DATA BREACH RESPONSE POLICY

16.18.01

1. BACKGROUND

The Data Breach Response Policy has been formulated in response to the amendments to the *Privacy and Personal Information Protection Act 1998,* focusing specifically on the Mandatory Notifiable Data Breach Scheme.

Weddin Shire Council (Council) adopted their Cyber Security Policy in October 2023, indicating a shift towards a more proactive approach in cybersecurity, particularly in the management and protection of sensitive data. In line with this, a Cyber Incident Register has been established. This register serves not only as a repository for recording cyber incidents but also as a tool for effectively triaging these incidents. It aids in determining whether an incident constitutes a breach and if it is notifiable under the scheme.

The Data Breach Response Policy is designed to work in harmony with these initiatives, providing clear guidelines and procedures for responding to data breaches, thereby enhancing our commitment to safeguarding personal and sensitive information.

2. PURPOSE

The purpose of the Data Breach Response Policy ('Policy') is to provide comprehensive guidelines for Council on adhering to the Mandatory Notifiable Data Breach Scheme as stipulated under Part 6A of the *Privacy and Personal Information Protection Act 1998* (PPIP Act).

With these guidelines staff will be able to identify, report, and manage data breaches effectively, ensuring that our response aligns with the legal requirements set forth by the NSW Mandatory Notification of Data Breach (MNDB) scheme.

The Policy is a local supplement to the provisions of the Act and Regulation.

3. POLICY OBJECTIVES

The objectives of this Policy are to:

- Comply with amendments to *Privacy and Personal Information Protection Act 1998* (PPIP Act).
- Provide guidelines to Council when responding to a data breach and outlining what qualifies as a notifiable data breach.
- Ensuring transparency in the process of handling a data breach.
- Minimise the impact of a notifiable data breach.
- Improve data security based on historic data breach information.

4. LEGISLATION

Council and its users have a responsibility to comply with relevant laws around Privacy and Personal Information.

The Policy relates to the following legislation:

- *Privacy and Personal Information Protection Act 1998*
- Privacy and Personal Information Protection Regulation 2019 (NSW)
- *State Records Act 1998 (NSW)*
- Weddin Shire Council Policy For Records Management
- Weddin Shire Council Cyber Security Policy

5. APPLICATION/SCOPE

This Policy applies at all times to employees, Councillors, consultants, and contractors, volunteers, work placement students or any other persons (Users) who access, handle, or manage personal or sensitive data stored within Council's file servers, software packages, and other data repositories on behalf of Council.

The Policy is supported by the Cyber Security Policy and any other user procedures developed to support the Policy.

6. POLICY

6.1. Roles and Responsibilities

The following table outlines the roles and responsibilities of personnel. Noting that the position titles may change, however, the responsibilities remain the same.

Roles	Responsibility
The Elected Council	Council has the responsibility to consider draft local policies and the adoption of the local policy
General Manager	The General Manager is responsible for the overall control and implementation of the Policy.
Director Corporate Services	The Director Corporate Services is responsible for updating the Data Breach Response Policy in line with legislative amendments and/or reviewing and updating as appropriate. They are responsible for implementing the Policy and ensuring compliance.
IT Officer/	The IT Officer is responsible for the implementation of the Policy and the development of accompanying procedures.
General Public	The general public must act in accordance with this policy and abide by any determination made as a result of this policy. The general public are able to review Council's Data Breach Register for openness and transparency.

6.2. Data Breach

A data breach involves unauthorised access, disclosure, or loss of personal information. It is deemed notifiable if it presents a likely risk of causing serious harm to the affected individual. A notifiable breach is also referred to as an eligible data breach.

A data breach could be identified during routine reviews of our systems and logs, a notification from a third party who host data on behalf of Council, or by external scan of Council infrastructure on behalf of Council. Once identified the table below can act as a guideline for how to proceed.

Action	Responsible Party	Timeline
Detect and Isolate	IT Officer	As soon as detected
Assess Severity	IT Officer, Director of Corporate Services.	Within 7 days of detection
Notify Decision	IT Officer, Director Corporate Services, General Manager	Within 14 days of detection
Document and Report	IT Officer, Director of Corporate Services.	Within 30 days of detection
Review and Improve	IT Officer, Director of Corporate Services.	Within 30 days of detection

6.3. Data Breach Register

Council must establish a Data Breach Public Notification Register. Details of the public notification for any notifiable data breach within the past 12 months under the PPIP Act will be available on Council's public register on the website.

