KAROO HOOGLAND LOCAL MUNICIPALITY

USER ACCOUNT MANAGEMENT POLICY

DATE OF ADOPTION: 30.05.2023

DATE OF IMPLEMENTATION: 01.07.2023

SIGNATURE OF SPEAKER: _____

DATE: _____

DATE OF REVIEWED: _____

SIGNATURE OF SPEAKER: _____

OVERVIEW

All employees and personnel that have access to the municipality computer systems must adhere to the password policies defined below in order to protect the security of the network, protect data integrity, and protect computer systems.

PURPOSE

This policy is designed to protect the municipality's resources on the network by requiring strong passwords along with protection of these passwords. Preventative controls should be implemented and detective controls are required to secure process.

SCOPE

This policy applies to any and all personnel who have any form of computer account requiring a password on the municipality's network.

PASSWORD PROTECTION

Each municipal employee is responsible for all the actions performed with his/her password, even if it's demonstrated that an action was carried out by another individual using the user's password.

Users should therefore follow good security practices in the selection and use of passwords and keeping in mind:

- Keep passwords confidential
- Avoid keeping a record of passwords, e.g. hard copy or electronic file
- Change passwords where there is any indication of possible system or password compromise
- Avoid reuse or cycling of old passwords
- Change passwords at regular intervals
- Change temporary passwords at first logon
- Never share individual passwords among users

UNATTENDED USER EQUIPMENT

All users should be made aware of the security requirements and procedures for protecting unattended equipment and implementation of such protection:

- Terminate active sessions when finished, unless such sessions can be configured by an appropriate locking mechanism, e.g. a password screen saver.
- Log computers off at end of session
- Secure computers from unauthorized use by means of a key lock e.g. password access, when not in use.

NEW USER REGISTRATION

Formal user registration procedure for granting access to users are as follows:

- The ICT Department should be informed in writing from HR department regarding new employer
- Access request form should be completed by user supervisor, signed by his/her Supervisor and Head of Department.
- The level of access granted to system should be appropriate and not compromise segregation of duties.
- The ICT department will open ticket according to access request form and when completed, signed off, ticket will be closed.
- Addendum 1- Access form should be use

CHANGE/MODIFICATION

Changes in user status include changes of job roles, responsibilities and transfers within the municipality. Procedure as follows:

- Change access form should be completed by users supervisor, signed by his/her supervisor and Head of Department.
- Ticket will be opened according to change form and completed, signed off by ICT official and ticket closed
- Addendum 1-Access form should be use

USER DEREGISTRATION

Access rights of users who have left the company should immediately be removed, procedure in place:

- IT should be informed in writing from HR Department regarding employer termination.
- User must complete access Removal form (Addendum 2) and signed off by Supervisor and Head of Department
- ICT will open ticket according to removal form, once completed, and signed off by ICT official and ticket closed.

REVIEW OF USER ACCESS RIGHTS

Review of user access rights is necessary to maintain effective control access to data and information services. User's access rights should be reviewed as follows:

- Annually- all users
- After any changes such as promotion, demotion, termination.
- Transfer from division to another within the municipality.

PASSWORD RESET PROCEDURE

Procedure to verify the identity of a user prior to a password reset is the following:

- Password reset request must be forwarded to ICT or head department by user.
- Password is reset to default password of the system, user must change password at first logon. Passwords changed should conform to password standards.

PASSWORD REQUIREMENTS (subject to change)

The following password requirements will be set by the ICT security department for Cloudware and Sebata EMS:

- Minimum Length - 8 characters recommended
- Maximum Length - 14 characters
- Minimum complexity - No dictionary words included. Passwords should use three of four of the following four types of characters:
    - Lowercase
    - Uppercase
    - Numbers
    - Special characters such as !@#$%^&*(){}[]
- Passwords are case sensitive and the username or login ID is not case sensitive.
- Password history - Require a number of unique passwords before an old password may be reused. This number should be no less than 12. According to system requirements of Cloudware and Sebata EMS.
- Account lockout threshold - 3 failed login attempts, the administrator reset the account lockout so they are aware of possible break in attempts on the network.

MONITORING OF USER ACCESS/ACTIVITIES

- Inactive users are monitored and must be blocked if inactive for 90 days.
- Periodically checks are done once a quarter to remove or block redundant user accounts.
- Repeated failed login attempts identified and investigated.
- If an unauthorized intrusion is detected, it is reported to the Director of Financial Services.
- System access logs are checked, monitored and signed by Accountant: ICT, with date verified, on regular basis.
- The logs will be reviewed/ verified by Director of Financial Services
- If any unusual activity is encountered it is entered into register and reported.
- If internal unauthorized intrusion is detected on an account it is, disabled temporally, until formal reset procedure is done.
- Where external intrusion is detected, all server, firewall, network and wireless device passwords should be changed immediately.

MONITORING OF ACCESS BY SERVICE PROVIDER

- All access is monitored by Accountant : ICT
- An access request needs to be filled in by service provider for access and only temporarily access may be granted
- An access request form should be filled in with detailing the tipe of access required.

RESPONSIBILITY

All Information Technology staff are responsible for maintaining the confidentiality and privacy of the data under our administrative control with our information technology systems and providing access only to those who have rights to this information Examples of confidential or private data may include, but are not limited to, employee information, financial data, assets, communications, personal data storage, network transaction contents, authorization codes/passwords for access to system etc.

POLICY COMPLIANCE

If any municipal user is found to have breached this policy, they may be subject to Karoo Hoogland Municipality's disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

User access may also be removed from system.

POLICY REVIEWS

At present there is a Clause in all approved policies whereby it be reviewed annually by the Council.

There is however only a certain number of policy statements (e.g. finance related) that must be reviewed annually according to legislation. This policy will be reviewed when changes are made.