EAST BAY
MUNICIPAL UTILITY DISTRICT

Computerized Maintenance Management System (CMMS) Project

Technical (Non-Functional) Requirements

October 2020

1 Introduction

The purpose of this document is to specify the technical requirements for the CMMS Project.

2 Definitions

CAS The Central Authentication Service (CAS) is a single sign-on protocol for the web. CAS allows a user to access multiple applications while providing login credentials once.

Cloud-based Services Applications, services or resources made available to users via the Internet.

CMMS Computerized Maintenance Management System. Some of the existing systems will not be covered by a new CMMS solution, such as the Backflow Prevention System which can be replaced by a separate COTS solution. The majority of the new CMMS solutions provide the capability to integrate/synchronize the asset data between the CMMS and the GIS allowing utilities to manage their assets and work activities in one system.

District East Bay Municipal Utility District (EBMUD).

Hybrid Cloud Solution A mix of both Cloud and On-Premise where Applications and servers are located within the District premise as well as other locations through the Internet.

On-Premise Solution Applications and servers are installed and run on premise at the District.

SAML Security Assertion Markup Language (SAML) is an open standard that allows identity providers to pass authorization credentials to service providers.

System The software solution including licenses and configurations which meets all defined requirements or an agreed upon subset of requirements.

Vendor Person or company that specializes in bringing together software subsystems into a functioning whole, integrating existing or new business processes and warrants configuration and services to meet defined requirements.

3 System Security / Authentication

3.1 Single Sign-On

3.1.1 The System shall use District's Single Sign-On Architecture: ADFS. The District supports SAML Version 2.0 and OAuth2 protocols.

2.1.2 The System shall support a configurable session timeout, requiring users to re-authenticate upon session expiry.

3.2 Encryption

3.2.1 The System shall utilize standard cryptographic protocols (TLS version 1.2) to encrypt any web page performing transaction processing for internal or external tasks.

3.2.2 The System shall strongly encrypt all confidential or personally identifiable information in transit (during transactions) and at rest (in the database).

3.2.3 Vendor shall provide specifications listing the encryption algorithms and protocols used to secure data in transit and at rest.

3.3 Role-based User Access

3.3.1 The System shall provide role-based access control throughout the System to implement least privilege access.

3.3.2 The System shall extend role-based access control to the application, transaction and data levels.

3.3.3 The System shall provide configuration tools for District staff to assign and modify users to and from different roles. District staff shall have the ability to add, delete, and modify roles and shall have the ability to customize security permissions assigned to each role.

3.4 Application Design

3.4.1 The System shall be designed, developed, deployed and tested in accordance with industry standards including but not limited to Open Web Application Security Project (OWASP) security principles. Evidence of regular testing should be provided to EBMUD.

3.5 Audit Trails and Logging

3.5.1 The System shall provide audit trails for all transactions generated by the System which includes capturing, storing and reporting on activities including but not limited to user activities, API calls, automated internal system activities, CRON jobs, interfaces, file transfers and errors. Audit trails reports shall support the ability to search, sort and filter based on functionality.

3.5.2 The System shall make audit trail information available to a select group of user roles designated by District system administrators.

2.5.3 The System should have the ability to send all logs via syslog via TCP/IP to a custom port.

3.6 Cloud-based Services or On Premise Solution

3.6.1 The Vendor will specify if the proposed solution is a Cloud-based Service, on premise or hybrid solution.

3.6.2 Regardless of the solution, it must comply with accepted industry standards and best practices.

3.6.2.1 Services shall be available 24 hours per day, seven days per week.

3.6.2.2 Services shall have a 99.9% or better uptime.

3.6.3 If an On Premise Solution is offered, provide the details of solution including but not limited to the following information:

3.6.3.1 Software requirements e.g. ability to run in a VM, operating system, middleware, database, etc.

3.6.3.2 Hardware requirements e.g. CPU, RAM, storage, etc.

3.6.3.3 Details of the type of vendor access needed to support the on premise systems

3.6.3.4 What is each party's responsibility for software installation and support?

3.6.3.4.1 What support is offered for on premise installation?

3.6.3.4.2 What support is offered post-installation?

3.6.3.5 Provide LAN, WAN and other related network requirements for hosting an On Premise Solution.

3.6.4 If a Cloud-based service or hybrid solution is offered, provide the details of the solution including but not limited to the following information:

3.6.4.1 If the solution is hosted by an Application Service Provider, provide Application Service Provide name and details.

