UMZIMVUBU

LOCAL MUNICIPALITY

ICT DISASTER RECOVERY PLAN

TABLE OF CONTENTS

SECTION 1 – OVERVIEW

1. OVERVIEW SECTION

1.1. ABBREVIATIONS AND DEFINITIONS

1.1.1. Throughout this document various acronyms, abbreviations and definitions are referred to. For the purpose of this Disaster Management Plan these are defined as follows:

1.1.1.1.	AG	Auditor General
1.1.1.2.	CoBit	Control Objectives for Information and Related Technology
1.1.1.3.	ULM	Umzimvubu Local Municipality
1.1.1.4.	DRP	Disaster Recovery Plan
1.1.1.5.	MM	Municipal Manager
1.1.1.6.	IS	Information System
1.1.1.7.	ISF	Information Security Forum
1.1.1.8.	ISO	Information Security Officer
1.1.1.9.	ISS	Information System Security
1.1.1.10.	IT	Information Technology
1.1.1.11.	ITIL	Information Technology Information Library
1.1.1.12.	KPA	Key Performance Area
1.1.1.13.	MFMA	Municipal Finance management Act
1.1.1.14.	SLA	Service Level Agreement
1.1.1.15.	CAB	Change Advisory Board
1.1.1.16.	DRP	Business Continuity Management

1.2. SCOPE

1.2.1. An IT Disaster Recovery Plan is an important component of business continuity planning. Where organisations rely on IT systems for their operations it is critical that IT disaster and consequent recovery thereof is appropriately planned for, and considered within the context of the organisation's wider business objectives.

1.2.2. ULM and its inherent council's operations are reliant on several IT systems across a broad range of services. The failure of any of these IT systems could have a significant impact on the municipality's ability to deliver services. Against this background, effective IT disaster recovery planning is essential to ensuring that municipality is able to respond to system failures in the event of a major disaster incident, in order to maintain operations of all critical systems.

1.2.3. The plan provides information for the pro-active handling of any crisis situation and

should include detailed procedures for Technology management. The plan also documents the responsibilities, procedures, and checklists that will be used to manage and control the situation following an emergency or crisis occurrence.

1.3. PURPOSE

1.3.1. The purpose of this IT Disaster Recovery Plan ("IT DRP") is to provide guidance to ULM's Information Technology Unit in recovering the IT infrastructure in the event of a major IT disaster, in line with the Recovery Time Objectives ("RTO") which are herein defined. More particularly the purpose of this document is to:

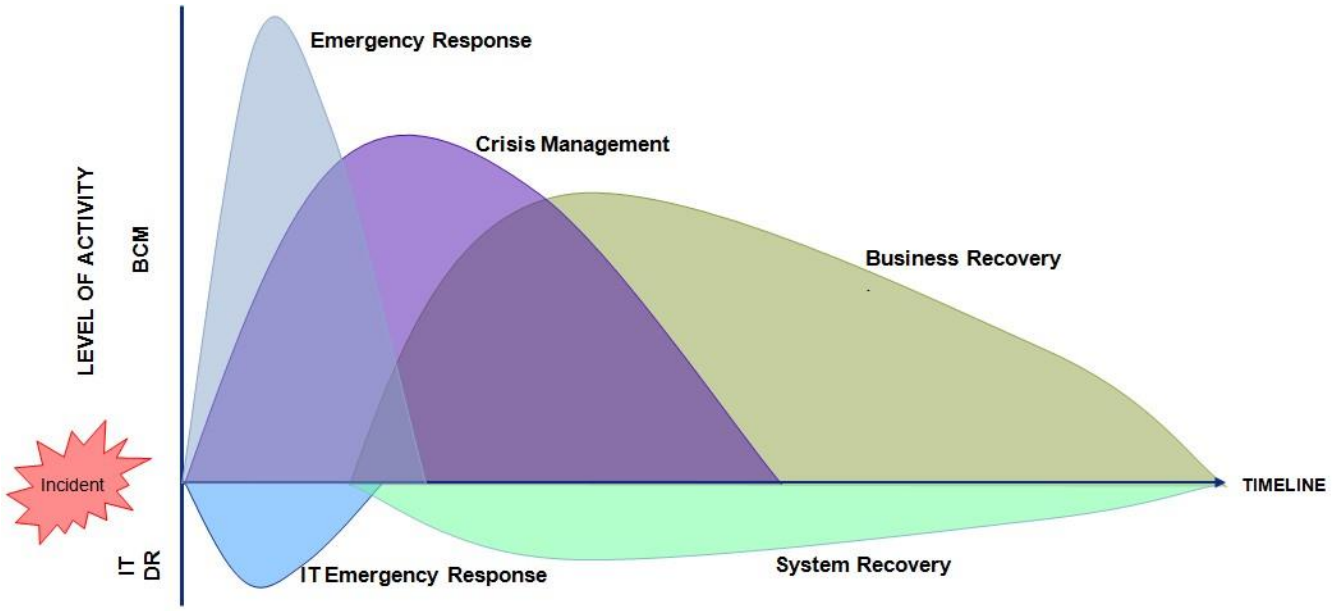
1.3.1.1. Protect the operations of the Municipality, consumers, licensees, stakeholders and staff by minimising the impact of significant interruption to the Municipality through the effective implementation and maintenance of ICT disaster recovery arrangements and solutions; and

