MORETELE LOCAL MUNICIPALITY

ICT SERVICE CONTINUITY AND DISASTER RECOVERY PLAN

Policy number	ICT-004-2026
Date of Management engagement	26 June 2026
Resolution Number	13001001-06-2026
Council Approval	30 June 2026
Review Date	26 June 2027
Signature: Municipal Manager	

Change Record

Author	Date	Change Version
Moretele Municipality	July 2016	1.1

Reviewers

Name	Date	Version
P.N Mahlo	January 2022	2
R.J Mophuting	January 2022	2

Name	Date	Version
RJ Mophuting	April 2023	3
ICT Steering committee	April 2023	3

Name	Date	Version
ICT UNIT	23 June 2026	4
ICT Steering committee	26 June 2026	4

TABLE OF CONTENTS

1. DISASTER DEFINITION

TERM	DEFINITION
MM	Municipal Manager
MLM	Moretele Local Municipality
ICT	Information and Communication Technology
DRP	Disaster Recovery Plan
BRP	Backup Resumption Plan
DISASTER	Shall mean any event that prevents the ICT systems from providing services needed by the participating applications for aperiod of 72 hours or longer
DRS	DISASTER RECOVERY SITE
DR	DISASTER RECOVERY

2. Executive Summary

This ICT Service Continuity and Disaster Recovery Plan (SCDRP) provides a framework for ensuring that critical municipal services and ICT systems continue operating during and after disruptive incidents. The plan outlines procedures for responding to emergencies such as cyberattacks, fire, flooding, power failures, hardware failures, and other events that may affect the Municipality's ICT infrastructure and operations.

The objective of this plan is to minimise downtime, protect municipal data and systems, restore services efficiently, and ensure continuity of essential municipal operations. The plan also establishes responsibilities, recovery strategies, communication procedures, and testing requirements necessary to maintain operational resilience.

3. INTRODUCTION

This documnent outlines the ICT Service Continuity and Disaster Recovery strategies adopted by Moretele Local Municipality. The plan is intended to ensure that critical ICT systems, infrastructure, applications, and services can be restored within acceptable timeframes following a disruption or disaster..

The ICT department is responsible for hardware, software, data, servers, firewalls and network infrastructure, and telecommunications services to ensure that systems remain available and operational..

Potential disasters include, but are not limited to:

Conditions that could be declared a disaster include, but not limited to

- extended electrical power outage,
- extensive fire, smoke, and water or explosion damage.
- Cybersecurity incidents and ransomware attacks
- Server or network failures
- Hardware or software failures
- Theft or vandalism
- Human error

4. SCOPE

This strategy document covers all systems that are managed and maintained by the ICT, that which includes all applications that are running on the database that aims managed by the Municipality ICT function and the Third Party Service provider for the ICT back-end management and support.

The scope further extends to all ICT systems and services that are operated, hosted, or supported by third-party service providers contracted by the Municipality, ensuring that such providers comply with the requirements of this plan and applicable policies.

Systems and ICT infrastructure Covered

The following critical systems and services are included within the scope of this plan:

- Microsoft Exchange Services
- Active Directory Services
- SQL Database Systems
- Network and Data Center Infrastructure (including servers, switches, Firewall and supporting hardware)
- Financial and Payroll Systems

- Internet and Communication Services

5. PURPOSE

The main purpose of this document is to outline a strategy that will guide the implementation of a disaster recovery process and will enable the recovery of ICT systems and minimize the impact to the business operations during and after a disaster has occurred. The plan describes the preparation and actions required to effectively respond to a disaster, assign responsibilities and describe procedures for testing and maintaining the plan

6. STRATEGY DOCUMENT

ICT will define and maintain an auditable disaster recovery and restoration strategy that covers all ICT systems and will describe the activities of key functions within the Municipality in the event of a disaster. The strategy will cover all activities from the time the disaster is detected, to the stage when all services are restored to normal operational use.

