MORETELE LOCAL MUNICIPALITY

TSOGA O ITIRELE

ICT DATA BACKUP POLICY

Policy number	ICT-006-2026
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	Version	Change
Moretele Municipality	July 2016	1.1	

Reviewers

Name	Date	Version
ICT Unit	23 June 2026	1
ICT Steering committee	26 June 2026	1

TABLE OF CONTENTS

GLOSSARY ABBREVIATIONS

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 a period of 72 hours or longer
DRS	DISASTER RECOVERY SITE
DR	DISASTER RECOVERY
AD	Active Directory
Downtime	Defined as the periods when a system is unavailable
Storage Capacity	Amount of space (Tb, Gb, Mb) utilized

1. EXECUTIVE SUMMARY

This Backup Policy establishes a standardized and secure framework for the protection of Municipal information assets through structured processes for data backup, storage, retention, restoration, and recovery. Its primary objective is to ensure the availability, integrity, and reliability of critical information systems and data.

The Municipality recognizes that information is a vital organizational asset, and that any loss, corruption, unavailability, or destruction of data can significantly disrupt operations, compromise service delivery, affect financial management, and expose the Municipality to legal and regulatory risks. Accordingly, this policy provides clear guidance to mitigate such risks through effective data protection practices.

Aligned with the Municipality's Business Continuity and Disaster Recovery Plan, this policy supports resilience against operational failures, technical issues, environmental incidents, and cybersecurity threats. It ensures that appropriate measures are in place to safeguard information assets and enable timely recovery, thereby maintaining continuity of services and upholding governance and compliance obligations.

2. INTRODUCTION

Moretele Local Municipality relies extensively on information systems and digital technologies to support its core operations and the delivery of essential services to the community. As such, the availability, integrity, and security of municipal data are critical to ensuring effective service delivery, sound financial management, and good governance.

To maintain business continuity and minimize the impact of disruptions, all critical Municipal information and systems must be regularly backed up and adequately protected against potential data loss. Such losses may arise from various risks, including hardware and software failures, human error, cyberattacks such as ransomware, power outages, natural disasters, theft, vandalism, data corruption, and other unforeseen incidents.

This policy establishes the standards, controls, and requirements governing backup activities within the Municipality. It aims to ensure that reliable backup processes are implemented and maintained, enabling timely recovery of data and systems in the event of an incident, thereby safeguarding municipal operations and services.

3. LEGISLATIVE FRAMEWORK

This policy has been developed in alignment with the applicable legislative environment of the Republic of South Africa, as well as to incorporate internationally recognized ICT standards and best practices for information security and data protection.

The following legislation and regulatory frameworks, among others, were considered in the drafting of this policy:

- Constitution of the Republic of South Africa, Act No. 108 of 1996
- Copyright Act, Act No. 98 of 1978
- Electronic Communications and Transactions Act, Act No. 25 of 2002
- Minimum Information Security Standards (MISS), as approved by Cabinet in 1996
- Municipal Finance Management Act (MFMA), Act No. 56 of 2003
- Municipal Structures Act, Act No. 117 of 1998
- Municipal Systems Act, Act No. 32 of 2000
- National Archives and Records Service of South Africa Act, Act No. 43 of 1996
- National Archives Regulations and Guidance
- Promotion of Access to Information Act (PAIA), Act No. 2 of 2000
- Promotion of Administrative Justice Act (PAJA), Act No. 3 of 2000
- Protection of Personal Information Act (POPIA), Act No. 4 of 2013
- Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA), Act No. 70 of 2002
- National Treasury Regulations, Regulation 17 of 2005 (applicable to departments, trading entities, constitutional institutions, and public entities)

The following standards and frameworks were leveraged in the development of this policy:

- DPSA Information and Communication Technology Governance Policy Framework. Provides guidelines for the governance and management of ICT within the public sector, ensuring alignment with national priorities and public accountability.

- Control Objectives for Information and Related Technologies (COBIT 5)
  Offers a comprehensive framework for the governance and management of

enterprise ICT, focusing on aligning IT objectives with business goals, managing risks, and ensuring value delivery.