1.3.1.2. Recover the critical prioritised operations and services, in a controlled manner to meet the requirements of the municipality, law, regulation or other governance factors.

1.4. IT DRP ROLE IN DRP

1.4.1. Figure 1 below shows the relationships that exist between the different elements of Business Continuity Management ("DRP") when an incident occurs. The IT DRP is defined to manage the recovery of IT services to allow for the continuation of critical business activities.

Figure 1. *The role of IT DRP in DRP*



The activities outlined in the above diagram include:

1.4.2. Emergency Response

1.4.2.1. Activities ULM as an institution engages in when a situation that poses an immediate risk to the health, life and property of ULM and/or its employees. The activities include urgent intervention to prevent a worsening of the situation and the management of incident response procedures (i.e. evacuations, liaising with emergency services, damage assessments etc)

Note: This portion of the response is entailed in the intuitional Business Continuity Plan

1.4.3. Crisis Management

1.4.3.1. Process by which ULM deals with a major event that threatens to harm the municipality, its stakeholders, or the general public. These activities normally include stakeholder management (i.e. government, media, public etc), collation of information and high-level instructions for business recovery activities.

1.4.4. Business Recovery

1.4.4.1. The activities that ULM engages in to restore operations. Recovery of IT applications is addressed by the IT DRP to support the restoration of business activities. The recovery of other operational requirements like workspace, manual documentation and office equipment is covered in a Business Continuity Plan.

1.4.5. IT Emergency Response and System Recovery

1.4.5.1. Activities ULM will follow to respond to emergency situations affecting IT systems

and restoring IT systems to normal. This is covered in this IT DRP document.

1.5. CUSTODIANSHIP AND OVERSIGHT OF THE ICT DRP

1.5.1. In order to ensure proper continuity of the IT systems and the information house in these datacenter it is important that the IT DRP be not in the custody of a single incumbent as this creates a single point of failure, instead a Committee needs to be set up to own and manage the living nature of the plan.

1.5.2. The ULM IT DRP is to be managed by a committee of key personnel chaired by the IT Manager. It should be noted that Each person in the committee is described herein by duty relevant to IT DRP and not by their daily job title. More than one function may be performed by one person.

