"The City of Heritage"

ULUNDI
MUNICIPALITY

INFORMATION TECHNOLOGY

Disaster Recovery Plan

Table of Contents

1. Introduction 3
2. Scope of this Plan 3
3. Disaster Scenarios 3
4. Current Practices and Procedures 3
    4.1. Data Backup and Restoration 4
    4.2. Application Restorations 4
    4.3. System Shutdown and Startup 4
    4.4. Critical Systems 4
    4.5. DRP Management 5
5. Notification and Activation 5
6. Recovery Process 5
    6.1. Phase 1 – Assessment and Planning 6
    6.2. Phase 2 – Recovery 7
        6.2.1. System Recovery Priority List 7
        6.2.2. Equipment List 7
        6.2.3. Re-establishment of Normal Operations 7
        6.2.4. Procedure for Retrieval of Backup Tapes 8
        6.2.5. Post Recovery Review 8
7. Plan Maintenance and Testing 8
8. Appendices 9
    8.1. Recovery Staff Details 9
    8.2. Vendors and Services Providers 9
    8.3. Emergency Services 9
    8.4. Utilities Services ..... **Error! Bookmark not defined.**

1. Introduction

The Municipality's IT system and networks provide services to what each department is dependent upon.

Without telephones or networks or any of several critical servers, some aspects of the municipality's services would come to a standstill should a failure occur.

In recognition of these dependencies, it is of utmost importance that Ulundi Municipality be prepared to respond to a disaster in an orderly, timely and efficient manner.

This document describes the Recovery Plan which will be used in the event of a disaster affect in its operation and services. It includes a summary of the current services, identifies the services critical to municipal operations and dictates how these services will be reconstituted following a disaster.

A current version of this plan, the plan's appendices and any other referenced policies and procedures must be kept in a secure offsite location to ensure that the plan is available in the event of a disaster.

2. Scope of this Plan

This plan provides Ulundi Municipality with the ability to address two areas:

- It enables the systems administrator to restore Ulundi Municipality's core information systems in the event of a disaster.
- It identifies areas of substantial risk and exposure to disaster and assist in reducing these risks.

3. Disaster Scenarios

This plan focuses on recovering from a disaster at Ulundi Municipality head office, BA131, Corner of Princess Magogo and Zwelithini Street, Ulundi. This building is deemed most critical. This is where core IT systems are housed. The Civic Centre, BA81, Prince Magogo Street will be used as a Disaster Recovery Centre.

4. Current Practices and Procedures

- An understanding of fundamental Municipal practices is the key to recovering departments operations, the key activities include:

4.1. Data Backup and Restoration

Backs are performed in accordance with the Municipalities Data Backup and Restoration policy and procedures. These require that all business critical systems are adequately backed up and tested to ensure that key system and information can be recovered.

4.2. Application Restorations

The different systems restoration procedures will define how each system/application will be restored. Where necessary, the expertise of the system Vendor or Service Provider will be utilized.

4.3. System Shutdown and Startup

Instructions for shutdown and startup of servers are located at the server room.

4.4. Critical Systems

The following systems are designated as critical systems. These systems are listed here because without awareness, it is possible that an oversight during a restoration could result in problems:

Category	**Hostname/description**	**Functionality provided**	**Database/folder**	**IP Address**
Windows Application (server 2012 R2)	PayDay	Payroll and HR	PayDay Data Files	192.0.1.1
Windows Application(server 2016)	mSOA Pastel Evolution (v.7.20.5)	Financial System	MS SQLSERVER	192.0.1.5
Windows Application(server 2016)	mSOA Pastel Evolution (v.7.20.5)	File Server - Shares	BIC$, EFT	192.0.1.5
Windows Application (server 2012 R2)	Metval	Property Management Systems	MS SQLSERVER	192.0.1.1
Web Application (Apache24 server)	Issue Tracking App	IT incidents management	MySQL	192.0.1.25

4.5. DRP Management

The DRP Manager is the primary person responsible for ensuring a DRP plans are regularly reviewed, tested and maintained. This person is required to liaise with all DRP teams on a regular basis to ensure all changes within the municipality and their impact on Disaster Recovery have been considered. This person is also responsible for ensuring that all staff, both team members within the municipality are provided with the necessary awareness and training.

The municipality will assign a person who will be responsible for ensuring that the Disaster Recovery Plan is kept in a safe and secure place. This person will further have to ensure that they do have the latest version of the plan.

5. Notification and Activation

Upon discovery of a disaster, the Municipal Manager, HOD Corporate Services, Chief Financial Officer or IT Administrator must be notified immediately. The person who has authority to declare a disaster is the Information Technology Manager in consultation with the Municipal Manager and Manager Corporate Services. The Municipal Manager and IT Administrator will then perform an assessment of the Municipalities IT Systems, based upon which the Municipal Manager will determine whether it is appropriate for the Disaster Recovery Plan to be activated and invoked. Should the Municipal Manager not be available the responsibility will then sit with the Chief Financial Officer.

The contact details of key staff members are:

Designation	**Contact Number**
The Municipal Manager	082 457 7373
HOD Corporate Services	083 561 6868
IT Manager	083 733 7902
Chief Financial Officer	073 472 1934

Once the plan has been formally invoked, the following procedures must be followed.

6. Recovery Process

The recovery process consists of two phases:

- An initial phase where notifications are made, the staff assembled, information gathered and an action plan developed.
- The recovery phase where resources are required, data recalled, and services are restored as much as possible.

- If there is a disaster of any kind, it must only take a maximum of three days to recover and have all users online.

