ELIAS MOTSOALEDI
LOCAL MUNICIPALITY

ICT ASSESTS MANAGEMENT POLICY

MUNICIPAL COUNCIL RESOLUTION NUMBER

M25/26-51

APROVED AT THE COUNCIL MEETING OF 28 MAY 2026
EFFECTIVE DATE 01/07/2026

MR

1. Policy Purpose

The purpose of this policy is to ensure that the Municipality maintains a **comprehensive, accurate, and up-to-date inventory** of all Information and Communication Technology (ICT) assets. This supports effective management, accountability, lifecycle tracking, and protection of municipal ICT resources, in compliance with applicable legislation and governance frameworks.

2. Overview

The municipality manages ICT assets to support effective and efficient frontline and corporate services. ICT assets include ICT hardware, software, systems and services that are handled at the local level. ICT asset management includes identification, acquisition, utilisation, disposal, recording and writing-off the municipality's ICT assets.

3. Policy Objective

a) To identify and document all ICT assets owned or managed by the Municipality.
b) To support ICT operational continuity, risk management, and compliance with MFMA, National Treasury guidelines, and internal audit requirements.
c) To enable integration between the ICT asset inventory and the official **Finance Asset Register** for accurate reporting and depreciation.
d) To strengthen security by ensuring only authorised devices are connected to the municipal network.

4. Legislative Framework

The policy was developed with the legislative environment in mind, as well as to leverage internationally recognised ICT standards. The following legislation, amongst others, was considered in the drafting of this policy:

Constitution of the Republic of South Africa Act, Act No. 108 of 1996
Copyright Act, Act No. 98 of 1978
Cybercrimes Act, Act No. 19 of 2020
Electronic Communications and Transactions Act, Act No. 25 of 2002
Electronic Communications Act, Act No. 36 of 2005
King IV Report on Corporate Governance (2016)
Minimum Information Security Standards, as approved by Cabinet in 1996
Municipal Finance Management Act, 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 Cybersecurity Policy Framework (NCPF), 2015
Promotion of Access to Information Act, Act No. 2 of 2000
Protection of Personal Information Act, Act No. 4 of 2013
Regulation of Interception of Communications Act, Act No. 70 of 2002
Treasury Regulations for departments, trading entities, constitutional institutions and public entities, Regulation 17 of 2005
State Information Technology Agency (SITA) Act, Act No. 88 of 1998
Standards for Records Management by Governmental Bodies (Issued under NARSSA)
ISO/IEC 27001 & 27002 (Information Security Management Standards)
ISO 55000 (Asset Management Standard)

5. Scope

This policy applies to:
All ICT assets owned or used by the Municipality, to every ICT equipment requester, or holder and all users of EMLM (contractors, service providers, interns, students, learners, councillors, and authorised 3rd party entities that need to use ICT equipment.
It covers all **hardware, software, network, and peripheral devices**, including:

a) Servers, desktops, laptops, mobile devices
b) Network infrastructure (switches, routers, firewalls, access points)
c) Printers, scanners, UPS units, projectors, displays
d) Software licenses, applications, and cloud services
e) External storage devices and backup media

f) Policy Statement

The Municipality shall:

a) Maintain a centralised ICT Asset Register containing detailed and verified records of all ICT assets.
b) Update the inventory whenever assets are procured, transferred, replaced, or disposed of.
c) Conduct quarterly updates of the ICT asset inventory.
d) Restrict network access to devices registered in the inventory.
e) Enforce accountability for all ICT assets through user assignment and custodian signatures.
f) To be allocated ICT equipment is not a right but a privilege that comes with the nature of specific responsibilities.

g) EMLM ICT will not provide any users with what they want; however, every effort will be made to provide for the ICT equipment needs of all users using only resources available for the provision of such ICT equipment.
h) ICT equipment needs will be prioritised over what users want. The purpose of this policy is to enable users to understand that their needs will be prioritised, informed and guided by the nature of their work.

6. Roles and Responsibilities

It is the responsibility of the ICT Unit to ensure the effective management, control, and protection of all ICT assets within Elias Motsoaledi Local Municipality.

