

WEST RAND DISTRICT MUNICIPALITY



BUSINESS CONTINUITY AND ICT DISASTER RECOVERY PLAN

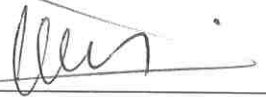
<u>NAME AND POSITION</u>	<u>DATE</u>	<u>SIGNATURE</u>
M E Kolozi	10/12/2024	

Table of Context

1. DISASTER DEFINITION 1

2. INTRODUCTION..... 1

3. PURPOSE..... 1

4. OBJECTIVES 1

5. SCOPE 1

6. DISASTER RECOVERY STRATEGY 2

7. DISASTER RECOVERY ACTION PLAN..... 3

8. DRS BACKUPS..... 3

9. FUNCTIONAL TEAMS AND RESPONSIBILITIES 6

10. TESTING THE DISASTER RECOVERY PLAN 8

11. MAINTAINING THE PLAN 8

1. DISASTER DEFINITION

TERM	DEFINITION
MM	Municipal Manager
WRDM	Shall mean the West Rand District Municipality
ICT	Information and Communication Technology
DRP	Shall mean Disaster Recovery Plan
BRP	Shall mean Backup Resumption Plan
Disaster	Shall mean any event that prevents the ICT systems from providing services needed by the participating applications for a period of 72 hours or longer.
DRS	Shall mean Disaster Recovery Site
DR	Shall mean Disaster Recovery

2. INTRODUCTION

The ICT Department has been mandated to be the main custodian of the ICT Systems, Hardware(s) and Software(s) in the Municipality. The ICT department is responsible for hardware, software, data, servers, firewalls, and business applications and ensures that they are all functioning to optimal levels of efficiency, that the networking and telecommunications are available to users at all times. Conditions that could be declared a disaster include, but not limited to extended electrical power outage to the computer server room, extensive fire, smoke, and water or explosion damage to computing equipment.

3. PURPOSE

This Disaster Recovery Plan documents the ICT Disaster Recovery Program for recovering ICT systems operations after a disaster. The plan describes the preparation and actions required to effectively respond to a disaster, assign responsibilities and describe procedures for testing and maintaining the plan.

4. OBJECTIVES

The primary objective of Disaster Recovery Plan is to protect WRDM in the event that all or part of its operations or computer services is rendered unusable. Preparedness is the key. The planning process should minimise the disruption of operations and ensure some level of organisational stability and an orderly recovery after a disaster.

Other objectives of the Disaster Recovery Plan included:

- Providing a sense of security
- Minimize risk of delays
- Guaranteeing the reliability of standby systems
- Providing a standard for testing the plan

5. SCOPE

This Disaster Recovery Plan is focused only on the municipal-owned and managed ICT systems. This plan addresses all preparation and steps necessary to restore processing or those systems

so that the participating applications can continue processing after a disaster has rendered any or all the systems inoperable.

6. DISASTER RECOVERY STRATEGY

Should the ICT systems encounter a disaster that prevents them from functioning; ICT unit and ICT service providers should be prepared to provide adequate computational, data storage and data communications services remotely from disaster recovery site for the participating applications.

The off-site disaster recovery site is a fully operational Munsoft Data Centre and that is prepared to host the Munsoft Financial Management Systems and Payday and Microsoft business applications as needed remotely though limited VPN access.

In the event that the main WRDM server room becomes dysfunctional, Munsoft Data Centre would be used to offer network and application services to critical users.

ICT together with Risk Coordinators, support Coordinator and Network Administrator, shall assume the role of Disaster Recovery Coordination and shall be responsible for:-

- Organising quarterly scheduled tests of the disaster/data recovery procedures
- Maintaining and updating the Disaster Recovery Plan based on changes in user requirements, personnel, hardware and software configurations and the results of disaster recovery tests and plan reviews; and
- Orchestrating the execution of the Disaster Recovery Plan where a disaster has been declared.

ICT Risk Coordinators and Network Administrator, shall be designated as the Disaster Recovery Technical Support Coordinator for each of the processing systems covered by this Disaster Recovery Plan. The Disaster Recovery Technical Support Coordinators' responsibilities shall include:

- Assisting the participating application users in preparing for the disaster recovery test events;
- Serving as liaison for the participating application users during the disaster recovery tests (by assisting users in resolving errors in jobs, reporting communications problems to the test of the Disaster Recovery Team and answering disaster recovery testing questions in general); and
- Assisting the participating application users in preparing their applications to run successfully at the Disaster recovery site in the event of a disaster.

Enhancement of disaster recovery capabilities is the responsibility of all ED's and managers.

7. DISASTER RECOVERY ACTION PLAN

Backup and off-site storage procedures for Munsoft Financial Management System, Payday and Microsoft Servers shall be as follows:

- Daily back-ups are done from Monday to Sunday
- Daily incremental backups
- Systems configuration information is backed up and stored off-site as well

8. DRS BACKUPS

8.1 MUNSOFT BACKUP SERVER

The Munsoft financial system, payday and HR are backed up offsite on a daily basis. In case of disaster, the latest copy of the backup taken daily, will be uploaded on to a loan server at the service provider premises and remote access will be given.

