DRAFT

POLICY

Central Tablelands Water

CYBER SECURITY POLICY

DOCUMENT CONTROL

Document Title		Cyber Security Policy			
Policy Number		Council-PR050			
Responsible Officer		Executive Manager Corporate Services			
Reviewed by		Executive Management Team			
Date Adopted		xx August 2026			
Adopted by		Council			
Review Due Date		August 2027			
Revision Number		1			
Previous Versions	**Date**	**Description of Amendments**	**Author**	**Review/ Sign Off**	**Minute No. (if relevant)**
New	August 2026	New policy to align with the Australian Cyber Security Essential 8 requirements and relevant regulatory requirements	EMCS	Council	

PURPOSE

Central Tablelands Water (Council) is committed to protecting its information, technology systems, operational infrastructure and services from cyber security threats.

The purpose of this Policy is to establish a clear framework for managing cyber security risks across the organisation and to promote a culture where cyber security is understood as a shared responsibility.

This Policy aims to protect Council's information, systems, networks and digital assets; maintain the confidentiality, integrity and availability of information; reduce the risk of cyber incidents, data breaches and service disruption; support the safe, reliable and continuous delivery of water services; protect operational technology, including SCADA, telemetry and related infrastructure; strengthen organisational resilience and business continuity; support compliance with relevant legislation, standards and governance expectations; and promote secure and responsible use of information technology resources.

SCOPE

This policy applies to all employees; contractors and consultants; volunteers; work experience personnel; Board members; third-party service providers with access to Council systems, data or infrastructure; and any person using Council information, technology or communication resources.

This policy concerns information and communication technology systems; cloud services; mobile devices; network infrastructure; email and communication systems; business applications; electronic records; customer, employee and corporate information; operational technology, including SCADA, telemetry, pump stations, reservoirs and treatment-related systems; Internet of Things devices; remote access arrangements; and any information stored, transmitted or processed on behalf of Council.

For a water utility, cyber security extends beyond corporate IT systems. Cyber risks may also affect water supply operations, treatment processes, telemetry, communications networks and critical infrastructure.

DEFINITIONS

Cyber Security	The protection of information, systems, networks, devices and technology from unauthorised access, attack, damage, misuse, interference or disruption.
Cyber Incident	An event that compromises, or has the potential to compromise, the confidentiality, integrity or availability of information, systems, networks or technology.
Operational Technology	Hardware, software and systems used to monitor, control or support physical processes and infrastructure, including SCADA, telemetry and control systems.
SCADA	Supervisory Control and Data Acquisition systems used to monitor and control operational infrastructure such as water treatment, pumping, storage and distribution assets.
Multifactor Authentication	An authentication method requiring two or more forms of verification before access is granted.

Critical Information Asset	An information, technology or operational asset that is essential to Council's operations, service delivery, legal obligations or reputation.
Essential Eight	A set of baseline cyber security mitigation strategies developed by the Australian Cyber Security Centre to help organisations reduce cyber security risk. [cyber.gov.au]

POLICY STATEMENT

Council recognises that cyber security is essential to the delivery of safe, reliable and efficient water services to the community.

Council is committed to implementing appropriate cyber security controls; managing cyber security risks within Council's broader risk management framework; protecting sensitive, confidential, personal, operational and corporate information; maintaining compliance with applicable legislative, regulatory and governance obligations; promoting cyber security awareness and accountability among employees and contractors; responding promptly and effectively to cyber security incidents; supporting continuous improvement in cyber security maturity; protecting critical systems that support water supply, treatment, distribution and business continuity; and ensuring cyber security risks are considered in procurement, project delivery, system upgrades and operational change.

Cyber security is the responsibility of all workers and is not solely an information technology function.

Principles

Cyber security activities at Council will be guided by the following principles.

- Risk-Based Approach: Cyber security risks will be identified, assessed and managed according to the likelihood and consequence of threats to Council's operations, information, systems and essential services.
- Shared Responsibility: All employees, contractors and service providers have a role in protecting Council's information, systems and services.
- Defence in Depth: Council will use multiple layers of technical, procedural and administrative controls to reduce cyber security risks.
- Protection of Critical Services: Priority will be given to protecting systems and assets that support the safe and reliable delivery of water services.
- Continuous Improvement: Cyber security practices will be regularly reviewed and improved in response to emerging threats, incidents, audit findings, technology changes and sector guidance.
- Compliance and Accountability: Council will comply with relevant legislative, regulatory, contractual and governance obligations relating to cyber security, privacy, records management and information protection.

