SHIRE OF COOROW

ALWAYS IN SEASON

AGENDA

FOR THE

AUDIT AND RISK COMMITTEE MEETING

TO BE HELD ON

WEDNESDAY 16 APRIL 2025

PLEASE READ THE FOLLOWING DISCLAIMER BEFORE PROCEEDING

Members of the public are cautioned against taking any action on Council decisions, on items in this Agenda in which they may have an interest, until such times as they have been advised in writing by Shire staff

NOTICE OF MEETING

PLEASE BE ADVISED THAT THE

AUDIT AND RISK COMMITTEE MEETING

COMMENCING AT 4:00 PM

WILL BE HELD ON

WEDNESDAY, 16 APRIL 2025

COOROW COUNCIL CHAMBERS

Mia Maxfield

Chief Executive Officer

DISCLAIMER

The advice and information contained herein is given by and to the Council without liability or responsibility for its accuracy. Before placing any reliance on this advice or information. A written inquiry should be made to the Council giving reasons for seeking the advice or information and how it is proposed to be used.

Agenda

1 DECLARATION OF OPENING/ANNOUNCEMENT OF VISITORS

1.1 SALUTATIONS AND OPENING OF MEETING

The Chairperson, Cr Guy SimsChair B A Jack, welcomed those present and opened the Meeting at Type time.

1.2 ACKNOWLEDGEMENT OF COUNTRY

The Shire of Coorow acknowledges the traditional owners of this land – the Yued people, and their continuing connection to land, water and community. We pay our respects to them and their cultures, and to elders both past, present and emerging.

1.3 VISITORS

2 RECORD OF ATTENDANCE/APOLOGIES/LEAVE OF ABSENCE

2.1 ATTENDANCE

Deputy President B A Jack

Councillor V J Muller

Councillor G Stangle

2.2 ATTENDANCE VIA TELEPHONE/INSTANTANEOUS COMMUNICATION

In accordance with regulation 14C (2) of the *Local Government (Administration) Regulations 1996* the Shire President or Council can approve the attendance of a person, not physically present at a meeting of Council or committee, by electronic means. The member must ensure they are in an appropriate location, being private and free from distractions. When a meeting is closed to the public (Behind Closed Doors) in accordance with Section 5.23 of the Local Government Act 1995 (the Act), members must ensure that the deliberations cannot be observed or overheard by any other person. Attendance of meetings by electronic means is capped at 50% as *per Local Government (Administration) Regulation* 14C(3).

2.3 LEAVE OF ABSENCE PREVIOUSLY APPROVED

Nil

2.4 APOLOGIES

Nil

3 DISCLOSURE OF INTERESTS

Section 5.65 and 5.70 of the Local Government Act 1995 requires an Elected Member or officer who has an interest in any matter to be discussed at a Committee/Council Meeting that will be attended by the Elected Member or officer must disclose the nature of the interest in a written notice given to the Chief Executive Officer before the meeting; or at the meeting before the matter is discussed. An Elected Member who makes a disclosure under section 5.65 or 5.70 must not preside at the part of the meeting relating to the matter; or participate in; or be present during, any discussion or decision making procedure relating to the matter, unless allowed by the Committee/Council. If Committee/Council allow an Elected Member to speak, the extent of the interest must also be stated.

4 PUBLIC QUESTION TIME

5 CONFIRMATION OF PREVIOUS MINUTES

Audit and Risk Committee Meeting - 16 October 2024

Audit and Risk Committee Meeting - 18 December 2024

Audit and Risk Committee Meeting - 19 March 2025

6 REPORTS

6.1 DEPUTY CHIEF EXECUTIVE OFFICER

6.1.1 ICT GOVERNANCE POLICIES

Reporting Officer:	**S Curulli, Deputy Chief Executive Officer**
Responsible Executive:	**S Curulli, Deputy Chief Executive Officer**
File Reference:	**ADM0138**
Disclosure of Interest:	**Nil**
Voting Requirement:	**Simple Majority**

COUNCIL'S ROLE:

Legislative: Includes adopting local laws, local planning schemes and policies.

REPORT PURPOSE

For the Audit and Risk Committee to endorse and recommend to Council the adoption of two new ICT Governance policies, being the Backup and Restore Policy and the Business Continuity and Disaster Recovery Plan.

BACKGROUND

Under section 2.7 of the Local Government Act 1995, Council has adopted several policies to govern the local government's affairs. It is good practice to continually review the existing policies in view of changing legislation and requirements.

A comprehensive policy review was presented at the September 2023 Ordinary Council Meeting, during which Council rescinded various policies and adopted a new Policy Manual containing several updated policies to guide the Shire's governance.

In December 2024, Council resolved to adopt and replace the following policies:

- ADM-0006 Acceptable Use Policy
- ADM-0007 Cyber Security Policy
- ADM-0008 ICT Change Management Policy
- GOV-014 IT Risk Management Policy.

The inclusion of the draft Backup and Restore Policy and the Business Continuity and Disaster Recovery Plan will satisfy the ICT Governance requirements for the Shire of Coorow, as raised in last year's annual audit. Further, the inclusion of these two policies will strengthen the Shire's level of control and best practice in Governance, aligning with the Shire's Strategic Priorities and Outcomes.

COMMENT

In 2024, Council began the process of strengthening its ICT Governance procedures, with a full review of all related policies and procedures. At its Ordinary Meeting of Council on 18 December 2024, Council endorsed the adoption and replacement of four ICT Governance policies to satisfy audit recommendations and to strengthen the level of control and practices regarding ICT Governance. This report seeks the Audit and Risk Committee's endorsement and recommendation for Council to adopt two new policies as below:

Document	Purpose
ADM-009- Backup and Restore Policy	The Backup and Restore Policy aims to ensure the protection, preservation, and availability of critical Shire data through regular backups and timely restoration processes. This policy establishes the framework for creating, managing, and restoring data backups to minimise the risk of data loss or corruption resulting from hardware failure, human error, malicious attacks, or other incidents compromising data integrity. While closely tied to a disaster recovery policy, a backup policy addresses more common scenarios and is likely to be used more frequently. This is a new policy.
Shire of Coorow Business Continuity and Disaster Recovery Plan	The Business Continuity and Disaster Recovery Plan aims to ensure that the Shire of Coorow can maintain its service delivery at an acceptable level during or after a disruptive event or disaster. Various incidents, such as floods, fires, cyclones, vandalism, and cyber-attacks, can significantly impact the Shire's operations. This plan addresses these threats to mitigate their impact on operational activities. This plan aims to ensure the restoration and continuity of essential IT systems during a disaster. This will be achieved by creating and maintaining a comprehensive Disaster Recovery Plan (DRP) to guide and manage the disaster recovery process. The DRP must enable the Shire to ensure preparedness before an event by: • Quickly and efficiently define, prioritise, and re-establish critical business functions.

	• Implement a systematic plan for managing any incident or disaster. • Outline immediate responses to minimise damage or loss during a critical incident. • Minimising the impact of an incident on the community, staff, and Council. This plan will be reviewed and updated every year, or whenever major business changes, to strengthen our resilience against possible damage to the business during a disaster or outage.

STAKEHOLDER ENGAGEMENT

Council

Shire of Coorow Executive Staff

External Consultant- Cohesis Pty Ltd

STATUTORY ENVIRONMENT

Local Government Act 1995

Role of council

(1) The council —

(a) governs the local government's affairs; and

(b) is responsible for the performance of the local government's functions.

(2) Without limiting subsection

(1), the council is to —

(a) oversee the allocation of the local government's finances and resources; and

(b) determine the local government's policies.

STRATEGIC IMPLICATIONS

STRATEGIC PRIORITIES	Outcome	Strategy
Civic Leadership Leadership that provides strategic direction for the community, supported by efficient and effective service delivery.	4.3 Skilled and well supported team Effective Governance and Leadership	• External audits and reviews confirm compliance • Council is supported by a skilled team • Ensure governance policies and procedures are in

Governance and an effective organisation		accordance with legislative requirements • Strengthen the governance role of Councillors by informing, resourcing, skilling and supporting their role

POLICY IMPLICATIONS

Update Policy Manual as listed:

- ADM-009- Backup and Restore Policy
- Shire of Coorow Business Continuity and Disaster Recovery Plan

FINANCIAL IMPLICATIONS

Nil.

RISK IMPLICATIONS

RISK	LIKELIHOOD	CONSEQUENCE	RISK ANALYSIS	MITIGATION
Governance: By adopting these policies, the Shire will become compliant with these provisions of the *Local Government Act 1995*.	Possible	Moderate	Low	Adopting the proposed amendments to this policy is low risk as it aligns with the *Local Government Act 1995* and the objectives of the policy.

ATTACHMENTS

1. **DRAFT Backup and Restore Policy- ADM-009** ⇩
2. **DRAFT Business Continuity and Disaster Recovery Plan** ⇩

OFFICER RECOMMENDATION

That the Audit and Risk Committee endorse and recommend to Council the adoption of the proposed Backup and Restore Policy, and the Shire of Coorow Business Continuity and Disaster Recovery Plan.

BACKUP AND RESTORE POLICY GOV-013

Responsible Department	Office of the CEO
Policy Owner	Chief Executive Officer
Resolution Number	
Resolution Date	
Old Policy Number	New
Register of Delegations	CEO
Relevant Legislation	State Records Act 2000
Link to Strategic Plan	N/A
Guidelines	N/A
Next Review	April 2026

Objective

This policy ensures the protection, preservation, and availability of critical Shire data through regular backups and timely restoration processes. This policy establishes the framework for creating, managing, and restoring data backups to minimise the risk of data loss or corruption resulting from hardware failure, human error, malicious attacks, or other incidents compromising data integrity.

While closely tied to a disaster recovery policy, a backup policy addresses more common scenarios and is likely to be used more frequently.

Scope

Shire's operations rely on the availability and integrity of its data. This policy provides the necessary rules and guidance for how the Shire can recover its data in the event of data loss, corruption, or a security breach. This policy, in conjunction with the Shire's Disaster Recovery Plan, is integral to safeguarding the Shire's data by:

a. Establishing a standardised framework for the backup process.
b. Ensuring all critical data assets are backed up regularly and securely.
c. Defining retention periods for backup data to comply with legal, regulatory, and operational requirements.
d. Facilitating timely data recovery to minimise disruptions in Shire's business operations.
e. Aligning with the Shire's legal obligations under the State Records Act 2000.

The consequence of data loss can be severe for the Shire as this could disrupt business operations.

This policy applies to all staff, contractors and vendor for the Shire of Coorow.

Policy

1. Key Terms

In this document, the terms “we”, “us”, “our”, and “the organisation” refer to The Shire of Coorow.

2. Roles and Responsibilities

Role	Responsibility	Details
Executive Management	Support policy implementation.	I. Align the backup policy with the Shire’s risk management and business continuity goals. II. Ensure that sufficient budget, personnel, and technology are allocated to implement the backup policy successfully. III. Coordinate with IT Support and Cloud Service Provider in the event of a data loss. IV. Enforce compliance with the backup policy across the Shire. V. Define and ensure adherence to Recovery Time Objectives (RTO) and Recovery Point objectives (RPO). VI. Oversee the periodic testing and review of the backup processes to confirm their effectiveness.
IT Support Provider	Implementing and managing backup processes for on-premises systems and records.	I. Assist the Shire with diagnosing and resolving data loss issues. II. Monitor backup systems to ensure they are functioning correctly. III. Manage and execute data restoration processes when needed. IV. Develop and maintain backup schedules that align with the Shire’s requirements and data retention policies.

