



**ICT Disaster Recovery Policy
2024/25**

SJK

Document No.	Revision	Print Date	Page
	1.3		Page 1 of 37

Contents

REVISION APPROVAL AND REVISION HISTORY.....	4
GLOSSARY OF TERMS AND ABBREVIATIONS	5
1. INTRODUCTION	8
2. OBJECTIVE OF THE PLAN	14
3. SCOPE OF PLAN.....	14
4. RESPONSIBILITY FOR PLAN MANAGEMENT AND ADMINISTRATION.....	14
5. PLAN FOR ICT DISASTER RECOVERY	15
5.1. Plan for business continuity	15
5.2. Disaster recovery plan	15
5.3. Disaster notification.....	16
6. DISASTER NOTIFICATION AND PLAN ACTIVATION.....	17
6.1. Initiation procedure indicating who should declare a disaster	17
6.2. Damage Assessment.....	17
6.3. Determination of Strategy to be followed.....	18
6.4. Activation of Recovery Site	19
6.5. Movement of backup materials.....	20
6.6. Notification of staff involved	20
6.7. Ordering of new equipment.....	20
6.8. Contact Details.....	20
6.9. Responsibilities of each party with regard to disaster recovery	21
7. SYSTEMS AND BUSINESS UNIT RECOVERY PROCEDURE.....	23
7.1. Business Unit Recovery.....	23
7.2. System Recovery.....	23
7.2.1. Install and test equipment	27
7.2.2. Recovery and test operating system and applications	27
7.2.3. Update to point of disaster	28
7.2.4. Process backlog transactions	28
7.2.5. Configure and test network connections (Local Area Network, Wide Area Network and remote access).....	28
7.2.6. Establish Communication links.....	28
7.2.7. Establish controls to ensure that security is maintained.....	28
8. PRIMARY SITE PROCEDURE	29
8.1. Establish site security.....	29

Document No.	Revision	Print Date	Page
	1.3		Page 2 of 37

8.2.	Perform a detailed damage assessment	29
8.3.	Obtain contractor and vendor estimates for repair or replacements	29
8.4.	Compile a salvage/refurbishment plan	29
9.	MONITOR PROGRESS	29
10.	RE-ESTABLISHMENT OF NORMAL OPERATIONS.....	30
10.1.	Order replacement furniture and equipment	30
10.2.	Install and test equipment	30
10.3.	Backup prior to move	30
10.4.	Recovery and Test operating system and applications	30
10.5.	Control and monitor completeness and accuracy of migration	30
10.6.	Process backlog.....	31
10.7.	Configure and test network	31
10.8.	Return to normal processing.....	31
11.	POST-RECOVERY REVIEW	31
12.	PLAN MAINTENANCE AND TESTING	31
13.	TRAINING THE RECOVERY TEAM	32
14.	DISASTER PREPAREDNESS	32
15.	APPENDIX A: DRP RECOMMENDED MAINTENANCE.....	33
16.	APPENDIX B: DRP TESTING	33
17.	APPENDIX C: DISASTER RECOVERY CONTACT DETAILS	37

List of Tables

Table 1:	Glossary of Terms and Abbreviations.....	5
Table 2:	Risk Assessment.....	9
Table 3:	Degrees of Damage.....	17
Table 4:	DRP Activation Criteria.....	18
Table 5:	Strategy to be followed when responding to a disaster	18
Table 6:	Recovery Site Details	19
Table 7:	Disaster Recovery Roles and Responsibilities	22
Table 8:	List of Critical Systems	23
Table 9:	Recovery Time Objective-Legend	24
Table 10:	Systems/Applications RTO.....	25
Table 11:	Systems/Applications Impact.....	26
Table 12:	Systems/Applications RPO	27

List of Figures

Figure 1:	Notification Tree.....	16
-----------	------------------------	----

Document No.	Revision	Print Date	Page
	1.3		Page 3 of 37

REVISION APPROVAL AND REVISION HISTORY

APPROVAL SIGNATURES RECORD			
APPROVALS	CHAIRPERSON NAME	SIGNATURE	DATE

REVISION NUMBER	PAGE NUMBER/S	CHANGES EFFECTED	DATE OF CHANGE
1.3	1-36	Review and update of Disaster Recovery Plan version 1.2	02-11-2023
1.3	1-36	Review and update of Disaster Recovery Plan version 1.2	13-06-2024

Document No.	Revision	Print Date	Page
	1.3		Page 4 of 37

SGK

GLOSSARY OF TERMS AND ABBREVIATIONS

Table 1: Glossary of Terms and Abbreviations

Abbreviation	Term	Description
BR Team	Business Recovery Team	Business unit operational teams responsible for the recovery of key business processes to a Revised Operating Level ("ROL") during the first stages of a crisis. Also responsible for the recovery of all business process during the normalisation phase of a crisis.
BIA	Business Impact Analysis	The process by which the impact of a disaster is on a business unit or function is assessed in terms of people, environmental, social, technological, legislative, and economic impacts.
BAU	Business As Usual	This indicates the normal state of business to which a recovery attempt should progress after the ROL has been achieved.
-	Battle box	A container (logical/physical) which is used at both the primary and recovery site to store recovery related equipment and supplies such as cordon tape, special forms etc.
-	Business Recovery Command Centre	<p>A predetermined location, room, or space from which an incident will be managed. Once established, this location should be the focal point for the organisation's response. An alternate meeting point should also be nominated in case access to the primary location is denied. The following categories of command centre locations can be selected:</p> <p>Hot site: An alternate facility that already has the computer, communications and environmental</p>

