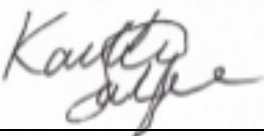
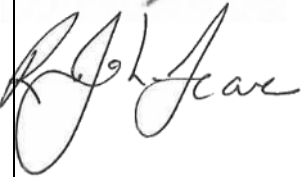




Murrumbidgee
COUNCIL

Cyber Security - Access Control Policy

	Name	Position	Signature	Date
Responsible Officer	Kaitlin Salzke	Chief Financial Officer		14 September 2023
Authorised By	John Scarce	General Manager		14 September 2023

Document Revision History	
Date adopted by Council:	12 September 2023
Minute Number:	146/09/23
Next Review:	See item 10 of this Policy
Revision Number:	
Review Date:	
Date adopted by Council:	
Minute Number:	
Next Review:	
Revision Number:	
Review Date:	
Date adopted by Council:	
Minute Number:	

September 2023

Contents

1. Purpose	3
2. Related Policies	3
3. Scope	3
4. Access Control	3
5. Access to Networks and Network Services	4
6. User Access Management	4
7. System and Application Access Control	6
8. Mobile Devices	7
9. Remote Connections	7
10. Review	7

1. Purpose

Murrumbidgee Council information assets need to be protected appropriately throughout their lifecycle to ensure the confidentiality, integrity and availability of ICT systems and information. Appropriately controlling and restricting access to information and systems ensures individuals are provided the right access at the right time for their role.

2. Related Policies

This Policy should be read in conjunction with the following policies:

- *Communication Devices, Internet and Intranet Policy*, which documents Council's requirements and expectations regarding the use of its communications devices (including password requirements, use of multi-factor authentication, etc.);
- *Cyber Security Policy*, which documents Council's approach to managing and improving its resilience to cyber threats;
- *IT Security Policy*, which documents the high-level requirements that Council expects from its ICT systems, to ensure information is being protected appropriately.

3. Scope

The requirements and expectations outlined by this policy apply to:

- All Murrumbidgee Councillors, permanent full time, part time, trainee and temporary staff, graduates, contractors, consultants and vendors engaged by Murrumbidgee Council;
- Anybody authorised to access and make use of any Murrumbidgee Council computing systems, networks, and/or information;
- Any other body authorised to administer, develop, manage and support Murrumbidgee Council information systems and assets.

4. Access Control

Access to information assets must be driven by information management requirements. These requirements must be translated into controls which deliver appropriate and enforceable access management.

Access to information and resources must be granted in a controlled manner. Appropriate approval must be sourced prior to the delivery of access. Where possible, the principle of least privilege should be applied to ensure the right person has the right access to only the information they need.

Applicable legislation or regulatory restrictions (such as privacy and records management) must be considered when creating or issuing access to Council information or systems. Any system covered under legislation must abide by the legislative restrictions within the access process.

5. Access to Networks and Network Services

Provision and de-provision of access to networks must be in line with this policy. Access to a network does not infer or assume access to a system or service; specific and unique authorisations must be obtained for each.

6. User Access Management

User Registration and De-Registration

Accounts must be registered in such a way that they uniquely identify the owner/user.

User registration and de-registration procedures must be implemented and documented when granting or revoking access rights.

These procedures must be documented and include:

- Recorded authorisation from appropriate management to perform the registration or de-registration;
- Verification that the registration or de-registration action performed is correct.

These documents must be kept for appropriate amounts of time, commensurate with legislative requirements. If no specific timeframes are articulated by legislation, this history must be kept for a reasonable amount of time to support an investigation, if required.

Where an account is required to be created for a specific business need, and is not associated to an individual, a system account or a generic account can be created to perform the required functions.

System Accounts

System accounts (also known as service accounts) are accounts which are primarily used by an application, and are only used by humans in the event of an emergency situation. Where possible, system accounts must be made non-interactive to prevent human interaction. System accounts should be registered and tracked by the information asset owner or delegate of the identity store that the account resides on.

Generic Accounts

Generic accounts (also known as shared network accounts) are accounts that are not associated to an individual, and are created to satisfy a specific business need. Multiple users can log in to a single generic account to authenticate to Council's network, application or other resources.