3.6.4.2 Whether the cloud service is public or private

3.6.4.2.1 If public cloud, how will the vendor protect each customer’s data from access by another customer in the shared environment?

3.6.4.2.2 If private cloud, is it hosted on District managed infrastructure or Vendor managed infrastructure? If hosted on District managed infrastructure, what kind of access will the Vendor require including authentication and firewall access?

3.6.4.3 State what access privileges will be available to District IT Systems staff?

3.6.5 Cloud-based services should be utilizing an industry recognized security framework such as CIS CSC-20 or NIST 800-53 SP4. Service provider must provide a current SOC2 Type II audit report to EBMUD annually. Scope of the audit report should include the physical compute environment as well as the ongoing operations/maintenance of the SAAS application and data.

3.6.6 Cloud-based service providers shall be obligated to immediately notify the District of any suspected or confirmed security breach and shall take immediate action to remedy such breach.

4 Usability

4.1 System Performance/Availability

4.1.1 95% of application pages displayed within 2 seconds.

4.1.2 99% of application pages displayed within 5 seconds.

4.1.3 Vendor shall provide a Service Level Agreement (SLA) that specifically identifies system uptime and performance guarantees.

4.1.4 The System shall have a mechanism to document system up-time that is available to the District to review.

4.1.5 The System shall have tools to evaluate real-time system performance and make them available to the District.

4.2 Mobility

4.2.1 The System shall provide access to all major functions through mobile devices running Android, Windows, or iOS mobile operating systems.

4.2.2 Mobile displays shall be optimized for the size of the mobile device.

3.2.3 The System will support data collection by Android, Windows, and iOS smartphones and tablets.

4.3 Accessibility

4.3.1 The System shall provide access to all functionality through HTML 5 compliant standard web browsers.

4.3.2 The System shall be accessible from District acceptable versions of Edge, Chrome, Firefox, Safari, and any other commonly used desktop and/or mobile web browser.

4.4 Design

4.4.1 The system shall incorporate well established user interface patterns to facilitate a good user experience. E.g. provide tips for form fields, provide drop down menus for fields that the customer may not know the correct terminology to type in, etc.

4.4.2 The system shall have the ability to match the District's systems look and feel. Samples of District systems include but are not limited to the following:

4.4.2.1 EBMUD.com – https://www.ebmud.com/

4.4.2.2 Splashpad – https://splashpad/ (District Intranet)

See Appendix B

4.4.3 The system shall have the ability to modify the look and feel should the District's look and feel change.

4.4.4 The system shall use responsive web design so that the solution displays and functions well on mobile devices.

4.5 Scalability / Flexibility

4.5.1 The District user profile will likely change in the future. The vendor shall provide a Capacity Management Plan containing scenarios for different predictions of business demand as well as costed options for delivering agreed upon service levels.

4.6 Analytics

4.6.1 Analytics shall be provided for all functionality.

4.6.2 Analysis and shall include but not be limited to the following:

4.6.2.1 Page hits

4.6.2.2 Requesting source

4.6.2.3 Errors and details

4.6.3 The max, min, and average (including the first & second standard deviation) of the time it takes to complete the functionality in a specified date range.

4.6.3.1 Time spent on each web page in the functionality

4.6.3.2 Visitor Flow Path to get to the functionality. I.e. the web pages the customer visited before executing a functionality

4.6.3.3 Abandonment rate and a list of pages on which a visitor abandoned a process

5 Interfaces

5.1 Appendix A

5.1.1 The District utilizes numerous custom-built, commercial off-the shelf and cloud software solutions. The System will need to exchange data with many of these applications in batch or real time. The System will provide standard interfaces to existing and future District systems/applications for incoming and outgoing data. **Appendix A** provides a list of applications/vendors with which the System may need to interface.