All ICT systems will be classified according to the impact of non-availability to the business of the Municipality and prioritised accordingly for the purposes of business continuity and disaster recovery. This classification will determine the strategy and priority of recovery, including the maximum period of non-availability or the minimum service levels when running in deteriorated mode that the Municipality core business functions can tolerate. The systems currently maintained, as well as new systems developed or procured by ICT will be documented, maintained and tested on a regular basis according to the system classification.

Different strategies will be outlined and an ideal strategy befitting the nature of the Municipality business will be adopted, elaborated on and approved accordingly. In order to prioritise and understand the level of importance of each system, A Business Impact Analysis "BIA" should be performed or an alternative approach should be adopted so long the outcome will be able to distinguish different systems in terms of thier importance to the business of the Municipality.

7. PRINCIPLES

The following principles will apply:

- The entire disaster recovery plan will be rehearsed at least once a year for arbitrary disaster scenarios that will include the recovery of at least one (1) business critical system.
- This exercise will take the form of a simulated disaster and all relevant staff will participate in the exercise. The rehearsal will be audited, a report generated and the process updated before the test can be considered complete.
- The disaster recovery and restoration strategy will be reviewed on an annaul basis by ICT Management in consultation with the relevant stakeholders.
- Any review and changes will follow the change management and versioning control procedures as outlined on this document under the titled "Change Record".

8. RISK ASSESSMENT

The Municipality recognises that several risks may affect Information and Communication Technology (ICT) operations and, consequently, the effective delivery of Municipal services. These risks may arise from internal and external factors, including system failures, cyber threats, data loss, infrastructure limitations, and human error. The Municipality is committed to identifying, assessing, and managing these risks proactively to ensure the continuity, security, and reliability of ICT services that support its core functions and service delivery objectives.

Risk	Likelihood	Impact	Mitigation Measures
Cyberattack/Ransomware	High	High	Firewalls, antivirus software, Endpoint Dedection and Response(EDR), Data protection software, MFA, staff awareness training
Load Shedding/Power Failure	High	High	UPS devices, generators, surge protection
Server/systems Failure	Medium	High	Redundant systems and regular maintenance
Data Loss	Medium	High	Daily backups and offsite storage

Risk	Likelihood	Impact	Mitigation Measures
Fire in Server Room	Low	High	Smoke detectors and fire suppression systems
Flooding/Water Damage	Low	High	Raise floor and water dector.
Internet Failure	Medium	Medium	Secondary internet service provider
Theft/Vandalism	Medium	Medium	CCTV, access control, alarms
Human Error	High	Medium	User access controls and staff training
Malware/Virus Infection	High	High	Antivirus software and continuous monitoring

The Municipality shall conduct annual ICT risk assessments and update mitigation measures accordingly to address identified risks and ensure continued alignment with organisational objectives and compliance requirements.

9. BUSINESS IMPACT ANALYSIS (BIA)

A Business Impact Analysis (BIA) shall be conducted to identify critical information systems and services, determine acceptable downtime (Recovery Time Objectives), define data loss thresholds (Recovery Point Objectives), and establish recovery priorities.

The BIA shall further:

- Identify key business processes and their supporting ICT systems;
- Assess the potential impact of disruptions on municipal operations and service delivery;
- Categorise systems based on their criticality to business continuity;
- Define recovery timeframes and resource requirements for each critical system; and
- Be reviewed and updated regularly, or whenever significant changes occur within the ICT environment or Municipal operations.

System	Business Impact	Classes	Recovery Time Objective	Recovery Point Objective	Priority
Financial Systems	Revenue and payment interruptions	A	4 Hours	4 Hours	High
Email Services	Communication disruption	A	4 Hours	4Hours	High
Payroll System	Delayed salary payments	A	4 Hours	4 Hours	High
Active Directory	User access disruption	A	4 Hours	NA	High
Internet and Communication Services	Communication disruption and unavailability of systems	A	4 Hours	NA	High
Firewall services	Cyberattcack	A	4 Hours	NA	High
File Services	Document access interruption	A	24 Hours	24 Hours	Medium
Printing Services	Limited operational disruption		72 Hours	NA	Low

10. STAKEHOLDERS

The stakeholders include:

