DAN HAVERTY
Interim Fire Chief

Sacramento Metropolitan Fire District

10545 Armstrong Ave., Suite 200 • Mather, California 95655 • Phone (916) 859-4305• Fax (916) 859-3715

POLICY COMMITTEE – REGULAR MEETING
Thursday, February 9, 2023 – 5:30 PM

Sacramento Metropolitan Fire District
10545 Armstrong Avenue, Boardroom, 2nd Floor
Mather, California
&
Remotely Via Zoom
Phone: (669) 900-6833
Webinar ID: 891 1373 8517#
Passcode: 466 493 073#

CALL TO ORDER

PUBLIC OPPORTUNITY TO DISCUSS MATTERS OF PUBLIC INTEREST WITHIN COMMITTEE'S SCOPE INCLUDING ITEMS ON OR NOT ON AGENDA

CONSENT AGENDA

The Consent Agenda is acted upon with one motion unless a committee member requests separate discussion and/or action.

Page No.

1. **Action Summary Minutes** **2**
Recommendation: Approve the Action Summary Minutes for meeting of May 12, 2022.

ACTION ITEM

1. **Election of Officers** *(Clerk Penilla)* *
Recommendation: Elect a Chair and Vice Chair to the Policy Committee for 2023.

PRESENTATION ITEMS

1. **Password Policy** *(Mathew Roseberry, Information Technology Director)* **3**
Recommendation: Review the revised policy for informational purposes, no further action required.

NEXT MEETING DATE: TBD

ADJOURNMENT

Posted on February 6, 2023

Melissa Penilla

Melissa Penilla, Clerk of the Board
* No written report

Sacramento Metropolitan Fire District

10545 Armstrong Ave., Suite 200 • Mather, California 95655 • Phone (916) 859-4305• Fax (916) 859-3715

TODD HARMS
Fire Chief

ACTION SUMMARY MINUTES – REGULAR MEETING

POLICY COMMITTEE
THURSDAY, MAY 12, 2022
SACRAMENTO METROPOLITAN FIRE DISTRICT
Remotely Via Zoom

CALL TO ORDER

The meeting was called to order at 5:30 p.m. by Director Goold. Committee members present: Goold and Clark. Committee members absent: White. Staff present: Chief Harms and Board Clerk Penilla.

PUBLIC COMMENT: None

CONSENT AGENDA

Action: Moved by Clark, seconded by Goold, and carried unanimously by members present to adopt the Consent Calendar as follows:

1. **Action Summary Minutes**
   Recommendation: Approve the Action Summary Minutes for meeting of February 10, 2022.
   Action: Approved the Action Summary Minutes.

ACTION ITEMS

1. **Use of Force – Peace Officer Policy** *(Paul Tualla, Investigator)*
   Recommendation: Approve the revised Use of Force – Peace Officer Policy and refer to the full Board.
   Action: Moved by Clark, seconded by Goold, and carried unanimously by members present to refer the Use of Force – Peace Officer Policy to the full Board.

PRESENTATION ITEMS

1. **Complaints Standards and Procedures - Peace Officer Policy** *(Paul Tualla, Investigator)*
   Recommendation: Review the revised policy for informational purposes, no further action required.
   Action: No action taken.

ADJOURNMENT

The meeting adjourned at 5:45 p.m.

Director Goold, Chair

Melissa Penilla, Clerk of the Board

DAN HAVERTY
Interim Fire Chief

Sacramento Metropolitan Fire District

10545 Armstrong Ave., Suite 200 · Mather, CA 95655 · Phone (916) 859-4300 · Fax (916) 859-3702

DATE: February 9, 2023

TO: Policy Committee Members

SUBJECT: Administration Policy
Policy 13.003.01 – Password Policy

TOPIC

Review new Administration Policy 13.003.01 Password Policy.

DISCUSSION

Attached is the updated Password Policy 13.003.01 written by the Information Technology Division. The Password Policy was written due to current cybersecurity attacks and breaches. A password policy details required password complexity, how often passwords are updated and how passwords should be stored. The Password Policy is attached for your review.

RECOMMENDATION

Administration Policy review is for informational purposes only as previously directed by the Policy Committee.

Submitted By:

Mathew Roseberry
IT Director

Approved By:

Ty Bailey
Deputy Chief, Administration

Sacramento Metropolitan Fire District

ADMINISTRATION POLICY

POLICY TITLE: Password Policy OVERSIGHT: IT

POLICY NUMBER: 13.003.01 EFFECTIVE DATE: 11/19/21 REVIEW DATE: 02/09/23

Background

The Sacramento Metropolitan Fire District (District) requires that all individuals are responsible for safeguarding their system access login and password credentials and must comply with the password parameters and standards identified in this policy. Passwords must not be shared with or made available to anyone in any manner that is not consistent with this policy.

