Department of Planning and Environment

Corporate policy

# Access Control Policy

## Purpose of this policy

The Department of Planning and Environment (the department) is committed to protecting the data it manages. Effective rules are enforced to ensure requirements are met for access to departmental assets. This policy describes the department's approach to managing authentication as it relates to business systems and ICT services. It aims to provide a consistent and integrated approach across the department and is aligned to the Code of Ethics and Conduct, the NSW Cyber Security Policy and the NSW Cyber Security Strategy.

## To whom this policy applies

This policy applies to all employees accessing the department's information and ICT resources, including individuals seconded from other organisations, volunteers, contingent or labour hire workers, professional services contractors and consultants.

## Policy statement

### Principle of least privilege

All accounts will follow the principle of least privilege. This means that, to help protect the security of the department's information, employees will have the minimum privileges on the department's ICT systems necessary to perform their role.

### Principle of need to know

Access is only provided to information and resources that are necessary to perform a role, noting that, under the Code of Ethics and Conduct, people leaders are responsible for ensuring their employees have access to the records they require to perform their role.

### User registration

- All user registrations are to take place via the approved process in the applicable service centre.
- Each user is to be granted a unique identifier.
- A unique identifier must not be reused after an account has been terminated.
- Standard user profiles must be created for common roles.
- A prerequisite for access is the agreement to the Code of Ethics and Conduct, Acceptable Use Policy and any related policy or standard issued under the order.
- Access to be granted based on role and business requirements.
- Accounts for contractors and non-permanent employees must contain an expiry date, same as their contract end date.

## Privileged, system and service accounts

- An approved business case is required for all privileged, system and service accounts (business case requires both people leader and Digital Information Office [DIO] approval).
- The account request must be submitted using the form on the applicable service centre.
- All privileged, system and service account passwords must conform with the standards defined in Appendix 3.
- Users must not use the same password for their standard account and privileged account.
- Privileged, system and service accounts must be distinguishable from standard user accounts.
- Privileged, system and service accounts must not be used for browsing the internet, email or downloading files from the internet.
- Account username and password must not be hardcoded.
- Account access and the activities undertaken with these accounts must be auditable.

## Password management

- Passwords must never be shared.
- If the confidentiality of a password is breached or suspected of being breached, the account owner must change the password as soon as possible and if this is not possible contact the service centre and request for the account to be suspended.
- A temporary password must be issued upon account creation. Users must be forced to change their password at first login or once the minimum time period has elapsed.
- Temporary passwords must be unique and communicated in a secure manner.
- Passwords must conform to the minimum standards as outlined in the Appendix 3.
- Passwords must be salted and hashed with an approved hashing algorithm for storage to ensure their confidentiality.
- A self-service password management system must be implemented for password resets.
- For password resets that cannot be performed via the self-service system, a user must supply verification of their identity, such as their Employee ID.
- Passwords must be managed via a password management system where possible.
- Applications/browsers must not remember/store passwords to restricted systems or data.
- Manufacturer passwords must be changed from the default and conform with Appendix 3.

## Review of accounts

- All user accounts must be reviewed at least annually.
- Privileged system and service accounts are subject to review twice per year at a minimum.
- User accounts must be reviewed upon change of roles to prevent privilege creep.

## Account suspension

- An individual’s account(s) must be suspended once DIO has been notified that the individual is no longer working for or performing work on behalf of the department.
- An individual’s account(s) that is deemed inactive according to the applicable HR system must be disabled until a request is made to the service centre for reactivation.
- An account holder is subject to investigation or undergoing disciplinary action, their account may be suspended or reduced access implemented based on a business risk assessment.
- A contractor/non-permanent employee account must be suspended once the end of their contract period has been reached without renewal.
- A third-party vendor/business partner account must be suspended when they no longer require access to perform a specific function.

## Account management

- Authentication information is stored separately from a system to which it grants access.
- Notification of account changes must be made as soon as possible to DIO to ensure timely responses to change.
- User accounts will be disabled automatically after three months of inactivity
- Suspended accounts must be unsubscribed from groups, email and have their password changed, unless otherwise stated.
- Expired accounts must be moved to a holding container or deleted after 60 days or at the discretion of the Chief Digital and Information Officer.
- Email accounts must have an auto-reply configured for up to 60 days or as per business requirements.
- No expectation of access to ICT systems, including email forward facility will be provided for account holders no longer performing work on behalf of the department. This includes personal email or files contained within departmental systems.
- If an account holder who has left had a privileged account, it must also be suspended as per the first point under Account suspension.
- If an account holder who has left, also had access to a system/service account, the password(s) for the account(s) must be changed.
- Departmental devices will be configured to lock automatically after a predefined period (see Appendix 4) of inactivity, requiring the password/pin to be re-entered for access.
- Remote sessions must be locked after a predefined period of inactivity, see Appendix 4.