Maturity Position

While Council's size, structure, and resources differ from larger utilities, this Policy adopts a proportionate approach that reflects the key areas of good practice relevant to a regional NSW water utility, including cyber security governance and executive oversight; protection of operational technology and SCADA environments; identification and protection of critical information and technology assets; alignment with the Australian Cyber Security Centre Essential Eight; cyber incident response and recovery planning; mandatory cyber security awareness activities; third-party and procurement-related cyber risk management; vulnerability and patch management; and integration of cyber risk into business continuity and disaster recovery planning.

Cyber Security Framework and Standards

Council will seek to implement cyber security controls that are proportionate to its risk profile, operational environment and available resources.

Where practicable, Council will align its cyber security approach with:

- Australian Cyber Security Centre Essential Eight;
- NSW Cyber Security Policy principles and mandatory requirement areas;
- ISO/IEC 27001 Information Security Management System principles;
- relevant Australian Government and industry cyber security guidance;
- local government governance, risk and audit expectations; and
- water utility operational technology and critical infrastructure good practice.

Council recognises that cyber security maturity is an ongoing process and will continue to strengthen its controls over time.

Cyber Security Requirements

- **Access Control**
  Council will:
  - restrict access to systems based on business need;
  - apply the principle of least privilege;
  - implement password and authentication requirements;
  - use multifactor authentication where available and appropriate;
  - restrict administrative access to authorised personnel;
  - remove or amend access promptly when employment, engagement or role requirements change;
  - regularly review user access permissions; and
  - monitor access to critical systems where practicable.

- **Device Security**
  Council devices must:
  - be protected by approved security software;
  - be configured according to established security standards;
  - receive security updates and patches in a timely manner;
  - be secured when unattended;
  - be protected from unauthorised installation of software; and
  - be returned promptly when no longer required.

- **Email and Internet Use**
  All users must:
  - exercise caution when opening emails, attachments and links;
  - report suspicious emails immediately;
  - comply with Council information technology policies;
  - avoid accessing inappropriate, unauthorised or unsafe websites;
  - not circumvent security controls;
  - take care when handling sensitive, personal or confidential information; and
  - use Council systems for authorised business purposes.

- **Data Protection**
  Council will:
  - classify and manage information according to its sensitivity and business value;

- protect confidential, personal, customer, corporate and operational information;
- securely store and transmit information;
- maintain appropriate backup and recovery arrangements;
- dispose of information securely in accordance with records management requirements;
- manage data breach risks in accordance with relevant privacy obligations; and
- ensure information is retained, accessed and disposed of in line with legislative and organisational requirements.

- **Vulnerability and Patch Management**
  Council's external IT provider will:
  - monitor vulnerabilities affecting organisational systems;
  - apply security patches in a timely and risk-based manner;
  - prioritise remediation of critical vulnerabilities;
  - conduct periodic vulnerability assessments where appropriate;
  - maintain processes to identify and manage unsupported or end-of-life systems; and
  - consider cyber security risks when implementing new systems or changes to existing systems.

NSW cyber security requirements identify vulnerability management, patching applications, patching operating systems, multifactor authentication and restricting administrative privileges as important baseline cyber controls.

Operational Technology and Critical Infrastructure Security

Council recognises that cyber security risks may affect operational technology and the delivery of essential water services.

Operational technology includes systems and assets used to monitor, control or support water supply operations, including SCADA, telemetry, treatment-related systems, pump stations, reservoirs, communications networks and related infrastructure.

Council will:

- maintain appropriate separation between corporate and operational technology networks where practicable;
- restrict and monitor remote access to operational systems;
- apply risk-based cyber security controls to SCADA, telemetry and operational technology environments;
- assess cyber risks associated with treatment plants, pump stations, reservoirs and other critical infrastructure;
- include operational technology in incident response, business continuity and disaster recovery planning;
- consider cyber security requirements when procuring, upgrading or maintaining operational technology systems;
- monitor emerging threats that may affect critical infrastructure and water utility operations; and
- ensure contractors or service providers accessing operational technology systems comply with relevant cyber security requirements.

Critical Information and Technology Assets

Council will identify and maintain an inventory of critical information and technology assets requiring enhanced protection.

Critical assets may include SCADA and telemetry systems; customer information systems; financial systems; payroll and employee information systems; asset management systems; GIS and mapping

systems; corporate network infrastructure; cloud platforms; backup systems; remote access systems; and other systems supporting essential business or water supply functions.

Council will apply additional controls to critical assets based on risk, operational importance and the potential impact of compromise.

Cyber Incident Management

All employees must immediately report:

- suspected cyber-attacks;
- data breaches;
- malware or ransomware infections;
- phishing emails;
- unauthorised access attempts;
- lost or stolen devices;
- accidental disclosure of information;
- unusual system behaviour; and
- any suspected compromise of operational technology or critical infrastructure.