Purpose

Assigning unique user logins and requiring password protection is one of several primary safeguards employed to restrict access to the District's network and the data stored within it to only authorized users. If a password is compromised, access to information systems can be obtained by an unauthorized individual, either inadvertently or maliciously. Individuals are responsible for keeping passwords secure and confidential.

Scope

This policy applies to all data created, collected, stored, transported, or used by any District employee, contractor, annuitant, or vendor of the District.

.

Definitions

1. **Password Spraying:** A type of brute force attack. For example, an attacker will use one password (say Secure@123) against many different accounts on the application to avoid account lockouts that would normally occur when brute forcing a single account with many passwords.
2. **iOS Device:** Products that use Apple's iPhone operating system, including the iPhone, iPod touch and iPad.

Policy

Individual Responsibilities

1. Passwords must be changed immediately upon issuance for the first-use. Initial passwords must be securely transmitted to the individual.

2. Passwords must never be shared with another individual for any reason or in any manner not consistent with this policy. A shared or compromised District password is a reportable IT security incident.

3. Employees and contractors must never ask anyone else for their password. If you are asked to provide your password to an individual or sign into a system and

provide access to someone else under your login, you are obligated to report this to IT.

4. Passwords must never be written down and left in a location easily accessible or visible to others. This includes both paper and digital formats on untagged (unsupported) devices. Passwords may be stored in a secure password manager as long as the master password is kept private and meets the requirements in the Password Requirements section of this policy.

5. Individuals must never leave themselves logged into an application or system where someone else can unknowingly use their account.

    a. To access shared workstations (e.g., camera system, CAD display), IT will provide a limited-use shared account for the workstation.

    b. IT will never ask for a password. In IT support scenarios where an IT account cannot be used, an individual may allow a technician to utilize his/her computer under the individual's account even if the individual is unable to be present during the entire support session. The individual should not share his/her password with the technician.

    c. When IT services iOS devices, IT will ask the user to provide their passcode in order to perform the repair.

    d. iOS device Apple ID passwords are kept in an IT encrypted password manager. IT manages the passwords in order to service iOS devices.

    e. In the event that a password needs to be issued to a remote user or service provider, the password must be sent with proper safeguards (e.g., sent via encrypted email message).

    f. If a password needs to be shared for servicing, IT should be contacted for authorization and appropriate instruction.

    g. Passwords for the District must be unique and different from passwords used for other personal services (e.g., banking).

    h. Passwords must meet the requirements outlined in this policy.

    i. Passwords must be changed at the regularly scheduled time interval (as defined in Password Expiration where applicable) or upon suspicion or confirmation of a compromise.

    j. Individuals with access to service accounts or test accounts must ensure the account password complies with this policy and must keep the password stored in a secure password manager.

    k. In the event a breach or compromise is suspected, the incident must be reported to IT immediately.

Responsibilities of Systems Processing Passwords

1. Passwords must be prohibited from being displayed when entered.

2. Passwords must never be stored in clear, readable format (encryption must always be used).

3. Passwords must never be stored as part of a login script, program, or automated process.

4. Systems storing or providing access to confidential data or remote access to the internal network must be secured with multifactor authentication.

5. Password hashes (irreversible encoded values) must never be accessible to unauthorized individuals.

6. Where possible, salted hashes (irreversible encoded values with added randomness) should be used for password encryption.

Procedures

Password Requirements

The following parameters indicate the minimum requirements for passwords for all individual accounts (except for passcodes defined in Mobile Devices).

1. At least twelve (12) characters (unless the application will not allow 12 characters);

2. At least one(1) uppercase character, one(1) lowercase character, and one(1) number or one(1) special character.

3. Not based on anything somebody else could easily guess or obtain using person-related information (e.g., names, employee ID, badge number, telephone numbers, dates of birth, etc.); and

4. Not vulnerable to a dictionary attack (see Recommendations for Creating Compliant Password).

5. Do not use the word Metro within your password or passphrase.

6. Cannot be an increment of your previous password (Password1, Password2, etc.)

Password Expiration

IT reserves the right to reset a user's password in the event a compromise is suspected, reported, or confirmed. This helps prevent an attacker from making use of a password that may have been discovered or otherwise disclosed.

Standard Users

Standard users consist of District employees (including temps and consultants) that are not system administrators.

1. Passwords are required to be changed every 365 days.
2. Passwords must not be reused for at least three (3) generations.
3. Passwords must comply with the criteria in section Password Requirements

Privileged Users

Privileged users consist of users with elevated access to administer information systems and applications (other than to a local device), most often in the Information Technology Division. Such users have administrator access via a shared account or to multiple systems at the District and these accounts are at a higher risk for compromise.

