CP.64 ICT Cybersecurity Incident Management

Responsible Department	Corporate Services
Resolution Number	C.5153
Resolution Date	16/10/2024
Next Scheduled Review	2026/27
Related Shire Documents	Council Policy CP.63 Remote Access Management Working from Home Agreement Council Policy CP.65 ICT Security Access Council Policy CP.56 Records Management Business Continuity Plan Data Breach Register Risk Register
Related Legislation	*OAG Information Systems Audit Local Government 2021/22* *Privacy Response and Information Sharing (PRIS)* *Data Protection Act*

OBJECTIVE

The purpose of this Policy is to:

1. Provide a structured and effective approach to managing and responding to a cybersecurity incident with the Shire's security and business objectives;
2. Aims to ensure timely identification, containment, resolution and recovery from incidents to minimise their impact;
3. Set up cyber security response team and responsibilities to manage response to a cyber security incident; and
4. Guide the internal and external communication process when responding to a cybersecurity incident.

SCOPE

This policy covers the management of cybersecurity for the Shire's information. This includes the technology infrastructure, applications, systems, people and services that store, process and access, the Shire's data and information. Information management and security is the responsibility of everyone in or associated with the Shire. This policy applies to all staff, Council members, volunteers, contractors and consultants working for the Shire, using the Shire's resources or accessing the Shire's technology environment or information. It covers all types of cybersecurity incidents, including but

not limited to malware infections, unauthorised access, data breaches, and denial-of-service attacks.

POLICY

A data breach is when personal information is lost or subjected to unauthorised access, modification, use or misuse. A data breach can be because of a cybersecurity attack. In case of any incident, individuals are required to report the incident to their Manager and ICT department.

1. Set up Cyber Security Response Team

The following roles comprise the Cybersecurity Response Team:

- ICT Business Solutions Coordinator
- Executive Manager Corporate Services
- ICT Contractors
- Shire ICT Team

2. Incident Identification

a. **Detection:** Encouraging users reports potential incidents, utilising threat intelligence and security monitoring tool.
b. **Classification:** Categorising incidents based on severity and impact.

3. Incident Reporting

Report suspected or confirmed incidents immediately to the Cybersecurity Response Team through designated communication channels. Where possible include details such as the nature of the incident, affected systems or data.

4. Incident Response

- The Response Team will access, contain and mitigate the effects of the incident.
- Conduct a detailed investigation to determine the root cause and its impact.
- Implement measures to resolve the incident and restore operations.

5. Communication

- ICT Business Solutions Coordinator will provide timely updates to relevant internal stakeholders regarding the incident's status and resolution progress.
- Manage communications with external parties and regulatory bodies

Type	Organisation to Notify
Ransomware	Australian Signals Directorates Australian Cyber Security Centre
Data breach	Office of the Australian Information Commissioner
Insurance	Insurance provider (LGIS)

6. Documentation

Maintain a comprehensive log of all incidents.

The incident is documented in an incident register maintained by ICT department. Following information to be noted:

- Date, time, location of the breach incident.
- How and by whom was the breach discovered.
- The cause and extent of the incident.
- Individuals affected by the incident.
- Risks to the Shire and other relevant parties.

7. Roles and Responsibilities

Employees: Report suspected incidents promptly to the Cybersecurity Response Team.

ICT Business Solutions Coordinator: Oversee the Cybersecurity Incident Management and ensure implementation of cybersecurity measures and compliances.

Cybersecurity Response Team: Manage the incident response process, including detection, assessment, containment, suppression, recovery and documentation.

8. Learn and Improve

- After the organisation has recovered its systems, services or network from cyber incident, report outcomes and recommendations to be given to the Executive Management Team (EMT).
- Take necessary actions to ensure further breaches do not occur.
- Update security and response plan if required.
- Make necessary changes to policies and procedures where necessary.
- Revise training as required.