STAKEHOLDER	RESPONSIBILITY
Municipal Manager	Approves disaster declaration and strategic decisions
ICT Manager	Coordinates ICT recovery and restoration
Risk Manager	Coordinates disaster management processes
ICT Technicians	Restore systems, backups, and infrastructure

Internal Audit	Assessing compliance with this policy and related procedures
Departmental Heads	Ensure continuity of business operations
Third-Party Service Providers	Provide technical support and restoration services
Employees and Councillors	Follow emergency procedures and report incidents

11. BUSINESS CONTINUITY PLAN - STRATEGY

The Business Continuity Plan (BCP) is a set of operational procedures that informs the business how to perform their functions when systems, personnel and facilities are not available for use in a prolonged period of time. The Disaster Recovery Plan for all ICT systems shall support the Municipality BCP. This document is not the BCP but a component of the BCP.

It should be noted that ***BCP is not the responsibility of ICT***, unless it comprises a technical solution, in which case ICT aids or enables the business in continuing their operations or resuming business as soon as possible subsequent to a disaster.

Some business processes in the Municipality are critical to the value chain. These processes need to be continually operational in order to prevent revenue loss, fraud, etc. For these critical systems, the Municipality cannot afford any down-time where employees will not have an Office space to operate the day-to-day activities or work stations have been stolen or completely damaged. For the less critical systems, it may suffice to switch to an alternative process to get the work done while the systems are replaced or repaired subsequent to a disaster. These business areas require a specific Business Continuity Plan. This is where arrangements can be made with other local Municipalities within the Province for temporary Office space or workstations to be loaned. It is important that this Local Municipalities are identified and a standing arrangement made. This arrangements should be formalized and signed by both parties.

The BCP should be supported by a manual procedure or a technical solution. The technical solution forms part of the system design and shall be fully documented in the design document.

The design document shall specify in detail how to perform the backup and recovery using the solution. With regard to the manual procedures, the DRP shall contain the instructions for invoking this procedure and instructions on how to synchronize the data after the disaster.

12. DISASTER RECOVERY STRATEGY

All the Municipality systems and applications should be defined and classified according to three (3) different level of priority. Each class will require a different level of support. The priority is mostly determined by the impact of non-availability of the systems to the user and the duration of downtime that the business can afford in case of disaster.

12.1 SYSTEMS CLASS

Three (3) standards are therefore defined for disaster recovery to accommodate all systems and to provide a suitable balance between cost and recovery time. Generally, the following disaster recovery strategies are used for the system classes:

Class	Dual Host	Data Mirror	Backups
A	Yes	Yes	Yes
B	No	Yes	Yes
C	No	No	Yes

Class A – Critical Systems

These systems are essential for core municipal operations and require the highest level of protection and rapid recovery capability.

- Is the most critical systems.
- Shall make use of high redundancy.
- High availability solutions in order to reduce downtime.

Examples:

- Financial Management Systems
- Active Directory Services
- Email Services

Class B – Important Systems

These systems support key operational functions but are not as time sensitive as critical systems.

- Is less critical compared to Class A.
- Shall have two (2) sets of synchronized data in different locations.
- Secondary copy can be used when primary data destroyed.

Examples:

- Virtual Private Network (VPN) Services
- RADIUS Server

Class C – Standard Systems

These systems have lower business impact and can tolerate longer recovery times.

- Least critical systems.
- May not require any means of safeguard other than the ability recover from backups.

Examples:

- End-user Workstations
- Non-critical Departmental Systems

The following table reflects the disaster recovery requirements for each class:

System Class	Recovery Time Objective (RTO)	Recovery Point Objective (RPO)
Class A	48 Hours	15 Minutes
Class B	1 Week	24 Hours
Class C	4–6 Weeks	72 Hours

Municipal Information Systems Classification

Municipal information systems shall be classified according to their level of business criticality to ensure that appropriate backup frequencies, storage solutions, and recovery measures are defined, implemented, and maintained in alignment with operational requirements and risk tolerance.

