# Digital & Technology Password Policy

## Purpose and Scope

To ensure all Murdoch University (MU) systems users follow the appropriate password security measures to prevent unauthorised access to MU systems and information.

Policy Scope:

1. Protect passwords from unauthorised or unintended disclosure.
2. Minimise the likelihood that passwords are guessed or cracked by threat actors.
3. Promote user awareness of good password composition and management practices.
4. Define additional security measures to protect special and privilege passwords.

This policy applies to all Staff, Students, past Students, tenants, contractors, visitors, and the public.

## Policy

1. User responsibility
    1.1. Authorised users are responsible for ensuring that their passwords are created and managed in accordance with this policy.
    1.2. Passwords issued to individuals must not be disclosed to anyone under any circumstances. This includes Digital and Technology (D&T) office staff, other colleagues, friends, other students or supervisors.
    1.3. When a new or changed password is issued to an individual, the individual must, if the system permits it, change the password immediately.
    1.4. Murdoch users are required to register at least one verification option i.e. a non-Murdoch email address or mobile phone number to facilitate password reset using a onetime code.
    1.5. Murdoch users who receive any emails requesting information on usernames and passwords must treat them as 'phishing' and use the "Report Message" function to notify of the receipt of a phishing email, then delete the email.
2. General (applies to all passwords)

    Passwords must be constructed in accordance with the *Password Standard* to minimise the likelihood of guessing or cracking.

2.1. Passwords used for Murdoch University systems must not be identical to passwords used for other systems external to the University.

2.2. Passwords should be actively defended to guard against unauthorised use:

2.2.1. Must be memorised or stored using appropriate technology such as a software tool utilising encryption technology;

2.2.2. Must not be recorded physically, unless stored in a secure manner such as a safe;

2.2.3. Must be provided to authorised individuals using a secure, encrypted method; and

2.2.4. Must be changed immediately when it is known or, if it is suspected, the confidentiality of the password is breached. The University may reset the password or disable the user account to prevent access to systems while the password breach incident is investigated and security is restored.

2.3. Authentications must have Mutli-Factor Authentication (MFA) enabled as directed by the *Password Standard*. If MFA is not possible, due to technical or procedural restrictions, an exception must be approved and registered by the IT Security team or delegate.

2.4. Default passwords on devices, applications, databases, and other systems must be changed immediately after installation.

3. Administrator and system passwords

3.1. Administrator and system passwords may only be stored in an approved password management system in accordance with the *Password Standard*.

3.2. The IT Security team must be notified where the confidentiality of an administrator or system password is breached.

3.3. Administrator and system passwords:

3.3.1. Must be unique for each account; and

3.3.2. Must be changed periodically in accordance with the Password Standard.

4. Shared Passwords

4.1. All individuals who know or have access to a shared password must be granted access using the password manager.

4.2. Shared passwords must be stored in a secure password management system.

4.3. Shared passwords must not be the same as passwords for individuals.

4.4. A shared password must be changed when an individual who knows or has access to the shared passwords is no longer authorised to know the password e.g. when an individual resigns or changes job role.

4.5. Generic accounts must have a password composition and MFA enabled as directed by the *Password Standard.*

5. Password Management

5.1. The user interface of any authentication system requiring a username and password must not give specific user feedback that a password entered is incorrect.

5.2. Passwords and shared passwords must not be embedded within program scripts or code. The password should be stored encrypted in a separate file located in a separate directory. When the password has been used to authenticate, programs should clear memory contents.

5.3. All efforts should be made to remove passwords stored unencrypted, even if the password is no longer current.

5.4. System logs must not contain passwords. This includes incorrect passwords.

5.5. Applications and systems must be configured to not save passwords unless the application or system has been approved by the IT Security team as secure for this purpose.

5.6. Where the number of attempts to enter a correct password exceeds the standard set for the application or system, the event must be logged, an alert sent immediately to the system administrator and IT Security team, and a lockout period applied.

5.7. Repeated failed attempts to enter a correct password must be investigated by the system administrator and reported to the IT Security team.

6. Non-Compliance

Violation of this policy may result in disciplinary action under relevant statutes, policies, or other legal action. This may include removal of access to University information systems, withholding of results, expulsion or in the case of employees, suspension or termination of employment as defined in the *Murdoch University Enterprise Agreement 2023*.

# Governance

| | |
|---|---|
| **Approval Authority** | Senior Leadership Team |
| **Owner** | Chief Experience Officer |
| **Legislation mandating compliance** | |
| **Category** | Primarily a function of management |
| **Related University Legislation and Policy Documents** | *Caller Identity Verification Standard*<br>*ICT Security Policy*<br>*IT Conditions of Use Policy*<br>*Password Standard* |
| **Date effective** | 09/02/2026 |

| | |
|---|---|
| **Review date** | 09/02/2029 |

# Revision History

| Approved/Amended | Date Approved | Resolution No. (if applicable) |
|---|---|---|
| Approved | 09/02/2026 | |
| Administrative Amendment | 06/10/2025 | |
| Administrative Amendment | 01/05/2024 | |
| Approved | 13/09/2023 | |
| Approved | 19/09/2022 | |
| Approved | 12/11/2019 | |
| Approved | 22/11/2016 | |
| Approved | 06/12/2013 | |
| Approved | 19/09/2022 | |

*Please refer to the electronic copy in the Policy and Procedure Manager to ensure you are referring to the latest version.*