UMUZIWABANT LOCAL MUNICIPALITY

ICT SECURITY CONTROLS POLICY

2026

Contents

CSZ TPC

TERMS

Term	Definition
Administrator rights	Access rights that allows an administrator to perform high level/administrative tasks on a device/application such as adding users, deleting log files, deleting users.
Biometric information	Personal information obtained through biometric measurements, such as fingerprints, retina etc.
Internal system processes	Processes that are performed by the system with no human intervention. Part of the internal working of the system or application.

ABBREVIATIONS

Abbreviation	Definition
BYOD	Bring Your Own Device
COBIT	Control Objectives for Information and Related Technology
ICT	Information and Communication Technology
IP	Internet Protocol
ISO	International Organization for Standardization
ODBC	Open Database Connectivity
PIN	Personal Identification Number
SSH	Secure Shell
UPS	Uninterrupted Power Supply

LSZ TPC

USB	Universal Serial Bus
WPA2	Wi-Fi Protected Access 2
VPN	Virtual Private Network

1. PURPOSE

The purpose of the ICT Security Controls Policy is to:

1.1. Establish and maintain employee and Councilor's accountability for the protection of information resources.
1.2. Promulgate the policy regarding the security of data and information technology resources.
1.3. Define the minimum-security standards for the protection of information resources.

2. APPLICATION OF THE POLICY

2.1. To all municipal employees and Councillors tthroughout the Municipality including and Consultants, who use ICT services and assets.
2.2. This policy applies to all equipment that is owned or leased by the Municipality.

3. LEGISLATIVE FRAMEWORK

3.1 The policy was drafted bearing in mind the legislative conditions, as well as to leverage internationally recognized ICT standards.
3.3 The following legislation, among others, were considered in the drafting of this policy:
3.4 Constitution of the Republic of South Africa Act, of 1996.
3.5 Copyright Act, Act No. 98 of 1978
3.6 Electronic Communications and Transactions Act, Act No. 25 of 2002
3.7 Minimum Information Security Standards, as approved by Cabinet in 1996
3.8 Municipal Finance Management Act, Act No. 56 of 2003
3.9 Municipal Structures Act, Act No. 117 of 1998
3.10 Municipal Systems Act, Act No. 32, of 2000
3.11 National Archives and Record Service of South Africa Act, Act No. 43 of 1996

CSZ TPC

3.12 National Archives Regulations and Guidance
3.13 Promotion of Access to Information Act, Act No. 2 of 2000
3.14 Protection of Personal Information Act, Act No. 4 of 2013
3.15 Regulation of Interception of Communications Act, Act No. 70 of 2002
3.16 Treasury Regulations for departments, trading entities, constitutional institutions and public entities, Regulation 17 of 2005.

The following internationally recognised ICT standards were leveraged in the development of this policy:

3.17 Western Cape Municipal Information and Communication Technology Governance
3.18 Policy Framework, 2014
3.19 Control Objectives for Information Technology (COBIT) 5, 2012
3.20 ISO 27001 & 27002:2013 Information technology — Security techniques — Code of practice for information security controls
3.21 King IV Code of Governance Principles.

4. OBJECTIVE OF THIS POLICY

The objective of this policy is to reduce the risk of harm that can be caused to the municipality's ICT systems, information and infrastructure. This policy also seeks to outline the acceptable use of ICT resources by Umuziwabantu LM employees, Councillors and 3rd party service providers, to ensure that the investment in modern technology is applied to the best advantage of the municipality.

This policy defines the collective controls to prevent Information Security related risk from hampering the achievement of the municipality's strategic goals and objectives.

5. AIM OF THE POLICY

The aim of this policy is to ensure that the Umuziwabantu LM conforms to a standard set of security controls for information security in such a way that it achieves a balance between ensuring legislative compliance, best practice controls, service efficiency and that risks associated to the management of Information Security are mitigated.

6. SCOPE OF THE POLICY

This ICT Security Controls Policy has been developed to guide and assist Umuziwabantu LM to be aligned with internationally recognized best practice ICT Security Controls. This policy recognizes that municipalities are diverse in nature and therefore adopts the approach of establishing and clarifying principles and practices to support and sustain the effective control of information security.

CSZ TPC

This policy is regarded as being critical to the security of ICT systems of the municipality.

The policy covers the following elements:

a) Security incident management
b) Physical security.
c) Application security.
d) Network security.
e) Database security.
f) Change control; and
g) Software authorization and licensing.

7. GENERAL CONTROL ENVIRONMENT

7.1. To ensure reliability of ICT services and to comply with legislation, all municipal systems and infrastructure must be protected with physical and logical security measures to prevent unauthorised access to municipal data.

