

Record Keeping Plan 2026

Disaster Recovery Plan

**SHIRE OF
WANDERING**

VERSION 2



Table of Contents

1 Introduction.....	4
2 Potential impacts of disasters	4
2.1 Breach of customer service levels	6
2.2 Staff down time	6
2.3 Uninformed decision making.....	6
2.4 Loss of corporate memory.....	6
2.5 Legal exposure	6
2.6 Cost of re-creating information	6
2.7 Legislative non-compliance	6
3 Risk Analysis.....	7
3.1 Inventory of Assets	7
3.1.1 Electronic Components.....	7
3.1.2 Physical Components.....	8
3.2 Disaster Recovery Requirements	9
3.2.1 Level 1: Civic Administration Centre compromised.....	9
3.2.2 Level 2: Paper Loss	9
3.2.3 Level 3: Server Room Compromised.....	9
3.2.4 Level 4: Server Failure.....	9
3.2.5 Level 5: Data Loss.....	9
3.3 Disaster Counter Measures	9
3.3.1 Logical security electronic records	9
3.3.2 Physical security electronic records.....	10
3.3.3 Physical Security Vital Records	10
3.3.4 Environmental Controls	10
3.3.5 Security copies of vital records.....	10
4 Disaster Recovery Strategy.....	11
4.1 Switch to emergency backup operating mode.....	11
4.2 Plan Recovery	11
4.3 Implement appropriate recovery operations.....	11
4.3.1 Level 2: Paper Loss:	11
4.3.2 Level 3: Computer Room Compromised:.....	11
4.3.3 Level 4: Server Failure:.....	12
4.3.4 Level 5: Data Loss:.....	12
4.4 Return to Normal Operating Mode	12
4.5 Disaster continuity procedures	12
4.5.1 Electronic Record Keeping System Down	12
4.5.2 Network down	12
4.5.3 All PCs down.....	12

4.6	Disaster recovery responsibilities.....	13
4.7	Disaster recovery resources	13
4.8	Disaster Recovery Plan training program	13
4.9	Disaster Recovery Plan testing program	13
5	Appendices	14
5.1	Shire of Wandering Information Technology Disaster Recovery Plan	14
5.1.1	Definition of a disaster.....	14
5.1.2	Prerequisites	14
5.1.3	Focus Networks – IT Service	14
5.1.4	Restoring to a new machine (Disaster Recovery).....	14
5.1.5	Backup and Recover of Server and System Data	14

RECORDKEEPING PLAN

DISASTER RECOVERY PLAN

2026

Version 2.0

<i>Document Status:</i>	FINAL
<i>Revision No:</i>	2.0
<i>Supersedes Version:</i>	
<i>Created Date:</i>	19/11/2020
<i>Revision Date:</i>	31/03/2021, 21/05/2026
<i>Prepared By:</i>	Lisa Boddy, Customer Service Coordinator
<i>Reviewed By:</i>	Dr. Alistair Pinto, Chief Executive Officer
<i>Endorsed By:</i>	Dr. Alistair Pinto, Chief Executive Officer
<i>Adopted by Council:</i>	
<i>Submitted to SRC:</i>	
<i>Accepted by SRC:</i>	
<i>Next Review Due:</i>	

1 Introduction

The Record Disaster Recovery Manual forms part of the Shire of Wandering's Record Keeping Plan.

The Shire of Wandering will ensure that all government records are appropriately protected and preserved as long as required for legal, legislative, financial, administrative and historical purposes.

A major threat to the preservation of records is the risk of disasters, natural or otherwise. A disaster recovery plan is essential to ensure the swift, efficient and effective resumption of the Shire's Record Keeping System (RKS) and the wide range of activities it supports following a disaster.

2 Potential impacts of disasters

The Shire of Wandering Record Keeping System (RKS) is a vital corporate system that manages, stores and provides access to the Shire's records. The impact resulting from the entire or partial loss of records in the RKS would be high.