Abbreviation	Term	Description
		<p>infrastructure in place that is required to recover critical business functions or information systems.</p> <p>Warm site: An alternate processing site which is equipped with some hardware, and communication interfaces, electrical and environmental infrastructure which is only capable of providing backup after additional provisioning, additional software, or modifications.</p> <p>Cold site: An alternate facility that already has the environmental infrastructure in place required to recover critical business functions or information systems, but does not have any pre-installed computer hardware, communications network, etc. These must be provisioned at time of disaster.</p>
CFO	Chief Information Officer	Chief Information Officer
-	Disaster	A sudden, unplanned catastrophic event causing great damage or loss. Any event that causes an organisation to be unable to provide critical business functions for a pre-determined period.
-	Incident	A sudden, unplanned event causing damage or loss. Depending on the severity of the event, the incident may be classified as a disaster if the event causes an organisation to be unable to provide critical business functions for a pre-determined period.
RTO	Recovery Time Objective	The minimum amount of time in which a business process or ICT systems must be recovered to prevent significant financial loss or service

59K

Abbreviation	Term	Description
		degradation.
RPO	Recovery Point Objective	The maximum amount of data loss which a business process can sustain to limit the amount of rework to reconstruct the data or reduce the backlog in recapturing the data.
ROL	Revised Operating Level	A percentage value of the normal business processes which are recovered to sustain business activities until such time that all business process can be recovered following a disaster.

Document No.	Revision	Print Date	Page
	1.3		Page 7 of 37

S.G.K

1. INTRODUCTION

The primary focus of this document is to provide a plan to respond to a disaster that destroys or severely cripples the MLM's computer systems operated by the ICT division. The intent is to restore operations as quickly as possible with the latest and most up-to-date data available. This plan is designed to reduce the number of decisions which must be made when, and if, a disaster occurs.

This plan is a "living document." It is the responsibility of everyone involved in MLM's disaster recovery efforts to ensure that the plan remains current. Any changes to personnel, hardware, software, vendors, or any other item documented in the plan, must be brought to the attention of the ICT Manager.

This ICT Disaster Recovery Plan has been prepared based on the following key assumptions and dependencies:

- The Emergency Response Plan has been developed by MLM.
- The Crisis / Incident Management Plan has been developed by MLM.
- The MLM head office has been rendered inoperable for occupation due to the disaster and the Emergency and Crisis Management activities relating to the disaster have already been completed. This means that personnel based at the head office and visitors to the building have been evacuated.
- The roles and responsibilities which relate to Emergency Management, Crisis Management and Business Recovery are assigned to appropriate individuals and these individuals are trained and are familiar with their role in dealing with and responding to a disaster.
- It is assumed that an information management plan has been defined and implemented which governs the creations, modification, and deletion of data. In addition to this, it is assumed that all vital records and data are included in the backup schedule.
- Telecommunication networks are available and operational at the time of the disaster, which allows for telephone calls to be made.
- ICT systems hosted by third parties were not impacted during the disaster and are available for use by staff.
- Specific Risk Assessment ("RA") and Business Impact Analysis ("BIA") documents are up-to-date and reflect the current environment.
- Technical ICT system recovery documents are documented and available in the event of a disaster.
- It is assumed that an offsite recovery location has been procured and adequately configured to accommodate the chosen recovery strategy.

Incident vs. Disaster

An incident is a sudden, unplanned event causing damage or loss. Depending on the severity of the event, the incident may be classified as a disaster if the event causes the Municipality to be unable to provide critical business functions for a pre-determined period. Incidents can be addressed by the ICT Helpdesk or equivalent procedures however disasters are addressed via DRP.

Document No.	Revision	Print Date	Page
	1.3		Page 8 of 37

The following events may be classified as ICT Disaster for Mandeni Local Municipality.

A table below defines the potential threats that might occur and interrupt the normal operations at MLM. The probability that each threat may occur is also defined, as well as the impact that might be caused by the occurrence of each threat to the business functions of the Municipality. The effective workable recovery strategies that can be implemented have been identified.

For probability rating: 1= Certain, 2=Expected, 3=4=Possible, 5=Unlikely.

For Impact rating: 1=Very low, 2=Low, 3=Medium, 4=High, 5=Very High.

Risk level must be calculated to determine which risks require a maximum attention and should be attended first. Risk level is calculated as follows:

Risk level = Probability * Impact

NB: This table should be reviewed to ensure the ratings are true reflection of the MLM environment.

Risk Level Legend	
≥20 and =25	Critical
≥15 and <20	High
≥10 and <15	Medium
≤5 and <10	Low

Table 2: Risk Assessment

Potential Threat	Brief Description of Potential Threat Consequences	Probability Rating	Impact Rating	Risk Level	Preventative Measures in place
Fire	Loss of computer or network equipment through fire damage.	3	5	15	Fire smoke detectors shall be installed

Document No.	Revision	Print Date	Page
	1.3		Page 9 of 37

SJK

Potential Threat	Brief Description of Potential Threat Consequences	Probability Rating	Impact Rating	Risk Level	Preventative Measures in place
Theft	Theft of critical computer equipment which results in total services shut down and or non-availability> this will include theft of a files server, router, Telkom line, core switches etc.	4	4	16	Access control systems such as biometrics as well as intrusion detection systems shall be in place and periodically reviewed
Vandalism	Vandalism of ICT infrastructure by aggrieved Staff. Public and or any other person wishing to disrupt Municipal processes, these will include cutting of fibre cables, destroying servers or any other equipment on the network which is required to access various services offered by ICT	4	5	20	ICT infrastructure shall be stored in areas that are not easily accessible especially by unauthorised persons. Disaster recovery strategies shall be provisioned for
Sabotage (Denial of Service)	Deliberate sabotage of computer or network equipment for the purpose of rippling Municipal operations, this includes deletion of data and of data bases or making changes thereof.	5	2	10	SIEM tool shall be implemented to monitor and control access to the municipal network
Wind	Damage to ICT equipment or services due to wind etc.	1	3	3	ICT equipment shall be placed in an environment that meets acceptable

