POLICY

CENTRAL TABLELANDS WATER

CYBER SECURITY POLICY

DOCUMENT CONTROL

Document Title		Cyber Security Policy			
Policy Number		CTW-PR050			
Responsible Officer		Director Finance and Corporate Services			
Reviewed by		Council			
Date Adopted		19 June 2024			
Adopted by		Council			
Review Due Date		19 June 2028			
Revision Number		1			
Previous Versions	Date	Description of Amendments	Author	Review/ Sign Off	Minute No: (if relevant)

Introduction

Strong cyber security is an important component in enabling the effective use of emerging technologies and ensuring confidence in the services provided by Central Tablelands Water.

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.

Cyber security is becoming more important as cyber risks continue to evolve. Rapid technological change in the past decade has resulted in increased cyber connectivity and more dependency on cyber infrastructure.

Purpose

The NSW Cyber Security Policy outlines the Mandatory Requirements to which all NSW Government agencies must adhere to. Each Mandatory Requirement is supported by detailed requirements. These detailed requirements are a baseline of minimum requirements expected of agencies.

The policy aims to reduce impacts to confidentiality, integrity and availability of services and information, by ensuring cyber security risks to the information and systems of NSW Government departments and agencies are appropriately managed.

Objectives

CTW's **Cyber Security Policy** endeavours to strengthen cyber security governance, identify Council's most valuable or operationally vital systems or information, strengthen cyber security controls, develop a cyber security culture, and have a thorough cyber incident response.

Council has developed an effective cyber security framework and embedded cyber security into risk management practices and assurance processes.

When cyber security risk management is done well, it reinforces organisational resilience, making entities aware of their risks and helps them make informed decisions in managing those risks.

The Framework will be complemented with meaningful training, communications, and support across all levels of Council.

This policy outlines the mandatory requirements to which Council must adhere, to ensure cyber security risks to the information and systems are appropriately managed.

Scope

This Policy applies to all Councillors, employees, contractors, volunteers, Committee members (referred to as Council Officers) in relation to Cyber Security Policy.

This policy operates in addition to all other obligations under the Local Government Act 1993 (the Act), any other legislation, or relevant codes and policies regarding the disclosure of any interests. This Policy also applies to:

- Information, data, and digital assets created and managed by the CTW, including outsourced information, data, and digital assets;
- information and communications technology (ICT) systems managed, owned, or shared by the CTW, and

The Cyber Security Policy

The Guidelines are based on the NSW Cyber Security Policy (the Policy), which has been edited to better suit the Council. The Policy outlines the mandatory requirements to which all NSW Government departments and Public Service agencies must adhere to ensure cyber security risks to their information and systems are appropriately managed.

For the scope of the Mandatory Requirements, agencies should ensure any use of exceptions for a system that are documented and approved by an appropriate authority through a formal process.

Documentation for exceptions should include the following:

- detail, scope, and justification for exceptions
- detail of compensating controls associated with exceptions, including:
  - detail, scope, and justification for compensating controls
  - expected implementation lifetime of compensating controls
  - when compensating controls will next be reviewed
- system risk rating before and after the implementation of compensating controls
- any caveats placed on the use of the system as a result of exceptions
- acceptance by an appropriate authority of the residual risk for the system
- when the necessity of exceptions will next be considered by an appropriate authority (noting exceptions should not be approved beyond one year).

Incident Reporting

All actual or suspected cyber incident are to be reported immediately via the Incident Response Report Form to any one of the members below:

- The General Manager (GM)
- Director Finance & the Corporate Services (DFCS)
- 3rd Party ICT provider (Fourier)

Where a cyber risk is reported the Cyber security/ Data Breach Review team will undertake a preliminary assessment. Where required, such as where the incident meets the requirements of an Eligible Data Breach or involves Sensitive Information, the Data Breach Review Team will be assembled promptly to review and respond to the breach.

Records of any incidents will be reported to the Audit, Risk & Improvement Committee.

Roles and Responsibilities

Council will have the following roles and responsibilities allocated as part of their cyber security function.

The General Manager

- Appointing or assigning an appropriate senior staff member in the council with the authority to perform the duties outlined in this policy.
- Supporting the council's cyber security plan.
- Ensuring the council develops, implements, and maintains an effective cyber security plan and/or information security plan.
- Determining the council's risk appetite.
- Appropriately resourcing and supporting council cyber security initiatives including training and awareness and continual improvement initiatives to support this policy.