Generic accounts must not be allocated an email address or given access to sensitive information such as employee or client details. Where possible, generic accounts should follow the principle of least privileges required to do the job they are intended for.

Generic or shared network accounts must have a defined owner who is responsible for managing access to the account, password resets etc. Requests for generic or shared accounts must undergo a formal review process, with approval obtained from the Manager, Corporate and Community Services.

User Access Provisioning

Access to Murrumbidgee Council information resources must be authorised by either the Finance Manager (for financial systems) or the Manager, Corporate and Community Services (for other systems), or the member of the executive team to which they report, prior to being provisioned. It is their responsibility to ensure that access privileges are aligned with the needs of the business, meet the information management requirements, and are assigned on a need-to-know basis.

Procedures for access provisioning must be documented and must ensure that access requests and approvals are documented. Furthermore, segregation of duties should be applied to ensure the requester is not provisioning their own access.

Management of Privileged Access Rights

Where technically feasible, administrative permissions should be applied to a secondary user account in order to prevent a user operating with heightened access privileges when they are not required. Privileged user accounts must not be used for general purposes such as browsing the Internet.

Where technically feasible, administrative permissions should be applied on a temporary basis unless a business need exists justifying their persistence.

All requests for privileged access rights must be approved by the Manager, Corporate and Community Services and documented following an approved procedure. The provision of elevated access must only be actioned after approval is obtained and cannot be actioned by the requester.

Generic administrative accounts must not be used unless a technical preclusion exists.

Management of Secret Authentication Information of Users

Should a Software as a Service (SaaS) model be utilised within Council which requires the use of email addresses as usernames, only unique individual email addresses should be used, not shared mailboxes.

Passwords must meet the requirements set out in Council's *Communication Devices, Internet and Intranet Policy*.

Review of User Access Rights

The Finance Manager (for financial systems) and Manager, Corporate and Community Services (for other systems) are responsible for ensuring that staff access entitlements are appropriate for the staff member's role and position.

They are also responsible for ensuring that User Access Reviews are conducted on a quarterly basis to ensure the right people are provided the right access at the right time.

Removal or Adjustment of Access Rights

Removal of a user's access rights must follow an approved process, and should secure appropriate approvals.

Adjustment of a user's access rights must be approved by either the Finance Manager (for financial systems) or the Manager, Corporate and Community Services (for other systems), or a member of the executive team to which they report.

Adjustments and removals of access rights must be documented, and verification that the rights were removed or adjusted as appropriate should occur.

7. System and Application Access Control

Before being given the opportunity to log onto a computer facility, intended users must be presented with a login screen.

Identification of network, location, system criticality, service supported or host should not appear prior to a successful login.

Systems must be configured not to give any information on an unsuccessful login. This includes identifying which portion of a login sequence (User ID or password) was incorrect. User account management controls must be established to lock user accounts after a defined number of failed authentication attempts.

Systems which manage passwords must implement techniques which ensure the quality of passwords, but also ensure the stored passwords are suitably protected.

Password management systems should:

- Ensure passwords are changed at scheduled intervals;
- Keep a password history;
- Provide uniqueness of user accounts to ensure accountability;
- Ensure temporary passwords are unique to an individual and selected at random;
- Store passwords in a non-reconstitutable form (i.e. one-way hash). This means the password is encrypted and, if the password file is compromised, the password will not display as clear text;
- Ensure password entry is secure.

8. Mobile Devices

Additional security measures must be implemented to protect data held on or accessed via mobile devices. All corporate data must be encrypted and, where technically feasible, corporate data and applications should be segregated to avoid inappropriate use or disclosure.

Mobile devices must be password protected by minimum 4-digit passcodes. Simple passcodes that are common and easily guessed are not to be used.

9. Remote Connections

All remote connections to the Council network must implement appropriate controls, including encryption, to mitigate the risks posed by being external to the protected facilities and computing equipment of the organisation by utilising two factor authentication. Cloud based systems that hold highly sensitive information and provide direct access should leverage two factor authentication.

10. Review

This Policy:

- To be reviewed within the first year of the new Council term;
- May be reviewed and amended at any time at Council's discretion (or if legislative or State Government policy changes occur).