ICT USER ACCESS MANAGEMENT POLICY

APPROVED BY:

MR M NAKO

MUNICIPAL MANAGER

DATE: 17/06/2022

APPROVED BY:

CLLR S JANDA

EXECUTIVE MAYOR

DATE: 17/06/2022

1. POLICY BACKGROUND

The municipality identified a gap on provision of user access rights to its employees and developed this policy to also comply to guidelines which will assist in:
Making sure users granted access to municipal system are as per request.
Update all user access rights.
Checking system audit trails.
Employees no longer serving the municipality are disabled from the municipal systems.

2. POLICY PURPOSE

The purpose of this policy is to prevent unauthorised access into Mbhashe Local Municipality information systems. The policy describes the registration (New Access) and de-registration (Deactivation of Access) process for all Mbhashe Local Municipality information systems and ICT services.

3. DEFINITIONS

IT – Information Technology
ICT – Information Communication Technology
Access – being able to connect on Mbhashe LM ICT infrastructure
HOD – Head of the Department (Senior Management)
User ID – user name of the user to access municipal ICT infrastructure

4. APPLICATION AND SCOPE

This policy applies to new employees, exiting employees and change in access requirements in terms of changes in employee's positions or responsibilities in line with systems used.

5. LEGISLATIVE FRAMEWORK

The policy is developed with the legislative environment and international ICT standards.

The following legislation, amongst others, are considered in the development of this policy:

5.1 Constitution of the Republic of South Africa Act, Act No. 108 of 1996;
5.2 Electronic Communications and Transactions Act, Act No. 25 of 2002;
5.3 Minimum Information Security Standards, as approved by Cabinet in 1996;
5.4 Municipal Finance Management Act, Act No. 56 of 2003;
5.5 Municipal Structures Act, Act No. 117 of 1998;
5.6 Municipal Systems Act, Act No. 32, of 2000;
5.7 Protection of Personal Information Act, Act No. 4 of 2013
5.8 Control Objectives for Information Technology (COBIT) 5, 2012;

5.9 ISO 27002:2013 Information technology — Security techniques — Code of practice for information security controls; and
5.10 King Code of Governance Principles, 2009.
5.11 State Information Technology Act (Act no 88 of 1988)
5.12 Data Protection Act 1998
5.13 Public Access of Information Act

These best practices, standards and legislation form the basis of the structures needed in order to implement the Corporate Governance of ICT.

6. PROCEDURES FOR IMPLEMENTING POLICY

6.1 User access management

6.1.1 New Users

Access to the municipality's information services is controlled through a formal user registration initiated by a formal notification from HOD of the new user.

Each user is allocated a unique User ID (username) for identification and accessing network resources. The use of group IDs is only permitted where they are suitable for the work carried out (i.e. Training).

Each user will be given a copy of the employee access form to provide written proof of their access rights provided, signed by the HOD of affected department, ICT Manager after being approved by Senior Manager: Corporate Services for implementation by Systems Administrator.

The user signs the form indicating that they understand the conditions of access. Access to all municipality systems is provided by ICT Unit and can only be started after proper procedures are completed.

A new user will be set up upon receipt of the written notification but not made available, until the individual's commencing date. ICT Unit will maintain a record of all requests in a folder named "New Users" in the ICT Unit.

Each system will have unique access form especially financial, Human Resource and Payroll system

A new users will be group as per municipal adopted organogram and specific groups as per nature of work on the municipal active directory.

6.1.2 Change of User Requirements

Changed requirements will normally relate to amendments to users' access rights to applications as well as network access, internet access and other municipal systems.

A request for additional access rights or removal thereof, must be made in writing by the employee's Supervisor/Manager, recommended by HOD's

and approved by Senior Manager Corporate Services and must be directed to the IT Manager

The request must be in internal memo format and state:

- Name of person making request
- Job title of the employee
- Application or network access to be provided or removed.
- Effective date of access rights provided or removed

Changes will be made on receipt of a properly completed request with new access form and the completed requests will be filed under "access change requests" in the ICT Unit.

6.1.3 Termination of Users

As soon as an individual's contract with the municipality is terminated through either end of contract or resignation, all his/her access rights to the system must be revoked within 24 hours. As part of the employee termination process Manager Human Resources or Manager responsible for a Service Provider will inform the Systems Administrator in writing of all exiting employees and their date of exit.

All notifications will be kept in a file called "Terminated Users" in the ICT Unit. Additionally, Systems Administrator will positively confirm exiting employees with Manager Human Resources, each month. Unless otherwise advised, the Systems Administrator will disable network access for all exiting employees at 16:30 on their exit date.

(Old user ID's are terminated and not re-issued). This will include access to all network services. The Systems Administrator will inform Third Party application owners of exiting employees to ensure that the respective systems are updated accordingly.

All exiting employees are expected to hand over current files within their workgroup. User's information will be left in its existing home directory; however, ICT Unit can move the employee's files to specific areas if requested.

It is the responsibility of the ICT Unit to make sure that all of the hardware and software is returned by the Employee and recorded in the Employee exit Form.

6.1.4 Responsibility of the Systems Administrator to do the following within 24 Hours of receiving the completed exit form from HR:

- Disable the Domain Account
- Disable all user system access rights in all systems.
- Arrange Forwarding of Emails on request in writing.
- Remove/disable System Access, Remote Access.
- Etc.

