CYBER SECURITY POLICY

Document Reference No:	GD23/15931	Version:	One
Service Unit:	Governance		
Author:	Governance Officer		
Responsible Director:	General Manager		
Authorisation Date:	30 August 2023	Review Date:	08/25
Minute No:	OCM 09-08-2023		

Purpose

Central Darling Shire Council (CDSC) aims to establish effective cyber security operational policies and procedures and embed cyber security into risk management processes. This will enforce organisational resilience and help make informed decisions in managing these risks, and will be supported by meaningful training, communication, and support across all levels of Council.

This policy is designed for use by the General Manager, Executive Management Team (ManEx), and the Audit and Risk Improvement Committee (ARIC) to embed cyber security into risk management processes. It outlines the high-level cyber security standards recommended for all NSW Local Government by Cyber Security NSW.

Application

Cyber Security covers all measures used to protect systems – and information processed, stored or communicated on these systems – from compromise of confidentiality, integrity, and availability.

The Cyber Security Policy applies to all Council Officials and contractors of Central Darling Shire Council (CDSC), as they are responsible for:

- Using and preserving CDSC's systems and digital assets in a secure way
- Familiarising themselves with CDSC's policies and standards and being aware of, and complying with, their responsibilities
- Reporting incidents or suspected cyber security breaches to the General Manager or delegate

Definitions

Breach – an incident that results in unauthorised access to, modification or disruption of data, applications, services, networks and/or devices by bypassing their underlying security mechanisms. This includes when data is lost or subjected to misuse or interference.

Council Official – as defined by the Council Code of Conduct and including Councillors, members of staff, administrators, council committee members, delegates of council, volunteers, contractors, and council advisors.

Crown Jewels – the most valuable or operationally vital systems or information in the organisation.

Cyber Security – measures used to protect the confidentiality, integrity and availability of systems and information.

Essential Eight – eight essential mitigation strategies that are recommended by the Australian Cyber Security Centre as a baseline to make it much harder for adversaries to compromise systems.

ICT – Information and Communications Technology, also referred to as Information Technology (IT). This includes software, hardware, network, infrastructure, devices, and systems that enable the digital use and management of information and the interaction between people in a digital environment.

Provisions

CDSC's process for enhancing risk management, governance, developing a cyber security culture, safeguarding records and systems, strengthening resilience against attacks and improved reporting is based on the Cyber Security Guidelines for Local Government and outlined below.

LEAD	PREPARE	PREVENT	DETECT	RESPOND	RECOVER
1	Councils should implement cyber security **planning and governance**. CDSC will:				
1.1	Allocate roles and responsibilities as detailed in this policy.				
1.2	Ensure there is a governance committee led by the General Manager to be accountable for cyber security including risks, plans, reporting and meeting the requirements of this policy.				
1.3	Develop, implement and maintain an approved cyber security plan that is integrated with our business continuity arrangements.				
1.4	Monitor cyber security in our risk register and consider cyber security threats when performing risk assessments.				
1.5	Be accountable for the cyber risks of our ICT service providers with access to or holding of government information and systems and ensure these providers understand and comply with the cyber security requirements of the contract, including the applicable parts of this policy and any other relevant CDSC policies.				

LEAD	PREPARE	PREVENT	DETECT	RESPOND	RECOVER
2	Councils should build and support a **cyber security culture** across their organisation. CDSC will:				
2.1	Implement regular cyber security awareness training for all Council officials and ensure that outsourced ICT service providers understand and implement the cyber security requirements of the contract.				
2.2	Increase awareness of cyber security risk across all staff including the need to report cyber security risks.				
2.3	Foster a culture where cyber security risk management is an important and valued aspect of decision-making and where cyber security risk management processes are understood and applied.				

2.4	Ensure that people who have access to sensitive or classified information or systems and those with privileged system access have appropriate security screening, and that access is removed when they no longer need to have access, or their employment is terminated.
2.5	Share information on security threats and intelligence with Cyber Security NSW and cooperate across NSW Local Government and the NSW Government to enable management of state-wide cyber risk.