Document No.	Revision	Print Date	Page
	1.3		Page 10 of 37

U.G.K

Potential Threat	Brief Description of Potential Threat Consequences	Probability Rating	Impact Rating	Risk Level	Preventative Measures in place
					environmental and security standards
Hardware Failure	System or services failure hardware faults on server and core network equipment.	2	3	6	SLAs with vendors shall clearly address such incidents. Disaster recovery strategies shall be provisioned for
Accident	Loss or damage to ICT equipment and services due to accidents.	4	3	12	ICT equipment shall be placed in an environment that meets acceptable environmental and security standards
Negligence	System and service down time due to negligent actions by users, technicians, or Management's failure to take decisions on critical ICT requests.	2	3	6	ICT requests shall be addressed via helpdesk. Policy on acceptable and unacceptable usage shall be enforced

Document No.	Revision	Print Date	Page
	1.3		Page 11 of 37

S.G.K

Potential Threat	Brief Description of Potential Threat Consequences	Probability Rating	Impact Rating	Risk Level	Preventative Measures in place
Air Conditioning Failure	Air conditioners may stop functioning due to power failure or they might just break due to poor maintenance.	2	3	6	Air Conditioner is installed and shall be properly maintained. A secondary air conditioner shall be acquired.
Water Damage	Loss of computer or network equipment through water damage which can be caused by rain, floods water overflows from broken pipes or wind etc.	1	5	5	Water Sensor that automatically sounds the alarm when there is water shall be installed
Power Failure	Loss of power to the municipality due to load shedding, power supply shortage, cable theft, generator failure etc.	1	5	5	Backup Generator shall be purchased. Backup UPSs shall be purchased
Lightning Damage	Lightning may occur during the thunderstorm and cause damage in the Municipality.	1	5	5	Lightning Rods shall be installed
Hardware Failure	The hardware might fail due to poor hardware quality and poor maintenance.	2	3	6	Hardware and Software Maintenance Policy shall be developed

Document No.	Revision	Print Date	Page
	1.3		Page 12 of 37

S.S.K

Potential Threat	Brief Description of Potential Threat Consequences	Probability Rating	Impact Rating	Risk Level	Preventative Measures in place
Hackers	Someone can attempt to break into Municipal's computer systems, by using programming or technical knowledge to break the Municipal's system's security.	3	5	15	Firewall is installed. Automated Patch Management System shall be used.
Cyber Terrorism	This may occur when someone sends data, especially email that contains viruses for the purpose of destroying a particular system in the Municipality.	3	5	15	Antivirus software shall be regularly updated in all computers.

Document No.	Revision	Print Date	Page
	1.3		Page 13 of 37

S.g.k

2. OBJECTIVE OF THE PLAN

ICT has become an integral part of the day-to-day operations of the Municipality which has made it to be one of the key resources which are required to assist the Municipality in achieving its service delivery mandates.

The Municipality depends 100% on ICT for the following:

- Communicating with the outside world for funding, compliance, information exchange, linking to other government sectors etc.
- Payment of Councilors, Employees, Suppliers, and other creditors for services rendered.
- Research and access to online information for decision making and service delivery improvements.
- Formulating Council documents namely resolutions, letters, contracts etc.
- Emailing documents
- Financial Management and Control
- Payroll Management
- Billing for Municipal Services
- Reporting to Provincial and National Treasury

The objective of this plan is to ensure that Mandeni Local Municipality can recover the above services in the event of a disaster. The plan also identifies the risks and precautions to be taken to minimize loss in case of a Disaster.

3. SCOPE OF PLAN

The scope of this plan is limited to defining the rules and procedures to be followed in restoring the critical ICT services from a disaster. The plan also identifies the precautions that may be taken by the Municipality to ensure that they recover from any disaster with minimum loss.

This plan will cover the following domains:

- Disaster notifications plan and activation
- Systems and business recovery procedure
- Primary site procedures
- Reestablishing processes
- Recover and test system.
- Post recovery steps.
- Plan maintenance.

4. RESPONSIBILITY FOR PLAN MANAGEMENT AND ADMINISTRATION

It is necessary that this plan is regularly reviewed and updated. The Disaster Recovery Team (DRT) should meet annually to review the plan, to organize and review the outcomes

Document No.	Revision	Print Date	Page
	1.3		Page 14 of 37

SGK

of testing and modify the plan where appropriate. The DRT should report to the Director of Corporate Services. Another specialist should be co-opted on to the DRT as necessary.

The plan should be stored in a fireproof safe located in the Office of the Municipal Manager. A copy of the plan must be stored on the designated disaster recovery Site; there should also be a copy in the server room.

MLM has established an ICT Steering Committee therefore all requests to review the plan must be submitted to the committee for approval.

The document shall be controlled by updating the history and the document version.

5. PLAN FOR ICT DISASTER RECOVERY

5.1. Plan for business continuity.

ICT systems are constantly threatened by downtime and loss of data. The threats are real and come from many directions. Not all of them can be avoided, the most important question is – is the Municipality ready to deal with any application downtime and how fast can it go back online in times of serious system failures?

The Municipality needs to develop a practiced and logistic plan on how it will recover and restore partially or completely interrupted critical functions within a predetermined time after a disaster or extended disruption.

There are various methods that can be applied to ensure business continuity can be implemented with minimum cost to the Municipality.

With the above in mind the Municipality needs to have a business continuity strategy which can address minor incidents which can manifest themselves into disasters. Some examples which can be used to explain this are:

- What plan is there to back up the switchboard if he/she is off sick?
- Who will run the payroll if the payroll officer is off sick on the day payroll run is due?
- What plan is there to pay salaries and services providers if internet is down?
- Who will take over from the project managers should they decide to resign or leave the Municipality in the middle of the project.
- Are there manual systems in place to ensure business continues despite minor down times?

5.2. Disaster recovery plan

This disaster recovery plan (this plan) outlines the process, policies and procedures related to preparing for recovery or continuation of technology infrastructure to the Municipality after natural or human induced disaster.