7.2. Physical and logical security is a layered approach that extends to user access, application security, physical security, database security, operating system security and network security.

8. PHYSICAL SECURITY

8.1. The ICT Manager must take reasonable steps to protect all ICT hardware from natural and man-made disasters, to avoid loss and ensure reliable ICT service delivery.

8.2. ICT hardware under control of the ICT function must be hosted in server rooms or lockable cabinets.

8.3. Server rooms must be of solid construction and locked at all times.

8.4. The ICT department must retain an access control register for the server room. Access must be reviewed quarterly by the ICT Manager.

8.5. All server rooms must be equipped with air-conditioning, UPS and fire detection and suppression.

8.6. A maintenance schedule for the server room must be created and maintained for all ICT hardware under the control of the ICT department. Maintenance activities must be recorded in a maintenance register.

8.7. Server rooms must be kept clean to avoid damage to hardware and reduce the risk of fire.

8.8. Cables must be neat and protected from damage and interference.

8.9. No ICT equipment may be removed from the server room or offices without prior authorisation from the ICT Manager.

8.10. Municipal officials will receive educational awareness and training initiatives to educate users on the acceptable use of ICT hardware and related resources.

LSZ EPC

8.11. All data and software on hardware must be erased prior to disposal or re-use.
8.12. Any hardware that carries data that can be carried off-site (e.g. laptop computers, removable hard disks, flash drives etc.) must be protected with encryption.
8.13. ICT hardware and software must be standardised as far as possible to promote fast, reliable and cost-effective ICT service delivery to the municipality.
8.14. The off-site location, used to store backup data media, must be protected with the following physical security measures: a) Building of solid construction.
8.14.1. Physical access control.
8.14.2. Fire detection and suppression; and
8.14.3. Environmental conditions adhere to vendor recommendations for storage of media.

9. DATABASE SECURITY

9.1. The ICT Manager must limit full access to databases (e.g. system admin server role, database owner role, sa built-in login etc.) to ICT staff who need this access. Officials who use applications may not have these rights to the application's databases.
9.2. The ICT Manager must ensure that Officials who access databases directly (e.g. through ODBC) only have read access.
9.3. The ICT Steering Committee must approve all instances where Officials have edit or execute access to databases.
9.4. The ICT Manager must review database rights and permissions on a quarterly basis. Excessive rights and permissions must be removed.

10. NETWORK SECURITY

10.1. The ICT Manager must document the network structure and configuration including IP addresses, location, make and model of all hubs, switches, routers and firewalls.
10.2. The ICT Manager must implement a firewall between the municipal network and other networks.
10.3. The ICT Manager must limit administrator access to the firewall and user accounts must have strong passwords of at least 8 characters with a combination of alphanumeric characters and symbols.
10.4. Remote firewall administration is only allowed using SSHv2 from the internal network.
10.5. The ICT Manager must check and install firewall upgrades and patches on a monthly basis. An obsolete firewall (one that is not supported by the vendor any longer and / or has known security vulnerabilities) must be replaced.
10.6. The ICT Manager must document the firewall rulesets and configuration settings. The rulesets and configuration settings must be reviewed quarterly to ensure that

CSZ TPC

it remains current (i.e. remove unused services) and that services that expose the municipality to security risk are reviewed continuously.

10.7. The ICT Manager must configure the firewall to block all incoming ports, unless the service is required to connect to a server on the internal network (e.g. port 80 and port 443 for web servers). When an incoming port is allowed, the service may only connect to the specific servers on the internal network. Internal IP addresses may not be visible outside of the internal network.

10.8. The ICT Steering Committee must approve all open incoming ports. The ICT Steering Committee must only approve requests that are absolutely necessary and with consideration of the associated security risks.

10.9. The system administrators must set the firewall to block intrusion attempts and to alert the ICT Manager when additional action needs to be taken. The ICT Manager must raise an incident and deal with the root causes of the event.

10.10. The ICT Manager must place infrastructure, user devices (e.g. personal computers) and servers facing externally on separate network domains.

10.11. The ICT department must scan the entire network with security software monthly to detect security vulnerabilities. The scans must be performed on the Internet, as well as from the internal network.

10.12. Officials and the ICT Manager must remove all modems from the internal network to avoid intruders bypassing the firewall.

10.13. System administrators must install personal firewalls on laptops and personal computers. Officials may not disable these firewalls. Officials must choose to deny a specific address when prompted by the personal firewall, unless approved by ICT.

10.14. The ICT department must ensure that all inactive network points are disabled.

10.15. All organizational devices accessing organizational systems or data must have approved antivirus and endpoint protection software installed and active.

