Information security manual

Guidelines for system access

Last updated: September 2026

Identity and access management

Context

Where these guidelines refer to security clearances, this includes both Australian security clearances and those from foreign governments that are formally recognised by Australia.

In addition, while some security controls in these guidelines apply specifically to human users, security controls for identifying, authenticating, authorising and monitoring users also apply to non-human users, such as services, applications, workloads and artificial intelligence (AI) agents.

System usage policy

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

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

System access requirements

Documenting access requirements for systems and their resources can assist in determining whether users meet requirements for access. In doing so, requirements should account for whether access is unprivileged or privileged and, for personnel, whether additional requirements apply because they are foreign nationals or contractors.

To reinforce personnel's agreement to abide by system usage policies as a condition of being granted access to a system and its resources, displaying a logon banner each time they log on to the system can provide a continual reminder of their security responsibilities. Logon banners may cover topics such as:

- the sensitivity or classification of the system
- access requirements for the system
- usage policies for the system and its resources

- details of any monitoring activities for the system.

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

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

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

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

Control: ISM-0408; Revision: 6; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Systems have a logon banner that reminds personnel of their security responsibilities when accessing the system and its resources.

User identification

Ensuring users are uniquely identifiable enables their access and activities to be attributed to them. Furthermore, where systems process, store or communicate Australian Eyes Only (AUSTEO), Australian Government Access Only (AGAO) or Releasable To (REL) data, and foreign nationals have access, it is important that the foreign nationals are identified as such.

Control: ISM-0414; Revision: 6; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Users granted access to systems and their resources are uniquely identifiable.

Control: ISM-0415; Revision: 4; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The use of shared user accounts is strictly controlled, and users of such accounts are uniquely identifiable.

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

Control: ISM-0420; Revision: 12; Updated: Jun-25; Applicable: S, TS; Essential 8: N/A
Where systems process, store or communicate AUSTEO, AGAO or REL data, personnel who are foreign nationals are identified as such, including by their specific nationality.

Artificial intelligence agent identification

In addition to the general requirement for users to be uniquely identifiable, assigning each AI agent its own unique identity ensures that actions taken by an AI agent can be distinguished from actions taken directly by a user on whose behalf it acts, as well as from actions taken by other AI agents. In doing so, identities assigned to AI agents should be managed in a similar manner to service accounts, including being disabled or removed when no longer required. Where an AI agent is assigned multiple identities, such as across different environments or platforms, all identities should be recorded in an organisation's AI agent register.

Control: ISM-2133; Revision: 0; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Each AI agent is assigned a unique identity that is distinct from the user accounts of personnel and the identities of other AI agents.

Unprivileged access to systems

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

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

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

Control: ISM-1852; Revision: 2; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Unprivileged access to systems and their resources is limited to only what is required for users to undertake their duties or functions.

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

Unprivileged access to systems by foreign nationals

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

Control: ISM-0409; Revision: 9; Updated: Sep-26; Applicable: S, TS; Essential 8: N/A
Foreign nationals, including seconded foreign nationals, do not have access to systems that process, store or communicate AUSTEO or REL data unless effective security controls are in place to ensure such data is not accessible to them.

Control: ISM-0411; Revision: 8; Updated: Sep-26; Applicable: S, TS; Essential 8: N/A
Foreign nationals, excluding seconded foreign nationals, do not have access to systems that process, store or communicate AGAO data unless effective security controls are in place to ensure such data is not accessible to them.

Privileged access to systems

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

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

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

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

Control: ISM-1508; Revision: 5; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: ML3
Privileged access to systems and their resources is limited to only what is required for users to undertake their duties or functions.

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

Control: ISM-1883; Revision: 2; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: ML1, ML2, ML3
Privileged user accounts explicitly authorised to access online services are strictly limited to only what is required for users to undertake their duties or functions.

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

Control: ISM-0445; Revision: 9; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: ML1, ML2, ML3
Privileged human users are assigned a dedicated privileged user account to be used solely for duties requiring privileged access.