1.5.3. The Committee will have the following functional responsibilities on an ongoing basis:

1.5.3.1. Determine current position on systems and its growth;

1.5.3.2. Provide documents and backup methodologies for off-site storage on an on-going basis;

1.5.3.3. Maintain critical systems overview and status;

1.5.3.4. Ensure that any new systems or changes in the IT network environment are included in the IT DRP;

1.5.3.5. Take full responsibility for their areas of functionality in the event of a disaster; and

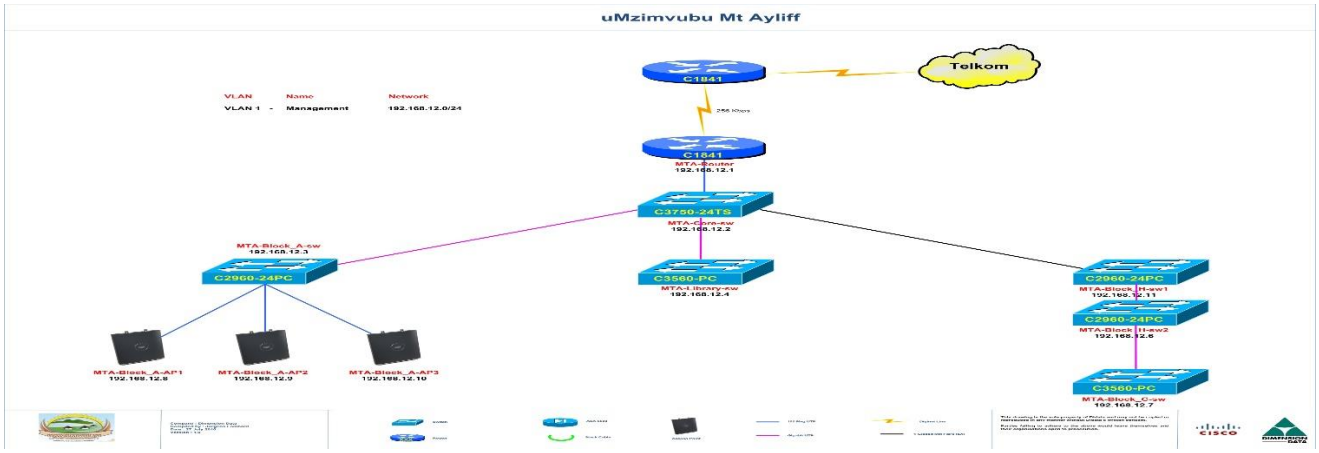
1.5.3.6. Ensure that recovery procedures are developed and tested in their areas.

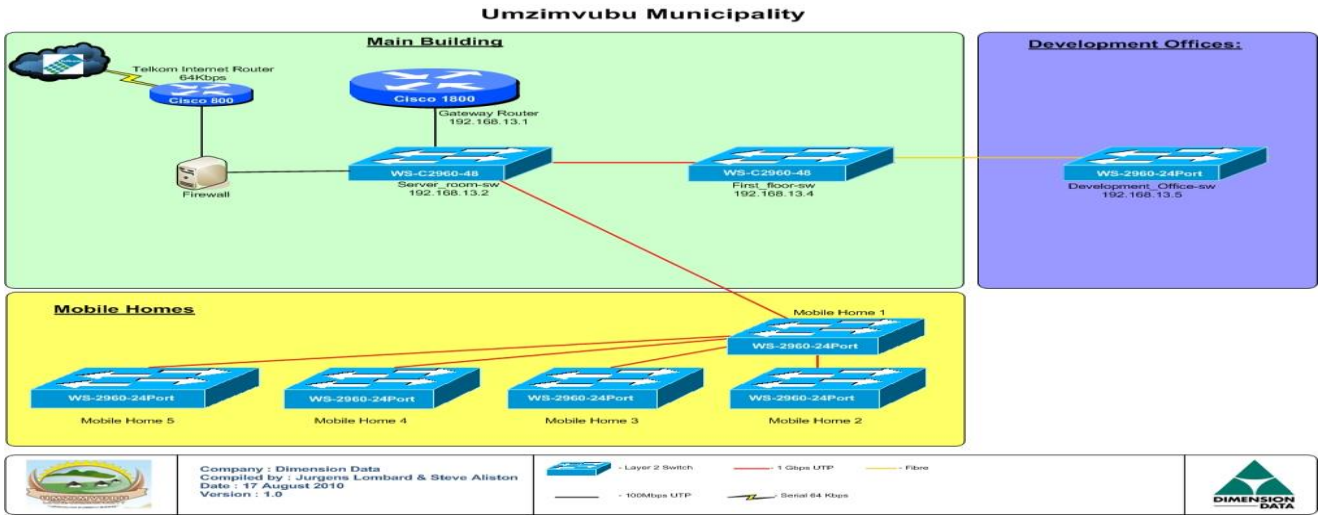
1.5.3.7. The committee comprises of the following members:

ROLE	NAME	CONTACT DETAILS
Chairperson – Team Leader (IT Manager)	Tozamile Funani	0795235309
Co-coordinator	Tinashe Fundira	076 511 3754
Infrastructure & Security Specialist	Sivenathi Cwati	0609606891

