City-wide Password Standard

PURPOSE AND SCOPE

The purpose of this document is to define required password standards for all City and County of San Francisco (City) systems and applications to protect the integrity, availability and confidentiality of information assets and systems.

This policy shall apply to all user accounts managed either centrally or at the departmental level.

PASSWORD STANDARD

- The City and County of San Francisco (CCSF) requires a strong password policy to mitigate against password attacks.
- Departments are authorized to use higher standards commensurate with the risk to their environment and / as required by regulatory and compliance needs.

Feature	Minimum Requirements
Password Expiration	Every 90 days
Minimum Length	12 characters
Password Complexity	Enabled, all four categories included (upper case, lower case, numeric, special character)
Minimum Password Age	1 day
Password History	Last 7
Account Lockout	After 5 unsuccessful consecutive logon attempts
Lock-Out Duration	10 minutes
Screen saver	Idle after a maximum of 10 minutes, password protected

All City departments must implement the password standard no later than 31 January, 2017.

COIT Policy Dates

Approved:
Next Review Date: FY2017-18

City-wide Password Standard

STANDARD REQUIREMENTS

1. Password Usage procedures

a. Passwords shall be memorized and never written down or recorded along with corresponding account information or usernames.

2. Password Sharing

a. Passwords shall not be transferred or shared with others unless the user obtains appropriate authorization to do so.

3. Electronic Transmission

a. All electronic password transmissions shall be encrypted. Passwords shall be transmitted using either transport layer security (TLS) or stronger transport security protocol.

4. Authentication and Error messages

a. Correct Response Example

b. "Login failed; Invalid userID or password"

5. Password Change

a. Users shall setup security questions to enable them change forgotten passwords.

ROLES AND RESPONSIBILITIES

1. City Chief information security officer

a. Shall be responsible for enforcing this policy across all City agencies.

b. Shall Ensure compliance across all City agencies

2. Departments

a. Shall ensure compliance to this policy

b. Shall educate users about their role in enforcing this policy

3. Departmental information security officer / Liaisons

a. Shall be responsible for enforcing this policy in their respective departments.

4. Directory Service administrators

a. To configure the new password standards in the user directories

5. **Users**

a. Shall comply with all the provisions of this policy

b. Shall setup security questions on the Identity and Access Management system to enable them reset their passwords.

EXCEPTIONS

Exceptions may be granted in case of legacy systems. The highest acceptable password for such legacy systems shall be implemented in consultation with the City CISO.

AUTHORIZATION

SEC. 22A.3. Of the City's Administrative Code states, "COIT shall review and approve the recommendations of the City CIO for ICT standards, policies and procedures to enable successful development, operation, maintenance, and support of the City's ICT."

REFERENCES

- City-wide Cybersecurity policy available at: http://sfcoit.org/coit-policies