Role	Responsibility	Details
		V. Implement and manage security measures to protect backup data from unauthorised access or breaches. VI. Develop and maintain documentation for all backup procedures, configuration, and schedule. VII. Record any changes to the backup process, including software, hardware or policy updates. VIII. Support Shire staff with backup-related issues.
Cloud Service Provider	Implementing and managing backup processes for cloud systems and records.	I. Enable automated and scheduled backup processes. II. Ensure data can be restored within the specified Recovery Time Objective (RTO) and Recovery Point Objective (RPO).
Shire Staff	Comply with the policies and procedures.	I. Ensure that all Shire-related documents are saved only on approved documents management software's within the Shire (Synergy, ECM, Altus). II. Store customer information directly on the Shire's systems/applications. III. Report any suspected data loss issues to the manager /supervisor.

3. Exceptions

Nil.

4. Policy Statement

This policy outlines a process for consistent data backup and preserving backup copies, ensuring the protection of critical information against loss from accidental deletion, corruption, system failures, or disasters.

5. Policy Requirements

5.1 Data Classification

Classification	Impact	Description	Examples
Confidential	High	Information whose unauthorised disclosure could reasonably be expected to cause damage to a person or the Shire's security.	• Social Security numbers. • Date of Birth. • Driver's License Numbers. • Home Address and Phone Numbers.
Internal	Medium	Data that is only intended for use within the Shire.	• Employee handbooks and policies. • Internal memos and communications. • Shire's intranet.
Public	Low	Freely available data that does not require special security measures can be openly shared with anyone without additional precautions.	• Community Announcements. • Government projects. • Community rules and regulations. • Shire Staff Members and Departments.

5.2 Backup Schedule and Frequency

The Shire of Coorow will conform t the following backup regimes:

Application	Business Process	On-Premise / SaaS	Retention Period	Backup Frequency
SynergySoft	Business Services	On-Prem	As per Shire and legislative requirements.	As per Shire's requirement.
Altus	Payroll / Timesheet / Finance	On-Prem	As per Shire and legislative requirements.	As per Shire's requirement.
MS 365	Outlook / MS application suite	SaaS	As per Shire and legislative requirements.	As per Shire's requirement.

Application	Business Process	On-Premise / SaaS	Retention Period	Backup Frequency
Workflows (Sirsi Dynix)	Library Management		As per Shire and legislative requirements.	As per Shire's requirement.
InfoCouncil 8.63	Council Agenda Management		As per Shire and legislative requirements.	As per Shire's requirement.
Code Two Signatures for Signatures	Email Signature Management		As per Shire and legislative requirements.	As per Shire's requirement.
Metro Count v5.06	Traffic Data Collection & Analytics		As per Shire and legislative requirements.	As per Shire's requirement.
SAP Crystal Reports 2020 SP4	Reporting		As per Shire and legislative requirements.	As per Shire's requirement.
TechSmith Camtasia 2024	Video Creation and Editing		As per Shire and legislative requirements.	As per Shire's requirement.
Universe 11.3.2	Database Management		As per Shire and legislative requirements.	As per Shire's requirement.

5.3 Backup Storage Locations

Backups are stored in one of four places. Each location is required to comply with the following requirements:

ID	Location	Responsible Party	Requirements	Device
1	On-Premise	IT Support Provider	I. Ensure effective execution and safekeeping of backups. II. Full on-prem failover with hourly backups during the work week.	Datto Backup Appliance

ID	Location	Responsible Party	Requirements	Device
			III. Transition on-prem backups to cloud storage weekly for offsite resilience. IV. Daily boot sequence tests with screenshots for verification, reviewed the following day.	
2	3rd Party DataCentre	IT Support Provider	I. Weekly replication of final backup to a secure, offsite location. II. Ensure a rolling twelve-month cloud data recovery window.	Cloud infrastructure
3	Non-M365 Saas / Cloud Vendors	Vendor	I. CPC relies on the internal controls of 3rd Party SaaS vendors to ensure an appropriate backup regime is in place.	Managed by SaaS providers
4	Microsoft 365	IT Support Provider	Ensure hourly backups of CPC's: • Outlook mailboxes • Shared accounts, • SharePoint Sites & • MS Teams conversations; and • OneDrive accounts.	

Backup Storage – minimum acceptable criteria – In all cases, the Shire of Coorow requires that its backups be stored.

1. Only authorised personnel have access to a secure, access-controlled area.
2. With appropriate environmental controls and fire suppression systems to prevent backup data from hazards like fire and flooding.
3. Within facilities with comprehensive security measures such as surveillance systems to safeguard backup data from unauthorised access, tampering and theft.

4. In Australia.
5. In an encrypted state.

5.4 Backup Recovery

The Shire must establish backup and restore routines. Data restoration is usually carried out by an ICT support provider, who will restore files from data specified by the user or from the nearest backed-up date.

1. Staff must request data restoration by creating a data restoration ticket via the IT Support portal.
2. Staff must provide the complete details of the data restoration via the electronic form provided in the IT Support portal.
3. The ticket will be raised and queued as a service ticket on the customer portal.
4. ICT support will perform the restoration of data.
5. ICT support will inform the resolution of the request via ticket closure.

5.5 Backup Schedule and Frequency

The Shire must follow data backup schedule and frequency regime:

Application	Owner	On-Premise / SaaS	Backup Schedule	Backup Frequency
SynergySoft	TBD	On-Prem	Daily (Incremental) Weekend (Full Backup)	As per CPC requirement
Altus	TBD	On-Prem	Daily (Incremental) Weekend (Full Backup)	As per CPC requirement
MS 365	TBD	SaaS		As per Vendor
Info-Cycle	TBD	SaaS		As per Vendor
Adobe	TBD	On-Prem	Daily (Incremental) Weekend (Full Backup)	As per Shire's requirement

Application	Owner	On-Premise / SaaS	Backup Schedule	Backup Frequency
Yemenite	TBD	On-Prem	Daily (Incremental) Weekend (Full Backup	As per Shire's requirement
Elude	TBD	On-Prem	Daily (Incremental) Weekend (Full Backup	As per Shire's requirement

5.6 Backup Retention

The Shire of Coorow requires backups to be retained as follows:

a) Daily Backups: Retained for 30 days.

b) Weekly Backups: Retained for 3 months.

c) Monthly Backups: Retained for 1 year.

d) Annual Backups: Retained for 7 years or as required by regulatory compliance.

Backup data/media that is no longer needed must be marked and recorded for secure disposal, taking due environmental consideration and regulation into account.

5.7 Testing of backup copies

The Shire of Coorow requires that all backups are:

1. Automatically tested for consistency and recoverability.
    a. Shire of Coorow must be notified of backup failures that may materially impact BCDR capabilities.
2. Able to be recovered and restored within 60 minutes.
3. The backup testing process and results will be subject to internal and external audits as required.

6. Review and Revision

This policy will be reviewed regularly to ensure its effectiveness and relevance. Amendments may be made as necessary to address changing circumstances or technology.

7. Acknowledgement

Staff will complete an acknowledgement form.
I confirm that I have read, understood and agree to adhere to this policy:

Full name .....

Position .....

Signature .....

Date .....

8. Definitions

Term	Meaning
Backup	The process of creating a copy of data at a specific point in time to protect against data loss or corruption.
Restore	The process of retrieving and returning backed-up data to its original or a new location after data loss occurs.
Data Loss	Data loss refers to the unintended or accidental deletion, corruption, or unavailability of data. It can occur due to various factors, such as hardware and software failure, cyberattacks, human error, or natural disasters.
Retention Period	The duration for which backup copies are kept before they are deleted or overwritten is based on business and regulatory requirements.
Backup Media	Physical or digital storage devices used to store backup copies, such as hard drives, tapes, or cloud storage.
Data Integrity	The accuracy and consistency of data over its lifecycle ensure that data remains unchanged during the backup process.
Encryption	The process of converting data into a coded format to prevent unauthorised access.
Disaster Recovery	A strategy and set of procedures to recover and protect the Shire's IT infrastructure in case of such a disaster.
Testing	Verifying that backup copies can be restored successfully and that the backup process functions correctly.

Term	Meaning
Data Classification	The process of categorising data based on its sensitivity and importance to determine appropriate backup and protection measures.
Access Control	Security measures that restrict access to backup data and systems to authorised personnel only, ensuring data confidentiality and integrity.

9. Related Documents

Document	Purpose
Cyber Security Policy	This policy establishes the Shire's framework for Cyber Security for official records, information, or data being processed or stored in an electronic system or database.
Acceptable Use Policy	The purpose of this policy document is to define what constitutes Acceptable Use of any systems or technologies used to conduct Shire business or access Shire's systems.
IT Change Management Policy	This IT Change Management Policy document establishes the requirements and procedures the Shire must follow to identify, document, and authorise changes within the ICT infrastructures. It requires the implementation of processes that minimise the likelihood of disruptions, unauthorised alterations, and errors occurring.
IT Risk Management Policy	This IT Risk Management Policy Document outlines the principles and procedures governing the management of Information Technology (IT) risks within the Shire of Coorow. This policy aims to establish a structured approach to identifying, assessing, mitigating, and monitoring IT-related risks to ensure the confidentiality, integrity, and availability of information assets and the continuity of IT services.

Policy End

Plan

Shire of Coorow

Business Continuity and Disaster Recovery Plan

Version 1.0 April 2025

Review Date May 2026

Contents

1.0 POLICY DETAILS

Responsible Department	**Office of the CEO**
Policy Owner	**Chief Executive Officer**
Policy	**Business Continuity and Disaster Recovery Plan**
Resolution Number	
Resolution Date	
Old Policy Number	**N/A**
Register of Delegations	**CEO**
Link to Strategic Plan	**4. Civic Leadership** **4.1 Forward planning and implementation of plans to achieve community priorities.**
Next Review Date	**May 2026**

1.1 Preparation

Action	Name	Date
Initial Draft	Simon Cohen, Cohesis Pty Ltd Sam Curulli, Deputy Chief Executive Officer Mia Maxfield, Chief Executive Officer Kelvin Bean, Manager Works and Services	07-04-2025
Final Copy endorsed	xxx	xxx

1.2 Version Control

Version	Date Released	Pages Affected	Comments

1.3 Approvals

Version	Date Released	Pages Affected	Comments

1.0			

2.0 KEY CONTACT SHEET

Person	Position	Mobile Number	Responsibilities Incident Response (IR) Team Leader
Mia Maxfield	Chief Executive Officer	0428 521 100	IR Team Leader
Sam Curulli	Deputy Chief Executive Officer	0428 521 107	IR Team Member
Kelvin Bean	Manager Works & Services	0428 521 103	IR Team Member
Ayu Muftidhati	Community Development Officer	0472 848 749	IR Team Member
Gary Roberts	Town Park Manager	0428 521 105	IR Team Member
Guy Sims	Shire President	0407 360 222	IR Team Member

Key Contacts	Contact Number(s)
Police	Carnamah Police Station 9951 1222 Leeman Police Station 9953 0400
Emergency Services	000
Fire Brigade	000
Ambulance	000
Nursing Post	9953 0100
Hospital	Leeman Nursing Post 9953 0400
Insurance Company	Local Government Insurance Scheme (LGIS) 9483 8841
Water Corporation	131 375

Western Power	131 087
Internet Services Provider - Telstra	132 200
Electrician	S & L Quantock Electrical Stuart Quantock 0428 521 192
Plumber	GLH Plumbing & Gas Giles Hegarty 0457 369 447
Mechanic	Shire of Coorow Mechanic- Coorow Depot 0428 521 104
Water and Sewerage	iVacWA Jack Nikich 0426 818 727
Wallis Computer Solutions (MSP)	Nathaniel Wallis 9661 1803
Altus	IT Vision Head Office 9315 7000
Synergy Soft	IT Vision Head Office 9315 7000
Department of Local Government	6552 7300 1800 634 541
ABC Radio	ABC Radio Midwest & Wheatbelt 1300 501 222
Lawyer	McLeods Lawyers 9383 3133
Australian Cyber Security Hotline	1300 CYBER1 (1300 292 371)
Office of the Australian Information Commissioner	1300 363 992

3.0 INTRODUCTION

3.1 Overview

A disaster is an event that significantly reduces the Shire of Coorow's ability to provide normal services to its clients.

