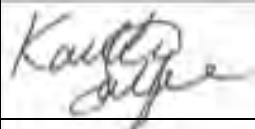





Murrumbidgee
COUNCIL

Cyber Security - IT Security 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 13 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. Equipment Maintenance | 3 |
| 4. Secure Disposal or Re-Use of Equipment | 3 |
| 5. Clear Desk and Clear Screen Policy | 3 |
| 6. Change Management | 4 |
| 7. Separation of Development, Testing and Operational Environments | 4 |
| 8. Controls Against Malware | 4 |
| 9. Information Backup | 5 |
| 10. Event Logging | 5 |
| 11. Installation of Software | 5 |
| 12. Management of Technical Vulnerabilities | 5 |
| 13. Review | 6 |

1. Purpose

This policy is designed to articulate the high level Murrumbidgee Council expects from its IT systems, to ensure information is being protected appropriately.

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;
- Access Control Policy, which documents the mechanisms for appropriately controlling and restricting access to information and systems to ensure individuals are provided the right access at the right time for their role.

3. Equipment Maintenance

All equipment must be correctly maintained to provide availability and protect the integrity and confidentiality of information. Equipment should be monitored and inspected in accordance with manufacturer's specifications. Only authorised maintenance personnel are allowed to perform repairs, and all repairs or service work must be recorded. If equipment must be sent offsite for repairs, the confidentiality and integrity of any information must be ensured. Any damage to the equipment should be reported to Council's IT Managed Service Provider. If the equipment is lost or stolen, staff must report to the Council's IT Managed Service Provider as soon as practicable.

4. Secure Disposal or Re-Use of Equipment

Information shall be removed from any information systems equipment which has been used for Council business before disposal, donation, or re-use. This sanitisation process must take place before releasing such equipment for disposal.

5. Clear Desk and Clear Screen Policy

All users must keep a clear desk and screen. This requires all information, whether it be on paper or screen, to be properly locked away or disposed of when a workstation is not in use or is unattended. The clear desk and clear screen policy will reduce the risk of unauthorised access, loss of, and damage to information during and outside of normal business hours or when workstations are left unattended.

Screensavers/session locks on all PCs/laptops and servers must be implemented. The lock must require the user to re-authenticate before system access is granted.

All printers and fax machines should be cleared of papers as soon as they are printed, to ensure that sensitive documents are not left in printer trays for the wrong person to pick up.

Sensitive physical documents should be shredded.

6. Change Management

All changes to Murrumbidgee Council information assets must be performed in a controlled and managed fashion. All changes must:

- Be formally documented;
- Be peer reviewed;
- Be tested prior to implementation; and
- Be reviewed and approved by an appropriately authorised audience.

Where changes to the information resources do not come under the province of change management (eg. new-user registrations), suitable audit trails and authorisation procedures should be established.

7. Separation of Development, Testing and Operational Environments

Separate and controlled environments should exist for development, test and production where business requirements support their necessity.

Appropriate access controls should be applied to the development and testing environments to ensure the confidentiality and integrity of development activities and data.

8. Controls Against Malware

To prevent the introduction of malicious software, approved malware protection software must be installed, where technologically possible, on Murrumbidgee Council resources, including services, user workstations, standalone workstations, mobile computing devices and laptops.

Malicious software controls must be regularly updated to ensure malicious software can be appropriately identified.

Instances of detected malicious code software outbreaks fall within the definition of a cyber security incident, and should be handled in accordance with Council's *Communication Devices, Internet and Intranet Policy*. The user should also physically disconnect their computer from the network as soon as possible to prevent spreading the infection.

9. Information Backup

Users of information should ensure that appropriate backup and recovery procedures exist for all information assets that have backup requirements. The types of backups and their minimum frequencies should be determined in consultation with the Manager, Corporate and Community Services and Council's IT Managed Service Provider.

10. Event Logging

Systems which facilitate access to, store, transfer or create Council information must, where technically feasible, have logging capabilities enabled which identify at a minimum:

- Who performed an action;
- What action was performed;
- When the event occurred.

All event logs should be kept for periods in line with legislative requirements. If no legal requirements are identified, the event logs should be kept for time periods that support an investigation.

Where supported, actions performed by users of authority (administrators or operators) should be logged.

Mechanisms should be in place to evidence when administrative tasks are performed which are outside of the bounds of normal application or system processes (i.e., clearing or flushing logs).

11. Installation of Software

The updating or installation of software and program libraries on servers must only be performed by authorised personnel and be in accordance with section 6 (Change Management). The updating or installation of software and program libraries on desktops and laptops must be restricted and controlled.

Only approved pieces of software should be installed on systems by an authorised individual. Controls should be implemented to control the installation of software by unauthorised individuals.

Staff seeking to have software approved for installation should approach the Manager, Corporate and Community Services in the first instance, with a review also to be undertaken by Council's IT Managed Service Provider.

12. Management of Technical Vulnerabilities

Council's IT Managed Service Provider, with the oversight of the Manager, Corporate and Community Services, is responsible for maintaining a risk register documenting known risks, and prioritising and mitigating those risks.

13. 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).