



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 10, 2022 – 5:15 PM

Remotely Via Zoom
Phone: (669) 900-6833
Webinar ID: 819 1376 4093#
Passcode: 458 167 716#

COMMITTEE MEMBERS

Director Grant Goid
Director D'Elman Clark
Director Walt White
Director Jennifer Sheetz - Alternate

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
Recommendation: Approve the Action Summary Minutes for meeting of November 9, 2021. | 3 |

ACTION ITEMS

- | | |
|--|---|
| 1. Election of Officers (<i>Clerk Penilla</i>)
Recommendation: Elect a Chair and Vice Chair to the Policy Committee for 2022. | * |
| 2. Capital Improvement Program Policy (<i>Dave O'Toole, Chief Financial Officer</i>)
Recommendation: Approve the new Capital Improvement Program Policy and corresponding updates to the Reserve Funding and Capital Asset Policies, and refer to the full Board. | 4 |

PRESENTATION ITEM

- | | |
|---|----|
| 1. Data Security Policy (<i>Mat Roseberry, Director of IT</i>)
Recommendation: Review the newly created policy for informational purposes, no further action required. | 22 |
| 2. Password Policy (<i>Mat Roseberry, Director of IT</i>)
Recommendation: Review the newly created policy for informational purposes, no further action required. | 28 |
| 3. Electronic Mail Policy (<i>Mat Roseberry, Director of IT</i>)
Recommendation: Review the newly created policy for informational purposes, no further action required. | 36 |
| 4. Cell Phone Policy (<i>Mat Roseberry, Director of IT</i>)
Recommendation: Review the newly created policy for informational purposes, no further action required. | 40 |



Sacramento Metropolitan Fire District

10545 Armstrong Ave., Suite 200 · Mather, California 95655 · Phone (916) 859-4300 · Fax (916) 859-3700

POLICY COMMITTEE AGENDA

THURSDAY, FEBRUARY 10, 2022

5. **Employee Personal Electronic Device Policy** (*Mat Roseberry, Director of IT*) **44**
Recommendation: Review the newly created policy for informational purposes, no further action required.

NEXT MEETING DATE: TBD

ADJOURNMENT

Posted on February 7, 2022

Melissa Penilla

Melissa Penilla, Clerk of the Board

* No written report



TODD HARMS
Fire Chief

Sacramento Metropolitan Fire District

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

ACTION SUMMARY MINUTES – REGULAR MEETING

POLICY COMMITTEE

TUESDAY, November 9, 2021 – 5:30 P.M.

SACRAMENTO METROPOLITAN FIRE DISTRICT

Held at the following locations:

10545 Armstrong Avenue – Board Room

Mather, California

&

Remotely Via Zoom

CALL TO ORDER

The meeting was called to order at 5:30 p.m. by Director Goold. Committee members present: Goold, Clark, and White. Committee members absent: None. Staff present: Chief Harms and Interim Clerk Dehoney.

PUBLIC COMMENT: None.

CONSENT AGENDA

Action: Moved by Clark, seconded by White, 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 October 14, 2021.

Action: Approved the Action Summary Minutes.

PRESENTATION ITEMS

1. **Data Security Policy** (*Mat Roseberry, Director of IT*) 4

Recommendation: Approve the newly created policy for informational purposes, no further action required.

Action: No action taken.

2. **Password Policy** (*Mat Roseberry, Director of IT*) 8

Recommendation: Approve the newly created policy for informational purposes, no further action required.

Action: No action taken.

ADJOURNMENT

The meeting adjourned at 5:41 p.m.

Grant Gold, Chair

Michelle Dehoney, Interim Clerk of the Board



Sacramento Metropolitan Fire District

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

TODD HARMS
Fire Chief

DATE: February 10, 2022
TO: Policy Committee
SUBJECT: Capital Improvement Program Policy

TOPIC

Establish a Capital Improvement Program Policy and make corresponding changes to the Reserve Funding Policy and Capital Asset Policy.

DISCUSSION

Staff recommends adoption of a Capital Improvement Program (CIP) Policy which will organize, facilitate, and memorialize capital needs and goals in order to efficiently and transparently develop and support the physical infrastructure of the District. Rigorous and methodical evaluation of facility, apparatus, and equipment needs and financing options will ensure that existing and future capital needs are met, in compliance with the District's strategic plan and financial resources.

The CIP Policy defines a capital improvement project as any expenditure for facilities, improvements, apparatus, or equipment with a cost greater than \$50,000 and an expected useful life of at least one year, and provides other related definitions of funds.

The CIP will be updated annually and presented for the board to consider alongside the preliminary budget. The CIP will include a five-year forecast, incorporating known costs of planned capital projects over that period. The submittal process and criteria are explained in the policy, as well as the review process for submitted projects. Finally, the contents of the annual CIP are identified and defined.

The CIP Policy establishes procedures and definitions that require corresponding modifications to the Capital Asset Policy and Reserve Funding Policy. The changes to the capital asset policy link the capital asset policy to the CIP policy by ensuring that the capital asset schedule of intended purchases for the fiscal year includes the CIP, and documents that the CIP is part of the budget process.

The Reserve Funding Policy changes include corresponding modifications to definitions where capital projects are addressed, to include "apparatus, equipment, and the construction, rehabilitation, and improvements to District facilities and properties." Additionally, the changes to definitions clarify the reserve fund source and how development impact fee revenues may be used.

FISCAL IMPACT

There is no fiscal impact associated with the establishment of a Capital Improvement Program, however the establishment of such policy is expected to improve clarity and planning for the capital elements of the District's annual budget process.

RECOMMENDATION

Staff recommends that the Policy Committee approve the Capital Improvement Program Policy and corresponding updates to the Reserve Funding Policy and Capital Asset Policy, and refer to the full Board.

Submitted By:

Approved By:



Dave O'Toole
Chief Financial Officer

Todd Harms
Fire Chief

Sacramento Metropolitan Fire District

BOARD POLICY

POLICY TITLE: Capital Improvement Program Policy OVERSIGHT: Administration
POLICY NUMBER: TBD EFFECTIVE DATE: TBD REVIEW DATE: TBD

Background

The Sacramento Metropolitan Fire District's (District) Capital Improvement Program (CIP) organizes, facilitates, and memorializes capital needs and goals in order to efficiently and transparently develop and support the physical infrastructure of the District. Rigorous and methodical evaluation of facility, apparatus, and equipment needs and financing options will ensure that existing and future capital needs are met, in compliance with the District's strategic plan and financial resources.

Purpose

This policy defines the process to identify and plan for funding of capital projects in order to ensure timely acquisition and replacement of needed capital assets, improvements, and facilities.

Scope

This policy is applicable to all District personnel involved in planning for the District's capital needs.

Definitions

- 1. Capital Project:** Any expenditure for facilities, improvements, apparatus, or equipment with a cost greater than \$50,000 and an expected useful life of at least one year. These projects include apparatus and equipment acquisition and replacement; improvements to District facilities; and the construction or rehabilitation of District properties and facilities including feasibility studies, land acquisition, architecture and engineering, and other associated planning costs.
- 2. Capital Facilities Fund:** A separate accounting for budgeting and reporting purposes used to track expenditures for capital outlay not associated with new development.
- 3. Capital Improvement Program (CIP):** A multi-year program and plan that identifies capital projects necessary for the implementation of the District's various long-range plans including the Standards of Cover, Growth Plan, Facility Condition Assessment, and Apparatus and Equipment Replacement Schedule. The CIP includes a five-year projection, including a one-year funding recommendation, and financing options.
- 4. Development Impact Fee CIP Reserves:** Reserves accumulated for the purchase of infrastructure to support new or expanding development. These reserves include funding from Development Impact Fees and General Fund transfers.
- 5. General Fund:** For budgeting and reporting purposes, Metro Fire records all

transactions in the General Fund that are not specifically accounted for in any other fund. The other funds include the Capital Facilities Fund, the Leased Properties Fund, the Grant Fund, the Development Impact Fees Fund, and the Intergovernmental Transfer (IGT) Fund.

