

Governance

Cyber Security and Data Breach Response

Objective

To enforce the protection of the Shire of Koorda's ("the Shire's") Information Communication Technology and information assets from information security threats through the implementation of targeted security controls and best practice standards.

To outline the mandatory requirements to respond to a data breach at the Shire and to mitigate future breaches.

Policy

Definitions

TERM	DEFINITION
Data Breach	A data breach happens when personal information is accessed, disclosed without authorisation, or is lost. For example, when: <ul style="list-style-type: none">• a USB or mobile phone that holds a individual's personal information is stolen• a database containing personal information is hacked• someone's personal information is sent to the wrong person.
ICT Resources	Electronic data exchange, via internal and external data networks, internet access, E-mail and any other electronic data transfer using Shire equipment and services.
Intangible ICT Asset	The Shire's intellectual property, typically data which is owned or held by the Shire and may have a value to others.
Personal Information	Personal information includes a broad range of information, or an opinion, that could identify an individual. What is personal information will vary, depending on whether a person can be identified or is reasonably identifiable in the circumstances.

Cyber Security

In order to protect ICT and information assets from attack by unauthorised parties ensuring that the confidentiality, integrity and availability of the Shire's information, the following policy has been adopted. The Shire will:

- Implement access controls over all systems and networks to prevent unauthorised access to Shire's ICT and information assets;
- Undertake regular information security audits and testing in order to prevent and allow remediation of
 - The potential for illegal access by unauthorised parties;
 - Loss or compromise of Shire owned ICT and information assets;
 - Potential disruption of the Shire's business activities;
- Proactively maintain systems in a secure state in response to evolving threats to the organisation;
- Monitor and report on suspected and attempted breaches and remedies applied;
- Source insurance cover to protect against any threats;

- Develop and Maintain Management Practices as required to provide direction to Council and the Shire's officers regarding the implementation of this policy in the workplace.

Data Breach

In alignment with State Government reforms regarding personal privacy protections and the accountability of information sharing, this policy seeks to formalise the Shire's commitment to the secure handling of personal information it collects and provide clear direction as to the actions that will be taken in the unlikely event of a data breach occurring.

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 Shire staff in the event that the Shire experiences a data breach, or suspects that a data breach has occurred.

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.

Data Breach Response (DBR) Team

The following roles make up the Data Breach Response Team:

- Chief Executive Officer
- Deputy Chief Executive Officer
- Payroll/Governance Officer
- IT Consultants (as required)

Data Breach Procedure

If any Shire staff member suspects or becomes aware of a data breach, this procedure activated and should be followed.

• Step 1: Contain Data Breach and complete preliminary ASSESSMENT

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

- The DBR Team is notified immediately of a suspected data breach when known and the reporting person provides updates as requested.
- DBR Team takes responsibility for the successful containment of the data breach by the IT Consultants.
- DBR Team takes responsibility for preliminary assessment process and ensures information is clearly documented and evidence is preserved:
 - 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 affected individuals, or possible affected individuals,
 - the risk of serious harm to the affected individuals, and
 - other risks to the Shire.
- A DBR Team meeting is convened (regardless of outcome of preliminary assessment).

- **Step 2: EVALUATION of a suspected Data Breach**

The second step is to evaluate the suspected data breach based on the information and evidence available;

- Results of the preliminary assessment are reported to the DBR Team at the meeting that is minuted.
- DBR Team review the information and evidence presented. In principle, if the;
 - data breach is confirmed to have taken place,
 - there is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that the Shire holds,
 - this is likely to result in serious harm to one or more individuals, and
 - the Shire 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](#).

- DBR Team assesses risks and priorities,
- keep appropriate records of the suspected breach and actions of the DBR Team, including steps taken to rectify the situation and the decisions made.

- **Step 3: NOTIFICATION of a confirmed Data Breach**

The third step is the notification of affected individuals and government agencies;

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

- **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 affected.
- Report outcomes and recommendations to Shire of Koorda stakeholders (IT Consultants, Executive Management Team, Elected Members)

- **Record Keeping**

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

Related Documents (Legislation/Local Law/Policy/Procedure/Delegation)

ISO 27001 Specification for Information Security Management Systems

Privacy Act 1998

Office of Digital Government Security Policy

ACSC Essential Eight

Australian Privacy Act 1988

Privacy Amendment (Notifiable Data Breaches) Act 2017

Commercial Crime and Cyber Protection Insurance Policy

[Preventing data breaches: advice from the Australian Cyber Security Centre](#)

Review History

Date	Council Resolution	Description of review/amendment
24/03/2025	RES: 040325	V1.0 Adoption of Policy. Introduced new policy as part of Audit Recommendations and as required as part of introduction of the Privacy and Responsible Information Sharing Bill 2024 (PRIS).