## Secure access

- Login banners must advise users of the terms and conditions of access where possible.
- No help facility must be offered to users during login.
- For failed logins, no indication must be provided to advise the user of whether it was an incorrect username or password.

- System logins must be configured to comply with the standards in the appendices.
- Where possible the previous login time and date must be displayed after successfully accessing a system.
- Passwords must be obscured during login and never transmitted in clear text.

## Multi-factor authentication

- Multi-factor authentication mechanisms must be implemented according to the business classification and risk of the information held within the system.
- Multi-factor authentication mechanisms must be implemented for accessing departmental assets hosted externally from outside the department network and on non-departmental devices according to the business classification and risk of the information to be accessed;
- Employees must always implement multi-factor authentication even when not compulsory.

## Remote access

- Remote access is only available through authorised mechanisms.
- All remote access must be authenticated.
- Where configurable, remote access sessions must time-out after a defined period.
- Where configurable, remote access sessions must expire after a defined period of inactivity.
- Where remote access is via a smart device or non-departmental asset, the device must have a pin or password to protect confidentiality.

## Return of ICT assets

- Whenever account access is terminated, ICT assets related to the provision of that account must be returned and accounted for prior to the account holder’s departure.
- The collection of assets is the responsibility of the account holder’s people leader or delegate.

## Logging and monitoring

- All systems that require authentication must log the following events:
  - date and time of the even
  - IP address the event originated from
  - types of events to log:
    - logon events
    - failed logon events
    - logoff events.
- Logs must be protected from unauthorised access, modification and deletion.
- Logs must be monitored utilising automated systems that notify by email/service centre ticket generation on the breach of a defined rule.
- Logs not monitored via automated systems must be periodically reviewed.

### Exemptions

- Exemptions to this policy must comply with the ISMS Exemption Request Management Standard.

## Failure to comply with this policy

Ethical and behavioural standards that employees are expected to demonstrate while working with the department are set out in the Code of Ethics and Conduct. If employees fail to meet those standards, corrective action may be taken in accordance the Code of Ethics and Conduct.

Individuals who are not government sector employees such as volunteers, contingent or labour hire workers, professional services contractors and consultants may have their services, contract or agreement terminated immediately, or legal action could be taken if they are found to have violated this policy.

## Review timeframe

Digital Information Office will review this policy no later than 3 years from the date the document is approved. The document may be reviewed earlier in response to post-implementation feedback, changes to legislation, or as necessary in accordance with the department's policy and procedures.

## Related documents

A full list of legislative requirements that may impact information security is maintained within the Information Security Management System (ISMS).

This policy should be read in conjunction with the following documents:

- Cyber Security Policy
- Acceptable Use Policy
- ISMS Exemption Request Management Standard
- Code of Ethics and Conduct
- NSW Cyber Security Policy

## Policy metadata

Table 1. Policy metadata

| Category | Description |
|---|---|
| **Status** | Final |
| **Date of approval** | 27.05.2021 |
| **Approver** | Group Deputy Secretary |
| **Group** | Corporate Services |
| **Division** | Digital Information Office |
| **Policy owner** | Chief Digital and Information Officer |
| **Document location** | DPE Intranet |
| **Next review date** | April 2024 |
| **Associated procedure** | N/a |
| **Any additional applicability** | Additional applicability will be considered in the future |
| **Superseded document** | N/A |
| **Further information** | cybersecurity@dpie.nsw.gov.au |
| **Document Reference** | POL21/12 |

## Version control

Table 2. Version Control

| Version | Date issued | Change |
|---|---|---|
| **1** | 27.05.2021 | New policy |
| **1.1** | 3.05.2022 | Updated to reflect new branding and name change |

## Appendices

Appendix 1 – Definitions

Appendix 2 - Roles and responsibilities

Appendix 3 – Active directory password standard

Appendix 4 – Session and screen locking standard

# Appendix 1 – Definitions

Table 3 - Definitions

| Term | Definition |
|---|---|
| Access privileges | Systems permissions associated with an account, including permissions to access or change data, to process transactions, create or change settings, etc. |
| Authentication | Provides a way of identifying a user, typically by having the user enter a valid username and password before access is granted. |
| Multi-factor Authentication (MFA) | An authentication method that requires a user to provide two or more factors to authenticate. Usually requires something you know (password) and something you have (soft token, hard token, one time password), in order to confirm the legitimacy of your identity for an online transaction or to gain access to an application. |
| Password | Any string of characters used to authenticate a user or system. |
| Principle of Least Privilege | Users of ICT resources will be provided with the minimum privileges necessary to fulfill their roles and responsibilities. |
| Principle of Need to Know | Access is only provided to information and resources that are necessary to perform a role. |
| Users | All employees including individuals seconded from other organisations, volunteers, contingent or labour hire workers, professional services contractors and consultants accessing the department’s information and ICT systems. |

