CM(SYS)/10/2023-24,
Date- 06/06/2023

From The Office of Chief Manager (Systems),
Information Technology Department,
48, Market Street,
Kolkata – 700 087

COMMUNIQUÉ

As directed by Municipal Commissioner, this is to be intimidated to all concerned that Computer Password Policy in KMC is to be strictly adhered to. In this regard, Municipal Commissioner's Circular No. 39 of 2010-11 dated 27/12/2010 is to be followed and maintained. Responsibility of password assigned to an employee of KMC is solely of the employee concerned.

This communiqué is circulated as a reminder to follow the existing password policy as laid down in detail in Municipal Commissioner's Circular No. 39 of 2010-11.

06/06/2023

Chief Manager (Systems)
I.T. Department, KMC

Distribution:

All Controlling Officers
All HoDs

THE KOLKATA MUNICIPAL CORPORATION
Central Municipal Office Buildings,
5 S N Banerjee Road, Kolkata 700 013

Municipal Commissioner's Department

Dated: October 27, 2010

Municipal Commissioner's Circular No. 39 of 2010-11

Computer Password Policy

The matter of streamlining the existing computer password protocol as circulated vide Municipal Commissioner's Circular No. 13 of 2005-06 dated 5th August 2005 was under consideration of the KMC authority for quite some time. After protracted deliberations on the issue a detailed password policy has been adopted. It is enjoined upon all concerned to follow the noted below password policy to keep the sanctity of the password in the interest of the Corporation as well as in the interest of the password selector. In case it is found that password is accessed by anybody other than the password selector then she/he shall be held responsible for any damage caused to the Corporation.

The main idea behind it is only to protect the interest of the Corporation as well as that of the password selector.

1. Passwords are an important aspect of system security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of KMC Application. As such, all the KMC employees (including contractors and vendors with access to KMC Applications) are responsible for taking appropriate steps, as outlined below, to select and secure their passwords.
2. The purpose of this policy is to set up a standard for creation of strong passwords, protection of those passwords and frequency of change.
3. a) A password should not be
    - A dictionary word
    - It should not have any bearing on the name/surname of the employee concerned or any office/family members, and
    - It should not contain numericals having any bearing with the KMC or the employee concerned, such as his date of birth or year of passing school or year of graduation or any such obvious number.

    b) A password should be a random alpha-numerical code (i.e. containing both alphabets and numerical) containing at least one
    - Letter in capital
    - 'underscore', and
    - at least three numerical

The capital letter(s) and the 'underscore' and the numerical may be placed at random within the password.

c) A password should be changed once in every twenty day.

d) While changing the password, adequate care should be taken to ensure that a new password selected should not have any resemblance with the previous password.

e) The length of a password must be at least eight characters.

f) A password must be changed by the user during the first Login. With a default password the user cannot access the Application.

g) 5 consecutive failed login attempts (due to wrong passwords) will lock the user account and the account will be locked for a period of 1 day. Only System Administrator is authorized to unlock the user account.

h) During login, the Application will send a warning message to change the password 5 days before the password expiration time.

i) During password change, the user cannot reuse the last three used passwords.

4. Guidelines to create a password

The following standard password guidelines should be followed by KMC users to secure the Application. KMC users must avoid poor password characteristics and adhere to the Strong password guidelines.

Poor, weak passwords have the following characteristics:

a. Such a password is a word found in a dictionary (English or foreign)
b. Such a 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 "KMC", 'kolkata', 'passward' or any derivation
    - Birthdays and other personal information such as addresses and phone numbers
    - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
    - Any of the above if written in reverse order.
    - Any of the above preceded or followed by a digit (e.g. secret 1, 1secret)

Strong passwords:

A. Contain both upper and lower case characters (e.g., A-Z, a-z)
B. Have digits as well as letters e.g., 0-9, A-Z, a-z
C. Are at least eight alphanumeric characters long
D. Is not a word in any language, slang, dialect, jargon, etc.
E. Are not based on personal information, names of families, etc.
F. Passwords should never be written down or stored online

6. Guidelines to secure a password

- Don't reveal a password over the phone to ANYONE
- Don't reveal a password in an email message
- Don't share password with friends, colleagues, relatives, superiors and subordinates. Responsibility of the password is solely of the employee concerned.
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name')
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't reveal a password to co-workers while on vacation Do not use the "Remember Password" feature of applications/browsers (e.g., Eudora, Outlook, Netscape Messenger).
- Don't write passwords and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption. If an account or password is suspected to have been compromised, change the password immediately.

This is issued with the approval of the Hon'ble Mayor.

(ARNAB ROY)
MUNICIPAL COMMISSIONER

Distribution:

1) All Controlling Officers
2) All Heads of the Department (The subordinate staff who operates computer may be intimated accordingly)
3) All Managers (Systems)/Dy. Managers (Systems)