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

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

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

Privileged access to systems by foreign nationals

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

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

Control: ISM-0447; Revision: 4; Updated: Jun-21; Applicable: S, TS; Essential 8: N/A
Foreign nationals, excluding seconded foreign nationals, do not have privileged access to systems that process, store or communicate AGAO data.

Recording authorisation for personnel to access systems

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

Control: ISM-0407; Revision: 7; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
A secure record is maintained for the life of systems and their resources that covers the following for each human user:

- *their unique identifier*

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

Artificial intelligence agent register

AI agents can be rapidly created and deployed across an organisation's systems, often by personnel operating outside of traditional software deployment processes. Each AI agent may be configured with its own instructions, AI models, tools, permissions, credentials and access to data repositories. Without visibility of the AI agents operating across its systems, an organisation cannot effectively restrict AI agents to the minimum permissions they require, review their continued need, identify unauthorised or abandoned AI agents, or investigate cyber security incidents involving them. As such, an organisation should develop, implement, maintain and regularly verify an AI agent register. An AI agent register may also record additional details, such as the AI models used by each AI agent and their versions, to support change management and cyber supply chain risk management activities.

Control: ISM-2134; Revision: 0; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
An AI agent register is developed, implemented, maintained and regularly verified.

Control: ISM-2135; Revision: 0; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
An AI agent register contains the following for each AI agent:

- *its unique identifier*
- *its owner and business purpose*
- *the identities assigned to it*
- *any user accounts and credentials it uses*
- *the tools, permissions and data repositories it can access.*

Suspension of access to systems

Removing or suspending access to systems and their resources, ideally using an automatic mechanism, can prevent them from being accessed when there is no longer a legitimate business requirement for their use, such as when users change duties or functions, or are detected undertaking malicious activities.

Control: ISM-0430; Revision: 9; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Access to systems and their resources are removed or suspended the same day users no longer have a legitimate requirement for access.

Control: ISM-1591; Revision: 2; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Access to systems and their resources are removed or suspended as soon as practicable when users are detected undertaking malicious activities.

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

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

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

Temporary access to systems

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

Control: ISM-0441; Revision: 10; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
When personnel are granted temporary access to systems and their resources, effective security controls are put in place to restrict their access to only data required for them to undertake their duties or functions.

Control: ISM-0443; Revision: 3; Updated: Sep-18; Applicable: S, TS; Essential 8: N/A
Temporary access is not granted to systems that process, store or communicate caveated or sensitive compartmented information.

Emergency access to systems

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

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

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

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

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

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

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

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

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

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

Control of Australian systems

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

Control: ISM-0078; Revision: 5; Updated: Jun-21; Applicable: S, TS; Essential 8: N/A
Systems processing, storing or communicating AUSTEO or AGAO data remain at all times under the control of an Australian national working for or on behalf of the Australian Government.

Control: ISM-0854; Revision: 6; Updated: Dec-21; Applicable: S, TS; Essential 8: N/A
AUSTEO and AGAO data can only be accessed from systems under the sole control of the Australian Government that are located within facilities authorised by the Australian Government.

Authenticating to systems

Before access to a system and its resources is granted to a user, it is essential that they are authenticated. For human users, this can be achieved via multi-factor authentication, such as a username, password and security key, or less preferably via single-factor authentication, such as a username and password.

In addition, access decisions should not rely solely on the successful presentation of authentication artefacts. Risk-based access decisions can draw upon contextual signals such as device compliance, authentication strength, privilege level and user behaviour to determine whether access should be granted, re-authentication should be required or access should be denied. In doing so, an organisation should be aware that sign-in location is a weak signal on its own, as malicious actors increasingly route their activities through residential internet protocol addresses and covert networks of compromised devices to defeat location-based and reputation-based measures.

Control: ISM-1546; Revision: 0; Updated: Aug-19; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Users are authenticated before they are granted access to a system and its resources.

