

UMUZIWABANTU LOCAL MUNICIPALITY



LAPTOP USAGE POLICY 2025 / 2026

UMUZIWABANTU LOCAL MUNICIPALITY
LAPTOP USAGE POLICY

LSZ

TRC

TABLE OF CONTENTS

PAGE	
1. Preamble.....	Pg. 3
2. Objectives.....	Pg. 3
3. Application of this Policy.....	Pg. 3
4. Legal framework and requirements.....	Pg. 3
5. Policy Statement.....	Pg. 4
6. Roles and Responsibilities	Pg. 4
7. User Access Management.....	Pg. 5
8. Physical Security & Theft Prevention.....	Pg. 5
9. Loss of a Laptop.....	Pg. 6
10. Commencement.....	Pg. 6
11. Interpretation of this Policy.....	Pg. 6
12. Amendment and/or repeal of this Policy.....	Pg. 6
13. Permanent/Temporary waiver of this Policy.....	Pg. 6
14. Violation of or non-compliance with this Policy.....	Pg. 6

1. PREAMBLE

- 1.1 Umuziwabantu Local Municipality is, as an employer, responsible for and is committed to providing members of its staff with access to a laptop for the performance of their duties, for the execution of managerial instructions and for communication purposes, in the office.
- 1.2 A laptop is thus provided as a matter of course on requisition through the normal procurement process. However, a laptop is not a standard piece of office equipment; a policy is thus needed to address a need by some staff members to acquire a laptop instead of a desktop computer.
- 1.3 The purpose of this policy is thus to provide fairness in the procurement and allocation of a laptop for use by employees as a work facility and to provide guidelines for the use of laptops.
- 1.4 This policy must be observed by all Umuziwabantu Local Municipality staff members & Council members who are assigned with laptops.

2 OBJECTIVES

- 2.1 The objective of this policy is to outline the acceptable use of computer equipment within the Municipality. These rules are in place to protect the employee and the Municipality. Inappropriate use exposes the Municipality to risks including malware attacks, compromise of network systems and services, and legal issues.
- 2.2 Furthermore, this policy defines principles for appropriate utilisation of ICT facilities within the Municipality.

3. APPLICATION OF THIS POLICY

- 3.1 This policy applies to all computer users (employees & Councillors) of the Municipality, including Contractors and Consultants, who use ICT services and assets.
- 3.2 This policy applies to all equipment that is owned or leased by the Municipality.

4. LEGAL FRAMEWORK AND REQUIREMENTS

- 4.1 Constitution of the Republic of South Africa of 1996
- 4.2 The Electronic Communications and Transactions (ECT) Act 25 of 2002
- 4.3 National Strategic Intelligence Act 2 of 2000 applicable for South Africa
- 4.4 Regulation of Interception of Communications Act 70 of 2002
- 4.5 State Information Technology Act 88 of 1998
- 4.6 POPIA no4 of 2013

5. POLICY STATEMENT

- 5.1 ICT systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, web browsing, and FTP, are the property of the Municipality.
- 5.2 These systems are to be used for official business purposes in serving the interests of the Municipality in the course of normal operations.
- 5.3 Effective security is a team effort involving the participation and support of every employee and affiliate who deals with information and information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.
- 5.4 While ICT desires to provide a reasonable level of privacy, users should be aware that the data they create on the systems remains the property of the Municipality.
- 5.5 Employees are responsible for exercising good practice regarding the reasonableness use of ICT systems.
- 5.6 For security and network maintenance purposes, ICT may monitor equipment, systems and network traffic at any time.
- 5.7 Employees must be aware that all data transmitted or received on computer equipment, are not private and are subject to viewing, downloading, inspection, release, and archiving by the Municipality at all times.
- 5.8 The ICT Unit has the right to inspect any and all files stored in areas of the network, officials Laptop, desktops or storage media in order to assure compliance with ICT policies.
- 5.9 A formal procedure shall be followed to give users access rights to ICT facilities.

6. ROLES AND RESPONSIBILITIES

6.1 The ICT Unit shall:

- 6.1.1 Inform and educate users on the access to and use of ICT infrastructure
- 6.1.2 Identify and address the potential risks associated with the use of ICT in the workplace.
- 6.1.3 Not allow private laptops onto municipal network or copy any Municipality related data to private laptops.
- 6.1.4 Ensure the confidentiality of information generally contained on ICT infrastructure.

6.2 The user shall:

- 6.2.1 Not share logon usernames or disclose passwords to any other party.
- 6.2.2 Ensure the confidentiality of client information, employee information and confidential information generally contained on ICT equipment issued to the user.
- 6.2.3 Not intentionally bypass the security mechanisms of the equipment or any third-party security system or web site, without obtaining prior written approval from the Director: Corporate Services/Manager: ICT or designee.
- 6.2.4 Not use ICT resources for downloading, storage, forwarding or accessing data unrelated to official business (e.g. video clips, music files or graphics, SPAM) of the Municipality.
- 6.2.5 Not install or use any unauthorised configuration items (software or hardware) without approval from the ICT Unit.

7. USER ACCESS MANAGEMENT

7.1 Allocation of access rights:

- 7.1.1 There shall be a formal user registration procedure for granting access to requested information systems and networks.
- 7.1.2 Access rights to external consultants or contractors must be authorised by the by the Manager: ICT.
- 7.1.3 Access rights to privileged systems must be formally screened and authorised by the Manager: ICT.
- 7.1.4 Logon names shall be unique to each user and standardised.
- 7.1.5 ICT Unit shall review all user access rights periodically and renewed or revoked when appropriate. The results of this review must be communicated to the affected users where feasible.
- 7.1.6 ICT Unit shall also review all user accounts with administrative rights on the active directory, financial applications quarterly and the results of such review shall be kept as evidence.

