RANCHO MURIETA COMMUNITY SERVICES DISTRICT

15160 Jackson Road, Rancho Murieta, CA 95683
Office - 916-354-3700 Fax – 916-354-2082

COMMUNICATION & TECHNOLOGY COMMITTEE

(Directors John Merchant and Linda Butler)

Regular Meeting
February 3, 2022 at 8:30 a.m.

This meeting will be held via ZOOM video conference only. You can join the conference by (1) logging on to https://us02web.zoom.us/j/85224103649, entering Meeting ID no. 852 2410 3649, and using the audio on your computer, or (2) dialing into 1-669-900-9128 and entering the meeting code 852 2410 3649. Those wishing to join with audio only can simply call the telephone number above and enter the code. Participants wishing to join the call anonymously have the option of dialing *67 from their phone. Please refer to your telephone service provider for specific instructions. ***PLEASE NOTE – MOBILE DEVICE USERS MAY NEED TO INSTALL AN APP PRIOR TO USE AND MAC AND PC DESKTOP AND LAPTOP USES WILL REQUIRE YOU TO RUN A ZOOM INSTALLER APPLICATION – PLEASE FOLLOW DIRECTIONS AS PROVIDED BY ZOOM. IT IS RECOMMENDED YOU ATTEMPT TO LOGIN AT LEAST 5 MINUTES BEFORE THE START OF THE MEETING.***

AGENDA

1. **Call to Order**

2. **Consider Finding That as a Result of the COVID-19 Emergency: (i) Meeting in Person Would Present Imminent Risks to the Health or Safety of Attendees; and (ii) the Meeting is Authorized to be Held by Teleconference Pursuant to Gov. Code, § 54953, subd. (e)(1)(C).**

3. **Comments from the Public**

4. **Monthly Website and Social Media Update**

5. **Review District Computer Password Policy**

6. **Discuss Reservoir Information and Education Ad Hoc Committee**

7. **Update on Website and FAQ's**

8. **Directors & Staff Comments/Suggestions**

9. Adjournment

"In accordance with California Government Code Section 54957.5, any writing or document that is a public record, relates to an open session agenda item and is distributed less than 24 hours prior to a special meeting, will be made available for public inspection in the District offices during normal business hours. If, however, the document is not distributed until the regular meeting to which it relates, then the document or writing will be made available to the public at the location of the meeting."

In compliance with the Americans with Disabilities Act if you are an individual with a disability and you need a disability-related modification or accommodation to participate in this meeting or need assistance to participate in this teleconference meeting, please contact the District Office at 916-354-3700 or awilder@rmcsd.com. Requests must be made as soon as possible.

Note: This agenda is posted pursuant to the provisions of the Government Code commencing at Section 54950. The date of this posting is January 27, 2022. Posting locations are: 1) District Office; 2) Post Office; 3) Rancho Murieta Association; 4) Murieta Village Association.

4 Website and Facebook - Pending

RANCHO MURIETA COMMUNITY SERVICES DISTRICT

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

PURPOSE

The purpose of this policy is to establish a standard for the creation of strong 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 password.

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 new password:

- Be a minimum length of eight (8) characters on all systems;
- Not be a dictionary word or proper name;
- Not be the same as the User ID;
- Expire within a maximum of 90 calendar days;
- Not be identical to the previous ten (10) 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 use your User ID as your password. 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;
- Don't reveal a password in an email message;
- Don't reveal a password to the boss;
- Don' 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	Adopted