

**ELIAS MOTSOLEDI LOCAL  
MUNICIPALITY-MASEPALA WA SELEGAE**



**DISASTER RECOVERY PLAN**

MUNICIPAL COUNCIL RESOLUTION NUMBER

M24/25-07

APPROVED AT THE COUNCIL SITTING OF 30 AUGUST 2024

MR M.D

## TABLE OF CONTENT

1. Introduction
  - 1.1 Definition of terms
  - 1.2 Objective of plan
  - 1.3 Scope of plan
  - 1.4 Responsibility for plan management and administration
  - 1.5 Plan for IT disaster recovery
  - 1.6 Plan for business continuity
2. Disaster notification, plan activation and initiation procedure
  - 2.1 Damage assessment
  - 2.2 Determination of strategy to be followed
  - 2.3 Activation of recovery site
  - 2.4 Movement of backup materials
  - 2.5 Notification of staff involved
  - 2.6 Ordering of new equipment
  - 2.7 Details of disaster recovery team
3. Primary site procedure
  - 3.1 Establish site security
  - 3.2 Perform detailed damage assessment
  - 3.3 Obtain contractor and vendor estimates for repairs and replacements
  - 3.4 Compile salvage / refurbishment plan
  - 3.5 Monitor progress
4. Re-establishment of normal operations
  - 4.1 Order replacement furniture and equipment
  - 4.2 Install and test equipment
  - 4.3 Back up prior to move
  - 4.4 Recover and test operating systems and applications
  - 4.5 Control and monitor completeness and accuracy of migration
  - 4.6 Process backlog
  - 4.7 Configure and test network
  - 4.8 Return to normal processing
5. Post-recovery review
  - 5.1 Conduct post recovery review
  - 5.2 Update plans if necessary
6. Plan maintenance and testing
  - 6.1 Responsibility for maintenance and testing of DRP
  - 6.2 Training of staff in DRP procedures and responsibilities of staff members
  - 6.3 Plan maintenance
  - 6.4 Testing the DRP



## 1. Introduction

The Information and Communication Unit has been mandated to be the main custodian of Information Technology systems, hardware and software within the municipality. The ICT Unit is charged with ensuring that the ICT hardware and software, data, servers, firewalls and business applications are all functioning at optimal levels of efficiency and that the networks and telecommunications are available to users at all times.

Events that might be classified as a disaster include but not limited to:

- Extended electrical power outage to the computer server room or municipal offices
- Extensive fire to computer equipment
- Extensive smoke to computer equipment
- Extensive water to computer equipment
- Explosion damage to computer equipment or municipal offices
- Human sabotage (stakeholders that pose threats)
- Heavy winds and storm damage
- Extensive lightning damage to computer equipment

### 1.1 Definition of terms

- MM Municipal Manager
- EMLM Elias Motsoaledi Local Municipality
- ICT Information and Communications Technology
- DRP Disaster Recovery Plan
- BRP Backup Resumption Plan
- Disaster Event that prevents ICT systems from providing services needed by the participating applications for a period of 72 hours or longer
- DRS Disaster Recovery Site
- IT Information Technology
- CFO Chief Financial Officer
- ISO Information Systems Officer
- DMT Disaster Management Team

### 1.2 Objective of plan

The primary objective of the Disaster Recovery Plan (DRP) is to develop a business continuity plan to protect EMLM in the event that all or part of its operations, or computer systems is rendered unusable. The planning process should minimise the disruption of operations and ensure some level of organisational stability and an orderly recovery after a disaster.

h/r  
M.D

Additional objectives of the DRP include:

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

### **1.3 Scope of plan**

The DRP is focused only on the ICT systems owned and managed by the municipality. It addresses all preparations and steps necessary to restore processing on those systems so that the participating applications can continue processing after a disaster has rendered any or all the systems inoperable.

### **1.4 Responsibility for plan management and administration**

In the event that the ICT systems are prevented from functioning due to a disaster, the ICT unit and ICT service providers should be prepared to provide adequate computational data network storage and data communications services and facilities at an offsite disaster recovery site for the participating applications.

The off-site disaster recovery site should be a fully operational Financial Management System enabled data centre, that is prepared to host the Financial Management Systems, Payroll applications, Domain controller, Mail Exchange and user data as needed.