- ISO/IEC 27002:2013 – Information Technology – Security Techniques – Code of Practice for Information Security Controls.
  Provides internationally accepted best practices for implementing information security controls, including data protection, access control, and risk management.
- King Code of Governance Principles (King III, 2009)
  Establishes principles of good corporate governance, including the effective governance of information technology to support organizational performance, risk management, and compliance.

4. AIMS AND OBJECTIVES

The Municipality seeks to achieve the following objectives through the implementation of effective data backup and recovery practices:

- **Ensure Continuous Availability of Municipal Data**
  To guarantee that critical municipal information remains accessible and available to support uninterrupted operations and service delivery.

- **Reduce the Risk of Permanent Data Loss**
  To minimize the likelihood of irreversible data loss resulting from system failures, human error, or unforeseen incidents.
- **Protect Information Assets from Cyber Threats**
  To safeguard municipal data against cyber risks such as malware, ransomware, and unauthorized access through secure and reliable backup mechanisms.

- **Maintain Recoverable Copies of Critical Information**
  To ensure that accurate, complete, and up-to-date copies of essential data are consistently backed up and can be restored when required.

- **Support Operational Resilience**
  To strengthen the Municipality's ability to withstand and recover from disruptions, ensuring continuity of essential services.

- **Improve Recovery Capabilities**
  To enable timely and efficient restoration of systems and data in the event of failure or disaster, thereby reducing downtime and operational impact.
- **Facilitate Migration Toward Modern Backup Technologies**
  To support the transition to advanced, scalable, and secure backup solutions, including cloud-based technologies, in line with best practices.

5. SCOPE

This policy applies to all information systems, data assets, and backup processes within Moretele Local Municipality. It governs the management, control, and implementation of data backup and recovery practices across all municipal departments, systems, and infrastructure, including on-premises and cloud environments where applicable.

This policy repeals and replaces any previous ICT Backup and Disaster Recovery policies, providing a unified and standardized approach to data protection.

The ICT Data Backup and Recovery Policy are designed to guide and assist the Municipality in aligning with internationally recognized best practices related to data backup, recovery controls, and procedures. It establishes a framework of principles, standards, and minimum requirements to ensure consistency, reliability, and security in backup and recovery activities.

Recognizing that Municipalities vary in size, structure, and operational complexity, this policy adopts a flexible approach by defining clear principles and best practices that support effective planning, implementation, and ongoing management of backup and recovery controls. It aims to ensure that all critical Municipal data is adequately protected and can be restored efficiently in the event of data loss, system failure, or disaster.

This policy applies to all employees, officials, contractors, service providers, and consultants who interact with or manage municipal information systems and data. It is regarded as critical to the effective protection of municipal information assets and ICT systems.

6. ADMINISTRATIVE POLICY STATEMENT

The ICT Manager, together with designated ICT personnel, shall be responsible for the implementation, maintenance, and enforcement of this policy, as well as ensuring ongoing compliance with its provisions.

This policy shall be subject to formal review by the ICT Steering Committee on an annual basis to ensure its continued relevance, effectiveness, and alignment with Municipal objectives and technological developments.

Where necessary, any proposed amendments or updates to this policy shall be submitted for approval by the Municipal Council in accordance with established governance and approval processes.

7. BACKUP PRINCIPLES

The Municipality shall adhere to the following principles to ensure the effective protection, availability, and integrity of its data:

7.1 Regular Backups

Backups shall be performed on a scheduled and consistent basis to ensure that all critical data is up to date and recoverable.

7.2 Automation of Backup Processes

Backup processes shall be automated wherever feasible to reduce the risk of human error and to ensure reliability and consistency.

7.3 Access Control and Security

Backup data shall be safeguarded against unauthorized access through appropriate access controls, authentication mechanisms, and security protocols.

7.4 Data Encryption

All backup data shall be encrypted both in transit and at rest to protect sensitive municipal information from unauthorized disclosure, this includes personal information protected by Protection of Personal Information Act.

7.5 Onsite and Offsite Storage

Backup copies shall be maintained in both onsite and geographically separate offsite locations to ensure data availability in the event of a disaster or system failure.

