Digital and Technology Password Standard

Purpose and Scope

This standard applies to all Staff, Students, tenants, contractors, visitors

Overarching Policy

Password Policy

Standard

1. User Account Types

User accounts are classified into one of five types:

1.1. Standard User: Normal user account with privileges appropriate to the user's position, with the exception of system/application administrators whose accounts are considered Privileged.

1.2. Privileged User: Accounts that exist for the purposes of system/application administration, e.g. 'root' or database administration accounts.

1.3. Active Directory System/Service Accounts: Accounts with special privileges created to allow system services to operate. Not used by a person, e.g. Used by a script or application.

1.4. Azure Active Directory Administrator Accounts: An Account that has the privilege of a Global Administrator that is used to Manage Microsoft Azure Environment.

1.5. Generic Accounts: An account that is not associated with any particular user and are frequently shared between a user group. The accounts are sometimes, but not always, used for interactive access to a system. Interactive access should be backed with Multi Factor Authentication. These accounts should only be used when absolutely necessary and new account must be reviewed and approved by the IT Security Team.

1.6. Past User Accounts: All past users Students, Staff and Others of Murdoch University.

1.7. Application Accounts: Privileged or high value accounts used to manage or maintain high value applications or data

All exceptions to the password standard must be reviewed, approved and registered by the IT Security Team.

2. Password Construction

System	Password length	Password formation	Password duration	Lockout
Standard User: For Staff, Students, Others [1] & Past Users[2]	Min=8	**Requires three out of the four of the following:** • At least one upper case alphabetic character (A-Z). • At least one lower case alphabetic character (a-z). • At least one numeric character (0-9). • At least one symbol. With the exception of Past user's passwords must NOT match any previous passwords. **Characters allowed** • A – Z • a - z • 0 – 9 • @ # $ % ^ & * - _ ! + = [ ] { } | \ : ' , . ? /`~ " ( ) ; • blank space **MFA must be enabled unless an exemption is authorised by the IT Security Team or delegate.**	Staff/Others: Unlimited Students: Unlimited Past Users: Unlimited	**Active Directory:** 10 consecutive invalid passwords within 30 minutes results in a 30-minute lockout. **Azure Active Directory:** More than 8 consecutive invalid passwords result in a 35-minute lockout.

[1] Standard User Account – Ref: Section 1.1
[2] Past User – Ref: Section 1.5

System	Password length	Password formation	Password duration	Lockout
Privileged User: Azure Administrator Passwords[3]	Min=8	**Requires Three out of the four of the following:** • At least one upper case alphabetic character (A-Z). • At least one lower case alphabetic character (a-z). • At least one numeric character (0-9). • At least one symbol. You cannot use your previous password. **Characters allowed** • A – Z • a - z • 0 – 9 • @ # $ % ^ & * - _ ! + = [ ] { } | \ : ‘ , . ? / `~ " ( ) ; • blank space **MFA must be enabled unless an exemption is authorised by the IT Security Team.**	Unlimited with MFA.	**Azure Active Directory:** More than 8 consecutive invalid password attempts in a 35-minute window.

[3] Privileged User – Ref: Section 1.2

System	Password length	Password formation	Password duration	Lockout
Privileged User: Administrator Accounts in Active Directory[4]	Min=12	**Requires Three out of the four of the following:** • At least one upper case alphabetic character (A-Z). • At least one lower case alphabetic character (a-z). • At least one numeric character (0-9). • At least one symbol. The password must NOT match any previous passwords **Characters allowed** • A – Z • a - z • 0 – 9 • @ # $ % ^ & * - _ ! + = [ ] { } | \ : ‘ , . ? /`~ " ( ) ; • blank space • **MFA must be enabled unless an exemption is authorised by IT Security Team.**	365 days, or earlier if it is a shared password and someone who knows the password leaves the organisation or changes job role.	**Active Directory**: 5 consecutive invalid password attempts within 15 minutes results in a 30-minute lockout.