This Business Continuity and Disaster Recovery Plan ensures that the Shire of Coorow can maintain its service delivery at an acceptable level during or after a disruptive event or disaster. Various incidents, such as floods, fires, cyclones, vandalism, and cyber-attacks, can significantly impact the Shire's operations. This plan addresses these threats to mitigate their impact on operational activities.

3.2 Objectives

This plan aims to ensure the restoration and continuity of essential IT systems during a disaster. This will be achieved by creating and maintaining a comprehensive Disaster Recovery Plan (DRP) to guide and manage the disaster recovery process. The DRP must enable the Shire to ensure preparedness before an event by:

- Quickly and efficiently define, prioritise, and re-establish critical business functions.
- Implement a systematic plan for managing any incident or disaster.
- Outline immediate responses to minimise damage or loss during a critical incident.
- Minimising the impact of an incident on the community, staff, and Council.

This plan will be reviewed and updated every year, or whenever major business changes, to strengthen our resilience against possible damage to the business during a disaster or outage.

3.3 Availability of the Plan

The Business Continuity Disaster Recovery (BCDR) plan will be available in hard-copy form at the administration office. Copies will also be placed in the Chief Executive Officer's and all Manager's vehicles. The document will also be saved on the Shire's T Drive for electronic access.

It should be noted that the Shire also maintains a separate Disaster Recovery Plan specifically for records, which should be referred to independently as required.

3.4 The Relationship between BCP and DR

The Shire's BCP Lifecycle is shown below and provides an overview of the phases for responding to a disruption. It demonstrates the importance of having effective preparation, enabling prompt responses to acceptable service levels until the recovery has been completed.

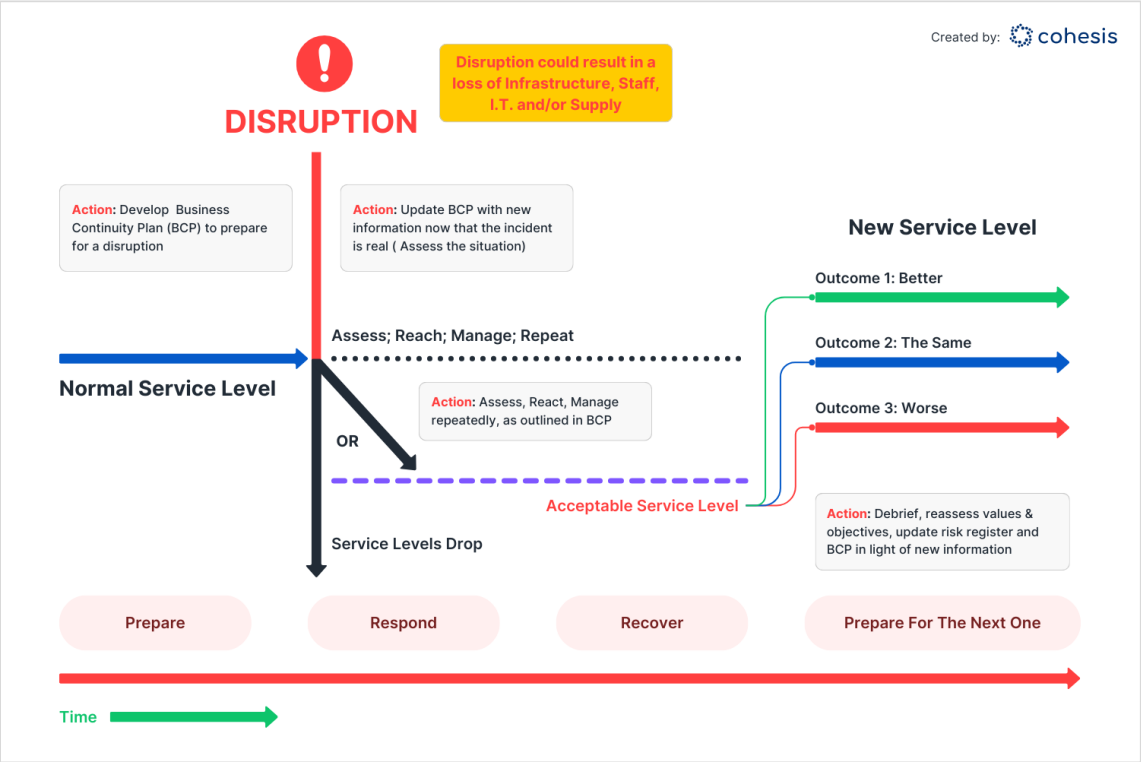

Figure 1 BCP Lifecycle

Business Continuity Planning has wider implications than ICT Disaster Recovery Planning but in organisations such as the Shire, which are highly dependent on ICT systems and networks for service delivery, there is a very high correlation.

Where operational services are reliant on IT systems and networks, their loss presents a business continuity event. Applications, systems, and networks usually have resilience enabling business operations to continue at reduced levels, but a disaster situation may involve significant technical outages and loss of business operations.

This document details the steps the Shire should take to 'Respond' and 'Recover' in a variety of the most likely 'disaster' situations.

3.5 The Governance Framework for IT BCDR

The Governance Framework for IT BCP/DRP is described by the relationship between data backups, time to recover and catastrophic consequences. The relationship assists in determining the investment required to support the BCP/DRP.

Data backups (Recovery Point Objective) - a Recovery Point Objective (RPO) is defined as the maximum amount of data – as measured by time – that can be lost after a recovery from a disaster, failure, or comparable event before data loss will exceed what is acceptable to an organisation. For example, an RPO of 60 minutes requires a system backup every 60 minutes. The RPO is usually prescribed for SaaS and hosted systems in the contractual relationship between the supplier and the customer. For on-premise systems, the backup frequency initiated on-site determines the RPO.

Time to recovery (Recovery Time Objective) - a Recovery Time Objective (RTO) is the duration of time and a service level within which a business process must be restored after a disaster to avoid unacceptable consequences associated with a break in continuity. The RTO is usually prescribed for SaaS and hosted systems in the contractual relationship between the supplier and the customer. For on-premise systems, the backup frequency initiated on-site determines the RTO.

Catastrophic consequence (Maximum Tolerable Period of Disruption) – a Maximum Tolerable Period of Disruption (MTPD) is the maximum allowable time that an organisation's key IT-dependent products or services are made unavailable or cannot be delivered before the impact is deemed unacceptable. The MTPD is peculiar to the customer regardless of whether it is SaaS, hosted, or on-premise. The MTPD for a customer cannot be less than the sum of the RPO and RTO as provided by a SaaS or hosted provider.

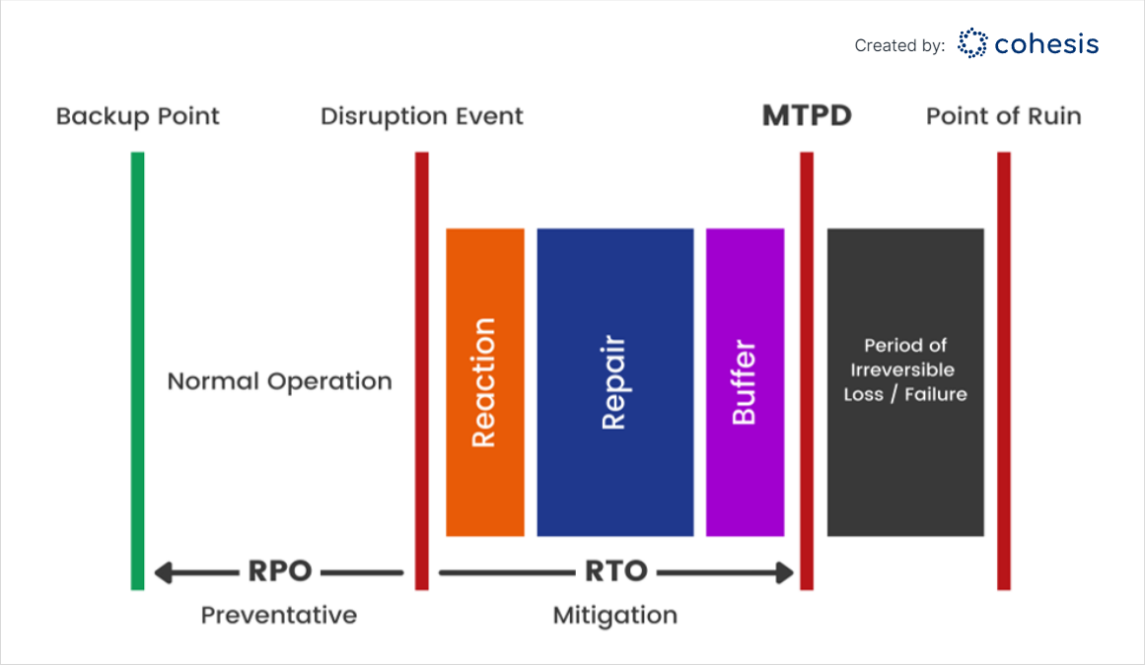

Figure 2: RPO-RTO-MTPD Relationship

3.6 Scope of Recovery

The plan is designed to manage a major disruption of the core IT infrastructure at the Shire of Coorow and will specifically focus on Information Technology and Telecommunications services.

4.0 BUSINESS CONTINUITY APPROACH OVERVIEW

4.1 Business Continuity Scenarios

The table below identifies typical Business Continuity scenarios and Shire's approach for activating this BCDR Plan, associated communications and return to BAU.