LEAD	PREPARE	PREVENT	DETECT	RESPOND	RECOVER	
3	Councils should **manage cyber security risks** to safeguard and secure their information and systems. CDSC will:					
3.1	Implement an Information Security Management System (ISMS), Cyber Security Management System (CSMS) or Cyber Security Framework (CSF), with scope at least covering systems identified as the Council's "crown jewels".					
3.2	Implement the ACSC Essential Eight.					
3.3	Classify information and systems according to their business value (i.e. the impact of loss of confidentiality, integrity or availability).					
3.4	Ensure cyber security requirements are built into procurement and into the early stages of projects. Any upgrades to existing systems must comply with CDSC's cyber risk tolerance.					
3.5	Ensure new ICT systems or enhancements include processes for audit trails and activity logging to assess the accuracy and integrity of data including processes for internal fraud detection.					

LEAD	PREPARE	PREVENT	DETECT	RESPOND	RECOVER
4	Councils should improve their **resilience** including their ability to rapidly detect cyber incidents and respond appropriately. CDSC will:				
4.1	Develop a current cyber incident response plan that integrates our business continuity plan.				
4.2	Test our cyber incident response plan at least every year and involve senior staff responsible for the management of external communications and media.				

4.3	Ensure that ICT systems and assets are monitored to identify cyber security events and verify the effectiveness of protective measures.
4.4	Report cyber security incidents to the General Manager, Statewide Mutual and/or Cyber Security NSW. If relevant, incident reporting will be compliant with Federal reporting requirements.
4.5	Participate in or observe state-wide cyber security exercises as required.

Roles and Responsibilities

The following roles and responsibilities apply to CDSC's cyber security functions:

General Manager

The General Manager is responsible for:

- Assigning appropriate members of the Management/Executive Group (ManEx) and 3rd party ICT providers with the authority to perform the duties outlined in this policy.

- Ensuring 3rd party ICT providers protect government systems outsourced to them or that they have access to.

- Supporting the organisation's cyber security plan.

- Ensuring CDSC develops, implements, and maintains an effective cyber security plan and/or information security plan.

- Determining CDSC's risk appetite.

- Appropriately resourcing and supporting cyber security initiatives including training and awareness and continual improvement initiatives to support this policy.

- Reporting cyber incidents to Cyber Security NSW, if appropriate.

- Collaborating with information technology, records management and risk officers to protect CDSC's information and systems.

- Managing the budget for the cyber security program.

Customer Services Manager

The Customer Services Manager is responsible for:

- Providing day-to-day management and oversight of operational delivery.

- Acting as a focal point within CDSC for all matters relating to information management that are required to support cyber security.

- Providing input and support to regulatory compliance issues.

IT Team Leader and Records Management Officer

The IT Team Leader and Records Management Officer are responsible for:

- Ensuring that a cyber incident that involves damage or loss, or a near-miss, is escalated and reported to the Risk and WHS Officer

Risk and WHS Officer

The Risk and WHS Officer is responsible for:

- Coordination of the updating of cyber security controls and responses in the Operational Risk Register

- Ensuring cyber security incidents are recorded in the incident register.

Human Resources Officer

The Human Resources Officer is responsible for:

- Co-ordinating training and awareness programs to increase employees' cyber security capacity.

Audit and Risk Committee (ARIC)

ARIC are responsible for:

- Assisting the General Manager to ensure the risk framework is applied in assessing cyber security risks and with the setting of the risk appetite.

- Assisting the General Manager in analysing cyber security risks

Legislation

State Records Act 1998

Privacy and Personal Information Protection Act 1998

Government Information (Public Access) 2009, NSW

Related Documents

<u>External</u>

NSW Cyber Security Policy

Cyber Security Guidelines for Local Government (Cyber Security NSW)

<u>Internal</u>

Records Management Policy

Risk Management Framework

Information Security Policy

Information Technology Security Policy

Data Security and Protection Policy

Information Access Control Policy

ICT Acceptable Use Policy

Cloud Security Policy

Codes of Conduct

Monitoring and Review

This policy will be monitored and reviewed by the General Manager to ensure compliance. Once adopted, it remains in force until it is reviewed by Council. It is to be reviewed approximately every two (2) years to ensure that it meets requirements, or sooner if the General Manager determines appropriate.