1.6. Umzimvubu Local Municipality ICT ENVIROMENT

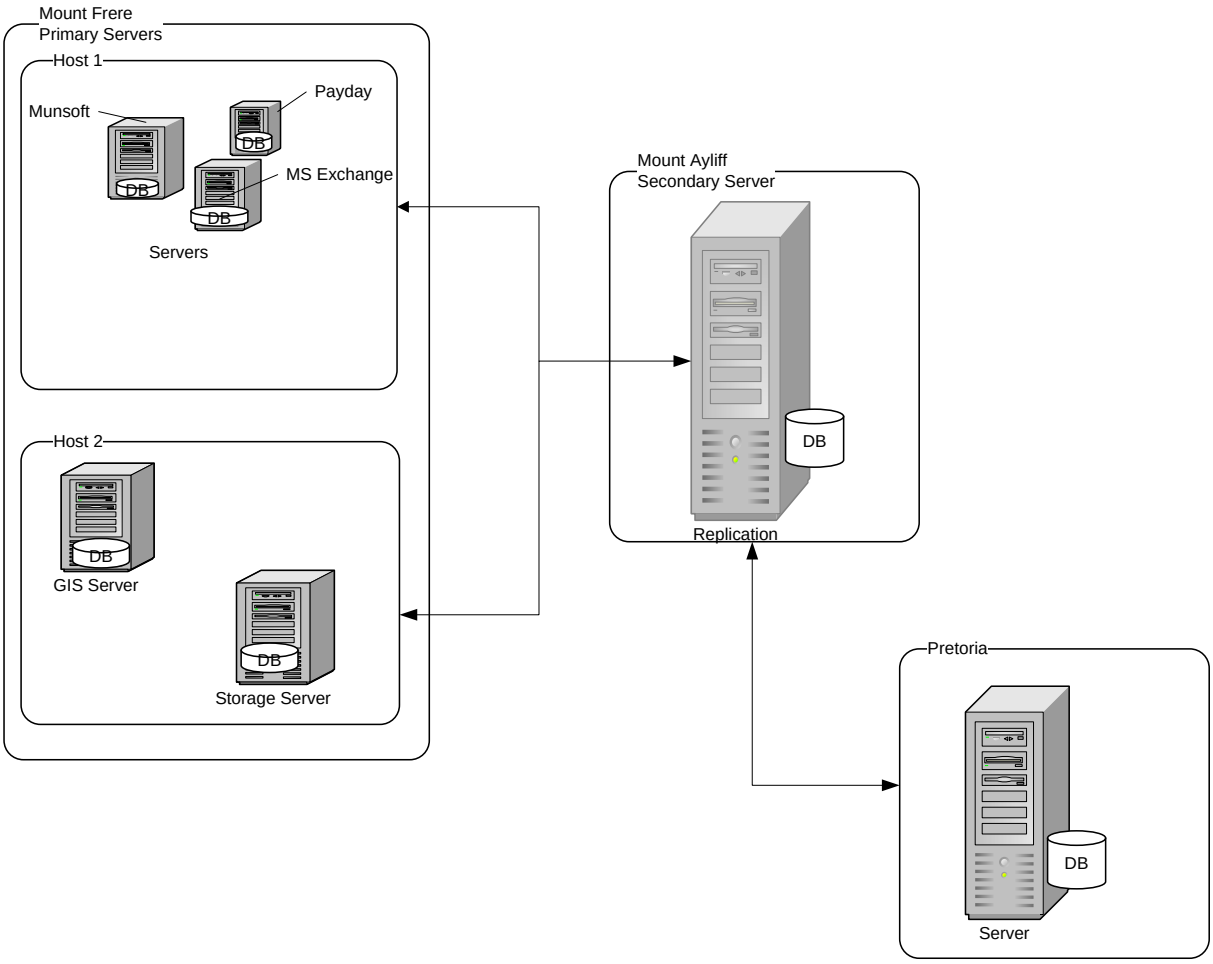
1.6.1. Network Diagram





1.6.2. ICT Replication Diagram

1.6.2.1. The current IT server replication environment is set up in the following manner



MOUNT FRERE SITE	MOUNT AYLIFF SITE	PRETORIA SITE
ULM has 5 primary servers that are running or hosted in Mount Frere. Munsoft, Payday and MS Exchange are situated in host1. Host 2 has GIS and Storage servers. Please note that the storage server is used to store/backup users folder every day between 10 A.M. to 12 P.M., if	The secondary server is situated in Mount Ayliff and this server replicates databases/files that are in the primary servers. The replications happen every day at 7 p.m. between primary	The Pretoria site copies all files that are in the secondary server/Mount Ayliff site every day after the secondary server/Mount Ayliff server has finished copying all files from

the laptop is not plugin on the network, the forced backup will automatically be done on the following day between 10 am to 12 pm. At 7 p.m. the data is copied from all primary servers to the secondary server in Mount Ayliff every day.	servers and secondary server.	the primary servers. A file can be retrieved back to the secondary server if something happened in the secondary server.

