Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Australian Government Information Security Manual

APRIL 2019

Guidelines for system hardening

Operating system hardening

Operating system versions

Newer versions of operating systems often introduce improvements in security functionality over older versions. This can make it more difficult for an adversary to craft reliable exploits for security vulnerabilities they discover. Using older versions of operating systems, especially those no longer supported by vendors, exposes organisations to exploitation techniques that have since been mitigated in newer versions of operating systems.

The x64 (64-bit) versions of Microsoft Windows include additional security functionality that the x86 (32-bit) versions lack. Using x86 (32-bit) versions of Microsoft Windows exposes organisations to exploitation techniques mitigated by x64 (64-bit) versions of Microsoft Windows.

Security Control: 1407; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
The latest version (N), or N-1 version, of an operating system is used for Standard Operating Environments (SOEs).

Security Control: 1408; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
When developing a Microsoft Windows SOE, the 64-bit version of the operating system is used.

Operating system configuration

When operating systems are deployed in their default state it can easily lead to an unsafe operating environment allowing an adversary to gain an initial foothold on a network. Many options exist within operating systems to allow them to be configured in a secure state to minimise this security risk. The Australian Cyber Security Centre (ACSC) produces hardening guidance to assist in securely configuring various operating systems.

Security Control: 1409; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
ACSC and vendor guidance is implemented to assist in hardening the configuration of operating systems.

Security Control: 0383; Revision: 6; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
Default operating system accounts are disabled, renamed or have their passphrase changed.

Security Control: 0380; Revision: 7; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
Unneeded operating system accounts, software, components, services and functionality are removed or disabled.

Security Control: 1491; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
Standard users are prevented from running all script execution engines shipped with Microsoft Windows including Windows Script Host (cscript.exe and wscript.exe), powershell.exe, powershell_ise.exe, cmd.exe, wmic.exe and Microsoft HTML Application Host (mshta.exe).

Local administrator accounts

When local administrator accounts are used with common account names and passphrases, it can allow an adversary that compromises these credentials on one workstation or server to easily transfer across a network to other workstations or servers.

Security Control: 1410; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
Local administrator accounts are disabled; alternatively, passphrases that are random and unique for each device's local administrator account are used.

Security Control: 1469; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
Unique domain accounts with local administrative privileges, but without domain administrative privileges, are used for workstation and server management.

Application management

While the ability to install applications may be a business requirement for users, this privilege can be exploited by an adversary who can email a malicious application, or host it on a compromised website, and use social engineering techniques to convince users into installing it. Even if privileged access is required to install applications, users will often use their privileged access if they believe, or can be convinced that, the requirement to install the application is legitimate. Additionally, if applications are configured to install using elevated privileges, an adversary can exploit this by creating a Windows Installer installation package to create a new account that belongs to the local administrators group.

Security Control: 0382; Revision: 5; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
Users do not have the ability to install, uninstall or disable software.

Application whitelisting

An adversary can email malicious code, or host malicious code on a compromised website, and use social engineering techniques to convince users into executing it. Such malicious code often aims to exploit security vulnerabilities in existing applications and does not need to be installed to be successful.

Application whitelisting, when implemented in its most effective form (i.e. using hashes for executables, software libraries, scripts and installers) can be an extremely effective mechanism in not only preventing malicious code from executing, but also ensuring only authorised applications can be installed. Other implementations of application whitelisting (e.g. using approved paths for installed applications, in combination with access controls requiring privileged access to write to those locations) can still be a very effective mitigation strategy.

When developing application whitelisting rule sets, defining a list of 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) and installers (e.g. .msi, .msp and .mst files) from scratch is a more secure method than relying on a list of those currently residing on a workstation or server. Furthermore, it is preferable that organisations define their own approved list of executables, software libraries, scripts and installers rather than relying on lists from application whitelisting vendors.

Security Control: 0843; Revision: 7; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
An application whitelisting solution is implemented on all workstations to restrict the execution of executables, software libraries, scripts and installers to an approved set.