10.15.1 The ICT Department shall ensure that:

10.15.1.1 Antivirus software is regularly updated.

10.15.1.2 Real-time protection and periodic system scans are enabled.

10.15.1.3 Malware threats are monitored and addressed promptly.

10.15.1.4 Users do not disable or remove antivirus protection without authorization.

10.15.1.5 Devices that do not comply with this control may be denied access to the organizational network.

11. ACCESS MANAGEMENT

11.1. Every account must have an owner. (Someone who is responsible for account usage, password changes etc.)

11.2. A record should be maintained showing each user's profile. All modifications to user accounts should be recorded.

CSL TPC

11.3. A new user may be registered on the system by submitting a written application with a list of services, programs and or data to which access is required. This application has to be recommended by the applicant's supervisor and approved by the Manager responsible for IT. After approval has been granted, the IT officer/s will register the new user.
11.4. Passwords are required to gain access to all the domain controllers and file servers. No one will be allowed to access any system without a valid password.
11.5. Users will be forced to change passwords on the domains and servers monthly.
11.6. Passwords will be encrypted by the system.
11.7. The minimum password complexity length is set to eight characters and must contain alpha as well as numerical characters.
11.8. Passwords must not be easily guessed or compromised. (E.g. names, month etc.)
11.9. Users will be allowed three login attempts before the account will be locked. Previously used passwords are not allowed.
11.10. Critical systems (HR and Financial) may require further authentication by means of user log-on (ID and password) to the applicable system.
11.11. The specific system administrator (authorized user) will control website uploads and any access thereof.
11.12. Network restrictions are enabled for HR and finance systems, and only users connected through a VPN are permitted to access these systems from external networks.
11.13. Exceptions to the above (9.12) VPN rights will only be granted with the approval or authorization of the Manager: ICT.

12. BACKUP

12.1. It is the responsibility of the specific user to ensure that his/her data is backed up regularly using (One Drive).
12.2. Critical applications and or data files should be backed up and safely stored.
12.3. The responsible IT persons must ensure that the approved corporate backup procedures are followed.

13. E-MAIL AND INTERNET

13.1. The ICT Manager must inform all users of the safe and responsible use of email and Internet services.
13.2. E-mail and Internet should only be used for official use. E-mail and Internet may not be used for any illegal or offensive activities.
13.3. All users may not use Internet cloud services (e.g. Google drive, Gmail, Dropbox etc.) for official purposes unless approved by the ICT Steering Committee.
13.4. The Umuziwabantu retains the right to access and monitor any information sent via the e-mail system.
13.5. No private information/images/data that may be offensive to any person, group or organization may be sent to any destination via the official e-mail system.

LSZ TPC

13.6. Internet access is provided for research and communication purposes only.
13.7. No unofficial or non-work-related material may be downloaded through municipal systems and networks.
13.8. Due to bandwidth limitations, live streaming on social media platforms over the Internet is not permitted unless authorised by the ICT Manager.

14. WIRELESS NETWORKS

14.1. System administrators must configure all wireless networks to the following standard:

a) WPA2 security protocol or better.
b) Password strength of at least 8 characters with a combination of alpha-numeric characters and symbols.
c) The latest firmware must be installed; and
d) Default system usernames and passwords must be removed.

14.2. Officials may not establish wireless networks attached to the internal network without the consent of the ICT Manager. All wireless networks must adhere to the secure configuration standard.

15. TRANSFER OF INFORMATION

15.1. The ICT Manager must ensure that classified information may only be transmitted over external networks using encryption.
15.2. Officials may not use personal storage devices (e.g. USB memory sticks or portable hard drives) to store municipal data. When required for official purposes, and the data is of a confidential nature, these devices must be encrypted by the ICT Manager.

16. MONITORING

16.1. The Municipal Manager authorizes the monitoring of municipal systems by the ICT Manager.
16.2. Municipal officials must be made aware that the network is being monitored to ensure network security, to track the performance of the network and systems, and to protect the network from viruses.
16.3. Internet and other network services may be monitored.

17. SECURITY INCIDENT MANAGEMENT

17.1. All municipal users must report actual or suspected security breaches or security weaknesses to the ICT Manager or the delegated authority. (e.g phishing, bogus emails etc)
17.2. The ICT Manager must record all information regarding security incidents.

17.3. The ICT Manager must review all the information on security incidents on a quarterly basis to ensure that the root causes of the problems are addressed.

