Glamorgan Spring Bay Council

Cybersecurity Policy

Version [1.0]

Adopted:23 September 2025
Minute No.: 201/25

Document Control

Cybersecurity Policy	
First issued/approved	23 September 2025
Source of approval/authority	Council
Last reviewed	-
Next review date	September 2029
Version number	1
Responsible Officer	Information Management & Technology Officer
Department responsible for policy development	Corporate and Financial Services
Related policies	• Information Management Policy • Communication Devices & Social Media Policy • Personal & Private Information Policy • Tasmanian Government Information Security policy framework • Tasmanian Government Cyber Security Strategy • Tasmanian Government Cyber Security Policy • Cyber security Act 2024
Publication of policy	Website

Contents

1 Introduction

1.1 Purpose

The purpose of this policy is to establish guidelines, standards, and procedures to ensure the protection, confidentiality, integrity, and availability of IT based information and IT based information systems used by the Council. This policy aims to minimise the risk of unauthorised access, disclosure, alteration, destruction, or disruption of information assets and to promote responsible and secure use of technology resources.

1.2 Scope

This policy applies to all employees, councillors, contractors, and third parties who have access to Council IT information assets, systems, networks, and services. It covers all devices, including desktops, laptops, mobile devices, servers, and network infrastructure owned or managed by the Council, and privately owned devices used to access Council information assets associated with any council activity. Compliance with this policy is mandatory for all users.

1.3 Definitions

IT	Information Technology
Information assets:	Any information or data, regardless of format, owned, created, received, or transmitted by the Council.
Information systems:	The combination of hardware, software, networks, and procedures used for the processing, storage, transmission, and dissemination of information.
Confidentiality:	The protection of information from unauthorised disclosure to ensure that only authorised individuals have access to it.
Integrity:	The protection of information from unauthorised modification, deletion, or corruption to ensure its accuracy, completeness, and reliability.
Availability:	The assurance that information and information systems are accessible and usable by authorised users when needed.
Council	Glamorgan Spring Bay Council

1.4 Related Policies and Legislation

This policy relates to and depends on other Council policies, as well as legislation, including:

- Communication Devices & Social Media Policy
- Personal & Private Information Policy
- Tasmanian Government Information Security policy framework
- Tasmanian Government Cyber Security Strategy
- Tasmanian Government Cyber Security Policy
- Cyber security Act 2024

1.5 Policy Review and Update Cycle

This policy is to be reviewed every 4 years or as necessary to respond to emerging risks.

2 Policy

2.1 Information Security Governance:

- Council will establish an information security governance framework that defines roles, responsibilities, and decision-making processes related to cybersecurity.
- The Executive Leadership Team will be responsible for overseeing and enforcing this policy and associated procedures.
- Routine audits and assessments will be conducted to ensure compliance with the governance framework.

2.2 Risk Management:

- Council will conduct regular risk assessments to identify and evaluate cybersecurity risks.
- Appropriate safeguards and controls will be implemented to mitigate identified risks based on their severity and potential impact.
- Risk treatment plans will be developed and implemented to address identified vulnerabilities and threats.

2.3 Access Control:

- Access to information assets and systems will be granted by Council' Directors. *Directors only* make the decisions on what access is given to each employee. Notification is sent to the Information and Technology Officer who will provide the access, ensuring employees only have access to the resources necessary for their job roles.
- Access rights will be reviewed and updated whenever employees' roles change to reflect changes in job roles and responsibilities.
- Strong authentication mechanisms, such as passwords, multi-factor authentication, and access controls, will be implemented to prevent unauthorised access.

2.4 Awareness and Training:

- Council will provide scheduled cybersecurity awareness and training programs to educate employees about potential threats, best practices, and their responsibilities in protecting information.
- Training sessions will cover topics such as phishing, social engineering, password hygiene, physical security, and data handling practices.
- Employees will be encouraged to report any suspicious activities or potential security incidents promptly.

2.5 Incident Response:

- Council's IT Support Provider in junction with Council will establish an incident response plan that outlines the steps to be taken in the event of a cybersecurity incident.
- Incident response procedures will include incident detection, containment, eradication, recovery, and lessons learned.
- All incidents, including actual or suspected breaches, unauthorised access attempts, malware infections, or data breaches, will be promptly reported, investigated, and documented.

2.6 Data Protection:

- Council's IT Support Provider will implement measures to protect personal and sensitive information from unauthorised access, loss, or disclosure.
- Data encryption, data classification, access controls, and scheduled backups will be utilised to safeguard information.
- Privacy impact assessments will be conducted for new initiatives or projects involving personal or sensitive information.

2.7 System and Network Security:

- Council's IT Support Provider will implement technical controls to safeguard information systems and networks from unauthorised access and attacks.
- Firewalls, intrusion detection and prevention systems, antivirus software, and routine patching and updates will be utilised to protect against known vulnerabilities and threats.
- Secure configuration practices will be followed for all systems and network infrastructure.

2.8 Vendor and Third-Party Management:

- Council's IT Support Provider will establish a vendor and third-party management process to ensure that third-party vendors and contractors adhere to cybersecurity standards and requirements.
- Contracts and agreements with third parties will include clauses related to cybersecurity obligations, data protection, and incident reporting.
- Scheduled assessments and audits will be conducted to ensure compliance with cybersecurity standards.

2.9 Compliance:

- Council will comply with all relevant cybersecurity legislation, regulations, and standards applicable to its operations.
- Scheduled reviews and updates will be conducted to ensure ongoing compliance with changing legal and regulatory requirements.
- Compliance monitoring and reporting mechanisms will be established to track and report on adherence to cybersecurity obligations.

2.10 Continual Improvement:

- Council will review and update the cybersecurity policy, along with associated procedures and controls, to address emerging threats, technologies, and best practices.
- Lessons learned from incidents and audits will be used to improve the effectiveness of cybersecurity measures.
- Council will stay informed about industry trends and collaborate with other organisations to exchange best practices and enhance cybersecurity resilience.

3 Implementation

Implementation of this Policy rests with the Chief Executive Officer.