City of Santa Ana Administrative Policies and Procedures	City Manager's Authorization Section	
Subject **Password Policy**	Date March 20, 2014	Number AD-01

1. Policy 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.

2. Policy Scope

The scope of this policy includes all End User Accounts with access to the City's computing network, specific applications and data.

3. Policy Description

Passwords are an important aspect of computer security and are usually the front line of protection for user accounts. A poorly chosen password may result in the compromise of the City's entire enterprise network. As such, all employees (including contractors, vendors, and temporary staff with access to City systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

4. Policy

4.1. General

• All user-level passwords must be changed at least every 90 days.

• Passwords must not be inserted into e-mail messages or other forms of electronic communication.

4.2. Standard

4.2.1. Password Rules

Strong passwords will have the following characteristics:

- Are at least eight characters long
- Contain both upper and lower case letters (e.g., a-z, A-Z).
- Valid character types are numbers, upper case letters, lower case letters and special characters (such as !,$,#,%).
- Must contain at least 3 of the 4 character types listed above.
- Expire in 90 days or less
- Cannot reset password within 30 days

- Cannot reuse the last 5 passwords
- Auto lockout: after 5 attempts
- Must not contain their Username

4.2.2. Password Protection

Do not share passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential information.

End User passwords should never be written down. Try to create passwords that can be easily remembered yet hard to guess. One way to do this is create a password based on a song title, affirmation, or other phrase. 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.

Here is a list of things to avoid:

- Giving your password over the phone to ANYONE, including support personnel.
- Sending a password in an e-mail message.
- Telling your boss your password.
- Talking about a password in front of others.
- Hinting at the format of a password (e.g., “my family name”).
- Writing in your password on questionnaires or security forms.
- Sharing your password with family members.
- Telling your co-workers your password while on vacation.
- A single word in any language, slang, dialect, jargon, etc.
- Based on personal information, names of family, etc.

If someone demands a password, refer him or her to this document or have him or her call someone in Information Technology.

Passwords stored in a file on ANY computer system (including mobile devices such as iPads, tablets or smart phones) can be compromised if encryption isn’t used to secure them.

If you suspect that your account or password is compromised, change all passwords and report the incident to your Supervisor.

Password strength checking may be performed on a periodic or random basis by departmental or City IT or its delegates. Any passwords found out during one of these scans will require the user to change it.

5. **Implementation**

5.1 Passwords for End Users.

5.1.1 New End Users will be given an initial temporary password as part of the Network Access procedure. They will then immediately change this temporary password to one of their own.

5.1.2 If an End User forgets his/her password, the Network Logon Procedure will prompt them for the steps to reset their password.

5.2 Dissemination of Password Policy

5.2.1 All new users to the City's computing network will be notified of this City policy prior to their gaining use of the system.

5.2.2 An **Electronic Password Policy Acceptance Statement** form [see Attachment A] must be signed by the new users and retained by their Agency/Department prior to submission of the request for service.

5.2.3 Each existing user of the City's computing network will be notified and provided access to a copy of this policy upon any change in the policy.

5.2.4 Subsequent reminders on and updates to this policy will be periodically transmitted via the system to all City computing network users.

6. Violations and Enforcement

6.1 Violations of the City's Password Policy will be evaluated on a case-by-case basis by the End User's Executive Director. Violation of this policy may result in disciplinary action, up to and including dismissal, and may include referral of a case to appropriate authorities for civil or criminal prosecution.

6.2 Users may be subject to random internal audits of password use.

7. Electronic Password User Responsibility

7.1 Each individual with access to the City's computing network is responsible for understanding and following this policy.

7.1.1 All such users must sign a statement acknowledging that they have been provided with a copy of the City's Electronic Password Policy and agree to abide by it as a condition of being provided such access.

7.1.2 Unauthorized or improper use of the City's computing network may result in terminating the individual's Network access, and depending on the severity of the circumstances may result in disciplinary action, including termination.

Electronic Password Policy
Acceptance Statement

Acceptance

Your signature below certifies that you have read the City's Electronic Password Policy and that you understand, accept and will abide by the provisions stated in it, or in the Policy as revised and distributed from time to time.

Signature of end user _____

Name (print) _____

Date _____

Agency/Department _____

Phone _____

Mail Station or Address _____

Note: The user's Agency/Department keeps one signed copy of this form on file.