The disaster recovery plan will not work if the Municipality is not prepared for a disaster, to do so the Municipality needs to have the following in place.

- Backups must be done daily.
- There must be remote backup storage.
- The disaster recovery site must be established and set up with basic services.
- The municipality must have insurance policies, SLA's, and warranties in place with credible service providers and vendors.

Document No.	Revision	Print Date	Page
	1.3		Page 15 of 37

SJK

- This plan must be updated monthly and tested quarterly.
- Everyone who will take part in the recovery process must be trained in this plan and their roles must be clearly outlined.

5.3. Disaster notification

The purpose of this section of the DRP is to enable the ICT division and the relevant stakeholders to notify all users quickly, efficiently, and effectively in the event of a disaster. The goal is to improve response time and to quickly mobilize all resources and bring back the ICT service online in the quickest time possible.

Notification Procedure:

- i. The following notification tree is to be followed in notifying users of an ICT disaster once it has been declared as such in terms of this DRP.

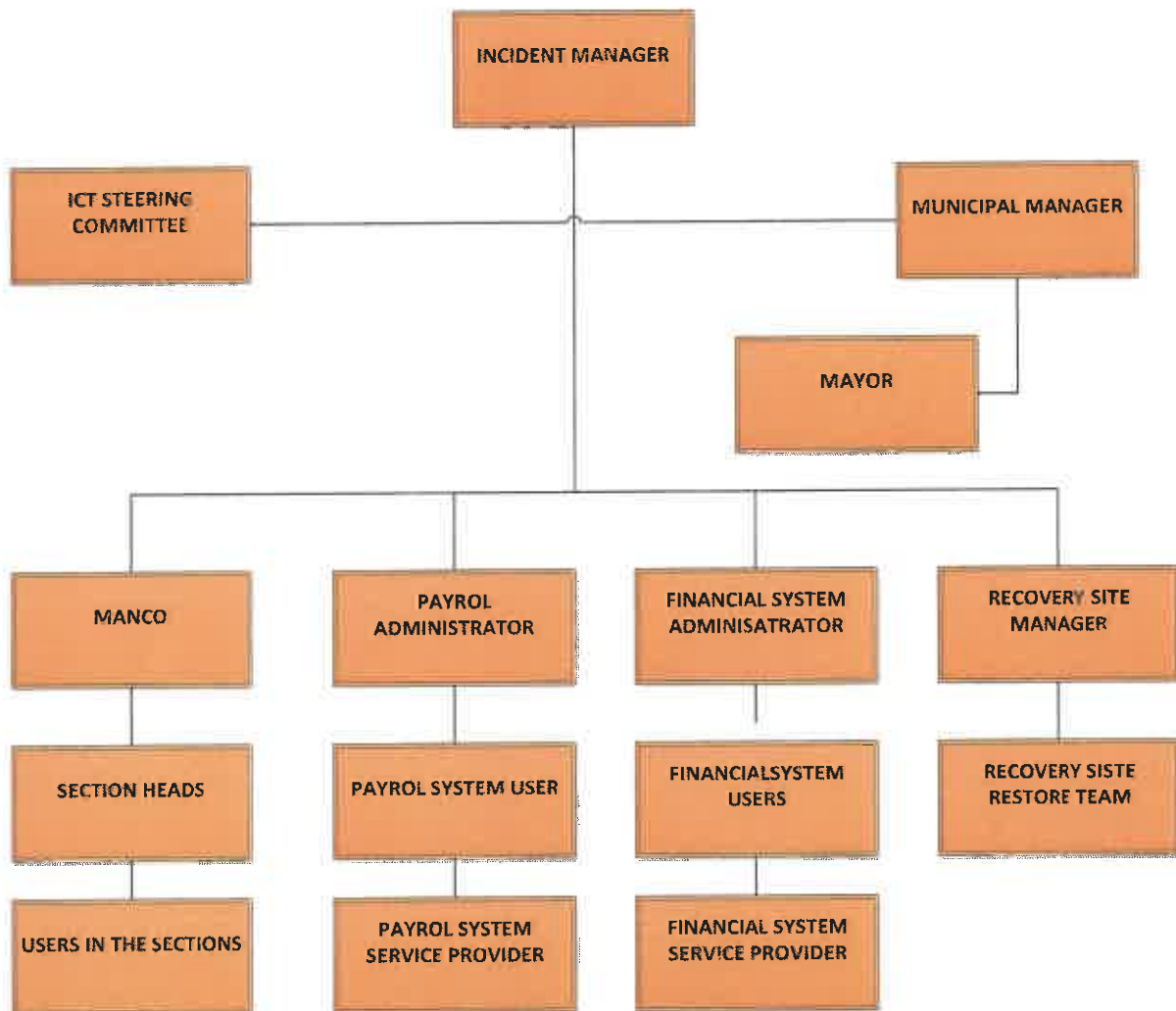


Figure 1: Notification Tree

- ii. Each member of the DRT must keep a copy of this plan and the latest contact details

Document No.	Revision	Print Date	Page
	1.3		Page 16 of 37

of all Municipal Staff at work and at home. If you have a vehicle, a copy must be kept in the car as well. The DRT lead must ensure that there are 10 copies or more of the DRP stored in a fireproof safe at the disaster recovery site.

- III. This plan and its content are highly confidential and should not be released to anyone without the written consent of the Municipal Manager.
- IV. Each of the above contact points shall have their own contact list which shall be kept in the server room and updated as and when there are changes in personnel.

6. DISASTER NOTIFICATION AND PLAN ACTIVATION

6.1. Initiation procedure indicating who should declare a disaster.

In an unlikely instant where a disaster has occurred which is likely to affect MLM ICT services and or the normal operation of the Municipality, the priority will be to ensure safety of the personnel on site and take measures to contain the situation including summoning emergency services.

