16.1. Identification, Authentication and Authorisation

Objective

16.1.1. Access to information and systems is securely controlled and only provided to authorised entities, at all times.

Context

Scope

16.1.2. Identification and authentication requirements are implemented in order to provide a secure means of access to information and systems.

Background

16.1.3. The NZ Government Department of Internal Affairs (DIA) publishes a set of Identification Standards that work together to provide assurance that an organisation has the right information about the right entities and can use that to make access control decisions to ensure access is only provided to authorised entities.

16.1.4. Controls in these Identification Standards related to identification and authentication are provided to facilitate credential provider's ability to manage credentials to a level that will reduce the introduction of systemic risk across the NZ Government. The controls are also broadly acceptable to relying parties that are managing access to NZ Government information and information systems.

16.1.5. Access Controls can be defined as any mechanism by which an individual, system, or application grants or revokes the right to access a location, system, data, or perform an action.

16.1.6. Although access controls remain fundamentally the same in any context, specific guidance and controls around virtualisation, cloud environments, microservices and containerisation are documented in Chapter 22 – Enterprise Systems Security and Chapter 23 – Public Cloud Security.

New Zealand Government Identification Standards

16.1.7. The New Zealand Government publishes four Identification Standards:

- Information Assurance
- Binding Assurance
- Authentication Assurance
- Federation Assurance

16.1.8. The first three standards are relevant to Relying Parties; all standards are relevant to Credential Providers.

Methods for user identification and authentication

16.1.9. Authentication is detailed in the Authentication Assurance Standard and is the process by which an entity is verified before access permissions are confirmed, and access is granted to the entity requesting authentication.

16.1.10. Authentication can be achieved by various means, including biometrics, cryptographic tokens, software tokens, passkeys, passphrases, passwords and smartcards.

NB: Where the NZISM refers to passwords it equally applies to passphrases.

16.1.11. Authentication mechanisms are invariably described in terms of factors of authentication as follows:

- Something the entity has – the possession factor.
- Something the entity knows – the knowledge factor.
- Something the entity is or does – the biometric factor.

16.1.12. These authentication mechanisms may not provide sufficient protection when used in isolation. Using two or more authentication mechanisms provides additional security and is strongly advised.

Methods for identification and authentication management

16.1.13. There are two distinct roles performed for identification management – a credential provider, and a relying party.

- **Credential providers** establish credentials that are used by relying parties to identify and authenticate users and systems. Entities expect these credentials to enable provision of service to the right systems.
- **Relying parties** provide the services that are being accessed by the authorised users (entities) and systems. Relying parties use an entities' credentials to ensure the right authorisations are in place prior to access of data or systems.

NB: **Entities** (eg, a person or system) use credentials from the credential provider to gain a service from a relying party. The entity can either present their credentials to a service provider or use the credential provider to directly present the credentials to the relying party.

Authenticating across multiple sign-ons

16.1.14. Federation allows credential service providers to provide authentication and subscriber attributes to a number of separately administered relying parties. These relying parties may use more than one credential service provider.

16.1.15. Definitions relating to Federation include:

- Federated Identification Management (FIM) - Where a credential from a single credential provider may be used by a number of relying parties through an agreement that signifies trust between parties. This trust agreement is usually implemented through a process of federation between the parties.
- Single Sign On (SSO) - Where credentials, specifically authenticators, are used within the context of a single organisation/domain, system owners can exercise more discretion regarding the acceptance of risk associated with the selection of identification, authentication, and authorisation controls.

Identification and authentication controls with Zero Trust

16.1.16. Zero Trust (ZT) is a security concept based around a central principle of 'never trust, always verify', being maintained through enforcing accurate, least privilege per-request access decisions on systems, services and networks.

16.1.17. ZT means continuous verification and enforcement of access controls, regardless of location. This includes continuous authentication of entities on internal network and zones.

