Information Communication and Technology (ICT)

Matjhabeng Local Municipality

(MLM)

IT Continuity Plan

Document Version: 1.0 (Draft)

POLICY DOCUMENT CONTROL PAGE

Document Number	ICT Continuity Plan v1.0

ORIGINATOR

Custodian	ICT Department
Responsible Person	IT Manager

APPROVAL

Approval date by Legal Services	
Approval date by Risk	
Approval date by ICT Steering Committee	
Approval date by Council	

CIRCULATION

Effective Date	
Circulated by	Pulane Rakotsoane

POLICY REVIEW

Recommended Review Period	Every 3 years

This plan has been endorsed by the Matjhabeng Local Municipality IT Manager:

_____

Pulane Rakotsoane

IT Manager   DATE: /   /

This plan has been endorsed by the Matjhabeng Local Municipality Municipal Manager:

_____

Thabiso Tsoaeli

Municipal Manager   DATE: /   /

Table of Contents

1. INTRODUCTION

1.1 EXECUTIVE SUMMARY

Planning for the Matjhabeng Local Municipality in the aftermath of a disaster is a complex task. Preparation for, response to, and recovery from a disaster affecting the operations of the department(s) requires the cooperative efforts of many stakeholders in partnership with the functional areas supporting the "business" of the Municipality.

This Document records the ICT recovery plan (DRP) indicating the steps to be taken to recover critical IT infrastructure.

Should the IT Systems encounter a disaster that prevents them from functioning, The IT Department and IT Service providers should be prepared to provide adequate computational data storage and data communications services and facilities at an off-site disaster recovery source for the participating applications.

The offsite Disaster Recovery Resource is a fully operational data centre that is prepared to host the critical systems such as Cash Drawer, File Sharing, Syntell, Solar, Telephony, PayDay, Paperless Agenda, Microsoft End User Computing (EUC) and MS Office 365 and Email.

1.2 HOW TO USE THIS DOCUMENT

Use this document for

- Recovering critical IT infrastructure from a disaster

- Planning for the continuity of the critical and essential business functions at the Municipality.

- As a checklist of preparation tasks.

- For training personnel.

1.3 PURPOSE

This Disaster Recovery Plan establishes procedures to recover the Matjhabeng Local Municipality systems following a disruption. The following objectives have been established for this plan:

- Maximize the effectiveness of contingency operations through an established plan that consists of the following phases:

  − **Notification Phase** to detect interruption and alert.

  - **Activation phase** to assess damage and to activate the plan.

  − **Recovery phase** to restore temporary ICT operations and recover damage done to the original system.

  − **Reconstitution phase** to restore ICT system processing capabilities to normal operations.

- Identify the activities, resources, and procedures needed to carry out Municipal systems processing requirements during prolonged interruptions to normal operations.

- Assign responsibilities to designated Municipal personnel and provide guidance for recovering systems during prolonged periods of interruption to normal operations.

- Ensure coordination with other Municipal staff who will participate in the Disaster Recovery planning strategies.

- Ensure coordination with external points of contact and vendors who will participate in the Disaster Recovery planning strategies.

1.4 APPLICABILITY

The Matjhabeng Local Municipality Disaster Recovery Plan applies to the functions, operations and resources necessary to restore and resume ICT systems operations. The Disaster Recovery Plan applies to Matjhabeng Local Municipality and all other persons associated with Matjhabeng Local Municipality ICT systems as identified under Section 3, Roles and Responsibilities.

1.5 SCOPE

The ICT continuity plan is aimed at restoring Matjhabeng Local Municipality critical ICT systems to enable business to continue to operate after a disaster has rendered any or all the systems inoperable.

2. AUDIENCE

The Disaster Recovery Champions and the associated teams responsible for ICT and security at system and operational levels can use the principles presented in this document. This description includes the following personnel:

- Management team responsible for overseeing ICT operations or business processes that rely on ICT systems.
- System administrators responsible for maintaining daily ICT operations
- Information System Security Officers (ISSOs) and other staff responsible for developing, implementing, and maintaining an organization's ICT security activities
- System engineers and architects responsible for designing, implementing, or modifying information systems.
- Users who employ desktop and portable systems to perform their assigned job functions
- Other personnel responsible for designing, managing, operating, maintaining, or using information systems.

In addition, emergency management personnel who may need to coordinate facility-level contingency may use this document with ICT Disaster Recovery Planning activities.