Council will:

- investigate cyber security incidents;
- implement containment, recovery and remediation measures;
- escalate incidents according to severity and operational impact;
- notify relevant authorities where required;
- maintain records of cyber incidents;
- conduct post-incident reviews;
- identify lessons learned and improvement actions; and
- include significant cyber incidents in risk and governance reporting.

Training and Awareness

Council will provide ongoing cyber security education and awareness activities to all employees.

Training may include phishing awareness; password and passphrase security; multifactor authentication; safe use of email and internet resources; data protection responsibilities; incident reporting requirements; remote working and mobile device security; protection of sensitive information; and emerging cyber threats.

All employees are expected to participate in mandatory cyber security training as required, in accordance with the NSW cyber security requirements for cyber security awareness activities and mandatory cyber security awareness training

Third-Party and Procurement Security

Third-party providers accessing Council information, systems or infrastructure may be required to:

- meet cyber security requirements specified by Council;
- implement appropriate security controls;
- protect Council information from unauthorised access, disclosure or loss;
- report cyber incidents affecting Council systems, services or data;
- comply with contractual cyber security, privacy and confidentiality obligations;
- support audit, assurance or review activities where appropriate; and
- ensure subcontractors comply with relevant cyber security obligations.

Cyber security risks must be considered during procurement, contract management, system implementation and supplier review processes. This is particularly important for ICT systems, cloud services, managed service providers, SCADA support providers, telemetry contractors and software vendors.

Governance, Reporting and Assurance

Council will maintain appropriate governance arrangements to oversee cyber security risk.

The Board (Council) will oversee organisational cyber security risk; ensure cyber security forms part of strategic and enterprise risk management; receive reporting on significant cyber security risks, incidents and improvement activities; and support a culture of cyber security accountability.

The Audit, Risk and Improvement Committee will review cyber security risks and controls; receive reports on significant cyber risks, incidents and mitigation actions; monitor cyber security assurance activities, including audits, reviews and improvement plans; and provide oversight of cyber security risks within Council's broader risk management framework.

The General Manager will promote a culture of cyber security; ensure appropriate resources are allocated to cyber security risk management; support implementation of this Policy; and ensure cyber security risks are appropriately escalated.

The Executive Management Team will monitor cyber security risks and performance; support implementation of this policy; ensure cyber risks are incorporated within organisational risk management processes; promote cyber security awareness within their areas of responsibility; and support timely action to address identified cyber security risks.

Managers and Supervisors will support compliance with this policy; ensure staff understand their cyber security responsibilities; promote reporting of cyber security concerns; consider cyber security risks when implementing business changes or new systems; and ensure staff complete required training.

Corporate Services employees will work with external providers to maintain cyber security controls; monitor systems, vulnerabilities and cyber security risks; coordinate incident response activities; implement cyber security improvements; support user awareness initiatives; provide advice on cyber security requirements; and maintain relevant cyber security documentation and records.

Employees and other workers must comply with this Policy and associated procedures; protect passwords and authentication credentials; complete required cyber security training; report cyber security incidents and suspicious activity; use Council systems responsibly; take reasonable care when handling information and using technology; and seek advice if unsure about cyber security requirements.

Compliance

Failure to comply with this Policy may expose Council to cyber security risks; compromise personal, customer, corporate or operational information; disrupt services or critical operations; result in disciplinary action; lead to withdrawal of system access privileges; result in contractual consequences for third-party providers; and result in legal or regulatory consequences where applicable.

Monitoring

Cyber security performance may be monitored through cyber incident reporting; security audits and reviews; vulnerability assessments; user awareness training completion rates; risk assessments; access reviews; business continuity and disaster recovery testing; Essential Eight maturity assessment activities; internal and external audit outcomes; supplier assurance reviews; and reporting to the Executive Management Team; Audit, Risk and Improvement Committee; and Board.

POLICY REVIEW

This Policy will be reviewed every four years, or earlier where legislative, operational, organisational or cyber threat changes require.

REFERENCES

- Local Government Act 1993 (NSW)
- Work Health and Safety Act 2011 (NSW) (where cyber incidents may impact critical operations and worker safety)
- Privacy and Personal Information Protection Act 1998 (NSW)
- State Records Act 1998 (NSW)
- Government Information (Public Access) Act 2009 (NSW)
- Australian Cyber Security Centre (ACSC) Essential Eight
- NSW Cyber Security Policy principles and best practice guidance
- Relevant Council policies including Code of Conduct, Information Technology Acceptable Use Policy, Records Management Policy and Risk Management Policy

VARIATION

Council reserves the right to review, vary or revoke this policy.