In the event of a disaster affecting the Shire's RKS the timely and complete recovery of the system would be essential in ensuring minimal impact on Shire of Wandering operations. Information is a key resource in all processes of the Shire and the loss of this resource would either significantly slow or halt processes entirely.

The RKS, as the primary repository for Shire of Wandering information, has the greatest potential to impact the widest range of operations if destroyed in a disaster.

To alleviate the impact of this significant work has been undertaken on the ICT systems with the establishment of regular and systematic backups. The Shire has also moved to a fully electronic records management system to secure the availability of information.

The loss of the Council's RKS could impact the Council in a number of ways. The major areas of likely impact are detailed below:

Area of Impact	Time to recovery and level of impact					
	4 Hours	1 Day	2 Days	1 Week	1 Month	Never
Customer Service Levels	L	M	M	H	H	H
Staff Down Time	L	M	M	H	H	H
Uninformed Decision Making	L	M	M	H	H	H
Loss of Corporate Memory	L	L	L	M	H	H
Legal Exposure	L	L	L	M	M	H
Cost of Recreating Information	L	L	L	M	M	H
Legislative Non-Compliance	L	L	L	L	M	H

Legend					
L	Low	M	Moderate	H	High

2.1 Breach of customer service levels

The slowing of Shire processes due to an inability to access required information, for even a short period of time, would quickly start to impact the Shire's ability to meet its customer service levels. This would result in a flow on impact to Shire customers and degradation of the Council's image in the community. The move to an electronic environment, and stability and processes in place for data recovery ensure that there would be minimal impact in the event of a minor emergency.

2.2 Staff down time

With all staff utilising the RKS in their day-to-day activities the effect of the unavailability of the system on staff productivity would be significant. For short periods of system unavailability, other work could be performed, however as the period of time increases so does the impact on staff productivity. The move to an electronic environment and stability and processes in place for data recovery ensure that there would be minimal impact in the event of a minor emergency.

2.3 Uninformed decision making

Access to the right information at the right time ensures that informed decision making by Shire staff is undertaken. If access to the RKS was interrupted in the short-term important decisions could be deferred, however as time pressures increase, decisions would have to be made without the benefit of potentially valuable information contained in Shire records.

2.4 Loss of corporate memory

The loss of the Shire's corporate memory could have a high impact in the long term. Corporate memory helps to provide the Shire with its corporate identity, heritage and historical reference, as well as empowering staff to make improved business decisions, prevent duplication of effort, increase administrative efficiency and learn from the Shire's previous mistakes.

2.5 Legal exposure

Shire of Wandering records are regularly utilised to support a legal defence or to substantiate prosecutions for the Council on various matters. The unavailability of such records would result in significant legal exposure for the Shire, by either not being successful in undertaking appropriate prosecutions under various empowering Acts or not being able to defend the Shire's actions in regard to contentious matters.

2.6 Cost of re-creating information

The loss of information used to support the Shire operations cannot be accepted in the medium to long term. Such information is necessary to carry out these operations and would need to be re-created so that the activities could continue. The re-creation of many years' worth of information is a very costly if not impossible task.

2.7 Legislative non-compliance

The Shire is required to comply with a myriad of Acts and Regulations covering all areas of the Council's diverse functions and operations. Of particular note is the *State Records Act 2000*. Non-compliance in terms of the retention and protection of Council records would result in heavy penalties and damage to the reputation of Shire of Wandering.

3 Risk Analysis

The following table details the major risks affecting the Shire's RKS. The event level refers to the level of severity of the disaster should it occur, with level 1 being the highest and level 5 being the lowest. The chance of the disaster occurring has been estimated in terms of low, moderate or high likelihood.

