Amahlathi Municipality

System Administration Policy and Procedure Manual

PURPOSE

The purpose of the backup policy is to:

- Ensure all systems are backed up
- Ensure that in the event of system failure, data loss is minimized or prevented.
- Provide guidelines to system administrators on backup type and frequency
- Establish prudent and acceptable practices regarding the backing up of systems

POLICY STATEMENTS

- Scheduling of Backups must take place as follows:
  - Daily backups are performed on BTO financial systems automatically (Monday to Friday) at 22:00 and 23:00 and must be performed daily by the dedicated official.
  - After the backup has been done the tape must be placed in a secured environment.
  - The backups must be tested on a quarterly basis
- Yearly backup tapes must be kept for a period of five years then the information must be copied away to a disk and be kept off-site in case it is needed and for the tapes to be re used.
- A Backup Log book must be created in order to track all work executed and people responsible. This will provide transparency of the process and assist with reviewing the process against this policy.
- The Systems Administrator must submit to the CFO to sign a schedule of all monthly backups done on the systems and quarterly tested backups after every quarter
- A specific naming for all backups and documentation covering the inventory and procedures must be implemented in order to facilitate the urgent restoration of data when required.
- Mirror image server must be installed in another site where all systems must be replicable so as to assist in backing up data in case the main building gets involved in disaster that will result in loss of data to restore data saved in a mirror image server
- Critical data or data that needs to be shared amongst other users must be stored in the network file server so that it can be backed up regularly.

DEFINITIONS

User - Employees that are using the systems
CFO - Chief Financial Officer

1. PURPOSE OF USER ACCOUNT MANAGEMENT POLICY

1.1 Establish a standard for creation of user accounts
1.2 Ensure proper access control to the system
1.3 Establish an appropriate control of passwords protection
1.4 Establish a minimum time between changes of passwords

2. THE SCOPE OF THIS POLICY

This policy is applicable to all users. This means all employees that are employed permanently, contracted or temporary including Portfolio Councillors. All employees/councillors will be referred to as "users" in the rest of this document.

This policy also applies to service providers when they are assisting the users using the systems.
A User Access Form must be filled indicating which access is required and also indicate the system that the access is needed for, the user access form must be signed by the relevant supervisor or the manager of the unit. The Systems Administrator must allocate the username, give access to functions then keep the records of the form in a user accounts file. The Systems Administrator is responsible for administering all the Financial Systems listed on this document.

All users must first logon to the network environment using the username and password given by ICT to login to the computer or laptop. They then must login to respective systems using their different usernames.

All access to the following systems (Venus, Payday, FNB online, Cash Drawer, Conlog, Baud and Case Ware) must be reviewed once every year during the third quarter of the municipality's financial year. All systems must enforce segregation of duties, e.g. one user captures and the other authorizes.

3. POLICY STATEMENTS

3.1 VENUS

Employees whose duties requires access to the system must be given access based on their duties. Each Departmental secretary or buyer must also be given access on Venus to view budget of their departments when requested.

3.1.1 The standard username must be six characters starting with "ama" then the number cumulative on the system.

3.1.2 The same username must be created on UNIX and Venus system to grant access.

There are different levels of access:

- Level 1- For the CFO and Systems Administrator
- Level 2- For users that views and authorize transactions.
- Level 3 – For users that captures transactions and those that are only viewing.

3.2 FNB ONLINE BANKING/ BANKIT

3.2.1 Users who are the signatories at the bank must have the username with authorization functionality (access) only. All other users must have access according to their duties.

3.2.2 All computers that will be used to run FNB online/Bank-it must have Java installed.

3.2.3 A user must be created and access be granted according to their duties and during that process a certificate to access FNB online/Bank-it must be created on their computers and it must be kept secretively by each user assigned to.

3.2.4 The system must have two administrators that add, disable and make changes on users' profiles.

3.2.5 The accounting officer must appoint users that will authorize payments

3.2.6 One of the two users that are authorizing must check the vouchers, sign the payments list and be the first to authorize on the system.

3.2.7 Audit trails must be printed, reviewed and signed at least once a month

3.3 PAYDAY

3.3.1 Employees whose duties are to work using this system must have user number and password that will give them access to the Payday System.

3.3.2 All access must be allocated according to the duties of each user.

3.3.3 One user number and password will give the user access to all payroll companies in the PAYDAY system.

3.3.4 The Systems Administrator must run a report from payday and compare with transactions on Venus to check accuracy of transactions imported from Payday to Venus and the report must be signed off to show that the transactions have been checked.

3.4 CONLOG

3.4.1 The Systems Administrator must allocate user name and access to the users based on duties assigned to the employee

3.5 CASHDRAWER

3.5.1 Employees that are involved in Income section and the Cash Management process must have a cashier number and a password to login to the system.

3.5.2 Access must be allocated according to the duties that they perform.

3.5.3 There are different levels of access control

3.5.3.1 Cashier- For capturing data

3.5.3.2 Supervisor – For Cashing up, balancing and Reporting

3.5.3.3 Systems administrator is responsible for income day end processes

3.5.4 Cashiers must not cancel receipt or do balancing without the authorization of the supervisor

4. CASEWARE

4.1. This system is used to draft Financial Statements and s71 reports.

4.2. The users must be given access to the systems by the Systems Administrator based on the duties to execute using CaseWare.

5. BAUD

- The Systems Administrator must be responsible for granting creating user name, reset user password and granting access based on responsibility of each user.

6. Customer care

- The systems administrator must create user name for each user as per request
- The allocation of user roles must be done by the Systems Administrator

7. USERNAME AND PASSWORDS

- All passwords must be changed after thirty (30) days
- Passwords must have a minimum length of 8 alphanumeric characters;
- Password changes must be unique from the previous two passwords
- Systems Administrator and the CFO must be the only users that can unlock user accounts and reset passwords
- Username and Passwords must not be shared with others;
- Passwords must be treated with high confidentiality;

- Passwords must not be written down;
- Passwords must not consist of anything that can be linked to the account owner such as username, name, birth date, nickname, child, spouse, pet's name or their birthdates;
- Users must change password at first logon after logging in with the one issued after the resetting of password specifically on PAYDAY
- Passwords must have upper and lower case characters;
- Passwords must have a combination of digits, punctuation characters as well as letters

5 DISABLING AND DELETING USERNAMES

5.1 Upon receiving communication from HR informing the retired and/or resigned employees, the systems administrator must disable the employee, ensuring that the account cannot be used / accessible.

5.2 The user account must not be deleted for a period of five years, in case later there's information requested from that account. This is also because the username holds audit trails that may be needed at some stage.

6 HOW THIS POLICY WILL BE APPLIED

- This policy must be applied to everyone who is using the system
- The manager of the employee alleged to have violated this policy must be responsible for ensuring that disciplinary proceedings are commenced with in terms of Amahlathi Local Municipality disciplinary procedure and policy.
- Managers must ensure that all their staff are made aware of the contents of this policy.

Implementation Date	Council Resolution no.	Approved Date