1.6.3. Server details

1.6.3.1. Currently the ULM has the following server infrastructure in its server farm

SERVER NAME	APPLICATION HOSTED	LOCATION	OPERATING SYSTEM
ZAULMEX 01	Exchange	Mt Frere	Windows Exchange 2016
ZAULMDC 01	Domain Controller	Mt Frere	Windows Server 2008
Munsoft	Munsoft	Mt Frere	Windows Server 2012
Storage	Storage Server	Mt Frere	Windows Server 2012
ZAULMDC 1	Replication	Mt Ayliff	Windows Server 2008

SECTION 2 – IT DISASTER REPONSE

2. IT DISASTER RESPONSE SECTION

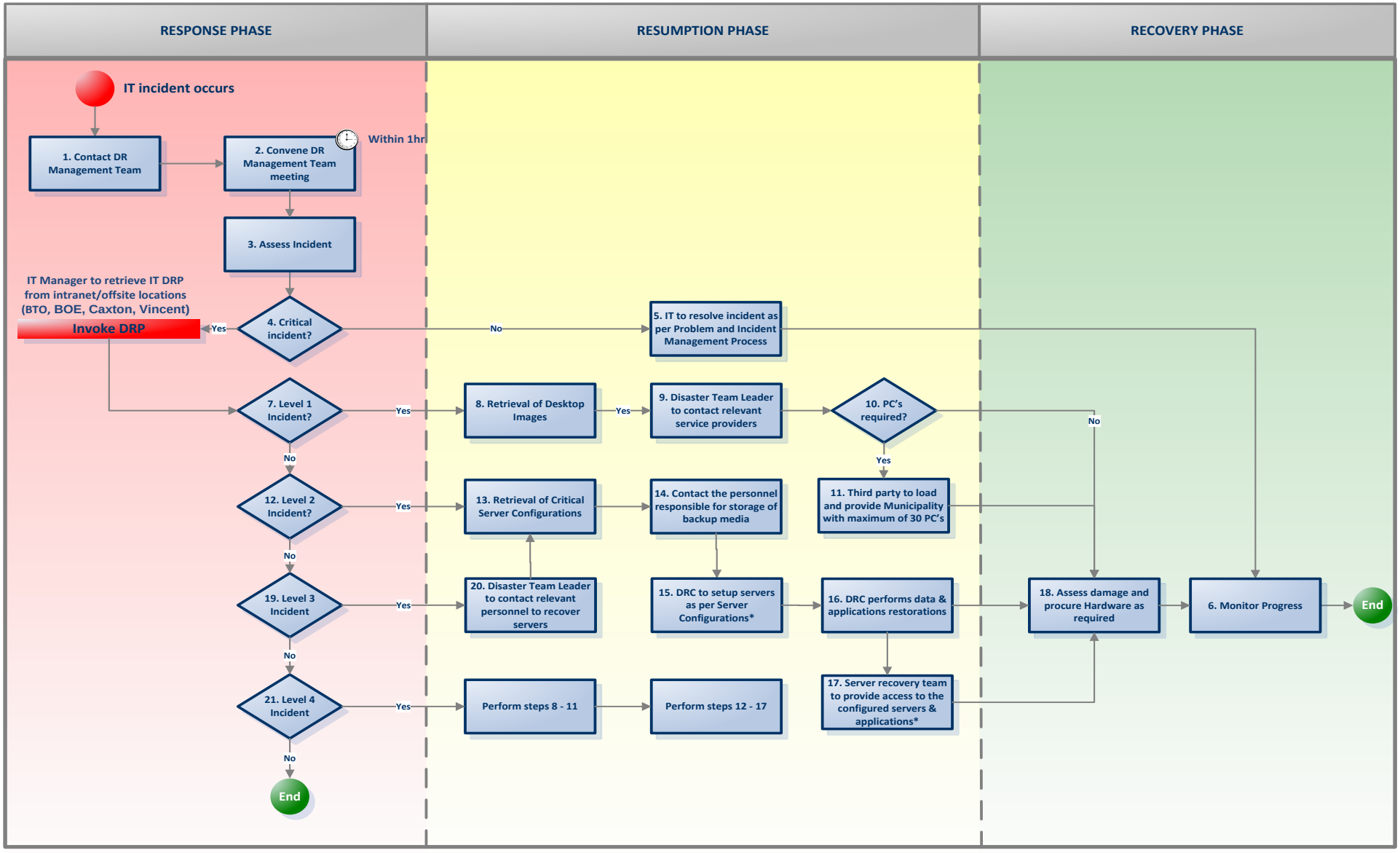
2.1. INCIDENT CATEGORIZATION

2.1.1. In the event of an incident occurring, the committee defined in section 1.5 would need to convene and assess the incident to determine its severity. Table 5 depicts the different incident types that would require invoking the DRP.

