West Rand District

Municipality

Disaster Recovery Plan

Version: 1

<table>
<thead>
<tr>
<th>Role</th>
<th>Signature</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manager: ICT</td>
<td></td>
<td>13/06/2013</td>
</tr>
<tr>
<td>Chief Financial Officer</td>
<td></td>
<td>20/06/2013</td>
</tr>
<tr>
<td>Municipal Manager</td>
<td></td>
<td>20/11/2010</td>
</tr>
</tbody>
</table>
TABLE OF CONTENTS
1.1. Definition of terms
1.2. Background
1.3. Purpose
1.4. Objectives
1.5. Scope
1.6. Disaster Recovery Strategy
1.7. Disaster Recovery Action Plan
2.1 Munsoft Back Up Server
2.2 Disaster Recovery Site
2.3 Network Shares
2.4 Off-Site Storage Services
2.5 Other Important Security Points Of Concern-Recommendations
2.6 DRS Hardware Configurations
2.7 Resuming Normal Operations
2.8 Security
3. Functional Teams And Responsibilities
3.1 Damage Assessment Team
3.2 Management Team
3.3 Restoration Team
3.4 Operations Team
3.5 Customer Support Team
3.6 Salvage/Reclamation Team
3.7 Administrative Support Team
4. Testing The Disaster Recovery Plan
4.1 DRS Test Procedures
4.2 DRS Test Planning
4.3 Application Testing Support
4.4 Post-Test Wrap-Up
4.5 DRS Test Schedule
4.6 Training
5. Maintaining The Plan
1.1 DISASTER DEFINITION

<table>
<thead>
<tr>
<th>TERM</th>
<th>DEFINITION</th>
</tr>
</thead>
<tbody>
<tr>
<td>MM</td>
<td>Municipal Manager</td>
</tr>
<tr>
<td>WRDM</td>
<td>Shall mean the West Rand District Municipality</td>
</tr>
<tr>
<td>ICT</td>
<td>Information and Communication Technology</td>
</tr>
<tr>
<td>DRP</td>
<td>Disaster Recovery Plan</td>
</tr>
<tr>
<td>BRP</td>
<td>Backup Resumption Plan</td>
</tr>
<tr>
<td>Disaster</td>
<td>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.</td>
</tr>
<tr>
<td>DRS</td>
<td>Disaster Recovery Site</td>
</tr>
</tbody>
</table>

1.2 INTRODUCTION

The ICT Department has been mandated to be the main custodian of the IT Systems, Hardwares and Softwares in the Municipality. It is charged with ensuring that the ICT hardware and software, data, servers, firewalls and business applications 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.

1.3 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.

1.4 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
- Minimise risk of delays
- Guaranteeing the reliability of standby systems
Providing a standard for testing the plan

1.5 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.

1.6 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 and facilities at an offsite disaster recovery site for the participating applications.

The off-site disaster recovery site should be a fully operational Munsoft Data Centre that is prepared to host the Munsoft Financial Management Systems and Payday business applications as needed. The second option could be a reciprocal arrangement between Mogale City Local Municipality and West Rand District Municipality whereby a mirrored server would be installed within Mogale City Local municipality disaster recovery site.

In the event that the main WRDM server room becomes dysfunctional, Munsoft Data Centre and Mogale City Local Municipality disaster recovery site would be used to offer network and application services to critical users.

ICT Manager, in conjunction with ICT, Risk Coordinators and Network Administrator, shall assume the role of Disaster Recovery Coordination and shall be responsible for:-

- Organising regularly scheduled, periodic 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 Manager, in conjunction with 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 HOD’s and managers. This includes participating in the periodic Disaster Recovery Plan tests and communicating with the Disaster Recovery Coordinator regarding significant changes or developments in the applications.