6. **Grant Fund:** For budgeting and reporting purposes, Metro Fire records all grant related revenue and expenditures in the Grant Fund, in accordance with Federal grant rules and regulations.
7. **Leased Properties Fund:** For budgeting and reporting purposes, Metro Fire records all transactions for real property owned by the District but leased to other entities in the Leased Properties Fund.

Policy

It is the policy of the District to prepare a Capital Improvement Program (CIP) that outlines capital needs of the District that:

- Are responsive to the changing needs of the District.
- Demonstrate excellence in quality and value.
- Enable District staff to carry out their duties in an efficient and customer-focused manner.
- Provide a healthy, safe, secure, productive, and equitable environment for our employees in order to promote efficient service delivery.

The CIP incorporates and is consistent with District master plans, Board of Directors goals, and other long-range plans of the District. Capital projects may be funded from capital improvement funds, development impact fees, grant funding, or debt financing, with operational costs funded by the General Fund.

Since capital projects may span multiple fiscal years, the CIP details anticipated annual capital expenditures for a five-year period. This allows the District's Board of Directors to regularly revisit the plan and project progress, and better anticipate future needs.

The CIP is updated annually, and a one-year CIP budget is included in the District's annual budget. The remaining four years of the five-year CIP provide a look-ahead of capital projects, including anticipated costs and funding sources. The recommendation to incur new indebtedness may be included in the annual CIP budget, and requires approval by the Board of Directors.

Procedures

1. PLAN DEVELOPMENT

The development of the CIP is a coordinated effort across the District, with the capital project planning process overseen by the Planning and Development Division and the finance and budget process elements overseen by the Finance Division. Plan development includes the following:

- Divisions submit capital project requests by submitting Capital Project Initiation Forms to the CIP administrator in the Planning and Development Division.

- Capital Project Initiation Forms document the project description, timeline, procurement type, funding amount, funding source, impact on operations, any relevant ties to other projects, project justification, and related supporting information.
- The CIP administrator compiles all submitted requests and works with the Finance Division to package the requests into the draft CIP.

2. CAPITAL PROJECT EVALUATION AND PRIORITIZATION

Capital project requests will be evaluated and prioritized as follows:

- The CIP Committee (Committee), made up of representatives from the Finance, Planning and Development, and Purchasing divisions, reviews all proposed capital projects submitted for the upcoming fiscal year.
- The Committee determines whether or not the District has the capacity to complete all or a portion of each proposed project within the upcoming fiscal year; whether or not each proposed project is ready for execution in the upcoming fiscal year; and determines a ranking for each proposed project according to the District's goals and objectives.
- Primary evaluation criteria for capital projects includes alignment with strategic plans, statutory and regulatory considerations, and impact on service delivery.
- Other considerations may include impact on operating costs, secondary financial impacts, management and oversight implications, and impact on constituents and stakeholders.
- After evaluation, the CIP Committee submits a proposed CIP, including a one-year CIP budget, to the Fire Chief for consideration in conjunction with the preliminary budget review process.

3. PLAN ADOPTION AND CIP BUDGET APPROVAL

- The proposed CIP is reviewed annually by the Fire Chief, Deputy Chiefs, and Chief Financial Officer as part of the preliminary budget review process.
- The Fire Chief may recommend to fund, partially fund, or not fund any given project based the criteria and considerations outlined in Section 2.
- Upon review, the CIP, including the one-year CIP budget, is presented to the Board of Directors for adoption on or before June 30 concurrent with the preliminary budget approval process.
- The CIP budget is reviewed annually and projects that span multiple fiscal years must be submitted for each year that funding is requested.
- Once the CIP budget is approved by the Board, budgeted funds are restricted for their intended use.

4. ORGANIZATION OF THE CIP DOCUMENT

The CIP document is organized by the following sections:

- Introduction – Provides the Fire Chief's transmittal letter and District's organizational profile.
- CIP Overview and Summary– Provides the purpose and background of the CIP, describes the CIP planning and development process, summarizes the five-year capital needs, and outlines year-one capital projects.

- Financing Plan – Provides the capital budget overview and revenue assumptions, summary displays by project type and revenue source, debt service schedule, and operating and maintenance costs by spending category.
- Capital Project Details by Priority and Type – Provides the high priority project details, and shows projects by type (property acquisition, new construction, facility remodel/expansions, facility maintenance/repair, apparatus and equipment replacement, other miscellaneous projects).
- Appendices – Provides additional information to understand the CIP, including the budget calendar, glossary and acronyms list, Board resolutions, and capital project list index.

References

1. Sacramento Metropolitan Fire District, Reserve Funding Policy 01.008.02, revised as of April 22, 2021
2. Sacramento Metropolitan Fire District, Capital Asset Policy 01.015.02, revised as of December 14, 2017
3. Sacramento Metropolitan Fire District, Purchasing and Contracting Policy, 01.010.02, revised as of June 12, 2014
4. City of Thousand Oaks, Capital Improvement Program Policy, 14.006, revised as of November 6, 2017
5. Government Finance Officers Association of United States and Canada, Best Practice for Capital Budget Presentation. (<https://www.gfoa.org/materials/capital-budget-presentation>)
6. Government Finance Officers Association of United States and Canada, Best Practice for Capital Planning Policies (<https://www.gfoa.org/materials/capital-planning-policies>)

Sacramento Metropolitan Fire District

BOARD POLICY

POLICY TITLE: Capital Asset Policy

OVERSIGHT: Finance

POLICY NUMBER: 01.015.02 EFFECTIVE DATE: 07/07/99 REVIEW DATE: 12/14/17

Background

The objective of the Capital Asset system is to provide a tool for controlling property acquisition, availability, and disposal.

Purpose

Define procedures concerning the acquisition, inventory, disposal, and tracking of Capital Assets and Non-Capital Inventoried Equipment.

Scope

This policy is applicable to all Sacramento Metropolitan Fire District (District) personnel involved in the acquisition, inventory, disposal, and/or accounting of Capital Assets and Non-Capital Inventoried Equipment.

Definitions

1. **Capital Assets:** Capital Assets are assets with an individual cost of \$5,000 or more and a useful life of at least one year. Capital Assets include Land, Buildings, Equipment, and other related improvements.
2. **Land and Land Improvements:** Land consists of all parcels acquired by purchase or donation. Land includes all infrastructure, with the exception of roadbeds, easements, and rights-of-way, regardless of the cost. Land Improvements are permanent improvements to land that have a limited useful life (e.g., fences, parking lots, retaining walls, sidewalks).
3. **Buildings:** Buildings are permanent structures and other related improvements placed onto District owned or leased land. Building alterations are considered Capital Assets when they increase the value or life of the building.
4. **Equipment:** Equipment is moveable personal property of a relatively permanent nature and of significant value. Relatively permanent nature should be interpreted as having an expected useful life of at least one year, and significant value should be interpreted as a unit cost of at least \$5,000.
5. **Non-Capital Inventoried Equipment:** Non-Capital Inventoried Equipment is equipment tracked for inventory purposes but not capitalized for accounting purposes, including:
 - a. All firearms with a cost less than \$5,000.
 - b. All electronic equipment including, but not limited to cameras, computer hardware, photocopiers, fax machines, video or projection equipment,

recording or transcribing machines, and two-way radios, with a cost of at least \$1,000 but less than \$5,000.