16.1.18. Implementation of ZT principles requires policy and procedure changes within organisations. The principles also guide and control through Network Access (ZTNA). Zero Trust implemented at a micro level (eg, segmentation of networks, applications, environments, user and process-based) allows more granular control of access enforcement of least privilege access policies.

16.1.19. SSO and FIM support ZT principles with a centralised model to approve and remove access to entities. The timely revocation of accesses when no longer required ensures strengthened security to services and data at a micro level.

16.1.20. Cloud services have been using a Zero Trust approach to security where policy decisions and policy enforcement points are used to control access based on authentication and privilege assignments. More information can be found in Chapter 23 - Public Cloud Security (reference 23.3.12).

16.1.21. Successful implementation of Access Controls for ZT at an organisation level can be supported by the following methods:

- Implementation of Multi-Factor Authentication (MFA).
- Use of adaptive authentication based on contextual factors (e.g. location, device, behaviour).
- Least Privilege Access – enforced at a micro level within systems and networks. This may also include just-in-time (JIT) delivery of privileges.
- Centralisation of user accounts and accesses.
- Passwordless authentication models adopted within organisations.

References

16.1.22. Additional information relating to Identification, Authentication and Authorisation can be found at:

Title	Publisher	Source
Identification Standards	DIA	Identification Management Standards | NZ Digital government
Authentication Assurance Standard	DIA	Authentication Assurance Standard | NZ Digital government
Assurance Services Panel	GCDO	GCDO Assurance Services Panel | NZ Digital government
Mitigating the use of stolen credentials	ASD	PROTECT - Mitigating the Use of Stolen Credentials (October 2021).pdf (cyber.gov.au)
Identity & Access Management	NIST	Identity & Access Management | NIST
Implementing a Zero Trust Architecture	NIST - NCCoE	Implementing a Zero Trust Architecture | NCCoE
Passwordless Authentication	Microsoft Security	Passwordless authentication | Microsoft Security
AWS Identity and Access Management	AWS	Access Management- AWS Identity and Access Management (IAM) - AWS
Identity and Network Access	Microsoft	Identity and Access Management System | Microsoft Security
Password Storage Cheat Sheet	OWASP	Password Storage - OWASP Cheat Sheet Series

PSR references

16.1.23. Relevant PSR requirements can be found at:

Reference	Title	Source
PSR Mandatory Requirements	GOV5, GOV6, GOV7, INFOSEC1, INFOSEC2, INFOSEC3, INFOSEC4, PERSEC1, PERSEC2, PERSEC3, PERSEC4, PHYSEC1, PHYSEC2	Home | Protective Security Requirements Security governance (GOV) | Protective Security Requirements Information security (INFOSEC) | Protective Security Requirements Personnel security (PERSEC) | Protective Security Requirements Physical security (PHYSEC) | Protective Security Requirements

Rationale & Controls

Policies and procedures

16.1.24.R.01. **Rationale**

Developing policies and procedures will ensure consistency in managing identification, authentication and authorisation across agency systems. Refer also to Section 16.4 – Privileged Access Management.

16.1.24.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:1827]

Agencies MUST:

- develop, implement and maintain a set of policies and procedures covering all system users':

    - identification;
    - authentication;
    - authorisation;
    - privileged access identification and management; and
- make their system users aware of the agency's policies and procedures.

Implement zero trust principles

16.1.25.R.01. **Rationale**

Agencies can be especially vulnerable to threats when internal systems can be accessed externally from the organisation. Implementing access through Zero Trust principles and architecture provides organisations with an enhanced security posture to ensure potential access threats on systems are minimised.

16.1.25.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:7541]

Agencies SHOULD design and implement Zero Trust principles and architecture to strengthen identification management.

Unique system user identification

16.1.26.R.01. **Rationale**

Having uniquely identifiable system users ensures accountability.

16.1.26.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:1829]

Agencies MUST ensure that all system users are:

- uniquely identifiable; and
- authorised and authenticated on each occasion that access is granted to a system.