17.4. Investigations into security incidents may only be carried out by the ICT Manager or a nominated person.

18. CHANGE CONTROL

18.1. All changes to municipal applications and infrastructure must be managed in a controlled manner to ensure fast and reliable ICT service delivery to the municipality, without impacting the stability and integrity of the changed environment.

18.2. Corrections, enhancements and new capabilities for applications and infrastructure will follow a structured change control process.

18.3. An emergency change must follow a structured change control process, but with the understanding that documentation must be completed afterwards.

18.4. Emergency changes are only reserved for fixing errors in the production environment that cannot wait for more than 48 hours.

18.5. Recurring change requests from users (e.g. user access requests, a password reset, an installation, move or change of hardware and software etc.) must follow the helpdesk processes designed to deliver ICT services in the most effective way.

18.6. Recurring operational tasks are excluded from the structured change control process.

18.7. The ICT Manager must establish the formal change control process.

18.8. The following additional rules with respect to change control must be adhered to. In some cases this may not be cost-effective or technically possible, in which case it is the duty of the ICT Steering Committee to review and approve alternative controls:

18.9. The same person who performs the change may not implement the change.

18.10. Systems must have a development environment where testing is conducted to avoid testing in the production environment.

18.11. If a vendor performs the change, the municipality must also test the change.

18.12. The data inside a database may not be edited, except through an approved application front-end. This excludes internal system processes or interfaces, or work required to convert data during system implementation.

18.13. Commercial software must be selected after considering information security requirements.

18.14. The affected user's willingness to change must always be considered when documenting all that can go wrong with the change.

18.15. Any system published to the Internet or on a mobile platform must be reviewed by security specialists before being deployed.

18.16. The ICT Manager must record all change requests across the municipality in a central tool, file server or spreadsheet. This implies that changes performed by ICT and those changes requested by the business from vendors, without ICT involvement, must be recorded together.

LSL TPC

19. SOFTWARE AUTHORISATION AND LICENSING

19.1. The ICT Manager must retain a record of all licenses owned by the municipality.

19.2. The ICT Manager must scan all ICT resources on an annual basis to verify that only authorised software is installed.

19.3. The ICT Steering Committee must approve all software being used in the municipality. An approved software list must be maintained by the ICT Manager and approved by the ICT Steering Committee.

19.4. The ICT Steering Committee may only authorise software from known, reputable sources to reduce the likelihood of introducing errors or security risks into the environment.

19.5. Officials may not install or change the software on their computers.

20. SECURITY AWARENESS AND TRAINING

20.1 The municipality shall provide regular ICT security awareness and training to all employees, Council & relevant stakeholders to promote the safe and responsible use of information systems and organizational data.

20.2 Training shall include awareness on:

20.2.1 Password and access security

20.2.2 Phishing and cyber threats

20.2.3 Safe internet and email usage

20.2.4 Data protection and confidentiality

20.2.5 Reporting of ICT security incidents

20.3 The ICT Department shall coordinate periodic training and awareness programs, and all staff are required to participate in such initiatives.

21. BREACH OF POLICY

21.1. Any User found guilty of failure to comply with the rules and standards set out herein will be regarded as misconduct and/or breach of this policy and appropriate disciplinary action or punitive recourse shall be instituted against such user who contravenes this policy, read together with other municipal sister policies/applicable laws.

21.2. All misconduct and/or breach of contract will be assessed by the municipality and evaluated on its level of severity

21.3. .1 Actions shall include, but not limited to:

a) Revocation of access to municipal systems and ICT services;

b) Disciplinary action in accordance with the municipal policy; or

c) Civil or criminal penalties e.g. violations of the Copyright Act, 1978 (Act No. 98 of 1978).

d) Punitive recourse against a service provider in terms of the contract.

LSL TPC

22. COMMENCEMENT

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

22.2. This policy may be reviewed with and/or upon recommendation of the ICT Steering Committee, subject to any changes approved by Council.

23. INTERPRETATION OF THIS POLICY

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

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

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

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

24. PERMANENT/TEMPORARY WAIVER OF THIS POLICY

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

24.2. Notwithstanding clause No. 20.1 the Municipal Manager may under circumstances of emergency temporarily waive this policy subject to reporting of such waiver to Council.

25. VIOLATION OF OR NON-COMPLIANCE WITH THE POLICY

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

25.2. It will be the responsibility of the Manger: ICT/ Designee, all Council members, Executive Committee, HODs, Managers and Supervisors to enforce compliance with this policy.

Council Resolution number: UMCR.../../../.../2025-2026

Approval Date:29 June 2026

MR T.P CELE	**CLLR D. S.L ZUNGU**	**CLLR PSHEBI**
MUNICIPAL MANAGER	**MAYOR**	**SPEAKER**