

INDEX OF REPORTS
OF THE ORDINARY MEETING OF CENTRAL TABLELANDS WATER
HELD ON WEDNESDAY 24 APRIL 2024

- 0. LATE REPORTS**
- 0.7 DATA BREACH POLICY, CYBER SECURITY POLICY & LEGISLATIVE COMPLIANCE POLICY (CM.PL.1) 2**

LATE REPORTS**0.7) DATA BREACH POLICY, CYBER SECURITY POLICY & LEGISLATIVE COMPLIANCE POLICY (CM.PL.1)**

Author: Governance Executive Support Officer
IP&R Link: – 1.2: Compliance and Regulation

RECOMMENDATION:

1. That Council note the policies.
2. Endorse the Data Breach Policy, Cyber Security Policy & Legislative Compliance Policy, and place on public display for a period of 28 days, and
3. If no submissions are received during the public display period the Data Breach Policy, Cyber Security Policy & Legislative Compliance Policy be adopted.

REPORT

There are three policies presented to Council which are the data breach policy, cyber security policy and legislative compliance policy.

The Data Breach Policy outlines the processes to contain, assess, manage and notify an eligible data breach under the Mandatory Notification of Data Breach (MNDB) scheme established by Part 6A of the Privacy and Personal Information Protection Act 1998 (NSW). The drafted policy will provide guidance for responding in case of a data breach, provide considerations around notifying persons whose privacy may be affected by the breach and assist Council in avoiding or reducing possible harm to both the affected individuals and the Council.

The Cyber Security Policy outlines the mandatory requirements to which Council must adhere, and to ensure cyber security risks to the information and systems are appropriately managed. The policy provides guidance in terms of incident reporting and eight essential mitigation strategies. An incident response report form has been drafted with the Cyber Security Policy to assist the response team to evaluate the incident and provide a response.

The Legislative Compliance Policy is also presented to Council and this policy will aim to prevent, identify and respond to breaches of laws, regulations, codes, or organisational standards occurring in the organisation. This policy contains appropriate processes and structures to ensure that legislative requirements are achievable and are integrated into the everyday running of the Council.

BUDGET IMPLICATIONS

Nil

POLICY IMPLICATIONS

As outlined in the report.

ATTACHMENTS

- 1 [↓](#) Data Breach Policy 10 Pages
- 2 [↓](#) Cyber Security policy 11 Pages
- 3 [↓](#) Legislative Compliance Policy 8 Pages



POLICY

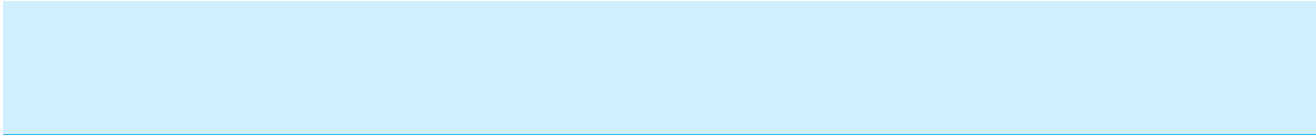


CENTRAL TABLELANDS WATER

DRAFT 2

DATA BREACH POLICY





DOCUMENT CONTROL

Document Title		Data Breach Policy			
Policy Number		CTW-PRO			
Responsible Officer		Director Finance and Corporate Services			
Reviewed by					
Date Adopted					
Adopted by		Council			
Review Due Date					
Revision Number		1			
Previous Versions	Date	Description of Amendments	Author	Review/ Sign Off	Minute No: (if relevant)

PURPOSE

The purpose of this policy is to provide guidance for CTW into responding to a Data Breach. This policy sets out the procedures for managing a Data Breach, including the considerations around notifying persons whose privacy may be affected by the breach. This policy also:

- provides examples of situations considered to constitute a Data Breach
- details the steps to respond to a Data Breach
- outlines the considerations around notifying persons whose privacy may be affected by the breach and our approach to complying with the NSW Mandatory Notification of Data Breach Scheme.

Effective breach management, including notification where warranted, assists CTW in avoiding or reducing possible harm to both the affected individuals/organization. It also provides the opportunity for lessons to be learned which may prevent future breaches.