Risk	Description	Event Level	Likelihood
Fire – Administration Office	Significant fire damage to whole of Administration Office	Level 1	Low
Fire – Off-site Storage Facility – Works depot	Significant fire damage to whole of off-site storage facility	Level 4	Low
Fire – Server Room	Significant fire or smoke damage to Server room in Administration Building	Level 2	Moderate
Fire – Compactus	Fire or smoke damage to paper records	Level 1	Moderate
Fire – Fireproof safe Administrative Office vital	Fire or smoke damage to paper records	Level 1	Low
Water Damage – Compactus	Water damage to paper records	Level 1	Low
Water Damage – Server Room	Water damage to computer equipment	Level 2	Moderate
Hardware failure	Failure of any computer hardware component of the RKS	Level 4	Low
Malicious Damage – Computer Equipment	Deliberate damage or destruction of all computer equipment in the Administration Office	Level 4	Low
Theft – Computer Equipment	Theft of ERMS Servers in Administration Building	Level 4	Low
Destruction of electronic data	Accidental or malicious destruction of computer data	Level 4	Low

3.1 Inventory of Assets

The following tables detail all the components of the RKS that require safeguarding. A ranking is given to each component to indicate the priority that should be given to each during any recovery activities. The inventory also provides details such as the format/operating system, location/host computer, custodian and security classification of each component.

3.1.1 Electronic Components

Item	Ranking	Operating System	Custodian	Security Classification
SynergySoft Software	1	Windows Server 2016 Standard	Focus Networks, Perth	Restricted
Shared Work Files F Drive	2	Windows Server 2016 Standard	Focus Networks, Perth	Sensitive
Electronic Mailboxes	3	Windows Server 2016 Standard/Exchange	Focus Networks, Perth	Sensitive
Personal Work Files	4	Windows Server 2016 Standard	Internal	Sensitive

3.1.2 Physical Components

Item	Ranking	Format	Location	Custodian	Security Classification
Property Files	1	Paper / Electronic	Compactus / RKS	Rates	Sensitive
Administration Files	1	Paper / Electronic	Off-site facility/ RKS	Senior Admin	Sensitive
Reserve Files	1	Paper / Electronic	Compactus/ RKS	EMTS	Sensitive
Delegation Register	1	Electronic	RKS	CEO	Sensitive
Town Planning Schemes	1	Electronic	RKS	CEO	Sensitive
Roads Files	1	Paper / Electronic	RKS	EMTS	Sensitive
Building Licenses	1	Paper / Electronic	Compactus / RKS	TS Admin	Restricted
Minute Books (Vital Records)	1	Paper / Electronic	Fire proof safe / RKS	Senior Admin	Public
Burial Register (Vital Records)	1	Paper	Fire proof safe	Senior Admin	Public
Personnel Files (Vital Records)	1	Paper / Electronic	CEO Office / RKS	CEO	Restricted
Payroll Files (Vital Records)	1	Electronic	RKS	Finance Officer	Restricted
Tender Register	1	Electronic	RKS	CEO	Restricted
Councillor Files	1	Electronic	RKS	Senior Admin	Restricted
Legal Agreements (Vital Records)	1	Paper / Electronic	Fire proof safe / RKS	CEO	Restricted
Lease Agreements (Vital Records)	1	Paper / Electronic	Fireproof safe / RKS	CEO	Restricted
Engineering Maintenance Files	1	Paper / Electronic	Operations / RKS	EMTS	Sensitive
Server Backup Tapes / Logs	1	Disk & Tapes	Fire proof safe / offsite facility	Admin Assist	Sensitive
Government Gazettes	1	Electronic	RKS	Senior Admin	Public
DOLA Maps	1	Paper	Map cupboard	EMTS	Public
Reserve Maps	1	Paper	Map cupboard	EMTS	Public
Locality Maps	1	Paper	Map cupboard	EMTS	Public
Recreation Files	1	Electronic	RKS	TS Admin	Sensitive
Environmental Files	1	Electronic	RKS	EHO	Sensitive
Councillor Enquiries	1	Electronic	RKS	Senior Admin	Sensitive
Works Requests	1	Electronic	Depot / RKS	EMTS	Sensitive
Council Property Files (Vital Records)	1	Paper / Electronic	Compactus / RKS	Senior Admin	Public
Archived Files	1	Paper	Off-site facility storage	Senior Admin	Sensitive
Temporary Storage Files	4	Paper	Off-site facility storage	Senior Admin	Sensitive

3.2 Disaster Recovery Requirements

Five major disastrous events have been identified that would impact the Council's RKS. These events have been ranked by the level of severity of the disaster should it occur, with level one being the highest and level five being the lowest. This section of the disaster recovery manual describes these five event levels.

