Password Policy

1. Preamble

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

This policy has been developed considering the following prescripts and or acts:

- Promotion of Access to Information Act (Act no 43 of 1996);
- Electronic Communications and Transactions Act (Act no 25 of 2002);
- The Constitution of the Republic of South Africa (Act 108 of 1996)
- The protection of Information Act (Act 84 of 1982)
- The Municipal Finance Management Act (act 1 of 2002)
- Organizational policies and Procedures (Mohokare Municipality)

2. Purpose

This policy is designed to protect the municipality resources on the network by requiring strong passwords along with protection of these passwords, and establishing a minimum time between changes to passwords.

3. Scope

This policy applies to any and all personnel who have any form of computer account requiring a password on the municipal network including but not limited to a domain account and e-mail account and financial systems (SebataFMS and VIP Payroll System).

4. Password Protection

4.1 Never write passwords down.
4.2 Never send a password through email.
4.3 Never include a password in a non-encrypted stored document.
4.4 Never tell anyone your password.
4.5 Never reveal your password over the telephone.
4.6 Never hint at the format of your password.
4.7 Never reveal or hint at your password on a form on the internet.
4.8 Never use the "Remember Password" feature of application programs such as Internet Explorer, your email program, or any other program.
4.9 Never use your corporate or network password on an account over the internet which does not have a secure login where the web browser address starts with https:// rather than http://
4.10 Report any suspicion of your password being broken to your IT department.
4.11 If anyone asks for your password, refer them to IT Unit.
4.12 Don't use common acronyms as part of your password.
4.13 Don't use common words or reverse spelling of words in part of your password.
4.14 Don't use names of people or places as part of your password.
4.15 Don't use part of your login name in your password.
4.16 Don't use parts of numbers easily remembered such as phone numbers, social security numbers, or street addresses.

4.17 Be careful about letting someone see you type your password.

5. Password Requirements

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

5.1 Minimum Length - 8 characters recommended
5.2 Maximum Length - 14 characters
5.3 Minimum complexity - No dictionary words included. Passwords should use three of four of the following four types of characters:
  5.3.1 Lowercase
  5.3.2 Uppercase
  5.3.3 Numbers
  5.3.4 Special characters such as !@#$%^&*(){}[]
5.4 Passwords are case sensitive and the user name or login ID is not case sensitive.
5.5 Password history - Require a number of unique passwords before an old password may be reused. This number should be no less than 24.
5.6 Maximum password age - 60 days
5.7 Minimum password age - 2 days
5.8 Account lockout threshold - 4 failed login attempts
5.9 Account lockout duration - The account lockout should be between 30 minutes and 2 hours.
5.10 Password protected screen savers should be enabled and should protect the computer within 5 minutes of user inactivity. Computers should not be unattended with the user logged on and no password protected screen saver active.
5.11 Users can press the CTRL-ALT-DEL keys and select "Lock Computer".

6. Other Considerations

Administrator passwords should be protected very carefully. Administrator accounts should have the minimum access to perform their function. Administrator accounts should not be shared.

7. Policy Review

This policy will be reviewed annually.