6.3.1. Data breach

Councils Cyber Incident Register includes provisions for keeping track of Data Breaches. This includes:

- Who has been notified of the breach (If notifiable)
- Date of breach notification
- Type of breach (including whether or not it is notifiable)
- Mitigation of breach
- Preventative action taken
- Estimated cost of breach

6.3.2. Eligible Data Breach

An Eligible data breach is any breach that presents the likely risk of causing serious harm to the affected individual. When a breach is identified it must be addressed within 30 day and if found to be an eligible

data breach must be notified to the Office of the Australian Information Commissioner (OAIC) and the affected individuals.

6.3.3. Data Breach Notification

A notification must be made if it is believed that an eligible data breach has occurred or if directed so by the OAIC.

Individuals should be promptly contacted if and where possible when an eligible data breach is detected. The notification to affected individuals will include details of the breach, specifying the nature of the exposure and the type of data that has been breached.

A public notice must be placed on the Council's website for transparency. The public notice will outline the details of the breach, including the type of data that has been breached. This ensures open communication with the public and fosters transparency regarding the incident.

6.4. Assessing Data Breach Severity

The severity of the data breach can be assessed on several factors.

- **Unauthorised Access:** Was the access to the data unauthorised by either an internal or external party.
- **Unauthorised Disclosure:** Has the data been made publicly available and visible to unauthorised parties.
- **Loss of Personally identifiable information (PII):** Does the data include PII.
- **Serious Harm Considerations:**
    - For unauthorised access: Assess the likelihood of harm for individuals in the breach.
    - For unauthorised disclosure: Evaluate the risk of serious harm if information is visible to unauthorised parties.
    - For loss of personally identifiable information: Assess the risk of unauthorised access due to lost personal information.
- **Context of the Data Breach:**
    - Consider whose information was involved and their vulnerability.
    - Evaluate sensitivity of disclosed information. Assess factors like time of accessibility and ease of access.

6.5. Data Breach Containment

While it is not possible to undo a data breach, Council will attempt to ensure the spread of the data is limited, as well as notifying users as per the requirements of an eligible data breach. Council will patch and identify vulnerabilities or misconfigurations in systems that allowed the breach to

happen and work to prevent a data breach of a similar nature happening again.

6.6. Post Breach Review

Throughout the post-breach review, Council will assess the information with the aim of preventing similar breaches. This approach also allows Council to gather valuable lessons from past errors and better protect system and data.

6.7. Data Breach Reporting

Notification is mandatory under this Policy solely in the case of an eligible data breach. Eligible data breaches must be reported to the OAIC. The report to the OAIC should include:

- A comprehensive description of the data breach, outlining the circumstances and details of the incident.
- Specific information regarding the type of information included in the breach.
- Details on the steps that have been taken to notify the individuals impacted by the breach.

This information can be communicated via the OAIC website, ensuring transparency and compliance with reporting obligations.

Cybersecurity incidents, including an eligible data breach, should also be reported to Cyber NSW. Proactive engagement with Cyber NSW ensures access to a range of products, services, and best practice advice to enhance the overall cybersecurity posture of Council.

Depending on the nature of the breach, other entities may also be notified:

- Financial services providers
- NSW Police
- The Australian Taxation Office
- The Australian Digital Health Authority
- The Department of Health
- Department of Customer Service
- Professional associations, regulatory bodies or insurers
- Service NSW

7. DEFINITIONS

Key Terms	Meaning
Council	Weddin Shire Council
Data Breach	Unauthorised access to, or disclosure of, personal information or a loss of personal information.
Eligible Data Breach	A data breach likely to result in serious harm, requiring notification
OAIC	Office of the Australian Information Commissioner
Patch	Software update designed to fix or improve a program by addressing vulnerabilities, bugs, or adding new features.
Personal Identifiable Information (PII)	Any information that can be used to identify a specific individual including full name, address, email address, phone number, date of birth, financial information, medical records, and biometric data.
Users	Council employees, Councillors, consultants, contractors, volunteers, and work placement students.
Vulnerability	A weakness, misconfiguration, or flaw that can be exploited by attackers to compromise the security and functionality of the system.

Title: Data Breach Response Policy		
Department: Corporate Services		
Version	**Date**	**Author**
0.1 - DRAFT	10 January 2024	IT Officer
0.2 – 16.18.01 - ADOPTED	15 February 2024 Resolution 015/24	
This policy may be amended or revoked at any time and must be reviewed at least three (3) years since its adoption (or latest amendment). The Director of Corporate Services will be responsible for the review of this policy. Review of this policy will incorporate relevant legislation, documentation released from relevant state agencies and best practice guideline. **Review Date: Three years from date of adoption**		
Amendments in the release		
Amendment History	**Date**	**Detail**
Annexure Attached:		
Noreen Vu **General Manager**		