[4] Privileged User – Ref: Section 1.2

System	Password length	Password formation	Password duration	Lockout
System/Service Accounts	Min=35	**Requires Three out of the four of the following:** • At least one upper case alphabetic character (A-Z). • At least one lower case alphabetic character (a-z). • At least one numeric character (0-9). • At least one symbol. The password must NOT match any previous passwords **Characters allowed** • A – Z • a - z • 0 – 9 • @ # $ % ^ & * - _ ! + = [ ] { } | \ : ‘ , . ? /`~ " ( ) ; • blank space	365 days, or earlier if it is a shared password and someone who knows the password leaves the organisation or changes job role. If an expiring password presents significant risk to service disruption a non expiring password is permitted by exception on approval from the IT Security Team.	**Active Directory**: 5 consecutive invalid passwords within 15 minutes results in a 30-minute lockout.

System	Password length	Password formation	Password duration	Lockout
Privileged User: Administrator Passwords	Min=12	**Requires Three out of the four of the following:** • At least one upper case alphabetic character (A-Z). • At least one lower case alphabetic character (a-z). • At least one numeric character (0-9). • At least one symbol. **The password must NOT match:** • a password used for a Murdoch Username. • a password used for an administrator user account of another application. • a system password. • a password you use for personal use. • any previous passwords.	365 days, or earlier if it is a shared password and someone who knows the password leaves the organisation or changes job role.	Active Directory: 5 consecutive invalid passwords within 15 minutes results in a 30-minute lockout.

System	Password length	Password formation	Password duration	Lockout
Generic Accounts	With MFA: Min=12 No MFA: Min=20	**Requires Three out of the four of the following:** • At least one upper case alphabetic character (A-Z). • At least one lower case alphabetic character (a-z). • At least one numeric character (0-9). • At least one symbol. The password must NOT match: • a password used for a Murdoch Username. • a password used for an administrator user account of another application. • a system password. • a password you use for personal use. • any previous passwords. **MFA must be enabled unless an exemption is authorised by IT Security or delegate**	365 days, or earlier if it is a shared password and someone who knows the password leaves the organisation or changes job role.	Active Directory: 5 consecutive invalid passwords within 15 minutes results in a 30-minute lockout.

System	Password length	Password formation	Password duration	Lockout
Application Account: Finance1 Admin/Service Accounts	Min=8	At least one character from at least three of the following groupings: • upper case alphabetic character (A-Z) • lower case alphabetic character (a-z) • numeric character (0-9) • punctuation and special characters Password history enforced: cannot reuse the past 10 passwords.	90 days	After 3 failed attempts the user account is locked out permanently. The user account must be reset by a Finance1 system administrator.
Application Account: Callista	Min=12	At least one character from at least three of the following groupings: • upper case alphabetic character (A-Z) • lower case alphabetic character (a-z) • numeric character (0-9) Password history enforced: cannot reuse the past 10 passwords.	180 days, or earlier if user leaves the organisation or changes job role.	After 5 failed attempts the user account is locked out permanently. The user account must be reset by a System administrator

Service Account: Callista	Min=30	At least one character from at least three of the following groupings: • upper case alphabetic character (A-Z) • lower case alphabetic character (a-z) • numeric character (0-9) Password history enforced: cannot reuse the past 2000 passwords.	Never Automated task scheduled to alert Admin to reset Password after 11 Months	Never
Work Day	Min=8	At least one character from at least three of the following groupings: • upper case alphabetic character (A-Z) • lower case alphabetic character (a-z) • numeric character (0-9) • punctuation and special characters Password history enforced: cannot reuse the past 10 passwords.	180 days	After 3 failed attempts the user account is locked out for 30 Minutes

3. Approved Password Management Systems

Password management system	Version	Passwords types that may be stored:
Password Manager Pro	Latest Updated Version Available -1	Any
KeyPass Password Safe	Latest Updated Version Available on Company Portal	Personal Passwords not to be shared

Governance

Approval Authority	Senior Leadership Team
Owner	Vice Chancellor
Legislation mandating compliance	
Category	Primarily a function of management
Related University Legislation and Policy Documents	
Date effective	09/02/2026
Review date	09/02/2029

Revision History

Approved/Amended	Date Approved	Resolution No. (if applicable)
Approved	09/02/2026	
Approved	13/09/2023	
Approved	19/09/2022	
Approved	12/11/2019	
Approved	23/11/2016	

Approved	27/01/2016
Approved	16/03/2015

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