8.2 MICROSOFT BACKUP SERVER

Data stored on Microsoft servers are backed up on-site and offsite, this is a backup and restore server, meaning it is not mirrored or replicated. Its purpose is to backup and restore data to another server if the main server breaks down, restoration tests are performed quarterly with a restore certificate issued to confirm successful restores.

8.3 NETWORK SHARES

Creation of network shares per department per user is an effort to save not only financial/accounting data, but also business information that is critical to departments and users alike. In the event of hard drives crashing or in the event of theft, individual business files that are on "My Documents" can be restored from the backup or the network share.

8.4 OFF-SITE STORAGE SERVICES

Most municipalities in South Africa have contracts with service providers to provide secure off-site storage services. Service provider has to have fire proof strong room that meets the acceptable standard for secure storage.

WRDM has a contract with Munsoft to provide offsite storage of financial system, HR and Payroll and data stored on their premises.

8.5 OTHER IMPORTANT SECURITY POINTS OF CONCERN – RECOMMENDATIONS

SITE – ACCESS CONTROL

Physical security of the systems servers is critical. Theft of important servers may be disastrous and can cause loss of time and money to the Municipality.

For that reason, the following measures should be implemented to minimise risk:

- The ICT server rooms have limited physical access control;

- The ICT environment power supply to critical systems, is protected with UPS and generators;
- The ICT environment humidity, ventilation and air-conditioning are controlled; and
- The ICT environment (server rooms) is protected by fire detection and suppression

DISASTER RESPONSE TEAM STRATEGY AND TEAM ROLES

- Damage Assessment Team – assess the damage to the ICT systems to determine if a disaster can be declared and determination of disaster phase.
- Damage assessment team – contact team members.
- Damage assessment team – make a decision to formally declare a disaster and notify executive management / Municipal manager.
- Operations team – Contact service provider to confirm available backups.
- Operations team – notify the off-site storage facility, municipal top management and the ICT service providers of the disaster declaration.
- Operation Team – work with the service provider staff to restore municipal operating systems and applications and establish the communications.
- Operations team – Reconstruct the servers at main office.
- Operations Team – conduct preparations to resume operations at the main server room.

8.6 DRS HARDWARE AND SOFTWARE CONFIGURATION

The standard ICT hardware and software infrastructure at DRS should include servers and network infrastructure for data communications.

The following are major hardware components of the disaster recovery site:

- Servers with sufficient processor speed and memory capacity;
- Be virtualised;
- Sufficient disk storage;
- At DRS, the functions of the multiple servers are consolidated in one machine;
- The following have to be provided to support data communications to the DRS:
 - Network Control Centre for communication support to server and workstations;
 - Dedicated internet line with appropriate routers, switches and firewalls for IP communication to ensure access to critical applications like Munsoft/payday/Hr.

8.7 RESUMING NORMAL OPERATIONS / BUSINESS CONTINUITY

While recovery operations are on-going, teams will be managing the restoration or rebuilding of the main server and network infrastructure in the main building.

RECOVERY TIME OBJECTIVE

This is the maximum tolerable time allowed to recover a system after disaster has been declared, this could be failure of server, networks, storage, telephony etc, for successful implementation of DR and BC, RTOs must be established.

RECOVERY POINT OBJECTIVE

This is the measure of acceptable data loss recorded by time, or maximum allowed age of the data when recovering a system, for successful DR and BC, RPO must be established.

BUSINESS IMPACT ANALYSIS

BUSINESS IMPACT ANALYSIS (BIA)			
SERVICE / SYSTEM	AFFECTED DEPARTMENTS	RECOVERY TIME OBJECTIVE (RTO)	RECOVERY POINT OBJECTIVE (RPO)
MUNSOFT	Finance	24hrs	48hours
PAYDAY / HR	Payroll and Human Resource	24hours	48hours
FILE STORAGE	All Departments	48hrs	120hrs
EMAILS	All Departments	72hrs	120hrs
TELEPHONES	All Departments	24hrs	24hrs
NETWORK CONNECTIVITY	WRDM and Libraries	48hrs	48hrs
INTERNET CONNECTIVITY	WRDM and Libraries	72hrs	72hrs

Business and ICT SERVICE CONTINUITY

Business continuity refers to the ability of the municipality to resume normal ICT operations from a systems point of view after a declaration of disaster at institutional level, regional level, provincial and national level at any given time.

Disaster in the WRDM shall consist of three phases:

Phase1 – Disaster does not require employees to vacate the premises.

In this phase, declaration of disaster does not require vacation of premises, the WRDM will assume normal operations based on the damage / disaster assessment.

Phase 2 – Disaster requires all employees to vacate the premises.