7.6 Integrity Verification

Backup data integrity shall be verified regularly through validation checks to ensure that backups are complete, accurate, and usable.

7.7 Restoration Testing

Restoration procedures shall be tested periodically to confirm that data can be successfully recovered within acceptable timeframes.

7.8 Documentation and Auditability

All backup activities, including schedules, procedures, and test results, shall be properly documented and maintained to ensure auditability and compliance with applicable regulations.

8. BACKUP CLASSIFICATION

Municipal information systems shall be classified according to their level of business criticality to ensure that appropriate backup frequency, storage, and recovery measures are applied.

Class A – Critical Systems

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

Examples:

- Financial Management Systems
- Active Directory Services
- Email Services

Backup Requirements:

- Incremental backups shall be performed every 15 minutes.
- Full backups shall be performed daily.
- Backup copies shall be stored both on cloud and in a secure offsite location.
- Systems shall be prioritized for restoration in the event of failure or disaster.

Class B – Important Systems

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

Examples:

- Virtual Private Network (VPN) Services
- RADIUS Server

Backup Requirements:

- Backups shall be performed daily.
- Full backups shall be conducted on a weekly basis.
- Backup copies shall be stored offsite to ensure disaster recovery capability.

Class C – Standard Systems

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

Examples:

- End-user Workstations
- Non-critical Departmental Systems

Backup Requirements:

- Backups shall be performed on a weekly basis.

- Data shall be archived monthly in accordance with retention requirements.

9. BACKUP SCHEDULE AND RETENTION

BACKUP TYPE	FREQUENCY	RETENTION PERIOD
Incremental Backup	Every 15 Minutes	30 Days
Daily Backup	Daily	90 Days
Weekly Backup	Weekly	6 Months
Monthly Backup	Monthly	12 Months
Annual Archive	Annually	10 Years

Retention periods may be adjusted in accordance with legislative and operational requirements.

10. BACKUP SECURITY REQUIREMENTS

All Municipal backup systems shall be implemented and managed in accordance with stringent security standards to ensure the confidentiality, integrity, and availability of backup data.

Security Controls

The following minimum-security controls shall be enforced:

- Data Encryption
  Backup data shall be encrypted both at rest and in transit using approved cryptographic standards to prevent unauthorized disclosure.
- Multi-Factor Authentication (MFA)
  Multi-factor authentication shall be implemented for all backup systems and administrative access where technically feasible.

- Role-Based Access Control (RBAC)
  Access to backup systems and data shall be granted based on defined roles and responsibilities, ensuring the principle of least privilege is enforced.
- Audit Logging and Monitoring
  All backup-related activities, including access, modifications, and restoration processes, shall be logged and monitored to ensure accountability and traceability.
- Malware and Antivirus Protection
  Backup systems shall be protected with up-to-date antivirus and anti-malware solutions to detect and prevent malicious activities.
- Secure Transmission Protocols
  All data transfers related to backup operations shall utilize secure communication protocols (e.g., TLS/HTTPS, SFTP) to prevent interception or unauthorized access.

Access Restrictions

Access to backup systems, infrastructure, and stored backup data shall be strictly limited to authorized ICT personnel. Such access shall be:

- Approved by designated management authority
- Periodically reviewed and validated
- Immediately revoked upon role change or termination

Compliance and Enforcement

All backup security controls shall comply with applicable Municipal policies, cybersecurity standards, and relevant legal and regulatory requirements. Non-compliance shall be addressed through appropriate corrective actions and disciplinary measures where necessary.

12. BACKUP STORAGE REQUIREMENTS

The Municipality shall implement a structured and secure backup storage model to ensure data availability, resilience, and protection against loss or disaster.

Backup Storage Model

Backup copies shall be maintained in accordance with the following multi-tier storage approach:

Primary Backup Storage

Primary backup storage shall be located within the Municipal ICT infrastructure and shall provide rapid access to backup data for routine recovery operations. This storage shall be securely managed and regularly maintained to ensure availability and performance.