Scope

- This Policy applies to all persons employed at CTW, including Councillors, contractors, volunteers and other officials.
- The scope of the Policy includes CTW data held in any format or medium (paper based or electronic). The Policy does not apply to information that has been classified as Public (e.g., posted on the website or Facebook).
- Where a data breach is also a cyber security incident, the cyber security and related procedures will also apply.

The Data Breach Policy

This policy sets out how we will respond to a Data Breach in a timely and effective manner, and includes our procedures for managing a Data Breach, including the considerations around notifying persons whose privacy may be affected by the breach.

This Policy will assist the Council to meet its legal obligations in respect of Mandatory Reporting Data Breaches under the Privacy and Personal Information Protection Act 1998 (PPIP Act) and Privacy Act and complies with best practice guidelines.

Council will, at all times, maintain appropriate records of all Data Breaches, regardless of the seriousness of the Data Breach or whether it is immediately contained.

Reporting a Data Breach

All actual or suspected Data Breaches are to be reported immediately via the Data Breach Reporting Form to any one of the Data Breach Review Team members below:

- The General Manager
- Director Finance & the Corporate Services

Any cyber security incident that involves unauthorized access to the CTW data must be reported as soon as possible to the Data Breach Review Team in accordance with the cyber security policy.

Where a Data Breach is reported the 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.

A member of the public can report an actual or suspected Data Breach by completing the form on the contact us section on the website or directly emailing to customer service on water@ctw.nsw.gov.au.

What is an eligible data breach?

A data breach occurs when personal information held by an agency (whether held in digital or hard copy) is subject to unauthorised access, unauthorised disclosure or is lost in circumstances where the loss is likely to result in unauthorised access or unauthorised disclosure.

This may or may not involve disclosure of personal information external to the agency or publicly. For example, unauthorised access to personal information by an agency employee, or unauthorised sharing of personal information between teams within an agency may amount to a data breach.

A data breach may occur as the result of malicious action, systems failure, or human error. A data breach may also occur because of a misconception about whether a particular act or practice is permitted under the Information Protection Principles (IPPs).

Examples of causes of data breaches include:

- Human error
 - when a letter or email is sent to the wrong recipient
 - when system access is incorrectly granted to someone without appropriate authorisation
 - when a physical asset such as a paper record, laptop, USB stick or mobile phone containing personal information is lost or misplaced
 - when staff fail to implement appropriate password security, for example not securing passwords or sharing password and log in information
- System failure
 - where a coding error allows access to a system without authentication
 - where a coding error results in automatically generated notices including the wrong information or being sent to incorrect recipients
 - where systems are not maintained through the application of known and supported patches
 - disclosure of personal information to a scammer as a result of inadequate identity verification procedures
- Malicious or criminal attack
 - cyber incidents such as ransomware, malware, hacking, phishing or brute force access attempts resulting in access to or theft of personal information
 - social engineering or impersonation leading into inappropriate disclosure of personal information
 - insider threats from agency employees using their valid credentials to access or disclose personal information outside the scope of their duties or permissions
 - theft of a physical asset such as a paper record, laptop, USB stick or mobile phone containing personal information.

Responding to a Data Breach

There are four key steps required in responding to a Data Breach. These are:

1. Contain the breach
2. Evaluate the associated risks
3. Consider notifying affected individuals
4. Prevent a repeat.

The first three steps may be undertaken concurrently.

Step 1: Contain the breach

Containing the Data Breach will be prioritised by the Council. All necessary steps possible must be taken to contain the breach and minimise any resulting damage. For example, recover or request deletion of the information, shut down the system that has been breached, suspend the activity that led to the breach, revoke or change access codes or passwords.

If a third party is in possession of the personal information and declines to return or erase it, it may be necessary for the Council to seek legal or other advice on what action can be taken to recover the information. When recovering information, the Council will make sure that copies have not been made by a third party or, if they have, that all copies are recovered.

Step 2: Evaluate the associated risks

To determine what other steps are needed, an assessment of the type of information involved in the breach and the risks associated with the breach will be undertaken.

