Murweh Shire Council

Information Security Policy

Policy No:	IT-001	**Date adopted:**	20 October 2023
Council Resolution Ref:	260/23	**Review Date:**	01 October 2026
Responsible Officer:	Director Community & Health Services	**Version No:**	3

1. Purpose

The business of Murweh Shire Council covers a range of industries and services, with varying technical and operational requirements in terms of information security controls. This policy enunciates the requirements when establishing, implementing and maintaining information security within Council.

This policy provides a starting point for information security management. Staff must assess specific risks and take reasonable steps to protect information from misuse and loss and from unauthorised access, modification or disclosure.

The requirements of this policy are based on the three elements of information security:

- **Confidentiality** Ensuring that information is accessible only to those authorised to have access;
- **Integrity** Safeguarding the accuracy and completeness of information and processing methods; and
- **Availability** Ensuring that authorised users have access to information and associated assets when required.

2. Policy Statement

Murweh Shire Council has responsibility for a significant amount of staff, vendor, and resident information. This policy requires that Council staff:

- are aware of information security and their expected security behaviour
- comply with software licences and with other legal, regulatory and contractual obligations
- report breaches of the information security policy and suspected information security weaknesses
- are prohibited from tampering with evidence in the case of information security incidents that may require forensic investigation.

3. Issue and Review

This policy was issued by the Chief Executive Officer in June 2020. Review of this policy will occur on an annual basis.

Current Version: V3.00 (Reviewed October 2023)

4. Implementation

The authority for the implementation of the mandatory principles of the information standards is primarily derived from the Financial Management Standard 1997.

Existing mandatory requirements of the previous version (V2.00) remain unchanged and have been amalgamated into V3.00.

Due to the increasing need for vigilance in the security of information, 6 additional procedures have been identified for development:

- Implementation of information classification guide;
- Implementation of Authentication procedure;

- Implementation of clear desk/clear screen policy;
- Development of Mobile and Teleworking security processes and risk assessments;
- Consideration of security requirements in all systems design and analysis; and
- Development of Disaster Recovery Plan.

5. Role and Responsibilities

CEO – Authorises the policy

Director of Community & Health Services – Owner of policy. Accountable for maintaining policy and communicating changes to Council.

Managers – Responsible for ensuring staff are aware of the policy.

Staff – Responsible for understanding the policy

6. Terminology

Access Management - The process responsible for allowing users to make use of IT services, data, or other assets. Access Management helps to protect the confidentiality, integrity and availability of assets by ensuring that only authorized users are able to access or modify the assets. Access Management is sometimes referred to as Rights Management or Identity Management.

Information Security Management – The process that ensures the confidentiality, integrity and availability of an organisation's assets, information, data and IT Services. Information Security Management usually forms part of an organisational approach to Security Management which has a wider scope than the IT Service provider, and includes handling of paper, building access, phone calls etc., for the entire organisation.

Information Technology - The use of technology for the storage, communication or processing of information. The technology typically includes computers, telecommunications, applications and other software. The information may include business data, voice, images, video, etc. information technology is often used to support business processes through IT Services.

Management of Risk – all the Activities required to identify and control the exposure to risk which may have an impact on the achievement of an organisation’s business objectives.

7. Audience

All Council employees that have been authorised to access Council information communication technology.