Secondary Backup Storage (Offsite)

Secondary backup copies shall be stored offsite through an approved and secure service provider. This arrangement shall ensure data availability in the event of a site-specific failure or disaster affecting Municipal facilities.

Protection of Backup Media

All backup media, whether physical or cloud-based, shall be adequately protected against potential risks, including:

- **Fire**

  Appropriate safeguards, such as fire-resistant storage and data centre protections, shall be implemented.
- **Flooding**

  Backup storage facilities shall incorporate measures to mitigate water damage and environmental exposure.
- **Theft**

  Physical and logical security controls shall be enforced to prevent unauthorized removal or access to backup media.

- **Unauthorized Access**
  Access controls, authentication mechanisms, and monitoring systems shall be implemented to restrict access to authorized personnel only.
- **Environmental Damage**
  Backup media shall be stored under suitable environmental conditions, including controlled temperature, humidity, and protection from dust or other hazards.

Compliance and Maintenance

All backup storage systems shall be:

- Regularly monitored and maintained to ensure reliability and performance
- Periodically reviewed to confirm compliance with municipal policies and applicable standards
- Quarterly tested to ensure data can be successfully restored when required.

13. BACKUP MONITORING AND VERIFICATION

The Municipality shall ensure that all backup processes are actively monitored and regularly verified to maintain data reliability, integrity, and recoverability.

Monitoring Responsibilities

The ICT Manager shall be responsible for the continuous monitoring and management of backup operations. This shall include:

- **Daily Monitoring of Backup Jobs**
  All scheduled backup jobs shall be monitored on a daily basis to confirm successful completion.

- **Immediate Investigation of Failures**
  Any backup failures, errors, or anomalies shall be promptly investigated and resolved to prevent data loss or extended downtime.

- **Maintenance of Backup Logs**
  Detailed backup logs shall be maintained, capturing information on backup status, errors, system performance, and corrective actions taken.
- **Reporting of Critical Issues**
  Critical backup failures or risks shall be escalated and reported to ICT Management without delay for appropriate action.

Backup Verification

To ensure the reliability and usability of backup data:

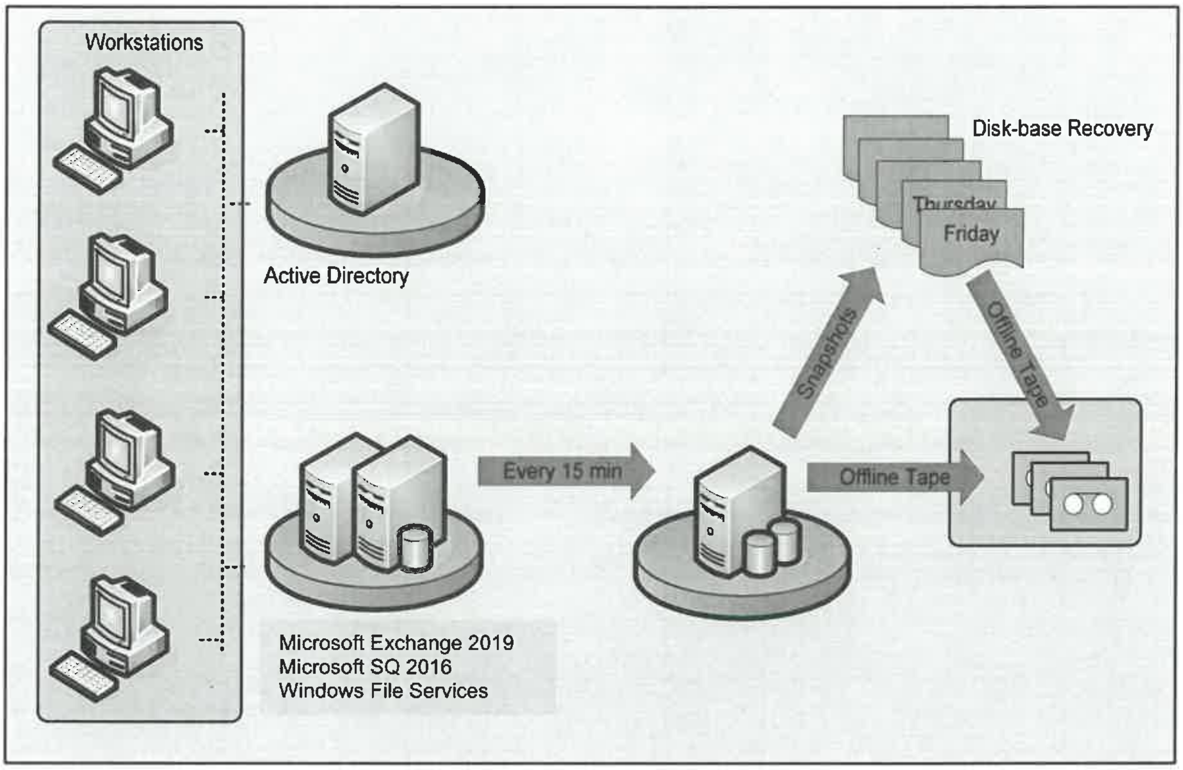
- **Integrity Verification**
  Backup data shall be regularly verified to ensure that it is complete, accurate, and free from corruption.
- **Verification Frequency**
  Formal backup verification processes shall be conducted at least on a monthly basis.
- **Validation Methods**
  Verification activities include checksum validation, test restores, and automated integrity checks.