Some types of information are more likely to cause harm if compromised. For example, financial account information, health information, and security classified information will be more significant than names and email addresses on a newsletter subscription list.

Given the Council's regulatory responsibilities, release of case-related personal information will be treated very seriously. A combination of information will typically create a greater potential for harm than a single piece of data (for example, an address, date of birth and bank account details, if combined, could be used for identity theft).

Factors to consider include:

- **Who is affected by the Data Breach?**
The Council will review whether individuals and organisations have been affected by the breach, how many individuals and organisations have been affected and whether any of the individuals have personal circumstances which may put them at particular risk of harm.
- **What was the cause of the Data Breach?**
The Council's assessment will include reviewing whether the breach occurred as part of a targeted attack or through human error or an inadvertent oversight.

The assessment will aim to determine:

- Was it a one-off incident, has it occurred previously, or does it expose a more systemic vulnerability?

- What steps have been taken to contain the breach?
- Has the data been recovered or erased by the recipient?
- Is the data encrypted or otherwise not readily accessible?

- **What is the foreseeable harm to the affected individuals/organisations?**

The Council's assessment will include reviewing what possible use there is for the data and any likelihood of Serious Harm. This involves considering if the data includes Personal Information or Health Information. The harm that arises as a result of a Data Breach will be context specific and vary for each case.

The assessment will aim to determine:

- Who is in receipt of the information?
- What is the risk of further access, use or disclosure, including via media or online?
- If case-related, does it risk embarrassment or harm to a client and/or damage the Council's reputation?

The Council's assessment will also include consideration of whether the Data Breach would be considered an Eligible Data Breach and reportable under the NSW Mandatory Notification of Data Breach scheme (see page 4).

Step 3: Consider notifying affected individuals/organisations

The Council recognises that notification to individuals/organisations affected by a Data Breach can assist in mitigating any damage for those affected individuals/organisations.

Notification demonstrates a commitment to open and transparent governance, consistent with the Council's values and approach.

The Council will also have regard to the impact upon individuals in recognition of the need to balance the harm and distress caused through notification against the potential harm that may result from the breach. There are occasions where notification can be counterproductive. For example, notifying individuals about a privacy breach which is unlikely to result in an adverse outcome for the individual, may cause unnecessary anxiety and de-sensitise individuals to a significant privacy breach.

Factors the Council will consider when deciding whether notification is appropriate include:

- Is it considered an Eligible Data Breach?
- Are there any applicable legislative provisions or contractual obligations that require the Council to notify affected individuals?
- What type of information is involved?
- Who potentially had access and how widespread was the access?
- What is the risk of harm to the individual/organisation?
- What is the ability of the individual/organisation to take further steps to avoid or remedy harm?

In situations when notification is required it should be done promptly to help to avoid or lessen any potential damage by enabling the individual/organisation to take steps to protect themselves.

The method of notifying affected individuals/organisations will depend in large part on the type and scale of the breach, as well as immediately practical issues such as having contact details for the affected individuals/organisations.

Considerations include the following:

When to notify

In general, individuals/organisations affected by the breach should be notified as soon as practicable. Circumstances where it may be appropriate to delay notification include where notification would compromise an investigation into the cause of the breach or publicly reveal a system vulnerability.

How to notify

Affected individuals/organisations should be notified directly – by telephone, letter, email or in person.

Public Notification will be provided when any or all of the individuals affected by an Eligible Data Breach are unable to be notified individually.

What to say

The notification advice will be tailored to the circumstances of the particular breach.

Content of a notification could include:

- information about the breach, including when it happened
- a description of what data has been disclosed
- what the Council is doing to control or reduce the harm
- what steps the person/organisation can take to further protect themselves and what the Council will do to assist people with this
- contact details for questions or requests for information
- the right to lodge a privacy complaint with the NSW Privacy Commissioner.

Step 4: Prevent a repeat

The Council will further investigate the circumstances of the breach to determine all relevant causes and consider what short or long-term measures could be taken to prevent any reoccurrence.

Preventative actions could include a:

- security audit of both physical and technical security controls
- review of policies and procedures
- review of staff/contractor training practices
- review of contractual obligations with contracted service providers.