The ICT manager, Risk manager, Network administrator, Systems administrator and Information Systems Officer (ISO) shall be designated as the Disaster Recovery Technical Support Coordinators for each of the processing systems covered by the DRP. The Disaster Recovery Technical Support Coordinators' responsibilities 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 communication problems to the test of the Disaster Recovery Team and answering disaster recovery testing questions in general)
- Assisting the participating application users in preparing their applications to run successfully at the Disaster recovery site in the event of a disaster.
- Manage the information security function in accordance with the established policies and guidelines.
- Function as an internal consulting resource on information security issues.
- Coordinate information security efforts with the Internal Audit Department.



- Provide periodic reporting on information security issues to the Municipal Manager.
- Assist in coordinating contingency plan tests on a regular basis

The ICT manager in conjunction with ICT, Risk manager and Network Administrator and Information Systems Officer (ISO), shall assume the responsibility of the DRP and includes:

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

Enhancement of disaster recovery capabilities is the responsibility of all directors and managers. This includes participating in the periodic DRP tests and communicating with the Disaster Recovery Coordinator regarding significant changes or developments in the applications.

## **1.5 Plan for IT disaster recovery**

The backup and off-site storage procedures for Financial Management System, Payroll system and Network shares shall be as follows:

- A weekly rotational backup strategy is being followed.
- Daily back-ups are done from Monday to Thursday and these are kept in a safe and will be over written in a weekly cycle.
- Weekly backups are done and will be overwritten in the following month.
- Monthly back-ups are done in full and are only over-written in the next year.
- Daily, weekly and monthly back-ups of the Financial Management System are all stored off-site in a strong room at the Service Provider as per the Service Level Agreement (SLA) signed.
- Systems configuration information is backed up and stored off-site.
- In a disaster, all backup drives will be taken to the disaster recovery site for installation and signed test results shall be provided periodically and stored in a safe for audit purposes.
- Quarterly workshops must be conducted to teach users on how to act or react at the time of the disaster.

MR M.D

## 1.6 Plan for business continuity

The municipality has identified a total of three sites that can be used as DRS. The most suitable is however Motetema Satellite Site as the necessary infrastructure required for a server room is readily available.

Live data is available immediately as a mirror server of the current server information will be implemented at the DRS that will allow data to be available immediately once the DRS systems are fully operational.

The following personnel will play active roles in the DRP process –

- ICT Manager
- Systems Administrator
- Network Administrator
- Information Security Officer
- Risk Manager
- Director Corporate
- Municipal Manager

## 2. Disaster notification, plan activation and initiation procedure

In the event of a disaster the Disaster Recovery Coordinator sets the following committees in motion:

- **Damage Assessment Team:**
  - Assess the damage of the ICT systems to determine if a disaster can be formally declared
- **Executive Team:**
  - Make a decision to formally declare a disaster
  - Establish a Disaster Command Post in another municipal building with adequate communications and support equipment
  - Notify the offsite storage facility, municipal top management and the ICT service providers of the disaster declaration
- **Restoration Team, Operation Team and Customer Support Team**
  - Work with the DRS staff to restore municipal operating systems and applications at DRS and establish the communications link to the DRS in preparation for operations at DRS for duration for the emergency, conduct preparations to leave DRS and to resume operations at the main server room
- **Salvage/Reclamation Team**
  - Reconstruct the servers at main office (salvage/reclamation team)

Mr M.D



Municipal Manager (MM) declares that a disaster has occurred, authorises the execution of the DRP and oversees the execution of the plan during the emergency.

## **2.1 Damage assessment**

The Damage Assessment Team assesses the extent of the damage to the Server Room, reports to the Municipal Manager and makes a recommendation on declaring a disaster.