Security Control: 1490; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
An application whitelisting solution is implemented on Active Directory servers, email servers and other servers handling user authentication to restrict the execution of executables, software libraries, scripts and installers to an approved set.

Security Control: 0846; Revision: 6; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
All users (with the exception of privileged users when performing specific administrative activities) cannot disable, bypass or be exempted from application whitelisting mechanisms.

Security Control: 0955; Revision: 5; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
Application whitelisting is implemented using cryptographic hash rules, publisher certificate rules or path rules.

Security Control: 1471; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
When implementing application whitelisting using publisher certificate rules, both publisher names and product names are used.

Security Control: 1392; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
When implementing application whitelisting using path rules, file system permissions are configured to prevent unauthorised modification of folder and file permissions, folder contents (including adding new files) and individual files that are approved to execute.

Security Control: 0957; Revision: 5; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
Application whitelisting solutions are configured to generate event logs for failed execution attempts, including information such as the name of the blocked file, the date/time stamp and the username of the user attempting to execute the file.

Enhanced Mitigation Experience Toolkit and Exploit protection

An adversary who develops exploits for Microsoft Windows will be more successful in exploiting security vulnerabilities when Microsoft's Enhanced Mitigation Experience Toolkit (EMET) has not been installed. EMET was designed to provide a number of system-wide mitigation measures while also providing application-specific mitigation measures. From Microsoft Windows 10 version 1709 and Microsoft Windows Server 2016 onwards, EMET functionality has been incorporated directly into the operating system as part of 'Exploit protection' functionality.

Security Control: 1414; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
If supported, the latest version of Microsoft's EMET is implemented on workstations and servers and configured with both operating system mitigation measures and application-specific mitigation measures.

Security Control: 1492; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
If supported, Microsoft's 'Exploit protection' functionality is implemented on workstations and servers.

Host-based Intrusion Prevention System

Many endpoint security solutions rely on signatures to detect malicious code. This approach is only effective when a particular piece of malicious code has already been profiled and signatures are current. Unfortunately, an adversary can create variants of known malicious code, or develop new unseen malicious code, to bypass traditional signature-based detection mechanisms. A Host-based Intrusion Prevention System (HIPS) can use behaviour-based detection schemes to assist in identifying and blocking anomalous behaviour, such as process injection, keystroke logging, driver loading and call hooking, as well as detecting malicious code that has yet to be identified by antivirus vendors.

Security Control: 1341; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
A HIPS is implemented on workstations.

Security Control: 1034; Revision: 6; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
A HIPS is implemented on high value servers such as authentication servers, Domain Name System (DNS) servers, web servers, file servers and email servers.

Software firewall

Network firewalls often fail to prevent the propagation of malicious code on a network, or an adversary from extracting important information, as they generally 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 (HTTP), Hypertext Transfer Protocol Secure (HTTPS), Simple Mail Transfer Protocol (SMTP) and DNS. Software firewalls are more effective than network firewalls as they can control which applications

and services can communicate to and from workstations and servers. The in-built Windows firewall should be used to control both inbound and outbound traffic for specific applications.

Security Control: 1416; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
A software firewall is implemented on workstations and servers to limit both inbound and outbound network connections.

Antivirus software

When vendors develop software they may not use secure coding practices. An adversary can take advantage of this by developing malicious code to exploit security vulnerabilities that have not been detected and remedied. As significant time and effort is often involved in developing functioning and reliable exploits, an adversary will often reuse their exploits as much as possible. While exploits may be profiled by antivirus vendors, they often remain a variable intrusion method in organisations that do not have any measures in place to detect them.

Security Control: 1417; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
Antivirus software is implemented on workstations and servers and configured with:

- *signature-based detection enabled and set to a high level*
- *heuristic-based detection enabled and set to a high level*
- *detection signatures checked for currency and updated on at least a daily basis*
- *automatic and regular scanning configured for all fixed disks and removable media.*

Security Control: 1390; Revision: 2; Updated: Sep-18; Applicability: O, P; Priority: Should
Antivirus software has reputation rating functionality enabled.