1.7. DISASTER RECOVERY ACTION PLAN

Backup and off-site storage procedures for Munsoft Financial Management System, VIP, and Network shares shall be as follows:-

- A two week 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 overwritten in the next two week 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
- Weekly and monthly backups are all stored off-site in the strong room at Protection Services
- Systems configuration information is backed up and stored off-site as well
- In a disaster, all backup tapes will be taken to the disaster recovery site

2.1 MUNSOFT BACKUP SERVER

The Munsoft Backup server is identical to the main server. Its purpose is to mirror the main server so that if the main server breaks down, the backup server takes over. Very little data and time will be lost in this instance.

2.2 DISASTER RECOVERY SITE (DRS)

ICT has to prepare a motivation to Council to request funds to implement DRS for WRDM. DRS will definitely serve as a replication server for the WRDM main and 107 Centre servers.

When all the servers at WRDM and 107 Centre are down, the DRS servers will work as the main server servicing users in both the WRDM and 107 also including users at stations. Data recovered will only be up to the last replication. Similar backup strategy will apply also at the Munsoft Disaster Recovery to offer further redundancy. Cost benefit factor needs to be considered when the motivation is prepared to council either to acquire services of a service provider.

2.3 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 crushing or in the event of theft, individual business files can be restored from the backup or the network share.

2.4 OFF-SITE STORAGE SERVICES

Most municipalities in South Africa has contracts with service providers to provide secure off-site storage services. Services provider has to have fire proof strong room that meets the acceptable standards for secure storage.
WRDM has contract with Munsoft to provide offsite storage of financial system, HR and Payroll.

2.5 OTHER IMPORTANT SECURITY POINTS OF CONCERN-RECOMMENDATIONS

FIREWALLS

➢ To be compliant with the organisation’s 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 usage of removable storage devices on desktops is restricted and anti-virus deployed.

ANTI-VIRUS SOFTWARE

➢ Viral attacks on systems can render them inoperable.
➢ Hence, Antivirus Products are deployed at external network entry points, on mail server and on all desktops and laptops.
➢ Antivirus products are automatically updated when released by vender and ICT team 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.
➢ Due budget constrain WRDM is still without patch management server. Vendor operating systems patches are not 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 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.
➢ ICT environment humidity, ventilation and air-conditioning are controlled.
➢ ICT environment (server rooms) is protected by fire detection and suppression.
➢ ICT environment is not protected by water detection but a motivation needs to be submitted to council.

DISASTER RESPONSE

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

➢ Damage Assessment Team – Assess the damage to the ICT Systems to determine if a disaster can be declared.
➢ Executive Team:- make a decision to formally declare a disaster.
Executive Team: Establish a Disaster Command Post, of necessary, in another Municipal building with adequate communications and support equipment

Executive Team: Notify the off-site storage facility, municipal top management and the ICT service providers of the disaster declaration.

(Replacement 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 of the emergency.

Reconstruct the servers at main office (salvage/reclamation team)

(Operations Team, Restoration Team and Customer Support Team) Conduct operation at the DRS until the computer centre is ready to resume operations.

(Operations Team and Restoration Team) Conduct preparations to leave DRS and to resume operations at the main server room

2.6 DRS HARDWARE AND SOFTWARE CONFIGURATIONS

The standard ICT hardware and software infrastructure at DRS should include a mainframe system (server), Advanced Windows Server 2003/8 Network infrastructure for data communications and a work recovery centre.

The following are major hardware components of the standard mainframe configuration:

- Servers with sufficient processor speed and memory capacity,
- Be virtualized
- Sufficient quantity of tape drives
- Sufficient disk storage
- Sufficient Printer capacity
- 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 mainframe/server and workstations
  - Dedicated T1 line with appropriate routers, switches, and firewalls for IP communication between main office, DRS main frame and all workstations
  - Web redirect services, for Internet connectivity to provide alternative connectivity the T1 line be inoperable

2.7 RESUMING 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.

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

3 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.

3.1 DAMAGE ASSESSMENT TEAM

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.

Recommended Team Members are:-

Public Safety Staff form Disaster management

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 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.
➢ Brief the MM or alternate, communicating the recommendation(s).

