UMZIMVUBU

LOCAL MUNICIPALITY

ICT ACCOUNT & PASSWORD MANAGEMENT POLICY

TABLE OF CONTENTS

1. INTRODUCTION

Policies are required to govern the passwords used when connecting to the ULM's network from any host and/or when accessing any operating system or application requesting a password. These policies are designed to minimize the potential exposure to the ULM from damages that may result from unauthorized use of resources. Damages include the loss of sensitive or municipal-confidential data, intellectual property, damage to public image and damage to critical municipality's internal systems.

2. PURPOSE

The purpose of this policy is to ensure that management and monitoring of computer users to gain access to ULM network, computers, servers, applications and all other security measures are in place to protect authorised and unauthorised access to information. This policy is applicable to all users authorised to use ULM's network services. This means all employees that are employed permanently, contracted or temporary including councillors. All these employees will be referred to as "users" in the rest of this document.

The policy aims to restrict access to information or systems within the municipality's computer environment to authorised users as well as to prevent unauthorised use, installation and viewing of information using IT resources.

This policy focuses on password and user ID requirements, access to the municipality's computer systems and networks, and segregation of duties related to IT to ensure that IT users are aware of their responsibility towards usage of information systems in order to minimise possible information security risks. In addition, it covers remote control access, administration and third party access.

3. SCOPE

The policy applies to all business units, employees, suppliers, vendor's contractors and any other resources requiring access to the ULM computing environment.

- Computing environment includes:
- physical and virtual environmental; and
- Hardware, software, system and applications.

This policy applies to any and all personnel who have any form of computer account requiring a password on the municipality’s network including e-mail accounts.

4. ROLES AND RESPONSIBILITIES

4.1. The Municipal Manager

The MM working in conjunction with the HOD’s shall be responsible for ensuring the effective implementation and compliance of the ULM policies, standards and procedures.

4.2. The IT Manager

The IT Manager must implement, enforce and monitor the controls in accordance with the requirements outlined by management, and must advise users on the correct ways to access information and systems.

4.3. The Steering Committee

Management helps achieving this objective by making sure that access to information and business processes is controlled on the basis of security requirements that are in- line with business requirements as per COBIT ethics.

4.4. Internal Audit

The Internal Audit Unit is authorised by management to assess compliance with all corporate policies at any time.

4.5. All employees, contractors and service providers

Users must keep their access information like usernames and passwords secure, ensure that they access systems only for those purposes they were authorized for.

4.6 a. Audit trails for financial systems must be reviewed and signed off by the CFO quarterly, CFO can delegate the Deputy CFO to sign off the audit trails.

b. ICT manager have to sign the audit trails before forwarded to CFO/DCFOs.

5. POLICY **STATEMENTS**

5.1. Issuing a new or changing a password

When issuing new or changed passwords it shall be ensured that:

a. The initial password is transferred to the individual in a secure way;
b. Disclosure of passwords is minimized when they are communicated to the user (e.g. using encrypted e-mails, using codes or forcing the user to change passwords when they first use them);
c. The display and printing of passwords must be masked, suppressed, or otherwise obscured so that unauthorized parties are not able delete, to observe or subsequently recover them. Where passwords are displayed to authorized third parties, for example to a system administrator, the following conditions shall be met:
   - The users shall be forced to change the password at first logon; and
   - The functions and information that can be accessed through using the password have been classified as low sensitivity by the ULM.
   - It involves the target user directly (i.e. the person to whom the password uniquely applies);
   - the identity of the target user is verified (e.g. via a special code or through independent confirmation); and
   - When a password is initially assigned to a user the password shall be a temporary one and the user shall be forced to change it immediately;
d. A procedure of providing users who have forgotten their passwords with a new password shall be in place; and
e. The procedure shall include the following components:
   - A temporary password is to be supplied to the user after a positive identification;
   - The temporary password shall be given to the users in a secure way;
   - The user shall be forced to change the temporary password immediately; and
   - A procedure for user who believes that their password has been compromised must be in place.
f. Passwords shall be changed at least every 31 days;
g. Users that have system-level privileges granted through group membership shall have unique passwords held by the user of that account.