Shared accounts

16.1.27.R.01. **Rationale**

Sharing of credentials (eg, passwords and UserIDs) may be convenient but doing so is highly risky. Shared credentials can defeat accountability and the attribution and non-repudiation principles of access controls. The risk increases when shared credentials are used for administrative privileges or access to classified information.

16.1.27.C.01. **Control System Classifications(s): Secret, Confidential, Top Secret; Compliance: Must Not** [CID:1832]

Agencies MUST NOT use shared credentials to access accounts.

16.1.27.C.02. **Control System Classifications(s): All Classifications; Compliance: Must Not** [CID:7542]

Agencies MUST NOT use shared credentials to access administrator or privileged access accounts.

NB: Break Glass accounts are exempt from this control. For further guidance on Break Glass accounts see Emergency accounts (Break Glass accounts section).

16.1.27.C.03. **Control System Classifications(s): All Classifications; Compliance: Should Not** [CID:1833]

Agencies SHOULD NOT use shared credentials to access accounts.

System user identification for shared accounts

16.1.28.R.01. **Rationale**

Agencies may have a compelling business reason for the use of shared accounts. These may include anonymous, guest and temporary employee credentials.

16.1.28.R.02. **Rationale**

As shared accounts are non-entity specific, agencies will need to determine an appropriate method for attributing actions undertaken using such accounts to specific personnel, and these are recorded or documented.

16.1.28.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:1837]

If agencies choose to allow shared, non user-specific accounts they MUST ensure that an independent means of determining the identification of the system user is implemented and logged.

Methods for system user identification and authentication

16.1.29.R.01. **Rationale**

A personal identification number (PIN) is typically short in length and employs a small character set, making it susceptible to brute force attacks.

16.1.29.R.02. **Rationale**

Combining multiple methods when authenticating users can help to create a layered defence, making it harder for successful brute force attacks. Eg, a PIN connected to a hardware backed security measure like a trusted platform module (TPM) means the PIN is bound to a specific device.

16.1.29.C.01. **Control System Classifications(s): All Classifications; Compliance: Must Not** [CID:1840]

Agencies MUST NOT use a numerical password (or personal identification number) as the sole method of authenticating a system user to access a system.

16.1.29.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1841]

Agencies SHOULD use multi-factor authentication (MFA) when identifying and authenticating system users.

Centralisation of Identification and Authentication Management

16.1.30.R.01. **Rationale**

Centralising authentication and the reliance on single credentials to access multiple systems and wider organisations (eg, SSO, FIM) enhances an organisation's security posture through:

- centralisation to control access (joiners, movers, leavers);
- reducing risk of password fatigue;
- enforcing strong access controls;
- enforcing password policies; and
- reducing the risk of misconfiguration.

16.1.30.R.02. **Rationale**

Centralised access management systems are beneficial to agencies; however, they also have the potential to introduce additional system risk to organisations. FIM may introduce additional risk due to sharing of credentials across external organisations.

16.1.30.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:7543]

Agencies SHOULD assess and determine the risk of centralised access management systems, including SSO, to safely manage integration into systems and when using FIM.

Passwords and policies

16.1.31.R.01. **Rationale**

Passwords have historically been the primary authentication mechanism for almost all information systems and are a fundamental part of access and authentication. While there are other forms of authentication mechanisms available that can provide more robust security to attack vectors and threats in the environment, passwords remain a cost-effective baseline for authentication systems.

16.1.31.R.02. **Rationale**

Passwords have traditionally been the terminology used for the memorised secrets allowing access and authorisation onto systems. The term 'passphrases' is often referred to in place of 'passwords', as it denotes longer (more secure), easier to remember memorised secrets.

Where the NZISM references passwords, it equally applies to passphrases.

16.1.31.R.03. **Rationale**

Passwords are subject to three primary groups of risks:

1. Intentional sharing.
2. Theft, loss or compromise.
3. Guessing and cracking.

16.1.31.R.04. **Rationale**

Associated with these risk groups are four principal methods of attacking passwords:

1. Interactive attempts including brute force attacks or some knowledge of the user or organisation.
2. Obtaining through social engineering or phishing.

