Document Type:	Exhibit
Number:	4.30aa
Effective:	07-21-21
Revised:	
Legal References:	

PASSWORD MANAGEMENT STANDARDS

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 in the below standards, to select and secure their passwords.

The scope of these standards 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.

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 User-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every 90 days.

C. 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.

D. All User-level and system-level passwords must conform to the guidelines described below.

The System shall:

A. Require password lengths of at least 8 characters

B. The use of at least one lowercase letter, one uppercase letter and one special character or number

C. Not be a dictionary word or proper name

D. Expire User passwords within 90 calendar days

E. Not be identical to the previous ten (10) passwords

F. Not be transmitted in the clear outside the secure location

G. Not display when entered

The User shall:

A. Never write password down

B. Share their password with anyone

C. Use the same password with another account or system

D. Never use their Username as part of their password