Directors and Managers roles and responsibilities

Senior Responsible Officers (or staff with these responsibilities) are responsible for:

- Managing and coordinating the response to cyber security incidents, changing threats and vulnerabilities
- Developing and maintaining cyber security procedures and guidelines
- Providing guidance on cyber security risks introduced from business and operational change
- Managing the life cycle of cyber security platforms including design, deployment, ongoing operation, and decommissioning
- Ensuring appropriate management of the availability, capacity and performance of cyber security hardware and applications
- Providing input and support to regulatory compliance and assurance activities and managing any resultant remedial activity
- Developing a metrics and assurance framework to measure the effectiveness of controls
- Providing day-to-day management and oversight of operational delivery

Council Staff Councillors and General Contractors

Staff, Councillors, and all general contractors are responsible for:

- Using and preserve Councils systems and digital assets in a secure way by adhering to security policies and operational standards.
- Familiarising themselves with Councils policies and standards and being aware of their responsibilities under these.
- Complying with the requirements of these policies and related operational standards.
- Report violations or suspected violations of these policies in a timely manner.

Internal Audit

Agency may engage an Internal Auditor to undertake the following tasks:

- Validating that the cyber security plan meets the agency's business goals and objectives and ensuring the plan supports the agency's cyber security strategy
- reviewing their agency's adherence to this policy and cyber security controls
- Providing assurance regarding the effectiveness of cyber security controls.

3rd Party ICT providers

Councils are responsible under the Guidelines for managing cyber security requirements. This includes contract clauses, monitoring and enforcement for 3rd party ICT providers and the ICT security of non-government organisations holding and/or accessing government systems. Councils should ensure that 3rd party ICT providers have the following in place to protect government systems outsourced to them or that they may have access to:

- Foundational Requirement 1.5: The third-party organisation has a process that is followed to notify the Council quickly of any suspected or actual security incidents and follows reasonable direction from the Council arising from incident investigations (noting this will vary based on risk profile and risk appetite).
- Foundational Requirement 2.1: The third-party organisation ensures that their staff understand and implement the cyber security requirements of the contract.
- Foundational Requirement 3.1: Any 'Crown Jewel' systems must be covered in the scope of an Information Security Management System (ISMS) or Cyber Security Framework
- Foundational Requirement 3.4: Cyber security requirements are built into the early stages of projects and the system development life cycle (SDLC), including agile projects.
- Foundational Requirement 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.

This does not prevent other contractual obligations being imposed.

The Essential Eight

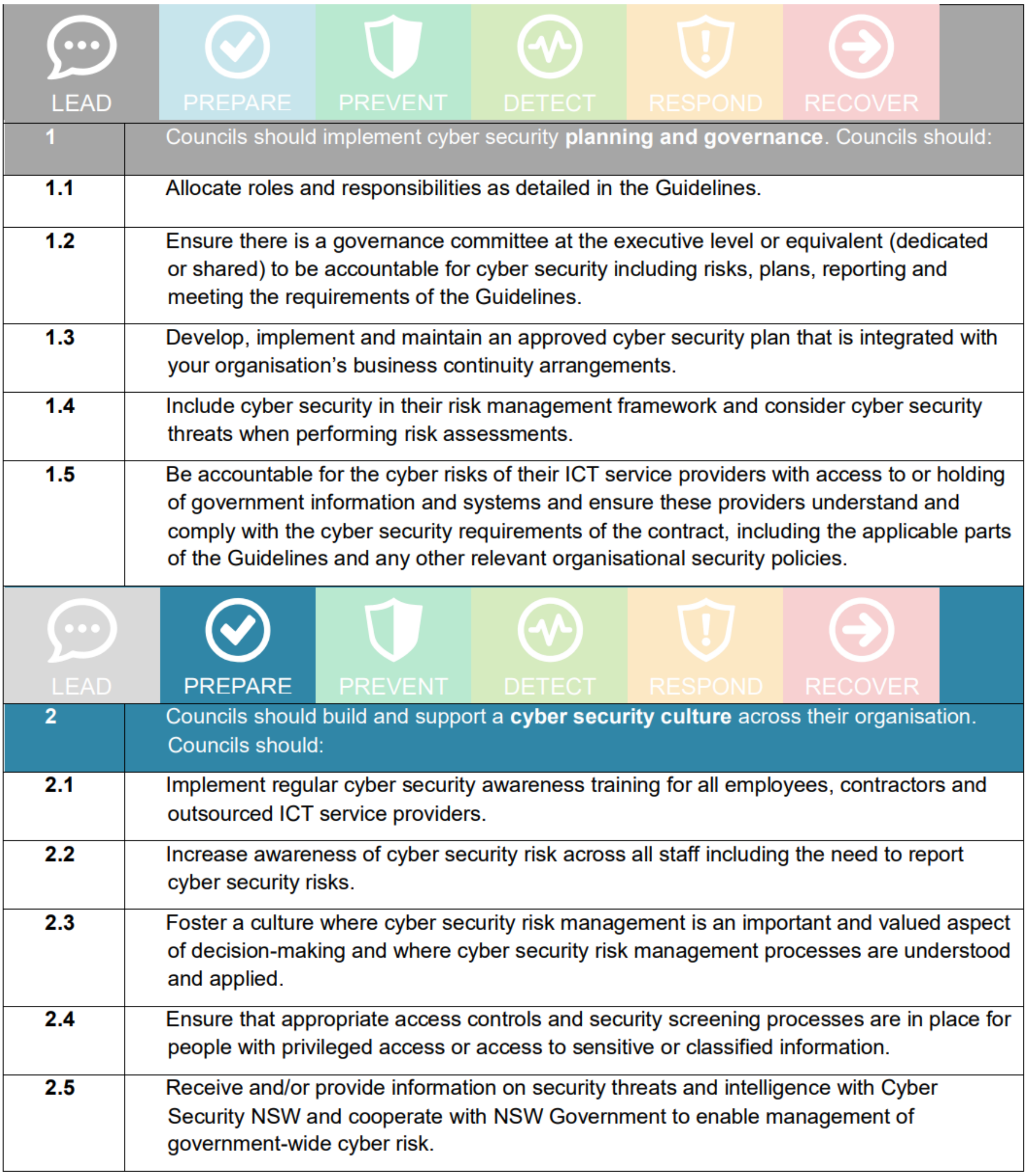
The Australian Cyber Security Centre's (ACSC) recommends that organisations implement eight essential mitigation strategies as a baseline. This baseline, known as the Essential Eight, makes it much harder for adversaries to compromise systems.

