TOGETHER FOR PROSPERITY

AMAHLATHI LOCAL MUNICIPALITY

FINANCIAL SYSTEMS USER ACCESS POLICY

TABLE OF CONTENTS

1. INTRODUCTION

Financial Systems user access policy is a set of guidelines and rules that seeks to dictate how employees and third parties are granted access to the information systems of the municipality. This policy is to ensure that internal controls are embedded within the financial systems, financial data is protected and minimise the risk of unauthorised access to the financial systems.

2. OBJECTIVE OF THE POLICY

The main objective of this policy is to provide the municipality with best practice user access management controls and security of financial data. This policy further seeks to define the user access management controls measures for both internal users and service providers.

3. THE AIM OF THE POLICY

The aim of this policy is to ensure that the Municipality conforms with standard user access management controls to achieve a balance between ensuring legislative compliance, best practice controls, service efficiency and that risks associated to the management of user access are mitigated.

4. LEGISLATIVE FRAMEWORK

This policy was developed to align with the legislations below.

4.1. Electronic Communications and Transactions Act, Act No. 25 of 2002;
4.2. Municipal Finance Management Act, Act No. 56 of 2003;
4.3. ISO 27002:2022 Information technology — Security techniques — Code of practice for information security controls

5. DEFINITIONS

5.1. User – Employees that have access to the financial systems.
5.2. Super user – An employee that has full access to the financial systems.

6. NEW USER REGISTRATION

6.1. New internal users must be registered in the Amahlathi Local Municipality domain to be granted access to the financial systems.
6.2. The relevant supervisor must submit a signed user access request form to the financial systems administration unit with the details of access to be granted.
6.3. Employees whose duties requires access to the system must be given access based on their duties.
6.4. A unique username must be provided for each system.
6.5. A username must also be provided for vendors or contractors and access be granted after the user department has approved all the necessary documentation.
6.6. Access must be provided after all approval has been obtained.
6.7. Records of all active users must be kept safe.
6.8. Only a super user that may have full access to the financial systems.

7. TERMINATION OF USERS

7.1. A formalised user termination process must be implemented and followed to revoke access rights.

7.2. All user termination requests must be formally documented and approved by duly authorised personnel.

7.3. All access provided to users created as part of 5.5 processes must be terminated on completion of contractual agreements.

7.4. Records of all termination must be kept safe.

8. USER PERMISSION CHANGE REQUEST

8.1. User access form must be completed by the relevant supervisor with details of the adjustment that must be effected to the user account.

8.2. The changes must be done after the approval processes have been completed.

8.3. User access must be reviewed every six months of the financial year and excessive rights must be removed.

9. GENERAL USER ACCESS RIGHTS ASSINGMENT

9.1. Access rights include but are not limited to:

9.1.1. Sage Evolution System

9.1.2. Payday Payroll and Human Resources System

9.1.3. First National Bank online system

10. USERNAME AND PASSWORDS PROCEDURES

10.1. All passwords must be changed after thirty (30) days.

10.2. Passwords must have a minimum length of 8 alphanumeric characters.

10.3. Password changes must be unique from the previous two passwords.

10.4. Username and Passwords must not be shared with others.

10.5. Passwords must be treated with high confidentiality.

10.6. Passwords must not be written down.

10.7. Passwords must not consist of anything that can be linked to the account owner.

11. BACKUP PROCEDURES

All the financial data must be backed up regularly so to enable to restore it should the need arise. Daily backups must be monitored to ensure that there are no errors.

12. BREACH OF POLICY

The manager or supervisor of the employee alleged to have violated this policy must be responsible for ensuring that disciplinary proceedings are commenced in terms of Amahlathi Local Municipality disciplinary procedure and policy.

ADOPTION AND APPROVAL OF THE POLICY BY COUNCIL

This policy is adopted and approved by Amahlathi Local Municipality Council for implementation

Effective from (Date)

Approved by Resolution Number _______ on this the ____day of ________20

Signed this the ________ day of ________ 20___________. Signed this the

day of _______________ 20___________.

MUNICIPAL MANAGER **DATE**

COUNCIL SPEAKER **DATE**