1. INTRODUCTION

This document sets out the policy of the City of Mount Gambier ("Council") follow for a consistent approach to establishing, implementing, and maintaining strong security postures for managing and safeguarding the community's information and information assets against security threats.

Scope

This policy applies to the City of Mount Gambier Council.

Purpose

The City of Mount Gambier provides a wide range of services to their community through the use of information and communications technology ('ICT') and operational technology ('OT'). In order to uphold the community's trust and confidence, it is imperative that councils safeguard their community's information and information assets against security threats. This policy leverages risk management process and control measures to reduce the likelihood or impact of security risks to Council.

The objectives of this policy are to

- Ensure security risks are managed in a standardised and acceptable manner across Council.
- Maintain the reputation of Council and the broader Local Government.
- Demonstrate alignment to industry recognised best practices in security risk management.
- Protect the confidentiality, integrity, and availability of information assets in alignment with necessary legal and regulatory requirements; and
- Provide assurance to the community and other interested parties that information provided to councils are sufficiently protected

2. DEFINITIONS

Key Term - Acronym	Definition
iServices Working Group	Internal working group of Council Officers including: General Manager Corporate and Regulatory Services General Manager City Infrastructure Manager Organisational Development Team Leader iServices iServices Systems Administrator IT Contractor

3. STATEMENT OF COMMITMENT

This document reflects the security policy and governance obligations of Council. This policy provides a commitment to a set of minimum-security requirements for Council as directed by the iServices Working Group to manage security risks to the Council's operations and its information assets. Council will develop principles, procedures, and processes to support compliance and operation of the Council's Cyber Security Program in accordance with the Local Government Security Framework (LGSF).
Compliance with the Local Government Security Framework and the Council's suite of security policies, practices and procedures is mandatory. This policy applies to all aspects of security risk within Council.

4. CYBER SECURITY PROGRAM OBJECTIVES

The City of Mount Gambier commits to the ongoing and emerging risks with managing security information by the ongoing development, implementation and review of a Cyber Security program that meets the below objectives;

- Implement effective security controls to ensure adequate protection of all information that has been entrusted to Council
- Demonstrate implementation of cyber security risk management practices
- Promote a structured and consistent approach to security risk management that spans the many business units of Council;
- Maintain the confidentiality, integrity, and availability of information assets in compliance with policy, legal and regulatory requirements;
- Create a culture of high security awareness amongst all staff;
- Monitor systems and investigate detected or suspected security breaches and weaknesses;
- Ensure the confidence of the community and interested parties of the security of their information whether in storage, processing, or transmission;
- Provide assurance to the community and other interested parties of the security of their information entrusted to Council;
- Monitor and measure Council's performance against security objectives to ensure commitment to the continual improvement of information security practices;
- Assign resources and responsibilities to provide a structured approach for identifying and managing information security risks;
- Ensure the integrity of critical information; and
- Align to the security requirements of key partners to ensure the ongoing viability of critical service delivery.

The Cyber Security program shall be monitored and reviewed through the Executive Leadership Team on a yearly basis and the Audit and Risk Committee at least annually.

5. REVIEW & EVALUATION

This Policy is scheduled for review by Council in January 2029 however, will be reviewed as required by any legislative changes which may occur.

8. AVAILABILITY OF POLICY

This Policy will be available for inspection at Council's principal office during ordinary business hours and on the Council's website www.mountgambier.sa.gov.au. Copies will also be provided to interested members of the community upon request, and upon payment of a fee in accordance with Council's Schedule of Fees and Charges.

File Reference:	AF23/81764
Applicable Legislation:	Local Government Act 1999 State Records Act 1997
Reference: Strategic Plan – Beyond 2015	Goal 5 Our Commitment
Related Policies:	F225 Fraud, Corruption, Misconduct and Maladministration Prevention Policy Internal Audit Policy Internal Controls Policy P155 Privacy Risk Management Policy
Related Procedures:	Information and Security Management - Administrative Principle
Related Documents:	Local Government Security Framework

DOCUMENT DETAILS

Responsibility:	General Manager Corporate and Regulatory Services
Version:	1.0
Last revised date:	23 January 2024
Effective date:	23 January 2024
Minute reference:	Council Meeting 23 January 2024 – Item 19.7 – Resolution 2024/16
Next review date:	January 2028
<u>Document History</u> First Adopted By Council: Reviewed/Amended:	 23 January 2024