### **The Damage Assessment Team Members are -**

- ICT Manager
- Risk Manager
- Electrical Engineer
- Deputy CFO
- Legal Advisor
- Disaster Management and Emergency Services
- Manager Traffic Department

### **The Recommendation Team Members are -**

- Corporate Services Director
- CFO
- Director Infrastructure
- Director Strategic
- Director Community Services
- Director Planning and LED
- Chief Internal Auditor

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

These Disaster Management Teams responsibilities and actions are:

- Receive the first alert regarding the disaster
- Ensure that 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
- Communicate the recommendations to the MM

## **2.2 Determination of strategy to be followed**

The following strategy is followed:

- MM approves ICT DRP and all material modifications to the plan

- Establish primary and alternate disaster command posts, ensuring that the posts are adequately prepared for a disaster
- Notify the DRS and the off-site storage facility of a possible disaster
- Review the report of the Damage Assessment Team
- Declare a disaster
- Establish the command post and communications
- Activate the Functional Teams
- Inform the DRS of the disaster declaration
- Initiate the transportation of the backup materials to the DRS
- Notify Key Executive Committee (EXCO)
- Report situation and progress to Audit Committee
- Monitor the performance of the Disaster Recovery Teams and the execution and effectiveness of the DRP
- Keep all directors and managers and the designated Information Officer/alternative informed of material/sensitive matters

### 2.3 Activation of recovery site

Motetema has been identified as the Disaster Recovery Site (DRS). This site is situated 14km's from the primary EMLM municipal building. Please see the attached report for the Motetema Satellite Site Survey for the implementing of a Disaster Recovery Site at these offices. The ICT Manager, Information's Security Officer and Risk Manager are responsible for the oversight and monitoring of the process of the Backup Server and Backup Server Room.

#### DRS Hardware & Software Configurations

The standard ICT hardware and software infrastructure at DRS should include:

- Server
- UPS
- Child domain servers
- Advanced Windows Server 2003/8/12
- Network infrastructure for data communications and a work recovery centre.
- Air Conditioners
- Raised server room floor with ramps
- Fire extinguishers
- Server racks
- Telephones
- Monitoring CCTV

The following are major hardware components of the server configuration:

- Server with sufficient processor speed and memory
- Be virtualized

M/R M/D



- Sufficient quantity of backup drives
- Sufficient disk storage
- Sufficient premier capacity
- At the 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 communications link with the appropriate routers, switches and firewalls for IP communication between main office, DRS server and all UPS's and Child Domain Servers.
  - Web redirect services, for Internet connectivity to provide alternative connectivity if the internet line deems inoperable.

## **2.4 Movement of backup materials**

- Information Security Officer and Risk manager is required to initiate the transportation to the backup materials to the DRS.
- Backups will be tested during installation thereof at the DRP site (weekly and monthly)
- Links mirror daily operations
- Store backups at bank or post office
- Automated backup system

