FETAKGOMO TUBATSE

LOCAL MUNICIPALITY

Password Protection Policy

Council Resolution OC148/2018

Password Protection Policy

Free Use Disclaimer: *This policy was created by or for the Fetakgomo Tubatse Local for the internal control measures. All or parts of this policy can be freely used for the Municipality.*

1. Overview

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of our resources. All staff, including contractors and vendors with access to Fetakgomo Tubatse Local Municipality IT systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2. Purpose

The purpose of this policy is to establish a standard for creation of strong passwords and the protection of those passwords in effecting the internal control for information.

3. Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any IT system that resides at any Municipal's Network, has access to the network, or stores any Municipality's information.

4. Policy

4.1 Password Creation

4.1.1 All user-level and system-level passwords must conform to the *Password Construction Guidelines*.

4.1.2 Users must use a separate, unique password for each of their work related accounts.

Users may not use any work related passwords for their own, personal accounts.

4.1.3 User accounts that have system-level privileges granted through group memberships or System such as Solar must have a unique password from all other accounts held by that user to access system-level privileges. In addition, it is highly recommend that some form of multi-factor authentication is used for any privileged accounts

4.2 Password Change

4.2.1 Passwords should be changed monthly or when there is reason to believe a password has been compromised.

4.2.2 Password cracking or guessing may be performed on a periodic or random basis by the IT Unit Team or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it to be in compliance with the Password Construction Guidelines.

4.3 Password Protection

4.3.1 Passwords must not be shared with anyone, including supervisors and co-workers. All passwords are to be treated as sensitive, Confidential Municipal information. Group Security policy recognizes that legacy applications do not support proxy systems in place. Please refer to the technical reference for additional details.

4.3.2 Passwords must not be inserted into email messages, Alliance cases or other forms of electronic communication, nor revealed over the phone to anyone.

4.3.3 Passwords may be stored only in “password managers” authorized by the Municipality.

4.3.4 Do not use the "Remember Password" feature of applications (for example, web browsers).

4.3.5 Any user suspecting that his/her password may have been compromised must report the incident to IT Unit and change all passwords.

4.4 Application Development

Application developers must ensure that their programs contain the following security precautions:

4.4.1 Applications must support authentication of individual users, not groups.

4.4.2 Applications must not store passwords in clear text or in any easily reversible form.

4.4.3 Applications must not transmit passwords in clear text over the network.

4.4.4 Applications must provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

4.5 Multi-Factor Authentication

4.5.1 Multi-factor authentication is highly encouraged and should be used whenever possible, not only for work related accounts but personal accounts also.

5. Policy Compliance

5.1 Compliance Measurement

The IT Unit team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, IT monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the IT Steering Committee in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action.

6 Related Standards, Policies and Processes

6.1 Password Construction Guidelines

a) The password should have a minimum of Eight (8) Characters, User need to choose a password that’s strong enough.

b) It should Include Numbers, Symbols, Capital Letters, and Lower-Case Letters: Use a mix of different types of characters to make the password harder to crack.
c) It Isn't a Dictionary Word or Combination of Dictionary Words: user(s) should stay away from obvious dictionary words and combinations of dictionary words. Any word on its own is bad. Any combination of a few words, especially if they're obvious, is also bad. For example, "house" is a terrible password. "Red house" is also very bad.
d) Users Doesn't Rely on Obvious Substitutions: Don't use common substitutions, either — for example, "H0use" isn't strong just because you've replaced an o with a 0. That's just obvious.

7 Policy Review and Maintenance

The Policy will be reviewed and updated, twenty four (24) months, or as needed, to ensure that the policy remains aligned with changes to relevant laws, contractually obligations and best practice.

8 Revision History

Date of Change	Responsible	Summary of Change
May 2018	IT Unit and Risk Management	Updated and converted to new format.
October, 2018	IT Steering Committee	Updated to confirm with Policy