Endpoint device control software

The use of endpoint device control software to control the use of unauthorised devices adds value as part of a defence-in-depth approach to the protection of workstations and servers.

Security Control: 1418; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
Endpoint device control software is implemented on workstations and servers to prevent unauthorised devices from being used.

Further information

Further information on identifying, authenticating and authorising users (including privileged users) of systems can be found in the ***System access*** section of these guidelines.

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

Further information on patching operating systems can be found in the ***System patching*** section of the ***Guidelines for system management***.

Further information on logging and auditing of operating system events can be found in the ***Event logging and auditing*** section of the ***Guidelines for system monitoring***.

Further information on securely configuring Microsoft Windows operating systems can be found in the following ACSC publications:

- ***Hardening Microsoft Windows 7 SP1 Workstations*** at https://www.cyber.gov.au/publications/hardening-microsoft-windows-7-sp1-workstations

- ***Hardening Microsoft Windows 8.1 Update Workstations*** at https://www.cyber.gov.au/publications/hardening-microsoft-windows-8-1-update-workstations
- ***Hardening Microsoft Windows 10 version 1709 Workstations*** at https://www.cyber.gov.au/publications/hardening-microsoft-windows-10-build-1709.

Further information regarding application whitelisting can be found in the ACSC's ***Implementing Application Whitelisting*** publication at https://www.cyber.gov.au/publications/implementing-application-whitelisting.

Further information on Microsoft's EMET is available at https://support.microsoft.com/en-au/help/2458544/the-enhanced-mitigation-experience-toolkit.

Further information on Microsoft's Exploit protection functionality is available at https://docs.microsoft.com/en-au/windows/security/threat-protection/windows-defender-exploit-guard/exploit-protection-exploit-guard.

Independent testing of different antivirus software and their effectiveness is available at https://www.av-comparatives.org/ and https://av-test.org/en/.

Application hardening

Application selection

When selecting applications it is important that organisations preference vendors that have demonstrated a commitment to secure coding practices and have a strong track record of maintaining the security of their applications. This will assist not only with hardening applications but also increase the likelihood that vendors will release timely patches to remediate any security vulnerabilities in their applications.

Security Control: 0938; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
Applications are chosen from vendors that have made a commitment to secure development and maintenance practices.

Application versions

Newer versions of applications often introduce improvements in security functionality over older versions. This can make it more difficult for an adversary to craft reliable exploits for security vulnerabilities they discover. Using older versions of applications, especially key business applications such as office productivity suites (e.g. Microsoft Office), PDF viewers (e.g. Adobe Reader), web browsers (e.g. Microsoft Internet Explorer, Mozilla Firefox or Google Chrome), common web browser plugins (e.g. Adobe Flash), email clients (e.g. Microsoft Outlook) and software platforms (e.g. Oracle Java Platform and Microsoft .NET Framework), exposes organisations to exploitation techniques that have since been mitigated in newer versions of applications.

Security Control: 1467; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
The latest releases of key business applications such as office productivity suites, PDF viewers, web browsers, common web browser plugins, email clients and software platforms are used when present within SOEs.

Security Control: 1483; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
The latest releases of web server software, server applications that store important data, and other internet-accessible server applications are used when present within SOEs.

Hardening application configurations

By default, many applications enable functionality that is not required by users while security functionality may be disabled or set at a lower security level. This is especially risky for key business applications such as office productivity suites, Portable Document Format (PDF) viewers, web browsers, common web browser plugins, email clients and software platforms that are likely to be targeted by an adversary. To assist in minimising this security risk, the ACSC

produces hardening guidance to assist in securely configuring key business applications. Further, to assist in securely configuring their applications, vendors may provide their own security guides.

Security Control: 1412; Revision: 2; Updated: Feb-19; Applicability: O, P, S, TS; Priority: Should
ACSC and vendor guidance is implemented to assist in hardening the configuration of Microsoft Office, web browsers and PDF viewers.

Security Control: 1484; Revision: 1; Updated: Jan-19; Applicability: O, P, S, TS; Priority: Must
Web browsers are configured to block or disable support for Flash content.