# Appendix 2 - Roles and responsibilities

Table 4: Roles and responsibilities

| Role | Responsibility |
|---|---|
| **All user account holders** | • Must create password that meet the length and complexity requirements as per Appendix 3<br>• Never share their passwords and never create a password that is blank even if the system allows it.<br>• Never use the same password for different systems (no password reuse).<br>• Must change their passwords on a regular basis as per the password standard in Appendix 3.<br>• If storing their passwords, must do so securely.<br>• Never leave a logged in session unattended (Win+L to the lock screen when using Windows device).<br>• Never leave documents or devices containing sensitive information physically unattended.<br>• Where a managed print service is unavailable, not leave documents uncollected from a printer.<br>The following are general recommendations for creating a Strong Password:<br>• Passphrases are recommended over a password.<br>• Passwords must not contain part of the account name, username, system name, date of birth, address or anything that is a personal attribute and easily guessed.<br>• Passwords must not contain more than two repetitive characters. |
| **People leaders** | • Securely providing new account information to their employees.<br>• Approving new or changed account privileges for their employees.<br>• Ensuring their employees comply with this policy.<br>• Notifying DIO in a timely manner of any account changes (role changes, termination or otherwise). |
| **Privileged account holder** | • Must conform with all the responsibilities of a user account holder.<br>• Must not use the privileged account for email or to browse/download from the internet.<br>• Must not have identical password for privilege and end user account. |

| Role | Responsibility |
|---|---|
| **System/ service account holder** | • Must conform with all the responsibilities of a user account holder.<br>• Must not use their system/service account for email or to browse/download from the internet.<br>• Must only use their account for its specific purpose.<br>• Must record the account password in the enterprise password management repository and never in the system documentation. |
| **Digital Information Office (DIO)** | • Must implement this policy.<br>• Must ensure systems are available to employees to ensure compliance.<br>• Ensure that accounts for contractors, third-parties or non- permanent employees have an expiry date set. |
| **Chief Digital and Information Officer (CDIO)** | • Approve exemptions to this policy. |
| **Chief Information Security Officer (or equivalent)** | • Must develop, maintain and improve this policy.<br>• Monitor and report on compliance to this policy (effectiveness measurements).<br>• Notify CDIO if account deletion requirements vary from this policy.<br>• Review exemptions to this policy. |

# Appendix 3 – Active directory password standard

Table 5: Active directory password standard

| Attribute | Description | ACSC Single Factor Authorisation recommendations | Minimum Requirement |
|---|---|---|---|
| Enforce password history | The number of passwords that must be remembered in order to avoid frequent re-use of passwords. | 8 | 6 |
| Maximum password age | The period of time (in days) that a password can be used before the system requires the user to change it. | 90 days | 90 days |
| Minimum password age | The period of time (in days) that a password must be used before the user can change it. | 1 day | 1 day |
| Minimum password length | The length of the shortest acceptable password. | 10 if complexity enforced<br>13 if complexity not enforced | 8 characters |
| Password must meet complexity requirements | Technical enforcement of password complexity requirements. | At least three of the following character sets:<br>• Lowercase alphabetic characters (a-z)<br>• Uppercase alphabetic characters (A-Z)<br>• Numeric characters (0-9)<br>• Special characters | Requires characters from 3 of the following categories:<br>• English uppercase characters (A-Z)<br>• Base digits (0-9)<br>• English lowercase characters (a-z)<br>• Special characters (for example, !, $, #) |
| Store passwords using reversible encryption | Storing passwords using reversible encryption is essentially the same as storing plaintext versions of the passwords. | Do not store in clear text | Disabled |
| Account lockout duration | How long a locked-out account will remain locked following failed login attempts? | | 30 minutes |

| Attribute | Description | ACSC Single Factor Authorisation recommendations | Minimum Requirement |
|---|---|---|---|
| Account lockout threshold | The number of failed login attempts prior to an account being automatically locked. | 5 | 5 |
| Reset account lockout counter after | The number of minutes following a failed login attempt before the counter is reset to zero. | Repeated account lockouts are investigated before reauthorizing access | 30 minutes |
| Password storage scheme | The storage scheme for passwords. | Hashed with a strong hashing algorithm and is uniquely salted. SHA-2 algorithm approved. | Salted SHA |
| LAN Manager | Local Area Network (LAN) Manager authentication uses a weak hashing algorithm which is subject to rainbow tables or brute force attacks. | Disabled on workstations and servers | |

# Appendix 4 – Session and Screen Locking Standard

Table 6: Session and Screen Locking Standard

| Attribute | Description | ACSC Multi-factor authentication recommendations |
|---|---|---|
| Inactivity lockout threshold | Minutes of inactivity the system waits before initiating a session or screen lock | 15 |
| Inactivity lockout action | What happens when screen lock initiate | Completely conceal the screen |
| Screen power save mode | Screen enters power save mode | Not entered into prior to inactivity or session lock implemented |
| Screen unlock | User required to re-authenticate to unlock | Re-authentication required |
| User control over session/ screen locking mechanisms | Ability of user to change the session/ screen locking mechanisms and settings | Denied |