3.2 Management Team

Municipal Manager (MM) declares that a disaster has occurred, authorizes the execution of the Disaster Recovery Plan, and oversees the execution of the plan during the emergency.

The pre-disaster responsibilities are:

➢ MM approves ICT Disaster Recovery Plan and all major or material modifications to the plan.
➢ Establish primary and alternate disaster command posts, ensuring that the posts are adequately prepared for a disaster.

The disaster responsibilities and actions are:

➢ Notify the DRS and the off-site storage facility of a possible disaster.
➢ Review the report of the Damage Assessment Team.
➢ Declare a disaster:

a) establish the command post and communications,
b) activate the Functional Teams,

c) inform the DRS of the disaster declaration, and

d) initiate the shipment of the backup materials to the DRS.

- Notify the Key Executives.
- Keep all senior managers and the designated Information Officer/alternate informed of material/sensitive matters.

3.3 RESTORATION TEAM

The Restoration Team brings the DRS municipal email systems to operational mode by managing the relocation of services to the DRS email processing site, initiating and managing the recovery procedures at the DRS, and responding to operational problems at the DRS. The Restoration Team also manages the relocation of services back to the server room.

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
<th>Contact Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mokgatlhe Ratlhogo</td>
<td>Chief Financial Officer</td>
<td>0731755607</td>
</tr>
<tr>
<td>Elias Koloi</td>
<td>Executive Manager: Public Safety</td>
<td>0832676601</td>
</tr>
<tr>
<td>Sivuyile Sbukwana</td>
<td>Manager: ICT</td>
<td>072 997 7313</td>
</tr>
<tr>
<td>Mzwandile Mkhize</td>
<td>Manager: Expenditure</td>
<td>083 267 8816</td>
</tr>
<tr>
<td>Tshiamo Senosi</td>
<td>Manager: Budget</td>
<td>0764532017</td>
</tr>
<tr>
<td>Yvonne Ratombo</td>
<td>Coordinator: ICT Support</td>
<td>071 600 9707</td>
</tr>
<tr>
<td>Casper Jordaan</td>
<td>Coordinator: 107 Centre</td>
<td>083 267 8814</td>
</tr>
<tr>
<td>Eugene Manyisa</td>
<td>ICT Support Technician</td>
<td>0716009709</td>
</tr>
<tr>
<td>Thabo Palaki</td>
<td>ICT Support Technician</td>
<td>0832911962</td>
</tr>
<tr>
<td>Tumi Mogole</td>
<td>ICT Support Technician</td>
<td>011 411 5044</td>
</tr>
<tr>
<td>Linda Theunissen</td>
<td>Helpdesk Administrator</td>
<td>011 411 5044</td>
</tr>
<tr>
<td>Mpho Manyapelo</td>
<td>Coordinator Risk</td>
<td>011 411 5000</td>
</tr>
</tbody>
</table>

The pre-disaster responsibilities are:

- Establish and maintain the recovery procedures for the DRS.
- Manage and maintain the backup procedures.
- Establish and maintain the disaster recovery data communications link to the DRS.
- Plan and conduct regular DRS recovery tests.

The disaster responsibilities and actions are:

- Coordinate recovery procedures with DRS personnel.
- Restore the operating systems environments on the DRS processing site host systems.
- Establish the data communications link to the DRS.
- Verify the operating systems and all other system and communication software are working properly.
- Restore the application/mailbox files.
➢ Support the operations at the DRS by resolving problems and monitoring and maintaining the data communications link to the DRS.
➢ Support operations at the alternate email processing site by resolving problems.
➢ Manage the backup tapes that were sent to the DRS.
➢ Ensure all required backups of the entire system are completed in preparation for leaving the DRS.
➢ Coordinate the return of the backup/storage media to the Server room.
➢ Install all municipal system/messaging software at the Server room.