As soon as safely possible, the ICT Manager or the Incident Director should be called to appraise the Situation. The ICT Manager must confirm with the Fire Officer that it is safe to enter the safe before entering. If the assessment confirms that significant damage, destruction, or loss has occurred then a disaster must be declared.

Once the ICT Manager has classified this, the Incident Director must then be notified and informed of the extent of the damage to determine the required intervention and notification.

6.2. Damage Assessment

Conducting a damage assessment after disaster is critical as it will allow the DRT to:

- Determine the severity and magnitude of the damage.
- Quantify the equipment impacted by the disaster.
- Determine whether existing resources will be sufficient for the disaster.

The damage assessment must be rapid, detailed, and accurate and adhere to the following:

- It should be completed and submitted to the Incident Director within 24 hours of the event.
- The data collected will be analyzed to determine the measures to be taken in response to the disaster.
- It must determine whether the need to activate the recovery site is necessary.
- Delays in completing the assessment may result in institutional damage.

There are 4 degrees of damage as shown in the table below.

Table 3: Degrees of Damage

Damage	Description	Response
Destroyed	Damage of data or equipment beyond repairs	Replace all destroyed equipment

Document No.	Revision	Print Date	Page
	1.3		Page 17 of 37

Damage	Description	Response
Major	Partly damage to data and or equipment	Replace damaged parts
Minor	Mild damage to data and or equipment	Fix faulty parts
Affected	Disturbance to some ICT services	Effect backup plan

The assessment may be unique for each system however the following areas must be addressed in the assessment:

- Cause of the outage or interruption.
- Damage to the information system or data.
- Potential for additional disruption of damage.
- Physical infrastructure status.
- Information system inventory and functional status.
- Requirement for repair or replacement; and
- Estimated time to recover or restore.

Table 4 below shows criteria to activate the DRP.

Table 4: DRP Activation Criteria

Information system Damage	Facility condition	System criticality	Anticipated disruption length
Total	Destroyed	High	30 days or more
Partial	Major	High	15 days
None	Major	High	15 days
none	Affected	High	10

6.3. Determination of Strategy to be followed.

The determined decision statement must determine the strategy to be followed when responding to a disaster:

Table 5: Strategy to be followed when responding to a disaster.

Service affected	State	Duration	Strategy
Internet and or Email	Not accessible	3 days	Use backup 3G or other service

Document No.	Revision	Print Date	Page
	1.3		Page 18 of 37

Service affected	State	Duration	Strategy
Domain Controller	Hardware/damage	2 days	Log call with HP
Any and or All	Loss through disaster event	Permanent	Replace and restore from backup
Pastel	System crash	1 day	Call Pastel to restore system and replace hardware
Fortinet firewall	System crash corruption	1 day	Re-installed system or replace if destroyed
Network device or cables	Damage	2 days	Replace
Front Peripherals	Hardware / software failure	3 days	Repair or replace
Data	Data loss and or corruption	1 day	Restore form backup
All IT Services	Facilities destroyed and not accessible	5 days	Activate recovery site

6.4. Activation of Recovery Site

MLM will designate a disaster recovery site which will be used to recover from a disaster. The following sites will be established for recovery system operations until restoration of the original site.

It must be noted that these sites will be activated in terms of this plan and each site must keep a copy of this DRP and contact details of every critical stakeholder.

The following table describes the sites that will be used for disaster recovery.

Table 6: Recovery Site Details

Site	Type	Description	Setup time
Protection services	Cold Site	Remote site with adequate space for servers etc. with telephone and Data line including electricity and Environmental controls.	24 Hours

Document No.	Revision	Print Date	Page
	1.3		Page 19 of 37

Site	Type	Description	Setup time
Technical services	Hot site	Alternate server room adequately sized to support the network and system infrastructure.	8 Hours

The above listed disaster recovery sites will be activated based on the following criteria.

- The primary site must be totally un-usable.
- Network services must be anticipated to be down for more than 15 days.
- The primary site must be non-functional.
- Use of current infrastructure must be impossible.

6.5. Movement of backup materials

MLM currently has 3 ways backup solution (NAS, tape, and cloud backup solution) to back up information, in case of a disaster these will be used to recover data by the ICT division.

6.6. Notification of staff involved.

The staff involved in the disaster recovery will be notified in terms of this plan. Each staff member must be issued a letter of indemnity in which they must agree to be part of the DRT. These staff members must be always present when testing this plan.

6.7. Ordering of new equipment

The MLM supply chain processes can be cumbersome and may delay the recovery time when ordering replacement or new equipment for the disaster recovery. To avoid this, the Municipality must:

- I. Ensure that all equipment and data are covered by a reputable Insurance company.
- II. Enter into Service Level Agreement with an ICT service provider for the provision of ICT infrastructure services in case of disaster this must cover the following critical devices and or software:
 - a. Servers
 - b. Firewalls
 - c. Switches
 - d. Network cables.
 - e. Printer
 - f. Desktops
 - g. Laptops
 - h. Data points and patch panels
 - i. Server cabinet
 - j. Routers

6.8. Contact Details

Document No.	Revision	Print Date	Page
	1.3		Page 20 of 37

A database of the critical contact persons and vendors must be kept in the server room and the disaster recovery sites. The ICT Manager must update these contact details monthly to ensure that the database is up to date and current.

The contact list must be attached to this plan and copies must be kept as follows:

- Server room.
- Recovery Site.
- Copies issued to the members of the DRT.
- Stored in the safe with backup tapes.

6.9. Responsibilities of each party about disaster recovery

To have a full proof disaster plan, the MLM needs to assemble the right team who will be key role players in formulating, implementing, maintaining, and reviewing the computer systems disaster recovery plan.