The ACSC Essential Eight was refreshed on 12 July 2021. This update focused on using the maturity levels to counter the sophistication of different levels of adversary tradecraft and targeting, rather than being aligned to the intent of a mitigation strategy. The redefinition of a number of maturity levels will also strengthen a risk-based approach to implementation of the Essential Eight strategies. As the maturity model has been redefined and many requirements have changed, maturity assessments for the July 2021 model should not be directly compared to earlier versions of Essential Eight.

Mitigation Strategy	What	Why
Application control	checking programs against a pre-defined approved list and blocking all programs not on this list	So unapproved programs including malware are unable to start and preventing attackers from running programs which enable them to gain access or steal data
Patch applications	Apply security fixes/patches or mitigations (temporary workarounds) for programs within a timely manner (48 Hours for internet reachable applications). Do not use applications which are out-of-support and do not receive security fixes	Unpatched applications can be exploited by attackers and in the worst case enable an attacker to completely takeover an application, access all information contained within and use this access to access connected systems.
Configure MS Office macro settings	Only allow Office macros (automated commands) where there is a business requirement and restrict the type of commands a macro can execute. Also monitor usage of Macros.	Macros can be used to run automated malicious commands that could let an attacker download and install malware
User application hardening	Configure key programs (web browser, office, PDF software, etc) to apply settings that will make it more difficult for an attacker to successfully run commands to install malware	Default settings on key programs like web browsers may not be the most secure configuration. Making changes will help reduce the ability of a compromised/malicious website from successfully downloading and installing malware.
Restrict administrative privileges	Limit how accounts with the ability to administer and alter key system and security settings can be accessed and used.	Administrator accounts are 'the keys to the kingdom' and so controlling their use will make it more difficult for an attacker to identify and successfully gain access to one of these accounts which would give them significant control over systems.
Patch operating systems	Apply security fixes/patches or temporary workarounds/mitigations for operating systems (e.g., Windows) within a timely manner (48 Hours for internet reachable applications). Do not use versions of an Operating system which are old and/or not receiving security fixes	unpatched operating systems can be exploited by attackers and in the worst case enable an attacker to completely takeover an application, access all information contained within and use this access to access connected systems
Multi-factor authentication	A method of validating the user logging in by using additional checks separate to a password such as a code from an SMS/Mobile application or fingerprint scan	Unpatched operating systems can be exploited by attackers and in the worst case enable an attacker to completely takeover an application, access all information contained within and use this access to access connected systems.
Regular backups	Regular backups of important new or changed data, software, and configuration settings, stored disconnected and retained for at least three months. Test the restoration process when the backup capability is initially implemented, annually and whenever IT infrastructure changes.	To ensure information can be accessed following a cyber-security incident e.g., a ransomware incident).