5.1.2 For new and existing interfaces the District will need specifications including but not limited to the following:

5.1.2.1 Authentication and authorization

5.1.2.2 Data fields, data types, source systems, and destination systems

5.1.2.3 Frequency

5.1.2.4 Communication protocol

5.1.2.5 How interface error processing and recovery are handled

5.1.2.6 How transactions are logged

5.1.2.7 SLA requirements for incoming and outgoing interface transactions

6 Data Management

6.1 Data Security

6.1.1 Vendor shall identify the data elements required from the District to deliver the functionality listed in the Functional requirements of this RFP.

6.1.2 Vendor shall eliminate local storage of customer PII, retrieving it only on an as-needed basis from the District via REST web services.

6.1.3 Vendor shall notify the District of any changes to its infrastructure after the initial implementation.

6.1.4 Vendor shall not share any District data (atomic or aggregated) with any 3rd party for any purpose.

6.1.5 Vendor will provide the current release version of its OS and application stack and indicate how often they are patched or updated and will report to the District any time the application stack is modified.

6.1.6 Vendor shall create a Data Management Plan and annually review it with the District.

6.2 Application Data Export

6.2.1 The System shall provide mechanisms for regularly scheduled and on-demand export of all data to District databases in a format specified by the District.

6.2.2 These mechanisms shall allow for full and incremental exports.

6.2.2.1 Full Export – a complete export of all data

6.2.2.2 Incremental Export – an export of changed data since the last full or incremental export

6.2.2.3 Periodic Export – a preset scheduled export defined by the District

6.3 Archiving Data

6.3.1 The System shall provide mechanisms for the moving of data to external storage utilizing predefined business rules.

6.3.2 The system will allow for the ability to configure data archive related criteria.

6.3.3 The system will allow the scheduling of data archive operations.

6.3.4 The system will allow for the ability to configure data eligible for purging.

6.4 Data Availability

6.4.1 All data entered or uploaded into the system shall remain the property of the District and shall not be disclosed or used without express written permission.

6.4.2 The System shall be able to associate data to predefined retention schedules. Retention schedules shall be permanently tied to the data but each retention schedule can be subject to change.

6.4.3 The System shall allow the District to retrieve data from the System at regular intervals.

7 Business Continuity and Disaster Recovery

7.1.1 The vendor shall provide a Business Continuity and Disaster Recovery Plan.

7.1.2 The System shall provide full data back-ups on a predetermined schedule and provide recovery capabilities. Desired recovery time objective is 12 hours or less.

7.1.3 The System shall provide transaction-level recovery up to 5 minutes or less, ideally to the time point immediately preceding the disaster.

7.1.4 The System shall have its business continuity plan tested on a regular, predetermined timeframe.

7.1.5 The System shall provide manual, hard copy workflow provisions during critical system failure.

7.1.6 Patches and Releases

7.1.6.1 The Vendor shall provide advance notice (minimum of five business days) and release notes for every software patch release. Thirty business days advance notice will be required for major software upgrades.

7.1.6.2 The Vendor shall perform system maintenance and upgrades within the following windows:

7.1.6.2.1 District IT Maintenance Window: Wednesday evenings after 4:30PM.

7.1.6.2.2 Releases and upgrades requiring 3 or more hours to deploy shall be performed over the weekend.

7.1.6.3 The Vendor shall provide dedicated test environments and current data sets to support periodic and ongoing system upgrades to ensure that the upgrades are successful and there are no regression issues. For a detailed list of dedicated environments see section 8.5.

7.1.6.4 Vendor shall provide ample time (minimum of 30 business days) for testing and training for every major system upgrade.

7.1.6.5 Vendor shall provide options to opt out of software upgrades.

7.1.6.6 Vendor shall provide system/application support regardless of whether the District chooses to upgrade the software.