Compliance and Assurance

Backup monitoring and verification activities shall:

- Be documented and retained for audit and compliance purposes
- Be subject to periodic internal review and audit
- Support continuous improvement of backup processes and controls

An example of a proposed backup process is depicted graphically below:



14. RESTORATION AND RECOVERY TESTING

The Municipality shall conduct regular restoration and recovery testing to ensure the effectiveness, reliability, and readiness of backup systems and processes.

Testing Requirements

To validate backup integrity and ensure data can be successfully restored when required, the following testing activities shall be performed:

- Monthly Sample File Restorations
  Sample file restorations shall be conducted on a monthly basis to verify that individual files can be accurately recovered from backup systems.

- Quarterly Full Restoration Tests
  Full system restoration tests shall be performed quarterly to confirm that complete systems and datasets can be restored within acceptable timeframes.
- Annual Disaster Recovery Simulations
  Comprehensive disaster recovery simulations shall be conducted annually to evaluate the Municipality's preparedness to recover critical systems and operations in the event of a major incident or disaster.

Documentation and Review

- All restoration and recovery testing activities shall be thoroughly documented, including scope, procedures, results, and any issues encountered.
- Test results shall be reviewed by ICT Management to assess performance, identify risks, and ensure compliance with recovery objectives.

Corrective Actions

- Any deficiencies, failures, or gaps identified during testing shall be addressed promptly.
- Corrective actions shall include remediation plans, system improvements, and process enhancements to strengthen overall backup and recovery capability.
- Follow-up testing shall be conducted where necessary to confirm that corrective measures have been successfully implemented.

Compliance and Continuous Improvement

Restoration and recovery testing shall support ongoing improvement by:

- Ensuring alignment with business continuity and disaster recovery requirements
- Providing assurance of backup reliability and system resilience
- Supporting audit and compliance obligations

15. RECOVERY PROCESS

A third party should be contracted for the safekeeping of the backup tapes. The process includes collection, storage, retrieval and delivering the backup tapes.

15.1 Collection

The tape canister will be stored in the ICT fire resistant strong room until the canister is filled with backup tapes, and ready for collection for offsite storage. The collection times are prescheduled and are part of the Service Level Agreement. When the canister is collected for offsite storage, a replacement canister is provided. The process is signed off by System Administrator and the contracted third party in a Service Level Agreement. Collections will be made every Friday afternoon or as per the agreement with the contracted third party.

15.2 Storage

On receipt of the canister, the contracted third party will store all the backup tapes at the address indicated in the agreement with the contracted third party. The contracted third-party premises are as follows:

Metrofile (PTY) LTD
Corner Eskia Mphahlele drive and Moot Street
Roseville
Pretoria
0001

The contracted third-party contact details are as follows:

Telephone N0: 012 379 6001
Call Center: 087 740 2701
Emergency contact N0: 083 661 2148
Fax No: 086 775 8343
Email address: SihleM@metrofile.co.za

15.3 Retrieval and Delivery

In the event of any backup media been recalled by the Municipality ICT, the following timelines will apply for the delivery of such media.

