

PURPOSE

This Policy outlines the Shire of Manjimup's approach to identifying, managing, and responding to information breaches.

The Shire is committed to protecting information it holds and maintaining the privacy of individuals. This Policy supports transparency, accountability, and responsible information handling, and aligns with applicable privacy, information sharing, and records management obligations.

SCOPE

This Policy applies to:

- All Shire employees, contractors, and elected members
- All information held by the Shire, including:
 - Personal information
 - Confidential and sensitive information
 - Corporate and operational information
 - Physical and digital records

DEFINITIONS

Information Breach: An information breach occurs when information is:

- Accessed without authorisation
- Disclosed without authorisation
- Lost or unavailable

Examples include:

- Sending information to the wrong recipient
- Loss or theft of devices or documents
- Cybersecurity incidents (e.g. phishing, malware)
- Unauthorised internal access or misuse
- System misconfiguration exposing data

Each breach is assessed on a case-by-case basis.

POLICY MEASURES

1. Policy Principles

The Shire will:

- Respond promptly to suspected or actual information breaches
- Take reasonable steps to contain and minimise harm
- Assess risks and impacts thoroughly
- Meet applicable legal, regulatory, and contractual obligations
- Maintain clear records of breaches and responses
- Continuously improve breach management practices

2. Preparedness

2.1 Integration with Existing Frameworks

Information breach management is aligned with:

- Information Classification Policy
- Information Management Policy
- Privacy Policy
- Acceptable Usage Policy
- Essential Eight Cybersecurity Framework
- Business Continuity and Disaster Recovery Plans

2.2 Training and Awareness

The Shire will:

- Provide regular training on privacy, cybersecurity, and information handling where relevant
- Promote awareness of emerging threats and breach risks
- Ensure staff understand how to identify and report breaches

2.3 Identification and Reporting

Suspected breaches may be identified through:

- Staff observation and reporting
- System alerts and monitoring tools
- Audits and reviews
- External notifications (e.g. suppliers or the public)

All staff must immediately report suspected breaches through designated internal channels.

2.4 External Providers and Partners

The Shire will:

- Include breach management obligations in contracts
- Monitor compliance of service providers
- Coordinate responses where third parties are involved

2.5 Policy Review

This Policy will be reviewed:

- At least annually
- Following significant breaches
- When legislative or operational changes occur

3. Containment, Assessment and Mitigation

3.1 Response Approach

The Shire will take the following high-level steps:

1. Identify
 - Confirm suspected breach and gather initial details
2. Contain
 - Limit further access, disclosure, or loss
 - Secure systems, retrieve information where possible
3. Assess
 - Determine:
 - Type and sensitivity of information
 - Number of individuals affected
 - Likelihood and severity of harm
 - Cause and scope of the breach
4. Mitigate
 - Reduce potential harm to individuals and the organisation
 - Provide support where appropriate
5. Review
 - Analyse root cause
 - Identify improvements

3.2 Third-Party Breaches

Where breaches involve external providers or partner agencies:

- Responsibilities will be clarified
- Coordination will occur to assess and manage the breach
- Contractual obligations will guide actions

4. Meeting Obligations

The Shire will comply with all applicable legal and regulatory requirements when managing information breaches.

This may include notification or engagement with relevant authorities or stakeholders, such as:

- Law enforcement agencies
- Regulatory or oversight bodies
- Cybersecurity authorities
- Affected individuals where appropriate

Decisions regarding notification will be based on:

- Risk of harm
- Legal obligations
- Public interest considerations

Detailed procedures are outlined in the Information Breach Response Plan.

5. Roles and Responsibilities

5.1 Chief Executive Officer (CEO)

- Overall accountability for breach management
- Ensures appropriate governance and resources

5.2 Executive and Management

- Ensure implementation of this Policy
- Support breach response and decision-making

5.3 Information Custodians / System Owners

- Assist in breach assessment and containment
- Ensure controls are maintained

5.4 All Staff and Contractors

- Protect information in their care
- Immediately report suspected breaches
- Comply with policies and procedures

5.5 Capability and Resourcing

The Shire will ensure access to:

- Skilled internal personnel
- External specialists (e.g. cybersecurity experts) where required
- Appropriate tools and systems to detect and respond to breaches

6. Record Keeping

The Shire will maintain records of:

- Suspected and confirmed breaches
- Actions taken
- Decisions made
- Notifications issued

This may include maintaining an Information Breach Register to:

- Track incidents
- Identify trends
- Support continuous improvement

All records will be managed in accordance with applicable recordkeeping obligations.

7. Review and Continuous Improvement

The Shire will:

- Conduct post-incident reviews
- Identify systemic issues or control weaknesses
- Update policies, procedures, and training accordingly

This ensures ongoing improvement in information protection and breach response capability.

8. Related Documents

- Information Classification Policy
- Information Management Policy
- Privacy Policy

- Information Breach Response Plan (internal)
- Information Breach Register (internal)

Document Control						
Document Responsibilities:						
Officer:	Director Business		Officer Business Unit:	Administration and Finance		
Reviewer:	Director Business		Decision Maker:	Council		
Document Management:						
Review Frequency:	Annual		Next Due:	June 2027	Records Ref:	D26/11781
Version #	Decision Reference:		Comment:			
1.	24 June 2026 / 29933		Introduction of new policy for PRIS Act			