6. **Capitalizable Cost:** The cost or, if acquired by donation, the appraised value or estimated fair market value on the date received. It also includes all ancillary charges to place the asset into its intended location and condition for use.

Policy

It is the policy of the District that a Capital Asset accounting system be established, implemented and maintained which will provide:

1. Guidelines for the accountability and financial and physical control of all District assets; and
2. Consistent and uniform procedures and transactions for accounting of Capital Assets throughout the District; and
3. Compliance with the requirements of the Code of Federal Regulations and any other funding entity requirements for grant-funded purchases.

Procedures

1. ACCOUNTING FOR CAPITAL ASSETS
 - a. For Land, the Capitalizable Cost includes the purchase cost or the appraised value on the date of the donation as well as land preparation costs (excavation, grading, etc.) that will have an indefinite useful life.
 - b. For Buildings, the Capitalizable Cost includes the cost or project cost, or, if acquired by donation, the appraised value of all buildings, permanent structures, and monuments. It also includes the cost of fixtures attached to and forming a permanent part of buildings and improvements.
 - c. The Capitalizable Cost of Equipment includes the purchase price less discounts received; freight charges; sales, use and transportation taxes; and installation charges. If acquired by donation, the cost capitalized shall be the appraised value or estimated fair market value at the date of donation.
 - d. Capital Leases include all arrangements to lease Land, Buildings, or Equipment with the District intending to assume ownership rights when the lease is paid off. If a purchase would normally meet the Capital Asset criteria, as stated above, it will be accounted for as a Capital Asset regardless of the financing method used.
 - e. Construction in progress is the cost of construction work undertaken but not yet completed. Finalized costs on completed construction projects, including vehicle and apparatus purchases, will be capitalized to the appropriate Capital Asset account.

- f. Maintenance and repairs are expenditures which neither materially add to the value of property nor appreciably prolong its life, but merely keep it in an ordinary efficient operating condition. Maintenance and repair costs shall not be capitalized.
- g. Improvements are expenditures that materially add to the value of the property or equipment by increasing their utility (through increased capacity or serviceability) or appreciably extend the total estimated useful life. The cost of capitalized expenditures should be added to the book value of the asset where the original cost of a component being improved can be specifically identified.
- h. Additions are new and separate units, or extensions of existing units, and are considered to be Capital Assets.

2. INVENTORY

- a. All Equipment and Non-Capital Inventoried Equipment must be tagged with an assigned, unique control number for tracking purposes.
- b. The District shall complete a physical inventory of all Capital Assets and Non-Capital Inventoried Equipment biennially, and when deemed necessary due to special circumstances.
- c. All Equipment purchased with grant funds must also be tagged with grant identification and must be inventoried according to Code of Federal Regulations or other funding entity requirements.

3. BOARD OF DIRECTORS APPROVAL

- a. A Capital Asset schedule of intended purchases for the fiscal year, including those included in the Capital Improvement Program (CIP), shall be submitted with the Preliminary Budget. The Capital Asset schedule shall include the description of the asset/project, the amount required for the purchase, and the budget account to be expended.
- b. Obligations for Capital Assets are not deemed appropriated until the adoption of the Preliminary Budget by the Board of Directors. Any subsequent changes to the Capital Asset schedule can be submitted in the Final Budget, Mid-year Budget, CIP development process, or through adoption of a separate budget amendment.

4. DISPOSAL OF CAPITAL ASSETS

- a. District division managers are authorized to declare Capital Assets within their division as surplus or non-serviceable property.
 - I. For grant-funded Equipment, prior approval to begin the disposal process must be received from the funding agency.
- b. Upon making such a declaration, the District division manager shall establish a current market value for each Capital Asset declared surplus or non-serviceable and forward that information to the Finance Division. The

Finance Division shall evaluate the information provided by the division manager, make modifications where deemed appropriate, and compile the information in detail for presentation by the division manager.

- c. The division manager shall prepare the staff report to the Board of Directors in the approved format. Detail presented to the Board of Directors shall include: inventory number, description, reason for recommendation, market value, historical cost, and recommended method of disposal (e.g., district surplus sale, donation, County of Sacramento surplus sale).
- d. The Board of Directors shall adopt a resolution authorizing the retirement of the Capital Asset declared surplus or non-serviceable before staff may dispose of the item.
- e. The division manager will arrange for disposal of Capital Assets declared surplus or non-serviceable as determined under this policy.
- f. Removal from District's Capital Asset records shall occur according to the following guidelines:
 - I. After appropriate Board of Directors' action to declare surplus, all Land, Land Improvements, and Buildings shall be removed from District Capital Asset records when sold or disposed of by other means.
 - II. After appropriate Board of Directors' action to declare surplus, all Equipment shall be removed from District Capital Asset records when declared surplus.

4. **Bondholders:** Investors who lend money to the bond issuer in return for interest and future repayment.
5. **California Employer's Retiree Benefit Trust (CERBT):** CERBT is Metro Fire's trust fund managed by the California Public Employees' Retirement System (CalPERS).
 - a. CalPERS maintains a separate trust fund to benefit Metro Fire retirees. CERBT is accumulating and investing funds for post-retirement medical premiums.
 - b. Amounts cannot be removed from CERBT except to pay retiree premiums.
 - c. CERBT is a separate legal entity. As such, CERBT assets are only disclosed in Metro Fire's audited financial statements, and not included in Metro Fire's Governmental Fund balance sheet assets.
7. **Capital Facilities Fund:** A separate accounting for budgeting and reporting purposes used to track expenditures for capital outlay not associated with new development.
8. **Capital Improvement Program (CIP):** A multi-year plan that identifies needed capital projects and equipment, provides a planning schedule, and financing options.
9. **CIP Reserves:** Reserves accumulated for the purchase of new apparatus, equipment, and the construction, rehabilitation, and improvements to District facilities and properties infrastructure. Funding is from Development Impact Fees and General Fund transfers. These reserves are comprised of the reserves from both the Capital Facilities Fund and the Development Impact Fees Fund.
10. **Capital Replacement Reserves:** Reserves accumulated to fund assets including replacement of existing infrastructure apparatus, equipment, and the construction, rehabilitation, and improvements to District facilities and properties when the asset's useful life has ended. This is accounted for in the Capital Facilities Fund.
11. **Committed Fund Balance:** A classification of Fund Balance. Committed Fund Balance amounts can only be used for specific purposes as determined by a formal action of the Metro Fire Board of Directors.
12. **Debt Service Reserves:** Money generally from bond proceeds that is set aside for additional security to bBondholders. This is a rRestricted rReserve and documentation of the requirement is in the bBond indenture.
13. **Development Impact Fee:** A fee charged by Metro Fire to mitigate the costs associated with property acquisitions, site preparation, design, construction, and equipping of fire stations that will serve new or expanding development within Metro Fire's service areas. This fee serves to protect the health and safety of the general public and preserve lives and property, and is authorized by California Government Code Section 66000 et seq.

14. **Development Impact Fees Fund:** A separate accounting for budgeting and reporting purposes used to track Development Impact Fee collection and spending. The reserves in this fund are used for new capital needed to serve new or expanding development.
15. **Dry Period Funding:** Dry period funding is a borrowing from the County of Sacramento. Dry Period Funding is automatically activated should Metro Fire have a negative cash position from July through the last Monday in April. The County Treasurer will cover Metro Fire's negative cash up to 85% of anticipated tax collections. Metro Fire must have positive cash balances from the last Monday in April until fiscal year end.
16. **Fund Balance:** Governmental Fund balance sheet assets less liabilities, equals **fFund bBalance**. Accountants distinguish up to five separate categories of **fFund bBalance**, based on the extent to which the government is bound to honor specific purposes spending constraints.

