

DR NKOSAZANA DLAMINI ZUMA LOCAL MUNICIPALITY



ICT DISASTER RECOVERY PLAN

Core Business Areas	Corporate Services Department
Operational Area	ICT Unit

Version	1
Date	
File Name	Disaster Recovery Plan
Business Owner	Corporate Services Manager
Date Approved	

Document Classification:

Confidential

IT DISASTER RECOVERY PLAN

Index

1. Aim of The Disaster Recovery Plan
2. Ownership
3. Disaster Recovery Plan Coverage
4. Emergency Contact Details of Key Persons
5. Priority Levels of Key Systems
6. Deadline for Key Recovery
7. Key System Requirements
8. Preventative Measures
9. Financial Management Systems
10. Disaster recovery procedures
11. Servers
12. Recovery Site

This is a formal Disaster Recovery Plan for Dr Nkosazana Dlamini Zuma local Municipality.

1. Aim of the Disaster Recovery Plan

The main aim of the ICT Disaster Recovery Plan is to ensure that should the Municipality experience disaster of any nature (e.g., firebreak, power surge or building is damaged etc.), the Municipality has contingency plans for backup systems. The plan is there to make staff aware of what procedures should be followed when connecting backup systems and who are the key contact persons for the systems. The DRP is there to ensure that a Disaster Recovery Team is appointed and trained properly, so that even if the IT staff is not in the office the team can take charge successfully.

This plan may be updated as necessary by the ICT Steering Committee or ICT Manager to ensure that it remains relevant.

2. Ownership

The Municipality has several departments amongst which there is Corporate Services Department. The Corporate Services Department is responsible for managing all computer systems for the Municipality; hence, they must make sure that in times of disasters they are supposed to have a proper plan in place. The Corporate Services Department is therefore the custodian of the Disaster Recovery Plan.

The designated Disaster Recovery Plan contact person is ICT Manager.

Copies of the Information Technology Disaster Recovery Plan shall be made available through offsite backups as part of the Backup Policy.

3. Disaster Recovery Plan Coverage

The person who has authority to declare a disaster is the Municipal Manager. The Disaster Recovery Team will consist of the ICT Manager, Senior Manager Corporate Support Services, Senior Manager Financial Services(CFO), Senior Manager Community Services, Senior Manager Public Works and Basic Services and Senior Manager Development and Town Planning Services, reporting to the Municipal Manager.

The systems at the Municipality include but are not limited to:

1. Financial Software (eg. SAMRAS)
2. Domain Controller Managing File Access (eg. Windows Server)
3. Internet and Email Facilities

Additional services may be added as determined by the ICT Steering Committee or other parties.

4. Emergency Contact Details of Key Persons

In the event when a problem cannot be resolved locally, the Disaster Recovery Team in consultation with the Municipal Manager and / or the ICT Officer would recommend the relevant companies to be contacted to resolve the problem.

Relevant Contact Information

Software	Company/ Service provider	Contact number
SAMRAS	Bytes Technology Systems	0218181411
Domain Controller	ICT Manager	0398331038
Email	PowerVision Technology	0735124102
Internet	MTN & PowerVision	
Brocad	Dept Arts & culture IT	0333413000
eNatis	Dept Transport IT	0333951800

5. Priority Levels of Key Systems

The municipal systems are listed below, according to their priority order, the first one being:

- ☐ Network, Routers and Hubs
- ☐ SAMRAS Financial Management
- System ☐ Domain Controller
- ☐ Mail Server & Internet
- Server ☐ Firewall

6. Tasks per IT Committee (Higher level)

These tasks include but are not limited to the following:

1.1.1 ICT Steering Committee

- a) Reviews and makes amendments to this document to ensure that it remains relevant.
- b) Ensures that recovery takes place as quickly as possible and provides the necessary support as needed.
- c) Assist in the event of a disaster scenario with internal and external communication to relevant parties.

1.1.2 Disaster Recovery Team

The Disaster Recovery Team coordinates the recovery process in accordance with the Disaster Recovery Plan.

1.1.3 ICT Disaster Recovery Team

Once a disaster is declared by the Municipal Manager and a decision was made to activate the Disaster Recovery Plan the ICT Disaster Recovery Team will:

- a) Obtains backups from offsite secure storage.
- b) Recover, reinstall or replace the affected systems.
- c) Installs security systems that are applicable.
- d) Establishes communications link - network connectivity.
- e) Loads applications and packages.
- f) Restore recovered data from backups.
- g) Provide other user support.
- h) Assists where possible with e-mail and Internet services.

7. IT Requirements for Recovery Site

A separate recovery site should be available to ensure business continuity in the event of a catastrophic event at the primary office. back-up servers in the order of importance as mentioned above. All of the servers should be installed and configured to be the same as the existing machines.

Once that exercise is complete those machines will be placed off-site, so that in the event that the whole building gets damaged the backup machines will just be taken from off-site, plug in and be online immediately thus minimising down time.

The off-site equipment should be tested once a month to make sure that everything is in order. Installing a duplicate server off-site with a direct fibre link in order to duplicate all information in real-time. In the event of a disaster occurring and affecting the primary server(s), the duplicate server can be switched to become the primary server in a relatively short period and with minimal reconfiguration (depending on the level of destruction to the network).

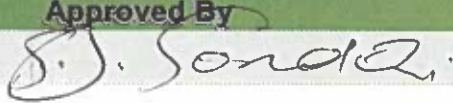
8. Backups and vital records

At least a weekly backup must be stored at the recovery site. Backups should be stored as per the Backup Policy.

9. Disaster recovery procedure

The following procedures outline suggested action in the event of certain disaster events:

- ☐ In the event of hardware failure / loss, the relevant hardware must be replaced first, after which the relevant software must be reinstalled and reconfigured. This will be done by the relevant person.
- ☐ The most recent back-up tape is to be obtained (either from onsite storage or the offsite safety deposit box).
- ☐ The relevant person will then restore the data from the back-up tape.

Signature	Approved By	Date
		28 May 2026