C. PASSWORD POLICY

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.

However, 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 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 non-public City information (excluding the Police Department network and systems). This policy applies to all City of Redlands employees that are considered authorized users of the City's systems as defined in the Computer and Electronic Communications Policy. City Department of Innovation and Technology (DoIT) staff has specific additional responsibilities.

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.
- 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, etc.

Passwords for other systems should also follow this policy whenever possible.

Principles

- Password Confidentiality
  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. Users will ensure the confidentiality of their passwords at all times.
- Password Construction
  To provide system security, a password must meet minimum length and complexity requirements. Because of technology constraints, password construction rules may vary from one system to another, but they will meet (or exceed) these requirements wherever possible.

Long and complex passwords may be difficult for users to remember. Therefore this policy provides guidance to end users on how to construct a memorable password that meets (or exceeds) these requirements.

- Password Construction Rules

  A password must be made up of:
  - Eight (8) or more characters.
  - At least one uppercase letter.
  - At least one lowercase letter.
  - At least one number (0 through 9).
  - At least one special character ($, @. # and so on).

  A password should not contain:
  - Your first name or your last name.
  - Names of family members, friends, pets, co-workers, fantasy characters, etc.
  - Personal information about yourself or family members. This includes generic information that can be obtained about you very easily, such as birth date, phone number, vehicle license plate number, street name, apartment/house number, etc.
  - Computer terms and names, commands, sites, companies, hardware, or software.
  - Words that are in the dictionary or are a word in any language.
  - Words that are slang, dialect, jargon, etc.
  - Geographical names or places.
  - Letter or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
  - Any of the above spelled backwards.
  - Any of the above preceded or followed by a number (e.g., secret1,1 secret).

- 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

  To minimize the window of opportunity for misuse by someone who has discovered a user's password, users will be forced to change their passwords periodically.

  A user's new password will be completely different from any recently used password. Users must create a new password that has no more than three (3) characters in common with a previous password.

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.

- Password Change and Reuse Rules
  - A user must change his or her password a minimum of every 90 days.
  - A user may not change his or her password more than once in two (2) days.
  - A user's password must be different from his or her previous four (4) passwords.

- Password Entry
  A system will allow five (5) login attempts ("grace logins"). If the password is not correct on the last allowed attempt, then the user's account will be locked out for a 15-minute wait period before it can be accessed again. Typically, the Department of Innovation and Technology should be contacted to unlock the account unless there is a legitimate attempt to break in.

4. Authorized End Users' Responsibilities

If you are an authorized end user of the City of Redlands' software systems, you have the following responsibilities regarding the passwords you use.

Note that these responsibilities apply even if the system does not enforce any specified rules.

- You must keep your password confidential at all times.
- You should not disclose your password to anyone or talk about a password in front of others.
- You should not hint at the format of a password to anyone.
- You should not use a password that you use on any City of Redlands system on any external system (including Internet banking and social networking services).
- You should not write down your password.
- You should not reveal your password on questionnaires or security forms.
- You should not use the "remember password" feature in any Web browser.
- You should not send a password electronically.
- You should not use any "password keeper" or "password wallet" software or service.
- You must choose a password that meets or exceeds the length and complexity requirements set out in the Password Construction Recommendations.
- You must choose a password that meets or exceeds the other requirements set out in the Password Construction Recommendations.
- You must change your password at least every 90 days.
- You should not use any of your previous four (4) passwords.
- You must choose a new password that has no more than three (3) characters in common with your previous password.
- You should not change your password more than more than once in two (2) days.

- If an account or password is suspected to have been compromised, you must report the incident to the Department of Innovation and Technology and change all passwords.
- When away from your workstation, you should lock your screen. The Department of Innovation and Technology has implemented a screen lock policy which will lock your screen when idle for more than twenty minutes.

5. Department of Innovation and Technology (DoIT) Staff Responsibilities

The City of Redlands Department of Innovation and Technology or its delegates have the following responsibilities regarding passwords on City systems:

- User Password Management
  - When a user asks to reset his or her password, the user's claimed identity must be corroborated in line with approved departmental procedures.
  - A user's new password must not be disclosed to anyone other than the user himself or herself.
  - A user's new password must not be written down.
  - A new password must not be sent to a user electronically.
  - A user must not be asked to disclose his or her password.
- System-level Password Management

  System-level passwords must conform to the guidelines described below.
  - All system-level passwords (e.g., root, enable, admin, application administration accounts, etc.) must be changed annually.
  - All production system-level passwords must be part of the DoIT administered global password management database.
    - Where Simple Network Management Protocol is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).
    - As a part of the device security hardening process, all passwords must be changed from the default password.

6. Application/System Standards

Applications developed or purchased by the City should ensure their programs contain the following security standards. Applications should:

- Support authentication of individual users, not groups.
- Not store passwords in clear text or in any easily reversible form.
- Provide for some sort of role management, so that one user can take over the functions of another without having to know the other's password.
- Support Remote Authentication Dial In User Service (RADIUS), X.509 with Lightweight Directory Access Protocol (LDAP) security retrieval, and/or Active Directory integration wherever possible.