12.1.1 Principles

- The recovery times listed in the above table refers to the period in which ALL systems of that particular class shall be recovered.
- The ICT Manager responsible for systems shall be responsible for scheduling and executing the reviews and tests.
- The verification period refers to the maximum interval between reviews. Reviews may occur more frequently than required to cater for any system changes. It is a requirement that all system changes be reflected in all relevant documentation, including the DRP Documents.
- DRP testing should be done once per annaum unless suggested otherwise by the Auditors especially on critical systems.
- Backup verification shall provide a high level of confidence in the ability to recover from backed-up data.

12.2 STRATEGIES

12.2.1 Dual Hosting

This solution is required for all ***Class A*** systems.

The solution comprises a reliable link between a primary and a secondary host that is used to feed all data changes (including application and configuration changes) on the primary server to the secondary server that is located in a different site. During a disaster at the primary site, the secondary site shall take over production until such time that the primary site is restored to its full operational condition. At this time data shall be synchronized again and the new primary site shall resume the operational functions again.

The secondary site shall be maintained at all times so as to be able to retain the capacity of taking over the production load at any time. The performance of the secondary host need not match the performance of the primary host, but shall at all times satisfy the Municipality requirements.

12.2.2 Data Mirror

This solution is required for all ***Class B*** systems.

The solution comprises a reliable link between a primary host and a data mirror at a secondary site that is used to feed all data changes (including application and configuration changes) on the primary server to the data mirror that is located at an off-site storage. The data mirror infrastructure on the secondary site shall be maintained at sufficient levels so as to ensure that a new host computer can be connected to the storage in the event of an emergency, after which the secondary site shall become the production site.

After the disaster, the secondary site will remain the production site until such time that the primary site is restored to full operational condition, at which time data shall be synchronized again and the new primary host shall take on the operational functions.

Relevant agreements with vendors shall exist to ensure that replacement equipment will be delivered in the event of an emergency and when required and should meet the Municipality SLA requirements.

12.2.3 Backup and Recovery

This solution is required for all ***Class A, B and C*** systems.

This solution comprises regular copies of data and program files to alternative removable storage media that can be stored offsite until such time that the media is required for rehearsal or restoration of services following a disaster.

All Class C system utilizing this strategy shall ensure that all relevant system, configuration information that can aid in the reconstruction of the system is collected and recorded daily and backed up in accordance with this strategy processes.

Although it is desirable to have the Dual Hosting and the Data Mirror as preferred options, their costs are quite exorbitant especially for the Local Municipality. The Backup and Recovery strategy as outlined below is practical and ideal for the operations of the Municipality. This could be an interim arrangement until the environment is virtualized.

13. THE MUNICIPALITY BACKUP AND RECOVERY STRATEGY

The Municipality shall adopt a comprehensive Backup and Recovery Strategy as the primary mechanism for disaster recovery and business continuity of ICT services.

This strategy is designed to ensure the protection, availability, and timely restoration of critical systems and data in the event of system failures, cyber incidents, or disasters.

The Backup and Recovery Strategy shall include the following elements:

- **Daily Full Backups**
  Full backups of critical systems and data shall be performed daily to ensure complete data capture and recoverability.
- **Frequent Incremental Backups**
  Incremental backups shall be conducted at regular intervals (every 15 minutes) to minimise data loss and support near real-time recovery.
- **Offsite Backup Storage**
  Backup copies shall be securely stored at offsite locations to safeguard against site-specific risks and disasters.
- **Backup Monitoring and Verification**
  Backup processes shall be continuously monitored, and backup data shall be regularly verified to ensure integrity, reliability, and completeness.
- **Periodic Recovery Testing**
  Regular restoration and recovery testing shall be conducted to validate the effectiveness of backup processes and ensure readiness for disaster recovery scenarios.

Future Enhancements

The Municipality may progressively enhance its disaster recovery capabilities by adopting advanced technologies, including:

- Virtualisation-based recovery solutions
- Cloud-based backup and disaster recovery services
- Automated failover and high-availability systems

Such enhancements shall be implemented in alignment with municipal strategic objectives, budget availability, and applicable security and compliance requirements.

14. RECOVERY PROCESS

A third party should be contracted for the safekeeping of the backup tapes. The process includes, the collection, storage, retrieval and delivering the backup tapes. Backup media collection, storage and retriavial are discussed in detail in the Moretele Local Municipality Backup policy.