3.4 OPERATIONS TEAM

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
<th>Contact Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mokgatlhe Ratlhogo</td>
<td>Chief Financial Officer</td>
<td>0731755607</td>
</tr>
<tr>
<td>Elias Koloi</td>
<td>Executive Manager: Public Safety</td>
<td>0832676601</td>
</tr>
<tr>
<td>Sivuyile Sbukwana</td>
<td>Manager: ICT</td>
<td>072 997 7313</td>
</tr>
<tr>
<td>Mzwandile Mkhize</td>
<td>Manager: Expenditure</td>
<td>083 267 8816</td>
</tr>
<tr>
<td>Tshiamo Senosi</td>
<td>Manager: Budget</td>
<td>0764532017</td>
</tr>
<tr>
<td>Yvonne Ratombo</td>
<td>Coordinator: ICT Support</td>
<td>071 600 9707</td>
</tr>
<tr>
<td>Casper Jordaan</td>
<td>Coordinator: 107 Centre</td>
<td>083 267 8814</td>
</tr>
<tr>
<td>Eugene Manyisa</td>
<td>ICT Support Technician</td>
<td>0716009709</td>
</tr>
<tr>
<td>Thabo Palaki</td>
<td>ICT Support Technician</td>
<td>0832911962</td>
</tr>
<tr>
<td>Tumi Mogole</td>
<td>ICT Support Technician</td>
<td>011 411 5044</td>
</tr>
<tr>
<td>Linda Theunissen</td>
<td>Helpdesk Administrator</td>
<td>011 411 5044</td>
</tr>
<tr>
<td>Mpho Manyapaolo</td>
<td>Coordinator Risk</td>
<td>011 411 5000</td>
</tr>
</tbody>
</table>

The pre-disaster responsibilities are:
➢ Ensure that appropriate backups are made on the prescribed, rotating basis and are ready to be taken off-site.
➢ Maintain current, up-to-date systems operations documentation, ensuring that this documentation is suitably stored off-site.

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).
➢ Coordinate the shutdown of the DRS operations and the transfer back to the Server room.
3.5 CUSTOMER SUPPORT TEAM

The Customer Support team provides assistance to customers during the disaster from the time the disaster is declared until operations resume at the Data Centre.

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
<th>Contact Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mokgatlhе Ratlhogo</td>
<td>Chief Financial Officer</td>
<td>0731755607</td>
</tr>
<tr>
<td>Elias Koloi</td>
<td>Executive Manager: Public Safety</td>
<td>0832676601</td>
</tr>
<tr>
<td>Sivuyile Sbukwana</td>
<td>Manager: ICT</td>
<td>072 997 7313</td>
</tr>
<tr>
<td>Mzwandile Mkhize</td>
<td>Manager: Expenditure</td>
<td>083 267 8816</td>
</tr>
<tr>
<td>Tshiamo Senosi</td>
<td>Manager: Budget</td>
<td>0764532017</td>
</tr>
<tr>
<td>Yvonne Ratombo</td>
<td>Coordinator: ICT Support</td>
<td>071 600 9707</td>
</tr>
<tr>
<td>Casper Jordaan</td>
<td>Coordinator: 107 Centre</td>
<td>083 267 8814</td>
</tr>
<tr>
<td>Eugene Manyisa</td>
<td>ICT Support Technician</td>
<td>0716009709</td>
</tr>
<tr>
<td>Thabo Palaki</td>
<td>ICT Support Technician</td>
<td>0832911962</td>
</tr>
<tr>
<td>Tumi Mogole</td>
<td>ICT Support Technician</td>
<td>011 411 5044</td>
</tr>
<tr>
<td>Linda Theunissen</td>
<td>Helpdesk Administrator</td>
<td>011 411 5044</td>
</tr>
<tr>
<td>Mpho Manyaapelo</td>
<td>Coordinator Risk</td>
<td>011 411 5000</td>
</tr>
</tbody>
</table>

The pre-disaster responsibilities are:

➢ Advise and consult with application users regarding their disaster recovery requirements.
➢ Assist application user during disaster recovery tests.