The ICT Unit will perform the following functions:

1. Asset Identification and Inventory Management

a) Ensure every ICT asset is tagged, labelled, and uniquely identifiable using an approved asset tag before being deployed to users or departments.
b) Record the asset's lifecycle information, including:

i. Asset description and model
ii. Serial number
iii. Asset tag number
iv. Owner/user
v. Department
vi. Location
vii. Date of issuance and return

2. Asset Deployment and Movement Control

i. Authorise and document all ICT asset allocations, reassignments, or relocations in accordance with municipal asset management procedures.
ii. Ensure all asset movements are supported by approved asset movement forms and captured in the Inventory Register.
iii. Validate that users receiving ICT equipment sign the required handover documentation acknowledging responsibility.
iv. Ensure ICT equipment taken off-site is accompanied by an approved off-site equipment permit, except for laptops officially allocated to employees.

3. Asset Security and Protection

i. Ensure ICT assets are deployed with appropriate security configurations, including domain enrolment, endpoint protection, hardening standards, and monitoring controls.
ii. Prevent unauthorised manipulation, repair, upgrading, or tampering with ICT hardware by ensuring only authorised ICT personnel perform such activities.
iii. Implement technical and administrative controls to detect unauthorised or rogue devices connected to the municipal network.

4. **Asset Retirement and Disposal**

i. Manage the secure decommissioning, data wiping, and disposal of ICT assets in line with municipal asset disposal procedures and information security requirements.

ii. Ensure all retired or disposed assets are updated in the Inventory Register and documented through approved disposal forms.

5. **Reporting and Compliance**

i. Provide quarterly reports on the ICT Asset Inventory, including asset status, discrepancies, movements, losses, and disposals.

ii. Report any missing, damaged, or unaccounted-for ICT assets to the ICT Steering Committee.

User Responsibilities for ICT Assets

To ensure the proper safeguarding, accountability, and management of ICT assets within Elias Motsoaledi Local Municipality, all users must comply with the following requirements:

1. **Prohibited User Actions**

Users are strictly prohibited from performing the following actions:

a) Moving or relocating any ICT equipment (including PCs, monitors, printers, telephones, and network devices) without prior notification and approval from the ICT Division.

b) Placing food, drinks (including coffee/tea), water bottles, or any liquid containers on or near ICT equipment may cause damage.

c) Disconnecting a computer, printer, network cable, or any ICT device for reasons not authorised or known to the ICT Division.

d) Attempting to repair, troubleshoot, tamper with, or perform any form of upgrade on municipal ICT equipment, including the opening of hardware casings.

e) Swapping, exchanging, or reallocating ICT equipment with other officials without following formal Municipal asset movement procedures, including asset transfer forms and ICT verification.

2. **Required User Actions**

Users are **required** to perform the following actions to protect municipal ICT assets:

MR

a) Switch off their desktop computers and related equipment at the end of the business day, unless instructed otherwise by ICT (e.g., for maintenance or updates).
b) Ensure they are logged into the Elias Motsoaledi Local Municipality network domain when using municipal computers, to support security monitoring and asset tracking.
c) Obtain an approved off-site equipment permit before taking any ICT asset out of municipal premises. Exception: Laptops officially allocated to the user for work purposes.
d) Maintain a clean, tidy, and safe workspace around ICT equipment to avoid accidental damage and ensure proper ventilation.
e) Immediately report to the ICT Division any suspected hardware failure, unusual behaviour, physical damage, or potential security issue affecting ICT equipment.

6. Allocation of ICT Equipment

a) No procurement of computer-related equipment and/or software shall take place without a formal recommendation from the ICT Division. This ensures standardisation, compatibility, security, and compliance with municipal ICT architecture.
b) A laptop (notebook) shall only be allocated to an employee whose daily responsibilities require site work and who is allocated a car allowance. This is to reduce the risk of theft and ensure the secure mobility of municipal ICT assets.
c) It is the employee's responsibility to ensure the physical security of ICT equipment allocated to them. Employees must exercise caution, apply good judgment, and remain aware of potential risks that could result in damage or loss of municipal ICT assets.
d) An employee who does not receive a car allowance must demonstrate, beyond a reasonable doubt, that the laptop will not be exposed to high theft risk. A motivational memorandum from the employee's Director must accompany the request. Without such justification and approval, a laptop (notebook) will not be issued.
e) No employee may be allocated both a desktop computer and a laptop (notebook), nor may any employee be issued multiple laptops or desktops at the same time. This is to prevent unnecessary financial expenditure, asset mismanagement, and potential system vulnerabilities.
f) In cases where the nature of an employee's job necessitates the use of a notebook (laptop) or handheld computing device, this policy section serves as clarification of the municipality's approach to the issuance and use of such equipment.