Breaches relating to external service providers

Depending on certain requirements, the Council's external contracted service providers have obligations under relevant privacy legislation to notify stakeholders of any Data Breaches that they may experience. Further the Council endeavours to ensure that contracts with vendors that store or manage data for and on behalf of the Council include appropriate provisions that require the prompt notification of a Data Breach to the Council. In the event of a Data Breach concerning the Council, the Council works closely with relevant external contractors to mitigate the effects of the Data Breach on the Council and its customers.

Any Data Breach relating to external service providers that impacts the Council should be reported immediately to the Data Breach Review Team.

Training and Awareness

The Council ensures that its Workers are aware of and understand this Policy including how to identify and report actual or suspected Data Breaches. This policy is published on the Council's website. We provide our Workers with regular reminders of their obligations regarding Sensitive Information and how to reduce the risk of human error Data Breaches from occurring.

NSW Mandatory Notification of Data Breach Scheme

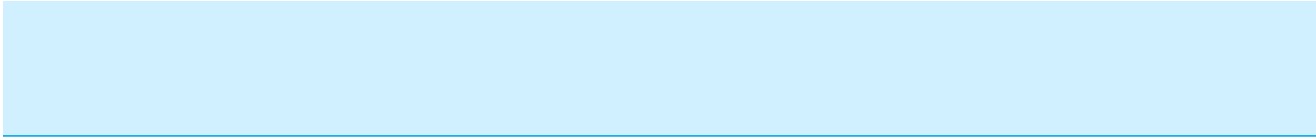
The Council will report all Eligible Data Breaches to the NSW Privacy Commissioner using the IPC online data breach notification form, in line with the NSW Mandatory Notification of Data Breach (MNDB) Scheme.

Under the MNDB, the Council will:

- undertake an assessment within 30 days where there are reasonable grounds to suspect there may have been an Eligible Data Breach
- during the assessment period, make all reasonable attempts to mitigate the harm done by the suspected breach
- decide whether a breach is an Eligible Data Breach or there are reasonable grounds to believe the breach is an Eligible Data Breach
- notify the Privacy Commissioner and affected individuals of the eligible data breach

Data breach documentation

Documentation relating to Data Breaches will be stored in the records document management system. The Council will maintain an internal register of Eligible Data Breaches.



Roles and Responsibilities

Council will have the following roles and responsibilities allocated as part of their Data Breach Policy.

Positions	Responsibilities
The General Manager & Directors	<ul style="list-style-type: none"> • Review, assess and remediate incidents escalated to the team. • Follow this policy when responding to a data breach. • Consult with internal and external stakeholders as required. • Determine if a Data Breach is an Eligible Data Breach. • Review and respond to data breaches impacting Council’s external service providers. • Determine recommendations to prevent a repeat incident. • Follow up on containment actions. • Notify the Council’s insurers as required.
Governance Executive support Officer	<ul style="list-style-type: none"> • Maintain an internal register of Data Breaches, including all Eligible Data Breaches. • Forward each Data Breach incident report to the Data Breach Review Team, which may include a recommendation to consider the incident as an Eligible Data Breach. • Follow up on containment actions.
All employees	<ul style="list-style-type: none"> • Ensuring they have read this policy and that they understand what is expected of them. • Follow the requirements of this policy and understand their obligations to minimise data breaches. • Immediately report any actual or suspected Data Breaches to the Data Breach Review Team.
3rd Party ICT	<ul style="list-style-type: none"> • Take immediate and any longer-term steps to contain and respond to security threats to the Council’s IT systems and infrastructure. • Reports any communications regarding data breach or eligible data breach to the Data Breach Management Team. • Determine recommendations to prevent a repeat incident.