The disaster responsibilities and actions are:

➢ Notify participating application users that a disaster has been declared.
➢ Advise users of the disaster recovery system status, availability, and accessibility.
➢ Provide problem diagnosis and resolution guidance/assistance to application owners and their users.

3.6 SALVAGE/RECLAMATION TEAM

The Salvage/Reclamation Team manages the restoration or rebuilding of the Server room.

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
<th>Contact Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mokgatlhе Ratlhogo</td>
<td>Chief Financial Officer</td>
<td>0731755607</td>
</tr>
<tr>
<td>Sivuyile Sbukwana</td>
<td>Manager: ICT</td>
<td>072 997 7313</td>
</tr>
<tr>
<td>Yvonne Ratombo</td>
<td>Coordinator: ICT Support</td>
<td>071 600 9707</td>
</tr>
<tr>
<td>Casper Jordaan</td>
<td>Coordinator: 107 Centre</td>
<td>083 267 8814</td>
</tr>
<tr>
<td>Eugene Manyisa</td>
<td>ICT Support Technician</td>
<td>0716009709</td>
</tr>
<tr>
<td>Thabo Palaki</td>
<td>ICT Support Technician</td>
<td>0832911962</td>
</tr>
<tr>
<td>Tumi Mogole</td>
<td>ICT Support Technician</td>
<td>011 411 5044</td>
</tr>
<tr>
<td>Linda Theunissen</td>
<td>Helpdesk Administrator</td>
<td>011 411 5044</td>
</tr>
<tr>
<td>Mpho Manyaapelo</td>
<td>Coordinator Risk</td>
<td>011 411 5000</td>
</tr>
</tbody>
</table>
The major pre-disaster responsibility is to maintain current copies of equipment inventory lists, physical plant layout/diagrams (floor plans), and other pertinent documentation describing ICT production hardware configuration in a suitable off-site location.

The disaster responsibilities and actions are:

- After the Restoration Team has implemented recovery operations at the DRS, assess the damage to the Server room and report the damage, with recommendations, to the Management Team.
- Organize the recovery of salvageable equipment, supplies and the physical plant.
- Initiate, coordinate, and expedite construction and work requests to prepare the municipal facility to receive equipment, supplies, tools, machinery, and utilities (electrical power, telephones, network connectivity, air conditioning, plumbing, water, gas, and etc).
- Order and expedite replacements for unusable ICT equipment.
- Monitor the construction of the new/repaired facility, and the installation of all utilities and other essentials.
- Monitor the installation of computers, peripherals, and other ICT equipment.
- Advise the Management Team regarding status, progress, and schedules, and any problems associated with the construction/reconstruction and installation.
- Inform the Management Team when the new/restored facility is ready for use by the participating applications and by other users.

3.7 ADMINISTRATIVE SUPPORT TEAM

The Administrative Support Team provides logistical and organizational support for all the other teams.