g) All other employees whose functions require access to a computer will be allocated a desktop computer as the standard ICT workstation.
h) Printers will be allocated to officials strictly based on operational requirements and the nature of their duties, as determined by the ICT Division in consultation with the relevant departmental manager.
i) Colour printers will only be allocated to officials whose duties require frequent colour printing of official work documents. Requests must be motivated and approved by the relevant Senior Manager and verified by ICT to ensure necessity and cost-effectiveness.
j) All other officials will be required to use designated network shared printers. This ensures efficient resource utilisation, cost control, monitoring, and adherence to print management standards.

7. Custody, Security and Usage of ICT Equipment

1. All ICT equipment remains the property of Elias Motsoaledi Local Municipality. Such equipment does not belong to any individual user or employee.
2. When ICT equipment is allocated, it is assigned to the employee occupying a specific post for the purpose of performing official duties associated with that position. The assigned equipment will remain under the custody of the employee occupying the post until:
    a) the job content changes,
    b) the employee is transferred,
    c) the employee resigns, or
    d) the employee ceases to occupy the post.
3. During the period of use, the employee is fully responsible for the proper care, security, and operational condition of the ICT equipment issued to them.
4. Portable ICT devices such as laptops, external storage media, digital cameras, tablet PCs, and other mobile gadgets often hold sensitive municipal information. Users must therefore ensure that these devices and the data they contain are always properly protected.
5. Any loss, damage, or theft of ICT equipment must be reported immediately as follows:
    i. To the Assets Management and ICT unit within forty-eight (48) hours of discovery; and
    ii. To the South African Police Service (SAPS) within twenty-four (24) hours of the incident.
    iii. A copy of the police report or case number must be provided to the Assets Management and ICT unit for record-keeping and investigation.
6. Any loss or damage resulting from negligence on the part of the user shall be addressed in accordance with the procedures prescribed by the municipality.

7. If the provision of this policy does not cover the scope and special needs of other job functions, the Senior Manager of the concerned directorate will request in writing for such special needs of ICT equipment for consideration. ICT will assess the request and make a recommendation to either provide the ICT equipment/or provide an alternative solution.

8. Transfers, Change of Duties, Terminations, and Office Relocation

When an employee is transferred, changes duties, terminates employment, or relocates to a different office, all ICT equipment allocated to that employee shall be handed over to the Human Resources Office in accordance with the Municipality's Asset Management Policies. The Asset Management Unit shall, thereafter, formally notify the ICT Unit to initiate ICT-related processes and ensure completeness of records.

ICT equipment may only be reconfigured or reassigned after the Asset Management Unit has completed all required administrative and asset transfer activities. Once the equipment has been officially transferred, ICT officials shall:

i. Configure and prepare the equipment for further use.
ii. Verify that the ICT Equipment Transfer Form is correctly completed with all required information; and
iii. Update the EMLM ICT Equipment Asset Register to reflect accurate and current asset allocation details.

9. Maintenance and Replacement of ICT Equipment

1. The ICT Unit is responsible for ensuring that all ICT equipment is maintained in good working condition to support uninterrupted municipal operations. The ICT Unit shall carry out preventive and corrective maintenance activities.
2. Users must promptly report any faults, damages, or malfunctions of ICT equipment to the ICT Unit through the ICT Helpdesk channels. The ICT Unit shall record, assess, and prioritise such incidents to ensure timely resolution.
3. No employee is permitted to tamper with, repair, or modify ICT equipment without prior authorisation from the ICT Unit. Only authorised ICT personnel or accredited service providers are permitted to perform maintenance, repairs, or component replacements.
4. The ICT Unit shall maintain a maintenance and service log for all ICT equipment, capturing details of reported issues, repair actions and parts replaced.
5. EMLM ICT Unit may replace desktop and laptop computers after at least thirty-six (36) months of use in accordance with ICT best practices and normal wear and tear of ICT equipment.
6. Laptops and desktop computers that are found to be beyond economical repair, are thirty-six (36) months or older, or no longer meet operational requirements shall be

replaced in accordance with the applicable Treasury Regulations and the Elias Motsoaledi Local Municipality (EMLM) Asset Disposal Policy.

