KGATELOPELE LOCAL MUNICIPALITY

USER ACCOUNT MANAGEMENT POLICY

2016/2017

FINAL

1. Overview

All employees and personnel that have access to organizational 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.

2. Purpose

The policy is designed to protect the organizational 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.

3. Scope

The policy applies to any and all personnel and service providers who have any form of access to our system or computer account requiring a password on the organizational network.

4. Password Protection

Each 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

5. 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.

6. New user registration

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

- IT Department should be informed in writing from HR department regarding new employer
- Access request form should be completed by user, 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.

7. Change/Modification

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

- Change access form should be completed by user, signed by his/her supervisor/ Head of Department.
- IT Official will sign off the form and change will be completed on system.

8. User Delete

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

- IT department should be informed in writing from HR Department regarding employer termination.
- User must complete access Removal form and signed off by Supervisor/ Head of Department
- Once User Removal form is completed, then the IT Official sign off the form.

9. Review of user access rights

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

- Annually
- After any changes such as promotion, demotion, termination.
- Transfer from division to another within the same company.

10. Password reset procedure

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

- Password reset form completed by user, his/ her Supervisor / Head of Department, form is send to IT Department.
- Password reset form completed by user should be resend to IT Official.
- Password is reset to default password of the system, user can change password at first logon. Passwords changed should confirm to password standards.

11. Password Requirements (subject to change)

The following password requirements will be set by the IT department:

- 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
- Maximum password age - 30 days

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.

12. Monitoring of user access/activities

- Inactive users are monitored and must be blocked if inactive for 60 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 IT Department, by completing an security incident form.
- System access logs are checked, monitored and signed by Management, with date verified, on regular basis.
- The logs will be reviewed/ verified by Municipal Manager or Director of Corporate service depending on availability.
- 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.

13. Responsibility

IT Official 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.

14. Policy Compliance

If any user is found to have breached this policy, they may be subject to KLM 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