## **2.5 Notification of staff involved**

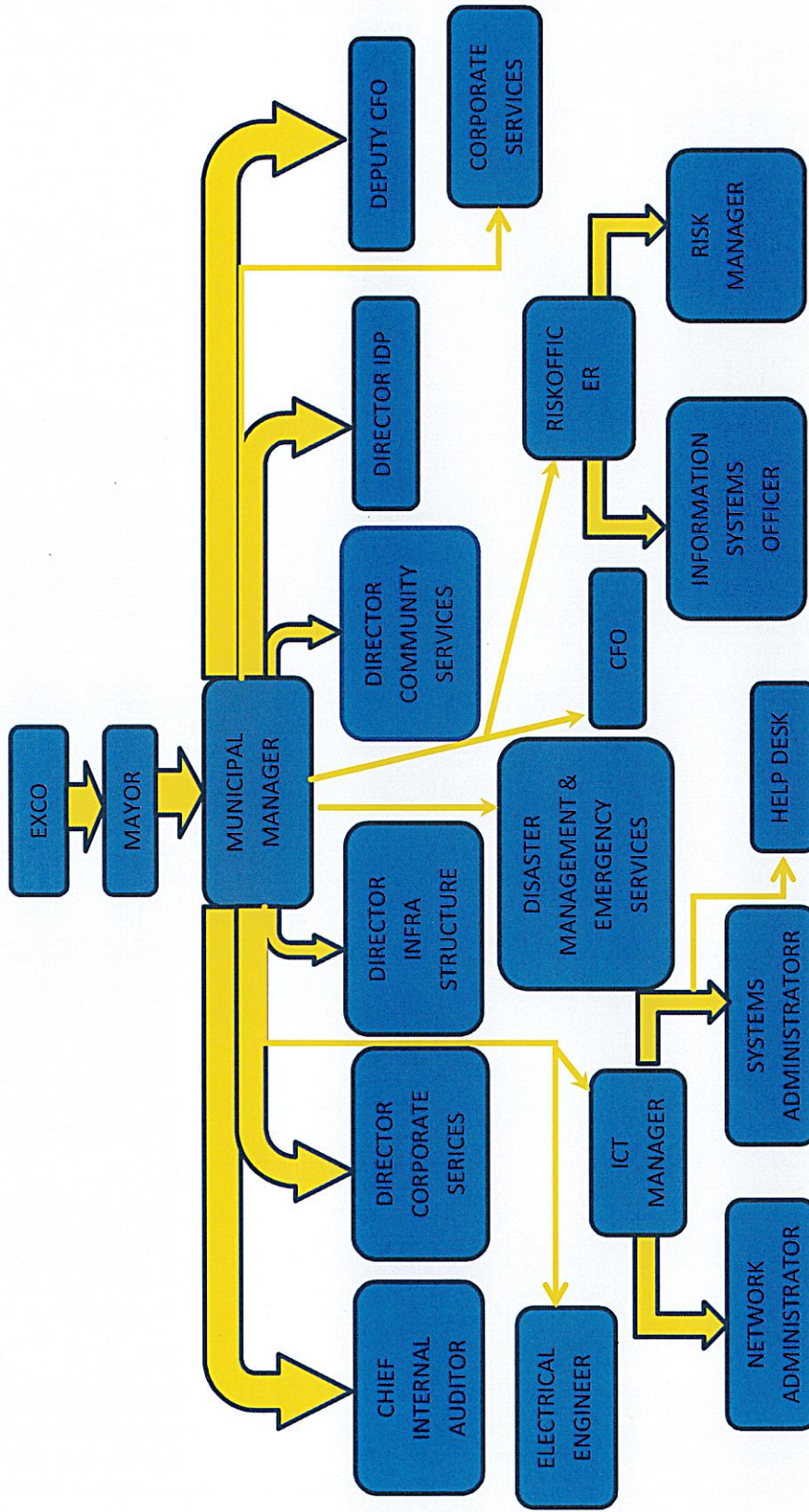
- ICT manager to inform Risk manager
- Convene meeting with DMT and discuss steps to be taken to implement DRP

## **2.6 Ordering of new equipment**

ICT manager, Risk manager and SCM manager to write proposal to deviate from normal SCM regulations due to the nature of the incident, being a disaster and as such an emergency which as per the SCM allows for the deviation from normal SCM regulations to enable equipment being purchased through deviation of the SCM regulations as allowed.

MR M.D

## 2.7 Details of disaster recovery team





### 3. Primary site procedure

#### 3.1 Establish site security

##### Firewalls

- To be compliant with the municipalities current security policy and that they have been compliance tested through regular penetration
- Recognised standard of encryption for all critical communications is used internally and externally. This will go a long way to curb hacking and cyber attacks.

##### Flash Disks

- The use of removable storage devices on desktops is restricted and anti-virus deployed.

##### Anti Virus Software

- Virtual attacks on systems can render them inoperable
- Hence, Antivirus products are deployed at external network entry points, on mail servers and on all desktops and laptops
- Antivirus products are automatically updated when released by vendor and ICT teams ensures regular scans are carried out on users machines
- Laptops are barred from connecting to the network unless they are authorised by ICT Technicians first
- A patch management server is installed and vendor operating systems patches are tested before being applied.

##### 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 this reason, the following measures should be implemented to minimise risk:

- The ICT server rooms have limited physical access control (Biometric Access Control)
- The ICT environment power supply to critical systems is protected with UPS generators
- ICT environment humidity, ventilation and air-conditioning are controlled
- ICT environment (server rooms) is protected by fire detection and suppression
- ICT environment is currently not protected by water detection devices

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 continuous at the DRS, the DRS host system will be closely monitored to ensure systems are not compromised.

### **3.2 Perform detailed damage assessment**

The Damage Assessment Team must provide a report regarding the damage that was caused during the disaster to the primary municipal building. The report must include at least the following information:

- Date damage occurred
- Type of damage
- Areas affected by damage
- Impact of damage caused
- Parties affected by damage

### **3.3 Obtain contractor and vendor estimates for repairs and replacements**

Obtain a list of emergency suppliers from the SCM section to determine which Vendors have the necessary equipment that needs to be replaced and obtain at least three quotations from the different Vendors. Document a proposal to the MM to deviate from the normal SCM regulations due to the fact that the nature of the disaster constitutes an emergency that allows for the deviation from the SCM regulations as stipulated in the SCM regulations. The requirements to enable the municipality to use a specific Vendor as an emergency supplier, is it that the Vendor may not be more than 90km's from the primary site where the disaster occurred.