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.
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.
Cyber security incident	means an occurrence or activity that may threaten the confidentiality, integrity or availability of a system or the information stored, processed or communicated by it.
Personal information	means information or an opinion about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion. In this policy, personal information also encompasses health information within the meaning of the HRIP Act and includes information about an individual’s physical or mental health, or disability, or information connected to the provision of a health service to an individual.
Unauthorized Access	Examples include: <ul style="list-style-type: none"> • an Employee browsing customer records without a legitimate purpose • a computer network being compromised by an external attacker resulting in Sensitive Information being accessed without authority.
Unauthorised Disclosure	Examples include: <ul style="list-style-type: none"> • an employee sending an email containing personal information to the wrong recipient • incorrect contact details entered into automatic information systems e.g., water account notices.
Sensitive Information	Information and data (including metadata) including Personal Information, Health Information, information protected under legal professional privilege, information covered by secrecy provisions under any legislation, commercial-in-confidence provisions, floor plans of significant buildings, Security Classified Information and information related to the Council’s IT/cyber security systems.
Serious Harm	Harm arising from a Data Breach that has or may result in a real and substantial detrimental effect to the individual. The effect on the individual must be more than mere irritation, annoyance or inconvenience.



POLICY

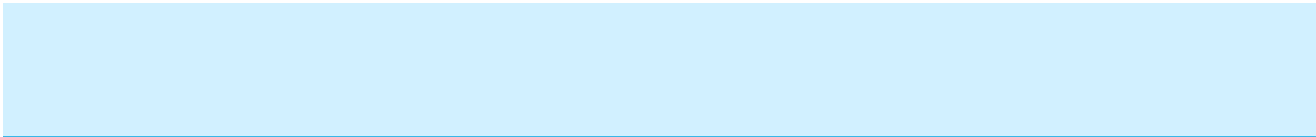


CENTRAL TABLELANDS WATER

DRAFT 3

CYBER SECURITY POLICY





DOCUMENT CONTROL

Document Title		Cyber Security Policy			
Policy Number		CTW-PRO			
Responsible Officer		Director Finance and Corporate Services			
Reviewed by					
Date Adopted					
Adopted by		Council			
Review Due Date					
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.

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 Internal Audit teams are responsible for:

- 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:

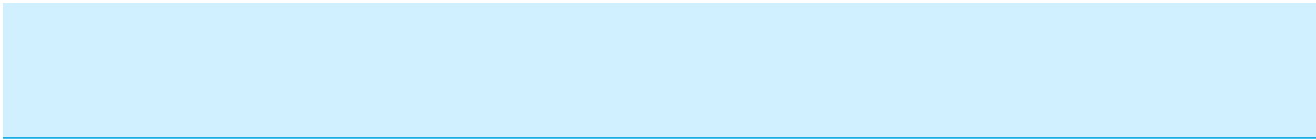
- Foundational Requirement 1.5: The third-party organisation has a process that is followed to notify the Council quickly of any suspected or actual security incidents and follows reasonable direction from the Council arising from incident investigations (noting this will vary based on risk profile and 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.

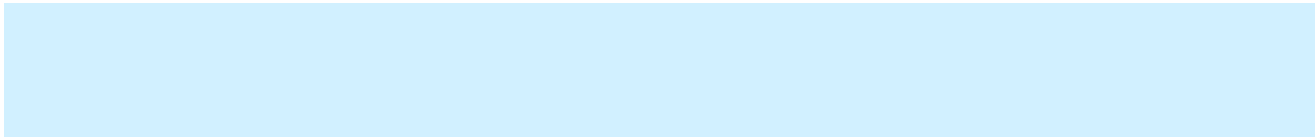














Mitigation Strategy	What	Why
Application control	checking programs against a pre-defined approved list and blocking all programs not on this list	So unapproved programs including malware are unable to start and preventing attackers from running programs which enable them to gain access or steal data
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).

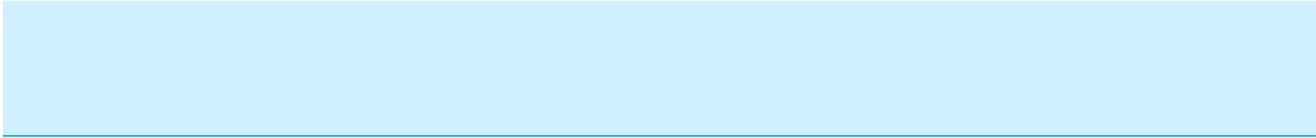
Mandatory Requirements

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.				