Security Control: 1485; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
Web browsers are configured to block web advertisements.

Security Control: 1486; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
Web browsers are configured to block Java from the Internet.

Security Control: 1541; Revision: 0; Updated: Jan-19; Applicability: O, P, S, TS; Priority: Must
Microsoft Office is configured to disable support for Flash content.

Security Control: 1542; Revision: 0; Updated: Jan-19; Applicability: O, P, S, TS; Priority: Must
Microsoft Office is configured to prevent activation of Object Linking and Embedding packages.

Security Control: 1470; Revision: 3; Updated: Mar-19; Applicability: O, P, S, TS; Priority: Should
Any unrequired functionality in Microsoft Office, web browsers and PDF viewers is disabled.

Security Control: 1235; Revision: 2; Updated: Apr-19; Applicability: O, P, S, TS; Priority: Should
The use of Microsoft Office, web browser and PDF viewer add-ons is restricted to organisation approved add-ons.

Microsoft Office macros

Microsoft Office files can contain embedded code (known as a macro) written in the Visual Basic for Applications (VBA) 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 sensitive or classified information. To reduce this security risk, organisations should disable or secure their use of Microsoft Office macros.

Security Control: 1487; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
Microsoft Office macros are only allowed to execute in documents from Trusted Locations where write access is limited to personnel whose role is to vet and approve macros.

Security Control: 1488; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
Microsoft Office macros in documents originating from the Internet are blocked.

Security Control: 1489; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
Microsoft Office macro security settings cannot be changed by users.

Further information

Further information on patching applications can be found in the ***System patching*** section of the ***Guidelines for system management***.

Further information on securely configuring Microsoft Office can be found in the ACSC's ***Hardening Microsoft Office 2013*** publication at https://www.cyber.gov.au/publications/hardening-microsoft-office-2013 and the ACSC's ***Hardening Microsoft Office 365 ProPlus, Office 2019 and Office 2016*** publication at https://www.cyber.gov.au/publications/hardening-microsoft-office-2016.

Further information on configuring Microsoft Office macro settings can be found in the ACSC's ***Microsoft Office Macro Security*** publication at https://www.cyber.gov.au/publications/microsoft-office-macro-security.

Further information on configuring Microsoft Office to block macros in documents originating from the Internet can be found at https://cloudblogs.microsoft.com/microsoftsecure/2016/03/22/new-feature-in-office-2016-can-block-macros-and-help-prevent-infection/.

System access

Account types

When this document refers to passphrase policies, it is equally applicable to all account types. This includes user accounts, privileged accounts and service accounts.

User identification

Having uniquely identifiable users ensures accountability. In addition, where systems contain Australian Eyes Only (AUSTEO), Australian Government Access Only (AGAO) or nationality releasability information, and foreign nationals have access to the systems, it is important that security controls are implemented to ensure foreign nationals are identified as such.

Security Control: 0414; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
All users are uniquely identifiable and authenticated on each occasion that access is granted to a system.

Security Control: 1538; Revision: 0; Updated: Sep-18; Applicability: P, S, TS; Priority: Must
Where systems contain nationality releasability information, all users who are foreign nationals, including seconded foreign nationals, are uniquely identifiable.

Security Control: 0420; Revision: 7; Updated: Sep-18; Applicability: S, TS; Priority: Must
Where systems contain AUSTEO or AGAO information, all users who are foreign nationals, including seconded foreign nationals, are uniquely identifiable.

Security Control: 0975; Revision: 6; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
Security controls used to identify users who are foreign nationals, including seconded foreign nationals, include identification measures that specify their nationality.

Shared user accounts

Shared user accounts can hamper efforts to attribute actions on a system to specific personnel, and their use should be avoided. However, if there is a strong business justification for their use, a method of attributing actions undertaken by shared accounts to specific personnel should be implemented. For example, a logbook may be used to document the date and time that a person takes responsibility for using a shared user account.

Security Control: 0415; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
The use of shared user accounts is controlled and auditable.