3.2.1 Level 1: Civic Administration Centre compromised

The total compromise of the Administration Building due to a major event such as fire, flood, earthquake or bombing, although highly unlikely, is a risk for the Shire. The compromise of the Civic Administration Building has been categorised as a level one event and would have an extreme impact on nearly all areas of operation within the Council.

The required recovery for an event of this magnitude would possibly need to include alternative accommodation, furniture, office equipment, information technology infrastructure and additional staffing, as well as the recovery of the Council's Record Keeping System.

3.2.2 Level 2: Paper Loss

The loss or damage of paper records due to fire, smoke or water damage has been categorised as a level 1 event.

Require Recovery Time: If no electronic copy: Never

3.2.3 Level 3: Server Room Compromised

The compromise of the Server Room in the Administration Building due to a localised event such as fire or flood has been categorised as a level 3 event.

Required Recovery Time: 1 day – 1 Month

3.2.4 Level 4: Server Failure

The failure of a Server (with the computer room) due to an event such as hardware failure, theft or malicious damage has been categorised as a level 4 event.

Required Recovery Time: 1 hour – 1 Week

3.2.5 Level 5: Data Loss

The loss of data from the Server (with the Server hardware) due to an event such as accidental or malicious destruction of data has been categorised as a level 5 event.

Required Recovery Time: 30 min – 1 Day

3.3 Disaster Counter Measures

The Shire of Wandering has developed and implemented counter measures to ensure the protection of the Shire's Record Keeping System, as detailed below. Some of these measures are preventative in nature, to avoid a disaster from occurring in the first instance, and others will aid in the recovery of the system should a disaster occur.

3.3.1 Logical security electronic records

Authorised and authenticated users only can access computer server data storage. All authentications are performed on a username and password basis. In all cases the authentication either directly or indirectly is performed by Windows 2008R2 Domain Controller. A strong password policy has been implemented on the Domain Controller that ensures users change their password annually under strict criteria.

3.3.2 Physical security electronic records

The Shire of Wandering currently utilises one physical server, located in the Administration Building's server room and kept behind locked doors, with limited access.

All data relating to the RKS is backed up to tape media. Full daily backups (stored on tape) are rotated weekly. Monthly backups are retained for one year.

3.3.3 Physical Security Vital Records

The majority of vital records are held electronically with hard copies stored in secured, fire retardant compactus and off-site sea container.

Restricted access records can only be viewed by duly-authorised staff members.

3.3.4 Environmental Controls

The server is housed in an air-conditioned environment, however no humidity controls are in place. Uninterruptible Power Supplies (UPS) are installed for all computer server equipment, providing power filtering and backup. Automated shutdown, in the event of a prolonged power outage, is provided for computer servers in the Administration Building.

Archived paper records are stored in a sealed sea container.

3.3.5 Security copies of vital records

The creation of security copies of records is the Shire's best defense in the event of a disaster. Security copies are stored in a separate location to original records so that in the event of the original being destroyed or damaged in a disaster, the security copy can be retrieved and used to replace the original record. It is essential that security copies are stored a significant distance from the original so that both are not destroyed by the same event. Security copies should be subjected to the same security and storage conditions as the original records.

- Duplication of Electronic Records: All documents stored in the Shire's Electronic Record Keeping System are backed up daily.
- Duplication of Vital Hard Copy Records: Hard copy vital records must be identified and duplicated on a regular basis. Hard copies of Lease contracts and Agreements are stored at the off-site storage facility.

