POLICY

CENTRAL TABLELANDS WATER

DATA BREACH POLICY

DOCUMENT CONTROL

Document Title		Data Breach Policy			
Policy Number		CTW-PR049			
Responsible Officer		Director Finance and Corporate Services			
Reviewed by		Council			
Date Adopted		19 June 2024			
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	• 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	• 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	• 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	• 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: • 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: • 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.