

ELIAS MOTSOLEDI LOCAL MUNICIPALITY



REVIEWED ICT BACKUP POLICY

Original Council Approval	
Date of Council Approval	26/06/2025
Resolution Number	C24/25-84
Effective Date	

MR
M.D

1.	Glossary of Abbreviation	3
2.	Purpose	4
3.	Legislative Framework	4
4.	Scope	4
5.	Policy Statement.....	5
6.	Objective.....	5
7.	Backup Types and Frequency	5
8.	Backup Storage Locations.....	5
9.	Backup Process Steps	6
10.	Backup Testing and Restoration	6
11.	Security Measures	6
12.	Responsibilities	6
13.	Roles and Responsibilities	6
14.	Reporting and Documentation.....	7
15.	Compliance and Monitoring.....	7
16.	Amendments	7

MR
M.D

1. Glossary of Abbreviation

Term	Meaning
MM	Municipal Manager
EMLM	Elias Motsoaledi Local Municipality.
ICT	Information and Communication Technology
DRP	Disaster Recovery Plan
DRS	Disaster Recovery Site
ISO	Information Systems Officer

112
M.D

2. Purpose

The purpose of this ICT Backup Policy is to ensure the integrity, availability, and recoverability of critical data and systems through systematic backup procedures. It aims to protect Elias Motsoaledi Local Municipality (EMLM)'s information against loss or corruption due to hardware failure, software issues, human error, or disasters.

3. Legislative Framework

- 3.1 The policy was developed with the legislative environment in mind, as well as to leverage internationally recognized ICT standards.
- 3.2 The following legislation, among others, was considered in the drafting of this policy:
 - i. Constitution of the Republic of South Africa Act, Act No. 108 of 1996.
 - ii. Copyright Act, Act No. 98 of 1978
 - iii. Electronic Communications and Transactions Act, Act No. 25 of 2002
 - iv. Minimum Information Security Standards, as approved by Cabinet in 1996
 - v. Municipal Finance Management Act, Act No. 56 of 2003
 - vi. Municipal Structures Act, Act No. 117 of 1998
 - vii. Municipal Systems Act, Act No. 32, of 2000
 - viii. National Archives and Record Service of South Africa Act, Act No. 43 of 1996
National Archives Regulations and Guidance
 - ix. Promotion of Access to Information Act, Act No. 2 of 2000
 - x. Promotion of Administrative Justice Act, Act No. 3 of 2000
 - xi. Protection of Personal Information Act, Act No. 4 of 2013
 - xii. Regulation of Interception of Communications Act, Act No. 70 of 2002
 - xiii. Treasury Regulations for departments, trading entities, constitutional institutions and public entities, Regulation 17 of 2005.
 - xiv. The following internationally recognized ICT standards were leveraged in the development of this policy:
 - xv. Control Objectives for Information Technology (COBIT) 5, 2019
 - xvi. ISO 27002:2013 Information technology - Security techniques - Code of practice for information security controls
 - xvii. King Code of Corporate Governance Principles, 2016

4. Scope

- 4.1 All employees, contractors, and third parties who handle or manage EMLM data.
- 4.2 All servers, databases, network configurations, user files, emails, and applications are maintained by the ICT UNIT.
- 4.3 All backup technologies and processes are used in the EMLM.

MR
M.D

- 4.4 Additionally, SharePoint is used as a centralized platform for storing documents required for audit purposes to ensure compliance and ease of retrieval in the event of disaster or loss.
- 4.5 The policy shall ensure that accountability is enforced, monitored and managed.

5. Policy Statement

The EMLM ICT Unit shall implement secure, reliable, and regular backup procedures for all critical systems and data to ensure business continuity and support recovery in the event of data loss.

6. Objective

The primary objective of this backup policy is to ensure the protection, integrity, and recoverability of critical data and systems in the event of data loss, corruption, system failure, or disaster.

7. Backup Types and Frequency

Data/Systems	Backup Type	Frequency	Retention Period
Email Systems	Full	Daily	3 Years
Databases (e.g. Finance)	Full & Transaction Logs	Daily	5 Years
Virtual Machines and System Images	Full	Weekly	1 Week
Workstations (Key Personnel)	Differential	Daily	3 Years

- 7.1 Backups are automatically scheduled by the backup software and monitored daily.
- 7.2 The service provider (Munsoft) backs up Premier VIP (Payroll System) and the financial system daily, and backup and restore certificates are submitted to the municipality as evidence of backup.
- 7.3 Microsoft Cloud services are utilised for backing up user data and M365 email accounts

8. Backup Storage Locations

- 8.1 Primary Backup Storage: On-site NAS/SAN servers located in the secure municipal ICT server room.
- 8.2 Encrypted off-site backups are maintained through a reputable **cloud service provider** that is fully **compliant with the Protection of Personal Information Act (POPIA)**. This ensures secure, remote data availability in the event of a primary storage failure or disaster.

7/12 M.D

9. Backup Process Steps

- 9.1 Initiation: The ICT System Administrator verifies that automated backup jobs are scheduled.
- 9.2 Execution: Backup software performs backup per schedule.
- 9.3 Verification: Logs and status reports are sent to the ICT System Administrator and reviewed by the Information Security Officer.
- 9.4 Encryption: All backups are encrypted before off-site transfer.
- 9.5 Storage: Backup copies are securely stored in **both on-site and off-site locations** to ensure redundancy and data availability. This dual-location strategy enhances disaster recovery capabilities and safeguards against data loss due to localized incidents.

10. Backup Testing and Restoration

- 10.1 Quarterly Test Restores will be performed on critical systems to ensure data is restorable and usable.
- 10.2 Restoration procedures will be documented and stored with DRP materials.
- 10.3 Any failed restore test must be escalated and corrected immediately.

11. Security Measures

- a. Access to backup systems is restricted to authorized ICT personnel.
- b. All backup data is encrypted using industry-standard encryption.
- c. Physical access to backup media is logged and monitored.

12. Responsibilities

Role	Responsibility
ICT Manager	Oversee policy compliance, review logs and reports
System Administrator	Execute and verify backup jobs, test restores
Information Security Officer	Oversee policy compliance, review logs and reports

13. Roles and Responsibilities

- 13.1 ICT Manager: Oversees policy implementation, conducts regular audits, and reports to management.
- 13.2 System Administrators: Perform backups, maintain logs, and ensure recovery procedures are followed.
- 13.3 All Staff: Must store data in designated directories to ensure it is included in backups.

MR M.D

14. Reporting and Documentation

41.1 EMLM ICT Unit maintain a Backup Log-register or System Log including:

- a. Backup date/time
- b. Type of backup
- c. Success/failure status
- d. Location of backup

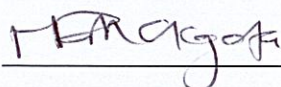
15. Compliance and Monitoring

- 15.1 Any failure to comply with this policy may lead to disciplinary action by the organization's ICT and HR policies.
- 15.2 The ICT Department will conduct regular audits to ensure adherence to this policy.

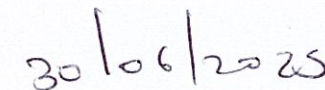
16. Amendments

This policy and procedure will be subject to amendments as and when the need arises.

17. SIGNATORIES



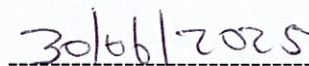
Ms. NR Makgata Pr Tech Eng
Municipal Manager



Date



The Mayor
Cllr. Tladi MD



Date