TSWELOPELE
LOCAL MUNICIPALITY
A MUNICIPALITY IN PROGRESS

ICT USER ACCESS MANAGEMENT POLICY

Table of Contents

1. Glossary of Abbreviations

Abbreviation	Definition
ICT	Information and Communication Technology
ISO	International Organisation for Standardisation
RAS	Remote Access Service
COBIT	Control Objectives for Information and Related Technology
PIN	Personal Identification Number
VPN	Virtual Private Network
ID	Identifier

2. Terms and definitions

Account holder / user	Any person granted an ICT user account with the Department
Authentication	Establishing the validity of a claimed entity / verification of the identity of an individual or application
Availability	Being accessible and useable upon demand by an authorised entity
Confidentiality	The principle that information is not made available or disclosed to unauthorised individuals, entities or processes
Identification and authentication	Functions to establish and verify the validity of the claimed identity of a user
Information and communication systems	Applications and systems to support the business, utilising information technology as an enabler or tool
Information technology	Any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of vocal, pictorial, textual and numerical data or information

Monitoring:	Performance measurement to ensure the confidentiality, availability and integrity of operational systems and information
Password	Confidential authentication information composed of a string of characters
ISO	Information Security Officer

3. INTRODUCTION

Information security is becoming increasingly important to the Municipality, driven in part by changes in the regulatory environment and advances in technology.

Information security ensures that ICT systems, data and infrastructure are protected from risks such as unauthorised access, manipulation, destruction or loss of data, as well as unauthorised disclosure or incorrect processing of data.

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, 1996 [Act 108 of 1996]
- Electronic Communications and Transactions Act, 2002 [Act 25 of 2002]
- Minimum Information Security Standards, as approved by Cabinet in 1996
- Municipal Finance Management Act, 2003 [Act 56 of 2003]
- Municipal Structures Act, 1998 [Act 117 of 1998]
- Municipal Systems Act, 2000 [Act 32 of 2000]
- National Archives and Record Service of South Africa Act, 1996 [Act 43 of 1996
- Promotion of Access to Information Act, 2000 [Act 2 of 2000]
- Protection of Personal Information Act, 2013 [Act 4 of 2013]
- Regulation of Interception of Communications Act, 2002 [Act 70 of 2002]
- 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:

- Control Objectives for Information Technology (COBIT) 5, 2012
- ISO 27002 : 2013 Information technology - Security techniques - Code of practice for information security controls
- King Code of Governance Principles, 2009.

5. AIM OF THE POLICY

The aim of this policy is to ensure that the municipality conforms to standard user access management controls 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 user access are mitigated. This policy supports the Municipality's Corporate Governance of ICT Policy.

6. SCOPE

The ICT User Access Management Policy has been developed to guide and assist
municipality to be aligned with internationally recognised best practice User Access
Management controls and procedures. This policy further recognises that municipalities are diverse and therefore adopts the approach of establishing principles
and practices to support and sustain the effective control of user access management
in the municipality.

The policy applies to everyone in the municipality, including its service providers / vendors. This policy is regarded as being crucial to the operation and security of ICT systems of the Municipality. The policy covers the following elements of user access management:

- New user registration
- Terminated user removal
- User permission / role change request
- User access rights assignment for networks, operating systems, databases and applications
- Reviewing user access permissions
- User and administrator activity monitoring.

Aspects relating to ICT security and operating system security controls are contained in the ICT Security Controls and ICT Operating System Security Controls policies.

7. BREACH OF POLICY

Any failure to comply with the rules and standards set out herein will be regarded as misconduct and / or breach of contract. All misconduct and / or breach of contract will be assessed by the municipality and evaluated on its level of severity.

Appropriate disciplinary action or punitive recourse will be instituted against any user who contravenes this policy. Actions include, but are not limited to:

- Revocation of access to municipal systems and ICT services
- Disciplinary action in accordance with the municipal policy
- Civil or criminal penalties e.g. violations of the Copyright Act, 1978 [Act 98 of 1978
- Punitive recourse against the service provider / vendor as stated in the service provider / vendor's SLA with the Municipality.

8. ADMINISTRATION OF POLICY

The ICT Manager or delegated authority within the municipality is responsible for maintaining this policy. The policy must be reviewed by the ICT Steering Committee on an annual basis and recommended changes must be approved by Council.

9. DELEGATION OF RESPONSIBILITY

In accordance with the ICT Governance Policy, it is the responsibility of the Municipal
Manager to determine the delegation of authority, personnel responsibilities and accountability to Management with regards to the Corporate Governance of ICT.

10. NEW USER REGISTRATION

10.1 A formalised user registration process must be implemented and followed in order to assign access rights.

10.2 All user access requests must be formally documented, along with the access requirements, and approved by authorised personnel by making use of the user access request form. The template for this type of request can be found attached to this policy as Annexure A.

10.3 User access requests must be obtained from HR on registration of a new employee. The form must be sent to the manager for access requirements to be requested. Once the requirements have been requested and signed off by the departmental director / manager, the form must be sent to the ICT department for approval following which the activation of the employee based on the specified requirements will be completed. The form must then be sent back to HR for record keeping purposes. Records of user access granted must be stored for a minimum of 10 years.