Control: ISM-2136; Revision: 0; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Risk-based access decisions, informed by contextual signals, are enforced for access to systems and their resources.

Insecure authentication methods

Authentication methods need to resist theft, interception, duplication, forgery, unauthorised access and unauthorised modification. For example, LAN Manager authentication protects credentials with a weak hashing algorithm, while all versions of NT LAN Manager lack mutual authentication and rely on password-derived hashes. As such, malicious actors can exploit these authentication methods via relay attacks, pass-the-hash attacks and the offline cracking of captured authentication exchanges. Instead, an organisation should use Kerberos for authentication within Microsoft Windows environments.

Control: ISM-1603; Revision: 0; Updated: Aug-20; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Authentication methods susceptible to replay attacks are disabled.

Control: ISM-1055; Revision: 4; Updated: Oct-20; Applicable: NC, OS, P, S, TS; Essential 8: N/A
LAN Manager and NT LAN Manager authentication methods are disabled.

Control: ISM-2076; Revision: 0; Updated: Dec-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Security questions are not used for authentication purposes.

Control: ISM-2077; Revision: 0; Updated: Dec-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Email is not used for out-of-band authentication purposes.

Multi-factor authentication

Multi-factor authentication uses two or more different authentication factors. This may include:

- something people know, such as a password
- something people have, such as a security key, smart card, smartphone or one-time password token
- something people are, such as a fingerprint pattern or their facial geometry.

Human users of online services, privileged human users of systems and human users with access to data repositories are more likely to be targeted by malicious actors due to their access. For this reason, it is especially important that multi-factor authentication is used for these user accounts. In addition, multi-factor authentication is vital when human users perform administrative activities as it can limit the consequences of a compromise by preventing or slowing malicious actors' ability to gain unrestricted access to assets. In this regard, multi-factor authentication can be implemented as part of jump server authentication where assets being administered do not support multi-factor authentication themselves.

When implementing multi-factor authentication, several different authentication factors can be implemented. Unfortunately, some authentication factors, such as biometrics or codes sent via Short Message Service, Voice over Internet Protocol or email, are more susceptible to compromise than others. For this reason, authentication factors that involve something people have should be used with something people know. Alternatively, something people have that is unlocked by something people 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.

Passkey authentication may provide either single-factor or multi-factor authentication, depending on how it is implemented and used. It typically uses a computer or smartphone, or a separate security key, to store or access a private key. Where use of the private key requires an activation factor, such as a password or biometric, passkey authentication satisfies multi-factor authentication requirements.

Finally, centrally logging and analysing multi-factor authentication events can assist in monitoring the security posture of systems, detecting malicious behaviour and contributing to investigations following cyber security incidents.

Control: ISM-1504; Revision: 4; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: ML1, ML2, ML3
Multi-factor authentication is used to authenticate human users to their organisation's online services that process, store or communicate their organisation's sensitive data.

Control: ISM-1679; Revision: 2; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: ML1, ML2, ML3
Multi-factor authentication is used to authenticate human users to third-party online services that process, store or communicate their organisation's sensitive data.

Control: ISM-1680; Revision: 2; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: ML1, ML2, ML3
Multi-factor authentication (where available) is used to authenticate human users to third-party online services that process, store or communicate their organisation's non-sensitive data.

Control: ISM-1892; Revision: 1; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: ML1, ML2, ML3
Multi-factor authentication is used to authenticate human users to their organisation's online customer services that process, store or communicate their organisation's sensitive customer data.

Control: ISM-1893; Revision: 1; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: ML1, ML2, ML3
Multi-factor authentication is used to authenticate human users to third-party online customer services that process, store or communicate their organisation's sensitive customer data.

Control: ISM-1681; Revision: 3; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: ML1, ML2, ML3
Multi-factor authentication is used to authenticate customers to online customer services that process, store or communicate sensitive customer data.