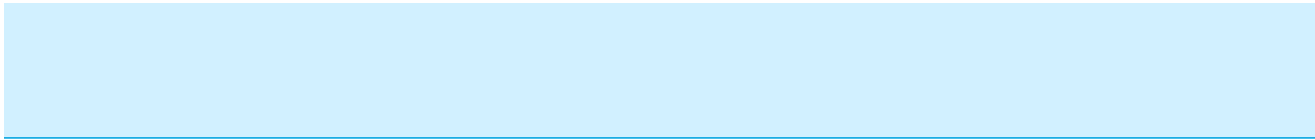


 LEAD	 PREPARE	 PREVENT	 DETECT	 RESPOND	 RECOVER
3	Councils should manage cyber security risks to safeguard and secure their information and systems. Councils should:				
3.1	Implement an Information Security Management System (ISMS), Cyber Security Management System (CSMS) or Cyber Security Framework (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 <i>NSW Government Cyber Incident Response Plan</i> .				
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.



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	
<input type="checkbox"/> Denial of Services <input type="checkbox"/> Malicious Code <input type="checkbox"/> Unauthorized Use <input type="checkbox"/> Unauthorized Access <input type="checkbox"/> Unplanned Downtime <input type="checkbox"/> Other	
Description on Incident:	
Names and Contact Information of others Involved:	
OFFICIAL USE INCIDENT NOTIFICATION	
<input type="checkbox"/> Director Finance & Corporate Services <input type="checkbox"/> General Manager <input type="checkbox"/> Fourier <input type="checkbox"/> 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	
<input type="checkbox"/> Director Finance & Corporate Services <input type="checkbox"/> General Manager <input type="checkbox"/> Fourier <input type="checkbox"/> Others	
Recommended actions carried out:	
Initial report completed by:	
Follow-up completed by:	



POLICY

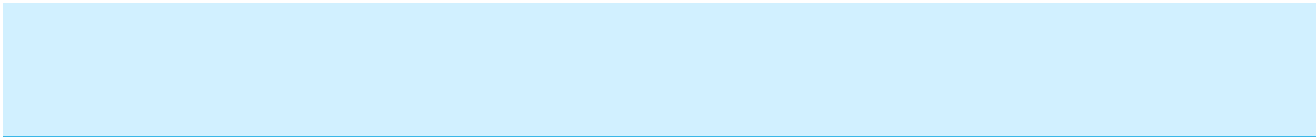


CENTRAL TABLELANDS WATER

DRAFT 2

**LEGISLATIVE
COMPLIANCE
POLICY**





DOCUMENT CONTROL

Document Title		Legislative Compliance Policy			
Policy Number		CTW-PRO			
Responsible Officer		Director Finance and Corporate Services			
Reviewed by					
Date Adopted					
Adopted by		Council			
Review Due Date					
Revision Number					
Previous Versions	Date	Description of Amendments	Author	Review/ Sign Off	Minute No: (if relevant)

Introduction

Central Tablelands Water is committed to compliance with all statutory and common law requirements relating to operations and governance of Council. The consequences of breaching legislation can vary greatly between minimal impact on Council to severe consequences of both a civil and criminal nature. The Council ensure that its legislative requirements are complied with. The community and those working at Council have a high expectation that Council will comply with applicable legislation and Council should take all appropriate measures to ensure that that expectation is met.

Policy Aim

This Policy, and the principles set out in this Policy, aim to:

- a.) Prevent, and where necessary, identify and respond to breaches of laws, regulations, codes or organisational standards occurring in the organisation.
- b.) Promote a culture of compliance within the organisation; and
- c.) Assist the Council in achieving the highest standards of governance.

Scope

This policy applies to all Council officials, areas of Council's operations, and covers compliance with Commonwealth and State legislation, Council codes and policies, contracts, funding agreements, and relevant standards. It is noted that Council has limited staff resources and senior staff have to pick up responsibilities for tasks that are routinely undertaken by the engagement of separate officers.

Policy

CTW is committed to complying with all applicable legislation, regulations, and recognised codes and guidelines, acknowledging that compliance with these obligations is both necessary and desirable. Council shall have appropriate processes and structures to ensure that legislative requirements are achievable and are integrated into the everyday running of the Council.