Event	Example Circumstances	Timeframe	Notify
Natural Disasters that cause significant damage to facilities and ICT structure	• Floods • Earthquakes • Bushfires • Severe storms	The plan will be activated immediately upon confirmation of significant impact.	• All Staff • Public • Emergency Services
Power Outages	• Equipment failure • Grid overload	The plan will be activated if the issue persists beyond the 4-hour resolution window.	• All Staff • Public • Electric Service Provider • Emergency Services. • ICT Support • Mechanic
Technical Failures Major hardware or software failures which cannot be resolved within 4 hours.	• Server crashes. • Data corruption. • Network outages. • Unable to access critical applications.	The plan will be activated if the issue persists beyond the 4-hour resolution window.	• All Staff • ICT Support and/or Application Vendor(s) • Public (CEO Decision)
Significant Cyber Breaches	• Ransomware attacks • Data breaches. • Malicious activities that compromise the integrity or availability of ICT services.	The plan will be activated immediately upon detection of such incidents.	• All Staff • ICT Support and/or Application Vendor(s) • Public (CEO Decision) • ACSC / OAIC • Cyber Insurance • Police
Human Error	• Any mistakes or accidents that lead to	The plan will be activated immediately	• Staff

Event	Example Circumstances	Timeframe	Notify
	significant data loss or system outages.	upon detection of the incident.	• IT Support and/or application vendor(s)
Other Emergencies	• Any other incident deemed by Senior Management that disrupts normal business operations and ICT services.	The plan will be activated as soon as senior management recognises the incident as critical.	• Staff • IT Support and/or application vendor(s) • Others as required.

As discussed in section 4.0, it is the CEO's responsibility to invoke the activation of the DRP.

4.2 Evacuation Procedures

Relevant procedures and plans are developed, displayed, and practiced by Council's OSH policy and procedures.

4.3 Emergency Kit

If there is damage to the Administration building or if it must be evacuated and operations need to be moved to the Disaster Recovery Site, the emergency kit can be picked up and quickly and easily carried offsite.

The items and documents included in the emergency kit are:

Documents:

- Business Continuity Plan incorporating key contact lists.
- Building site plan (this could help in a salvage effort), including location of gas, electricity and water shut-off points.
- Evacuation plan.
- Latest stock and equipment inventory.
- Sufficient records to undertake manual transaction processing (i.e. creditors, contractors, banks, etc.)
- Procedure manuals.
- Instructions for the diversion of telephone lines.
- Headed stationery and Shire seals and documents.

Equipment:

- Spare keys/security codes.
- Message pads and flip chart.
- Marker pens (for temporary signs).
- General stationery (pens, paper, etc).

4.4 Communication Plan

Alerts and communications are essential for effective internal and external coordination during a crisis. They form the backbone of the Shire's BCDR plan, ensuring all stakeholders are aligned and informed when a disaster occurs. Clear and timely communication will help to manage the incident effectively, minimise damage, and facilitate a swift recovery.

Objectives

1. Inform stakeholders, including employees, management, partners, and the public, about the incident status and recovery efforts.
2. Supply timely information to support informed decision-making by the Incident Management and Recovery Team.
3. Provide accurate and transparent information to maintain trust and confidence among staff and stakeholders. Reduce the impact of the incident through proactive communication, mitigating misinformation and panic.

Strategies for Delivering Information

1. Determine communication frequency.
   a. The Frequency shall be decided by the IMRT based on the nature of the incident, the potential for data loss, and the expected time for recovery.
   b. Regular updates must be provided at intervals that reflect the severity and developments of the situation.

2. Communication channels
   a. The default communication mechanisms will be email and phone.
   b. Information will be posted on the Shire's website and social media channels such as Facebook.
   c. Subject to the availability of these communication channels, fallback measures such as direct phone calls and messaging will be employed if primary methods are unavailable.
   d. If available, the Shire will use its website as its central information hub, where stakeholders can access up-to-date information and status reports.

3. Spokesperson
   a. Internal communications will be managed by the Deputy CEO.
   b. External communications will be overseen by the CEO.

4.5 Return to Business as Usual (BAU)

As systems and/or hardware are brought back online and service delivery activities resume, it is important that any temporary measures required to restore services are transitioned back to their normal BAU state.

As appropriate, the Shire should also seek to address the root cause of the incident to prevent reoccurrence.

5.0 INCIDENT MANAGEMENT

5.1 Roles And Responsibilities

Should a significant 'disruption event' occur, the Shire will convene its Incident Management Response Team (IMRT). This will determine the nature and severity of the event and whether a disaster has or is about to occur.

The roles and responsibilities of the IMRT are shown in the table below.

Role	Responsibility
Shire President	• Authorise emergency expenditure. • Media communications.
Recovery Team Leader Chief Executive Officer	• Provide overall leadership and direction during the disaster recovery process. • Primary point of contact for all disaster recovery activities. • Approve the Disaster Recovery Plan (DRP) activation and oversee its implementation. • Spokesperson to external parties. • Decide when the Shire can return to its original infrastructure when the disaster has been resolved. • Conduct a post-disaster review to evaluate the effectiveness of the recovery efforts.
Recovery Coordinator Deputy CEO / Manager Works and Services	• Spokesperson to internal staff. • Coordinate with various teams and departments to ensure a cohesive and effective response. • Identify lessons learned and areas for improvement in the disaster recovery plan. • Implement changes and updates to the DRP based on the review findings to enhance resilience.

Role	Responsibility
Administration Executive Assistant to the CEO	• Capture meeting minutes, documenting actions. • Assist in arranging and coordinating 3rd parties and overseeing practical recovery steps.
IT Recovery Managed IT Support provider	• Re-establish IT operations, including print and security services. • Assist in restoring the data network infrastructure, which encompasses the recovery of hardware components, connectivity to the recovery site, and the restoration of essential network software. • Assist in the restoration of critical servers and applications. • Coordinate with the appropriate telephony and internet service providers. • Collate documentary evidence if the incident is caused by a Cyber Attack or malpractice.
Network Services Recovery Internet Provider/Telephone Service Provider	• Recovery of voice and data network infrastructure.

5.2 Incident Management Response Process

The image below shows the Shire's Incident Response Process. Although an incident may not necessarily constitute a disaster, this process should be followed by the IMRT for all incidents significantly affecting service delivery.

Each phase has distinct tasks that collectively aim to manage and mitigate an incident's impact effectively. This structured approach ensures thorough handling, from detection to post-incident learning and improvement.

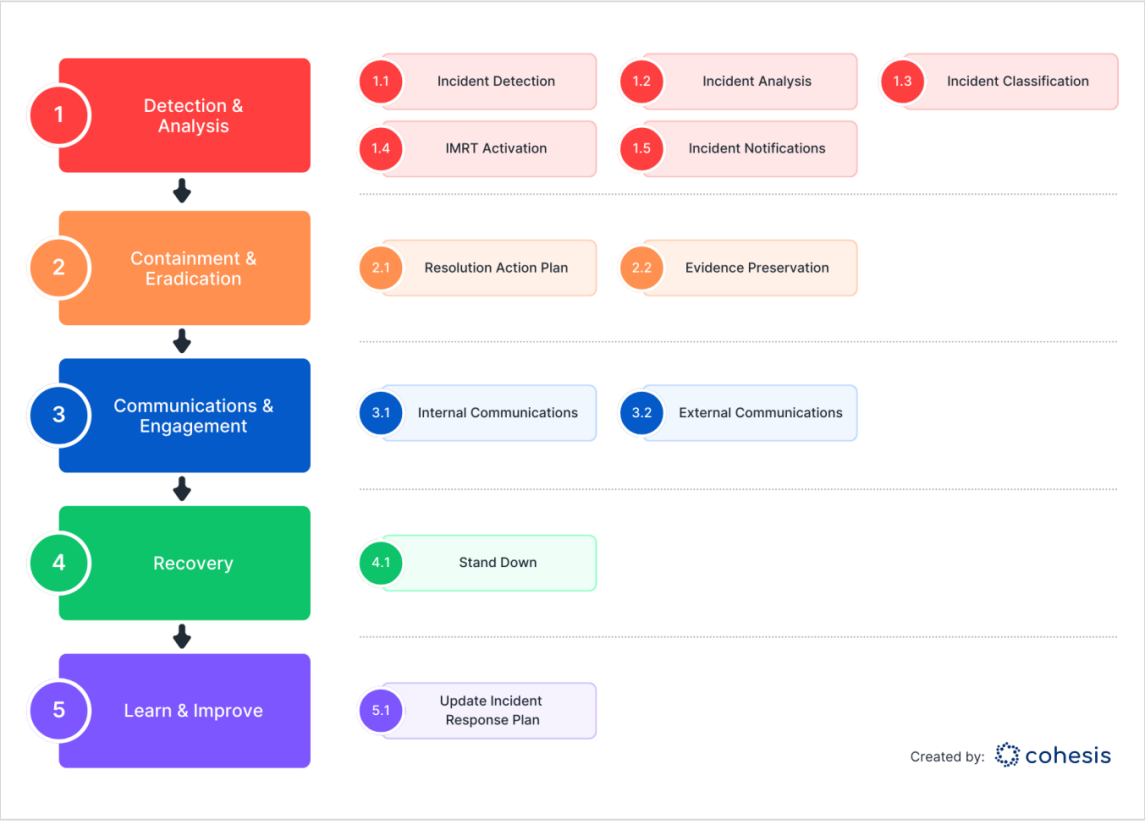

Figure 3: The Shire of Coorow Incident Management Process

Step 1 – once an incident has been detected, initial analysis should be performed to determine whether a disaster event has occurred. Depending on the severity the Incident Management Response Team may need to be convened. Disasters relating to a Cyber Attack or data breach may necessitate the need to notify the Australian Cyber Security Centre, and the Office of the Australian Information Commissioner as well as the police. For this reason, it is important to determine early in the process what type of documentation and evidence needs to be collected.

Organisation	Contact Number	Notes
Australian Cyber Security	1300 CYBER1 (1300 292 371)	Available 24/7
Office of the Australian Information Commissioner	1 300 363 992	Available Monday to Thursday 10 am to 4 pm (AEST/AEDT)
Police	(08) 9963 8800	Mon-Fri 8am-4pm
Insurance	(08) 9483 8841	LGIS WA

Step 2 - Once the nature and severity of the disaster incident are known, an Action Plan is required to remediate the issue and return to a normal service state. The remediation plan is likely to include mechanisms to preserve evidence.

Step 3 - Depending on the nature of the incident, the Shire may need to communicate both internally and externally. These communications may be different and delivered in different ways. For example, if a Cyber-attack brought the website down, the Shire's Facebook page may be an appropriate means of communication with the community. Internal communications may consist of text messages or emails.

Step 4 – As the Shire recovers from the Incident, steps should be taken to stand down the Incident Management Response Team ensuring that all documentation is completed. This may be necessary for insurance purposes.

Step 5 – As normal service provision resumes, a review should be performed to determine what lessons can be learned and to ensure they are captured in updated policies, procedures, and plans (including this document).

6.0 KEY RISK SITUATIONS & MITIGATIONS

6.1 Loss of the Shire of Coorow Administration Centre & Leeman Office Building

The Shire of Coorow operates two separate administration centres: the Admin Centre and the Office building which are located over an hour's drive apart. Due to the significant distance, the risk of losing both sites simultaneously is low.