Next Day Retrieval	- within 24 hours
Request before 16H30 delivery by	- 16H00 the following day
Same Day Retrieval (Express)	- within 6 hours

16. ROLES AND RESPONSIBILITIES

To ensure effective implementation, management, and oversight of backup and recovery processes, the following roles and responsibilities are defined:

Municipal Manager

The Municipal Manager shall provide executive oversight and strategic direction by:

- Approving the municipal backup governance framework and related policies
- Supporting the allocation of adequate resources, including budget, personnel, and technology

ICT Manager

The ICT Manager shall be responsible for the overall management and governance of backup processes by:

- Overseeing the implementation and enforcement of this policy
- Ensuring compliance with established backup standards, procedures, and regulatory requirements
- Monitoring performance and providing regular reports to Municipal Management
- Approving backup schedules, tools, and technologies

System Administrators

System Administrators shall be responsible for the operational execution of backup activities, including:

- Performing and managing daily backup operations in accordance with approved schedules
- Monitoring backup jobs and resolving failures or anomalies
- Maintaining backup logs and ensuring proper documentation
- Conducting restoration and recovery testing as required

Third-Party Service Providers

Third-party service providers engaged in backup services shall:

- Deliver backup and support services in accordance with contractual agreements and service level requirements
- Maintain agreed service levels, including availability, security, and response times
- Comply with Municipal security, data protection, and regulatory requirements

Internal Audit

The Internal Audit function shall provide independent assurance by:

- Assessing compliance with this policy and related procedures
- Reviewing the effectiveness and adequacy of backup controls and processes
- Reporting findings and recommending improvements to strengthen backup governance

17. COMPLIANCE AND AUDIT

Compliance with this Backup and Recovery Policy is mandatory for all Municipal employees, contractors, and third-party service providers involved in backup-related activities.

Audit and Review Activities

To ensure adherence to this policy and the effectiveness of backup controls, the Municipality may conduct the following:

- Internal Audits
  Periodic internal audits shall be conducted to assess compliance with policy requirements and internal procedures.
- Backup Verification Reviews
  Regular reviews shall be conducted to validate the integrity, availability, and recoverability of backup data.
- Security Assessments
  Security assessments shall be undertaken to evaluate risks, identify vulnerabilities, and ensure appropriate safeguards are in place.

Non-Compliance

Failure to comply with this policy may result in:

- Disciplinary action in accordance with Municipal policies and procedures
- Implementation of corrective and remedial measures to address identified gaps
- Escalation to management for further action where significant risks are identified

18. POLICY VIOLATIONS

Any deliberate or negligent action that compromises the integrity, availability, or security of Municipal backup systems or data protection measures shall be treated as a violation of this policy.

All suspected or confirmed violations shall be:

- Promptly investigated in accordance with established Municipal procedures

- Documented and reported to the appropriate management authorities
- Addressed through corrective actions to mitigate risks and prevent recurrence

Disciplinary measures shall be applied in line with Municipal disciplinary procedures and may include appropriate sanctions depending on the severity and impact of the violation.

19. POLICY REVIEW

This Backup and Recovery Policy shall be reviewed annually to ensure its continued relevance, effectiveness, and alignment with municipal objectives, technological developments, and regulatory requirements.

20. CONCLUSION

This Backup and Recovery Policy establish the standards, controls, and governance framework necessary to protect Municipal information assets and ensure that critical data remains secure, available, and recoverable in the event of operational disruptions or disasters.

Furthermore, this policy supports the Municipality's long-term strategic direction of transitioning toward secure, scalable, and resilient cloud-based backup solutions, while maintaining a robust hybrid backup environment.

All stakeholders are required to adhere to this policy to ensure the continued integrity, reliability, and protection of municipal data assets.

END OF DOCUMENT