INCIDENT TYPE	INCIDENT NAME	INCIDENT DESCRIPTION
	Desktop computer unavailability	Occurs that results in more than 30 desktops/laptops that are in use by ULM employees are not available, such that the physical desktops, software and data is not available
	Server crash	Occurs resulting in 1 or more ULM servers crashing such that the server hardware is **still** available however the services/systems/data residing on those servers are
	Complete server unavailability	Occurs that results in the ULM servers being unavailable, such that the server hardware, software and data are
	IT Disaster	Occurs that results in **both** of the following scenarios: • The ULM servers are unavailable, such that the server hardware, software and data is unavailable; and • The desktops/laptops that are in use by ULM employees are not available, such that the physical
	Business Disaster	An IT incident occurs that results in the following scenarios: • The ULM servers are unavailable, such that the server hardware, software and data is unavailable; • The desktops/laptops that are in use by ULM employees are not available, such that the physical

2.1.2. Minor operational issues such as a faulty desktop computer, network connection issue, failed disc etc. should be covered by a Service Level Agreement (“SLA”) and normal operational processes. These minor issues will not form part of the IT DR plan unless they occur for an extended period of time, therefore affecting ULM’s continuity.

2.2. DISASTER RECOVERY PROCESS



2.3. DISASTER RECOVERY CHECKLIST

In the event of a disaster the following checklist should be complied to:

	ACTIVITY	RESPONSIBLE PARTY	INCIDENT TYPE					Done? (□/□)
			□	□	□	□	□	
1	Contact DR Management Team (refer to 4.1)	DR Team Leader	□	□	□	□	□	
2	Facilitate and manage initial briefing	DR Team Leader	□	□	□	□	□	
3	Invoke the IT DRP plan	DR Team Leader	□	□	□	□	□	
4	Perform and/or assist with the IT damage assessment	DR Team Leader DR Co-ordinator	□	□	□	□	□	
5	Contact relevant personnel responsible for storage of backup media (refer to 6.1.3)	DR Co-ordinator		□	□	□	□	
6	Liaise with ULM Manager Financial Services to start insurance claim procedures (if necessary)	DR Team Leader	□		□	□	□	
7	Establish hardware requirements (including PCs) based on damage incurred	DR Team Leader	□		□	□	□	
8	Set up IT helpdesk	DR Co-ordinator			□	□	□	
9	Manage and populate the incident log (refer to 7.1)	DR Co-ordinator	□	□	□	□	□	
10	Hold regular checkpoint meetings	DR Team Leader		□	□	□	□	
11	Record expenditures incurred during the recovery effort	DR Co-ordinator	□	□	□	□	□	
12	Order and procure hardware based on any hardware requirements	DR Co-ordinator	□		□	□	□	
13	Receive equipment that was ordered from vendors	DR Co-ordinator	□		□	□	□	

	ACTIVITY	RESPONSIBLE PARTY	INCIDENT TYPE					Done? (□/□)
			□	□	□	□	□	
14	Liaise with Incident management team to coordinate people, security and the media	DR Team Leader					□	
15	Set up alternative helpdesk number	DR Co-ordinator				□	□	
16	Lead and co-ordinate the recovery process at the designated backup site	DR Team Leader					□	
17	Setup and restore desktops	DR Technical Specialist	□			□	□	
18	Keep the overall crisis management team aware of developments on an ongoing basis	DR Team Leader				□	□	
19	Set up servers to perform recovery	DR Technical Specialist		□	□	□	□	
20	Load applications for business on restored servers on site	DR Technical Specialist		□	□			
21	Load applications for business at alternative site	DR Technical Specialist				□	□	
22	Manage, direct and coordinate helpdesk queries	DR Co-ordinator		□	□	□	□	
23	Test the restored system	DR Technical Specialist DR Co-ordinator		□	□	□	□	
24	Retrieve desktop images	DR Technical Specialist	□			□	□	
25	Populate Recovery form templates (refer to section 7)	DR Team Leader	□	□	□	□	□	

SECTION 3 – SYSTEM RECOVERY

3. SYSTEMS RECOVERY SECTION

3.1. RECOVERY TIME & POINT OBJECTIVES

3.1.1. For each department at ULM, the systems that are required to perform critical processes have been identified by ULM.