3. Compromising through oversight, observation, use of keyloggers, cameras etc.
4. Decryption of network traffic interception, misconfiguration, data capture etc.

16.1.31.R.05. **Rationale**

Password controls detailed in this section are designed to manage and mitigate these risk groups and attack methods. These controls will only be effective alongside organisation specific password policies and mandatory training for all system users.

16.1.31.R.06. **Rationale**

Whilst passwords provide some security to systems, they still carry inherent risks. A layered approach to authentication is essential to ensuring systems and organisations are not made vulnerable from the authentication mechanisms used.

This includes establishing additional system controls alongside passwords. For example, ensuring MFA is mandatory in organisations, or mandating secure storage of passwords within organisations.

16.1.31.R.07. **Rationale**

Mandatory training for all employees, including senior management, on these policies is essential to manage and mitigate risks associated with password attacks.

16.1.31.R.08. **Rationale**

While implementing long and complex passwords is regarded as a fundamental security practice, it does not fully mitigate the risks associated with password-related attacks. A primary challenge can come from human behaviours. Unless password generators are employed, users often create non-unique passwords based on predictable patterns, even for lengthy credentials.

Multi-layered approaches such as MFA, passwordless authentication, and password expiries can help to mitigate these attacks.

16.1.31.R.09. **Rationale**

Ensure a balance of security and usability considerations when deciding on implementing a password expiry policy for the organisation.

16.1.31.R.10. **Rationale**

It is vital that the security posture of a system is not weakened through authentication mechanisms. This relies on increasing the authentication and authorisation controls, including moving to appropriate multi-factor authentication, and stronger identify access management.

16.1.31.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:7544]

Agencies MUST ensure adequate password policies are implemented and enforced across all systems.

16.1.31.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:7545]

Agencies MUST implement a password policy enforcing **at least annual** password changes on systems that **have not** implemented MFA or passwordless authentication.

16.1.31.C.03. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:7546]

Agencies MUST implement a password policy enforcing:

- A minimum password length of 16 characters (e.g four words).
- Passwords must be **long, strong and unique**. This means passwords must be a minimum character length, and are a combination of unique random words, characters or numbers.

NB: no explicit complexity requirements are enforced (e.g. numbers or special characters), however passwords must be unique, or random and **may** include special characters and numbers to achieve this.

16.1.31.C.04. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:7547]

To ensure security of systems are not weakened through authentication mechanisms, at a minimum, agencies MUST:

- apply MFA appropriately (refer to controls in Section 16.7);
- ensure authentication secrets (including passwords) are securely stored;
- remove knowledge-based questions from authentication process (eg, dog's name, first school etc.);
- new passwords are screened to reduce the likelihood of previously compromised passwords;
- remove hints from authentication process; and
- change passwords when a suspected or known compromise of an account has occurred.

16.1.31.C.05. **Control System Classifications(s): All Classifications; Compliance: Must Not** [CID:1869]

Agencies MUST NOT:

- allow predictable reset passwords;
- store passwords in the clear on the system; and
- reuse passwords when resetting multiple accounts.

16.1.31.C.06. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:7548]

Agencies SHOULD consider the use of location-based factors in the authentication process, (e.g., Users must be at an expected location (city, country, IP address) and provide the correct credentials for the authentication to succeed).

16.1.31.C.07. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:7549]

When creating password policies, agencies SHOULD consider implementing annual password changes.

Protecting stored authentication information

16.1.32.R.01. **Rationale**

When moving to passwordless authentication, agencies SHOULD carry out a risk assessment and evaluate passwordless authentication models to choose authentication mechanisms and factors that best fit the organisation's security and authentication requirements.

16.1.32.C.01. **Control System Classifications(s): All Classifications; Compliance: Must Not** [CID:1844]

Agencies MUST NOT allow storage of unprotected authentication information that grants system access, or decrypts an encrypted device, to be located on, or with the system or device, to which the authentication information grants access.