### **3.4 Compile salvage / refurbishment plan**

The risk assessment team in conjunction with the salvage and refurbishment team need to compile a salvage/refurbishment plan to determine what can be salvaged and what needs to be replaced at the disaster site. This report must be submitted to MM, ICT and Risk assessment to be approved,

### **3.5 Monitor progress**

ICT manager and Risk manager is responsible for the monitoring of the progress of the DRP process. Daily reports will be made available to the MM as the accounting officer to keep the administration up to date with the progress and inform EXCO if there are any new developments that occurred during the implementation of the DRP.



#### **4. Re-establishment of normal operations**

While recovery operations are on-going at the DRS the Salvage/Reclamation Team will be managing the restoration or rebuilding of the main server and network infrastructure in the main building

##### **4.1 Order replacement furniture and equipment**

ICT in conjunction with SCM section must complete the necessary orders at the suppliers who were approved by the MM to purchase equipment lost or damaged during the disaster. Once the orders have been placed the budget finance section needs to be informed of the total amount that needs to be made available for payment due to the occurrence of the disaster.

##### **4.2 Install and test equipment**

ICT manager and team are responsible to draw up a plan regarding the installation of the damaged equipment being replaced. A list of all possible equipment that will have to be replaced is included below to enable management to get an overview of what type of equipment will be required and to enable comparison with the amount budgeted for the implementation of the DRP.

- Servers
- UPS's
- Child domain servers
- Lap tops
- Desk tops
- Networks (Switches & Cabling)
- CCTV Cameras
- Applications
- Programmes
- Biometric Access Control System

##### **4.3 Back up prior to move**

Backup of data at the recovery site to original site  
Standard daily backup process will be followed as per the ICT backup policy.

##### **4.4 Recover and test operating systems and applications**

Test if all applications, data, systems Financial Management System, Payroll system etc. are fully functional.  
Involve Financial Management System vendor as per SLA, and Payroll application vendors for installation.

#### **4.5 Control and monitor completeness and accuracy of migration**

ITC manager, ICT team, Risk assessment manager, CFO, Corporate Director, Risk officer and Internal Auditor will be responsible to control and monitor the completeness and accuracy of the migration. Reporting will be done to the MM and Audit Committee who will then report back to EXCO on the situation at hand.

#### **4.6 Process backlog**

CFO and Debtors Section needs to put a plan in place to address the process backlog regarding the utilities that needs to be delivered and billed on a monthly basis to ensure that normal service is delivered and normal accurate monthly billing is done.

This team will have to report back to the MM on the processes put in place and the monitoring of the execution of these processes.

#### **4.7 Configure and test network**

Network administrator, ICT manager, Systems administrator and ICT Unit will be responsible for the configuration and testing of the networks. The team will report back to MM on the progress of the configuration and testing result.

#### **4.8 Return to normal processing**

Information Systems Officer, ICT Unit and Directors will monitor the processes put in place to return to normal processing after installation of backups. This team will report back to the MM and audit committee who will inform Exco of the progress made and indicate if there are any unforeseen matters that have been identified during this process.

### **5. Post-recovery review**

#### **5.1 Conduct post recovery review**

Damage Assessment Team, Recommendation Team and Directors will conduct a post recovery review to determine if the implementation of the DRP was successful. They will report to the MM on the implementation results and the MM will then report to Exco. If any matters are identified that have not been properly addressed these matters will be addressed as a matter of urgency and once completed the MM will be informed of the status quo.



## **5.2 Update plans if necessary**

The DRP will be a standing item on the ICT Steering Committee meetings agenda and where necessary, amendments will be made and communicated to the entire DRP team and published on the municipality's intranet.

## **6. Plan maintenance and testing**

### **6.1 Responsibility for maintenance and testing of DRP**

The ICT manager, Risk manager, Systems administrator and Network administrator is responsible for the maintenance and testing of the DRP.