3.1.2. **Recovery time objective ("RTO")** – the first point at which a process requires access to the system. The RTO for each system is defined by the shortest RTO for the processes it supports.

3.1.3. **Recovery point objective ("RPO")** – the maximum data loss that is tolerable to the processes.

SYSTEM NAME	PRIORITY	RECOVERY TIMEFRAME
SERVER APPLICATIONS		
MunSoft	1	4 hours
PayDay	1	8 hours
Storage Server	2	8 hours
Email (Exchange Server)	1	8 hours
Internet	3	72 hours
Antivirus	3	72 hours
DESKTOP APPLICATIONS		
Microsoft Office (including Word, Excel, Outlook, and Access)	3	72 ours

3.2. 3RD PARTY SCHEDULE

Whilst the DRP is an internal plan that is driven by and has internal dependency for its success, the fact that there are 3rd party service providers which support or have applications running on the ULM network means that some system recovery procedures would need these 3rd party providers to co-operate in order to be timeously executed. This schedule seeks to highlight these 3rd parties for easy reference to the officials that will have invoked this plan at any time.

Furthermore, it is important that going forward the municipality adds to any new SLAs that the municipality expects a particular turnaround time in this recovery process should the provider be identified as a key enabler in making the process of disaster recovery possible.

Entity Name	Support Area	Contact person	Contact Details
Name of Service Provider	Financial Applications	Ndiafhi Rerani	**T:086 123 4862** **C:076 682 0123**
Name of Service Provider	Website	Heselyn Bramdeow	**T:031 514 7345** **C:084 417 6398**
Telkom	Internet Connectivity	Vikesh Parshad	**T:031 560 9476** **C:081 354 2122**

3.3. Incident log

				RESOLUTION			
INCIDENT NAME/DESCRIPTION	**AREAS AFFECTED**	**DATE**	**LOGGED BY**	**DATE**	**RESOLVED BY**	**CAUSE**	**HOW RESOLVED?**

The above template must be used to manage incidents that occur during the recovery of the IT infrastructure and applications.
The Incident Log template must be reproduced, printed and kept in a safe place together with the IT DR Plan.

73 ANNEXURE A: TESTING AND MAINTAINANCE PLAN

4. PURPOSE

4.1. The purpose of this Testing and Maintenance Guideline is to provide the ULM with a consistent approach to testing and maintaining the ULM ITDRP solution.

4.2. The overall objective of the Testing and Maintenance Guideline within the ULM is to ensure that the plan remain accurate, relevant and operable in the event of a major disruption. Externally, testing demonstrates compliance to regulatory requirements and internally, provides a level of comfort to the business with regards to the recoverability of its critical business functions.

5. TESTING

5.1. To ensure that the implementation is successful and to provide the assurance that the plans can be executed in the event of disaster, it is imperative to test the plan. Testing can take various forms and the results should be recorded for future reference and learning.

5.2. The objectives of the testing process include the following:

5.2.1. The testing process will not disrupt normal business operations;
5.2.2. The testing process must gradually increase the level of complexity;
5.2.3. The testing process will increase awareness within the ULM;
5.2.4. The testing process will uncover inadequacies within the plans and identify improvements; and
5.2.5. The testing process will test multiple scenarios to ensure that the plans are realistic.

The following table below depicts the level of severity for each testing option. ULM is currently in their first year of DRP planning and therefore will need to complete the simple to medium testing levels. The complex levels of testing will provide a greater level of comfort, but should only be conducted once all issues have been resolved through the lower levels of testing.

Note: ULM business / municipal operations should not be disrupted by the testing process.

