CITY OF NORWALK TECHNOLOGY DEPARTMENT

POLICY: PASSWORD PROTECTION POLICY

EFFECTIVE DATE: 10/1/2018

Passwords are an important aspect of computer and online security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of the City of Norwalk's entire network. As such, Norwalk employees (including contractors and vendors with access to Norwalk systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords. The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

This policy applies to all City personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides on any system used to conduct the City's business whether stored at a City Department/facility or in the Cloud or hosted at a vendor location, or has access to the Norwalk network, or stores any non-public City information.

I. Current Practices & Procedures

Users will be issued a standard User identification by the Information Technology Department which identification is to be used by only that user. An initial password will be assigned to that identification by the Information Technology Department and must be changed when the User first logs on to the network. Additional safe practices regarding passwords are as follows:

a. All user-level passwords (network, email, web, desktop computer, application, etc.) must be changed at least every 180 days (6 months).
b. Users will not be able to repeat any of their previous five (5) passwords.
c. User-level passwords will follow the "complex password" standard.
d. Users will be locked out of the network after five (5) consecutive unsuccessful password attempts. In order to be "unlocked," users must contact the Information Technology Department.
e. Passwords must not be transmitted through email or any form of electronic communication.

II. Guidelines

a. Default, out-of-the-box passwords shall not be used for any City equipment or devices.
b. Passwords will be required to contain at least 12 characters.
c. Passwords should not be found in a dictionary (English or foreign).
d. The password should not be a common usage word such as:
    - Names of family pets, friends, co-workers, fictional characters, etc.

- Computer terms and names, commands, sites, companies, hardware, or software.
- The phrase "City of Norwalk" or any derivation.
- Birthdays or any other personal information such as addresses and phone numbers.
- Word or keyboard patterns like aaabbb, qwerty, 123456, etc.
- Any of the above followed or proceeded by a digit (e.g., password1, 1password).

e. City passwords must be complex. Complex passwords have the following characteristics:
   - Cannot contain all or part of the user's account name or 3 or more consecutive characters of the user's full name.
   - Be at least 12 characters in length.
   - Contain characters from three of the following four categories:
     i. English uppercase characters (A to Z).
     ii. English lowercase characters (a to z).
     iii. Numbers (0 to 9).
     iv. Non-alphabetic characters (!, $, #, %, etc.).

f. For assistance, including tips and tricks to creating and remembering strong, secure passwords, refer to the City's Password Policy Creation document or contact the Information Technology Department.

III. Password Protection Standards

a. Do not use the same password for your Norwalk network accounts as for other non-City accounts (personal email, online trading, etc.).
b. Where possible, do not use the same password for various City applications.
c. Do not share your passwords with anyone, including administrative assistants, vendors, contractors, interns, temporary staff, etc. All passwords are to be treated as sensitive, confidential Norwalk information. Users are responsible for all transactions made using their userIDs and passwords.
d. The Norwalk Information Technology Department will NEVER ask for request an employees' password.
e. If anyone requests your password, refer them to this document or have them talk to the Information Technology Department.
f. Do not write your password down or store it anywhere near your desk (under your keyboard, taped to your monitor, etc.).
g. Log off of your computer at the end of the day.
h. Use a password-protected screensaver/screenlock if you leave your computer, even for a few minutes. Press CTRL+ALT+DELETE and then press ENTER to do so.
i. If an account password is suspected to have been compromised, report it immediately to a member of the Norwalk Information Technology Department.

IV. Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

V. Document Distribution & History

This document is the property of the City of Norwalk and is distributed to all employees, contractors, and vendors with network access privileges for reference. Questions regarding this Password Protection document can be directed to the Norwalk Information Technology Department at (203) 854-7714.

Approvals:

ITT Committee: June 6, 2018

Director, Information Technology

Corporation Counsel

Director, Personnel and Labor Relations

Mayor Harry W. Rilling