 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 and unpredictable with a minimum length of 30 characters.

***Control: ISM-1685; Revision: 2; Updated: Jun-23; Applicability: All; Essential Eight: ML2, ML3***
*Credentials for break glass accounts, local administrator accounts and service accounts are long, unique, unpredictable and managed.*

***Control: ISM-1795; Revision: 1; Updated: Jun-23; Applicability: All; Essential Eight: N/A***
*Credentials for break glass accounts, local administrator accounts and service accounts are a minimum of 30 characters.*

***Control: ISM-1619; Revision: 0; Updated: Oct-20; Applicability: All; Essential Eight: 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 accounts, or groups of 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 an adversary gains access to a network), being discovered stored on networks in the clear, being transferred across networks in the clear, when membership of shared accounts change and if they haven’t been changed in the past 12 months.

***Control: ISM-1590; Revision: 2; Updated: Jun-23; Applicability: All; Essential Eight: N/A***
*Credentials 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 account changes*
- *they have not been changed in the past 12 months.*

***Control: ISM-1847; Revision: 0; Updated: Mar-23; Applicability: All; Essential Eight: N/A***
*Credentials for the Kerberos Key Distribution Center’s service account (KRBTGT) are changed twice, allowing for replication to all Microsoft Active Directory Domain Services 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.*

## Protecting credentials

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 an adversary gaining unauthorised access to systems. For example, when smart cards are left on desks, one-time password tokens are left in laptop bags, security keys are left connected to computers or passphrases are written down and stuck to computer monitors. Furthermore, obscuring credentials as they are entered into systems can assist in protecting them against screen scrapers and shoulder surfers.

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. In addition, Windows Defender Credential Guard, Windows Defender Remote Credential Guard and Protective Process Light for the Local Security Authority Subsystem Service (LSASS), preferably with a Unified Extensible Firmware Interface (UEFI) lock, can be enabled to provide additional protection for credentials.

When using Microsoft Windows systems, cached credentials are stored in the Security Accounts Manager database and can allow a user to logon to a workstation they have previously logged onto even if the domain is not available. Whilst this functionality may be desirable from an availability perspective, this functionality can be abused by an adversary who can retrieve these cached credentials. To reduce this security risk, cached credentials should be limited to only one previous logon.

***Control: ISM-0418; Revision: 6; Updated: Dec-22; Applicability: All; Essential Eight: N/A***
*Credentials are kept separate from systems they are used to authenticate to, except for when performing authentication activities.*

***Control: ISM-1597; Revision: 0; Updated: Aug-20; Applicability: All; Essential Eight: N/A***
*Credentials are obscured as they are entered into systems.*

***Control: ISM-1402; Revision: 6; Updated: Mar-22; Applicability: All; Essential Eight: N/A***
*Credentials stored on systems are protected by a password manager; a hardware security module; or by salting, hashing and stretching them before storage within a database.*

***Control: ISM-1686; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML3***
*Windows Defender Credential Guard and Windows Defender Remote Credential Guard are enabled.*

***Control: ISM-1861; Revision: 0; Updated: Jun-23; Applicability: All; Essential Eight: N/A***
*Protective Process Light for LSASS is enabled with a UEFI lock.*

***Control: ISM-1749; Revision: 0; Updated: Mar-22; Applicability: All; Essential Eight: N/A***
*Cached credentials are limited to one previous logon.*

## Account lockouts

Locking an account after a specified number of failed logon attempts reduces the likelihood of successful credential spraying attacks by an adversary. However, care should be taken as implementing account lockout functionality can increase the likelihood of a denial of service. Alternatively, some systems can be configured to automatically slowdown repeated failed logon attempts (known as rate limiting) rather than locking accounts. Implementing multi-factor authentication is also an effective way of reducing the likelihood of successful credential spraying attacks.

***Control: ISM-1403; Revision: 3; Updated: Jun-23; Applicability: All; Essential Eight: N/A***
*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 both system maintenance activities as well as removing an adversary that may have compromised a system but failed to gain persistence.

***Control: ISM-0853; Revision: 3; Updated: Sep-22; Applicability: All; Essential Eight: 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 and screen locking

Session and screen locking prevents unauthorised access to a system which a user has already authenticated to.