Protecting authentication data in transit

16.1.33.R.01. **Rationale**

Secure transmission of authentication information will reduce the risk of interception and subsequent use of the authentication information by an attacker to access a system under the guise of a valid system user.

16.1.33.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:1847]

Agencies MUST ensure that system authentication data is protected when in transit on organisation networks or All-of-Government systems.

Hashing

16.1.34.R.01. **Rationale**

Hashing is a means of protecting stored passwords or other authentication secrets by cryptographically converting the password to fixed length ciphertext. This protects against incidents where an unsanctioned copy of the password or authentication database has been made, exported or the database otherwise compromised. Approved cryptographic protocols are discussed in Chapter 17 - Cryptography. See also section 17.2 - Approved Cryptographic Algorithms for discussion on the use of salts to strengthen the cryptographic resistance of a hash.

16.1.34.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:6553]

Password and other authentication secrets MUST be hashed before storage using an approved cryptographic protocol and algorithm. See Chapter 17 – Cryptography.

16.1.34.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:7562]

Passwords and other authentication secrets MUST be stored securely including being:

- salted (32 bits or more),
    - salts should be unique to each password and should be randomly generated.
- hashed (HMAC using SHA-2/3), and
- "stretched" (such as PBKDF2 with at least:
    - 600k iterations with internal hash function of HMAC-SHA-256; or
    - 210k iterations with internal hash function of HMAC-SHA-512).

Identification of foreign nationals

16.1.35.R.01. **Rationale**

Where systems contain NZEO or other nationalities releasability marked or protectively marked information, and foreign nationals have access to such systems, it is important that agencies implement appropriate security measures to assist in identifying users that are foreign nationals. Such measures will assist in preventing the release of sensitive information to those not authorised to access it.

16.1.35.C.01.

Control System Classifications(s): All Classifications; Compliance: Must [CID:1850]

Where systems contain NZEO or other nationalities releasability marked or protectively marked information, agencies MUST provide a mechanism that allows system users and processes to identify users who are foreign nationals, including seconded foreign nationals.

16.1.35.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1851]

Agencies using NZEO systems SHOULD ensure that identification includes specific nationality for all foreign nationals, including seconded foreign nationals.

Resetting passwords and authentication vectors

16.1.36.R.01. **Rationale**

To reduce the likelihood of social engineering attacks aimed at service desks, agencies will need to ensure that system users provide sufficient evidence to prove they are the owner of the system account when requesting a password reset for their system account.

This evidence could be in the form of:

- the system user physically presenting themselves and their security pass to service desk personnel who then reset their password;
- physically presenting themselves to a known authorised colleague who uses an approved online tool to reset their password; or
- providing a MFA code.

16.1.36.R.02. **Rationale**

Issuing complex reset passwords maintains the security of the user account during the reset process. This can also present an opportunity to demonstrate the selection of strong passwords.

16.1.36.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:1875]

Agencies MUST ensure system users provide sufficient evidence to prove they are the owner of the account when requesting a password reset for their system account or making changes to their multi-factor authenticators.

16.1.36.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:7551]

Where passwords are not set by the account holder, agencies MUST use temporary passwords when resetting system user accounts.

16.1.36.C.03. **Control System Classifications(s): All Classifications; Compliance: Should Not** [CID:7552]

Agencies SHOULD NOT use single factor authentication when changing users' Multi-Factor Authentication details.

Securing Passwords

16.1.37.R.01. **Rationale**

Security of passwords is fundamental to ensuring system security across organisations. Password policies need to include how passwords are kept secure while passwords are in transit, stored or being used.

16.1.37.R.02. **Rationale**

Use of password managers within agencies provide employees a system to generate, secure, store, and distribute passwords. The paradigm behind a password manager is for an individual to store passwords and memorised secrets securely in a vault behind a single strong password. This generally means authentication secrets are at less risk of attacks and help to support a strengthened organisation security posture.