3. ICT MISSION CRITICAL SYSTEMS

The following ICT provided services are important for the Matjhabeng Local Municipality's daily operations

- Cash Drawer
- Syntell
- Solar
- PayDay

- Paperless Agenda

The following ICT provided services are essential but not critical for the Matjhabeng Local Municipality's daily operations:

- Office 365 and Email

- Internet and Intranet

- Computer Equipment

- Telephony,

The details of these systems, including Vendor, Functionality and Location are found in *Appendix B.*

4. DRP TEAMS & RESPONSIBILITIES

The DR plan will rely principally on key members of management and staff who will provide the technical and management skills necessary to achieve a smooth technology and business recovery.

The following teams have been developed and trained to respond to a Disaster event affecting the ICT system. Disaster Recovery Plan establishes several teams assigned to participate in recovering Matjhabeng Local Municipality system operations.
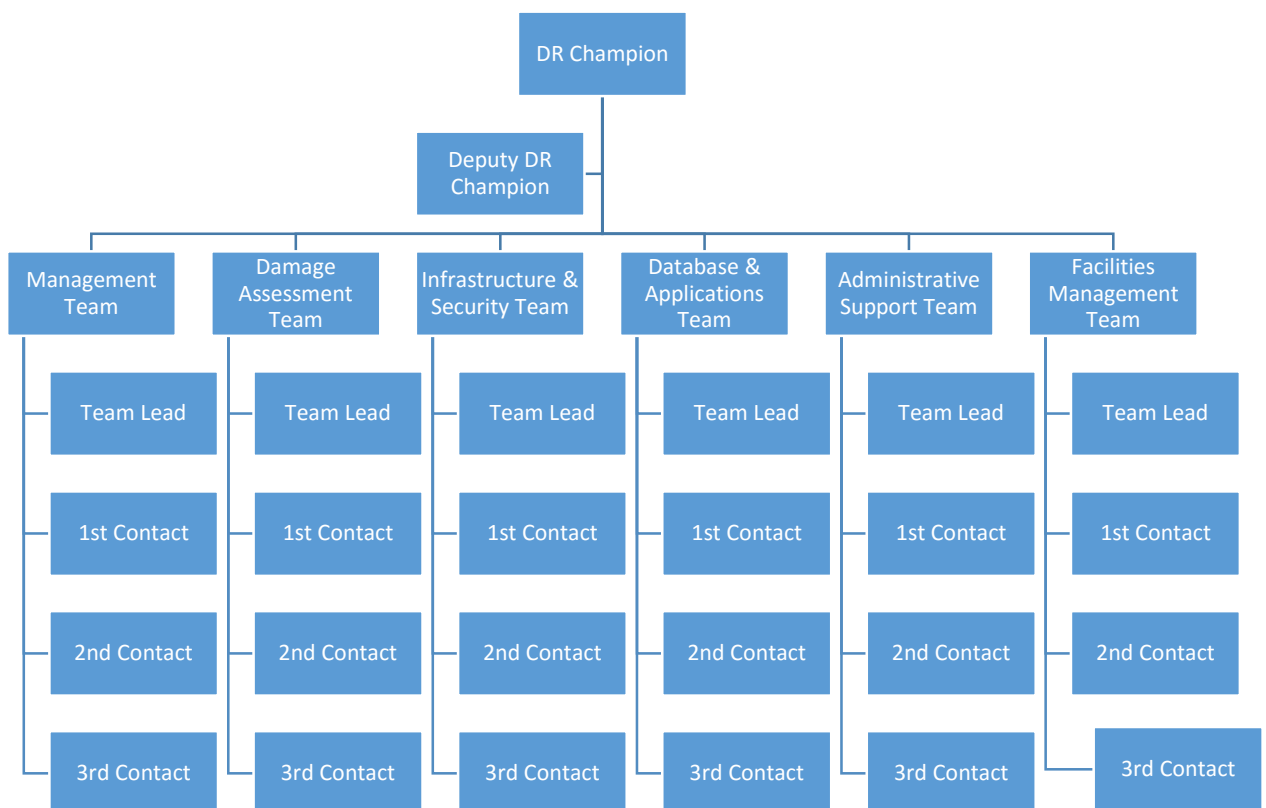
- DRP Champion

