COUNCIL INFORMATION SECURITY POLICY

ECM DSID:	4422673
First Issued / Approved:	14 February 2023
Last Reviewed:	Date of last review
	C140223/7338
Next Review:	14 February 2026
Responsible Officer:	**Manager, Innovation and Technology**
Date Placed on Webpage/ Intranet:	20 February 2023

1. PREAMBLE

1.1 Background

Data, information and the systems that hold and operate it are essential assets and consequently, need to be suitably protected. Information security is achieved by implementing controls (based on risk profile) such as policies, processes, procedures, organisational structures and software and hardware functions. These controls need to be established, implemented, monitored, reviewed and improved continuously to ensure that security objectives are met.

1.2 Purpose

This policy articulates the security requirements that Council must meet in order to meet its obligations and to manage the confidentiality, integrity, availability and privacy of both Council and external client-owned data and information.

This policy has the following objectives:

- **Access Control Objective:** To limit access to information and information processing facilities in support of business requirements.
- **Digital Messaging Objective:** To establish and maintain the protocol for using digital messaging in all its forms, including the security aspects of information transfer within Council and with any external entities.
- **Communications and Operation Management Objective:** To ensure the protection of information and the secure operations of networks and supporting processing facilities.
- **Physical and Environmental Security Objective:** To prevent unauthorised physical access, damage and interference to Council's information and information processing facilities.
- **Supplier Relationships Objective:** To ensure the protection of Council's information assets that are accessible by service providers if/as required.
- **Information Security Incident Management Objective:** To ensure a consistent and effective approach to the management of information security incidents, including security events and vulnerabilities.
- **Information Security aspects of Business Continuity Management Objective:** ensure information security continuity is embedded in business continuity plans and management processes.
- **Compliance Management Objective:** To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security.

1.3 Scope

This policy applies to all information that is generated, received, stored, printed, filmed, or keyed and to the IT applications and systems that create, use, manage and store information and data, including:

- information in any form, including print, electronic, audio, video, and backup and archived data
- computer systems, peripheral devices, software applications, databases, middleware and operating systems
- physical premises occupied by the personnel and equipment
- operational environments including power supply and related equipment
- processes and procedures
- transmission pathways for communications.

This policy applies to Elected Members, staff (including work experience placements and trainees), volunteers, and consultants and contractors across Council, including Alwyndor.

1.4 Definitions

Users – refers to any person using or accessing Council's data, systems, tools or infrastructure.

1.5 Strategic Reference

The innovation focus area includes aspirations of creating conditions for early adoption and experimentation with beneficial technologies, and using digital tools to create transparency and enable direct participation.

2. PRINCIPLES

2.1 Council is committed to providing a secure environment that protects the integrity and confidentiality of information without compromising access and availability.

2.2 To ensure the information environment and information resources are safeguarded against security threats, Council will:

- define roles and responsibilities to establish clear lines of accountability
- enable the protection of information assets against internal and external threats
- enable the identification and treatment of security risks to Council's information environment through appropriate physical, technical and administrative channels
- enable the development of best practices for effective information security.

2.3 Users are required to:

- take responsibility for developing information security awareness, education and training to safeguard Council's assets
- only access information needed to perform their authorised duties

- understand/determine the classification of the information they are using and producing
- protect the confidentiality, integrity and availability of Council's information in accordance with the relevant information classification level
- safeguard any physical key, ID card or computer/network account that enables access to Council or external Client information
- maintain appropriate password creation and protection measures as set out in the Council's password requirements
- report any activities likely to compromise sensitive information to the relevant Manager, General Manager or Chief Executive Officer
- maintain confidentiality even after separation from Council and not in any way divulge, copy, release, sell, loan, alter or destroy any information, except as specifically authorised by a General Manager or Chief Executive Officer.

2.4 In addition to complying with general user requirements, managers and supervisors must:

- ensure that team processes support the objectives of confidentiality, integrity and availability and that those procedures are followed
- ensure that any relevant restrictions are effectively communicated to those who use, administer, capture, store, process or transfer information in any form.

2.5 The Information and Technology Team is responsible for:

- ensuring adequate security for computing and network environments that capture, store, process and/or transmit information
- ensuring that the requirements for confidentiality, integrity and availability are being appropriately managed within their respective environments
- understanding the classification level of the information that will be captured by, stored within, processed by, and/or transmitted through Council technologies and providing an appropriately enabling and supportive environment
- developing, implementing, operating and maintaining a secure information environment that includes:
    - a cohesive architecture
    - system implementation and configuration standards
    - procedures and guidelines for administering network and system accounts and access privileges in a manner that satisfies the security requirements
    - an effective strategy for protecting information against generic threats posed by computer hackers that adheres to industry-accepted information management best practices for the system or service.

2.6 Security requirements are identified by a methodical assessment of security risks. Expenditure on controls needs to be balanced against the operational damage likely to result from security failures. The results of the risk assessment help to guide and determine the appropriate management action and priorities for managing information security risks, and for implementing controls to protect against these risks.

2.7 No corporate information is to be stored and retained in non-authorised online file sharing solutions (for example, DropBox, iCloud, Google Drive and MS SkyDrive).

2.8 Mobile devices are not to be used as the sole repository for Council information. All Council information stored on mobile devices is to be backed up to an appropriate network location and ECM as appropriate.

3. REFERENCES

3.1 Legislation

Local Government Act 1999
State Records Act 1997

3.2 Other References

Acceptable Use Policy
Mobile Device Policy
Risk Management Policy
Elected Member Code of Conduct
Employee Code of Conduct
AS ISO/IEC 27001:2015
AS ISO/IEC 27002:2015
Fair Treatment Procedures
Managing Misconduct & Disciplinary Procedures
Workplace Relations Policy
Quality Working Culture Policy