

Cybersecurity Policy

September 2026

Prepared by: Information Management and Technology Unit

1. Purpose

This policy sets out Council's commitment to protecting the confidentiality, integrity, and availability of its information assets through a risk based approach to support the secure and reliable delivery of services to the community.

2. Application

This Policy applies to 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. Confidentiality

Council is committed to safeguarding the confidentiality of data by ensuring controls are in place to grant access only for appropriately authorised use.

3.3. Integrity

Council is committed to ensuring information is accurate, complete, reliable and protected from unauthorised change.

3.4. Availability

Council is committed to ensuring information and systems are accessible and usable when required for authorised purposes only.

3.5. Privacy

Council is committed to implementing safeguards (including this policy and the Privacy Management Plan) that prevent unauthorised access, misuse, loss, or disclosure of personal information and by ensuring compliance with applicable privacy legislation.

3.6. Authoritative Guidance and Direction

Council aligns its cybersecurity framework with relevant guidance issued by government authorities, including Cyber Security NSW and the Australian Cyber Security Centre, to the extent that it is applicable and appropriate to Council's risk profile and operating environment.

This includes adopting and maintaining controls consistent with the Cybersecurity Guidelines - Local Government and considering authoritative government guidance when responding to significant cybersecurity incidents, including those involving ransomware demands, to support informed, risk-based decision-making.

3.7. Risk-Based Approach

Council identifies its most critical and valuable information assets and prioritises the maturity of security controls accordingly.

4. Cybersecurity Assurance and Operational Resilience

This section outlines the activities Council undertakes in each cybersecurity capability area.

4.1. Protect

Council protects critical and valuable information assets using security controls aligned with the Cyber Security Guidelines - Local Government. These guidelines encompass the key Essential Eight controls (and any future revisions) defined by the Australian Cyber Security Centre.

Protection controls include, but are not limited to:

- Access to Council systems and information is limited, as far as practicable, to only what is needed.
- Higher level access to Council systems is regularly reviewed to ensure it is appropriate and removed when no longer needed.
- An extra step is required when system users sign in, via a secure app, to better protect Council systems and information from unauthorised access.
- Software and systems are regularly updated to address security issues and reduce the risk of cyber-attacks.
- Council systems and devices are configured using secure settings to reduce exposure to common cybersecurity risks.
- Email security controls are in place to help stop fake or fraudulent emails impersonating Council.
- Additional safeguards are applied to sensitive and personal information to help prevent unauthorised access, misuse, or loss.
- Secure backups of information are maintained and protected from alteration or deletion, enabling services and data to be restored if there is a cybersecurity incident.
- All Council staff and Councillors receive cybersecurity training when they start and annually thereafter to support safe working practices and protection of information.

- Simulated email scam exercises are conducted regularly to help staff and Councillors recognise suspicious messages and reduce the risk of real phishing attacks.
- Cybersecurity is considered when engaging suppliers who access Council systems or information, with appropriate security requirements embedded in contracts, where possible, and ongoing monitoring in place to help protect community data.

4.2. Detect

Council maintains processes to identify cybersecurity threats, vulnerabilities and incidents to support timely response and remediation.

Detection controls include, but are not limited to:

- Council systems are monitored on a continuous basis to help identify unusual activity that may indicate a cybersecurity issue.
- Notifications and alerts from system vendors, Cyber Security NSW and the Australian Cyber Security Centre are actively monitored to support early awareness of emerging threats and vulnerabilities.
- Regular internal vulnerability scanning is undertaken to help identify and address known security weaknesses.
- Independent cybersecurity testing is conducted periodically by external specialists, who safely test Council systems to identify potential weaknesses in a similar way to real cyber-attacks. Any findings are assessed and addressed as appropriate.

4.3. Respond

Council maintains a Security Incident Response Plan to support a coordinated, effective and timely response to cybersecurity incidents, helping protect critical information and maintain business continuity.

The Security Incident Response Plan is regularly reviewed and supported by a designated incident response team with defined roles, responsibilities and escalation pathways to respond to real or suspected cybersecurity incidents.

To strengthen response capability during major incidents, Council participates in a reciprocal arrangement with other councils to access additional cybersecurity resources when incidents exceed internal capacity.

4.4. Recover

Council undertakes regular disaster recovery testing and maintains secure backups to support business continuity and recovery following cybersecurity incidents.

Recovery activities focus on restoring systems and services safely and learning from each exercise or incident to continually strengthen resilience and recovery capabilities.