Six monthly reports on the results of the testing will be provided to the MM and audit committee to ensure that the DRP is implemented as required.

The MM, Directors and ICT Manager are members of the ICT Steering Committee meeting and will receive first-hand knowledge of the maintenance of the DRP as part of these meetings.

### **6.2 Training of staff in DRP procedures and responsibilities of staff members**

In addition to regular training, team members and managers receive annual refresher training regarding the emergency alert procedures and responsibilities of staff members.

### **6.3 Plan maintenance**

The Disaster Recovery Coordinator or the DMT is responsible for the maintenance of the DRP. This document is updated as needed:

- In response to events such as office moves, telephone numbers changes, new personnel joining the Municipality, retirements, duty changes and additions or deletion of participating applicants
- After each DRS test to reflect the recommendations resulting from the post-test wrap-up debriefings
- After a periodic review of the plan
- All changes to 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 the DR Team Members and DR Participants. These DR Team Members and DR Participants are then 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.

## **6.4 Testing the DRP**

Testing and exercising the DRP helps to verify that the recovery procedures work as intended and that the supporting documentation 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, the ICT Unit must regularly schedule exercises of its DRP at the DRS. Included as Annexure "B" is the process that must be followed and completed when conducting a DRS test.

### **DRS test procedures:**

ICT schedules two DRS tests per year with sufficient time to test the operating system and customer application recovery procedures. The initial hours are dedicated to exercising the system recovery procedures and establishing the communications link. The remaining hours are dedicated to testing the recovery of participating applications. The DRS test are managed and conducted by members of the Restoration Team, the Operations Team and the Helpdesk Team referred to collectively as the DRS team.

Prior to the DRS test, the DRS team determines which backup drives will be used for the tests, establishes the test plan which outlines the DRS Team goals and activities for the given test, conducts the necessary preparations for the test, and assists users in their preparations for the DRS test. (Users set their own DRS objectives). During the tests, in addition to providing customer assistance, the DRS team participants maintain a running log of the test activities to assist in the post-test review.

After every test, the DRS Team participants meet to discuss the tests in order to improve the recovery procedures and the plan documentation. The DRS Team also schedules a meeting with the users to gain their input and suggestions for improvements.

### **DRS test planning**

The following process will be followed by the DRS team:

- Confirm that the DRS mainframe and data communications configuration will meet the DRS needs, and that the DRS will be ready for the test. (Two to three months prior to the scheduled test)



- Set the DRS Team objectives for the test and establish action items for the team in preparation for the test. (At least two months prior to the scheduled test)
- Disseminate information to the user community regarding the test. (Six to eight weeks prior to the scheduled test)
- Confirm that preparatory tasks are being completed and review the schedule of events for the days of the DRS. (Four to six weeks prior to the scheduled test)
- Discuss the final test preparations with the DRS vendor to confirm the DRS configurations to obtain the information required for the mainframe backups and to reconfirm the DRS will be ready. (Two to three days before the scheduled backups prior to the scheduled test)
- Send the backup drives and drive lists to the DRS. (one week prior to the scheduled test)

### **Application testing support**

The DRS Team offers user support during a DRS test to assist the application owners/participants in successfully running the applications at the alternative site. The assistance includes help with test preparations, on-call support during the duration of the test, resolving reported problems and serving as the liaison between the user and the DRS Team. The DRS Team consists of the following members –

- Chief Financial Officer
- ICT Manager
- Coordinator : Network Administrator
- Coordinator : Systems Administrator
- Coordinator : Information Security Officer
- Coordinator : Risk Manager
- ICT Support Technicians
- ICT Website Officer
- Helpdesk Administrator

Complete Annexure “A” for the contact details for DRS Team Members.

### **Test preparation support includes:**

- Ensuring the users have made all appropriate preparations for their data to be available for the DRS
- Ensuring the users are ready for the DRS and have no further questions
- Ensuring users have the necessary contact phone numbers for user support during the DRS

**DRS test support includes:**

- Notifying those users who have not logged on that the disaster system is up and ready for user testing
- Responding to general user questions and to user problem reports, ensuring they are resolved
- Recording all problem reports and general notes to a system status database that is made available to users to read

**Post-Test Wrap Up**

Two debriefings are scheduled on the days immediately following the DRS test. One is for the DRS Team participants to assess the systems software recovery procedures. The second is for the user community who participated in the DRS.