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
<th>Contact Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mokgatlhe Ratlhogo</td>
<td>Chief Financial Officer</td>
<td>0731755607</td>
</tr>
<tr>
<td>Elias Koloi</td>
<td>Executive Manager: Public Safety</td>
<td>0832676601</td>
</tr>
<tr>
<td>Sivuyile Sbukwana</td>
<td>Manager: ICT</td>
<td>072 997 7313</td>
</tr>
<tr>
<td>Mzwandile Mkhize</td>
<td>Manager: Expenditure</td>
<td>083 267 8816</td>
</tr>
<tr>
<td>Tshiamo Senosi</td>
<td>Manager: Budget</td>
<td>0764532017</td>
</tr>
<tr>
<td>Benjamin Mogale</td>
<td>Fleet Management</td>
<td>0828396605</td>
</tr>
<tr>
<td>Eric Orr</td>
<td>Fleet Management</td>
<td>0834608464</td>
</tr>
<tr>
<td>Yvonne Ratombo</td>
<td>Coordinator: ICT Support</td>
<td>071 600 9707</td>
</tr>
<tr>
<td>Casper Jordaan</td>
<td>Coordinator: 107 Centre</td>
<td>083 267 8814</td>
</tr>
<tr>
<td>Eugene Manyisa</td>
<td>ICT Support Technician</td>
<td>0716009709</td>
</tr>
<tr>
<td>Thabo Palaki</td>
<td>ICT Support Technician</td>
<td>0832911962</td>
</tr>
<tr>
<td>Tumi Mogole</td>
<td>ICT Support Technician</td>
<td>011 411 5044</td>
</tr>
<tr>
<td>Linda Theunissen</td>
<td>Helpdesk Administrator</td>
<td>011 411 5044</td>
</tr>
<tr>
<td>Mpho Manyaapelo</td>
<td>Coordinator Risk</td>
<td>011 411 5000</td>
</tr>
</tbody>
</table>

The major pre-disaster responsibility is to prepare up-to-date property management lists, inventory lists, and other pertinent documentation on the physical assets of the Server room, ensuring current copies of this documentation are suitably stored off-site.
The disaster responsibilities and actions are:

- Prepare travel orders and other documents to facilitate the Restore Team activities.
- Provide general administrative support to the Executive Team and to all other Disaster Recovery Teams as necessary.

4 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 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, ICT regularly schedules exercises of its Disaster Recovery Plan at the vendor DRS, referred to as DRS tests.

4.1 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 tests are managed and conducted by members of the Restoration Team, the Operations Team, and the Customer Support Team, referred to collectively as the DRS Team.

Prior to the DRSs, the DRS Team determines which backup tapes will be used for the tests; establishes a 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. (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.

4.2 DRS TEST PLANNING

To ensure a successful DRS test, the DRS team will:

- Confirm with the DRS vendor that the DRS mainframe, Unix computer, and data communications configurations 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 for the test will be taken)

Send the backup tapes and tape lists to the DRS. (One week prior to the scheduled test)

4.3 APPLICATION TESTING SUPPORT

The DRS Team offers user support during a DRS test to assist the application owners/participants in successfully running their applications at the alternate 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.

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
<th>Contact Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mokgatle Rathogo</td>
<td>Chief Financial Officer</td>
<td>073 175 5607</td>
</tr>
<tr>
<td>Sivuyile Sbukwana</td>
<td>Manager: ICT</td>
<td>072 997 7313</td>
</tr>
<tr>
<td>Yvonne Ratombo</td>
<td>Coordinator: ICT Support</td>
<td>071 600 9707</td>
</tr>
<tr>
<td>Casper Jordaan</td>
<td>Coordinator: 107 Centre</td>
<td>083 267 8814</td>
</tr>
<tr>
<td>Eugene Manyisa</td>
<td>ICT Support Technician</td>
<td>071 600 9709</td>
</tr>
<tr>
<td>Thabo Palaki</td>
<td>ICT Support Technician</td>
<td>083 291 1962</td>
</tr>
<tr>
<td>Tumi Mogole</td>
<td>ICT Support Technician</td>
<td>011 411 5044</td>
</tr>
<tr>
<td>Linda Theunissen</td>
<td>Helpdesk Administrator</td>
<td>011 411 5044</td>
</tr>
<tr>
<td>Mpho Manyaapelo</td>
<td>Coordinator Risk</td>
<td>011 411 5000</td>
</tr>
</tbody>
</table>

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, and
- 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, and
- Recording all problem reports and general notes to a system status database that is made available to users to read.

4.4 POST-TEST WRAP-UP

Two debriefings are schedule 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, and
Suggestions for improvements.

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

4.5 DRS TEST SCHEDULE

The bi-yearly tests are scheduled approximately six months apart beginning 6 months after approval of this DRP.

4.6 TRAINING

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

5 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 briefings; and
- 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 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.