- 7.2 Movement, Retirement, Suspension, and termination of employment/term expiry (in a case of a Councillor).

7.2.1 Once notified by the Human Resource Unit of a dismissal, suspension or resignation of an employee the ICT personnel will take the following action:

7.2.1.1 Dismissal – access rights will be disabled immediately

7.2.1.2 Suspension – access rights will be disabled immediately until reinstatement

7.2.1.3 Resignation – access rights will be disabled on last day of work.

7.2.1.4 Disabled accounts will be permanently deleted after three months.

7.3 In the event of an on-the-spot suspension/termination from service, the Human Resource Management Unit and/or Admin Support Unit in the case of a Councillor, should inform the ICT Unit to disable all access to ICT facilities.

8. PHYSICAL SECURITY & THEFT PREVENTION

8.1 In order to ensure physical security of laptops and data therein, all laptop users are required to undertake the following actions:

- 8.1.1 The physical security of the Municipality's provided laptops is the user's personal responsibility.
- 8.1.2 Each user is therefore required to take all reasonable precautions, be sensible and stay alert to the risks.
- 8.1.3 Keep your laptop in your possession and within sight whenever possible, just as if it were your wallet, handbag, or mobile phone.
- 8.1.4 Be extra careful in public places such as airports, ranks, railway stations or restaurants.
- 8.1.5 Never leave the laptop unattended when using it outside / inside the office.
- 8.1.6 Lock the laptop away out of sight when you are not using it, preferably in a strong cupboard, filing cabinet or safe. This applies at home, in the office or in a hotel.
- 8.1.7 Never leave a laptop visibly unattended in a vehicle/open and unlockable workstation/place or any unauthorised place.
- 8.1.8 Carry and store the laptop in a padded laptop computer bag or strong briefcase. to reduce the chance of accidental damage.

9. LOSS OF A LAPTOP

9.1 In all situations in which the laptop is stolen within the municipal offices, you must report this to Security immediately, then report to the SAPS and follow the procedure of reporting to the relevant office.

9.2 In all situations in which the laptop is stolen outside of the municipal offices you must report this to South African Police Service immediately and to follow the Procedure of reporting to the relevant office withing the municipality lodging an insurance claim.

9.3 If you have taken all of the precautions as indicated in this policy and the laptop is stolen or damaged, then the laptop will be replaced.

9.4 If your laptop is stolen or damaged in situations in which you have not taken all of the precautions identified in this policy you shall be personally responsible for the loss and will be responsible for replacement and/or repair

9.5 The penalty, thereof, shall be determined in terms of the applicable legislated/regulated disciplinary procedure/municipal sister policy/Standard Operating Procedure.

10. ALLOCATION OF TABLETS

- 10.1** Tablets issued to Councillors/ HODs are provided to support the execution of official duties.
- 10.2** Due to the expected useful life, depreciation, and technological obsolescence of these devices, tablets will not be required to be returned to the ICT Department at the conclusion of a Councillor's term of office / when an HOD leaves the office, provided that the device has reached or exceeded its prescribed replacement cycle or useful lifespan.
- 10.3** The ICT Department shall maintain an asset register of all tablets issued to Councillors and ensure that such devices are appropriately recorded and managed throughout their lifecycle.
- 10.4** Prior to the end of a Councillor's term / departure of an HOD , the ICT unit shall ensure that all municipal data, applications, and accounts are removed, disabled.
- 10.5** In the event where a tablet has not yet reached the end of its useful life, the Municipal Manager may determine whether the device should be returned to the Municipality, reallocated, or otherwise disposed of in accordance with the Municipality's Asset Management Policy and applicable legislation.

11. COMMENCEMENT

11.1 This policy will come into effect on the date of adoption by the Council.

12. INTERPRETATION OF THIS POLICY

12.1 All words contained in this policy shall have a direct grammatical meaning unless the definition or context indicates otherwise.

12.2 The dispute on interpretation of this policy shall be declared in writing by any party concerned.

12.3 The Office of the Municipal Manager shall give a final interpretation of this policy in case of written dispute.

12.4 If the party concerned is not satisfied with the interpretation; a dispute may then be pursued with the South Local Government Bargaining Council.

13. AMENDMENT AND/OR REPEAL OF THIS POLICY

13.1 This may be partly amended or wholly amended by the Council

13.2 This policy may be partly or wholly repealed by the Council

14. PERMANENT/TEMPORARY WAIVER OF THIS POLICY

14.1 This policy may be partly or wholly waived by the Municipal Council on temporary or permanent basis.

14.2 Notwithstanding clause No. 13.1 the Municipal Manager may under circumstances of emergency temporarily waive this policy subject to reporting of such waiver to Council.

15. VIOLATION OF OR NON-COMPLIANCE WITH THE POLICY

15.1 Violation of or non-compliance with this policy will give a just cause for disciplinary steps to be taken.

15.2 It will be the responsibility of all Council, Executive Committee, General Managers, Managers and Supervisors to enforce compliance with this policy.

Council Resolution number: **UMCR.....**

Approval Date: 26 June 2026



MR T.P CELE
MUNICIPAL MANAGER



CLLR L.S ZUNGU
MAYOR



CLLR P SHEBI
SPEAKER