



**Islamic Republic Of Afghanistan
Kabul Municipality**



PASSWORD POLICY

IT DEPARTMENT

H.E Mohammad Yonus Nawandesh

Signature: _____



Islamic Republic Of Afghanistan Kabul Municipality



1. Purpose and Objective:

This policy is designed to protect the KM computer resources by requiring difficult passwords along with the protection of these passwords, and establishing a minimum time between changes to passwords.

2. Scope:

This policy applies to any and all personnel who have any form of computer account requiring a password including but not limited to a computer account, FMIS account, and/or e-mail account.

3. Policy:

All KM employees and personnel that have access to the Kabul Municipality computer systems must adhere to the following guidelines in order to protect the security of the network, protect data integrity, and protect computer systems.

1. Never write passwords down.
2. Never send a password through email.
3. Never include a password in a non-encrypted stored document.
4. Never tell anyone your password.
5. Never reveal your password over the telephone.
6. Never reveal or hint at your password on a form on the internet.
7. Never use the "Remember Password" feature of application programs such as Internet Explorer, your email program, or any other program.
8. Never use your 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://`
9. Report any suspicion of your password being broken to your IT department office.
10. If anyone asks for your password, refer them to your IT department office.
11. Don't use common acronyms as part of your password.
12. Don't use common words or reverse spelling of words in part of your password.
13. Don't use names of people or places as part of your password.
14. Don't use part of your login name in your password.
15. Don't use parts of numbers easily remembered such as phone numbers, social security numbers, or street addresses.



Islamic Republic Of Afghanistan Kabul Municipality



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

17. Administrator passwords should be protected very carefully. Administrator accounts should not be shared and only IT staff should have access to Administrator accounts on each and every system.

4. Procedures:

4.1 Password/Password Construction. All users at KM should be aware of how to select strong passwords.

Strong passwords have the following characteristics:

- Contain at least three of the five following character classes:
 - Lower case characters
 - Upper case characters
 - Numbers
 - Punctuation
 - “Special” characters (e.g. @#\$%^&*()_+|~=-\`{ }[]:”;’<>/ etc)
- Contain at least eight (8) alphanumeric characters.

Weak passwords have the following characteristics:

- The password contains less than eight characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
 - Names of family, pets, friends, co-workers, fantasy characters, etc.
 - Computer terms and names, commands, sites, companies, hardware, software.
 - The words "Kabul Municipality", "Municipality", "Kabul" or any derivation.
 - Birthdays and other personal information such as addresses and phone numbers.
 - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.

Try to create passwords that can be easily remembered. One way to do this is create a password based on a well-known title, affirmation, or other phrase. For example, the phrase might be: "One Tree for Myself, One for My Country" and the password could be: "13fm1fmc" or "otfmofmc" or some other variation.

(NOTE: Do not use either of these examples as passwords!)



Islamic Republic Of Afghanistan Kabul Municipality



Some additional points about the password setting and security;

1. Passwords are case sensitive and the user name or login ID is not case sensitive.
2. 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. Users should be in the habit of not leaving their computers unlocked. They can press the CTRL-ALT-DEL keys and select "Lock Computer".

5. Consequences of Violations:

Since password security is critical to the security of the organization and everyone, employees that do not adhere to this policy may be subject to disciplinary action according to the *"Disciplinary Policy of Kabul Municipality."*

6. Policy Evaluation:

This policy should be regularly evaluated to ensure it is enabling and effectively moving Kabul Municipality towards its sustainability goal.

7. Policy Enforcement:

The contents of this policy are enforceable after His Excellency the Mayor's approval.