Control: ISM-1919; Revision: 1; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
When multi-factor authentication is used to authenticate human users or customers to online services or online customer services, all other authentication protocols that do not support multi-factor authentication are disabled.

Control: ISM-1173; Revision: 5; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: ML2, ML3
Multi-factor authentication is used to authenticate privileged human users of systems.

Control: ISM-0974; Revision: 7; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: ML2, ML3
Multi-factor authentication is used to authenticate unprivileged human users of systems.

Control: ISM-1505; Revision: 4; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: ML3
Multi-factor authentication is used to authenticate human users of data repositories.

Control: ISM-1401; Revision: 6; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: ML1, ML2, ML3
Multi-factor authentication uses either: something people have and something people know, or something people have that is unlocked by something people know or are.

Control: ISM-1872; Revision: 2; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: ML2, ML3
Multi-factor authentication used for authenticating human users of online services is phishing-resistant.

Control: ISM-1873; Revision: 1; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: ML2
Multi-factor authentication used for authenticating customers of online customer services provides a phishing-resistant option.

Control: ISM-1874; Revision: 1; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: ML3
Multi-factor authentication used for authenticating customers of online customer services is phishing-resistant.

Control: ISM-1682; Revision: 4; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: ML2, ML3
Multi-factor authentication used for authenticating human users of systems is phishing-resistant.

Control: ISM-1894; Revision: 1; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: ML3
Multi-factor authentication used for authenticating human users of data repositories is phishing-resistant.

Control: ISM-2011; Revision: 1; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
When phishing-resistant multi-factor authentication is used by human users, other non-phishing-resistant multi-factor authentication options are disabled for their user accounts.

Control: ISM-1920; Revision: 1; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
When multi-factor authentication is used to authenticate human users to online services, online customer services, systems or data repositories – that process, store or communicate their organisation's sensitive data or sensitive customer data – human users are prevented from self-enrolling into multi-factor authentication from untrustworthy devices.

Control: ISM-1683; Revision: 2; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: ML2, ML3
Successful and unsuccessful multi-factor authentication events are centrally logged.

Single-factor authentication

A significant threat to the compromise of user accounts is password cracking tools. When malicious actors gain access to a list of usernames and hashed passwords from a system, they can attempt to recover username and password pairs by comparing the hashes of known passwords with the hashed passwords they have gained access to. By finding a match, malicious actors will know the password associated with a given username. To reduce this security risk, an organisation should implement multi-factor authentication.

In addition, centrally logging and analysing single-factor authentication events can assist in monitoring the security posture of systems, detecting malicious behaviour and contributing to investigations following cyber security incidents.

Control: ISM-0417; Revision: 6; Updated: Dec-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
When systems cannot support multi-factor authentication, single-factor authentication using passwords is implemented instead.

Control: ISM-1895; Revision: 0; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Successful and unsuccessful single-factor authentication events are centrally logged.

User account lockouts

Locking user accounts after a specified number of repeated failed logon attempts reduces the likelihood of successful forms of credential brute-force attacks by malicious actors, such as credential guessing attacks, credential spraying attacks and credential stuffing attacks. However, care should be taken when implementing indefinite account lockouts in response to repeated failed logon attempts as this can increase the likelihood of a denial of service. Alternatively, some systems can be configured with risk-based

lockout mechanisms in combination with automated lockout durations to slow down repeated failed logon attempts. Implementing multi-factor authentication is also an effective way of reducing the likelihood of successful credential brute-force attacks.

Control: ISM-1403; Revision: 5; Updated: Jun-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
User accounts, except for break glass accounts, are protected by fixed or risk-based lockout mechanisms aligned to a maximum of five failed logon attempts, with either indefinite or automated lockout durations.

Session locking

Session locking prevents unauthorised access to services that a human user has already authenticated to.

Control: ISM-0428; Revision: 11; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Services are configured with a session lock that:

- *activates after a maximum of 15 minutes of human user inactivity, a maximum of 12 hours of overall session time or when manually activated*
- *blocks access to all session content*
- *requires re-authentication by human users using all authentication factors to unlock the session*
- *denies human users the ability to disable the session locking mechanism.*

Screen locking

Screen locking prevents unauthorised access to a system that a human user has already authenticated to.