10.4 User access must only be granted once approval has been obtained

11. TERMINATED USER REMOVAL

11.1 A formalised user termination process must be implemented and followed in order to revoke access rights.

11.2 All user termination requests must be formally documented and approved by duly authorised personnel. Access must be disabled immediately, with accounts being removed after 6 months once authorisation has been obtained by line manager.

11.3 Terminated user requests must be obtained from HR on the termination of an employee. The template for this type of request can be found attached to this policy in Annexure B. The form must be sent to the line manager for

access revocation to be signed off. Once access revocation has been signed off, the form must be sent to the ICT department for approval and deactivation of employee based on specified requirements. The form must then be sent back to HR for record keeping purposes. Records of use access removal must be stored for a minimum of 10 years.

12. USER PERMISSION / ROLE CHANGE REQUEST

12.1 A formalised user access management process must be implemented and followed in order to adjust user access rights.

12.2 All user access change requests must be formally documented, along with their access requirements, and approved by duly authorised personnel.

12.3 Access must only be granted once approval has been obtained by the respective line manager.

12.4 User access change requests must be obtained from HR on change of an employee's role or permissions. The template for this type of request can be found attached to this policy in Annexure C. The form must be sent to the service provider/line manager for access requirements to be signed off.

Once the access requirements have been signed off, the form must then be sent to the ICT department for approval and adjustment of employee's access rights based on specified requirements. The form must then be sent back to HR for record keeping purposes. Records of user access granted and removed must be stored for a minimum of 10 years.

12.5 User access rights that are no longer required must be removed immediately.

13. GENERAL USER ACCESS RIGHTS ASSIGNMENT

13.1 Access rights include, but are not limited to:

(a) General office applications [E-mail, Microsoft Office, SharePoint, etc.]
(b) Department specific applications and/or databases
(c) Network Shares
(d) Administrative tasks
(e) RAS / VPN Access
(f) Wi-Fi.

13.2 Access must follow a "principle of least-privilege" approach, whereby all access is revoked by default and users are only allowed access based on their specific requirements.

13.3 The levels or degrees of access control to classified information must be restricted in terms of legislative prescripts.

13.4 Access rights must be assigned to a group / role. A user must then be assigned to that group. Access rights must not be assigned to individual users.

14. NETWORK USER ACCESS RIGHTS ASSIGNMENT

14.1 Access to the Municipality's network must only be allowed once a formal user registration process has been followed.

14.2 Access to Wi-Fi must only be provided to users who require access to the network throughout the Municipality, to fulfil their business function.

14.3 RAS / VPN access must only be granted to users who require the service to fulfil their business function.

14.4 Best practice states that RAS access must only be granted to employees who require remote access to a system in order to administer the environment.

14.5 Best practice states that VPN access must only be granted to employees who:
(a) Work remotely [Not at the office];
(b) Work overtime, or not within regular office hours.

14.6 It is the responsibility of the ICT Steering Committee to ensure all users must be made aware of the security risks and obligations associated with RAS / VPN access.

14.7 RAS / VPN access must be monitored and audit logs reviewed every quarter [three months] by system administrators.

14.8 All reviews must be formally documented and signed off by the ICT Manager. Documentation must be kept for record keeping purposes. Records of RAS / VPN access reviews must be stored for a minimum of 10 years.

14.9 The ICT Manager must approve all hardware and software, owned by municipal employees and service providers / vendors.

14.10 The ICT team must ensure that all mobile devices must be protected with a PIN.

15. OPERATING SYSTEM ACCESS RIGHTS ASSIGNMENT

15.1 Each system administrator must be given their own accounts within the administrator group. Should shared accounts be required to fulfil a business function, then this account must be approved and documented by the Risk Management Committee.

15.2 The default guest account must be removed or renamed and disabled.

16. APPLICATION USER ACCESS RIGHTS ASSIGNMENT

16.1 Segregation of duties must be practiced, in such a way that application

administrators cannot perform general user tasks on an application. This is to prevent any fraudulent activity from taking place.

16.2 Applications administrators must remain independent of the department utilising the application, with the exception of the ICT department.

17. REVIEWING USER ACCESS AND PERMISSIONS

17.1 User access and user permissions must be reviewed every quarter [3 months] by system administrators.

17.2 On a monthly basis, HR must send a list of all terminated employees for that month to the ICT department. This list must be used to ensure that all terminated users have had their access revoked. Should one or more terminated users still have access to the environment, an investigation into the finding must be conducted.

17.3 On a monthly basis, the ICT Manager must review all users with administrative access to the environment and assess their rights for appropriateness. Should a user be found with excessive rights, a user access change request must be performed.

17.4 All reviews must be formally documented and signed off by the ICT Manager. Documentation must be kept for record keeping purposes. Records of user access review must be stored for a minimum of 10 years.

18. USER AND ADMINISTRATOR ACTIVITY MONITORING

18.1 User and administrator activity must be monitored through audit and event logging.

18.2 Once a month, system administrators and application owners must review audit and event logs for suspicious and malicious activities.

18.3 Dormant accounts should be disabled and a request to remove the access should be performed in line with section 11- User Permission / Role Change Request.

18.4 All reviews must be formally documented and signed off by the ICT Manager. Documentation must be kept for record keeping purposes. Records of user activity monitoring must be stored for a minimum of 10 years.