Complexity	Exercise	Process	Test Areas	Testing Frequency
Simple	Walkthroughs / Read-through's	Review content of plan	• Test content	Annually / plan change
	Scenario tests	Use hypothetical situations to validate the response to the situation	• Test content • Test people	Annually
Medium	Component test	Use hypothetical situations to validate the recovery of individual components	• Test content • Test people • Test recovery	Annually
	Integrated test	Use hypothetical situations to validate the integration between plans	• Test content • Test people • Test recovery	Annually
Complex	Live runs	Run operations from the DR site	• Test full solution	Annually or less
	Unannounced testing	Simulate a real disaster and react as if one occurred	• Test full solution • Test response times	Annually or less

6. Testing Approach

6.1. The testing approach begins by conducting a pre-test workshop in which testing requirements will be decided and agreed on. The testing requirements will include:

6.1.1. Testing Process

6.1.2. Location

6.1.3. Objectives

6.1.4. Scope
6.1.5. Scenarios
6.1.6. Limitations
6.1.7. Budget
6.1.8. Setup requirements
6.1.9. Teams
6.1.10. Pre-test actions
6.1.11. Post-test actions
6.1.12. Testing activities

6.2. The actual test will follow the actions detailed in the pre-test workshop. The output of the test will provide documented observations and recommendations and the outstanding actions will be assigned to a responsible individual or team for resolution. The post-test workshop will provide an opportunity to reflect on the achievements and issues identified during the testing exercise.

6.3. UPDATING AND MAINTENANCE

6.3.1. ULMs environment is subject to change in people, processes, geography, and municipal strategy. To ensure that the DRP capability (including strategies and plans) continues to reflect the nature, scale, sensitivity and complexity of ULMs operations, it must be up-to-date, accurate, complete, exercised and understood by all relevant stakeholders and participants.

6.3.2. In essence, to retain their effectiveness the IT DRP must be vigorously maintained. In particular this will ensure the ongoing availability of competent and capable key people who clearly understand their roles and responsibilities in the plans in the event of a disaster occurring.

6.3.3. A cycle of constant enhancement, expansion and maintenance of the DRP programme is required to ensure that it is viable at any given time. Maintaining the DRP programme will ensure that it is:

6.3.3.1. Kept up-to-date taking into account changing circumstances;
6.3.3.2. Reviewed and updated at least annually; and Updated with feedback received from the tests performed or the invocation of the respective plans.

The table below details the required maintenance schedule:

Maintenance Requirements		
DRP Programme Element	Standard Occurrence	Exceptions
Business Impact Analysis (BIA)	Annually	Major process or systems change
Plans	At least once per year	Plan updates to be exercised within six months of major business changes
Testing/Exercising	At least once per year	Plan changes to be exercised within six months of major business changes

6.4. Once the plan has been updated the document control sheet within the plan must be completed and the updated; the soft copy of the plan must be saved on the DRP folder on

the shared drive and the hard copy must be kept with the DRP Coordinator of each department.

7. COMMENCEMENT OF THE POLICY

7.1. The policy will come into effect on the date signed by ICT Governance Champion

8. INTERPRETATION OF THE POLICY

8.1. All words contained in this policy shall have the ordinary meaning attached thereto, unless the definition or context indicates otherwise
8.2. Any dispute on interpretation of this policy shall be declared in writing by any party concerned.
8.3. The Municipal Manager shall give a final interpretation of this policy in case of written dispute.
8.4. If the party concerned is not satisfied with the interpretation, a dispute may then be pursued with the South African Local Government Bargaining Council.

9. PERMANENT/TEMPORAL WAIVER OR SUSPENSION OF THE POLICY

9.1. This policy may be partly or wholly waived or suspended by the ICT Governance Champion on temporary or permanent basis however the Municipal Manager/Council may under circumstances of emergency temporarily waive this policy subject to reporting of such waiver or suspension to Council

10. COMPLIANCE AND ENFORCEMENT

10.1. Senior management is required to ensure that internal audit mechanisms exist to monitor and measure compliance with this policy.

10.2. Failure to comply with this policy may result in disciplinary action, which may include termination of employment.

10.3. Any conduct that interferes with the normal and proper operation of the municipality's IT systems, which adversely affects the ability of other users to use those IT systems, or which is harmful or offensive to other users, shall constitute violation of approved IT policies.

10.4. The municipality management reserves the right to revoke the privileges of any user at any time.

11. AMENDMENT AND/OR ABOLITION OF THIS POLICY

11.1. This policy may be amended or repealed by ICT Governance Champion /Council as it may deem necessary.

12. Document Owner and Approval

12.1. The Municipality is the owner of this document. The Executive Management of the Municipality is responsible for ensuring that this policy document is reviewed regularly to ensure that it remains relevant to the organization.

12.2. This document was approved by the Executive Management and is issued on a version controlled basis under the signature of the ICT Governance Champion.

12.3. Every page of this document must also be initialed by the Governance Champion.