6.1. Phase 1 – Assessment and Planning

6.1.1. Notify and Assembly the Recovery Staff

All recovery staff should be notified as soon as the decision to invoke the Disaster Recovery Plan has been made. The recovery team should then assemble at an agreed upon location. Refer Recovery Staff Details for names and contact details of the Recovery Team. Once the recovery team has been assembled, they should go through the Disaster Recovery Plan to assign roles and responsibilities and ensure that everyone knows and understands their specific roles and tasks.

6.1.2. Perform Primary Site Procedure

It is the Recovery Team's responsibility to conduct a site survey of affected area to assess the nature and extent of any damage. They must take stock of any salvageable or usable equipment and note what equipment will need to be replaced. They must also secure the primary site so as to ensure that there is no unauthorized access to what may remain of the Municipalities IT systems and to prevent any further damage.

6.1.3. Inform Vendors and Services Providers

Once the nature and extent of the disaster has been determined, the Municipality's vendors and service providers should be notified and informed that the Municipality has invoked its Disaster Recovery Plan what assistance or equipment they should provide.

6.1.4. Establish Communication Plan

A communication plan will need to be implemented. The communication plan will ensure that:

- All Municipal staff and contractors impacted by the Disaster are informed and instructed on what they should do, i.e. stay at home, report to DR site etc;
- MANCO is kept up-to-date on a regular basis with status updates and estimated timelines;
- All relevant Municipal Suppliers, Vendors, Service Providers or Customers should be informed and kept updated where appropriate;
- Communication with the relevant authorities, Police, Fire Department etc, is centralized and the responsibility of a specific individual/s who can then relay any messages with the Disaster Recovery team.

- Any and all communication with the Media, if required or requested, should be direct to a specific, authorized individual who can speak on the Municipality's behalf.

6.2. Phase 2 – Recovery

6.2.1. System Recovery Priority List

The priority of the Municipality's Systems and the order in which they should be recovered are:

Priority	Service
1	PayDay
2	Pastel Evolution
3	File Server
4	Metval

The recovery/restoration procedures for each of the above systems is documented within the Municipalities Backup Policy and Procedure or detailed by the Vendor/Service Provider. Vendor and/or Service Provider expertise will be utilized during the recovery procedure if required to ensure that the systems are effectively restored in as short a time as possible.

6.2.2. Equipment List

The following equipment is required to re-establish the priority service to a basic nominal level of service. It is not intended to duplicate the original performance, but rather to provide a minimally acceptable level. This equipment will be obtained from service providers and from the open market. This equipment will be set up at the Civic Centre building which will be used as a Disaster Recovery Centre as a precautionary measure in case a disaster strikes.

- Desktop Computer
- Backup media
- Windows Server
- Network Disaster Recovery Server
- Printers

6.2.3. Re-establishment of Normal Operations

As part of the recovery process consideration must also be given to restoring the Municipalities systems to a normal state of operations. Whilst priority will be given to restoring the minimal operating requirements of the municipality, once this is achieved

focus must shift to re-establishing the normal state of operations. Steps required to be taken will depend on the nature and extent of the disaster but, at a minimum, may include the following:

- Acquisition of equipment to permanently replace destroyed or damaged equipment. This equipment should be of a suitable specification to enable pre-disaster performance to be achieved;
- Identification of a suitable server room if the original one is no longer suitable;
- Implementation of a cutover plan to transfer all data from DR systems back onto Production systems.

6.2.4. Procedure for Retrieval of Backup Tapes

The type of backup media used for PAYDAY, Pastel and Network is CD/DVD. Email backup is done by Service provider. Data is also stored on external hard drives.

- If on-site backups are available, restore using the most recent backup tape.
- If on-site backups are destroyed, retrieve latest weekly backup from off-site location and restore.

6.2.5. Post Recovery Review

Within a month of normal operations having been restored a post recovery review should be performed by the Recovery Team. This review should identify and document any and all weaknesses or issues identified during the recovery process. The remediating actions taken must be documented and the Disaster Recovery Plan updated accordingly. The review should also identify areas where efficiencies could be made and these should be included in the next test of the Disaster Recovery Plan

7. Plan Maintenance and Testing

This Disaster recovery plan must be tested, at a minimum, on an Annual basis. The testing should simulate a Disaster and all necessary recovery steps must be performed as per the documented plan. The testing must be documented and all documentation must be retained. Any weaknesses or issues identified during testing should be remediated and the Disaster Recovery Plan updated accordingly.

8. Appendices

8.1. Recovery Staff Details

Name	Designation	Contact Number
Mr. M.T. Nkosi	IT Manager	083 733 7902
Mr. N. Dlamini	IT Security Officer	078 868 5121
Mr. L Mpungose	IT Controller	078 676 7233
Mr. Z. Mpontshane	IT Controller	072 129 2734
Mr. Z.G. Dhlamini	HoD – Corporate	083 463 3907
Mr. De Wet	HoD - Technical	083 561 7719
Mr. N.G. Zulu	Municipal Manager	083 407 0870
Mr. R.C. Mazibuko	HoD - Planning	064 651 8980

8.2. Vendors and Services Providers

The following are the municipality's key vendors and service providers:

Service Provider	System/Service	Contact Person	Contact Number
PayDay Solutions	PayDay	AJ Deena	012) 803 7730 083 262 5121
Metgovis	Metval	Ayanda	083 825 9577
Camelsa Consulting Group	mSOA Pastel Evolution	Titus Dube	(011) 805 1027 078 042 1150
Telkom	Telephone	Errol Xolo	081 475 1941
Liquid Telecom	Internet	May Jeremiah	082 677 9056

8.3. Emergency Services

The following are emergency services details:

Emergency Services	Contact Number
Police	10111
Fire Department	(035) 874 500
Ambulance	10177

8.4. Approvals

The table below provides necessary approvals of this plan.

Approver	**Signature**	**Date**
Chairman of the Council		
Chairman of the Audit and Risk Committee		
Ulundi Municipal Manager		