Mandatory Requirements

Outlined below are foundational requirements that focus on enhancing planning and governance, developing a cyber security culture, safeguarding information, and systems, strengthening resilience against attacks and improved reporting.



LEAD PREPARE PREVENT DETECT RESPOND RECOVER

1	Councils should implement cyber security **planning and governance**. Councils should:
1.1	Allocate roles and responsibilities as detailed in the Guidelines.
1.2	Ensure there is a governance committee at the executive level or equivalent (dedicated or shared) to be accountable for cyber security including risks, plans, reporting and meeting the requirements of the Guidelines.
1.3	Develop, implement and maintain an approved cyber security plan that is integrated with your organisation's business continuity arrangements.
1.4	Include cyber security in their risk management framework and consider cyber security threats when performing risk assessments.
1.5	Be accountable for the cyber risks of their 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 the Guidelines and any other relevant organisational security policies.

LEAD PREPARE PREVENT DETECT RESPOND RECOVER

2	Councils should build and support a **cyber security culture** across their organisation. Councils should:
2.1	Implement regular cyber security awareness training for all employees, contractors and outsourced ICT service providers.
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 appropriate access controls and security screening processes are in place for people with privileged access or access to sensitive or classified information.
2.5	Receive and/or provide information on security threats and intelligence with Cyber Security NSW and cooperate with NSW Government to enable management of government-wide cyber risk.

LEAD PREPARE PREVENT DETECT RESPOND RECOVER

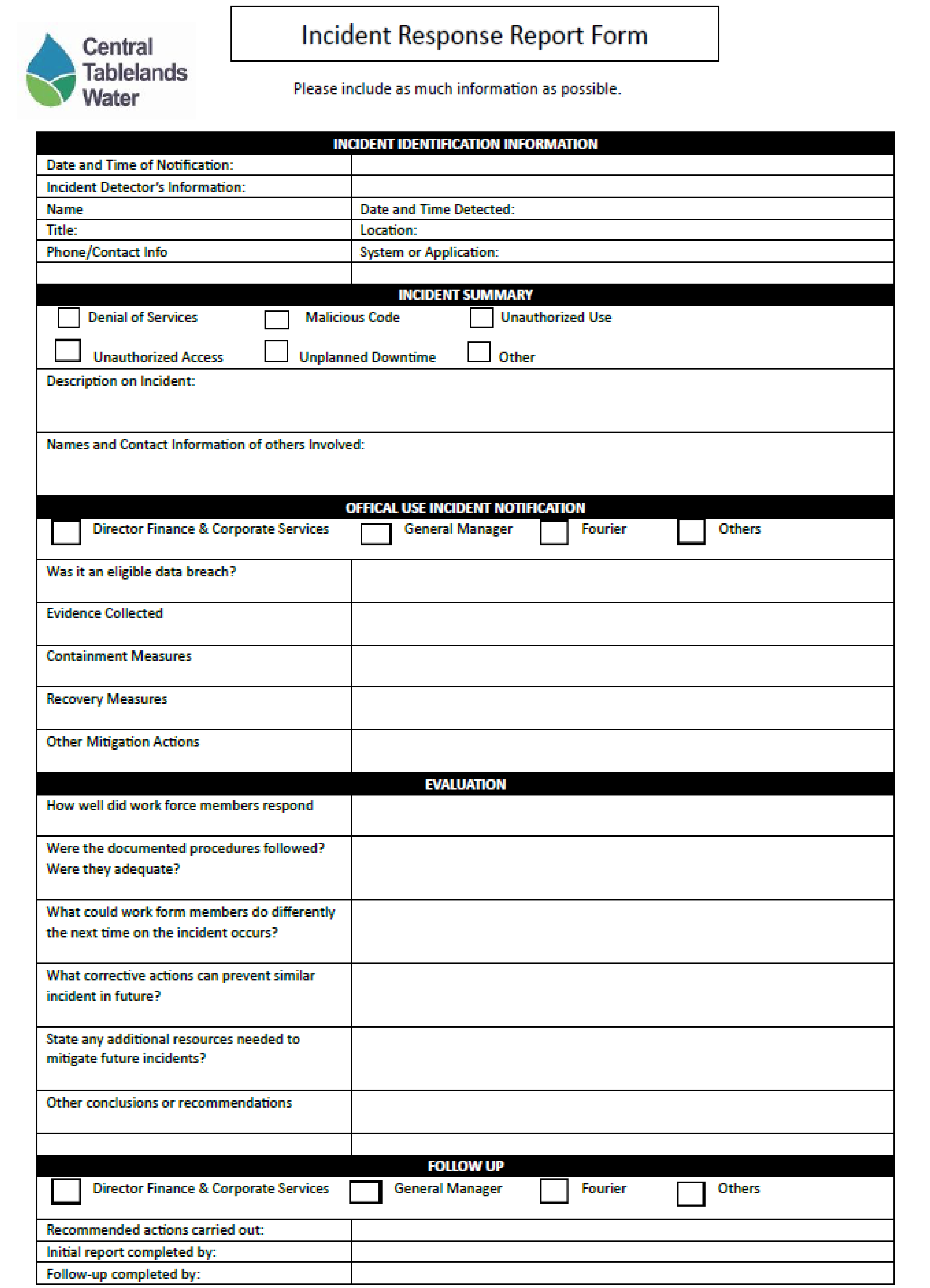
3	Councils should **manage cyber security risks** to safeguard and secure their information and systems. Councils should:
3.1	Implement an Information Security Management System (ISMS), Cyber Security Management System (CSMS) or Cyber Security Framework (CSF).
3.2	Implement the ACSC Essential Eight[3].
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 procurements and into the early stages of projects and the system development life cycle (SDLC), including agile projects. Any upgrades to existing systems must comply with your organisation's cyber risk tolerance.
3.5	Audit trail and activity logging records are determined, documented, implemented and reviewed for new ICT systems and enhancements.

