SAN BERNARDINO MUNICIPAL WATER DEPARTMENT

POLICIES & PROCEDURES MANUAL

POLICY 61.040 - PASSWORDS

Date:	July 2024
Revision No:	2
Supersedes:	July 2022
First Adopted:	April 24, 2018

POLICY:

This policy shall apply to all Department employees who have, or are responsible for, any system account (or any form of access that supports or requires a password) on any system that resides at any Department facility, has access to the Department network, or stores any Department information. This includes network logins, applications, or any other accounts that store Department information, regardless of location or form. The provisions of this policy shall also apply to any vendor, contractor, consultant, or other entity that in the course of their duties may require access to Department data and resources.

In order to preserve the security of the Department's information assets, including communication systems and equipment, passwords shall be changed at regular intervals. Employees shall change their network passwords every 180 days. The system will be configured so that each employee will be required to change his/her password at the established interval. Passwords for Department system and network infrastructure shall be changed every 180 days, or as required.

PROCEDURE:

Password Attributes:

Passwords are used for various purposes within the Department. Some of the more common uses include software/database accounts, web accounts, email accounts, screen saver protection, voicemail password, and network logins. All employees should be aware of the difference between poor/weak passwords and strong passwords.

Poor/weak passwords have the following characteristics:

- The password contains less than twelve (12) characters

- The password is a word found in dictionary (English or other languages)
- The password is a common word such as:
  - Names of family, pets, friends, coworkers, fantasy characters, etc.
  - Computer terms and names, commands, sites, companies, hardware, software
  - The words "San Bernardino Municipal Water Department", or any variation thereof
  - Birthdays and other personal information such as addresses and phone numbers
  - Letter, word, or number patterns such as aaabbb, qwerty, zyxwvuts, 123321, etc.
  - Any of the above spelled backwards
  - Any of the above followed by a digit (i.e. qwerty1 or 1qwerty)

Strong passwords have the following characteristics:

- Contain both upper and lower case letters
- Have digits and punctuation characters as well as letters
- Are at least twelve (12) characters long and is a passphrase (Ohmy1stubbedmyt0e!)
- Are not words in any language, slang, dialect, or jargon
- Are not based on personal information, names of family or pets, etc.

Department Password Requirements

Passwords must be random and not contain common words, family names, or pet names. Passwords must be a minimum of twelve (12) characters and must meet three (3) of the following four (4) conditions:

1. Uppercase letters
2. Lowercase letters
3. Numbers
4. Special characters (@, ?, !, #, etc.)

Password Security

Passwords shall not be written down or stored online unless stored in a secure password manager approved by the Information Technology section. Employees should try to create passwords that can be easily remembered. One way to do this is to create passwords that

are based on song titles, affirmations, or passphrases. For example, the phrase might be "This May Be One Way to Remember" and the password could be "TmB1w2R!" or "Tmb1W>r~", or some other variation.

NOTE: Do not use any of the examples included in this policy as passwords.

Upon resignation, retirement, or termination of an employee, Human Resources will notify the Information Technology section to disable all associated user accounts. All user files and data shall be placed on administrative hold until a determination is made with respect to the distribution of this information.

Password Protection Standards

Employees shall not use the same password for Department accounts and other non-Department access (e.g., personal email accounts, bank accounts, benefits, etc.). Employees shall not use the same password for multiple network and application accounts.

Employees are not to share passwords to Department accounts with anyone, including administrative assistant staff, without the authorization of Human Resources, the Deputy General Manager, or General Manager. Questions or concerns regarding requests to share or divulge passwords should be directed to Human Resources. All passwords are to be treated as sensitive and confidential Department information.

Unless authorized by Human Resources, the Deputy General Manager, or the General Manager, employees, with the exception of Information Technology staff, should not:

- Reveal a password over the phone to anyone
- Reveal a password to a supervisor

Employees should never:

- Discuss passwords in the presence of others
- Hint at the format of a password
- Reveal a password in an email
- Reveal a password on questionnaires or security forms
- Share passwords with family members
- Reveal passwords to coworkers while on vacation or otherwise out of the office
- Use the "Remember Password" feature of applications

- Write passwords down or store them anywhere in their work area
- Store passwords in a file on any computer system, including smart phones or similar devices, without encryption

If an account or password is suspected to have been compromised, employees must immediately report the incident to the Information Technology section and change all passwords.

Policy Review

Board approved:	5/18/2018
No changes:	7/2019
No changes:	7/2020
No changes:	7/2021
Minot changes GM approved:	7/2022
No changes:	7/2023
Minor changes (removed Lockout on last page) GM approved:	7/2024

ACKNOWLEDGEMENT OF MANDATORY COMPLIANCE WITH CITY OF SAN BERNARDINO MUNICIPAL WATER DEPARTMENT POLICY ON PASSWORDS

I hereby acknowledge receipt of the City of San Bernardino Municipal Water Department Policy on Passwords (Policy No. 61.040). I have read the policy and understand that compliance with this policy is mandatory, and violation of this policy may result in discipline up to and including termination.

_____ _____

Date Employee Signature

_____

Employee Name (Print)