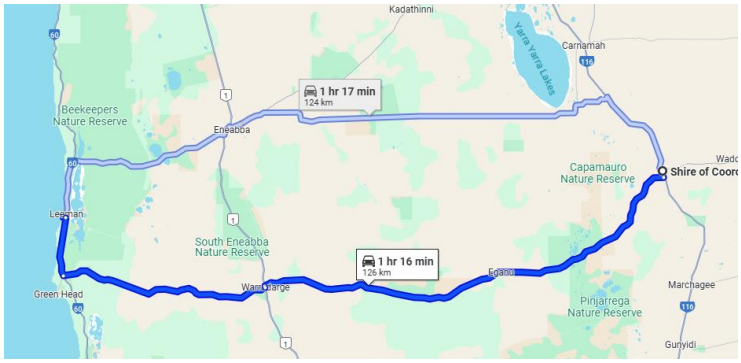

Figure 4: Shire of Coorow and Leeman Building Locations

The physical IT infrastructure is housed in the Shire of Coorow Office Building. This infrastructure includes critical components such as:

- Firewall to manage and secure network traffic.
- Patch panels for network connectivity.
- Primary and backup servers for operational continuity.
- CCTV infrastructure providing surveillance across the town.
- Datto devices utilised for backups.
- Multiple virtual machines hosted on Hyper-V

6.1.1 Task 1 - Immediate Response

Recovery Criteria	Details
Time Objective	Within 24 hours
Locations	Primary Site: Shire of Coorow Office & Leeman Administration Building Secondary Site: Townhall/Mailey Park
Resource Requirements	Mobile Phones

Procedure	
Undertake the following Steps:	a) Ensure the site has been evacuated and all personnel are accounted for. b) Secure the site and prevent access. c) Contact Emergency Services and Police. d) Identify any injuries and render assistance. e) Undertake an initial assessment of damage and risks at both sites. f) Coordinate with the Spokesperson/Shire to post notifications on the website and social media regarding the closure of both admin offices. g) Determine the time frame for switching to the disaster recovery site.
Considerations	The town hall is currently leased. Consider informing the CRC that it will be designated as a disaster recovery site. Coorow CRC- 9952 1266

6.1.2 *Task 2 - Commence operations from Disaster Recovery Site*

Recovery Criteria	Details
Time Objective	Within 72 hours
Resource Requirements	1. Office furniture and stationery 2. Administration, Cleaners and Works & Services staff 3. IT hardware and software communications (landline and internet)

Procedure	
1. Establish the disaster recovery site.	a) Set up workspaces using available furniture. b) Layout workspace utilising tables and chairs. c) If desktop computers are damaged, procure new devices to enable administrative operations. d) Source telephones establish communications and redirect calls to landlines. e) Allocate staff to customer service and disaster recovery assistance. f) Liaise with other Incident Response Team members to determine items to be immediately replaced and what is recoverable. g) Contact Managed Support Provider, Shire's IT supplier and stationery supplier. h) Recover backup disks from external sites.

	i) Recover software stored offsite. j) Cancel all forward bookings of the Shire of Coorow and Leeman Office.
2. Assess damage and undertake salvage operations.	a) Undertake an initial assessment of salvageable materials, items records and assets. b) Contact staff to remove items to the salvage site.
3. Coordinate all communications, media and elected members, Local Government insurers and general co-ordination of recovery process – **Deputy CEO/ Executive Assistant to the CEO**.	a) Liaise with the Shire President to issue a media statement. b) Coordinate meetings with the Incident Response team. c) Authorise all immediate purchasing requirements. d) Liaise with Shire's insurers.

6.1.3 *Task 3 - Assess damage and prepare medium-term Recovery Plans*

Recovery Criteria	Details
Time Objective	4 Weeks
Locations	N/A
Resource Requirements	1. IT contractors. 2. Additional infrastructure as identified. 3. Contractors to clean up disaster sites.

Procedure	
1. Establish the disaster recovery site for full operations in the medium or longer term.	a) Recover data from the pre-disaster state. b) Bring all records up to date. c) Contact all necessary persons to inform them of the incident and expected delays and seek documentation where necessary. d) Establish necessary equipment and infrastructure requirements to provide full operations from the recovery site, including demountable buildings and other office accommodations.
2. Finalise the damage assessment of the building, determine the action to rebuild it, and make	a) Undertake an assessment of the building, determine action to rebuild fully or partially, and make recommendations to the Council.

recommendations to the Council fully or partially.	
3. Coordinate all communications, media, elected members, local government insurers, and general coordination of recovery process – **Deputy CEO/ Executive Assistant to the CEO**.	a) Oversee assessment and recovery. b) Coordinate meetings with the Incident Management Response Team. c) Oversee planning for medium-term operation from Disaster Recovery Site (6-12 months).

6.1.4 Task 4 - Long-term Recovery Plan and Relocation to permanent Shire office building

Recovery Criteria	Details
Time Objective	From the commencement of this task, after 4 weeks from the incident, the target is to have all Shire functions permanently operating from the rebuilt Shire of Coorow and Leeman office within 12 months.
Resource Requirements	1. IT contractors. 2. Additional infrastructure as identified. 3. Contractors to clean up disaster sites.

Procedure	
1. Undertake the following steps: **CEO**	a) Review operations for the location of new premises. b) Undertake design and tendering processes. c) Oversee construction of new premises. d) Oversee commissioning of new premises. e) Present review findings to the Council for decision. f) Appoint an architect, exterior and interior designers, engineers, and other necessary assistance to design, specify, and document new premises. g) Issue tenders, appoint a contractor and commence construction. h) Commission new premises and commence operations from the new building.

6.2 Loss of the Shire of Coorow Administration Centre

Types of incidents include fire; flood/storm and earthquake (Refer to Appendix 9.3 Immediate Response Checklist).

6.2.1 Task 1 - Immediate Response

Recovery Criteria	Details
Time Objective	Within 24 hours
Locations	Primary Site: Shire of Coorow Office Secondary Site: Mailey Park / Townhall *The **Leeman Office** can temporarily handle the Shire's critical functions while the Disaster Recovery (DR) site is being established.*
Resource Requirements	Mobile Phones

Procedure	
Undertake the following Steps:	h) Ensure the site has been evacuated and all personnel are accounted for. i) Secure the site and prevent access. j) Contact Emergency Services and Police. k) Identify any injuries and render assistance. l) Undertake an initial assessment of damage and risks. m) Contact IT Support to update the IVR recording advising callers that all calls will be diverted to the Leeman office. n) Work with the Leeman Office so that it can temporarily manage the Shire's critical functions. o) Determine the time frame for switching to the disaster recovery site.

6.2.2 Task 2 - Commence operations from Disaster Recovery Site

Recovery Criteria	Details
Time Objective	Within 72 hours
Resource Requirements	4. Office furniture and stationery 5. Administration, Cleaners and Works & Services staff 6. IT hardware and software Communications (landline and internet)

Procedure

4. Establish the disaster recovery site.	k) Layout workspace utilising tables and chairs. l) Source telephones establish communications and redirect calls to landlines. m) Allocate staff to customer service and disaster recovery assistance. n) Liaise with other Incident Response Team members to determine items to be immediately replaced and what is recoverable. o) Contact Managed Support Provider, Shire's IT supplier and stationery supplier. p) Recover backup disks from external sites. q) Recover software stored offsite. r) Cancel all forward bookings of the Shire of Coorow Office. s) Coordinate with the Leeman Office to determine which activities should be managed from Leeman and which should be transitioned to the DR site.
5. Assess damage and undertake salvage operations.	c) Undertake an initial assessment of salvageable materials, items records, etc. d) Contact staff to remove items to the salvage site.
6. Coordinate all communications, media and elected members, Local Government insurers and general co-ordination of recovery process – **Deputy CEO/ Executive Assistant to the CEO**.	e) Liaise with the Shire President to issue a media statement. f) Coordinate meetings with the Incident Response team. g) Authorise all immediate purchasing requirements. h) Liaise with Shire's insurers.

6.2.3 Task 3 - Assess damage and prepare medium-term Recovery Plans

Recovery Criteria	Details
Time Objective	4 Weeks
Locations	N/A
Resource Requirements	1. IT contractors. 2. Additional infrastructure as identified. 3. Contractors to clean up disaster sites.

Procedure

4. Establish the disaster recovery site for full operations in the medium or longer term.	e) Recover data from the pre-disaster state. f) Bring all records up to date. g) Contact all necessary persons to inform them of the incident and expected delays and seek documentation where necessary. h) Establish necessary equipment and infrastructure requirements to provide full operations from the recovery site, including demountable buildings and other office accommodations.
5. Finalise the damage assessment of the building, determine the action to rebuild it, and make recommendations to the Council fully or partially.	b) Undertake an assessment of the building, determine action to rebuild fully or partially, and make recommendations to the Council.
6. Coordinate all communications, media, elected members, local government insurers, and general coordination of recovery process – **Deputy CEO/ Executive Assistant to the CEO**.	d) Oversee assessment and recovery. e) Coordinate meetings with the Incident Management Response Team. f) Oversee planning for medium-term operation from Disaster Recovery Site (6-12 months).

6.2.4 *Task 4 - Long-term Recovery Plan and Relocation to permanent Shire office building*

Recovery Criteria	Details
Time Objective	From the commencement of this task, after 4 weeks from the incident, the target is to have all Shire functions permanently operating from the rebuilt Shire office within 12 months.
Resource Requirements	4. IT contractors. 5. Additional infrastructure as identified. 6. Contractors to clean up disaster sites.

Procedure	
2. Undertake the following steps: **CEO**	i) Review operations for the location of new premises. j) Undertake design and tendering processes. k) Oversee construction of new premises. l) Oversee the commissioning of new premises. m) Present review findings to the Council for decision. n) Appoint an architect, exterior and interior designers, engineers, and other necessary assistance to design, specify, and document new premises. o) Issue tenders, appoint a contractor and commence construction. p) Commission new premises and commence operations from the new building.

6.3 Complete IT Hardware Failure

This section provides the necessary steps to recover the Shire's IT hardware in the event of total failure. (Refer to Appendix 4 Immediate Response Checklist).

Recovery Criteria	Details
Time Objective	Temporary arrangements and virtual server – 48hours Onsite replacement – 2 weeks
Resource Requirements	IT suppliers (hardware/software, SynergySoft, Altus, Licensing, etc.)

Procedure	
1. Undertake the following steps: **CEO**	a) Assess the severity of the outage through the shire's IT provider and determine the likely outage time and business impact. b) Determine whether hardware is recoverable. c) Inform Council, community, and business contacts (i.e., banks, creditors, and contractors) of potential service delays. d) Seek quotations and place orders for replacement components. e) Contact Shire's insurers and Police if necessary.
2. Temporary Virtual Environment: MSP Provider	f) Load the latest backed-up data onto a virtual server. g) Arrange for logins and access to a virtual server for staff.
3. Hardware Replacement and Post Recovery Verification	h) Set up and install new hardware. i) Install all software and restore from backups. j) Reconcile and rebuild all data. k) Conduct operational tests to ensure full functionality.

6.4 Loss of the Leeman Office Building

Types of incidents include fire, flood/storms, and earthquake (Refer to Appendix 4 Immediate Response Checklist).