Single-factor authentication

A significant threat to the compromise of user accounts is offline passphrase cracking tools. When an adversary gains access to a list of usernames and hashed passphrases from a system, they can attempt to recover passphrases by comparing the hash of a known passphrase with the hashes from the list of hashed passphrases that they obtained. By finding a match, an adversary will know the passphrase associated with a given username. Combined, this often forms a complete set of authentication information for an account. In order to reduce this security risk, organisations can implement multi-factor authentication. Alternatively, an organisation may attempt to increase the time on average it

takes an adversary to compromise a passphrase by increasing both its complexity and length while decreasing the time it remains valid.

Security Control: 0417; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
A numerical password is not used as the sole method of authenticating a user.

Security Control: 0421; Revision: 5; Updated: Sep-18; Applicability: O, P, S; Priority: Must
Passphrases used as the sole method of authentication enforce a minimum of 13 alphabetic characters; or a minimum of 10 characters consisting of at least three of the following character sets:

- *lowercase alphabetic characters (a-z)*
- *uppercase alphabetic characters (A-Z)*
- *numeric characters (0-9)*
- *special characters.*

Security Control: 0422; Revision: 5; Updated: Sep-18; Applicability: TS; Priority: Must
Passphrases used as the sole method of authentication enforce a minimum of 15 alphabetic characters; or a minimum of 11 characters consisting of at least three of the following character sets:

- *lowercase alphabetic characters (a-z)*
- *uppercase alphabetic characters (A-Z)*
- *numeric characters (0-9)*
- *special characters.*

Security Control: 0423; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
Passphrase management practices:

- *ensure that passphrases are changed at least every 90 days*
- *prevent passphrases from being changed by a user more than once a day*
- *prevent passphrases from being reused within eight passphrase changes*
- *prevent the use of sequential passphrases where possible*
- *prevent passphrases being stored in cleartext.*

Security Control: 1426; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
When systems cannot be configured to enforce passphrase complexity and management practices, passphrases are checked by alternative means for compliance with passphrase policies.

Multi-factor authentication

Multi-factor authentication uses independent methods to confirm a user's identity. It may include:

- something a user knows, such as a passphrase or a response to a security question
- something a user has, such as a passport, physical token or an identity card
- something unique about a user, such as a fingerprint or their face's geometry.

Any two of these methods are required to have multi-factor authentication. If something a user knows is written down, or typed into a file and stored as plaintext, this evidence becomes something that a user has rather than something a user knows.

Privileged users, positions of trust, 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 level of access. For this reason, it is especially important that multi-factor authentication is used for these accounts.

When implementing multi-factor authentication, a number of different authentication factors can be implemented in addition to passphrases. Unfortunately, some authentication factors such as those sent via Short Message Service (SMS) are more susceptible to compromise by an adversary than others. For this reason, a limited number of authentication methods are recommended for use as part of a multi-factor authentication implementation.

The benefit of implementing multi-factor authentication can be diminished when credentials are reused on other systems. For example, when usernames and passphrases used as part of multi-factor authentication for remote access are the same as those used for corporate workstations. In such circumstances, if an adversary had compromised the device used for remote access they could capture the username and passphrase for reuse against a corporate workstation that did not require the use of multi-factor authentication.

Security Control: 0974; Revision: 5; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
Multi-factor authentication is used to authenticate standard users.

Security Control: 1173; Revision: 3; Updated: Mar-19; Applicability: O, P, S, TS; Priority: Must
Multi-factor authentication is used to authenticate all privileged users and any other positions of trust.

Security Control: 1504; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
Multi-factor authentication is used to authenticate all users of remote access solutions.

Security Control: 1505; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
Multi-factor authentication is used to authenticate all users when accessing important data repositories.

Security Control: 1401; Revision: 3; Updated: Mar-19; Applicability: O, P, S, TS; Priority: Must
Multi-factor authentication uses at least two of the following authentication factors: passwords with six or more characters, Universal 2nd Factor (U2F) security keys, physical one-time password (OTP) tokens, biometrics or smartcards.

