CS.104 Information & Cyber Security Policy

1 OBJECTIVE

The objectives of this policy are to:

- Protect the confidentiality, integrity and availability of Council's information assets;
- Ensure compliance with relevant legislation regulation and industry best practices;
- Promote a culture of security awareness and responsible information handling; and
- Establish clear roles and responsibilities for the management of cybersecurity and information Security.

2 SCOPE

This policy is applicable to the whole of Council, its employees, Councillors, contractors, consultants, and any other party including cloud based and external system, given access to council owned information technology assets or confidential information.

This policy applies to all information and physical assets that are owned or leased by Council or in Council's custody and control, and to Council's confidential information.

3 STATEMENT

3.1 INFORMATION CLASSIFICATION

All information assets within Council shall be classified based on their sensitivity, criticality, and regulatory requirements. The classification levels shall include at least the following categories:

a. Public: Information intended for public disclosure with no restrictions on access.
b. Internal: Information intended for internal use only, not to be shared with external parties without proper authorisation.
c. Confidential: Highly sensitive information that requires strict access controls and protection measures.
d. Restricted: Information with legal or contractual obligations, requiring additional access restrictions.

3.2 ACCESS CONTROL

a. User Access to information systems and resources shall be granted based on the principle of least privilege, ensuring that users are provided with the minimum access required to perform their job functions.
b. Strong user authentication mechanisms such as unique usernames, strong passwords, and multi-factor authentication shall be enforced for all users.
c. User accounts shall be managed and regularly reviewed, and dormant or unused accounts shall be promptly disabled or removed.
d. Remote Access maybe granted to users by an approved extended user authentication methods like VPN.

3.3 Information Security Responsibilities

a. The Information Security Officer will be responsible for the overall management and coordination of information security activities within Council. This includes developing and maintaining information security policies, procedures, and standards, as well as conducting regular risk assessments and security audits.
b. All employees have a responsibility to adhere to the policies, procedures, and guidelines outlined in this document. They must promptly report any suspected security incidents or breaches to the appropriate authorities.
c. Management is responsible for supporting and promoting information security initiatives, allocating necessary resources, and ensuring compliance with this policy across the organisation.
d. The IT officer will be responsible for the implementation and maintenance of technical security controls, monitoring system logs, performing regular vulnerability assessments, and responding to security incidents.

3.4 Security Awareness and Training

Council shall provide regular cybersecurity awareness training to all employees. This training will cover topics such as identifying phishing attacks, secure password practices, social engineering, and safe internet browsing habits. Training programs shall be updated to address emerging threats and technologies.

3.5 Incident Response

a. All security incidents, including suspected breaches, malware infections, or unauthorised access attempts, must be reported immediately to the IT department and the Information Security Officer.
b. Council shall maintain an up-to-date incident response plan that outlines the procedures to be followed in the event of a security incident. The plan will include incident assessment, containment, eradication, recovery, and post-incident analysis.

3.6 Annual External Network Penetration Testing

Council will annually engage an external network penetration test to identify vulnerabilities and weaknesses of the organisation's external network infrastructure. It involves simulating real-world cyber-attacks to assess the security posture from an external perspective and provides the following.

a. Vulnerability Identification: Identifies network weaknesses and vulnerabilities.
b. Risk Mitigation: Enables proactive measures to reduce the likelihood of attacks.
c. Enhanced Security Posture: Improves overall network security.
d. Compliance: Helps meet regulatory and compliance requirements.

3.7 Compliance and Audit

Council shall regularly assess its compliance with this policy and relevant regulations through internal audits and independent assessments. Non-compliance with this policy may result in disciplinary action, including termination of employment or contractual obligations.

4 HUMAN RIGHTS COMPATIBILITY STATEMENT

This Policy has been assessed as compatible with the Human Rights protected under the Human Rights Act 2019

5 DEFINITIONS

Information Assets:	All electronic and physical data, records, documents, and information resources owned or managed by Council.
Phishing:	A malicious activity where attackers impersonate legitimate entities to trick individuals into revealing sensitive information through deceptive emails, messages, or websites.
Social Engineering:	The manipulation of individuals to deceive them into disclosing confidential information or performing actions that compromise security.
Multi-Factor Authentication:	A security mechanism that requires users to provide multiple forms of identification, such as passwords, physical tokens, or biometrics, to access an account or system.
Information Systems:	Computer systems, networks, servers, databases, and associated infrastructure used by Council to store and process data.
Confidentiality:	The principle of protecting information from unauthorised disclosure, ensuring that access is limited to authorised individuals or entities.
Integrity:	The assurance that information remains accurate, complete, and unaltered throughout its lifecycle and is protected against unauthorised modifications.
Availability:	The state of ensuring timely and reliable access to information and information systems by authorised individuals or entities when needed.
Access Control:	The process of managing and restricting user access to information systems and resources based on the principle of least privilege.
User Authentication:	The process of verifying the identity of users attempting to access information systems, typically through unique usernames, strong passwords, or multi-factor authentication methods.
User Account Management:	The practice of creating, managing, reviewing, and disabling user accounts to ensure that only authorised individuals have access to information systems and resources.
Security Awareness Training:	Training programs designed to educate employees and stakeholders about cybersecurity threats, best practices, and the importance of responsible information handling.

Incident Response:	The organised approach to address and manage security incidents, including steps for assessment, containment, eradication, recovery, and post-incident analysis.
Compliance:	The state of adhering to applicable laws, regulations, and industry standards related to cybersecurity and information security.
Risk Assessment:	The process of identifying, evaluating, and prioritising potential risks to information assets and systems, enabling effective risk management strategies to be implemented.
Vulnerability Assessment:	The process of systematically identifying and analysing vulnerabilities within information systems, networks, or applications to proactively address security weaknesses.

6 RELATED POLICIES | LEGISLATION | OTHER DOCUMENTS

Title	Document ID
Essential Eight Cyber Security Standards	https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-maturity-model
ISO 27001 Standard	https://www.cssia.org/wp-content/uploads/2020/01/ISO_27001_Standard.pdf
Privacy Act 1988	https://www.legislation.gov.au/Series/C2004A03712
QSC Incident Response Plan	

7 VERSION CONTROL

V1	18-Jul-23	Developed and adopted