6.4.1 Task 1 - Immediate response

Recovery Criteria	Details
Time Objective	The time frame for this activity is within 1 hour of being called by the Incident Response Team Leader.
Location	Shire of Coorow Admin Office & Recreation Centre.
Resource Requirements	Mobile Phones

Procedure	
1. Undertake the following steps: **CEO**	a) Ensure the site has been evacuated and all personnel are accounted for. b) Secure the site and prevent access. c) Contact Emergency Services and Police. d) Identify any injuries and render assistance. e) Engage Incident Response Team. f) Undertake an initial assessment of damage and risks. g) The Team Leader determines the time frame for switching to the Disaster Recovery site. h) Arrange diversion of phone lines to existing Shire mobiles.
Other Considerations	a) Secure the affected area as necessary. b) Restrict access to the building/site. c) Liaise with Emergency Services and Police. d) Inform Local Government Insurance Services. e) Inform Elected Members, employees. f) Liaise with the Shire President to make a press release.

6.4.2 Task 2 – Commence operations from disaster recovery site

Recovery Criteria	Details
Time Objective	Within 72 hours.
Location	Primary site: Leeman Office. Secondary site: Shire of Coorow Administration Centre.
Resource Requirements	1. Office furniture and stationery. 2. Administration and Works staff. 3. IT hardware and software. 4. Communications (landline and internet).

Procedure	
1. Establish the disaster recovery site.	a) Assess the suitability of the Leeman Office as the primary DR site; if unusable, activate the secondary DR site at the Coorow Administration Centre. b) Set up the temporary site with necessary resources, including furniture, IT hardware, and communication equipment. c) Resume administration functions at the designated DR site to maintain continuity of operations.
2. Assess damage and undertake salvage operations.	a) Undertake an initial assessment of salvageable materials, items, and records, etc. b) Engage staff to remove items to the salvage site.
3. Co-ordinate all communications, media and elected members, Local Government insurers and general co-ordination of recovery process – **Deputy CEO/ Executive Assistant to the CEO**.	a) Liaise with the Shire President to issue a media statement. b) Oversee assessment and recovery. c) Coordinate meetings of the Incident Response team. d) Authorise all immediate purchasing requirements. e) Liaise with Shire's insurers.

6.4.3 *Task 3 – Assess damage and prepare medium-term Recovery Plans*

Recovery Criteria	Details
Time Objective	4 weeks
Resource Requirements	1. IT contractors. 2. Additional infrastructure as identified. 3. Contractors to clean up disaster sites.

Procedure	
1. Establish the disaster recovery site for full operations in the medium to longer term.	a) Establish an appropriate temporary site. b) Administration function to resume from the Shire office (or alternate site). c) Contact all necessary persons to inform them of the incident and expected delays and seek documentation where necessary. d) Liaise with the CEO to establish necessary equipment and infrastructure requirements to provide full operations from the recovery site.
2. Finalise damage assessment and commence planning for re-establishing services through full or partial rebuild.	a) Undertake an assessment of the building, determine action to rebuild fully or partially, and make recommendations to the Council.
3. Co-ordinate all communications, media and elected members, Local Government insurers and general co-ordination of recovery process – **Deputy CEO/ Executive Assistant to the CEO**.	a) Oversee assessment and recovery. b) Coordinate meetings with the Incident Response Team. c) Oversee planning for medium-term operation from Disaster Recovery Site (6-12 months)

6.4.4 *Task 4 – Long-term Recover Plan and relocation to permanent Shire Depot Building*

Recovery Criteria	Details
Time Objective	From the commencement of this task, after 4 weeks from the incident, the target is to have all Shire functions permanently operating from the rebuilt Leeman Office in 12 months.
Resource Requirements	1. Planning assistance 2. Consultants/architects 3. Contractors

Procedure	
1. Establish a working party to:	a) Review operations for the location of new premises. b) Undertake design and tendering processes. c) Oversee construction of new premises. d) Oversee commissioning of new premises. e) Present review findings to the Council for decision. f) Appoint an architect, exterior and interior designers, engineers, and other necessary assistance to design, specify, and document new premises. g) Issue tenders, appoint a contractor and commence construction. h) Commission new premises and commence operations from the new building.

6.5 Loss of the Depot Building(s)

The Shire of Coorow operates three depot sites:

1. Shire of Coorow Depot - The Shire of Coorow Depot is located near the Shire of Coorow Admin Office. It features an office area, a mechanics workshop housing essential tools and equipment, and a small office dedicated to depot administrative functions.
2. Leeman Depot - Like the Shire of Coorow Depot, the Leeman Depot comprises an office area and a mechanics workshop, supporting maintenance and operational needs.
3. Greenhead Depot - The Greenhead Depot, measuring **6m x 6m**, is significantly smaller than the other depots and serves a more limited operational capacity.

The incidents that could impact the depot include fire, floods/storms, and earthquakes (Refer to Appendix 4 – Immediate Response Checklist**).**

6.5.2 Task 1 - Immediate response

Recovery Criteria	Details
Time Objective	The time frame for this activity is within 24 hours of the incident.
Location	Shire of Coorow Depot Building
Resource Requirements	Mobile Phones

Procedure	
1. The Incident Response Work Services Manager and CEO are to undertake the following steps:	a) Assess the extent of the damage and determine the operability of equipment and materials stored at the depot. b) Notify staff, Council, and affected Stakeholders about the incident and potential disruptions.
Other Considerations	a) Liaise with Emergency Services and Police. b) Inform elected members and employees. c) Inform the Press and community where possible. d) Inform Local Government Insurance Services.

6.5.3 Task 2 – Commence operations from temporary recovery site

Recovery Criteria	Details
Time Objective	Within 1 week.
Location	The Shire of Coorow Depot
Resource Requirements	1. Temporary workspaces or facilities. 2. Communication devices (mobile phones, radios, internet access). 3. Basic office equipment (laptops, printers, desks, chairs). 4. Procurement of tools, machinery, and vehicles needed for ongoing operations. 5. Transportation for staff and equipment.

Procedure	
1. Clean up and secure the site	a) Staff or contractors to clear debris and ensure site safety. Estimated cleanup times: Shire of Coorow Depot – 1 week, Leeman Depot – 1 week, Green Head Depot – half a day. b) Clean up and assess for hazards.
2. Establish temporary operations.	a) Contact relevant personnel about the incident and expected delays. b) Allocate staff to customer service and disaster recovery assistance. c) Identify and procure necessary equipment and infrastructure to restore operations at the Disaster Recovery Site. d) Temporarily relocate office and administrative functions to the Shire of Coorow Admin Office/Leeman Office. e) A mechanic will construct a temporary shed outside for immediate operations. f) Arrange for the delivery and installation of a mobile toilet at the temporary depot site.
3. Assess damage and undertake salvage operations.	a) Contact staff to remove items from the affected depot site.
4. Coordinate all communications, media, elected members, local government insurers, and general coordination of recovery process – **Deputy CEO / Executive Assistance**.	a) Liaise with the Shire President to issue a media statement. b) Coordinate meetings with the Incident Response team to Authorise all immediate purchasing or equipment/machinery lease requirements. c) Liaise with Shire's insurers.

6.5.4 *Task 3 – Assess damage and prepare medium-term Recovery Plans*

This task provides the necessary steps to commence planning for medium-term operations from the Disaster Recovery Site.

Recovery Criteria	Details
Time Objective	4 weeks
Resource Requirements	1. IT contractors. 2. Additional infrastructure as identified. 3. Staff or Contractors to clear debris and ensure safety at disaster sites. 4. Additional infrastructure, including temporary storage facilities, equipment, and utilities. 5. Procurement of tools, machinery, and vehicles necessary for ongoing operations.

Procedure	
1. Establish the disaster recovery site for the Shire's entire operations in the medium to longer term.	a) Contact all necessary persons to inform them of the incident and expected delays and seek documentation where required. b) Identify and procure necessary equipment and infrastructure for full operational capacity at the Disaster Recovery Site.
2. Finalise damage assessment and commence planning for re-establishing services through full or partial rebuild.	a) Conduct a detailed site assessment to evaluate the extent of the damage and determine safety concerns. b) Develop a comprehensive plan for the restoration or rebuild of the depot, including cost estimates, timelines, and resource requirements. c) Present recommendations to the Council for decision-making on a full or partial rebuild.
3. Co-ordinate all communications, media and elected members, Local Government insurers and general co-ordination of recovery process – **Deputy CEO / EA**	a) Oversee and support damage assessment and recovery planning activities. b) Schedule and lead meetings with the Incident Response Team to discuss progress and challenges. c) Liaise with insurers, contractors, and elected members to ensure efficient resource allocation and communication. d) Manage public and media relations by providing timely updates, ensuring transparency, and maintaining community confidence. Oversee medium-term operational planning for continued services from the Disaster Recovery Site (6-12 months).

6.5.5 *Task 4 – Long-term Recover Plan and relocation to a permanent site.*

Recovery Criteria	Details
Time Objective	From the commencement of this task, 4 weeks from the incident, the target is to have all Shire functions permanently operating from the rebuilt Shire Depot Building within 12 months.
Resource Requirements	1. Planning assistance 2. Consultants/architects 3. Contractors

Procedure	
1. Undertake the following steps:	a) Establish a working party to: o Review operations for the location of new premises. o Undertake design and tendering processes. o Oversee construction of new premises. o Oversee the commissioning of new premises. b) Present review findings to the Council for decision. c) Appoint an architect, exterior and interior designers, engineers, and other necessary assistance to design, specify, and document new premises. d) Issue tenders, appoint a contractor and commence construction. e) Commission new premises and commence operations from the new building.

6.6 Loss of Data – Server/On-premise Applications

The loss of a data server or on-premise applications poses a critical risk to the Shire's operations, impacting essential systems like Synergy Soft, Altus & Definitiv, and InfoCouncil, which support core business operations.

Recovery Criteria	Details
Time Objective	Within 72 hours
Locations	Primary Site: Admin Building
Resource Requirements	Mobile Phones/Phone

Procedure	
1. Contact the Shire's MSP/IT Support/Application Vendor and work with them to	a) Identify the point of failure and the extent of data loss. b) Initiate the failover process to switch to the secondary server. c) Restore the most recent backup. d) Verify the integrity of the restored data. e) Ensure all systems and services are operational.
2. In the event of a server failure,	a) Proceed to 6.9.
Other Considerations	a) Communicate the likely restoration timeline to staff. Depending on the nature of the impact on services, consider posting this information on the Shire's website. b) Ensure appropriate cloud file storage services are provided so that staff can save and collaborate on files.

6.7 Loss of Data – Cloud Applications

The Shire's cloud applications include Altus Payroll & Timesheet and Code Two Signatures.

Recovery Criteria	Details
Time Objective	Within 72 hours
Requirements	1. Mobile Phones/Phone 2. Cloud Application Vendor contact details. 3. Internet Connectivity 4. Admin Staff (to test the integrity of data)

Procedure	
1. Contact Cloud Vendor Application Support to report the data loss incident and request data recovery.	a) Coordinate with Cloud Vendor Application Support on the data recovery. b) When data is recovered, verify the integrity and completeness of restored data.
Other Considerations	a) Ensure the data is recovered within the agreed SLAs with the Cloud Application Vendor. b) Coordinate with Cloud Application Vendor to align recovery protocols and ensure swift response times. c) If the Cloud Application Vendor requires an extended period to recover the data, revert to manual procedures for capturing information to ensure continuity of operations.

6.8 Loss of an Application

Shire's on-premises applications include Synergy Soft, Altus, Info-Council, Adobe, Workflows (SirsiDynix), SAP Crystal Reports, TechSmith Camtasia, and Universe 11.3,2. In the event of an on-premise application failure, Shire will restore from the most recent backup.