As a minimum the team will consist of:

- The Head of Corporate Services (Incident Director)
- Chief Financial Officer
- Head of Information and Communication technology (ICT)
- ICT Service providers for each system
- Payroll administrator
- Financial system user
- Dually designated user for each application
- Technical services representative
- ICT Steering Committee

The team is headed by the Head Corporate Services who is a member of the organization's senior management team. She/he will bring a broad strategic perspective to the team and provide a link to the major decision-making forums of the organization.

The ICT Manager has a detailed knowledge of network topology, hardware development, security precautions, backup systems and technical specifications.

Finance and payroll are among the most mission critical systems for the MLM. The system users have a detailed knowledge of these systems, their backup and recovery precautions.

Lastly the DRT must involve a senior representative from Technical Services. Many potential disasters could involve fires, floods etc. and the priority in these cases will be to evacuate the building safely. Additionally, the disaster will most often be discovered by a member of the building or care taking staff, and the plan will have to clearly identify lines of communication so that key personnel can be informed, and the plan activated if appropriate.

The Technical Services representative will bring a detailed knowledge of the procedures for raising the alarm evacuation procedures, including emergency services, building and electricity repair services.

Each team member must have a copy of the plan and copies must be placed in a secure location at each of the Municipality's buildings, namely, Protection services, Technical Services and at the Head Office.

The responsibilities of the above mentioned shall be the following:

Document No.	Revision	Print Date	Page
	1.3		Page 21 of 37

Table 7: Disaster Recovery Roles and Responsibilities

Role Player	Responsibilities
Incident Director	Declares the incident and runs the command Centre
CFO	Lead the Financial application disaster recovery team
Head ICT	Conduct an assessment and recommend the strategy to be followed in response to a disaster.
ICT Service Providers	Provide specialised support and advice on their applications and or hardware
Payroll super user	Restore payroll to the last backed up status
Financial system Super User	Restore the finance application to the last backed up status
Supply Chain Manager	Provide logistical support to fast track the procurement of Recovery equipment

7. SYSTEMS AND BUSINESS UNIT RECOVERY PROCEDURE

7.1. Business Unit Recovery

The recovery of each business unit may vary, the following priority will be considered when recovering from a disaster:

- a. ICT division (server room and network)
- b. Finance Department
 - I. Financial Management (Debtor and Creditors)
 - II. Supply chain.
 - III. Billing
 - IV. Payment
 - V. Payroll
- c. Office of the Municipal Manager
- d. Corporate services
- e. Technical services
- f. Planning and Development

7.2. System Recovery

This section details the systems that are required to perform critical processes for each Business Unit hosted at the head office. These have been collected by means of a Business Impact Assessment ("BIA"). The information that was collected is as follows:

- **RTO:** The amount of time that elapses between the failure occurring and the application and data being recovered and brought back online i.e., acceptable amount of downtime. e.g., 0-6 hours, 6-12 hours, 24 hours, etc.
- **RPO:** The point in time to which MLM needs to recover its data for a particular application i.e., how much data loss can be tolerated. e.g., last successful backup performed.
- **Impact:** A ranking system of critical, high, medium, and low is used to determine the impact that might be caused by loss of or disruption to each application. This helps to determine applications' recovery priorities.

From an organizational perspective, the business processes can be mapped to a set of critical application systems. These applications can therefore be seen as enablers in the process of conducting business. The following table identifies and describes the critical systems for the MLM with an indication of where they are hosted (location).

Table 8: List of Critical Systems

#	System	Description	Location
1.	Pastel	Financial System	On premise
2.	PAYDAY	Payroll System	On premise

Document No.	Revision	Print Date	Page
	1.3		Page 23 of 37

#	System	Description	Location
3.	AMS360	Infrastructure Asset Management System	Cloud based
4.	ArcGIS	Geo-Database System	Cloud based
5.	Conlog	Prepaid electricity system	Hosted system
6.	PASTEL & DEBTPACK	Enterprise Resource Management	On premise
7.	Ms Exchange	Email system	On premise

The table below shows the first point of recovery for each system within MLM, based on their shortest identified Recovery Time Objective (RTO). RTO refers to the length of time a business can operate without a particular function or application. The RTO is based on the maximum tolerable time or period the MLM can survive without a particular function or application. A table also defines the impact that may be caused by the outage of the function or application. Impact is rated as Critical, High, Medium, and Low, respectively.

Table 9: Recovery Time Objective-Legend

Criticality	Description
1 – Critical (C)	Very serious/disastrous impact: Inability to conduct business or perform business functions.
2 – High (H)	Serious impact: Partial or very little ability to conduct business or perform business functions.
3 – Medium (M)	Manageable impact: Impaired ability to conduct business or perform business functions.
4 – Low (L)	Limited to minimal impact: Disruption with limited impact on ability to conduct business or performance of business functions.

Table 10: Systems/Applications RTO

#	System	RTO										
		Immediate	0-6 hrs	6-12 hrs	12-24 hrs	24-48 hrs	5 Days	1 Week	2 Weeks	1 Month		
1.	Pastel	√										
2.	AMS360							√				
3.	PAYDAY	√										
4.	ArcGIS											√
5.	Conlog	√										
6.	PASTEL & DEBTPACK	√										
7.	Ms Exchange		√									

Table 11: Systems/Applications Impact

#	System	Impact									
		Immediate	0-6 hrs	6-12hrs	12-24 hrs	24-48 hrs	5 Days	1 Week	2 Weeks	1 Month	
1.	Pastel	C	C	C	C	C	C	C	C	C	C
2.	AMS360	L	L	L	M	M	H	C	C	C	C
3.	PAYDAY	C	C	C	C	C	C	C	C	C	C
4.	ArcGIS	L	L	L	L	L	M	M	H	C	C
5.	Conlog	L	M	H	C	C	C	C	C	C	C
6.	PASTEL & DEBTPACK	C	C	C	C	C	C	C	C	C	C
7.	Ms Exchange	C	C	C	C	C	C	C	C	C	C

Recovery Point Objective (RPO) reflects the estimated point in time to which recovery would be made based on current configurations and operations. The exact recovery point for each server will vary due to the time when backup takes place and when the disaster occurs.