- DRP Management Team

- DRP Damage Assessment Team

- Server and LAN Recovery Team

- Database & Applications Recovery Team

- Hardware Salvage Team

- Security (IT & Physical) Team

- Telecommunications & WAN Recovery Team

- Alternate Site Recovery Coordination Team

- Original Site Restoration/Salvage Coordination Team

- Test Team

- Communications & Administrative Support Team

- Procurement Team (Equipment & Supplies) Team

All the teams above will work together under the supervision of the DRP Champion and the Management team and all will be responsible for recovery of the Matjhabeng Local Municipality computer systems environment and all applications. Members of the DRP teams include personnel who are also responsible for the daily operations and maintenance of Matjhabeng Local Municipality systems. The Damage Assessment team leader directs the DRP team. Teams, information details, roles and responsibilities are described in *Appendix F*

Below is depiction various DRP teams organogram.

```
                          DR Champion
                              |
                       Deputy DR
                       Champion
                              |
  ┌───────────┬──────────────┬──────────────┬──────────────┬──────────────┬──────────────┐
Management   Damage      Infrastructure &  Database &    Administrative   Facilities
  Team      Assessment    Security Team   Applications   Support Team    Management
             Team                            Team                          Team
    |           |             |               |              |              |
Team Lead   Team Lead     Team Lead       Team Lead      Team Lead      Team Lead
    |           |             |               |              |              |
1st Contact 1st Contact   1st Contact     1st Contact    1st Contact    1st Contact
    |           |             |               |              |              |
2nd Contact 2nd Contact   2nd Contact     2nd Contact    2nd Contact    2nd Contact
    |           |             |               |              |              |
3rd Contact 3rd Contact   3rd Contact     3rd Contact    3rd Contact    3rd Contact
```

5. NOTIFICATION AND ACTIVATION PHASE

The Notification/Activation Phase defines the initial actions taken once a system disruption or emergency has been detected or appears to be imminent. This phase includes activities to notify recovery personnel, assess system damage, and implement the plan. At the completion of the Notification/Activation Phase, recovery staff will be prepared to perform contingency measures to restore system functions on a temporary basis.

5.1 NOTIFICATION PROCESS

The notification sequence is listed below:

- The first responder is to notify the Disaster Recovery Planning Champion.

- All known information must be relayed to the Disaster Recovery Planning Champion.

- The Disaster Recovery Planning Champion will instruct the Damage Assessment Team Leader to begin assessment procedures.

- The Damage Assessment Team Leader is to notify team members and direct them to complete the assessment procedures outlined below to determine the extent of damage and estimated recovery time.

More notification procedures defining this phase are described in *Appendix C.*

5.2 DAMAGE ASSESSMENT PROCESS

The Damage Assessment Team assesses and determines the following:
- Cause of the emergency or disruption and potential for additional damage;
- Status of physical infrastructure such as structural integrity of computer room, condition of electric power, telecommunications, and heating, ventilation, and air-conditioning
- Inventory and functional status of ICT equipment such as fully functional, partially functional, and non-functional
- Type of damage to ICT equipment or data such as water damage, fire and heat, physical impact, and electrical surge

- Items to be replaced such as hardware, software, firmware, and supporting materials
- Once the impact to the system has been determined, the appropriate teams will be notified of updated information and planned response to the situation.
- Notifications will be executed using the procedures described in *Appendix G*
- The Damage Assessment team will personally visit the site and make an initial determination of the extent of the damage. Based on their assessment, all or part of the Disaster Recovery Plan will be initiated. The team will decide:
- If the action plan requires the assistance of other recovery team members, those team members will be notified.

6. PLAN ACTIVATION PHASE

The Disaster Recovery Plan should be activated only when the damage assessment indicates that one or more of the activation criteria for that system are met. If an activation criterion is met, the Disaster Recovery Champion will activate the plan.

Plan and Activation phase will be executed using the procedures described in *Appendix C.*

6. RECOVERY PHASE

Recovery operations begin after the contingency plan has been activated, damage assessment has been completed (if possible), personnel have been notified, and appropriate teams have been mobilized.

Recovery phase activities focus on contingency measures to execute temporary ICT processing capabilities, repair damage to the original system, and restore operational capabilities at the original or new facility.

At the completion of the Recovery Phase, the ICT system will be operational and performing the functions designated in the plans. All the plans for operations in the recovery site are documented in *Appendix G.*

6.1 RECOVERY PROCESS

Procedures assigned to the appropriate recovery team address the following actions:
- Obtaining authorization to access damaged facilities
- Notifying internal and external business associated with the system

- Obtaining necessary office supplies and work space
- Obtaining and installing necessary hardware components
- Obtaining and loading backup media
- Restoring critical operating system and application software
- Restoring system data
- Testing system functionality including security controls
- Connecting system to network or other external systems
- Obtaining user acceptance

The sequence of recovery activities are documented in the plans found in *Appendix G*

7. RECONSTITUTION PHASE

In the reconstitution phase, operations are transferred back to the facility once it is free from the disaster after effects, and execution phase activities are subsequently shut down. If the original system or facility is unrecoverable, this phase also involves rebuilding. Hence the reconstitution phase can last for a few days to a few weeks or even months, depending on the severity of the destruction and the site's fitness for restoration.