Control: ISM-2012; Revision: 1; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Systems are configured with a screen lock that:

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

Session termination

Implementing measures to terminate interactive user sessions and restart workstations at least daily can assist in system maintenance activities and removing malicious actors that may have compromised a system but failed to gain persistence.

Control: ISM-0853; Revision: 5; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Interactive user sessions are terminated and workstations are restarted at least daily.

Third-party application access and device code authentication

Malicious actors can abuse legitimate Open Authorization (OAuth) flows to obtain enduring access to data without stealing credentials. In an illicit consent grant attack, a human user is tricked into granting a malicious third-party application consent to access data, after which the application holds OAuth tokens

that operate independently of the human user's credentials and survive credential resets. Separately, the device code authentication flow can be abused so that a human user, believing they are signing themselves in, authorises a malicious actor's session.

Importantly, malicious actors do not need to establish new consent grants if they can compromise an existing third-party application that has already been granted access, such as via a cyber supply chain attack against the application's vendor. As such, in addition to controlling how new consent is granted, an organisation should regularly review existing consent grants, revoke those that are unused or hold excessive permissions, and centrally log consent and token issuance activity to support the detection of anomalous use.

Finally, while the device code authentication flow should be disabled by default, an organisation may have a legitimate business requirement for its use, such as for input-constrained devices. In such cases, its use should be restricted to the specific user accounts and managed devices that require it.

Control: ISM-2137; Revision: 0; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Human users are prevented from granting consent to third-party OAuth applications, with such consent granted only by an authorised administrator.

Control: ISM-2138; Revision: 0; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
OAuth application consents, including their granted permissions, are reviewed at least every six months, with unused applications and excessive permissions revoked.

Control: ISM-2139; Revision: 0; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Consent grants, token issuance and token use for third-party OAuth applications are centrally logged.

Control: ISM-2140; Revision: 0; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The OAuth device code authentication flow is disabled unless required, and where required, is restricted to authorised user accounts and managed devices.

Further information

Further information on access to government resources, including required security clearances, can be found in the Department of Home Affairs' *Protective Security Policy Framework*.

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

Further information on restricting the use of privileged user accounts can be found in ASD's *Restricting administrative privileges* publication.

Further information on administering systems and their resources can be found in the 'System administration' section of the *Guidelines for system management*.

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

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

Further information on implementing multi-factor authentication can be found in ASD's *Implementing multi-factor authentication* publication.

Credential management

Context

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

Password strength

When implementing passwords as an authentication factor, it is important that suitably robust and secure passwords are used. In doing so, the degree of password security required will depend on the sensitivity or classification of the system involved and whether passwords are implemented as part of multi-factor authentication or single-factor authentication.

Control: ISM-1559; Revision: 4; Updated: Dec-25; Applicable: NC, OS, P; Essential 8: N/A
Passwords used for multi-factor authentication on non-classified, OFFICIAL: Sensitive and PROTECTED systems are a minimum of 6 characters.

Control: ISM-1560; Revision: 3; Updated: Dec-25; Applicable: S; Essential 8: N/A
Passwords used for multi-factor authentication on SECRET systems are a minimum of 8 characters.

Control: ISM-1561; Revision: 3; Updated: Dec-25; Applicable: TS; Essential 8: N/A
Passwords used for multi-factor authentication on TOP SECRET systems are a minimum of 10 characters.

Control: ISM-0421; Revision: 11; Updated: Dec-25; Applicable: NC, OS, P; Essential 8: N/A
Passwords used for single-factor authentication on non-classified, OFFICIAL: Sensitive and PROTECTED systems are a minimum of 15 characters.

Control: ISM-1557; Revision: 3; Updated: Dec-25; Applicable: S; Essential 8: N/A
Passwords used for single-factor authentication on SECRET systems are a minimum of 17 characters.