In this phase, the disaster will require vacation of premises, business continuity procedure will be invoked in which critical staff in specific directorates will be identified, offered alternative laptops if needed, 3G cards and VPN access to continue work remotely, for services that require VPN access e.g.: financial system, payroll and HR system. Services that require regular internet access e.g., website access and email through outlook and / or outlook web access / Zimbra web client will continue to function. This phase will also enable the institution to hold online virtual meetings using Microsoft teams or Zoom as a collaborative platform.

Phase 3 – Disaster requires all employees to vacate the premises and on-site infrastructure is rendered inaccessible.

Phase 3 disaster will invoke business continuity procedure in which critical staff in specific directorates will be identified, offered alternative laptops if needed, 3G and VPN access to continue work remotely, the financial system will migrate all recently backed up data, restore it in their premises, offer VPN access and account credentials for systems hosted at their premises. This phase will also enable the institution to hold online virtual meetings using Microsoft teams or Zoom as a collaborative platform. Phase 3 disaster does not cater for mail access and website access as the applications are not yet cloud based but self-hosted.

8.8 SECURITY

While operating at the DRS, information security will be assured by firewall restrictions and the security controls on the DRS host systems which will be configured in accordance with the policies and procedures governing ICT systems in the Municipality. As processing continues at the DRS, the DRS host systems will be closely monitored to ensure systems are not compromised.

9. FUNCTIONAL TEAMS AND RESPONSIBILITIES

The following subsections describe each functional team's role as well as its responsibilities in preparing for and responding to a disaster. The responsibility for planning, coordinating and managing this program is assigned to the Disaster Recovery Coordinator with assistance from technical advisors.

9.1 DAMAGE ASSESSMENT TEAM

The Damage Assessment Team assesses the extent of the damage to the server room, reports to the MM and makes recommendations on declaring a disaster.

Title	Contact Number
Manager: ICT	083 267 8816
Network Administrator	071 351 2546
	NA
Coordinator: 107 Centre	083 267 8814
ICT Support Technician	071 600 9709
ICT Support Technician	071 163 0519

Coordinator: Risk	071 351 6791
-------------------	--------------

The major pre-disaster responsibility is to determine appropriate considerations / criteria for identifying the extent of the damage and the estimated duration of the outage.

The disaster responsibilities and actions are:

- Receive the first alert regarding the disaster;
- Ensure that the Department Public Safety have been notified;
- Coordinate with the security personnel and / or fire department to provide for safety, security and access to the damaged facility;
- Assess the damage to each area of the computer facility; and
- Brief the MM or alternate, communicating the recommendation(s).

9.2 OPERATIONS TEAM

The Operations Team assists in the recovery operations and manages the operations of the computer systems at the DRS.

Title	Contact Number
Manager: ICT	083 267 8816
Network Administrator	071 351 2546
	NA
Coordinator: 107 Centre	083 267 8814
ICT Support Technician	071 600 9709
ICT Support Technician	071 163 0519

The pre-disaster responsibilities are:

- Ensure that appropriate backups are made.
- Ensure all configurations are store offsite.

The disaster responsibilities and actions are:

- Provide assistance to the Restoration Team in the restoration of the system software and customer files, as required.
- Run system and operation jobs, as required.
- Implement and maintain a problem log.
- Provide information to the Customer Support Team regarding the status of the system operations, and the customer jobs.
- Effect the transfer of media and print output from the DRS to suitable customer pickup location(s).
- Coordinator the shutdown of the DRS operations and the transfer back to the server room

10. TESTING THE DISASTER RECOVERY PLAN

Testing and exercising the Disaster Recovery Plan helps to verify that the recovery procedures work as intended and that the supporting is accurate and current. Testing also provides an opportunity to identify any omissions in recovery procedures or documentation and to determine whether personnel are adequately prepared to perform their assigned duties. Therefore, ICT regularly schedules exercises of its Disaster Recovery Plan. DR test certificates are issued out to the WRDM once the service provider has performed the tests on their side as well and DR test repots will be developed once tested by the WRDM teams.

10.1 DRS TEST PROCEDURE

ICT schedules two (2) DRS tests per year.

11. MAINTAINING THE PLAN

The Disaster Recovery Coordinator of the DRS is responsible for the maintenance of this document. The plan is updated as needed:

- in response to events such as office moves, telephone number changes, new personnel joining the Municipality, retirements, duty changes and additions or deletions of participating applications;
- after each DRS test to reflect the recommendations resulting from the post-test wrap-up debriefings; and
- after a periodic review of the plan
- all changes of the DRP will have to be noted and attached to this document.

As sections of the plan are updated, the revised sections are posted to the municipal intranet to ensure the most current information is available to DR team members. DR participants are notified of the changes and are encouraged to produce printouts for their copies of the disaster recovery plan.

Additionally, the plan will be updated in the event an actual disaster occurs. The plan will be reviewed and updated at a convenient point after the initial responses to the disaster have been completed.

12. DRP REVISION

The Disaster recovery plan will be reviewed biennial.