The following major activities occur in this phase:
- Ensuring adequate infrastructure support, such as electric power, water, telecommunications, security, environmental controls, office equipment, and supplies
- Installing system hardware, software, and firmware. This activity includes detailed restoration procedures as documented in the Recovery Phase
- Establishing connectivity and interfaces with network components and external systems
- Testing system operations to ensure full functionality
- Backing up operational data on the contingency system and uploading to restored system
- Shutting down the contingency system
- Terminating contingency operations
- Securing, removing, and/or relocating all sensitive materials at the contingency site
- Arranging for recovery personnel to return to the original facility.

Reconstitution phase will be executed using the procedures described in *Appendix H.*

8. POST DISASTER RECOVERY REVIEW

Two debriefings are schedule on the days immediately following the hot site test. One is for the Team participants to assess the systems software recovery procedures. The second is for the user community who participated in the recovery.
These meetings are general discussions to address:

- Areas where the exercise was successful;

- Problems that were encountered; and

- Suggestions for improvements.

Based on the conclusions, an action list of improvements to be made prior to the next test is developed and responsibility for implementing them is assigned
Post Disaster Recovery Review phase will be executed using the procedures described in *Appendix H.*

9. TESTING THE DISASTER RECOVERY PLAN

The Matjhabeng Local Municipality ICT Disaster Recovery plan is tested to confirm the accuracy of individual recovery procedures and the overall effectiveness of the plan. The test provides an opportunity to identify any omissions in recovery procedures or documentation and to determine whether personnel are adequately prepared to perform their assigned duties. Therefore, IT regularly schedules exercises of its disaster recovery plan at the Recovery Site. The following areas are addressed in the Disaster Recovery test:

- Readiness of Disaster recovery site
- System recovery on an alternate platform from backup media
- Coordination among recovery teams (including service providers)
- Internal and external connectivity
- System performance using alternate equipment and support teams
- Restoration of normal operations
- Notification procedures.

Testing the Disaster Recovery Review Plan will be executed using the procedures described in *Appendix I.*

8 TRAINING AND AWARENESS

In addition to regular test, team members, managers and support team receive annual refresher training regarding the emergency alert procedures.

Recovery personnel will be trained on the following plan elements:

- Purpose of the plan
- Cross-team coordination and communication
- Reporting procedures
- Security requirements
- Team-specific processes (Notification, Damage Assessment, Activation, Recovery, and Reconstitution Phases)
- Individual responsibilities (Notification, Damage Assessment, Activation, Recovery, and Reconstitution Phases).

All other users are provided with appropriate disaster recovery awareness information.

9 PLAN MAINTENANCE

The Disaster Recovery Champion is responsible for the maintenance of this document. The Disaster Recovery Plan need to be kept up to date with the current organisation environment.

Matjhabeng Local Municipality plan will be reviewed for accuracy and completeness annually. At a minimum, the plan reviews will focus on the following elements:

- Operational requirements
- Security requirements
- Technical procedures
- Hardware, software, and other equipment (types, specifications, and amount)
- Names and contact information of team members
- Names and contact information of vendors, including alternates

- Alternate and offsite facility requirements
- Vital records (electronic and hardcopy).

Additionally, the plan will be updated in the event an actual disaster occurs. The plan will be reviewed and updated at a convenient point after initial responses to the disaster have been completed.

10 PLAN APPENDICES

The appendices provide key details not contained in the main body of this plan. The appendices associated with this document are:

Appendix A: GLOSSARY OF TERMS

Appendix B: LIST OF ICT MISSION CRITICAL SYSTEMS

Appendix C: SPECIFIC TECHNICAL, OPERATIONS AND MANAGEMENT REQUIREMENTS

Appendix D: EMERGENCY CONTACT NUMBERS

Appendix E: CRITICAL SYSTEM PROCESSING INFORMATION

Appendix F: DISASTER RECOVERY SUPPORT TEAMS

Appendix G: DAMAGE ASSESSMENT PROCEDURES

Appendix H: RECOVERY SITE OPERATION PROCEDURES

Appendix I: DRP RECOVERY GUIDES