Control: ISM-0422; Revision: 9; Updated: Dec-25; Applicable: TS; Essential 8: N/A
Passwords used for single-factor authentication on TOP SECRET systems are a minimum of 20 characters.

Control: ISM-1558; Revision: 3; Updated: Dec-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Passwords using a sequence of words for single-factor authentication are not constructed using:

- *a list of categorised words*
- *a real sentence in a natural language*
- *song lyrics, movie or television show quotes, literature, or any other publicly available material*
- *less than 4 random words for non-classified, OFFICIAL: Sensitive and PROTECTED systems; 5 random words for SECRET systems; or 6 random words for TOP SECRET systems.*

Control: ISM-2078; Revision: 0; Updated: Dec-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Passwords appearing in lists of commonly used passwords or lists of compromised passwords are not used.

Control: ISM-2079; Revision: 0; Updated: Dec-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Maximum length limits for passwords are not less than 64 characters.

Control: ISM-2080; Revision: 0; Updated: Dec-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Password complexity requirements are not imposed for passwords.

Control: ISM-2081; Revision: 0; Updated: Dec-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
All ASCII printable characters are supported for passwords.

Setting credentials for user accounts

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

Control: ISM-1593; Revision: 2; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Human users provide sufficient evidence to verify their identity when first requesting credentials, when requesting the reset of any credentials, when requesting the temporary disabling of any credentials, and when requesting the enrolment or re-enrolment of any credentials.

Control: ISM-1227; Revision: 5; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Credentials set for user accounts are randomly generated.

Control: ISM-1594; Revision: 2; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Credentials for human users are provided via a secure communications channel or, if not possible, split into two parts with one part provided to the human user and the other part provided to their supervisor.

Control: ISM-1595; Revision: 2; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Credentials provided to human users are changed on first use.

Control: ISM-1596; Revision: 3; Updated: Dec-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Credentials are not reused by users across different systems.

Setting credentials for built-in Administrator accounts, break glass accounts, local administrator accounts and service accounts

When built-in Administrator accounts, break glass accounts, local administrator accounts and service accounts use common usernames or weak credentials, it may allow malicious actors that compromise credentials on one workstation or server to compromise other workstations and servers. As such, it is critical that credentials for the built-in Administrator account, break glass accounts, local administrator accounts and service accounts in each domain are long, unique, unpredictable and managed.

To provide additional security and credential management functionality for service accounts, Microsoft introduced group Managed Service Accounts to Microsoft Windows Server. In doing so, service accounts that are created as group Managed Service Accounts do not require manual credential management by system administrators, as the operating system automatically ensures that they are long, unique, unpredictable and managed. This ensures that service account credentials are secure, not misplaced or forgotten, and that they are automatically changed regularly. However, in cases where the use of group

Managed Service Accounts is not possible, credentials for service accounts should still be unique, unpredictable and random with a minimum length of 30 characters.

Control: ISM-1953; Revision: 0; Updated: Sep-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Credentials for the built-in Administrator account in each domain are long, unique, unpredictable and managed.

Control: ISM-1685; Revision: 2; Updated: Jun-23; Applicable: NC, OS, P, S, TS; Essential 8: ML2, ML3
Credentials for break glass accounts, local administrator accounts and service accounts are long, unique, unpredictable and managed.

Control: ISM-1795; Revision: 2; Updated: Sep-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Credentials for built-in Administrator accounts, break glass accounts, local administrator accounts and service accounts are a minimum of 30 characters.

Control: ISM-1954; Revision: 0; Updated: Sep-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Credentials for built-in Administrator accounts, break glass accounts, local administrator accounts and service accounts are randomly generated.

Control: ISM-1619; Revision: 0; Updated: Oct-20; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Service accounts are created as group Managed Service Accounts.