16.1.37.R.03. **Rationale**

Password managers store highly sensitive data, therefore it is imperative that agencies have completed a risk analysis and due diligence to ensure that passwords are suitably protected with the password manager, and are not accessible to third parties.

16.1.37.R.04. **Rationale**

When using password managers, passwords may be stored in an encrypted form rather than salted and hashed. This is required for a password manager to function, and the technical risks associated with this are considered acceptable when addressing the risks of password re-use due to users needing to remember many different passwords. To mitigate this additional technical risk we recommend using MFA on the password manager.

16.1.37.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:7558]

Password managers provide no additional security to the sign-in password. Agencies using password managers MUST ensure sign-in passwords adhere to the password security policies used by the organisation.

16.1.37.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:7559]

Agencies using password managers SHOULD consider the use of MFA to access the password manager.

Passwordless Authentication

16.1.38.R.01. **Rationale**

Use of passwords are a common method of authenticating entities. Due to high reliance (from organisations) on passwords to control accesses, threat actors commonly use passwords as an attack vector to gain access into networks.

16.1.38.R.02. **Rationale**

Passwordless authentication provides additional security mechanisms by moving away from 'something you know' and placing emphasis on other verification factors such as 'something you have' or 'something you are'. These alternative authentication models can rely on other factors such as something you are or something you have (eg, biometrics, tokens, and authentication applications).

16.1.38.R.03. **Rationale**

Implementation of these alternative authentication models can be accomplished based on systems requirements and the access controls needs of organisations and systems. These alternative authentication models provide a range of security levels. Security levels of these passwordless authentication models, and how these are implemented in agencies have a significant impact on the level of security provided.

16.1.38.R.04. **Rationale**

Prior to moving to passwordless authentication, agencies will need to consider cost, risks, and benefits to identify which authentication models are best suited to their systems.

16.1.38.R.05. **Rationale**

Passwordless authentication **does not** mean 'no authentication'.

16.1.38.R.06. **Rationale**

Passwordless authentication moves systems toward possession factors (something you have or something you are) and away from using memorised secrets (something you know) as the primary way to authenticate users. This can provide additional security measures to ensure adequate authentication, and when used in conjunction with adequate controls and security policies, passwordless authentication can minimise the success of a phishing attack.

16.1.38.R.07. **Rationale**

Security strength of passwordless authentication models rely on what and how organisations implement architecture to support this. Although implementation of passwordless authentication by itself can be more secure than passwords, MFA used in conjunction with this architecture will significantly minimise the risk of compromise within agencies by adding another layer of security.

16.1.38.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:7556]

When moving to passwordless authentication, agencies SHOULD carry out a risk assessment and evaluate passwordless authentication models to choose authentication mechanisms and factors that best fit the organisation's security and authentication requirements.

Disabling vulnerable authentication mechanisms

16.1.39.R.01. **Rationale**

The use of adequate and secure authentication mechanisms is an essential part of ensuring and maintaining secure systems and user accounts. Replacing mechanisms with known vulnerabilities for products with stronger authentication protocols should be considered.

16.1.39.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:7554]

Agencies MUST ensure authentication methods that are susceptible to replay attacks are disabled.

16.1.39.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:1878]

Agencies MUST disable LAN Manager for password authentication on workstations and servers.

Session termination

16.1.40.R.01. **Rationale**

Developing a policy to automatically logout workstations after an appropriate time of inactivity will assist in preventing the compromise of unattended workstations.

16.1.40.R.02. **Rationale**

Restarting of workstations after automatically logging out ensures cached credentials, authentication tokens or session keys that may persist after logging out are removed. It can also ensure any services and drivers are securely reloaded on systems.

16.1.40.R.03. **Rationale**

Session tokens are a vector for account compromise. The session length of a session token is the lifespan of the token; specifically, how long the user remains authenticated before reauthentication is required. The length of these session tokens should be considered to minimise risk of attacks through this mechanism. Length of session tokens will be different across organisations and systems, based on risk appetite and specific requirements.