4 Disaster Recovery Strategy

Upon the identification of a disaster affecting the Shire's Record Keeping System, the Customer Service Coordinator and the CEO are to be immediately contacted. These staff should then commence the recovery strategy detailed in this section of the plan.

4.1 Switch to emergency backup operating mode

The first task of the Customer Service Coordinator is to immediately switch the RKS to the emergency backup-operating mode. The following steps should be followed:

- Evaluate the extent of damage to the RKS and select an appropriate RKS Continuity Procedure (See Section 7.7 for details)
- Assemble appropriate staff to discuss continuity plan
- Implement the relevant continuity procedures
- Notify all staff of system unavailability

4.2 Plan Recovery

The following steps should then be followed prior to the commencement of the recovery activities:

- Immediately assemble all relevant staff
- Evaluate extent of damage or loss
- Determine recovery tasks required
- Notify all RKS stakeholders of recovery strategy and estimated time frame for recovery

4.3 Implement appropriate recovery operations

As a guide, the following recovery operations should be executed by the Customer Service Coordinator. Different operations have been selected depending on the level of the event.

During recovery operations a recovery team will be established, and will meet regularly. Communication should be channeled through the Customer Service Coordinator. At the completion of the selected recovery strategy a debriefing will be held and a full report produced detailing the recovery operations and any recommendations regarding improvements to the Disaster Recovery Manual.

4.3.1 Level 2: Paper Loss:

In the event of the loss or damage of paper records, the following recovery steps should be taken:

- Stabilise affected record storage area
- Assess damaged records for restoration
- Identify local freezer storage if required for wet records and transfer immediately
- Contact restoration services company if required
- Transfer damaged records requiring repair to restoration company
- Locate and retrieve security copies (if available) from off-site storage facility
- Arrange duplication of security copies
- Return security copies to off-site storage facility
- Replace lost records with duplicates
- Return restored records
- Prepare a final listing of records that are unrecoverable

4.3.2 Level 3: Computer Room Compromised:

In the event of the failure of one or more servers in the computer room, CEO will implement the ICT Disaster Recovery Procedure.

4.3.3 Level 4: Server Failure:

In the event of the failure of a server, with the computer room stable, the CEO will implement the ICT Disaster Recovery Procedure.

4.3.4 Level 5: Data Loss:

In the event of loss of data from the Server, with the Server hardware stable, the CEO will implement the ICT Disaster Recovery Procedure.

4.4 Return to Normal Operating Mode

Once all the essential recovery activities are completed, the steps below should be followed to return the RKS to normal operating mode:

- Cease RKS Continuity procedures and return to RKS to normal mode
- Notify all staff of system availability
- Load document metadata generated during system downtime

4.5 Disaster continuity procedures

Shire of Wandering will develop a Business Continuity plan in the 2021/2022 financial year, which is to be used during any extended period of system downtime during office hours to ensure the continued processing of records into the Record Keeping System and delivery of records to Council staff. Three separate continuity procedures will be used for different types of system problems, as described below. A combination of these individual procedures may be required.

4.5.1 Electronic Record Keeping System Down

In the case of the Electronic Record Keeping System not being available to store and retrieve records, the following procedure should be implemented:

- Date and Stamp incoming mail items
- Write File Number and Action Officer on the document
- Photocopy the document
- Input the details of the original documents into a Spreadsheet on the local PC or laptop
- Print out the document list and put aside with the originals in date order and store in the fireproof safe
- Process the mail as per normal procedures distributing the copies of the documents to staff
- Once the Electronic Records Keeping System is reinstated, input all the original documents in date order following normal registration procedures.

4.5.2 Network down

In the case of the computer network not being available, the above-mentioned procedure should be followed.

4.5.3 All PCs down

In the case of all computers and copiers not being available due to a power outage, the Shire's backup power generator will automatically start up within 5min and restore complete power to the site.