Table 12: Systems/Applications RPO

#	System	RPO		
		Previous Day Backup	Last Transaction	To last monthly backup
1.	Pastel		√	
2.	AMS360			√
3.	PAYDAY		√	
4.	ArcGIS			√
5.	Conlog		√	
6.	PASTEL & DEBTPACK		√	
7.	Ms Exchange	√		

Each system is unique and as such shall be recovered differently; the following steps will be taken when recovering the systems.

7.2.1. Install and test equipment.

Systems are dependent on hardware; therefore, the first step will be to procure or revive the hardware required to run the system in the following order of priority.

- Servers
- Network peripherals and cables.
- Desktops and Laptops
- Printers

Each of the above listed equipment will be installed and tested by the system recovery team which will consist of the ICT Technicians, system vendors and super users.

7.2.2. Recovery and test operating system and applications

Once the equipment has been installed and tested the next step will be to install the operating system and the applications, these shall be installed as follows:

- Network operating system on all servers.
- Microsoft Exchange (email services)
- Finance application system.
- Payroll application
- Antivirus

- Firewall and proxy servers.
- Desktop operating Systems
- Desktop applications and clients

Note: Screen shots of each application configuration must be captured and attached to this plan. The ICT division must update these screen shots and when there is a configuration change.

7.2.3. Update to point of disaster.

The data will be restored to the last successful and available backup which was made of all the systems in the network. The recovery software media and the license keys including contact details for the support must be attached to this plan and copies must be kept in a category safe on the recovery sites.

Upon total system recovery the data and databases will be restored in the following order:

- Finance system database.
- Payroll database
- User files
- Mailboxes

7.2.4. Process backlog transactions.

A data capturing team will be set up to capture transaction backlogs from the manual system. Each system will have a team of data capturers. Batch files will be used to capture and upload large data into the different applications.

7.2.5. Configure and test network connections (Local Area Network, Wide Area Network, and remote access)

- a. The Local Area Network will be set up and configured to use both wireless and cat6e technologies.
- b. Laptops will connect via wireless, and desktops will use cables including printers.
- c. The Wide Area Network will be connected using 3G and Telkom VPNS or whichever other connection to the internet is available. The internet service providers will be contacted to route SMTP and HTTP traffic accordingly.

7.2.6. Establish Communication links.

Telecommunications and data services will be totally dependent on the availability of network signal and connection. The two critical communication links required for operations are the internet connection and the voice connection.

The disaster recovery site must be equipped with an ADSL line, PRI, or ISDN line and 3G cards to be used for recovering communication links.

7.2.7. Establish controls to ensure that security is maintained.

Document No.	Revision	Print Date	Page
	1.3		Page 28 of 37

Data protection and equipment security is of vital importance during the recovery process. The security officer will be responsible for ensuring that all equipment and data are safe and secure.

PC lock cables must be used to secure computer equipment to prevent theft at the recovery site. The server must be kept in a secure location preferable away from the users.

8. PRIMARY SITE PROCEDURE

8.1. Establish site security.

The DRT must first ensure that it is safe to return to the recovery site with approval from the fire officer. Site security must then be assessed in line of the following:

- Parameter Security
- Logical Access
- Physical Security
- Environmental security

8.2. Perform a detailed damage assessment.

A damage assessment team will be informed to assess the damage and to facilitate the replacement of equipment. This team shall be made up of the ICT Manager, Asset Controller, Supply Chain Manager, and the assessor from the insurance company. The responsibility of this team will be to conduct a detailed assessment of the damage and to compile an assessment report which must stipulate the following:

- List of damage equipment
- The impact of the damage
- The cost of the equipment lost.
- Recovery
- Future recommendations

8.3. Obtain contractor and vendor estimates for repair or replacements.

The Supply Chain division must use the damage assessment report to facilitate the procurement of the damaged equipment and software. Some equipment and software may require that the Supply Chain division be vendor specific.

8.4. Compile a salvage/refurbishment plan.

Every disaster is unique and as such the damage will vary, therefore crucial equipment, services and data which are salvageable will be repaired or furnished considering E-waste and cost service.

9. MONITOR PROGRESS

Progress will be monitored by the incident's director from the incident command Centre. The head of each disaster team will give four hourly reports to the command Centre.

Document No.	Revision	Print Date	Page
	1.3		Page 29 of 37

10. RE-ESTABLISHMENT OF NORMAL OPERATIONS

The process of re-establishing normal operation must be done as follows:

10.1. Order replacement furniture and equipment.

The list of equipment to be ordered will be identified by the disaster assessment team and funding shall be sourced from the insurance if applicable else from other means possible, the last resort being from a loan or why entering a budget contract with treasury.

10.2. Install and test equipment.

New equipment will be installed by the ICT technician who will design the installation checklist which will also be used to test the equipment. The users will also assist in testing the equipment and will also check if all their data has been recovered.

10.3. Backup prior to move

Before returning to the primary site, all data which was processed at the recovery site must be backed up and tested to ensure that it can be recovered. Two copies of this data must be kept avoiding a disaster of data loss and corruption. The data must be backed up on two different backup media and technologies.

10.4. Recovery and Test operating system and applications

The primary site systems will be restored from the recovery site, the procedure to be followed will be as follows:

- Restore the server in the server room.
- Install all network equipment in the server room.
- Connect the firewall routers and switches and configure them.
- Install the finance application and other mission critical systems.
- Restore user files and profiles.
- Restore exchange.
- Re-direct SMTP and http traffic to its original IP address
- Restore users' desktops and printers.

10.5. Control and monitor completeness and accuracy of migration.

The following control and testing mechanisms will be used to monitor the migration process.

