G. PASSWORD POLICY IMPLEMENTATION

PURPOSE

Passwords are an important part of the City of Redlands' efforts to protect its technology systems and information assets by ensuring that only approved individuals can access these systems and assets. Passwords are used for various purposes at the City. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and network equipment logins.

The City of Redlands recognizes, however, that passwords have limits as an access control. For some systems, other approved authentication methods that provide higher levels of assurance and accountability than passwords will be used.

The City of Redlands key systems continue to utilize passwords as the primary method for authentication and access control. This policy is designed to establish best practices for the composition, lifecycle and general usage of passwords.

POLICY

1. Policy Application

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 network, or stores any City information (excluding the Police Department network and systems). This policy applies to all City of Redlands employees that are considered users of the City's systems as defined in the Computer and Electronic Communications Policy.

2. Systems Covered

The following systems are covered in this policy:

- Windows Network (Microsoft Windows Active Directory) or systems that utilize Microsoft Windows Active Directory authentication and access control.
- Enterprise applications utilizing local authentication
  - Examples include enQuesta and BiTech.
- Systems that use Simple Network Management Protocol (SNMP)
  - Examples of such systems include: Microsoft Outlook, email Over the Web Access (OWA), user desktops, virtual private networks (VPN), Laserfiche, Cityworks, ArcGIS Online (including Collector, Survey123, and Workforce for ArcGIS), etc.
  - Passwords for other systems should also follow this policy whenever possible.

PROCEDURE

Everyone should be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:

- The password contains less than eight characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
  - Names of family, pets, friends, co-workers, fantasy characters, etc.
  - Computer terms and names, commands, sites, companies, hardware, software.
  - The words "City", "Redlands", "Department" or any derivation.
  - Birthdays and other personal information such as addresses and phone numbers.
  - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
  - Any of the above spelled backwards.
  - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9,!@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- Are at least eight alphanumeric characters long and is a passphrase (Ohmy1stubbedmyt0e).
- Is not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. 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.

NOTE: Do not use either of these examples as passwords.

Password Protection Standards

To provide authentication effectively, it is essential that a password be known to only the individual user, unless there are delegates to or sharers of accounts. Do not share City passwords with anyone. All passwords are to be treated as sensitive, Confidential City Information.

Password Construction Recommendations

- A strong password that meets the minimum construction rules will be rather complex. Here are some recommendations on creating a strong password:
  - Use uppercase letters in random places.
  - Misspell words.
  - Construct a password from the initial letters of a favorite quotation, song lyric, movie and so on, capitalizing some letters and substituting a number or special character in an appropriate place.

Password Change and Reuse

A user will be free to choose a new password at any time, but a user may not perform multiple changes in quick succession in order to enable continued use of a recently used password.

a. Password Change and Reuse Rules
   1. A user must change his or her password a minimum of every 365 days.
   2. It is recommended that a user change their password as frequently as time permits, i.e., quarterly, semi-annually, etc.
   3. A user may not change his or her password more than once in two (2) days.
   4. A user's password must be different from his or her previous four (4) passwords.
   5. A user's password may need to be updated after a change in devices or transfer to other departments.

The Password Policy can be found in the Personnel Roles and Regulations