Application and workload credentials

Applications and workloads may require credentials to authenticate to systems, services and data repositories without direct human involvement. Where such credentials are long-lived or reused by multiple applications, workloads or operating environments, their compromise can provide malicious actors with persistent access to systems and increase the extent of a compromise.

Applications and workloads should use short-lived dynamically issued credentials in preference to long-lived static credentials. Where static credentials are required, centrally managing them using a credential or secrets management solution can assist with their secure storage, access control and lifecycle management. In addition, applications and workloads should use unique credentials that are not shared with other applications or workloads, or across development, testing, staging and production environments.

Control: ISM-2141; Revision: 0; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Applications and workloads use short-lived dynamically issued credentials in preference to long-lived static credentials.

Control: ISM-2142; Revision: 0; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Static credentials used by applications and workloads are centrally managed using a credential or secrets management solution.

Control: ISM-2143; Revision: 0; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Applications and workloads use unique credentials that are not shared with other applications or workloads, or across development, testing, staging and production environments.

Changing credentials

Generally, credentials should not need to be changed; however, some events may necessitate a requirement for credentials to be changed. For user accounts, this can include credentials being compromised (such as appearing in an online data breach database) or being suspected of being

compromised (such as when malicious actors gain access to a network), being discovered stored on systems in the clear, being transferred across networks in the clear, or when membership of shared user accounts change.

Similarly, static credentials used by applications and workloads should be changed when they are compromised or suspected of being compromised, discovered stored on systems in the clear, or discovered being transferred across networks in the clear.

Control: ISM-1590; Revision: 5; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Credentials for user accounts are changed if:

- *they are compromised or suspected of being compromised*
- *they are discovered stored on systems in the clear*
- *they are discovered being transferred across networks in the clear*
- *membership of a shared user account changes.*

Control: ISM-2144; Revision: 0; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Static credentials used by applications and workloads are changed if:

- *they are compromised or suspected of being compromised*
- *they are discovered stored on systems in the clear*
- *they are discovered being transferred across networks in the clear.*

Control: ISM-1955; Revision: 1; Updated: Dec-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Credentials for computer accounts are changed if they are compromised, they are suspected of being compromised or they have not been changed in the past 30 days.

Control: ISM-1847; Revision: 2; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Credentials for the Kerberos Key Distribution Center's service account (KRBTGT) are changed twice, allowing for replication to all Microsoft AD DS domain controllers in-between each change, if the domain has been directly compromised, the domain is suspected of being compromised or they have not been changed in the past six months.

Control: ISM-1956; Revision: 1; Updated: Dec-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Microsoft AD FS token-signing and encryption certificates are changed twice in quick succession if they are compromised, they are suspected of being compromised or they have not been changed in the past 12 months.

Revoking credentials

Credentials that are no longer required should be revoked to prevent their subsequent use to gain unauthorised access to systems and their resources. This includes credentials associated with user accounts that are no longer required, as well as static credentials used by applications and workloads that have been decommissioned or are no longer required for access.

Control: ISM-2145; Revision: 0; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Credentials for user accounts are revoked when they are no longer required.

Control: ISM-2146; Revision: 0; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Static credentials used by applications and workloads are revoked when they are no longer required.

Protecting credentials

Obscuring credentials as they are entered into systems can assist in protecting them against screen scrapers and shoulder surfers. In addition, physical credentials, such as written down credentials (e.g. passwords) and dedicated devices that store or generate credentials (e.g. security keys, smart cards and one-time password tokens), when kept together with systems they are used to authenticate to, can increase the likelihood of malicious actors gaining unauthorised access to systems. For example, when smart cards are left on card readers, one-time password tokens are left in laptop computer bags, security keys are left connected to computers or passwords are written down and stuck to computer monitors. To reduce this security risk, physical credentials should be kept separate from systems they are used to authenticate to, except for when performing authentication activities.

If storing credentials on systems, sufficient protection should be implemented to prevent them from being compromised. For example, credentials can be stored in a password manager or hardware security module, while credentials stored in a database should be hashed, salted and stretched.

