Document Type:	Exhibit
Number:	4.30aa
Effective:	03-31-25
Revised:	03-05-25
Legal References:	

PASSWORD MANAGEMENT EXHIBIT

I. INTRODUCTION

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

II. PURPOSE

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.

III. 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 system that resides at any City facility, has access to the City's network, or stores any the City's non-public information.

IV. REGULATION

A. General

a) All system-level passwords (e.g., root, enable, Windows Administrator, application administration accounts, etc.) must be changed upon departure of any user who knows the password or annually, whichever occurs sooner.

b) All shared account passwords must be changed any time personnel that know the password either leave the organization or change roles where they no longer need access to that shared account.

c) All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every 365 days. This includes shared accounts.

d) User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user.

e) All user-level and system-level passwords must conform to the guidelines described below.

B. Effective March 31, 2025, the System shall:

a) Require password lengths of at least 12 characters

b) Require the use of at least one lowercase letter, one uppercase letter and one special character or number

c) Enable a banned word list

d) Not allow passwords from list of known breached passwords

e) Not allow the use of two numbers in a row

f) Expire user passwords within 365 calendar days

g) Not be identical to the previous ten (10) passwords

h) Not be transmitted in the clear outside the secure location

i) Not display when entered

C. The user shall:

a) Never write password down

b) Never share their password with anyone

c) Never use their city password with any other account or system

d) Never use their username as part of their password