4.5. Govern

Council applies a structured approach to managing and continually improving the security of its information assets through an Information Security Management System (ISMS) aligned with the ISO 27001 standard.

Cybersecurity roles and responsibilities are clearly defined, supported by established decision making and reporting frameworks to ensure effective oversight and accountability.

An ISMS Steering Committee sets cybersecurity objectives annually on behalf of the Executive, ensuring alignment with Council strategy, risk tolerance and control effectiveness.

ISMS objectives are risk based and address people, processes, technology and partners.

The ISMS Steering Committee meets quarterly to review progress against objectives and provide guidance to the Security Working Group.

4.6. Report

Council provides timely and accurate reporting on cybersecurity objectives, risks, incidents and control effectiveness to support informed decision making, transparency and continual improvement.

Regular reporting is provided to the Audit, Risk and Improvement Committee (ARIC).

Council undertakes annual cybersecurity maturity assessments and voluntarily reports results to Cyber Security NSW against the requirements of the Cybersecurity Guidelines - Local Government.

4.7. Partnerships

Council actively partners with Cyber Security NSW and the Australian Signals Directorate to strengthen its cybersecurity posture through shared intelligence, trusted guidance, expertise and access to state and national resources.

5. Responsibilities

5.1. Responsible Officer

The Chief Information Officer (CIO) is the Responsible Officer for this policy and is responsible for ensuring it remains current.

Example: The Manager Corporate Governance is responsible for this Policy and for keeping the Policy current.

5.2. Chief Information Officer

The CIO is also the Chief Information Security Officer (CISO) and responsible for defining and implementing council's cybersecurity strategy.

5.3. Chief Executive Officer

Council has delegated to 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 cybersecurity risk management activities.

5.4. Director Corporate

Sponsor of the Enterprise Risk Committee / ISMS Steering Committee.

5.5. Directors

Directors are responsible for ensuring their directorate adheres to the requirements of this Policy, acceptance of any residual cyber security risks related to their data or services, ensuring the completion of cybersecurity awareness training, and providing guidance in respect of key information assets within their directorate and the organisation.

5.6. Employees

Employees are responsible for:

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

6. 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.

7. 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.

8. 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.

9. Related documents

- Code of Conduct for Council Staff
- Code of Conduct for Councillors
- Privacy Management Plan
- Data Breach Notification Policy

10. Relevant legislation and regulations

- *Local Government Act 1993 (NSW)*
- *Local Government (General) Regulation 2021*
- *State Records Act 1998 (NSW)*
- *Privacy and Personal Information Protection Act 1998 (NSW)*
- *Health Records and Information Privacy Act 2002 (NSW)*
- *Government Information (Public Access) Act 2009 (NSW)*
- Cyber Security Guidelines - Local Government (NSW)
- ISO 27001 Information Security Management System

11. Definition of terms

Term	Meaning
Critical Information Assets	Information and systems that are essential to Council operations, service delivery, or legal and regulatory obligations.
Cybersecurity incident	An unwanted or unexpected event that has or is likely to compromise the confidentiality, integrity or availability of information, systems, or services.
Essential Eight	A set of basic cybersecurity controls recommended by the Australian Cyber Security Centre (ACSC) to help protect systems and reduce the likelihood and impact of cyber-attacks. The Essential Eight mitigation strategies consist of: • Application control • Patch applications • User application hardening • Configure Microsoft Office macro settings

	• Patch operating systems • Multifactor authentication • Restrict administrative privileges • Regular backups
Information Security and Cybersecurity	Information Security is the protection of information to ensure the core components of confidentiality, integrity, and availability.
ISMS – Information Security Management System	Cybersecurity is the subset of Information Security and is the practice of protecting digital information, devices and networks from unauthorised access, disruption, damage or theft.
ISO 27001	An ISMS is a framework for systematically identifying, assessing, and managing information security risks using a continual improvement approach across the elements of people, process, technology, and partners.
Phishing	Is an internationally recognized framework that provides best practice requirements for organisations to establish, implement, operate, monitor, review, maintain and continually improve an Information Security Management System (ISMS).
Ransomware Demand	A cybercrime where cybercriminals trick individuals into providing personal information, often through fraudulent emails or messages that appear to be from legitimate organisations.
Security Incident Response Plan	Is a demand for payment made by cyber attackers after they have encrypted, disrupted, stolen, or threatened to release data or systems, in exchange for restoring access or preventing the disclosure of compromised information.

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: 2	Approved by: Council	Minute No: 310 (12.2)	Date approved: 14 September 2026
Original: July 2022	Last Version: July 2022	Next Revision: August 2030	