Email	: telnet port 25 of the SMTP server, router, and external mail relay server
Internet	: Access an external internet site
Proxy	: go to www.whatismyipaddress.com to verify proxy server
Payroll	: check the last month rolled over and print a list of all employees
Finance	: Setup a quality assurance team that will check and test each module
Database	: Run database integrity checks
User files	: Each user must check their files to ensure they have been restored.
Active Directory	: Force active directory replication and check the event log for errors.

Document No.	Revision	Print Date	Page
	1.3		Page 30 of 37

10.6. Process backlog.

Each business unit must set up a team to assist with the processing of any backlog that may have occurred during the recovery process. This will include responding to email etc.

10.7. Configure and test network.

The network will be setup and tested during the installation process however the configuration and testing will involve the following:

- Password protecting all switches, printers, and other peripherals.
- Firewall configuration includes mail and internet filtering.
- Configure WSUS
- Optimization of DNS, DHCP and replication services
- Apply the security policy recommendations.
- Setup backup and test it.
- Re-deploy the antivirus solution and update all machines.
- Conduct the network audit.

10.8. Return to normal processing.

The success of the disaster recovery process will be realized when the users are back to normal working operations pre-disaster. Following the above process will ensure that the users are back online.

11. POST-RECOVERY REVIEW

Once the site has been successfully restored and all the services and users are back online the ICT Steering Committee will conduct the special meeting to assess and evaluate the response time of the DRT.

The DRT will then conduct the post disaster review and update this plan accordingly where necessary.

The ICT Manager must update all network diagrams and conduct a detailed ICT audit so that the plan is updated. The list of new equipment must be submitted to the insurance company and any changes to the IP addresses must be communicated with the ISP and the various stakeholders.

12. PLAN MAINTENANCE AND TESTING

The ICT Manager is the custodian of this plan. He/she will be responsible for updating the plan and ensuring all the critical stakeholders have the latest version of the plan. A quarterly test must be conducted to analyze the effectiveness of the plan and to ensure minimum down time in case of a disaster.

The objectives of testing the Plan are as follows:

- Simulate the conditions of an ACTUAL recovery situation.
- Determine the feasibility of the recovery process.
- Identify deficiencies in the existing procedures.
- Test the completeness of the recovery information stored at the offsite storage location.
- Train members of the DRT.

Document No.	Revision	Print Date	Page
	1.3		Page 31 of 37

The initial test of the plan will be in the form of a structured walk-through and should occur within two months of the plan's acceptance. Subsequent tests should be to the extent determined by the ICT Manager that are cost effective and meet the benefits and objectives desired.

13. TRAINING THE RECOVERY TEAM

The purpose of this training is twofold:

- To train recovery team participants who are required to execute plan segments in the event of a disaster.
- To train MLM management and key employees in disaster prevention and awareness and the need for disaster recovery planning.

The training of MLM personnel in disaster recovery planning benefits and objectives is crucial. A DRP must have the continued support from MLM's personnel to ensure future effective participation in plan testing and updating. It is not sole the responsibility of the ICT Manager to initiate updates to the DRP. All personnel must be aware of the basic recovery strategy; how the plan provides for rapid recovery of their information technology systems support structure; and how the plan's effectiveness may be compromised without notification to the ICT Manager as their business operations evolve and expand significantly.

It is the responsibility of each recovery team participant to fully read and comprehend the entire DRP, with specific emphasis on their role and responsibilities as part of the recovery team. On-going training of the recovery team participants will continue through plan tests and review of the plan contents and updates provided by the ICT Manager.

14. DISASTER PREPAREDNESS

A critical requirement for disaster recovery is ensuring all necessary information is available to assure that hardware, software, and data can be returned to a state as close to "pre-disaster" as possible. Specifically, the section addresses the backup and storage policies as well as documentation related to hardware configurations, applications, operating systems, support packages and operating procedures.

Backup/Recovery tapes are required to return systems to a state where they contain the information and data that was resident on the system shortly prior to the disaster. At MLM, full backups of all servers are performed weekly.

Document No.	Revision	Print Date	Page
	1.3		Page 32 of 37

TEST OBJECTIVES:

1. _____
2. _____
3. _____

Table 23: Sample Recovery Test Plan

Task #	Task Description	Completed?
1	Determine appropriate test date	
2	Schedule a test date	
3	Meet and plan preliminary test criteria and goals	
4	Determine who will be participating in the test	
5	Meet with entire test team to discuss goals and objectives	
6	Determine hardware requirements	
7	Determine software requirements	
8	Determine printing requirements	
9	Determine network requirements.	
10	Determine what other documentation needs to be brought to the test location	
11	If necessary, call vendors with licensing dependent products and get required information to run products on the test systems	
12	Get network specific information	
13	Final meeting to review plans	
14	Perform test following procedures in the test script	
15	Conduct post-test debriefing before leaving test site	
16	Remove data from test system disk drives	
17	Destroy confidential information	
18	Gather documentation from all test teams	
19	Complete documenting the test	
20	Meet with test participants and analyse the test	
21	Update the Plan based on test results	

ICT Disaster Recovery Plan Testing Forms

TEST DATE: __/__/__ TEST # ____

Estimated Start	Actual Start	Finish	Step Description

3. During the test, were there any deviations from the plan?

4. Were all the materials used during the test retrieved from an offsite source? If not, what items from the data center or on-site offices were used?

Document No.	Revision	Print Date	Page
	1.3		Page 36 of 37

SGK


17. APPENDIX C: DISASTER RECOVERY CONTACT DETAILS

[Attach up-to-date contact details here]

PREPARED BY: P.E NTANZI

DATE OF ADOPTION BY COUNCIL: 10 JULY 2024

COUNCIL RESOLUTION NO: C01


MUNICIPAL MANAGER
S.G KHUZWAYO

11/07/2024
DATE

Document No.	Revision	Print Date	Page
	1.3		Page 37 of 37