5.2. Minimum password length

The length of the password shall always be checked automatically at the time that users log in and will not be accepted should it does not meet the requirements. All passwords shall have at least eigth alpha-numeric and one special character.

5.3. Difficult-to-guess passwords required

All user-chosen passwords for computers, web accounts, email accounts, servers and networks shall be difficult to guess. Words in a dictionary, derivatives of user-IDs, and common character sequences such as "123456", “qwerty”, “aaabbb”, “zyxwvuts” shall not be employed. Likewise, personal details such as spouse's name, license plate, and birth date shall not be used unless accompanied by additional unrelated characters;

- Backward spelling of any name or recognizable words shall not be used; Avoid using days or months of the year;
- Passwords shall contain uppercase, lower case, digits and any special characters.

5.4. Display and printing of passwords

The display and printing of passwords shall be masked, suppressed, or otherwise obscured so that unauthorised parties shall not be able to observe or subsequently recover them.

5.5. Periodic forced password changes

All users shall be automatically forced to change their passwords at least once every 31 days. Users shall be informed of the password expiry seven (7) days before the expiry date.

5.6. Assignment of expired passwords

The initial passwords issued by a helpdesk official shall be valid only for the involved user's first on-line session. At that time, the user shall be forced to choose another password before any other work can be done.

5.7. Account lockout

A user's account shall be locked after three unsuccessful logon attempts and the system administrator can unlock user accounts or account will automatically unlock after 30 minutes.

5.8. Disclosure

a. A password shall never be disclosed to any third party.
b. A password shall not be written down.
c. The last ten (10) passwords should not be reusable, and a period of 15 days between password changes should be set to ensure that users do not change their passwords several times in a row to return to their known old password.
d. In order to prevent unauthorized access to other user's computers, information and/or data, requests to reset passwords shall be strictly and constantly monitored. System administrators shall not reset a password unless the user has logged the call with IT Helpdesk and has duly communicated in writing with Helpdesk.
e. In the case of death or when a user is on leave, the Senior Manager must request the password reset of the user in writing.

6. COMMENCEMENT OF THE POLICY

a. The policy will come into effect on the date signed by ICT Governance Champion

6.1. INTERPRETATION OF THE POLICY

a. All words contained in this policy shall have the ordinary meaning attached thereto, unless the definition or context indicates otherwise
b. Any dispute on interpretation of this policy shall be declared in writing by any party concerned.
c. The Municipal Manager shall give a final interpretation of this policy in case of written dispute.
d. If the party concerned is not satisfied with the interpretation, a dispute may then be pursued with the South African Local Government Bargaining Council.

6.2. PERMANENT/TEMPORAL WAIVER OR SUSPENSION OF THE POLICY

a. This policy may be partly or wholly waived or suspended by the ICT Governance Champion on temporary or permanent basis however the Municipal Manager/Council may under circumstances of emergency temporarily waive this policy subject to reporting of such waiver or suspension to Council

6.3. COMPLIANCE AND ENFORCEMENT

a. Senior management is required to ensure that internal audit mechanisms exist to monitor and measure compliance with this policy.

b. Failure to comply with this policy may result in disciplinary action, which may include termination of employment.

c. Any conduct that interferes with the normal and proper operation of the municipality’s IT systems, which adversely affects the ability of other users to use those IT systems, or which is harmful or offensive to other users, shall constitute violation of approved IT policies.

d. The municipality management reserves the right to revoke the privileges of any user at any time.

7. AMENDMENT AND/OR ABOLITION OF THIS POLICY

a. This policy may be amended or repealed by ICT Governance Champion /Council as it may deem necessary

8. Document Owner and Approval

The Municipality is the owner of this document. The Council of the Municipality is responsible for ensuring that this policy document is reviewed regularly to ensure that it remains relevant to the organization.

This document was approved by the Council and is issued on a version controlled basis under the signature of the ICT Governance Champion.