These meetings are general discussions to address:

- Areas where the exercise was successful
- Problems that were encountered
- Suggestions for improvements

Based on the conclusions, and action list of improvements to be made prior to the next test is developed and responsibility for implementing them is assigned.

**DRS Test Schedule**

The bi-yearly tests are scheduled approximately six months apart beginning six months after approval of the DRP.

**POLICY REVIEW**

This Policy shall be reviewed as and when necessary



**ANNEXURE "A"**

**DRS Team Members**

Title	Name	Contact Number
Chief Financial Officer		
ICT Manager		
Coordinator: Network Administrator		
Coordinator: Systems Administrator		
Coordinator: Information Security Officer		
ICT Support Technician		
ICT Support Technician		
ICT Website Officer		
Helpdesk Administrator		
Coordinator: Risk Manager		

MR. M.D.

**Outlining the Disaster Recovery Plan Test Scenario****Outline Scenario**

Test scenario	
Remedial actions required	
Goal(s) of test scenario	
Date of test	
Type of test(s) to be performed	<input type="checkbox"/> Walkthrough <input type="checkbox"/> Simulation <input type="checkbox"/> Parallel Test <input type="checkbox"/> Full-Interruption Testing
People/groups/departments involved in test	
Downtime forecasted	

M.D

~12



ANNEXURE "B"

Assignment of Action Items

Action Item	Person Assigned to Action Item

MR  
M.D

**Testing the Disaster Recovery Plan**

Test Scenario: Walkthrough

**Testing Documentation**

Step	Action	Team	Results/Comments/Time
1			
2			
3			



## ANNEXURE "B"

### Walkthrough Checklist

Step	Walkthrough Checklist	Results
1	Did the recovery team have adequate information to restore the service?	
2	Was the documentation readily available to assist the team?	
3	Were all resources and tools available to do the job?	
4	Were the right people involved on the teams?	
5	How long did it take to restore this service?	

### Test Scenario: Simulation

#### Testing Documentation

Step	Action	Team	Results/Comments/Time
1			
2			
3			

re M.D

**ANNEXURE "B"**

4			
---	--	--	--

**Simulation Checklist**

Step	Simulation Checklist	Results
1	Did the recovery team have adequate information to restore the service?	
2	Was the documentation readily available to assist the team?	
3	Were all resources and tools available to do the job?	
4	Were the right people involved on the teams?	
5	How long did it take to restore this service?	

Mr M.D



**ANNEXURE "B"**

**Test Scenario:** Parallel

**Testing Documentation**

Step	Action	Team	Results/Comments/Time
1			
2			
3			

**Parallel Checklist**

Step	Walkthrough Checklist	Results
1	Did the recovery team have adequate information to restore the service?	
2	Was the documentation readily available to assist the team?	
3	Were all resources and tools available to do the job?	
4	Were the right people involved on the teams?	

MR  
M.D

**ANNEXURE "B"**

5	How long did it take to restore this service?	
---	---	--

**Test Scenario:** Full-Interruption

**Testing Documentation**

Step	Action	Team	Results/Comments/Time
1			
2			

**Full-Interruption Checklist**

Step	Walkthrough Checklist	Results
1	Did the recovery team have adequate information to restore the service?	
2	Was the documentation readily	

MR  
M.D



**ANNEXURE "B"**

	available to assist the team?	
3	Were all resources and tools available to do the job?	
4	Were the right people involved on the teams?	
5	How long did it take to restore this service?	

**Making Changes to the Disaster Recovery Plan**

**Remedial Actions Required**

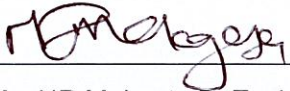
<b>Remedial Action Required</b>	<b>Person/Team Assigned to Action Item</b>	<b>Expected Date of Completion</b>

MR M.D

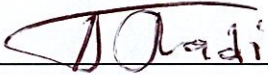
ANNEXURE "B"

--	--	--

**SIGNATORIES**

  
Ms. NR Makgata Pr Tech Eng  
Municipal Manager

30/08/2024  
Date

  
The Mayor  
Cllr. MD Tladi

30/08/2024  
Date