7.1.6.7 Vendor shall provide options to roll back to the previous version of the system if issues are encountered in the new upgrade.

7.1.6.8 Vendor shall provide service and support to the District to migrate all data to District databases or a destination specified by District should the District decide to switch to a different product.

7.1.6.9 Vendor shall provide no less than 90 business days for the District to complete such data migration.

8 Implementation Plan and Schedule

8.1 Implementation Approach

8.1.1 **Phased Implementation** - Vendor shall provide a phased implementation plan and schedule which details major project phases, tasks to be performed in each phase, dependencies, assumptions made, staff time and resources required from vendor and District, etc. This implementation plan will be reviewed for acceptance by the District and is subject to change during the course of the project.

8.2 Implementation methodology

8.2.1 **Agile** – An agile development process by the Vendor is required so that District can obtain frequent deliverables weekly/bi-weekly for testing. This shortens the feedback cycle and helps detects major problems/issues sooner in the project. Vendor staff shall be reasonably available to meet regularly with District staff.

8.2.2 Vendor shall provide a proposed detailed implementation methodology. Details will include but are not limited to the following

8.2.2.1 Project Management

8.2.2.2 Initiation

8.2.2.3 Planning

8.2.2.4 Executing

8.2.2.5 Monitoring/Controlling

8.2.2.6 Closing

8.3 Data Conversion

8.3.1 Vendor shall provide the framework, tools, guidance and validation methods for the conversion of existing District data to a format compatible with the System.

8.3.2 Vendor shall load converted data into the System as required to thoroughly test and prepare the System for production deployment.

8.3.3 Forward data mapping (from District systems to vendor's system) must be designed to facilitate straightforward reverse data mapping (from vendor's system to District systems).

8.3.3.1 Forward and reverse data mapping must not be treated as independent activities. Forward data mapping must be explicitly designed with the understanding that District will have an ongoing need to obtain data from vendor's systems in an automated manner. Such data must be reverse mapped so as to be compatible with District systems and data structures.

8.3.3.2 The vendor shall be responsible for the following in terms of reverse data mapping:

8.3.3.2.1 Provide the initial reverse data mapping methodology and configuration.

8.3.3.2.2 Provide analysis and modifications as needed.

8.3.3.2.3 Provide finalized reverse data mapping methodology and configuration. Provide regularly scheduled and on-demand extracts of reverse mapped data from vendor's system to District systems.

8.4 Data Handling and Retention

8.4.1 The system will support SOAP and REST web services.

8.4.2 The system will be able to exchange data via flat files and web services.

8.4.3 The system will retain data up to a District configurable number of years.

8.4.4 The system will allow for the storage and easy retrieval of documents by established Metadata which can include but not be limited to the following:

8.4.4.1 Functionality

8.4.4.2 Author

8.4.4.3 Date

8.4.4.4 Keywords

8.5 Development, Test, Training, and Staging Instances

8.5.1 In addition to the production instance, Vendor shall provide the below Instances (each independently including all required components, such as application servers and databases) during the implementation period as well as post go-live for the life of the contract. Such instances shall provide functionality identical to that of the production environment except for changes being developed or tested.

8.5.1.1 Vendor shall provide a Development instance in order to perform software development and unit testing.

8.5.1.2 Vendor shall provide a Test instance in order to verify patches and upgrades before they are implemented in production.

8.5.1.3 Vendor shall provide a Training instance in order to allow District staff to train on the system without using the production instance.

8.5.1.4 Vendor shall provide a Staging instance in order to allow the District to test integrations with other non-vendor applications.

8.5.2 Vendor shall provide details regarding managing the various instances. Some features can include but are not limited to the following:

8.5.2.1 Environment refresh procedures

8.5.2.2 Administration

8.5.2.3 Backup/Restore

8.5.2.4 Infrastructure as a Service (IaaS) details if applicable

8.5.3 The system will support scripted configuration moves, allowing automated transfer from one environment to another or from the configuration repository within a 24 hour period.

8.5.4 Upon request by District, the Vendor shall refresh non-Production instances specified by District with a copy of Production data. Vendor shall perform and complete such refreshes within 5 business days.

9 Exit Strategy

9.1.1 Upon contract termination for any reason, Vendor shall provide District with a current copy of Production data. The data shall be in a format specified by District.

9.1.2 Subsequent to providing District with a current copy of Production data, Vendor and all of its subcontractors will securely destroy all copies of District data upon contract termination and attest to this destruction.

9.1.3 If the vendor goes out of business or ends support for the product used by District, the District must have access to the source code so that District can continue to maintain the system and function. Source code escrow is mandatory.

10 Preliminary Security Information Gathering (PSIG)

10.1.1 As a component of the supplemental RFP process, the District will be performing a qualifying evaluation of each of the RFP respondents Information Protection program.

10.1.2 Vendor shall complete the Preliminary Security Information Gathering (PSIG) document in Attachment C of this RFP document.

11 Technology Stack

11.1.1 General - The system must be web enabled and have web access to 100% of its functionality. The system, including the software, architecture and environment, must use modern technology that meets accepted industry standards and best practices. The system should provide tools for monitoring the system health and performance. The technology stack to support the system will be made up of the following parts:

10.1.2 Operating System – The system shall be required to run on an operating system that is designed for enterprise applications and it must be patchable and maintainable into the future. The OS must be in a current maintenance and release cycle. The system will be required to run on District acceptable versions of Windows Server or Red Hat Linux. Other operating systems may be considered at the District's discretion.

10.1.2 Web Server – The web server must be a current and supported release of Apache or Microsoft IIS. Other web servers may be considered at the District's discretion.

10.1.3 Database – The database must be an Oracle enterprise relational database system and must be in a current maintenance and release cycle compatible with the District's current versions (Oracle 9, 10g, 11g, 12c). Other database systems may be considered at the District's discretion.

10.1.4 Programming Language – The programming language must be a modern web enabled programming language that is either object oriented or object based. The list includes but is not limited to Ruby, Java, Python, PHP, JavaScript and C #. Other programming languages may be considered at the District's discretion.

10.1.5 Reporting Engine –Reporting engines must be approved as functionally and technically robust by the District. Elements to the reporting engine include but are not limited to the following:

11.1.1.1 Usability – A non-technical user should be able to create reports and dashboards with a short learning curve. Reports shall be exportable to Microsoft Excel, .pdf, and .csv formats.

11.1.1.2 Web access – The reporting engine should allow users to output to the web for easy access to all users within the District.

11.1.1.3 Dashboards – The reporting engine shall allow for the creations of dashboards to efficiently provide graphical representations of key CMMS attributes including but not limited to the following:

11.1.1.3.1 Open work orders

11.1.1.3.2 Work order counts based on status

11.1.1.3.3 Shop

11.1.1.3.4 Application

11.1.1.3.5 Individual backlog

11.1.1.3.6 Measurable Asset Characteristics (MAC)

11.1.1.3.7 Location

12 Appendix A

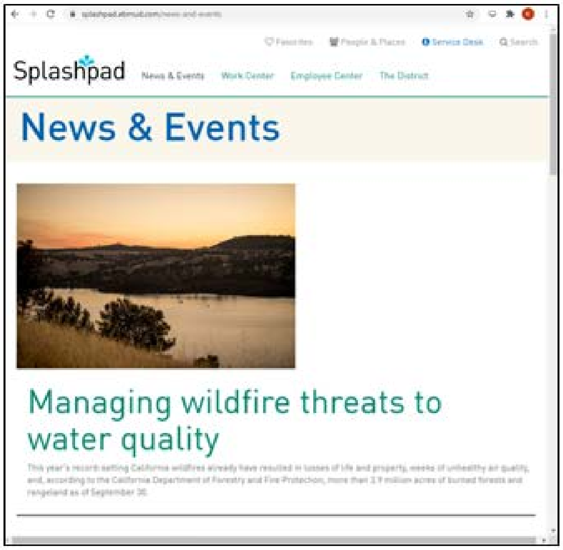
12.1 High level List

The table below provides a list of applications/vendors that may need to interface with the new CMMS:

Current Systems		
System Name	**Description**	**Interface Types**
Concrete5 CMS	Website CMS	Web Service API
Customer Watch	Customer Billing/Information System	Web Service API (work orders originate in CW)
DOCS	Document Management	Page links with parameters
Electronic Timesheets	Timesheet/Time Tracking	Flat File (ability to charge time by order numbers)
PeopleSoft HRIS	Human Resources	Flat File
Oracle Fusion ERP Financial (Future System)	Financial ERP System (There is an active project to replace the current FIS and MMIS system)	Web Service API
PI	Plant Historian Database	Web Service API
PIMS	Pretreatment Information for Wastewater	Flat File
Sedaru	GIS Based tool managing outages for Operations and Maintenance	Web Service API
Single Sign On	CAS/SAML Sign On Protocols	Web Service API
System Water Quality	Water Quality Application Reporting Tool	Flat File
Truck Track	Internal Waste Load Tracking for Main WWTP	Flat File
WTRM	Water Treatment Report Manager Reporting Tool	Flat File
WQDB	Water Quality Database Reporting Tool	Flat File
InfoNet (Innovyze)	Provides contractors and operators a Central Hub for routine and reactive maintenance	Web Service API Flat File
GIS	GIS Mapping Software (ESRI 10.7.1)	Web Service API
Inventory/Purchasing	New Purchasing System, SaaS	Web Service API
Main Break Viewer (Current system)	Public alert application	Web Service API
Public Alerts (Current system)	Public alert application	Web Service API
Outage Map (Future System)	CSSP Project involved with public alerts (There is an active project to replace the current public alert application)	Web Service API

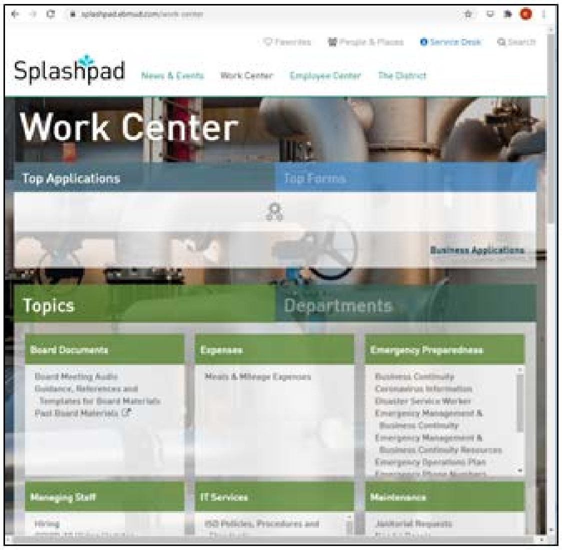
13 Appendix B

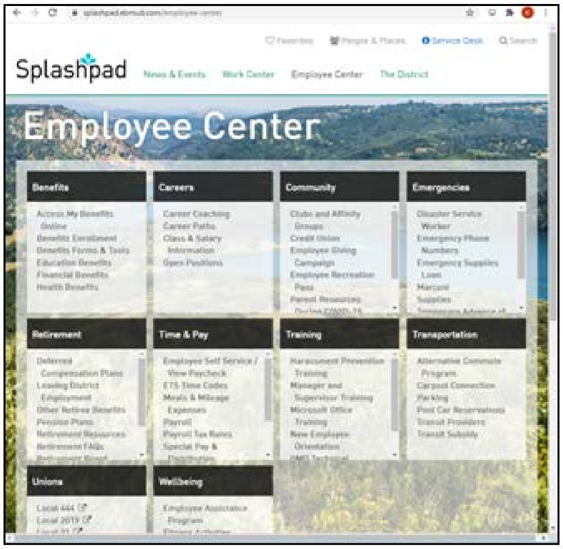
13.1 Splashpad alternate screens screenshots

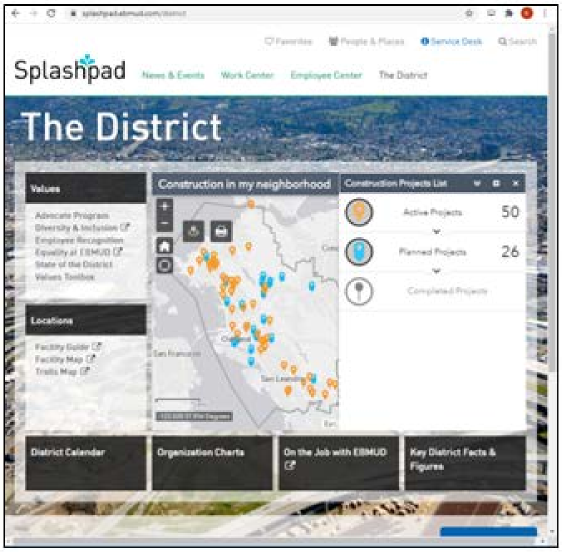


Managing wildfire threats to water quality

This year's record-setting California wildfires already have resulted in losses of life and property, weeks of unhealthy air quality, and, according to the California Department of Forestry and Fire Protection, more than 3.9 million acres of burned forests and rangeland as of September 30.


splashpad.ebmud.com/work-center
Favorites
People & Places
Service Desk
Search
Splashpad
News & Events
Work Center
Employee Center
The District
Work Center
Top Applications
Top Forms
Business Applications
Topics
Departments
Board Documents
Board Meeting Audio
Guidance, References and Templates for Board Materials
Past Board Materials
Expenses
Meals & Mileage Expenses
Emergency Preparedness
Business Continuity
Coronavirus Information
Disaster Service Worker
Emergency Management & Business Continuity
Emergency Management & Business Continuity Resources
Emergency Operations Plan
Emergency Phone Numbers
Managing Staff
Hiring
IT Services
ISO Policies, Procedures and
Maintenance
Janitorial Requests


splashpad.ebmud.com/employee-center
Favorites
People & Places
Service Desk
Search
Splashpad
News & Events
Work Center
Employee Center
The District
Employee Center
Benefits
Access My Benefits Online
Benefits Enrollment
Benefits Forms & Tools
Education Benefits
Financial Benefits
Health Benefits
Careers
Career Coaching
Career Paths
Class & Salary Information
Open Positions
Community
Clubs and Affinity Groups
Credit Union
Employee Giving Campaign
Employee Recreation Pass
Parent Resources
During COVID-19
Emergencies
Disaster Service Worker
Emergency Phone Numbers
Emergency Supplies Loan
Marconi Supplies
Temporary Advance of
Retirement
Deferred Compensation Plans
Leaving District Employment
Other Retiree Benefits
Pension Plans
Retirement Resources
Retirement FAQs
Retirement Board
Time & Pay
Employee Self Service / View Paycheck
ETS Time Codes
Meals & Mileage Expenses
Payroll
Payroll Tax Rates
Special Pay & Classification
Training
Harassment Prevention Training
Manager and Supervisor Training
Microsoft Office Training
New Employee Orientation
OMS Technical
Transportation
Alternative Commute Program
Carpool Connection
Parking
Pool Car Reservations
Transit Providers
Transit Subsidy
Unions
Local 444
Local 2019
Local 21
Wellbeing
Employee Assistance Program
Fitness Activities


splashpad.ebmud.com/district
Favorites
People & Places
Service Desk
Search
Splashpad
News & Events
Work Center
Employee Center
The District
The District
Values
Advocate Program
Diversity & Inclusion
Employee Recognition
Equality at EBMUD
State of the District
Values Toolbox
Locations
Facility Guide
Facility Map
Trails Map
Construction in my neighborhood
San Francisco
Oakland
San Leandro
Construction Projects List
Active Projects 50
Planned Projects 26
Completed Projects
District Calendar
Organization Charts
On the Job with EBMUD
Key District Facts & Figures