Security Control: 1357; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
When multi-factor authentication is implemented, none of the authentication factors on their own can be used for single-factor authentication to another system.

Passphrase authentication

Local Area Network (LAN) Manager's authentication mechanism uses a very weak hashing algorithm known as the LAN Manager hash algorithm. Passphrases hashed using the LAN Manager hash algorithm can easily be compromised using rainbow tables or brute force attacks.

Security Control: 1055; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
LAN Manager is disabled for passphrase authentication on workstations and servers.

Account lockouts

Locking an account after a specified number of failed logon attempts reduces the likelihood of successful passphrase guessing attacks. However, care should be taken as implementing account lockout functionality in a web application can increase the likelihood of a denial of service.

Security Control: 1403; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
Accounts are locked after a maximum of five failed logon attempts.

Security Control: 0431; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
Repeated account lockouts are investigated before reauthorising access.

Resetting passphrases

To reduce the likelihood of social engineering being used to compromise accounts, users should provide sufficient evidence to verify their identity when requesting a passphrase reset. This evidence could be in the form of the user:

- physically presenting themselves and their security pass to service desk personnel who then reset their passphrase
- physically presenting themselves to a known colleague who uses an approved online tool to reset their passphrase
- establishing their identity by responding correctly to a number of challenge response questions before resetting their own passphrase.

In addition, issuing accounts with unique complex reset passphrases ensures the security of the account is maintained during the passphrase reset process.

Security Control: 0976; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
Users provide sufficient evidence to verify their identity when requesting a passphrase reset.

Security Control: 1227; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
Passphrases resets are:

- *random for each individual reset*
- *not reused when resetting multiple accounts*
- *not based on a single dictionary word*
- *not based on another identifying factor, such as the user's name or the date.*

Protecting authentication information

Storing authentication information with a system that it grants access to increases the likelihood of an adversary gaining access to the system. For example, a passphrase should never be written down and stuck to a laptop or computer monitor.

If storing authentication information on a system, sufficient protection should be implemented to prevent the authentication information from being compromised as part of a targeted cyber intrusion. For example, usernames and passphrases for databases should be stored in a password vault rather than in a Microsoft Word or Excel document. In addition, secure transmission of authentication information reduces the likelihood of an adversary intercepting and using the authentication information to access a system under the guise of a valid user.

Security Control: 0418; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
Authentication information is stored separately from a system to which it grants access.

Security Control: 1402; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
Authentication information stored or communicated by a system is protected from unauthorised access.

Session and screen locking

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

Security Control: 0428; Revision: 6; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
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 the user*
- *completely conceals all information on the screen*

- *ensures that the screen does not enter a power saving state before the screen or session lock is activated*
- *requires the user to reauthenticate to unlock the system*
- *denies users the ability to disable the session or screen locking mechanism.*

Logon banner

Displaying a logon banner to users after they authenticate to a system reminds them of their security responsibilities. Logon banners may cover topics such as:

- access to the system being restricted to authorised users
- acceptable usage and security policies for the system
- the user's agreement to abide by abovementioned policies
- legal ramifications of violating the abovementioned policies
- details of monitoring and auditing activities
- a point of contact for any questions.

Security Control: 0408; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
Systems have a logon banner that requires users to acknowledge and accept their security responsibilities before access is granted.

Security Control: 0979; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
Legal advice is sought on the exact wording of logon banners.

Further information

Further information on authorisations, security clearances and briefings for system access can be found in the ***Access to systems and their resources*** section of the ***Guidelines for personnel security***.

Further information on restricting administrative privileges can be found in the ACSC's ***Restricting Administrative Privileges*** publication at https://www.cyber.gov.au/publications/restricting-administrative-privileges.

Further information on implementing multi-factor authentication can be found in the ACSC's ***Implementing Multi-Factor Authentication*** publication at https://www.cyber.gov.au/publications/multi-factor-authentication.

Further information on mitigating the use of stolen credentials can be found in the ACSC's ***Mitigating the Use of Stolen Credentials*** publication at https://www.cyber.gov.au/publications/mitigating-the-use-of-stolen-credentials.