16.1.40.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1881]

Agencies SHOULD develop and implement a policy to automatically logout and shutdown workstations after an appropriate time of inactivity. This includes invalidating any session tokens.

Screen and session locking

16.1.41.R.01. **Rationale**

Screen and session locking will prevent access to an unattended workstation.

16.1.41.R.02. **Rationale**

Ensuring that the screen does not appear to be turned off before entering the locked state will prevent system users from forgetting they are still logged in and will prevent other system users from mistakenly thinking there is a problem with a workstation and resetting it.

16.1.41.C.01. **Control System Classifications(s): Confidential, Top Secret, Secret; Compliance: Must** [CID:1885]

Agencies MUST:

- configure systems with a screen and session lock;
- configure the lock to activate:
    - after a maximum of 10 minutes of system user inactivity; or
    - if manually activated by the system user;
- configure the lock to completely conceal all information on the screen;
- ensure that the screen is not turned off or enters a power saving state before the screen or session lock is activated;
- have the user reauthenticate to unlock the system; and deny users the ability to disable the locking mechanism.

16.1.41.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1886]

Agencies SHOULD:

- configure systems with a session or screen lock;
- configure the lock to activate:
    - after a maximum of 10 minutes of system user inactivity; or
    - if manually activated by the system user;
- configure the lock to completely conceal all information on the screen;
- ensure that the screen is not turned off or enters a power saving state before the screen or session lock is activated;
- have the system user reauthenticate to unlock the system; and
- deny system users the ability to disable the locking mechanism.

Suspension of access

16.1.42.R.01. **Rationale**

Locking a user account after a specified number of failed logon attempts will reduce the success of brute force attacks.

16.1.42.R.02. **Rationale**

Removing a system user account when it is no longer required will prevent personnel from accessing their old account and reduce the number of accounts that an attacker can target.

16.1.42.R.03. **Rationale**

Suspending inactive accounts after a specified number of days will reduce the number of accounts that an attacker can target.

16.1.42.R.04. **Rationale**

Investigating repeated account lockouts will reduce the security risk of any ongoing brute force logon attempts or inappropriate use of user accounts for services and allow security management to act accordingly.

16.1.42.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:1892]

Agencies MUST:

- Record all successful and failed logon attempts;
- lock system user accounts after three failed logon attempts;
- use a temporary lock out feature to unlock system (max [] times);
- have a system administrator reset locked accounts if [] times is superseded;
- remove or suspend system user accounts as soon as possible when personnel no longer need access due to changing roles or leaving the organisation; and
- remove or suspend inactive accounts after a specified number of days.

NB: Agencies can determine the risk of using a temporary lock out feature on their specific systems.

[] indicates the chosen 'value of times' an agency has decided to use for the temporary lock out feature.

Investigating repeated account lockouts

16.1.43.R.01. **Rationale**

Repeated account lockouts may be an indicator of attempted account compromise.

16.1.43.C.01. **Control System Classifications(s): Confidential, Secret, Top Secret; Compliance: Should** [CID:1896]

Agencies SHOULD ensure that repeated account lockouts are investigated before reauthorising access.

Logon banner

16.1.44.R.01. **Rationale**

A logon banner for a system serves to remind system users of their responsibilities when using the system. It may also be described as a “Splash Screen”, “Acceptable Use Policy” or “User Consent Screen”.

16.1.44.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1899]

Agencies SHOULD have a logon banner that requires a system user to acknowledge and accept their security responsibilities before access to the system is granted.

16.1.44.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1900]

Agencies SHOULD seek legal advice on the exact wording of logon banners.

16.1.44.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1901]

Agency logon banners SHOULD cover issues such as:

- the system’s classification;
- access only being permitted to authorised system users;
- the system user’s agreement to abide by relevant security policies;
- the system user’s awareness of the possibility that system usage is being monitored;
- the definition of acceptable use for the system; and
- legal ramifications of violating the relevant policies.