CENTRAL DARLING SHIRE COUNCIL

DATA BREACH POLICY

Document Reference No:	GD/	**Version:**	One
Service Unit:	Customer Service		
Author:	Governance Officer		
Responsible Director:	General Manager		
Authorisation Date:	26 June 2024	**Review Date:**	
Minute No:			

Purpose

Central Darling Shire Council (CDSC) has adopted the Data Breach Policy to inform the public of our processes for identifying, responding to, and reporting data breaches of CDSC held information. This is required by the Information and Privacy Commissioner of NSW (IPC).

In accordance with the guidelines provided by the IPC, the Data Breach Policy includes:

- Examples of situations considered to constitute a data breach.
- Key steps involved in responding to a data breach.
- Considerations around notifying persons whose privacy may be affected by a data breach on a mandatory basis where required, or on a voluntary basis where warranted, to ensure CDSC responds appropriately.
- Assisting CDSC in avoiding or reducing possible harm to both the affected individuals and CDSC.

Application

The Data Breach Policy applies to all Council Officials and contractors of Central Darling Shire Council (CDSC), as they are responsible for:

- Using and preserving CDSC's systems and digital assets in a secure way.
- Familiarising themselves with CDSC's policies and standards and being aware of, and complying with, their responsibilities.
- Reporting incidents or suspected records security breaches to the General Manager or delegate.
- Considering what measures could be taken to prevent any recurrence.

Definitions

For the purposes of this policy:

Data Breach – a failure that has caused unauthorised access to, or inadvertent disclosure, access, modification, misuse or loss of, or interference with, confidential information held by CDSC.

Confidential 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 CDSC's IT/cyber security systems.

Council Official – as defined by the Council Code of Conduct and including Councillors, members of staff, administrators, council committee members, delegates of council, volunteers, contractors, and council advisors.

Data Breach Review Team – appropriate members of the Management/Executive (ManEx) Group appointed by the General Manager according to the nature and circumstances of the breach.

Eligible Data Breach – where there is unauthorised access to or unauthorised disclosure of personal information, and a reasonable person would conclude that this would be likely to result in serious harm to an individual to whom the information relates.

Health Information - A specific type of Personal Information which may include information about a person's physical or mental health or their disability. This includes, for example, medical certificates, information about medical appointments or test results.

Personal Information - Information or an opinion (including information or an opinion forming part of a database and in recorded form) about an individual whose identity is apparent or can be reasonably ascertained from the information or opinion. This includes, for example, their name, address, email address, phone number, date of birth or photographs.

Security Classified Information - Information and data (including metadata) that is marked as Protected, Secret, or Top Secret as per the Commonwealth Attorney Generals' Department's Protective Security Policy Framework.

Unauthorised access – examples include a Council Official browsing records without a legitimate purpose, and a computer network being compromised by an external hacker or social engineering fraud resulting in personal information being accessed without authority.

Provisions

CDSC has established a range of measures for managing data security. These include policies and procedures, projects to increase cyber security maturity, cyber security training and a records management framework. The risk of a data breach, which may involve a cyber-security incident, is identified in the Risk Register along with established controls to mitigate this risk and its impacts on CDSC systems, and individuals. The loss of ITC systems and responses are also included in CDSC's Business Continuity Plan.

CDSC will form a Data Breach Review Team, which has the role of investigating, responding to, and reporting on any known or notified Data Breach involving confidential information. A data breach may occur as the result of malicious action, systems failure, or human error. The General Manager will appoint team members from the ManEx Group according to the type of incident, to:

Contain the breach

Containing the Data Breach will be prioritized by CDSC. All necessary steps possible will be taken to contain the breach and minimize any resulting damage. This may include recovering or requesting deletion of the information, shutting down the system that has been breached, suspending the activity that led to the breach, and revoking or changing access codes or passwords.

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.

Release of case-related personal information will be treated very seriously, as 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 included in this assessment will be:

- Who is affected by the Data Breach?
- What was the cause?
- What is the foreseeable harm to the affected individuals?

Consideration of notification

CDSC recognises that notification to individuals/organisations affected by a Data Breach can assist in mitigating any damage for those affected individuals/organisations. CDSC will also consider the impact of notification compared to any potential harm that may result from the breach, as there could be occasions where notification would be counter-productive – 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.

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 will depend on the type and scale of the breach, as well as immediate practical issues such as having contact details for the affected individuals/organisations.

CDSC will notify the IPC of a data breach in accordance with the IPC's guidelines, where personal information has been disclosed and there are risks to the privacy of individuals.

Preventing a Repeat

CDSC will 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 service providers.

Roles and responsibilities

All Council Officials

- Immediately report any actual or suspected data breach by way of an incident report to the Risk & WHS Officer

Risk and WHS Officer

- Notify the General Manager and appropriate members of the Management Executive Group (ManEx) to form a Data Breach Review Team, according to the type of incident

Data Breach Review Team

- assemble promptly to review and respond to a data breach
- follow this policy when responding to a data breach
- consult with internal and external stakeholders as required
- review reports for each separate Data Breach incident.

Customer Services Manager

- take immediate action to contain and respond to security threats to CDSC's records and information technology systems, including notification to ITC/Cyber Security providers
- recommend longer-term steps to prevent a repeat
- ensure all records relating to data breaches are securely secured in CDSC's Electronic Document Management System

Governance Officer

- undertake external notifications as needed, including mandatory eligible data breach notifications per legislation and to CDSC's insurers.

Legislation

Privacy and Personal Information Protection Act 1998

Health Records and Information Privacy Act 2002

Related Documents

External

IPC Data Breach Guidance for NSW Agencies (May 2023)

Office of Local Government Circular to Councils 24-06 / 29/05/2024 Privacy and the Mandatory Notification of Data Breach Scheme

Internal

Business Continuity Plan

Incident Reporting Procedure

Legislative Compliance Policy

Records Management Framework

Risk Management Framework

Monitoring and Review

This policy will be monitored and reviewed by the General Manager to ensure compliance. Once adopted, it remains in force until it is reviewed by Council. It is to be reviewed approximately every two (2) years to ensure that it meets requirements, or sooner if the General Manager determines appropriate.