Administrative Regulations

Number AR 8-29
Issue 1

Subject: Network Password Policy

I. Purpose

The purpose of this policy is to ensure a secure computer network by establishing standards for the creation of strong passwords, the protection of those passwords and the frequency of changes to passwords. A poorly chosen password may compromise the City's entire information technology network. This could result in the loss of sensitive data or network downtime.

II. Scope

This regulation is applicable to all City personnel (including contractors and vendors) under the direction of the City Manager, who are responsible for an account with access to the City's network.

III. Policy

All accounts on the City's network shall automatically be prompted to change their passwords every 90 days. Prompts shall occur upon logging onto the network. Passwords must have a minimum of 8 characters. All network passwords shall conform to the guidelines described below. These guidelines are based on federal and state standards. Violation of this policy will result in disciplinary action.

IV. General Guidelines for the Creation of Strong Passwords

All passwords must: contain 3 of the following 4 character sets:

1. Upper case letters
2. Lower case letters
3. Numbers
4. Special characters or symbols (i.e., @,-,#,+,&)

Other strong password guidelines include:

- Password should not be a *singular* word in any language, slang, dialect, jargon, or common usage

- Password should not include the terms "longbeach" or any other derivation

- Password should not be based on personal information, names of family, etc.

- Password should be updated every 90 days. Fourteen (14) days before the password is due to expire Active Directory will display a dialog box reminding the user to change the password

One way to create strong passwords that is relatively easy to remember is to base the password on a multiword song title, affirmation, or phrase. For example, the password might be “8-Day$aweek”. Longer passwords or pass-phrases are more secure against standard network attacks. Solid pass-phrases contain a combination of upper and lowercase letters, as well as numeric and punctuation characters.

A strategy for remembering the password when changes are required every 90 days is to develop a strong password, and use a number or letter sequence at the end of this root password. For example “8-Day$aweek1, 8-Day$aweek2, 8-Day$aweek3, etc.” Passwords published as the examples above are not to be used.

V. Password Protection Standards

The standards discussed here were developed using Federal and State government guidelines.

City personnel shall not share passwords with anyone, including administrative assistants, supervisors, or family members. Personnel shall not reveal passwords in email messages or save passwords on files in any computer system. All passwords are to be treated as confidential City information.

City personnel shall not use the "Remember Password" feature included in some applications (e.g., Eudora, Outlook, Netscape Messenger).

City personnel should not use the same password for City accounts and other non-City accounts (e.g., personal email account, online banking, benefits, etc.). Where possible, City personnel should not use the same password for various City access needs. In addition, an employee’s user name and password should not be the same.

After four bad attempts at using a password, users will be locked out of the network and will be required to call the Help Desk (x86100).

Any person requesting a password shall be referred to this document or to the Technology Services Department (TSD) Help Desk at x86100. If it is believed that an account or password has been compromised, the incident should be reported to the TSD Help Desk, where the password will be reset. Managers will be able to reset an employee's password at the Manager's discretion.

It is advised that City personnel lock their computer if the user is going to be away from the computer.

VI. Password Reset Policy

Callers to the TSD Help Desk who request password resets shall be required to provide a unique personal identifier.

TSD or its delegates shall perform password cracking or guessing on a periodic or random basis. If a password is guessed or cracked during one of these scans, the user shall be required to change it.