Recovery Criteria	Details
Time Objective	Within 72 hours
Requirements	1. Mobile Phones/Phone 2. Cloud Application Vendor contact details 3. IT Support

Procedure	
1. For on-premise applications (Synergy Soft and Altus)	1. Identify the point of failure and the extent of application loss. 2. Restore the most recent backup from the backup repository. 3. Verify the functionality and integrity of the restored application. 4. Resume normal operations and monitor the application closely for any issues.

6.9 Loss of Communication

This plan addresses the loss of internet connectivity at the Shire office, including scenarios where both the primary internet Fusion Broadband and backup Telstra 4G fail. Internet connectivity is critical for operational continuity, communication, and access to cloud and on-premise systems. This DR plan ensures that connectivity is restored promptly and alternative measures are in place to minimise operational disruption.

Recovery Criteria	Details
Time Objective	Within 24 hours
Locations	Primary Site: Coorow Office Secondary Site: Leeman Office
Resource Requirements	1. Mobile Phones (4G/5G Connectivity) / Telstra Connectivity 2. IT Support 3. Internet Provider Contact Details

Procedure	
1. Loss of internet connectivity – Shire of Coorow Administration Centre	a) Initial triage: o Determine the cause and impact of the outage. o Call IT Support to assist with the initial troubleshooting. o Call the Internet Service Provider. b) Enable the Backup Internet (Telstra 4G). If the 4G connection is operational, reroute all network traffic through the backup. c) If the Primary and backup internet is down, contact IT support to confirm the redundancy failure and assist with advanced troubleshooting. d) Communicate likely recovery timeframe to staff. e) Depending on the likely outage period, notify Shire's website and social media channels of the potential impact on services. f) Where feasible, advise staff to work from locations with stable internet connectivity, such as other offices or home setups, to maintain productivity. g) Advise staff once internet connectivity is restored. h) Remove notifications from the Shire's website and social media platforms.
2. Loss of internet connectivity – Leeman Office	a) Initial triage: o Determine the cause and impact of the outage.

	○ Call IT Support to assist with the initial troubleshooting. ○ Call the Internet Service Provider. b) Communicate likely recovery timeframe to staff. c) Depending on the likely outage period, notify Shire's website and social media channels of the potential impact on services. d) Where feasible, advise staff to work from locations with stable internet connectivity, such as other offices or home setups, to maintain productivity. e) Advise staff once internet connectivity is restored. f) Remove notifications from the Shire's website and social media platforms.
3. In the event of loss of telecommunications	a) Initial triage: ○ Determine the cause and impact of the outage. ○ Call IT Support ○ Call Phone Vendor Support b) Divert the Shire's main phone number to an alternative number. (It may be necessary to contact IT and phone Vendor support for assistance). c) Advise staff of phone outages. Place notifications on the Shire's website and social media channels.

6.10 Loss of ICT Infrastructure

The Shire depends heavily on its ICT infrastructure to provide business services. This plan will enable the Shire to recover from losing switches, networks, routers, and/or servers.

- In the event of a primary server failure, the failover mechanism will activate the on-prem failover server within minutes, restoring operations to the last backed-up state. While this process may result in a potential loss of up to one hour of data, the Shire's systems will be quickly operational again.
- The Shire's data is backed up at the Managed Service Provider's (MSP) data centre. In the event of a failure of both the primary and on-prem failover servers, the Shire can recover their data from the MSP data centre.

Recovery Criteria	Details
Time Objective	Within 24 hours
Resource Requirements	1. Mobile Phones (4G/5G Connectivity) / Telstra Connectivity 2. IT Support

Procedure	
1. Loss of Network	a) Initial triage: o Call IT Support to assist with the initial troubleshooting. o Determine the nature and scale of the impact. o Liaise with the internet service provider if applicable. b) Communicate likely recovery timeframe to staff. c) Depending on the likely outage period, notify Shire's website and social media channels of potential service impact. d) Work with the IT support provider to determine the optimal recovery approach. If IT Support needs to come onsite, facilitate access if they need to bring replacement hardware.
2. Loss of Switch/Routers/Firewall	a) Initial triage: o Call IT Support to assist with the initial troubleshooting. o Assess the nature and extent of hardware failure and work with IT Support to procure and implement replacement hardware. If the hardware (e.g., switch, router, firewall) issue is not fixable, work with IT Support for purchasing and implementing replacement hardware. b) Communicate likely recovery timeframe to staff. c) Depending on the likely outage period, notify Shire's website and social media channels of the potential impact on services. d) Work with the IT support provider to determine the optimal recovery approach. If IT Support needs to come onsite, facilitate access if they need to bring replacement hardware.

6.11 Loss of Power

Recovery Criteria	Details
Time Objective	Within 24 hours
Locations	Primary Site: Shire Administration Building Secondary Site: Shire's DR Location
Resource Requirements	1. Mobile Phones (4G/5G Connectivity)/Telstra Connectivity 2. IT Support 3. Western Power Contact Details

Procedure	
2. Loss of Power	a) Initial triage: ○ Call Western Power (Power Provider) to determine the outage length. ○ Call IT Support to assist with the graceful shutdown of the servers. b) Communicate likely recovery timeframe to staff. c) Depending on the likely outage period, notify Shire's website and social media channels of potential service impact. d) Arrange for Shire's phone numbers (e.g. Senior management mobile numbers). You may need to contact IT and phone Vendor support for assistance. e) Advise staff to work from another location with power and internet connectivity. f) Advise staff once power is restored. g) Remove notifications from the Shire's website and social media platforms.

6.12 Cyber Attack

A Cyber Attack may result in one or more of the above disaster situations, such as data loss and/or server(s) loss. In each case, the Shire should react and respond based on the type of attack and its impact using the information in conjunction with the appropriate sections above.

6.12.1 Task 1 - Immediate Response

Recovery Criteria	Details
Time Objective	Within 4 hours of detecting of a Cyber Attack
Location	Any Shire facility or endpoint.
Resource Requirements	1. Mobile Phones/Phone 2. IT Support contact details 3. Cloud or On-Premises Application Vendor contact details 4. Australian Cyber Security contact detail (1300 CYBER1 (1300 292 371) 5. Office of the Australian Information Commissioner contact details (1 300 363 992). 6. Police contact details ((08) 9963 8800). 7. Insurance contact details and policy details (LGIS (08) 9483 8888)

Procedure	
1. Cyber Attack – On-Premise Applications / Servers	a) Detection and Initial Response ○ Alert the Incident Response Team immediately. ○ Contact IT Support ○ Work with IT Support to identify the type of cyber-attack and determine its impact. ○ Assess if customer data is compromised. ○ Take affected systems and servers offline to prevent the cyber-attack from spreading. ○ Disconnect devices from the internet, isolate critical systems and change passwords on crucial accounts if needed. a) Depending on the severity of the attack, contact the following organisations/parties to report the incident: ○ Local Government Agencies such as the Australian Cyber Security and the Office of the Australian Information Commissioner. ○ Application Vendor Support

	○ (Cyber) Insurance Provider ○ Police
2. Cyber Attack – Cloud Applications	a) Detection and Initial Response ○ Alert the Incident Response Team immediately. ○ Contact Cloud Vendor Support and assess the impact on the Shire's data business processes. ○ Determine whether a Data Leak has occurred and, if so, the data types leaked (e.g. personal, sensitive, health, confidential) ○ Suspend access to affected cloud services to prevent the further spread of the attack. ○ Update passwords for essential/admin/temporary accounts where necessary. ○ Disable or remove temporary user accounts that may have been compromised. b) Contact the following organisations/parties to report the incident: ○ IT Support ○ Local Government Agencies such as the Australian Cyber Security (ACSC) and the Office of the Australian Information Commissioner (OAIG). ○ Application Vendor Support
Other Considerations	If a data breach has occurred, the Incident Response Team will need to assess whether it is notifiable. The following link provides guidance on Notifiable Data Breaches (NDBs). https://www.oaic.gov.au/__data/assets/pdf_file/0008/2240/oaic-ndb-form-for-training-purposes-only.pdf The link below directs to the OAIG's NBD form, which should be completed in the event of a Notifiable Data Breach affecting the Shire. https://webform.oaic.gov.au/prod/?entitytype=DBN&layoutcode=DataBreachWF

6.12.2 Task 2 – Containment and Eradication

Recovery Criteria	Details
Time Objective	Within 72 hours of detecting a Cyber Attack
Location	Shire's Administration Building
Resource Requirements	1. Mobile Phones/Phone 2. IT Support contact details 3. Cloud or On-Premise Application Vendor contact details 4. Australian Cyber Security contact details 5. Office of the Australian Information Commissioner contact details.

Procedure	
1. Cyber Attack – On-Premise Applications	a) IT Support (and/or ACSC) to contain the cyber attack o Determine which systems, applications and data have been compromised o Understand how the attack was carried out to prevent further exploitation b) IT Support (and/or ACSC) to eradicate the malicious threats by: o Removing malware and threats. The measures to remove malware and threats differ depending on the type of cyber-attack. o Review security measures and recommend/implement measures to strengthen security within the Shire's systems and network. c) If needed, restore data and systems from the most recent backup. d) Test the integrity of the restored data and application(s). c) Conduct forensic analysis to understand the attack and improve defences. This will be needed for Cyber Insurance claims.
2. Cyber Attack – Cloud Applications	a) Cloud Vendor Support (and/or ACSC) to contain the cyber attack o Determine which cloud services and data have been compromised. o Reset credentials for affected accounts and applications. b) Cloud Vendor Support shall help eradicate the malicious threat by: o Identifying malicious sessions in the cloud environment. o Terminating and cleaning infected instances or containers. o Restoring data from the cloud backup. o Applying security patches and updates to fix vulnerabilities. e) Test the integrity of the restored data and application(s).

	f) Conduct forensic analysis to understand the attack and improve defences.

6.12.3 Task 3 – Communication & Engagement – Customers, Staff and Public

Recovery Criteria	Details
Time Objective	Within 48 hours of detecting a Cyber Attack
Location	Shire's Administration Building
Resource Requirements	1. Laptops/Computers. 2. Access to the Shire's Website and Social Media Accounts.

Procedure	
1. Initial Notification	a) Draft a concise initial statement about the cyber-attack. Here are some considerations for the content: o Acknowledgement of the incident. o Assurance that the situation is being handled. o Brief description of the impact. o Commitment to providing further updates. o Contact information for further inquiries. b) Obtain approval from the CEO and/or legal. c) Post the initial statement on the following channels: o Shire's Website o Social media platforms o Email
2. Follow up-Communication	a) Draft a follow-up communication about the cyber incident and its impact. Here are some pointers for the content: o Detailed explanation of what happened. o Impact assessment, including potential data exposure. o Steps taken to mitigate the incident. o Measures being implemented to prevent future occurrences. o Assurance of transparency. b) Obtain approval from the CEO and/or legal. c) Post the follow-up update on the following channels: o Shire's Website o Social media platforms o Email

6.12.4 *Task 4 – Reporting and Documentation*

Recovery Criteria	Details
Time Objective	Within 48 hours of detecting a Cyber Attack
Location	Shire's Administration Building
Resource Requirements	1. Laptops/Computers. 2. Access to the Shire's Website and Social Media Accounts.