These five categories are: Non-spendable Fund Balance, Restricted Fund Balance, Committed Fund Balance, Assigned Fund Balance, and Unassigned Fund Balance (all separately defined herein).
17. **Funding Policy Contribution (FPC):** A level of funding that if paid on an ongoing basis is projected to cover post-retirement medical explicit subsidies for current employees and amortize any unfunded actuarial liabilities over a period not to exceed 30 years.
18. **Early Debt Extinguishment Reserves:** Reserves accumulated to retire the Pension Obligation Bonds at the earliest dates allowed under the Bond Indenture.
19. **General Fund:** For budgeting and reporting purposes, Metro Fire records all transactions in the General Fund that are not specifically accounted for in any other fund. The other funds include the Capital Facilities Fund, the Leased Properties Fund, the Grant Fund, the Development Impact Fees Fund, and the Intergovernmental Transfer (IGT) Fund.
20. **General Fund Operating Reserves:** These are Unassigned Reserves accounted for in the General Fund that are used for unexpected costs, revenue shortfalls, and smoothing cash flow prior to the receipt of expected revenue. In particular, cash flow is needed prior to the receipt of property taxes in January, May and June.
21. **Governmental Fund Financial Statements:** Governmental Fund Financial Statements report using the modified accrual basis of accounting and generally reports financial resources collected and used within 90 days of fiscal year end. Capital assets are expenditures when purchased.
22. **Government-Wide Financial Statements:** Government-Wide Financial Statements are reported using the accrual basis of accounting. The Statement of Net Assets in the Government-Wide Financial Statements include all capital assets, and the Statement of Activities shows annual depreciation of the capital assets.

23. **Grant Fund:** For budgeting and reporting purposes, Metro Fire records all grant related revenue and expenditures in the Grant Fund.
24. **Intergovernmental Transfer (IGT) Fund:** For budgeting purposes, Metro Fire records all transactions associated with Medi-Cal intergovernmental transfers in the IGT Fund.
25. **Labor Agreements:** All agreements with Local 522, along with resolutions and employment agreements passed by the Board of Directors covering unrepresented employees.
26. **Leased Properties Fund:** For budgeting purposes, Metro Fire records all transactions for surplus real property in the Leased Properties Fund. In addition, real property temporarily not in use is also recorded in this fund. Rent from these properties offsets non-operating expenditures such as utilities and special assessments.
27. **Net Budgeted General Fund Operating Expenditures:** Current year budgeted operating expenditures in the General Fund, adjusted to exclude one-time expenditures and include transfers out for ongoing expenditures.
28. **Non-spendable Fund Balance:** A classification of **fFund bBalance**. Non-spendable Fund Balance amounts cannot be spent because they are not in spendable form or cannot be spent because legally or contractually are required to be maintained intact. Examples of Non-Spendable Fund Balance are inventory and prepaid items.
29. **Pension Obligation Bonds:** Bonds issued by Metro Fire in 2004 to pay down unfunded pension liabilities with CalPERS and the Sacramento County Employee Retirement System (SCERS).
30. **Reserve Analysis:** Comparing actual reserve levels to target reserve levels.
31. **Restricted Fund Balance:** A classification of **fFund bBalance**. Restricted Fund Balance amounts can only be spent for specific purposes, which are stipulated outside the control of Metro Fire's Board of Directors by State law, granting entities, legal agreements, or enabling legislation, etc. Restricted Fund Balance examples are grant funds, debt proceeds, and Development Impact Fees.
32. **Self-Insurance Reserves:** Reserves accumulated for the payment of workers' compensation claims.
33. **Unassigned Fund Balance:** A classification of **fFund bBalance**. Any **fFund bBalance** amounts not classified as Restricted Fund Balance, Committed Fund Balance, and Assigned Fund Balance.

Policy

1. Unassigned Fund Balance
 - a. General Fund Operating Reserves will be used for unexpected costs or revenue shortfalls.
 - I. The minimum amount of General Fund Operating Reserves shall be 1.8 months of Net Budgeted General Fund Operating Expenditures (15%). Metro Fire is able to operate with this minimum amount due to a County of Sacramento "Dry Period Funding" credit line used in anticipation of property tax receipts.
 - II. The maximum amount of General Fund Operating Reserves shall be 6 months of Net Budgeted General Fund Operating Expenditures (50%) as reflected in the most current Metro Fire budget. This amount would allow Metro Fire the cash flow needed to operate without the County of Sacramento "Dry Period Funding" credit line.
2. Committed Fund Balance
 - a. Metro Fire is self-insured for most workers' compensation claims, and maintains excess coverage for extraordinary claims of \$3 million or more. This coverage amount may be adjusted each budget cycle.
 - I. To allow for future payment of workers' compensation claims, the minimum General Fund Self-insurance Reserves should equal the most recent short-term liability disclosed in Metro Fire's Audited Financial Statements.
 - II. The maximum General Fund Self-insurance Reserve should equal the most recent total liability of unpaid claims and expenses as reported in the most recent Audited Financial Statements.
 - b. Reserves should be accumulated to replace existing infrastructure upon the end of the assets' useful life. Capital Replacement Reserves should be in keeping with the Metro Fire CIP.
 - I. The minimum Capital Replacement Reserves should be equivalent to the annual depreciation in Metro Fire's most recent audited Government-Wide Financial Statements.
 - II. The maximum Capital Replacement Reserves should be equal to the accumulated depreciation in Metro Fire's most recently audited Government-Wide Financial Statements.
 - c. The District's Pension Funding Bonds Early Payoff Policy, 01.014.02, adopted in 2008 and revised in 2017, extinguishes the Pension Obligation Bonds at the earliest dates allowed under the Bond Indenture, to avoid the interest rate associated with the variable rate securities. Each year additional reserves will be budgeted pursuant to the Pension Funding Bonds Payoff Schedule incorporated within the revised Early Payoff Policy.

- I. The minimum amount of Early Debt Extinguishment Reserves should be the beginning balance plus the annual deposit amount calculated according to the procedures outlined in the Early Payoff Policy.
 - II. The maximum amount of Early Debt Extinguishment Reserves should be the total outstanding Pension Obligation Bond principal due to the Bondholders.
3. Restricted Reserves
- a. Development Impact Fees Fund ~~CIP~~ Reserves will be accumulated to fund Metro Fire's new infrastructure apparatus, equipment, and the construction, rehabilitation, and improvements to District facilities and properties needed to maintain Metro Fire's service level standards. CIP funding ~~will~~ may be ~~be~~ from the Development Impact Fees that mitigate the impact of new development. All Development Impact Fee amounts collected are restricted in use until such time as they are spent on capital outlay as provided for in State law. Capital spending over and above the Development Impact Fees should be provided as a transfer from the General Fund.
 - I. The minimum ~~CIP Development Impact Fee r~~Reserves shall be 10% of the current year's planned CIP expenditures in the Development Impact Fee Fund. These reserves are a buffer for deviations in bid amounts or construction costs.
 - II. The maximum CIP Reserves shall be the amount needed to fully fund the CIP plan projects funded from the Development Impact Fee Fund.
 - b. Bondholders and other lenders require Debt Service Reserves to provide additional security for obligations due to them from Metro Fire. Metro Fire will maintain at all times the Debt Service Reserve levels provided for in all outstanding debt and capital lease agreements.
4. Trust Fund
- a. Post-retirement medical insurance coverage is currently, and will continue to be, pre-funded in CERBT:
 - I. At a minimum, an amount should be the cumulative of Funding Policy Contributions plus earnings. This amount is reported to Metro Fire by CERBT on a quarterly basis.
 - II. At a maximum, an amount should be accumulated in CERBT to equal the Actuarial Present Value. This amount is determined by Metro Fire's actuary in its most recent Actuarial Valuation of Other Post-Employment Benefits.
5. Transition to Target Reserve Amounts
- a. Any budgeted Unassigned Reserve amounts remaining at fiscal year-end will initially be General Fund Operating Reserves. The Board of Directors

will review appropriate levels and uses for reserves during the budget process and may reclassify reserves as deemed appropriate.

