



**DR NDZ LOCAL MUNICIPALITY**

# **ICT DISASTER RECOVERY PLAN**

Core Business Areas	Corporate Services Department
Operational Area	IT Unit

Version	
Date	
File Name	DISASTER RECOVERY PLAN
Business Owner	Corporate Services Manager
Date Approved	

Document Classification:  
**Confidential**  
©Ingwe Local Municipality 2015

## 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 Ingwe 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 Officer 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 IT 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 IT Manager, Senior Manager Corporate Support Services, Senior Manager Financial Services, 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 (eg. Exchange Server)
4. Auditing Software (eg. Caseware)

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 IT Officer would recommend the relevant companies to be contacted to resolve the problem.

##### Relevant Contact Information

<i>Software</i>	<i>Company/ Service provider</i>	<i>Contact number</i>
Samras FMS	Bytes	0216806870
PAYDAY Payroll	VIP	0832625121
Domain Controller	IT Officer	0398331038
Email	Symphonypc	0333453500
Internet	Futurenet	0398342963
Caseware	Bytes	0216806870
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**

- a) A separate recovery site should be available to ensure business continuity in the event of a catastrophic event at the primary office.
- b) The recovery site that will be host offsite storage and should have a minimum of 2 work stations (PCs) all connected to the network.
- c) All workstations must have connectivity to the internet and e-mail.
- d) Operating software including security software licenses must be stored as part of the backup policy.
- e) All system documentation, configuration documentation, system images, duplicate software (including licenses) and printers access.

## **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:

### **Power Supply Failure**

In the event of the server's UPS failing, another unit will be installed, and the server restarted and it will be checked that the system is functioning. If it is a specialised UPS then the original UPS will be sent off for repair, and reinstalled once it has been repaired, or it will be replaced.

### **Memory Failure**

Replacement memory will be installed and the faulty memory be swapped out or replaced if not under warranty.

### **Main Board Failure**

The server will then be removed and returned to the supplier for repair or replacement if under warranty. If it is not under warranty, a quote for repair and a quote for replacement will be obtained and a decision made on which route to follow. Once the server has been sorted out by either repair or replacement, a backup will be taken of the current data, and then restored to the repaired server.

### **File Server Network Card Failure**

A new network card will be installed into the file server and either the on-board disabled or the faulty board removed. The operating system will then be reconfigured to recognise the new hardware together with the appropriate addresses.

### **Theft of Server**

The stand-by server will be installed and the latest backup restored.

### **Server Destroyed by Fire, Flood**

The stand-by server will be installed in a suitable environment, and the latest backup restored. The problem with this is that in most installations the wiring closet or cabinet is installed in the same location as the server. In this circumstance, the central core of the cabling system may also be damaged or destroyed. This may result in the damage being assessed and the server together with a loan hub being installed in the most practical position.

### **Total Site Destruction by Fire, Flood and other circumstances.**

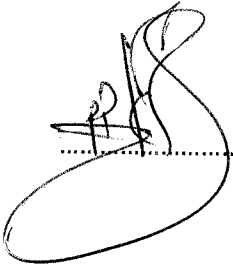
In the event of the site being completely destroyed, an alternate venue and the server installed and latest backup restored. Hubs and a minimum of three workstations will be made available to get the core function operational. This could take a little longer as the workstations would have to have the corresponding client software installed off the server and that could only happen once the server has been restored completely.

**COUNCIL APPROVAL AND EFFECTIVE DATE**

Approval of Policy by Council and Effective date: 06/06/2017

MUNICIPAL MANAGER

DATE



A handwritten signature in black ink, consisting of several loops and a long horizontal stroke at the bottom, positioned above a dotted line.

19/06/2017