

EME037	DATA BREACH		
POLICY OWNER:	Council		
DEPARTMENT:	Office of the CEO	**RESPONSIBLE OFFICER:**	Manager People, Culture & Systems
CREATION DATE:	24/09/2024	**REVIEW SCHEDULE:**	Annually
RELATED DOCUMENTS:	Acceptable & Secure use Policy – ICT Privacy Policy (not published) Disposal of Surplus IT and minor Assets Policy Data Breach Response Plan (not published) Server Access and data Security Policy (ICT) (not published)		
LEGISLATION:	Local Government Act 1995 State Records Act 2000		
DOCUMENT CONTROL			
DATE REVIEWED:	**REVIEWED BY:**	**CHANGES (IF ANY):**	**ENDORSED BY COUNCIL:**
24/09/24	Council	New Policy	OCM03/09/24

EME037 Data Breach

OBJECTIVES

This Data Breach Policy sets out the Shire of Carnarvon's (the Shire) policy for identifying, managing and preventing data breaches. Effective breach management, including notification where warranted, assists the Shire in avoiding or reducing possible harm to both the affected individuals/organisations and the Shire, and may prevent future breaches.

The purpose of this policy is to ensure alignment with the *Australian Privacy Act 1988* and *WA Privacy and Responsible Information Sharing legislation (PRIS)* (the Shire has drafted this policy in anticipation of the PRIS legalisation coming into effect).

SCOPE

This policy applies to all Employees, Contractors, Agents and third-party service providers of the Shire who gather, manage or have access to data, personal or sensitive information in the course of their duties or work for the Shire.

POLICY STATEMENT

1. Purpose

- Provides definitions and examples of data breach events
- Steps involved in responding to a data breach, and reviewing systems, policies and procedures to prevent future data breaches; and
- Roles and responsibilities for reporting, reviewing and managing data breaches



2. Identifying Data Breach Events

A data breach occurs when there is a failure that has caused or has the potential to cause unauthorised access to or unauthorised disclosure of any Shire data held.

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

Examples of data breaches include:

a. Human error
   - When a letter or email is sent to the wrong recipient;
   - 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; or
   - When an employee fails to implement appropriate password security measures, for example sharing password and log in information.

b. System failure
   - When a coding error allows access to the systems by an unauthorised user.

c. Malicious or criminal attack
   - Cyber incidents such as ransomware, malware, hacking, phishing or brute force access attempts resulting in access to or theft or personal information;
   - Social engineering or impersonation leading to inappropriate disclosure of personal information;
   - Shire employees using their valid credentials to access personal and/or sensitive information outside the scope of their duties or permissions; or
   - Theft of a physical asset such paper record, laptop, USB stick or mobile phone containing personal information.

3. Reporting a Data Breach

All Employees, Elected members, contractors and third-party agents are encouraged to report any concerns or incidents to their supervisor or Manager, they should report any suspected or confirmed data breaches immediately to the Data Breach Response Team.

4. Data Breach Response Team

Following a data breach the Shire will establish a Data Breach Response Team (DBRT) responsible for coordinating and executing the response plan. The team should include representatives from IT, Information Management, Communications, and any other relevant departments.



5. Responding to a Data Breach

The Shire will implement all necessary procedures according to its *Data Breach Response Plan*, including the following key steps in response to a data breach:

- Contain the breach
- Evaluate the associated risks
- Consider notifying affected individuals (where applicable)
- Take steps to prevent repeat actions

6. Investigation and Assessment

The DBRT will promptly investigate and assess the nature and extent of the data breach in accordance with the Shire's Data Breach Response Plan, the team will assess the circumstance of the data breach to determine the risk of harm to individuals and any potential legal obligations.

7. Notification Requirements

The DBRT will comply with the requirements of the Privacy Act and other applicable laws regarding the notification of affected individuals and relevant authorities and notify any affected individuals and authorities as soon as practicable after identifying a data breach.

8. Roles and Responsibilities

All employees, elected members, contractors and third-party agents are responsible for understanding and adhering to this policy.

9. Review and Update

This Data Breach Policy is designed to create a framework for preventing, managing, and learning from data breaches within the Shire. It should be reviewed regularly and employees, elected members and contractors updated with the necessary training to reflect changes in technology, regulations, and organisational processes.

This policy is to be read in conjunction with the related documents.