1. Passwords are required to be changed every 365 days.
2. Passwords must not be reused for at least three (3) generations.
3. Passwords must comply with the criteria in section Password Requirements.

Service Accounts

Service accounts are accounts used by a system, task, process, or integration for a specific purpose.

1. Passwords are required to be changed if compromised.
2. Passwords should be stored in the IT Password Manager system.
3. Passwords must comply with the criteria in section Password Requirements.

Test Accounts

Test accounts are accounts used on a temporary basis to imitate a role, person, or training session.

1. Passwords are required to be changed every 180 days.
2. Passwords must not be reused for at least three (3) generations
3. Passwords should be stored in the IT Password Manager.
4. Passwords must comply with the criteria in section Password Requirements.

Local Admin Accounts

Local Admin accounts are used to manage a local computer or local server.

1. Passwords are required to be changed if compromised.
2. Passwords should be stored in the IT Password Manager.
3. Passwords must comply with the criteria in section Password Requirements.

4. Passwords must be changed when IT staff leave the IT division.

Account Lockout

In order to limit attempts at guessing passwords or compromising accounts, an account lockout policy is in effect for all systems. Account lockout thresholds and durations vary based on the type of user, as defined below.

Standard Users

1. Accounts will lockout after five (5) invalid password attempts in fifteen minutes.
2. Accounts will remain locked for a duration of fifteen (15) minutes, unless the IT helpdesk is contacted and the user's identity is verified in order for the account to be unlocked sooner.

Privileged Users

1. Accounts will lockout after five (5) invalid password attempts in fifteen minutes.
2. Accounts will remain locked for a duration of fifteen (15) minutes, unless the IT helpdesk is contacted and the user's identity is verified in order for the account to be unlocked sooner.

Test Accounts

1. Accounts will lockout after five (5) invalid password attempts in fifteen minutes.
2. Accounts will remain locked for a duration of fifteen (15) minutes, unless the IT helpdesk is contacted and the user's identity is verified in order for the account to be unlocked sooner.

Mobile Devices

Mobile devices accessing or storing District data, such as smartphones and tablets, issued by IT shall be managed by the mobile device management (MDM) platform. The following minimum password policy is in effect for all mobile devices, where passwords are:

1. At least four (4) digits.
2. No repeating or sequential digits (e.g., 111, 123456, 101010).

Biometric authentication (e.g., facial or fingerprint recognition) on mobile device may be used to unlock the device, but a compliant password must still be established.

The device manufacture may automatically impose time limitations after several unsuccessful password attempts before a wipe is triggered. IT can provide assistance in resetting device passwords.

Recommendations for Creating Compliant Passwords

Passphrase

A passphrase is similar to a password, but it is generally longer and contains a sequence of words or other text to make the passphrase more memorable. A longer passphrase that is combined with a variety of character types is exponentially harder to breach than a shorter password. However, it is important to note that passphrases that are based on commonly referenced quotes, lyrics, or other sayings are easily guessable. While passphrases should not be famous quotes or phrases, they should also not be unique to you as this may make them more susceptible to compromise or password-guessing attacks.

1. Choose a sentence, phrase, or a series of random, disjointed, and unrelated words.
2. Use a phrase that is easy to remember.
3. Examples:
   a. Password: When I was 5, I learned to ride a bike.
   b. Password: Fetch 1 unsubtly unspoken h@unt unopposed
   c. Password: stack3 process overbid Press#
   d. Password: Agil3 Stash Perpetual Creatable!

Use a Secret Code

A secret code can be used in conjunction with the previous methods simply by substituting letters for other numbers or symbols. Combining these methods will make it easy to incorporate the four character types in order to meet the password complexity requirements.

1. Use a phrase that is easy to remember.
2. Capitalize the first letter of every word.
3. Substitute letters for numbers or symbols.
4. Incorporate spaces or substitute with a different character.
5. Example:
   a. Phrase: "When I was five, I learned how to ride a bike."
   b. Password: WhenIwa$5,Ilh0wt0rab1k3.

Password Reset Options

Various options are available to assist users with changing a forgotten or expired password.

1. Contact IT and provide your employee PIN number.

2. Stop by the IT helpdesk at HQ.

3. Use the “forgot password” feature from the application, if applicable.

Reporting a Suspended Compromise, Security Incident, or Breach

1. If you believe your password has been compromised or if you have been asked to provide your password to another individual, including IT, promptly notify the IT helpdesk.

Password Verification and Validation

1. IT will perform random password spraying to determine if user passwords have been stolen, are on common password lists, or are not meeting the requirements within this policy.

2. If IT determines a user's password has been stolen, is on a common password list, or does not meet the requirements within this policy, IT will contact the user to reset their password. The user will have up to 96 hours to reset their password or they will be locked out of the application or system.