7. EMLM ICT will replace a printer after at least sixty (60) months of use in accordance with ICT best practice. Only those printers that are not operational before sixty (60) months will be replaced, provided the cause is not negligence.
8. All replaced or decommissioned ICT equipment must be recorded in the ICT Asset Register, and any data stored on such devices must be securely erased before reallocation, storage, or disposal.

Software Installation, Upgrades and Maintenance

1. No software may be installed on any municipal computer, server, or ICT device without prior verification by the ICT Division that the municipality holds a valid and current software licence for that application. All software installations must be approved, documented, and performed by authorised ICT personnel only.
2. The ICT Division and relevant management, against the anticipated operational benefit, security impact, licensing requirements, and technical compatibility, must carefully assess the installation of any additional software.
3. Management reserves the right to amend, waive, or provide exceptions to this provision in justified instances, provided such exceptions are documented and approved in line with ICT governance processes.
4. The ICT Division will only install, upgrade, or perform maintenance on software or hardware that is recorded on the Municipal Asset Register and has an official municipal asset barcode (sticker) attached.
5. Under no circumstances may ICT personnel install, configure, or maintain hardware or software on privately owned or personal computers, as this poses significant security, legal, and support risks.
6. Severely damaged equipment will be subject to assessment by the ICT Unit. Where the cost of repair exceeds the equipment's value, or where repair is not feasible, replacement will be recommended in line with the Municipality's asset management policies.
7. No user may attempt to repair, alter, or modify municipal ICT equipment. Only the ICT Unit or an approved service provider is authorised to perform any form of hardware or software maintenance.
8. The Municipality retains exclusive rights to determine, approve, and configure the hardware and software specifications for all ICT equipment purchased or funded by the Municipality. This includes, but is not limited to, the following:

i. Network accessories
ii. Printers
iii. Notebooks
iv. Desktops
v. Mobile devices

vi. Any other peripheral ICT equipment

8. Asset Inventory Procedure

Step 1: Asset Registration

a) Upon acquisition, each ICT asset shall be recorded in the **ICT Asset Register**.
b) Record all key details (e.g., asset type, serial number, location, assigned user, warranty, unique asset tag/barcode, and purchase information).

Step 2: Asset Movement and Transfers

a) When an asset is transferred between departments, the ICT Unit must update its location and custodian in the register.
b) Transfers require **authorisation** by the ICT Manager and **acknowledgement** from the receiving department.

Step 3: Disposal and Replacement

i. ICT assets that are obsolete or beyond repair shall be formally decommissioned (backed up, physical hard drive removed and removed from the asset inventory) and written off to the Assets unit for disposal.
ii. Data-bearing devices must undergo **secure data wiping or destruction** before disposal.

Step 5: Security and Access Control

i. Only assets listed in the register may connect to the municipal network.
ii. Unauthorised or unidentified devices must be isolated until verified.
iii. Network Access Control (NAC) tools may be used to enforce compliance.

8. Asset Information Fields

Each ICT asset record must include at least the following fields:

i. Asset ID / Barcode
ii. Asset Type and Description
iii. Manufacturer / Model / Serial Number
iv. Assigned User
v. Location (physical or virtual)
vi. Operating System / Software Version
vii. Date of Acquisition / Warranty Expiry
viii. Asset Status (Active / In Repair / Retired / Disposed)
ix. Remarks / Condition

9. Monitoring and Reporting

i. The Network Administrator and the Information Security Officer must review the asset inventory monthly to record asset movements, disposals, and any identified discrepancies.

10. Compliance and Review

i. Non-compliance with this policy may result in disciplinary action in line with the Municipal Code of Conduct and ICT Policies.

ii. The ICT Asset Inventory Policy shall be **reviewed annually** or when significant ICT or organisational changes occur.

Signatories

Ms. NR Mahlakwane Pr Tech Eng **19/06/2026**

Municipal Manager **Date**

The Mayor **19/06/2026**

Cllr. Tladi MD **Date**