Procedure	
1. Prepare Reports and Documentation	To increase the chance of getting an insurance claim after a cyber incident, it's crucial to collect and maintain comprehensive evidence. Ensure to gather and document the following: a) Detailed information about the incident and its potential for damage. b) Provide evidence of the incident, such as screenshots, data logs, and other digital evidence. c) Document all costs associated with the incident, such as investigation expenses, data recovery, and system. d) Digital forensic reports or security audit results.

7.0 KEY SYSTEMS AND RECOVERABILITY REQUIREMENTS

The table below shows the key systems and the priority order in which they should be recovered in the event of a disaster.

Restore Priority	System	RPO	RTO	Comments
1	Firewall, Switches, Routers	Last Known Good Configuration or State.	24 Hrs	Watchguard Firebox T40 (Firewall), Cisco SG300-52P 48 port PoE (Switch)
2	Network, Internet	Last Known Good Configuration or State.	24 Hrs	Telstra Fibre NTU. Refer to Telstra SLAs
3	Server & Backup Infrastructure	Last Known Good Configuration or State.	24 Hrs	Subject to available server hardware, power supplies at the time of disaster.
4	Email System	1 Business Day	Office 365 – Microsoft SLAs.	
5	Payroll	Last Known Good Configuration or State.	Altus – Altus SLAs	
6	Timesheet	Last Known Good Configuration or State.	Altus – Altus SLAs	
7	Finance	Last Known Good Configuration or State.	Altus – Altus SLAs	
6	Document Management Drive	Last Known Good Configuration or State.	24 Hrs	
7	ERP Business Systems (Records Management)	24 Hrs – but requires internal confirmation	24 Hrs – but requires internal confirmation	

Restore Priority	System	RPO	RTO	Comments
8	ERP Business Systems (Property and Rating)	24 Hrs – but requires internal confirmation	24 Hrs – but requires internal confirmation	
9	ERP Business Systems (Name and Address Register)	24 Hrs – but requires internal confirmation	24 Hrs – but requires internal confirmation	
10	InfoCouncil	24 Hrs – but requires internal confirmation	24 Hrs – but requires internal confirmation	
12	File & Print Services	24 Hrs – but requires internal confirmation	24 Hrs – but requires internal confirmation	
13	Phone Systems	48 Hrs – but requires internal confirmation	48 Hrs – but requires internal confirmation	
14	Other Systems (Code Two Signatures for Signatures, Metro Count v5.06, SAP Crystal Reports, TechSmith Camtasia, Universe)	72 Hrs – but requires internal confirmation	72 Hrs – but requires internal confirmation	
15	Website & Social Channels	5 Business Days – requires internal confirmation	5 Business Days – requires	

Restore Priority	System	RPO	RTO	Comments
			internal confirmation	

8.0 DISASTER SITUATIONS & RESPONSES

ID	Disaster Scenario	Results in DC being offline?	Actions	Requires Restore	Requires Failover to Alternative DC
1	Data Centre offline (e.g. Fire, flood, weather event)	Yes	• Activate Failover site. • Activate affected applications at failover site. • Restore all applications as required. • Transfer traffic to failover site.	Yes	Yes
2	Server Failure	Yes	• Activate Failover site (if required) or spin up resilient virtual servers in the cloud. • Copy server to new VM. • Install and/or configure affected applications as required. • Update user machines to enable them to use the VPN service. • Transfer traffic to the failover site.	Yes	Yes
3	Network Outage	Yes	• Identify the source of the outrage, whether internal (e.g., hardware failure) or external (e.g., ISP Issue) • Set up alternative internet such as 4G/5G or Starlink to maintain critical operations.	No	No

ID	Disaster Scenario	Results in DC being offline?	Actions	Requires Restore	Requires Failover to Alternative DC
			• If the issue is external, contact service provider for fault repair.		
4	Datacentre building deemed unsafe	Maybe	• Activate Failover site. • Activate affected applications at failover site. • Restore all applications as required. • Transfer traffic to failover site.	Maybe Restore / failover likely to be required if re-entry to DC presumed to be greater than 1 business day.	Yes
5	Extended Loss of power to the DataCentre	Maybe	• Activate Failover site. • Activate affected applications at failover site. • Restore all applications as required. • Transfer traffic to failover site.	Maybe	Maybe
6	Cyber Attack (believed to have corrupted systems and/or backups)	Yes	• Detect whether systems and/or backups have been corrupted. • Take systems offline. • Assess impact. • Restore from most recent 'good' backup.	Yes	Maybe If partial corruption or if failover site not active, then restore will be performed from MSP's DC.
7	Data Breach (compromising sensitive information of residents and employees)	Maybe	• Isolate affected systems to prevent further unauthorised access. • Assess impact. • Implement security patches and strengthen access	No	No

ID	Disaster Scenario	Results in DC being offline?	Actions	Requires Restore	Requires Failover to Alternative DC
			controls to prevent future breaches.		
8	Sabotage – internal corruption of systems.	Maybe	• Assess level of breach, damage. Determine if it can be successfully contained, repaired. • If not repairable, assess whether Primary environment is recoverable. • If not rebuilt at primary site or recover at failover site.	Maybe	Maybe If partial corruption or if failover site not active, then restore will be performed from MSP's DC.
9	Physical Server(s) outage	No	• Bring Servers back online in DataCenter • If not possible provision spare servers and restore from offsite backups • Restore servers to IaaS Service Provider at a premium.	No – unless servers can't be brought back online.	No – unless primary DC is not available or no suitable failover hardware available at the primary site.
10	Key Application(s) Extended Outage	No	• Restore from most recent 'good' backup source. • Contact Vendor for Urgent/Site Down Support	Yes	Maybe
11	Cloud Service Disruption	No	• Contact the cloud service provider for status updates and expected resolution time. • Implement temporary solutions to resume operations.	No	No

ID	Disaster Scenario	Results in DC being offline?	Actions	Requires Restore	Requires Failover to Alternative DC
			• Review and enforce Service Level Agreements (SLAs) with cloud providers to ensure reliability.		
12	Hardware Theft (critical infrastructure hardware is stolen)	Maybe	• Report the theft to law enforcement and relevant authorities. • Replace with spare hardware. • If not immediately replaceable, failover to secondary server/	Maybe	Yes
13	Phishing Attack (several employees disclosing their login credentials resulting to unauthorised access to internal systems)	Maybe	• Assess level of breach. • Immediately revoke and reset affected credentials. • Conduct security audit to identify unauthorised access or changes made using the compromised accounts.	Maybe	Maybe

9.0 REHEARSE MAINTAIN AND REVIEW

It is critical that the plan is rehearsed to ensure that it remains relevant and useful. This may be done as part of a training exercise and is a key factor in the successful implementation of the plan during an emergency.

The Shire must also ensure that they regularly review and update the plan to maintain accuracy and reflect any changes inside or outside the business.
The following points may help:

- Prepare a training schedule for all people who may be involved in an emergency at the site.
- Pay attention to staff changes.
- It is best to use staff titles rather than names.
- Amend the plan based on changes to organisational structure or suppliers/contractors.
- After an event it is important to review the performance of the plan, highlighting what was handled well and what could be improved upon next time.
- Upload Business Continuity Plan to all mobile devices under Docs on Tap.

10.0 APPENDIX

10.1 Definition of Terms

Term	Meaning
Australian Cyber Security Centre (ACSC)	The Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) leads the Australian Government's efforts on cyber security. It brings together capabilities to improve the cyber resilience of the Australian community and help make Australia the most secure place to connect online.
Backup	The process of copying and archiving data to ensure it is preserved in case of a disaster.
Business Continuity Plan (BCP)	A plan to ensure that business operations can continue during and after a disaster.
Business Continuity and Disaster Recovery (BCDR) Plan	A comprehensive approach to ensuring the continuation of business operations and quick recovery of IT systems in the event of a disaster.
Cyber Attack	An attempt by hackers to damage or destroy a computer network or system.
Disaster Recovery Plan (DRP)	A plan for restoring IT systems and operations after a disaster.
Data Breach	An incident where information is accessed without authorisation.
Data Center (DC)	A facility used to house computer systems and associated components.
ERP Business Systems	Enterprise Resource Planning systems.
Failover Site	An alternate location where operations can continue in case the primary site fails.
Incident Management Response Process	The process for managing and responding to incidents that affect service delivery.

Term	Meaning
Maximum Tolerable Period of Disruption (MTPD)	The maximum time that an organisation's key IT-dependent products or services can be unavailable before unacceptable consequences occur.
Recovery Point Objective (RPO)	The maximum amount of data that can be lost after a disaster before it exceeds the organization's tolerance level.
Recovery Time Objective (RTO)	The maximum acceptable length of time that can pass before the recovery of business processes after a disaster.
Service Level Agreement (SLA)	The commitment between a service provider and a client, including details of the service, the standards the provider must adhere to, and the metrics to measure the performance.
Synergy Soft	The Shire's on-premise software solution for enterprise resource planning.
Altus	The Shire's on-premise software solution for Timesheet/Payroll/Finance processes.
InfoCouncil	The Shire's meeting minutes/agenda software solution.
T Drive	The Shire's on-premise Document Management System.

10.2 Event Log

The event log is used to record information, decision and actions in the period immediately following the critical event or incident.

Date	Time	Information/Decisions/Actions	Initials

10.3 Immediate Response Checklist

Incident Response	✓	Actions Taken
Have you: Assessed the severity of the incident?	☐	
Evacuated the site if necessary?	☐	
Accounted for everyone?	☐	
Identified any injuries to persons?	☐	
Contacted Emergency Services?	☐	
Implemented your Incident Response Plan?	☐	
Started an Event Log?	☐	
Activated staff members and resources?	☐	
Appointed a spokesperson?	☐	
Gained more information as a priority?	☐	
Briefed Team Member on incident?	☐	
Allocated specific roles and responsibilities?	☐	
Identified any damage?	☐	
Identified critical activities that disrupted?	☐	
Kept staff informed?	☐	
Contacted key stakeholders?	☐	
Understood and compiled with any regulation/compliance requirements?	☐	
Initiated media/public relations response?	☐	

10.4 Incident Recovery Checklist

Incident Response	✓	Actions Taken
Now that the crisis is over have you: Refocused efforts towards recovery?	☐	
Deactivated staff members and resources as necessary?	☐	
Continued to gather information about the situation as it affects you?	☐	
Assessed your current financial position?	☐	
Reviewed cash requirements to restore operations?	☐	
Contacted your insurance broker/company?	☐	
Developed financial goals and timeframes for recovery?	☐	
Kept staff informed?	☐	
Kept key stakeholders informed?	☐	
Identified information requirements and sourced the information?	☐	
Set priorities and recovery options?	☐	
Updated the recovery plan?	☐	
Captured lessons learnt from your individual, team and business recovery?	☐	

10.5 Related Documents

- Back-Up Policy
- Records Disaster Recovery Plan

7 NEW BUSINESS OF URGENT NATURE

8 CLOSURE

8.1 DATE OF NEXT MEETING

Next Audit and Risk Committee Meeting will be held on from .( )

8.2 CLOSURE OF MEETING

There being no further business the Chairperson, Chair B A Jack closed the meeting at type time**.**