DRAFT

POLICY

Central Tablelands Water

DATA BREACH POLICY

DOCUMENT CONTROL

Document Title		Data Breach Policy			
Policy Number		CTW-PR049			
Responsible Officer		Executive Manager Corporate Services			
Reviewed by		Council			
Date Adopted		Xx July 2026			
Adopted by		Council			
Review Due Date		June 2028			
Revision Number		2			
Previous Versions	**Date**	**Description of Amendments**	**Author**	**Review/ Sign Off**	**Minute No: (if relevant)**
1	June 2024		DFCS	Council	24/043
2	June 2026	Standard review; move operational tasks into a procedure	EMCS	Council	

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 Council officers, staff, authorised representatives, and consultants who are formally approved to undertake procurement activities on behalf of Council.

The scope of the policy includes Council data held in any format or medium (paper based or digital). The policy does not apply to information that has been classified as public.

POLICY STATEMENT

This policy sets out how we will respond to a data breach in a timely and effective manner, including the considerations around notifying persons whose privacy may be affected by the breach.

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 to:

- The General Manager
- Executive Manager Corporate Services.

Where a data breach is reported a preliminary assessment will be undertaken. Where required, such as where the incident meets the requirements of an eligible data breach or involves sensitive information, the Executive Manager Corporate Services will promptly 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 of the CTW website www.ctw.nsw.gov.au or emailing 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 Council. For example, unauthorised access to personal information by a council employee, or unauthorised sharing of personal information between teams within Council, 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, such as 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 information
  - social engineering or impersonation leading into inappropriate disclosure of information
  - insider threats from Council employees using their valid credentials to access or disclose 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 information.

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 Council 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 Council include appropriate provisions that require the prompt notification of a data breach. In the event of a data breach concerning Council, staff work closely with relevant external contractors to mitigate the effects of the data breach on Council and/or its customers.

Any data breach relating to external service providers that impacts the Council should be reported immediately the General Manager or Executive Manager Corporate Services.

Training and Awareness

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 Council's website. We provide our staff 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

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, 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 Records

Records relating to data breaches will be stored in Councils records management system. Council will maintain an internal register of Eligible Data Breaches.

Roles and Responsibilities

Council has the following roles and responsibilities allocated

Positions	Responsibilities
General Manager and Executive Managers	• Review, assess, and remediate incidents • 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 Council's insurers, if required
Governance Executive Support Officer	• Maintain an internal register of data breaches • Forward each data breach incident report to the Executive Manager Corporate Services
All staff	• Ensure they have read this policy and 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 Executive Manager Corporate Services
Third Party ICT provider	• Take immediate and any longer-term steps to contain and respond to security threats to Council's IT systems and infrastructure. • Reports any communications regarding data breach or eligible data breach to the Executive Manager Corporate Services. • Determine recommendations to prevent a repeat incident.

Definitions

Council	Central Tablelands Water
Delegation	any staff member that holds a financial delegated authority to undertake the engagement of a contractor, for the purchase of goods and services.
Staff	All Council staff, including permanent (whether full-time or part-time), temporary, casual, trainees, or 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 Unauthorised Disclosure of, data held by 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.
Unauthorised Access	Examples include (but not limited to): • an staff member 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 (but limited to): • a staff member sending an email containing personal information to the wrong recipient • incorrect contact details entered into information systems e.g., water account notices.
Sensitive Information	Information and data (including metadata) including Personal Information, information protected under legal professional privilege, information covered by secrecy provisions under any legislation, commercial-in-confidence provisions, floor plans of significant facilities, Security Classified Information and information related to 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 REVIEW

This policy will be reviewed every 2 years or more frequently if needed, with reference to any relevant legislation, best practice guides, or other related factors.

REFERENCES

- Privacy and Personal Information Protection Act 1998 (NSW)
- Government Information (Public Access) Act 2009 (NSW)
- NSW Mandatory Notification of Data Breach Scheme (Part 6A PPIP Act)
- NSW IPC Data Breach Policy Guidance
- Council Cyber Security Policy
- IPC Guide to Preparing a Data Breach Policy May 2023

VARIATION

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