- b. When reclassifying reserves, consideration will be made to all Metro Fire contractual obligations including the agreements with Local 522.

6. Use of Reserves

- a. Operating and Self-Insurance Reserves can be used at any time to meet cash flow requirements and Workers' Compensation claims, respectively. Authority to use the funds should be consistent with Metro Fire's budget, Purchasing and Contract Policy, and Labor Agreements. Any other use requires authorization of the Board of Directors.
- b. The Board of Directors will authorize use of Capital Replacement and CIP Reserves during the budget process. Capital Replacement and CIP Reserves are also available for unplanned (unbudgeted) capital replacement. Authorization for the use of Capital Replacement Reserves for unplanned capital replacement will be consistent with Metro Fire's Purchasing and Contract Policy.
- c. Early Debt Extinguishment and Debt Service Reserves use, is limited to the repayment of principal and interest of the related debt obligations.
- d. CERBT Reserves will be used exclusively for the payment of retiree medical premiums and CERBT management fees.

Procedures

1. The Chief Financial Officer shall perform a Reserve Analysis to be submitted to the Board of Directors upon the occurrence of the following events:
 - a. Board of Directors' budget deliberations; or
 - b. When changes are made to the amount of Workers' Compensation self-insurance excess insurance coverage; or
 - c. When updated Post-Retirement Medical or Workers' Compensation actuarial valuations are issued; or
 - d. When a major change in conditions threatens the targeted reserve levels established within this policy.
2. If the Reserve Analysis indicates projected or actual reserve levels are not within the target levels outlined in this policy, the following shall be included with the analysis:
 - a. An explanation of why reserve levels are not at the targeted level, and;
 - b. A course of action to bring reserve levels within the minimum and maximum levels prescribed.

References

1. Sacramento Metropolitan Fire District, Pension Fund Bonds Early Payoff Policy, 01.014.02 revised as of September 28, 2017.
2. Sacramento Metropolitan Fire District, Purchasing and Contracting Policy, 01.010.02, revised as of June 12, 2014.
3. Government Finance Officers Association of United States and Canada, Best Practice for Appropriate Level of Unrestricted Fund Balance in the General Fund.
4. Governmental Accounting Standards Board (GASB) Statement No. 54, Fund Balance Reporting and Governmental Fund Type Definitions, effective for fiscal years June 30, 2011 and later.



Todd Harms
Fire Chief

Sacramento Metropolitan Fire District

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

DATE: February 10, 2022
TO: Policy Committee Members
SUBJECT: Administration Policy
Policy 13.004.01 – Data Security Policy

TOPIC

Review new Administration Policy 13.004.01 Data Security Policy.

DISCUSSION

Attached is the new Data Security Policy 13.004.01 written by the Information Technology Division. The Data Security Policy identifies the different types of data, how to protect data, and how to properly dispose of media that contains data. The Data Security Policy is attached for your review.

RECOMMENDATION

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

Submitted By:

Approved By:



Mat Roseberry
IT Director



Ty Bailey
Deputy Chief, Administration

Sacramento Metropolitan Fire District

ADMINISTRATION POLICY

POLICY TITLE: Data Security

OVERSIGHT: IT

POLICY NUMBER: 13.004.01

EFFECTIVE DATE: 11/09/21

REVIEW DATE: 11/09/21

Background

Security is a team effort involving the participation and support of everyone who interacts with data and information systems for the Sacramento Metropolitan Fire District (District). Therefore, it is the responsibility of every user to know this policy and to conduct their activities in accordance with this policy.

Purpose

Protecting the District's information and systems that collect, process, and store this information is critical. The security of data and information systems must include controls and safeguard to offset possible threats and reduce exposure to risk as well as ensure confidentiality, integrity, and availability of data. Security measures must be taken to guard against unauthorized access to, alteration, disclosure, or destruction of data and information systems; this includes accidental loss or destruction.

Scope

This policy applies to all data. It is not limited to electronic information found in email, databases, applications, and other media, or paper information, such as hard copies of electronic data, employee files, internal memos, and so on. It is inclusive of data outside of the Sacramento Metropolitan Fire District stored in a cloud service, and/or held on a mobile computing device.

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. **Confidential Data:** Information maintained by the District and other agencies that is exempt from disclosure under the provisions of the California Public Records Act (Government Code Sections 6250-6265) or other applicable state or federal laws including the District Public Records Policy 114.01.
2. **Sensitive Data:** Information maintained by the District and other agencies that requires special precautions to protect it from unauthorized modification, dissemination, or deletion.
3. **DOD Wipe:** Because of the sensitive nature of the information at the Department of Defense, standards have been set for data wipes. In short, a DOD Wipe complies with those standards, writing over the original deleted information 7 times before it is considered unrecoverable.

4. **Penetration Testing:** Also known as pen testing, security pen testing, and security testing, is a form of ethical hacking. The pen test attempts to pierce the armor of an organization's cyber defenses, checking for vulnerabilities in networks, web apps, and user security.
5. **Mobile Devices:** Cell phones, laptops, flash drives, external hard drives.

Policy

1. Data security is not an option or choice; it is a legal requirement. In regulatory requirements, data security is embedded in the law. These requirements are implemented via the district policies and procedures.
2. It is the responsibility of everyone who works for the District to ensure the security of any personal, sensitive and confidential information contained in documents email, faxed, copied, scanned or printed.
3. **Printing/Copying/Faxing**
 - a. Anyone sending a confidential or sensitive fax should notify the recipient before it is sent.
 - b. Staff should ensure that the entire document has been copied or printed and check that the copier has not run out of paper. This is particularly important when copying or printing large documents.
 - c. When printing confidential or sensitive documents to a common area printer staff should not leave the printer unattended when using it, as another person may pick up the printing by mistake.
4. **Email**
 - a. When sending sensitive or confidential information via email carefully check the recipient's email address before pressing send.
 - b. If emailing sensitive or confidential information to outside email addresses encrypt the email.
5. **Mobile devices**
 - a. Mobile devices must not be left unattended in public spaces or left in plain sight in unattended vehicles at any time.
 - b. Staff should ensure that any mobile device not routinely connected to the District network, is brought in regularly to receive updates by IT.
 - c. Staff must ensure that all data is stored on the District network and not solely on the laptop.

- a. Data that falls under Confidential and/or Sensitive classifications must be encrypted with a minimum of 256-bit cryptography while in transit.
6. Staff working from home must ensure appropriate security is in place to protect equipment and information.
 7. Workstation Security
 - a. Secure workstations (screen lock or logout) prior to leaving the area to prevent unauthorized access.
 - b. Enabling a password-protected screen saver with a short timeout period to ensure that workstations that were left unsecured will be protected.
 - c. Ensuring that monitors are positioned away from public view. If necessary, install privacy screen filters or other physical barriers to public viewing.
 - d. Never install unauthorized software on workstations.
 8. Network/Server Security
 - a. Servers should be physically located in an access-controlled environment. Unrestricted access to the server room will be confined to designated staff whose job function requires access to that particular area/equipment. Restricted access may be given to other staff or third-party support where there is a specific job function needed for such access.
 - b. The most recent security patches must be installed on the system as soon as practical, the only exception being when an immediate application would interfere with business requirements.
 - c. Servers should have security software (Anti-Virus and Anti-Spyware) installed appropriately to the machine's specification.
 - d. Servers should always be password protected and locked when not in use.
 9. Data Backups
 - a. Backup software must be scheduled to run routinely, as required, to capture all data as required.
 - b. Backups should be monitored to make sure they are successful.
 - c. A test restoration process will be run regularly.
 - d. Data shall be backed up onsite, offsite and to the cloud.
 - e. Backups sent to the cloud must be encrypted with a minimum of 256-bit cryptography while in transit.

10. Control and security standards are designed to protect all of us. Appropriate controls and cost-effective safeguards ensure that each person is accountable for their actions. With security in place, controls make it possible to identify potential problem areas and also limit the extent of damage that mistakes can cause.
11. These are the accepted technologies used to enforce and ensure data security:
 - a. Access controls
 - b. Strong passwords
 - c. System monitoring
12. Failure to adequately protect the District's information from misuse, alteration, or destruction could result in a loss of public confidence.
13. The loss of data can cost time and money. Missing data can have major ramifications
 - a. Lost/Missing data may be extremely difficult, time-consuming, and costly to re-create.
 - b. Inaccurate information sent to the public, media, allied agency, vendor, or an employee may result in financial loss and/or discredit to the District.
 - c. Divulging private information about the District, allied agency, or an employee may result in adverse publicity and legal action against the District and the individual involved.
14. Hard drives, flash drives, and any other external media must be wiped using a DOD Wipe or shredded prior to disposal.
15. Federal and state laws make managers and employees legally responsible for preserving data integrity.
16. Management is responsible for ensuring that their direct reports understand the scope and implications of this policy.
17. A breach or suspected breach of this policy may result in the temporary withdrawal of hardware, software or services from the offending individual.

Procedures

1. IT will perform penetration testing against the District's network and applications to validate the efficacy of the security measures in place as well as end-user adherence to security policies.
2. Report any breach, or suspected breach of security without delay IT.

3. Report any lost or stolen devices as soon as practical to IT.

References

1. Sacramento Metropolitan Fire District Policy - Public Records
2. California Public Records Act (Government Code Sections 6250-6265)



Todd Harms
Fire Chief

Sacramento Metropolitan Fire District

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

DATE: February 10, 2021
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 new 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:

Approved By:


Mat Roseberry
IT Director


Ty Bailey
Deputy Chief, Administration

Sacramento Metropolitan Fire District

ADMINISTRATION POLICY

POLICY TITLE: Password Policy

OVERSIGHT: IT

POLICY NUMBER: 13.003.01

EFFECTIVE DATE:

REVIEW DATE:

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

1. Individual Responsibilities
 - a. Passwords must be changed immediately upon issuance for the first-use. Initial passwords must be securely transmitted to the individual.
 - b. 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.
 - c. Members 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.

- d. 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.
- e. Individuals must never leave themselves logged into an application or system where someone else can unknowingly use their account.
 - I. To access shared workstations (e.g., camera system, CAD display), IT will provide a limited-use shared account for the workstation.
 - II. 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.
 - III. When IT services iOS devices, IT will ask the user to provide their passcode in order to perform the repair.
 - IV. iOS device Apple ID passwords are kept in an IT encrypted password manager. IT manages the passwords in order to service iOS devices.
 - V. 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).
 - VI. If a password needs to be shared for servicing, IT should be contacted for authorization and appropriate instruction.
 - VII. Passwords for the District must be unique and different from passwords used for other personal services (e.g., banking).
 - VIII. Passwords must meet the requirements outlined in this policy.
 - IX. 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.
 - X. 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.
 - XI. In the event a breach or compromise is suspected, the incident must be reported to IT immediately.

2. Responsibilities of Systems Processing Passwords

- a. Passwords must be prohibited from being displayed when entered.
- b. Passwords must never be stored in clear, readable format (encryption must always be used).
- c. Passwords must never be stored as part of a login script, program, or automated process.
- d. Systems storing or providing access to confidential data or remote access to the internal network must be secured with multifactor authentication.
- e. Password hashes (irreversible encoded values) must never be accessible to unauthorized individuals.
- f. Where possible, salted hashes (irreversible encoded values with added randomness) should be used for password encryption.

Procedures

1. Password Requirements

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

- a. At least twelve (12) characters (unless the application will not allow 12 characters);
- b. 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
- c. Not vulnerable to a dictionary attack (see Recommendations for Creating Compliant Password).

2. 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.

3. Standard Users

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

- a. Passwords are required to be changed every 365 days.
- b. Passwords must not be reused for at least five (5) generations.

- c. Passwords must comply with the criteria in section Password Requirements

4. 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.

- a. Passwords are required to be changed every 365 days.
- b. Passwords must not be reused for at least five (5) generations.
- c. Passwords must comply with the criteria in section Password Requirements.

5. Service Accounts

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

- a. Passwords are required to be changed if compromised.
- b. Passwords should be stored in the IT Password Manager system.
- c. Passwords must comply with the criteria in section Password Requirements.

6. Test Accounts

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

- a. Passwords are required to be changed every 180 days.
- b. Passwords must not be reused for at least five (5) generations
- c. Passwords should be stored in the IT Password Manager.
- d. Passwords must comply with the criteria in section Password Requirements.

7. Local Admin Accounts

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

- a. Passwords are required to be changed if compromised.
- b. Passwords should be stored in the IT Password Manager.
- c. Passwords must comply with the criteria in section Password Requirements.
- d. Passwords must be changed when IT staff leave the IT division.

8. 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.

9. Standard Users

- a. Accounts will lockout after five (5) invalid password attempts in fifteen minutes.
- b. 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.

10. Privileged Users

- a. Accounts will lockout after five (5) invalid password attempts in fifteen minutes.
- b. 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.

11. Test Accounts

- a. Accounts will lockout after five (5) invalid password attempts in fifteen minutes.
- b. 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.

12. 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:

- a. At least four (4) digits.
- b. 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.

13. 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.

- a. Choose a sentence, phrase, or a series of random, disjointed, and unrelated words.
- b. Use a phrase that is easy to remember.
- c. Examples:
 - I. Password: when I was 5, I learned to ride a bike.
 - II. Password: fetch unobtrusively unspoken haunt unopposed
 - III. Password: stack process overbid press
 - IV. Password: agile stash perpetual creatable

14. 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.

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

15. Password Reset Options

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

- a. Contact IT and provide your employee PIN number.

- b. Stop by the IT helpdesk at HQ.
- c. Use the "forgot password" feature from the application, if applicable.

16. Reporting a Suspended Compromise, Security Incident, or Breach

- a. 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.

17. Password Verification and Validation

- a. 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.
- b. 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.



Todd Harms
Fire Chief

Sacramento Metropolitan Fire District

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

DATE: January 13, 2021
TO: Policy Committee Members
SUBJECT: Administration Policy
Policy 13.005.01 – Electronic Mail Policy

TOPIC

Review new Administration Policy 13.005.01 Electronic Mail Policy.

DISCUSSION

Attached is the new Electronic Mail Policy 13.005.01 written by the Information Technology Division. The purpose of the policy is to ensure that information sent or received by District members or anyone working on behalf of the District, who is using the District's electronic mail systems, is managed consistently across the organization and in compliance with District policies and the law.


RECOMMENDATION

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

Submitted By:

Approved By:


Mat Roseberry
IT Director


Ty Bailey
Deputy Chief, Administration

Sacramento Metropolitan Fire District

ADMINISTRATION POLICY

POLICY TITLE: Electronic Mail

OVERSIGHT: IT

POLICY NUMBER: 13.005.01

EFFECTIVE DATE:

REVIEW DATE:

Background

Email is a critical mechanism for business communications at Sacramento Metropolitan Fire District (District). However, use of the District's electronic mail system and services are a privilege, not a right, and therefore must be used with respect and in accordance with the policies and procedures of the District.

Purpose

The purpose of the policy is to ensure that information sent or received by District members or anyone working on behalf of the District, who is using the District's electronic mail systems, is managed consistently across the organization and in compliance with District policies and the law.

Scope

This policy applies to all email systems and services owned by the District, all email account users/holders at the District and all District email records.

Definitions

1. **Electronic Mail:** Electronic Mail (email) may include non-interactive communication of text, data, images, or voice messages between a sender and designated recipient(s) by systems utilizing telecommunications links. It may also include correspondence transmitted and stored electronically using software facilities called "email, facsimile, or messaging" systems; or voice messages transmitted and stored for later retrieval from a computer system.
2. **SPAM:** Unsolicited commercial email sent to a large number of recipients.

Policy

1. The District's email system is to be used for business purposes in serving the interests of the District and its customers.
2. All messages communicated over the District's electronic systems must be courteous and professional in nature. Email is not to be used for gossip, sharing of personal information, or for emotional responses to business correspondence or work situations.
3. Material that is fraudulent, harassing, embarrassing, sexually explicit, obscene, intimidating, defamatory, discriminatory or otherwise unlawful or inappropriate may not be sent by email or other forms of electronic communication or displayed

or stored in any computers of the District, except as necessary in the investigation of any crimes or the investigation of misconduct by members.

4. The email system is capable of broadcasting messages to all users of the email system, or all the users within a group. Messages sent to all members shall be restricted to business purposes only.
5. The District's email system is not intended to function as an information storage device or electronic filing system. The system shall be used for transmission and temporary short-term storage. Accordingly, the District may limit the storage capacity of members' mailboxes and limit the size of email attachments.
6. Email users are responsible for mailbox management, including organization and cleaning. If a user subscribes to a mailing list, they must be aware of how to unsubscribe from the list and is responsible for doing so if their current email address changes.
7. The District often delivers official communications via email. As a result, members of the District with email accounts are expected to check their email in a consistent and timely manner so that they are aware of important District announcements and updates, as well as for fulfilling business and role-oriented tasks.
8. Email access at the District is controlled through individual accounts and passwords. It is the responsibility of the member to protect the confidentiality of their account and password information.
9. Members shall not send an email under another member's identity without the explicit permission from the member.
10. Members shall not attempt to disguise the origin of any electronic communication sent from the District's equipment. The sole exception shall be for communications used in criminal investigations in cases where disguising the identity of the sender is vital to the successful completion of the investigation and when duly authorized by the Fire Chief or his/her designee to conduct an investigation in that manner.
11. The District email system and all messages, attachments, and images are the sole property of the District. This gives the District the right to monitor any and all email traffic passing through its email system. This monitoring may include, but is not limited to, inadvertent reading by IT staff during the normal course of managing the email system, review by the legal team during the email discovery phase of litigation, observation by management in cases of suspected abuse, or to monitor member efficiency.
12. Electronic records, including but not limited to email messages, may be disclosed by the District to outside parties in connection with litigation, investigations, audits, requests for public records under the California Public Records Act, or by any other law or policy.

13. The District has an obligation to take necessary actions to ensure the email system is consistently and reliably available and operates efficiently in a safe and secure environment that is free from unauthorized users, unauthorized use, and virus/malware attacks. Accordingly, the District may limit the type of email attachments and apply SPAM blocking.
14. Archival and backup copies of email messages may exist, despite end-user deletion, in compliance with the District's Record Retention Policy. The goals of these backups and archiving procedures are to ensure system reliability, prevent business data loss, meet regulatory and litigation needs, and to provide business intelligence.

Procedure

1. Any allegations of misuse should be promptly reported to the IT division. If you receive an offensive or SPAM email, do not forward, delete, or reply to the message. Instead, report it directly to the IT division.

References

1. Sacramento Metropolitan Fire District Policy - Public Records
2. California Public Records Act (Government Code Sections 6250-6265)



Todd Harms
Fire Chief

Sacramento Metropolitan Fire District

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

DATE: February 10, 2021
TO: Policy Committee Members
SUBJECT: Administration Policy
Policy 13.006.01 – Cell Phone Policy

TOPIC

Review new Administration Policy 13.006.01 Cell Phone Policy.

DISCUSSION

Attached is the new Cell Phone Policy 13.006.01 written by the Information Technology Division. The cell phone policy outlines cell phone use in accordance with applicable state and local laws for our members.

RECOMMENDATION

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

Submitted By:

Approved By:


Mat Roseberry
IT Director


Ty Bailey
Deputy Chief, Administration

Sacramento Metropolitan Fire District

ADMINISTRATION POLICY

POLICY TITLE: Cell Phone Policy

OVERSIGHT: IT

POLICY NUMBER: 13.006.01 EFFECTIVE DATE: XX/XX/XX REVIEW DATE: XX/XX/XX

Background

The Sacramento Metropolitan Fire District (District) recognizes the need for cellular phones to conduct its business. For this reason, the District provides cell phones and accessories to some District employees based on position and function.

Purpose

This policy identifies use criteria for both the District and the individual user.

Scope

This policy is applicable to all District personnel, temporary employees, and annuitants.

Definitions

1. **Business calls:** Telephone calls made for the purpose of the District's business.
2. **Personal calls:** Telephone calls that are not for the purpose of the District's business.

Policy

1. Employees may be provided a cell phone with their duties as a member of the District. Employees should check with their supervisor or manager regarding eligibility and authorization procedures.
2. Employees should only use District provided cell phones for necessary District business related purposes.
3. The District recognizes that employees may have to make personal calls. Employees should minimize District cell phone use for personal calls. Employees who are out of town on District business can use the District cell phone to contact family and /or caregivers. Such use should be reasonable. Employees that are making personal calls on the District cell phone should switch to an incoming call and provide the required level of service as needed before returning to a personal call.
4. Employees are responsible for the safekeeping, care and custody of the cell phone and assigned accessories.

5. Cell Phone Use While Driving:
 - a. Employees must adhere to all federal, state or local rules and regulations regarding the use of cell phones while driving. Accordingly, employees must not use cell phones if such conduct is prohibited by law, regulation or other ordinance.
 - b. Employees should not drive a motor vehicle while using a cell phone unless that telephone is specifically designed and configured to allow hands-free listening and talking, and is used in that manner while driving.
 - c. Employees should not drive a motor vehicle while holding and operating a handheld cell phone or an electronic communications device unless the cell phone or electronic communications device is specifically designed and configured to allow voice-operated and hands-free operation, and it is used in that manner while driving.
 - d. A handheld cell phone or electronic communications device may be operated in a manner requiring the use of the driver's hand while the driver is operating the vehicle only if both of the following conditions are satisfied:
 - I. The handheld cell phone or electronic communications device is mounted on a vehicle's windshield in the same manner a portable Global Positioning System (GPS) is mounted or is mounted on or affixed to a vehicle's dashboard or center console in a manner that does not hinder the driver's view of the road.
 - II. The driver's hand is used to activate or deactivate a feature or function of the handheld cell phone or communications device with the motion of a single swipe or tap of the driver's finger.
 - e. An employee may use a handheld cell phone or electronic communications device while performing functions related to emergency duties, when no other reasonable option exists and as allowed by law, however minimal use is preferred.
6. All call records, text messages and Internet browsing is subject to California Public Records Act requests.
7. Employees will not use the District issued cell phone for illegal, disruptive, unethical or unprofessional activities, for personal gain, or for any purpose that would jeopardize the legitimate interests of the District.

