CYBERSECURITY POLICY

July 2022

PREPARED BY:

INFORMATION MANAGEMENT AND TECHNOLOGY UNIT

4-20 Eton Street,
Sutherland NSW 2232
T 02 9710 0333
sutherlandshire.nsw.gov.au

1. PURPOSE

Council owns and is the custodian of a large portfolio of information assets including information on physical assets such as roads, land, equipment plus information relating to its operations, staff, and customers.

The purpose of this Policy is to articulate Council's commitment to the security of its information assets in particular, the confidentiality, integrity and availability of digital information.

2. APPLICATION

This Policy applies to all members of the public, Councillors, Council employees and contractors of Sutherland Shire Council who provide or use council services.

3. PRINCIPLES

3.1 Application of Principles

No one principle should be applied to the detriment of another. Principles must be collectively considered and applied to the extent that is reasonable and practicable in the circumstances.

3.2 Information Security and Cybersecurity

Council will implement a systemic approach to continually improving the security of its information assets via an Information Security Management System (ISMS) aligned with ISO 27001.

Information Security includes the core components of confidentiality, integrity, and availability.

Cybersecurity is the subset of Information Security that focuses on information assets in digital form.

3.3 Agreement of Objectives

The ISMS Steering Committee will review and agree the objectives for the ISMS on an annual basis. The objectives will support Council’s strategic objectives, and consider the elements of people, process, technology, and partners.

The Enterprise Risk Committee is a sub-committee of Council’s Executive and will act as the ISMS Steering Committee.

3.4 Risk based approach

Council will identify its most critical and valuable information assets and prioritise the maturity of security controls accordingly. The security controls will include, but not be limited to, the Essential 8 as defined by the Australian Cyber Security Centre.

3.5 Continual improvement

The ISMS Steering Committee will review progress against the agreed objectives on a quarterly basis. An Essential 8 maturity assessment will be performed and reported at least annually.

4. RESPONSIBILITIES

4.1 Responsible Officer

The Chief Information Officer is the Responsible Officer for this policy and is responsible for keeping the Policy current.

4.2 Chief Executive Officer

Council has delegated the Chief Executive Officer the authority to exercise the responsibilities detailed in this Policy including the definition of the Council risk appetite and providing support and resourcing for cyber security risk management activities.

4.3 Director Corporate Services

Sponsor of the Enterprise Risk Committee / ISMS Steering Committee.

4.4 Directors

Directors are responsible for ensuring their directorate adheres to the requirements of this Policy including ensuring the completion of cyber security awareness training for their staff and providing guidance in respect of key information assets within their directorate and the organisation.

4.5 Employees

Are responsible for:

- Completing mandatory Cybersecurity Awareness training.
- Reporting any issues – real or suspected related to cyber security to the Information Management & Technology (IM&T) Service Desk; and
- Adhering to the requirements of this Policy and operating within its authorities.

5. POLICY COMPLIANCE

Ongoing, scheduled monitoring of the efficacy of the implementation of the policy will be undertaken by the Enterprise Risk Management Committee on behalf of the Executive.

6. RECORD KEEPING, CONFIDENTIALITY AND PRIVACY

Council adheres to and complies with the NSW State Records Act 1998 and Privacy and Personal Information Protection Act 1998 through its Access to Information Policy and Privacy Management Plan.

7. BREACHES OF POLICY

Breaches of this Policy will be dealt with in accordance with normal disciplinary procedures and may be advised to the Chief Executive Officer and / or Director via the Chief Information Officer where appropriate.

8. RELATED DOCUMENTS

- Code of Conduct for Council Staff
- Code of Conduct for Councillors
- Code of Conduct for Council Committee Members, Delegates of Council and Council Advisers

9. RELEVANT LEGISLATION AND REGULATIONS

- Local Government Act 1993 (NSW)
- State Records Act 1998 (NSW)
- Privacy and Personal Information Protection Act 1998 (NSW)
- Government Information (Public Access) Act 2009 (NSW)
- Health Records and Information Privacy Act 2002 (NSW)
- ISO 27001 Information Security Management System

10. DEFINITION OF TERMS

Term	**Meaning**
Information Security	The preservation of confidentiality, integrity, and availability of information.
Confidentiality	Information is not available or disclosed to unauthorised people, entities or processes.

Term	Meaning
Integrity	Information is complete and accurate, and protected from corruption.
Availability	Information is accessible and usable by authorised users.
Essential 8	A set of baseline mitigation strategies recommended by the Australian Cyber Security Centre to make it much harder for systems to be compromised by adversaries. The mitigation strategies that constitute the Essential Eight are: application control, patch applications, configure Microsoft Office macro settings, user application hardening, restrict administrative privileges, patch operating systems, multi-factor authentication and regular backups
ISO 27001	A standard framework that helps organisations establish, implement, operate, monitor, review, maintain and continually improve an ISMS
ISMS – Information Security Management System	An ISMS is a framework for systematically identifying, assessing, and systematically identifying, assessing, and managing information security risks information security risks using a continual improvement approach across the element of people, process, technology and partners.

.

End of Document

UNCONTROLLED COPY WHEN PRINTED - For up to date copy please refer to Sutherland Shire Council Intranet / Website			
Document Name: Cybersecurity Policy		**Policy Accountability**: Chief Information Officer	
Version: 1.0	**Approved by**: Council	**Minute No**: 152	**Date approved:** 25 July 2022
Original: July 2022	**Last Revision**: N/A		**Next Revision**: August 2026