These processes and structures will aim to:

- a.) Develop and maintain a system for identifying the legislation that applies to Council's activities.
- b.) Assign responsibilities for ensuring that legislation and regulatory obligations are fully implemented in Council.
- c.) Provide training for relevant staff, Councillors, volunteers and other relevant people in the legislative requirements that affect them.
- d.) Provide people with the resources to identify and remain up to date with new legislation.
- e.) Conduct of audits to ensure there is compliance.
- f.) Establish a mechanism for reporting non-compliance.
- g.) Review accidents, incidents and other situations where there may have been non-compliance.
- h.) Review audit reports, incident reports, complaints and other information to assess how the systems of compliance can be improved.

Roles and Responsibility

This policy is issued under the authority of the General Manager and will be reviewed and amended as required in consultation with the Directors and staff of CTW

Position	Responsibility
Councillors and Committee Members	<ul style="list-style-type: none"> • Councillors and Committee members have a responsibility to be aware of and abide by legislation applicable to their role. • providing appropriate resourcing for the management to comply obligations • reviewing and making recommendations regarding the annual compliance certification report and providing the report to the Audit Committee of CTW
Senior Management (General Manager and Directors)	<ul style="list-style-type: none"> • Ensuring all relevant internal compliance controls are applied within their department. • Taking all necessary actions to resolve breaches • Senior management should ensure that directions relating to compliance are clear and unambiguous and that legal requirements which apply to each activity for which they are responsible are identified. • Senior management should have systems in place to ensure that all staff are given the opportunity to be kept fully informed, briefed and/or trained about key legal requirements relative to their work within the financial capacity to do so. • Reporting all breaches that occur in their department. • Providing compliance certification for selected legislation as required and any other required reporting
Audit and Risk Committee	<ul style="list-style-type: none"> • responsible for endorsement and the monitoring of the legislative compliance framework. • assistance to Council on risk management, control, governance, and external accountability responsibilities.
Governance Officer	<ul style="list-style-type: none"> • Responsible to maintain the legislative compliance register.
Employees	<ul style="list-style-type: none"> • Employees shall report through their supervisors to senior management any areas of non-compliance that they become aware of. • Reporting breaches to supervisor

General Principles

- a) Council is committed to achieving compliance in all areas of its operations.
- b) Council will maintain a Legislative Compliance Policy that sets out its commitment to compliance with applicable laws, regulations, codes and Council standards.
- c) Council will provide sufficient resources to ensure that its Compliance Program can be implemented, maintained and improved.
- d) Council will ensure that all managers, supervisors and staff generally understand, promote and be responsible for compliance with relevant laws, regulations, codes and Council standards that apply to activities within their day-to-day responsibilities.
- e) Council will use its established Enterprise Risk Management Framework to accurately identify, rate and treat compliance risks.
- f) Council will ensure that compliance requirements are integrated into day-to-day operating procedures as appropriate.
- g) Council will maintain a compliance register in association with its Risk Register.
- h) Council will investigate, rectify and report all compliance failures.
- i) Council will allocate appropriate responsibilities for managing compliance at various levels.
- j) Council will provide appropriate education and training of staff in order for them to meet their compliance obligation.
- k) Council will actively promote the importance of compliance to staff, contractors and other relevant third parties.
- l) Council will review its legislative compliance programme regularly to ensure its effectiveness.

Reporting a Compliance Breach

If staff identify actual or suspected non-compliance with legislative obligations, this must be reported where required and as soon as practicable. If an established reporting pathway exists for an obligation, it must be reported through this pathway. If there is no established compliance pathway, or the pathway is unknown, staff should report to their supervisor, or General Manager, who must promptly action the report and manage any impacts arising from the non-compliance. The legislative compliance register outlines where non-compliance should be reported for compliance focus areas only.