4.6 Disaster recovery responsibilities

The following matrix identifies the positions responsible for the various activities that must be performed as part of the RKS Disaster Recovery Plan.

Activity	Responsible Officer	Frequency
Backup of all data on Servers	Focus Networks, Perth	Every business day
Security and integrity maintenance of servers	Focus Networks, Perth	Daily
Administration building security	CEO	Daily
Administration building safety	CEO	Daily
Review Disaster Recovery Plan	CEO	Annually

4.7 Disaster recovery resources

Dependent on the nature and severity of the disaster, the following resources may be required to restore the Council's RKS. The table below details the source, location and availability of each item.

Item	Location	Availability
RKS Disaster Recovery Plan	Electronic – Shire website Hard copy - Fireproof Safe	Immediately
RKS Disaster Recovery Plan (Backup)	Off-site facility	15 minutes
Vital Records Copies	Double locked strongroom accessible to administration staff. Scanned and held on electronic file in Synergysoft	Immediately
Backup Tapes (older than 5 days)	Offsite - Focus Networks	15 minutes
Backup Tapes (within previous 5 days)	Offsite - Focus Networks	15 minutes

4.8 Disaster Recovery Plan training program

All members of the RKS Disaster Recovery Team will be trained in the operation of the RKS Disaster Recovery Plan and associated procedures. Training will be conducted annually.

4.9 Disaster Recovery Plan testing program

All members of the RKS Disaster Recovery Team will be involved in the testing of the RKS Disaster Recovery Plan and associated procedures as a part of the annual Business Continuity Plan testing. The RKS Disaster Recovery Plan is to be refined if any inadequacies or inefficiencies are discovered during testing.

5 Appendices

5.1 Shire of Wandering Information Technology Disaster Recovery Plan

5.1.1 Definition of a disaster

As a result of fire, water or other hazard (physical or otherwise) there is damage or shutdown that results in the Shire of Wandering administration being unable to have access to its computer services for the immediate future.

5.1.2 Prerequisites

In order for disaster recovery to be effective it is agreed that:

- An adequate backup of data should be lodged off-site. This will include all system data and electronic data normally stored on Wandering Shire Council's server network.
- Sufficient free space will be set aside on computer systems to handle any loaded data.
- Insurers for the Shire will be made fully aware of these arrangements.
- A supply of up-to-date stationery will be stored for printing.

5.1.3 Focus Networks – IT Service

Loan computers are available free of charge, at the discretion of Focus Networks, to ensure that disruption to Wandering Shire Council's business is kept to a minimum while equipment is repaired or replaced. This includes Switches, Monitors and Laser Printers and other components vital to the running of the Shire's business.

Focus Networks can arrange urgent supply of replacement computer and IT equipment, usually within 3-4 working days. This is based on replacing existing equipment as part of the network diagram supplied.

Focus Networks has a pre-built server on site, which will suit the needs of the Shire client base who they support. From this point Focus Networks will simply need to install drives with the correct Operating System (OS) prior to importing any saved data and system software.

Following the installation of either or loan IT equipment, the process for the retrieval of the Shire's remote data stores is as follows:-

5.1.4 Restoring to a new machine (Disaster Recovery)

Focus Networks has the software and license keys at their site so the relevant OS can be installed to the loan server which is a spare server set up at their premises.

5.1.5 Backup and Recover of Server and System Data

Two types of backups occur:

- 1) Internal shadow copies, performed twice a day at around 7am and 12pm, copies of the Shire data are shadowed to a fixed hard drive inside the server, so this is NOT offsite. When documents are lost, or accidentally deleted this provides a quick avenue to copy the files back to the Shire Data folder. This has been performed on a couple of occasions to recover lost files, so we can consider it tested.
- 2) System Backups – automatic back up of critical files for the Operating System, email (Exchange) and data (both Synergy and Shire Data) occur each evening. Reports are generated that are reviewed by our IT service provider – Focus Networks. They verify the logs and determine any fault and course of action to rectify. These reports are also provided to the CEO on a monthly basis.