When using Microsoft Windows systems, Local Security Authority protection, Credential Guard and Remote Credential Guard functionality, all preferably with a Unified Extensible Firmware Interface lock, can be enabled to provide additional protection for credentials. In addition, malicious actors that have access to systems may attempt to steal cached credentials. To reduce this security risk, cached credentials should be limited to only one previous logon.

Finally, an organisation should regularly scan their systems to detect and remediate any credentials that are being stored in an unprotected manner, such as in the clear in documents, configuration files, network file shares, software repositories, cloud storage or other data repositories.

Control: ISM-1597; Revision: 0; Updated: Aug-20; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Credentials are obscured as they are entered into systems.

Control: ISM-1980; Revision: 0; Updated: Dec-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Credential hint functionality is not used for systems.

Control: ISM-0418; Revision: 7; Updated: Dec-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Physical credentials are kept separate from systems they are used to authenticate to, except for when performing authentication activities.

Control: ISM-1402; Revision: 6; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Credentials stored on systems are protected by a password manager; a hardware security module; or by salting, hashing and stretching them before storage within a database.

Control: ISM-1957; Revision: 0; Updated: Sep-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Private keys for Microsoft AD CS certification authority servers are protected by a hardware security module.

Control: ISM-1861; Revision: 2; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: ML3
Local Security Authority protection functionality is enabled.

Control: ISM-1686; Revision: 1; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: ML3
Credential Guard functionality is enabled.

Control: ISM-1897; Revision: 0; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: ML3
Remote Credential Guard functionality is enabled.

Control: ISM-1749; Revision: 0; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Cached credentials are limited to one previous logon.

Control: ISM-1875; Revision: 1; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Systems are scanned at least monthly to identify any credentials that are being stored in the clear.

Protecting authentication artefacts

Once a user has authenticated, malicious actors may target the resulting authentication artefacts rather than the user's credentials. Adversary-in-the-middle phishing and information-stealing malware can capture these authentication artefacts and replay them to bypass authentication measures, including multi-factor authentication. As such, it is important that authentication artefacts are protected to limit their usefulness to malicious actors if stolen. This includes cryptographically binding authentication artefacts to the devices on which they were issued to help prevent successful replay from other devices.

In addition, revoking active sessions and refresh tokens when trust in a user account or device changes reduces the window in which stolen authentication artefacts remain useful to malicious actors. This includes when credentials are reset or re-enrolled, when credentials are compromised or suspected of being compromised, when a device no longer meets compliance requirements, or when high-risk sign-in activity is detected. Notably, revoking active sessions and refresh tokens following credential resets and re-enrolments is an important companion to verifying human user identities when such requests are made, as malicious actors that have socially engineered a credential reset may seek to establish durable access via stolen authentication artefacts before the activity is discovered.

Control: ISM-2147; Revision: 0; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Authentication tokens, session cookies and refresh tokens are cryptographically bound to the device on which they were issued.

Control: ISM-2148; Revision: 0; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Active sessions, refresh tokens and other authentication artefacts are revoked when credentials are reset or re-enrolled, when credentials are compromised or suspected of being compromised, when a device no longer meets compliance requirements, or when high-risk sign-in activity is detected.

Further information

Further information on randomly generating passphrases is available from the Electronic Frontier Foundation while a random dice roller is available from RANDOM.ORG.

Further information on how to secure group Managed Service Accounts in Microsoft Windows Server is available from Microsoft.

Further information on changing credentials for the Kerberos Key Distribution Center's service account can be found in Microsoft's *Active Directory accounts* and *Active Directory Forest Recovery - Reset the krbtgt password* publications. A script for changing credentials for this service account is also available from Microsoft.

Further information on Local Security Authority protection functionality is available from Microsoft.

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

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

Copyright

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the Department of the Prime Minister and Cabinet website (https://www.pmc.gov.au/resources/commonwealth-coat-arms-information-and-guidelines).

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre