COUNCIL POLICY

Data Breach Response Policy & Procedure

Policy No: 3.10

Policy Subject: Data Breach Response Policy & Procedure

Objectives:
The Privacy Amendment (Notifiable Data Breaches) Act 2017 established a Notifiable Data Breaches scheme in Australia which requires organisations covered by the *Australian Privacy Act 1988* (the Act) to notify any individuals likely to be at risk of serious harm by a data breach.

As required by the Act, this Data Breach Response Policy and Procedure outlines definitions, sets out the procedure and clear lines of authority for the Shire of Katanning staff in the event that the Shire of Katanning experiences a data breach, or suspects that a data breach has occurred.

Scope:
A data breach occurs when personal information is lost or subjected to unauthorised access, modification, use or disclosure or other misuse. Personal information is information or an opinion about an identified or reasonably identifiable individual.

Not all data breaches require notification. The Notifiable Data Breaches (NDB) scheme only requires organisations to notify when there is a data breach that is likely to result in serious harm to any individual to whom the information relates.

The procedure attached to this policy facilitates the assessment of the breach and what action is required.

Policy Statement:
The Shire of Katanning is committed to protecting the privacy of personal information it records, in accordance with the *Australian Privacy Act 1988*.

Legislative and Strategic Context:
The following Federal legislation provides a broad framework within which this policy operates:

- *Australian Privacy Act 1988*
- *Privacy Amendment (Notifiable Data Breaches) Act 2017*

Review Position and Date
This policy and procedure must be reviewed every two years.

Associated Documents

Documents & resources that have a bearing on this policy and that may be useful reference material for users of this policy, can be sourced from the www.oaic.gov.au website and via the following link;

- Preventing data breaches: advice from the Australian Cyber Security Centre

Definitions

Key terms and acronyms used in the policy, and their definitions:

- **Data Breach** – data is released in error. For example, a spreadsheet of names and addresses.

Procedures

A: Data Breach Response Team

The following roles make up the Data Breach Response Team

- Executive Manager of Corporate Services
- Managed services (IT) provider
- Coordinator Administration
- CEO PA (minute taker)

B: Data Breach Response Procedure

If any Shire of Katanning staff member suspects or becomes aware of a data breach, this procedure is activated.

Step 1: Contain Data Breach and complete preliminary ASSESSMENT

The first step is to contain the data beach and complete the preliminary assessment;

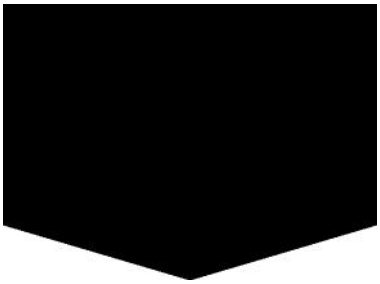
STEP 1

☐	The Executive Manager of Corporate Services is notified immediately when a suspected data breach is identified.
☐	The Managed Services (IT) provider is advised of the suspected data breach and takes responsibility for the successful containment of the data breach.
☐	The Managed Services (IT) provider provides updates as requested
☐	Executive Manager of Corporate Services takes responsibility for preliminary assessment process and ensures information is clearly documented and evidence is preserved, including. • the date, time, duration and location of the breach • the type of personal information involved in the breach • how the breach was discovered and by whom • the cause and extent of the breach • a list of the affected individuals, or possible affected individuals • the risk of serious harm to the affected individuals
☐	Executive Manager of Corporate Services convenes a meeting of the Data Breach Response Team (regardless of outcome of

Step 2: EVALUATION of a suspected Data Breach

Evaluate the suspected data breach based on the information and evidence available;

☐	Executive Manager of Corporate Services presents the results of the preliminary assessment to the Data Breach Response Team at meeting that is minuted.
☐	Data Breach Response Team reviews the information and evidence presented. In principle, if the... • data breach is confirmed to have taken place and • there is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that the Shire of Katanning holds • this is likely to result in serious harm to one or more individuals, and • the Shire of Katanning hasn't been able to prevent the likely risk of serious harm with remedial action ...then the Data Breach is confirmed and Steps 3 & 4 of this procedure should be completed. *Further information on determining data breaches is available on the Office of the Australian Information Commissioner website* *https://www.oaic.gov.au/privacy/notifiable-data-breaches/when-to-report-a-data-breach/*
☐	Data Breach Response Team assesses risks and priorities
☐	Keep appropriate records of the suspected breach and actions of the Response Team, including the steps taken to rectify the situation and the decisions made.



Step 3: NOTIFICATION of a confirmed Data Breach

Notify affected individuals and government agencies.

☐	Confirm the notification list; • Individuals affected • Shire of Katanning stakeholders (Executive Management Team, Elected Members) • Office of the Australian Information Commissioner • Shire of Katanning Insurers • WALGA • WA Police • *Other organisations as required*
☐	Draft and agree the notification messages
☐	Send the notification messages through most appropriate medium (letter, email etc.).

STEP 3

Consider breach notifications

Step 4: Lessons Learnt / Future Data Breach Prevention. The last step is to prevent further data breaches.

☐	Fully investigate the cause of the breach.
☐	Take action to ensure further data breaches do not occur • update security and response plan if necessary • make appropriate changes to policies and procedures if necessary • revise staff training practices if necessary • consider the option of an audit to ensure necessary outcomes are effected
☐	Report outcomes and recommendations: • Shire of Katanning stakeholders (ICT Steering Committee, Executive Management Team, Elected Members)

STEP 4

Review the incident and take action to prevent future breaches

C: Record keeping

Records should be maintained throughout the Data Breach Response process including responses from individuals and organisations that were notified.

Resolution No: OC12/26
Resolution Date: 24 February 2026
Amended:
Review Frequency Biennially
Responsible Officer Executive Manager Corporate Services