***Control: ISM-0428; Revision: 9; Updated: Dec-22; Applicability: All; Essential Eight: N/A***
*Systems are configured with a session or screen lock that:*

- *activates after a maximum of 15 minutes of user inactivity, or if manually activated by users*
- *conceals all session content on the screen*
- *ensures that the screen does not enter a power saving state before the session or screen lock is activated*
- *requires users to authenticate to unlock the session*
- *denies users the ability to disable the session or screen locking mechanism.*

## Logon banner

Displaying a logon banner to users before access is granted to a system reminds them of their security responsibilities. Logon banners may cover topics such as:

- the sensitivity or classification of the system
- access to the system being restricted to authorised users
- acceptable usage and security policies for the system
- an agreement to abide by acceptable usage and security policies for the system
- legal ramifications of violating acceptable usage and security policies for the system
- details of any monitoring activities for the system.

***Control: ISM-0408; Revision: 4; Updated: Sep-18; Applicability: All; Essential Eight: N/A***
*Systems have a logon banner that requires users to acknowledge and accept their security responsibilities before access is granted.*

***Control: ISM-0979; Revision: 4; Updated: Sep-18; Applicability: All; Essential Eight: N/A***
*Legal advice is sought on the exact wording of logon banners.*

## Further information

Further information on 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 implementing multi-factor authentication can be found in the ACSC's *Implementing Multi-Factor Authentication* publication.

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

Further information on randomly generating passphrases (preferably using five dice rolls and a long word list) is available from the Electronic Frontier Foundation while a random dice roller is available from RANDOM.ORG.

Further information on 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 *AD Forest Recovery - Resetting the krbtgt password* publications. A script for changing credentials for this service account is also available from Microsoft.

Further information on Windows Defender Credential Guard and Windows Defender Remote Credential Guard is available from Microsoft.

Further information on Protective Process Light for LSASS is available from Microsoft.

Further information on mitigating the use of stolen credentials can be found in the ACSC's *Mitigating the Use of Stolen Credentials* publication.

Further information on mitigating the use of stolen credentials can also be found in Microsoft's *Mitigating Pass-the-Hash (PtH) Attacks and Other Credential Theft Techniques, Version 1 and 2* publication.

## Virtualisation hardening

### Hypervisors

This section is applicable to both 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 both 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-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.

An adversary who has compromised a single computing environment, or who legitimately controls a single computing environment, might exploit a misconfiguration or security vulnerability in the isolation mechanism to compromise other computing environments on the same physical server or compromise the underlying operating system of the physical server. As such, it is important that additional controls are implemented when a software-based isolation mechanism is used to share a physical server's hardware.

***Control: ISM-1460; Revision: 4; Updated: Mar-23; Applicability: All; Essential Eight: N/A***
*When using a software-based isolation mechanism to share a physical server's hardware, the isolation mechanism is from a vendor that has demonstrated a commitment to secure-by-design and secure-by-default principles, use of memory-safe programming languages where possible, secure programming practices, and maintaining the security of their products.*

***Control: ISM-1604; Revision: 0; Updated: Aug-20; Applicability: All; Essential Eight: N/A***
*When using a software-based isolation mechanism to share a physical server's hardware, the configuration of the isolation mechanism is hardened by removing unneeded functionality and restricting access to the administrative interface used to manage the isolation mechanism.*

***Control: ISM-1605; Revision: 1; Updated: Mar-22; Applicability: All; Essential Eight: N/A***
*When using a software-based isolation mechanism to share a physical server's hardware, the underlying operating system is hardened.*

***Control: ISM-1606; Revision: 1; Updated: Mar-22; Applicability: All; Essential Eight: N/A***
*When using a software-based isolation mechanism to share a physical server's hardware, patches, updates or vendor mitigations for security vulnerabilities are applied to the isolation mechanism and underlying operating system in a timely manner.*

***Control: ISM-1848; Revision: 0; Updated: Mar-23; Applicability: All; Essential Eight: 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: 0; Updated: Aug-20; Applicability: All; Essential Eight: N/A***
*When using a software-based isolation mechanism to share a physical server's hardware, integrity and log monitoring are performed for the isolation mechanism and underlying operating system in a timely manner.*

***Control: ISM-1461; Revision: 5; Updated: Mar-22; Applicability: S, TS; Essential Eight: N/A***
*When using a software-based isolation mechanism to share a physical server's hardware for SECRET or TOP SECRET computing environments, the physical server and all computing environments are of the same classification and belong to the same security domain.*

### Further information

Further information on container security can be found in National Institute of Standards and Technology Special Publication 800-190, *Application Container Security Guide*.

Further information on 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 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*.