Once all of the above has been completed the ICT Unit must sign and file the Form.

6.1.5 HOD's responsibility

Senior Managers should review activities of Line Managers / Supervisors.

Logs should be signed by either the Senior Manager or Line Manager and ICT Systems Administrators as evidence of review and evidence must be adequately maintained for recordkeeping.

HOD's should inform ICT unit in writing on receiving resignation letter of the employees and detailing assets to be collected from the employee on respected date.

6.1.6 Line Manager / Supervisor responsibility

Line Manager / Supervisor should ensure that activities, user rights and access logs of their subordinates are reviewed monthly.

6.1.7 Service Provider Access

Service provider will be only granted access to ICT infrastructure during contract agreement as per Service level Agreement (SLA) Support.
During support remote access form shall be completed by service provider before granted access to any system. There will be an official designated to review the service provider activities on the system after each session and ensure logs are signed as evidence of review to adequately maintain record keeping.

The Manager ICT shall assist in pulling out the logs and review for exceptions in the logs.

6.2 Privilege Management

Administrative privileges are the highest level of permission that is granted to a computer user. In business and networked systems, this level of permission normally allows the user to install software, and change configuration settings. Only the IT Managers or System Administrator or System owner or System Programmer and ICT technicians are granted administrative privileges. The unnecessary allocation and use of special privileges is often found to be a major contributing factor to the vulnerability of systems that have been breached.

Privileged access must be authorised by the Senior Manager Corporate Services, using the request form. All completed forms, both current and expired, will be held by the Systems administrator who is authorised by the completed form to set up the access specified.

All requests for access outside normal services must be supported by a completed and authorised Privilege Access form. The IT Manager will maintain a master list of privileged accesses, which are in use, and this will be checked and confirmed by the Systems Administrator on a three months' basis. The list will identify all separate logons for each system and service.

6.3 User Password Management

Temporary access may be granted on a need to use basis. Such logons may be granted by the Systems Administrator and must be recorded on the normal

form. Temporary logons must be identified by a specific login (starting temp.....) and must be disabled immediately after use.

6.3.1 Change of User Password

Where a user has forgotten his/her password, the ICT Unit is authorised to issue a reset. Upon receipt of such a request the ICT Unit will

- Confirm the identity of the user by question about existing services/access or by reference to a work colleague.
- Ensure the request is logged.
- Issue a temporary, single use, password which will enforce the user to change the password at first logon.
- Users are encouraged to frequently change their password every expiry date.

Procedure to follow when it's not the account owner requesting password reset:

- Written formal request must be submitted signed by the HOD
- Account owner should indicate that his aware of the request and the request is made on his behalf due to his absence.
- All request be implemented and documented by System Administrator after IT Managers approval.
- Temporal password will be generated non-owner of the account and the owner of the account will be instructed for password change immediately.

6.3.2 Password Lockout

When an employee inputs an incorrect password more than 3 times, the employees access into his/her account will be locked.

The Reset Lockout needs to be reported to ICT and the System Administrator will unlock the account or in other systems will need to wait for few minutes before attempt to login again. An employee may attempt to log into his/her account after few minutes has elapsed. Where an employee requires immediate access, the employee is required to contact the ICT Unit to unlock his/her account.

6.4 Review of user access rights

The Systems Administrator will institute a review of all network access rights, internet access, and all municipal systems that are in use at least once every quarter, which is designed to positively confirm all users. Any lapsed or unwanted logons, which are identified, will be disabled immediately and will be deleted unless positively reconfirmed.

At least once a quarter the Systems Administrator will institute a review of access to applications. This will be done in cooperation with the application owner and will be designed to positively re-confirm all users. This includes the Municipal Financial System.

The review will be conducted as follows.

- The Systems Administrator will generate a list of users, by application.

- The appropriate list will be sent to each Application owner (Departments) who will be asked to confirm that all users identified are authorised to use the system.
- Any user not confirmed will have his/her access to the system removed.
- The Systems Administrator will maintain a record of the lists sent over to Department Heads and Department Heads responses.
- A departmental heard response will be implemented accordingly.
- The review will be conducted quarterly by System Administrator.
- Error logs must be reviewed regularly and follow up on access violations must be conducted immediately.
- The IT Manager will then review the whole process accordingly and sign-off.

➢ Independent reviews of the activities of the person responsible for granting user access privileges.

➢ Assist in pulling out the logs and review for exceptions in the log.

➢ Develop and implement a register or create a file of all access violations and record times of violation with critical data violated.

➢ Periodic reviews should be conducted in accordance with the hierarchy and structure of IT function, taking into account independence from the activity and segregation of duties

The above processes will be followed for user access rights to all municipal systems including financial system of the municipality.

6.5 Audit logs

Audit log or trail reports shall be routinely generated and reviewed by the systems administrator for user accounts and evidence of the review shall be retained for future reference.

Additionally, management should ensure that the job description of the it systems administrator is reviewed and updated in order to align with current duties.

The following audit policy settings should be enabled on the systems:

- Audit object access
- Audit privilege use
- Audit process tracking

The active directory audit plus should be installed on the active directory and once functioning it will be reviewed by the systems administrator and ict unit monthly or quarterly.

7. IMPLEMENTATION

2022/2023

8. REVIEWAL

Annually