LEAD PREPARE PREVENT DETECT RESPOND RECOVER

4	Councils should improve their **resilience** including their ability to rapidly detect cyber incidents and respond appropriately. Councils should:
4.1	Have a current cyber incident response plan that integrates with the agency incident management process and the *NSW Government Cyber Incident Response Plan*.
4.2	Exercise their cyber incident response plan at least every year.
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 their CISO and/or Cyber Security NSW. If relevant, ensure incident reporting is compliant with Federal reporting requirements.

Definitions

Council means	Central Tablelands Water
GM, Directors, Managers,	any person employed by Council that holds a financial delegated authority to undertake the engagement of a contractor for the purchase of goods and services.
Employees	All Council employees including permanent (whether full-time or part-time), temporary, casual employees and apprentices).
Cyber attack	A deliberate act through cyberspace to manipulate, disrupt, deny, degrade, or destroy computers or networks, or the information resident on them, with the effect of seriously compromising national security, stability, or economic prosperity. Note: There are multiple global definitions of what constitutes a cyber-attack.
Cybercrime	Crimes directed at computers, such as illegally modifying electronic data or seeking a ransom to unlock a computer affected by malicious software. It includes crimes where computers facilitate an existing offence, such as online fraud or online child sex offences.
Cyber crisis	Major disruptions to services and operations, with genuine risks to critical infrastructure and services that pose risks to the safety of citizens and businesses. These often result in intense media interest as well as large demands on resources and critical services.
Cyber incident	An occurrence or activity that may threaten the confidentiality, integrity or availability of a system or the information stored, processed, or communicated by it.
Cyber security	Measures used to protect the confidentiality, integrity and availability of systems, devices and the information residing on them.
Essential Eight	The eight essential mitigation strategies that the ASD recommends organizations implement as a baseline to make it much harder for malicious actors to compromise their systems and data.
Data Breach	For the purposes of this policy, a data breach occurs when there is a failure that has caused Unauthorized Access to, or Unauthorized Disclosure of, data held by the Council.



Central Tablelands Water

Incident Response Report Form

Please include as much information as possible.

INCIDENT IDENTIFICATION INFORMATION	
Date and Time of Notification:	
Incident Detector's Information:	
Name	Date and Time Detected:
Title:	Location:
Phone/Contact Info	System or Application:

INCIDENT SUMMARY

□ Denial of Services □ Malicious Code □ Unauthorized Use

□ Unauthorized Access □ Unplanned Downtime □ Other

Description on Incident:

Names and Contact Information of others Involved:

OFFICAL USE INCIDENT NOTIFICATION

□ Director Finance & Corporate Services □ General Manager □ Fourier □ Others

Was it an eligible data breach?	
Evidence Collected	
Containment Measures	
Recovery Measures	
Other Mitigation Actions	
EVALUATION	
How well did work force members respond	
Were the documented procedures followed? Were they adequate?	
What could work form members do differently the next time on the incident occurs?	
What corrective actions can prevent similar incident in future?	
State any additional resources needed to mitigate future incidents?	
Other conclusions or recommendations	

FOLLOW UP

□ Director Finance & Corporate Services □ General Manager □ Fourier □ Others

Recommended actions carried out:	
Initial report completed by:	
Follow-up completed by:	