Procedure

1. Employees are responsible to return their District issued cell phone and all assigned accessories to the IT division when they no longer have a need for a

cell phone, if the IT division requests the cell phone back, or when they are no longer employed by the District.

References

1. Sacramento Metropolitan Fire District Policy - Public Records
2. California Public Records Act (Government Code Sections 6250-6265)
3. California Vehicle Code 23123
4. California Vehicle Code 23125.5



Todd Harms
Fire Chief

Sacramento Metropolitan Fire District

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

DATE: February 10, 2021
TO: Policy Committee Members
SUBJECT: Administration Policy
Policy 13.002.01 – Employee Personal Electronic Device Policy

TOPIC

Review new Administration Policy 13.002.01 Employee Personal Electronic Device Policy.

DISCUSSION


Attached is the new Employee Personal Electronic Device Policy 13.002.01 written by the Information Technology Division. The purpose of the policy is to establish District guidelines for employee use of personally owned electronic devices for work-related purposes.


RECOMMENDATION

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

Submitted By:

Approved By:


Matthew Roseberry
IT Director


Ty Bailey
Deputy Chief, Administration

Sacramento Metropolitan Fire District

ADMINISTRATION POLICY

POLICY TITLE:	Employee Personal Electronic Device Policy	OVERSIGHT:	Information Technology
POLICY NUMBER:	13.002.01	EFFECTIVE DATE:	Xx/xx/xx
		REVIEW DATE:	xx/xx/xx

Background

The Sacramento Metropolitan Fire District (District) does not require employees to purchase or use their own personal electronic devices to use for District business, however, some employees want access to their email, calendar and computer from their personal electronic devices.

Purpose

This policy establishes District guidelines for employee use of personally owned electronic devices for work-related purposes.

Scope

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

Definitions

1. **Personal Electronic Device:** cellular telephone, smart phone, tablet, laptop computer, and desktop computer.
2. **VDI:** Virtual Desktop Interface.
3. **Sensitive District Files:** Documents or data whose loss, misuse, or unauthorized access can adversely affect the privacy or welfare of an individual (personally identifiable information), the outcome of a charge/complaint/case, proprietary information, or District financial operations.
4. **Jail Brake:** installing software that allows the user to bypass standard built-in security features and controls.
5. **Root:** discovering a bug of some sort that allows you to bypass internal protections and gain complete control over the operating system — to become the “root” user, who has all privileges and all access.
6. **PIN:** Personal Identification Number.
7. **Smart Phone:** a device that combines a cell phone with a hand held computer, typically offering Internet access, data storage, and email capability.
8. **Tablet:** a wireless, portable personal computer with a touch screen interface.

9. **Remote Access APP:** a remote access application in which allows employees to view information on District servers using their personal electronic device.
10. **Authorized Users:** employees granted a license for remote access to District servers.

Policy

1. Privacy – All email from the District email account is stored on the District's email server and may be subject to a Public Records Act Request. As such, an employee has limited expectation of privacy in the information that is stored on the District's server, including email.
2. Security – In order to add your District email to your smartphone it will require you to add a PIN code. This PIN code is mandatory and is not authorized to be removed from the device while having the District email configured. See the **Password Policy** for Mobile Device requirements.
3. Remote Access – Authorized users will have the ability to access their VDI session from their personal electronic devices via the Horizon View client APP or application. When using the Horizon View client all activity is done on the District's servers and nothing will be stored to the user's personal electronic device.
4. Files – Users will not download or transfer sensitive District files to their personal electronic devices. User agrees to delete any sensitive District files that may be inadvertently downloaded and stored on the device through the process of viewing e-mail attachments.
5. Operating System - User agrees to maintain the original device operating system and keep the device current with security patches and updates, as released by the manufacturer. The user will not "Jail Break" or Root the device.
6. User agrees that the device will not be shared with other individuals or family members, due to the business use of the device (potential access to District e-mail, etc)
7. Backing-Up - User will not download/transfer sensitive District files to any non-District device or cloud account. In the event that a need arises to transfer District files to your personal cloud account then see the **Password Policy** for cloud account requirements.
8. Applications – In the event the device is no longer used or the user is no longer employed with the District, the user agrees to remove any installed applications that were installed using their District Apple ID or other District related account.
9. Support – The District IT division will provide limited support for your personal electronic device. This will include providing information needed to add your District email account and where to find the remote access APP or application. Examples of support not provided include but not limited to:

- a. Troubleshooting device performance or hardware problems
 - b. Troubleshooting software applications or cloud services
 - c. Installing OS upgrades, OS patches or District owned software
 - d. Troubleshooting printers
 - e. Troubleshooting routers and or wireless access points.
 - f. Backing up device data including text messages or migrating data to a new device
 - g. Removing malware or spyware.
10. Restrictions on Authorized Use –
- a. While at work, employees are expected to exercise the same discretion in using their personal electronic devices as is expected for the use of District devices. District policies pertaining to harassment, discrimination, retaliation, confidential information, ethics, Internet and Electronic Connection Use apply to employee use of personal electronic devices for work-related activities.
 - b. Excessive personal calls, e-mails or text messaging during the workday, regardless of the device used, can interfere with employee productivity and be distracting to others. Employees must handle personal matters on non-work time.
11. Liability – The District is not liable for the loss, theft, damage, security, or data loss of the user's personal electronic device. This includes, but is not limited to, when the device is being used for District business, on District time or during business travel.
12. Compensation – If you choose to use your personal electronic device for District use off shift, including to access your email, without express permission or instruction from your supervisor, the District will not compensate you for straight time or overtime.
13. PRA Requests - In holding that the PRA covers communications on an employee's personal device or account, the California Supreme Court affirmed that under the California Constitution, people have a right to access information held by the government. But, the Court held, such a right to information must be balanced against individual privacy rights. As an example of how to balance the right to information under the PRA versus the right to privacy, the Court provided the following guidance:
- a. The PRA only requires the disclosure of records that can be located with "reasonable effort." Thus, agencies do not have to undertake "extensive or intrusive searches."
 - b. Once an agency receives a PRA request, it must communicate the scope of the request to its custodian of records.

- c. If the information is held by an employee on his or her personal device or account, then the employee would be the custodian of records for that information and must be notified accordingly.
- d. The agency can then “reasonably rely on these employees to search their own personal files, accounts, and devices for responsive material.” However, the employee should be provided training on how to distinguish public records from personal records.
- e. The employee may justify withholding a potentially responsive writing by providing a declaration containing enough details for a court to determine whether the items are public versus personal records.

Procedures

1. District employees occasionally need remote access to the District servers to conduct work on a project outside normal working hours. Employees that would like to use their personal electronic device to remotely access District servers will need to contact the IT Division and request to be added to the authorized remote access group. IT will then provide the employee information on how to add their District email account and where to find the remote access APP or application.
2. Lost or Stolen– If your device is lost or stolen you need to notify the IT helpdesk as soon as practical after you notice the device is missing. IT will be able to remotely wipe your smartphone or tablet. User understands that all data on the device will be erased and the District is not responsible for its loss.
3. Upon termination with the District, the IT Division will remove the employee from the remote access group in which the employee will no longer be authorized to remotely access District servers.

References

1. Stored Communications Act (Title II of the Electronic Communications Privacy Act of 1986)
2. Fourth Amendment to the United States Constitution
3. U.S. Equal Employment Opportunity Commission
4. U.S. Department of Labor: Wage and Hour Division
5. Society for Human Resources Management (SHRM)
6. Sacramento Metropolitan Fire District Policy - Public Records
7. California Public Records Act (Government Code Sections 6250-6265)
8. California Supreme Court Case No. S218066
9. All current policies can be found in the Policies APP