Password Policy

Printed copies are for reference only. Please refer to the electronic copy in the Policy and Procedure Manager (PPM), the electronic policy management system (EPMS), to ensure you are referring to the latest version.

Purpose:

Assist in the prevention of unauthorised access to University systems and information.

Audience:

Staff, Students, past Students, tenants, contractors, visitors, public

Objectives:

- To protect passwords from unauthorised or unintended disclosure.
- To minimise the likelihood that passwords are guessed or cracked.
- To promote end-user awareness of good password composition and management practices.
- To define additional security measures to protect special and privilege passwords.

Definitions:

Any defined terms below are specific to this document. The definition of common terms appears in the Murdoch University Dictionary of Terms.

There are no terms.

Policy Statement:

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 Information Technology Services 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, spear-phishing scams’ by forward the email as an attachment to spam report i.e. spam.report@murdoch.edu.au and delete the email.

2. General (applies to all passwords)

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

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

2.3 Passwords should be actively defended to guard against unauthorised use and:

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

2.3.2 Should not be recorded physically unless stored in a secure manner such as a safe;

2.3.3 Must be provided to authorised individuals following the *Password Procedure*; and

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

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 IT Security 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;

3.3.2 Must be changed periodically; and

3.3.3 Must not be the same as a password for an individual.

4. Shared passwords

4.1 All individuals who know or have access to a shared password must be registered.

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.

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 IT Security 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, 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 IT Security.

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 Enterprise Agreement.

Performance Indicators:

There are no performance indicators.

Related Documents:

Caller Identity Verification Standard

ICT Security Policy

IT Conditions of Use Policy

Password Standard

References:

There are no references.

Approval and Implementation:

Approval Authority:	Director, Information Technology Services
Responsible Officer(s):	Director, Information Technology Services
Approval Authority for supporting procedures:	There are no supporting procedures.
Approval Authority for supporting guidelines:	There are no supporting guidelines.
Approval Authority for supporting standards:	Director, Information Technology Services
Contact Officer:	Director, Information Technology Services

Revision History:

Approved/ Amended/ Rescinded	Date Approved	Effective Date	Next Review Date	Resolution No. (if applicable)
Approved	12/11/2019		12/11/2022	
Approved	22/11/2016		22/11/2019	
Approved	06/12/2013		06/12/2016	