EPHRAIM MOGALE LOCAL MUNICIPALITY

PASSWORD SECURITY POLICY & PROCEDURE

DOCUMENT APPROVAL

Responsible Person:	Name	Signature	Date

Date approved: _____

1. OVERVIEW

Password are an important aspect of the any computer security. They are in the for front of the protection of user accounts. A poorly chosen password may compromise the entire Ephraim Mogale Local Municipality network. All employees including contractors and vendors with access to the Municipal systems are responsible for taking appropriate steps to select and secure password.

2. PURPOSE

The purpose of the policy is to establish a standard code for the creation of credible passwords, their security and how frequent shall they be changed.

3. SCOPE

The scope of the policy include all personnel who have access or are responsible for an account or any form of access that support or requires a password on any system that reside at any Municipal facility.

4. POLICY

4.1 GENERAL

i. all systems level password i.e root, enable, NT admin, application administration accounts, etc.
ii. all production system level password must be part of the administered global password management database.
iii. all users level password i.e emails, web, desktop computer, etc shall be changed at least every month.
iv. password must not be inserted in email messages or any other form of electronic communication.
v. all user level and system level password shall conform to the guidelines as described:

5. GUIDELINES

Password are used for various purposes. Some of the more common uses include user level accounts, web accounts, email accounts, screen saver protection, voicemail password and local router logins. Since very few systems have support for one time tokens (i.e dynamic password which are only used once), everyone should be aware of how to select strong password.
Poor, weak password are identified by having the following characteristics:

i. password contains less than six charaters.
ii. Password is a word found in a dictionary.
iii. Password contains common usage word such as:

- names of family, pets, friend, co-worker, fantasy characters, etc.
- computer terms and names, commands, sites, companies, hardware, software, etc.
- birthdays and other personal information such as addresses and phone numbers.
- words or numbers patterns like aaaabbb, qwert, 123321, etc.
- words patterns preceded by a digit (e.g secrete1, 1secrete).

Strong password are identified by having the following characteristics

i. contains both upper and lower case characters such (e.g a-z, A-Z).
ii. have digits and punctuation characters as well as letters (e.g 0-9, #$@*^>.
iii. are at least six alphanumerical characters long and is a passphrase.
iv. are not a works in any language, slang, dialect, jargon, etc.
v. are not based on personal information, names of family etc.
vi. aassword should never be written down or stored on line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase.

6. PASSWORD PROTECTION STANDARDS

Do not use the same password for Ephraim Mogale Local Municipality accounts and other non Municipal access such as personal ISP account.
Where possible do not use the same password for various Municipal access needs, select one password for each access needs.

Do not share your password with anyone, including supervisors, managers and secretaries, all password are to be treated as sensitive and confidential information.

7. THINGS NOT TO BE DONE

- Reveal a password over the phone to anyone.
- Reveal a password via an email.
- Talk about a password in front of others.
- Hint at the format of the password.
- Share password with family members.
- Reveal password to co-workers while on vacation.
- Don not write down and store password and store them in your office and never store such a password in a file on any computer without encryption.

8. THINGS TO DO

- Change password on monthly basis
- In the event an account is suspected to have been compromised, it must be reported immediately and be changed.

Password cracking or guessing shall be performed on a periodic or random basis, should the password be cracked the user shall be required to change it.

9. APPLICATION DEVELOPMENT STANDARDS

Application developers shall ensure that their programme contain the following security precautions:

i. application should support authentication of individual users, not group.
ii. application should not store passwords in clear text or in am easily reversible form.
iii. application should provide some sort of role management, such as one user can take over the functions or another without having to know the other's password .

10. USE OF PASSWORDS AND PASSPHRASES FOR REMOTE ACCESS USERS

Access to the Ephraim Mogale Local Municipality network via remote access shall be controlled using one time password authentication key system with strong passphrase.

11. PASSPHRASE

Passphrases are not the same as passwords, they are longer than the password and is therefore more secure. It is typically composed of multiple words.

A good passphrase is relatively long and contain a combination of upper and lowercase letters and numeric and punctuation character e.g "The&*%#Marblehall?<>is a City'

12 ENFORCEMENT

Any employee found to have violated this policy may be subjected to disciplinary action.