15. COMMUNICATION AND ESCALATION PLAN

During a disaster or major incident, all communication shall be coordinated centrally through the ICT Department in collaboration with Municipal Management to ensure consistency, accuracy, and timely dissemination of information.

Communication channels may include:

- Email notifications
- Telephone communication
- SMS alerts
- Municipal website announcements
- Internal communication platforms

The escalation process shall follow the following order:

1. ICT System Administrator
   Tshegofatso Masia – 012 716 1308
   Tshegofatso.masia@moretele.gov.za
2. ICT Manager
   Joseph Mophuting – 012 716 1326
   Joseph.mophuting@moretele.gov.za
3. Risk Manager

Ronal Mahumani – 012 716 1319
Ronald.mahumani@moretele.gov.za

4. Municipal Manager – 012 716 1300
   Sipho.ngwenya@moretele.gov.za
5. Executive Management

16. DECLARING A DISASTER

It is the responsibility of the Municipal Manager or a delegated personnel within the Municipality to declare a situation a disaster when a disruption significantly affects municipal operations or ICT services.

The responsibility of the ICT division is to ensure that connectivity is restored and the respective users with the same credential are able to access the backend and perform their duties as normal as possible.

In case where a disaster occurred in the Server Room "Backend", new hardware will have to be procured or loaned which ever process is the shortest. Once installed, backup media will be recalled from the contracted third party. In this case ICT Management in liaison with the Risk Manager will declare a situation a Disaster.

A post moterm will be help subsequent to a disaster. A WAR ROOM will be identified where all the procedures will be discussed. All the affected stakeholders will be invited for a briefing and for their input. Once all the services are restored a post moterm will be held and lessons learned documented.

17. CYBERSECURITY INCIDENT RESPONSE

The Municipality recognises cybersecurity as a significant operational risk that may impact service delivery, data integrity, and the confidentiality of information. Accordingly, appropriate measures shall be implemented to effectively respond to and manage cybersecurity incidents.

The following procedures shall apply during cybersecurity incidents:

- Isolate affected systems immediately
- Notify ICT Management and relevant stakeholders
- Conduct incident investigations
- Restore systems from verified backups
- Change compromised credentials
- Report incidents according to applicable legislation and municipal procedures

Employees shall receive periodic cybersecurity awareness training to promote vigilance, reduce risk exposure, and ensure proper response to potential threats.

18 TESTING AND MAINTENANCE

The Municipality shall:

- Conduct annual disaster recovery testing;
- Verify backups regularly;
- Review the effectiveness of recovery procedures;
- Update the plan after major system changes;
- Maintain documentation of all tests and reviews.

Testing may include:

- Full disaster simulations;
- Backup restoration testing;
- Tabletop exercises;
- Cybersecurity response drills.

19. LESSONS LEARNED

The WAR ROOM and post moterm deliberations should be documented. The input from various parties should be assessed and be used as lessons learned from the disastreous event and be used as input to update the disaster recovery strategy and related documents.

Following any disaster or recovery exercise, a formal post-incident review shall be conducted to assess the effectiveness of the response and recovery processes.

The review shall:

- Identify weaknesses and gaps;
- Evaluate the effectiveness of recovery actions;
- Document lessons learned;
- Recommend improvements to policies, systems, and procedures.

All findings and recommendations shall be formally documented and incorporated into future updates of the Business Continuity and Disaster Recovery Plan (BCDRP) to ensure continuous improvement.

20. REVIEW

This plan shall be reviewed annually or whenever significant changes occur within the ICT environment, municipal operations, legislation, or risk profile. The ICT Steering Committee shall oversee the review process.

21. CONCLUSION

This Business Continuity and Disaster Recovery Plan establishes a structured framework for protecting Municipal ICT systems, maintaining service delivery, and ensuring operational resilience during disruptive events. The successful implementation of this plan requires cooperation among all stakeholders, continuous testing, and regular updates to ensure ongoing effectiveness.

--- END OF DOCUMENT ---