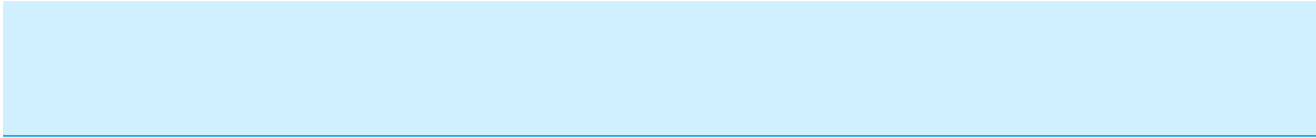
Procedure

Council will have a system in place (legislative compliance register) to ensure that when legislation changes, steps are taken to ensure that actions comply with the amended legislation. A Legislative Compliance Register has been prepared and is an attachment to this policy.

Acknowledgement

CTW would like to extend acknowledgement to the following organizations from which samples were taken to draft this policy.

- Parkes Shire Council
- Information and Privacy Commission NSW
- Office of Local Government Legislative Compliance Calendar



Review

This Policy will be reviewed at least every four years in the absence of any significant changes or more frequently where required taking into account legislative or organisational changes, risk factors and consistency with other supporting policies.

Definitions

Codes	Mandatory industry codes and voluntary industry codes with which the Council chooses and/or is required to comply.
Compliance	Ensuring that the requirements of laws, regulations, industry codes and Council standards are met.
Compliance failure	A breach, of applicable laws, regulations, codes and Council standards.
Compliance culture	The promotion of a positive attitude to compliance within the Council.
Legislation	Effective control of legal risks in order to ensure that the law is complied with.
Council standards	Any codes of ethics, codes of conduct, policies, procedures and charters that Council may deem to be appropriate standards for its day-to-day operations.

Central Tablelands Water Legislative Compliance Procedure

1. Identifying Current Legislation

(a) Electronic Versions of Legislation

Council accesses electronic up-to-date versions of legislation through the New South Wales legislation website at www.legislation.nsw.gov.au. The NSW legislation website is the official NSW Government site for the online publication of legislation and is provided and maintained by the Parliamentary Counsel's Office.

Federal laws and instruments should be accessed through the Federal Register of Legislation at www.legislation.gov.au

(b) Australian Standards

Council will review the standards Australia website Store | Standards Australia Store to get details of the latest or new standards.

2. Identifying New or Amended Legislation

a) NSW Government Gazette

Council provides website access for its staff to the NSW Government Gazette which publishes all new or amended legislation applicable to New South Wales.

b) Office of Local Government

Council receives regular circulars from the Office of Local Government on any new or amended legislation relevant to Local government. Such advice are received through Council's main email address i.e. water@ctw.nsw.gov.au and must be distributed by the Customer Service staff to the relevant Council Officer for implementation and Councillors for information where applicable.

c) Local Government NSW

Council receives a weekly circular from the Local Government NSW. These circulars have sections on legal, finance and water matter that highlight changes in legislation applicable to Councils and must be distributed to relevant Council officers and Councillors for information.

3. Obtaining Advice on Legislative Provisions

Advice on matters of legislative interpretation may be sought when deemed necessary.

4. Informing Council of Legislative Change

If deemed necessary, the General Manager or a nominated officer, will, on receipt of advice of legislative amendments, submit a report to a Council meeting on the new or amended legislation where any changes will impact significantly on Council or its operations.

5. Review of Incidents and Complaints for Non-compliance

Council shall review all incidents and complaints in accordance with its incident reporting and complaint handling procedures. Such reviews and investigations will assess compliance with legislation, standards, policies and procedures that are applicable.

6. Reporting of Non-compliance

All instances of non-compliance shall be reported as soon as practicable to the respective supervisor/manager. The manager shall determine the appropriate response and ensure the legislative compliance register is updated appropriately. If the matter is deemed a significant breach or significant fines and/or criminal sanctions apply, the matter must be reported immediately to the relevant Director.

Directors should report the matter to the General Manager via Senior Staff Meetings on a fortnight basis and report the matter to the General Manager immediately if the breach in question is significant or criminal sanctions may be involved.

The General Manager may instigate an investigation into any non-compliance matter and will report significant non-compliance matters to the Council and external agencies as required.

7. Auditing Legislative Compliance

Council shall incorporate a review of its processes to ensure legislative compliance is included in its internal audit function.

8. Review of Legislative Compliance Procedures

Legislative compliance procedures will be reviewed as the regulatory environment changes.