RANCHO MURIETA COMMUNITY SERVICES DISTRICT

Category:	Information Technology	**Policy #**2022-01
Title:	District Password Policy	

PURPOSE

The purpose of this policy is to establish a standard for the creation of strong computer and Internet related passwords, the protection of those passwords and the frequency of change.

BASIC POLICY AND OBJECTIVES

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

1.0 General Scope of Policy

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 Rancho Murieta Community Services District facility, has access to the Rancho Murieta Community Services District network and/or LEIN/NCIC network, or stores any non-public Rancho Murieta Community Services District LEIN-based Criminal Justice Information (CJI).

2.0 Guidelines for Password Construction

The following are password construction requirements to be used when creating a new password:

- Be a minimum length of eight (8) characters on all systems;
- Contain a mixture of capital and lowercase letters, numbers and special characters (if allowed)
- Not be the same as the User ID;
- Expire within a maximum of 180 calendar days;
- Not be identical to the previous twenty (20) passwords;
- Not be transmitted in the clear or plaintext outside the secure location;
- Not be displayed when entered;
- Ensure passwords are only reset for authorized user.

3.0 Password Deletion

All passwords that are no longer needed must be deleted or disabled immediately. This includes, but is not limited to, the following:

- When a user retires, quits, is reassigned, released, dismissed, etc.
- Default passwords shall be changed immediately on all equipment.

- Contractor accounts, when no longer needed to perform their duties.

4.0 Password Protection Standards

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

- Don't reveal a password over the phone to anyone, including your boss;
- Don't reveal a password in an email message;
- Don't talk about a password in front of others;
- Don't hint at the format of a password (e.g., "my family name");
- Don't reveal a password on questionnaires or security forms;
- Don't share a password with family members;
- Don't reveal a password to a co-worker while on vacation;
- Don't use the "Remember Password" feature of applications;
- Don't write passwords down and store them anywhere in your office;
- Don't store passwords in a file on ANY computer system unencrypted.

If an account or password is suspected to have been compromised, report the incident to the Director of Administration and change all passwords.

Password cracking or guessing may be performed on a periodic or random basis by the MSP/FBI or Rancho Murieta CSD. If a password is guessed or cracked during one of these scans, the user will be required to change it.

5.0 Application Development Standards

Application developers must ensure their programs contain the following security precautions:

- Should support authentication of individual users, not groups;
- Should not store passwords in clear text or in any easily reversible form;
- Should provide some sort of role management, such that one user can take over the function of another without having to know the other's password.

6.0 Remote Access Users

Remote access to the Rancho Murieta Community Services District networks is to be controlled by using either a Virtual Private Network and/or remote desktop (in which a password and user id are required) or a form of advanced authentication (two-factor or multi-factor authentication).

7.0 Penalties

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Approved by Rancho Murieta Community Services District Board of Directors	Updated 05/18/2022 Adopted 2/16/2022