EAST BAY
MUNICIPAL UTILITY DISTRICT

Private Sewer Lateral System (PSL)

Technical Requirements

March, 2023

Private Sewer Lateral System (PSL) Technical Requirement

Definitions

District	East Bay Municipal Utility District (EBMUD)
Cloud-based Services	Applications, services, or resources made available to users external to the EBMUD business network via the Internet.
Vendor	A software vendor is a company that develops and sells software
System	The software solution including licenses and configurations which meets all defined requirements or an agreed upon subset of requirements.
PSL	Private Sewer Lateral System the requirements for which are specified in this document; also referred to as 'System'

Personally Identifiable Information (PII)	PII includes data related to customers and employees that would reasonably be considered private or has been specifically defined as private under state or federal laws. Data types that constitute PII include (but are not limited to):
	• An individual's first initial and last name, or first name and last name, with:
	  • Social security numbers, or portions thereof
	  • Driver's license numbers
	  • Financial account numbers (e.g., credit card numbers, bank accounts, etc.)
	• Online account usernames and passwords
	• Information related to specific customer accounts (water consumption, account numbers, financial data, phone numbers, home address, etc.)
	• Personnel records (birthdates, home address, phone numbers, etc.)

PCI DSS	Payment Card Industry Data Security Standard

1 System Security / Authentication

1.1 Single Sign-On

1.1.1 The System shall use the District's Single Sign-On Architecture (SSO) - Microsoft Azure AD for the District internal users.

1.1.2 The System shall support a configurable session timeout. Users shall be required to reauthenticate upon session expiration.

1.1.3 Customer Self-service portal shall give customers the ability to: learn about program requirements, request certificates, check on compliance status, pay program fees, and schedule sewer lateral inspections. The System shall offer a self-service portal that supports web browser and mobile devices for all features and functionality defined in functional requirements.

- The System shall not require authentication for customers using the customer self-service portal for certain actions (i.e., some functions are public including but not limited to view outstanding fees, submit requests, print, and or download program information). Customer authentication shall not tie to the District SSO.
- The System shall provide customers with a tool or mechanism for submitting supporting documentation to PSL Program staff through a secure portal.
- The System shall require a simple sign in process to schedule or reschedule an inspection appointment.

1.2 Encryption

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

1.2.2 The System shall strongly encrypt all data in transit (during transactions) and at rest (in the database). For data at rest, AES-256 or a cipher with equivalent or greater cryptographic strength is required.

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

1.2.4 The Vendor shall test their application web interface with ssllabs.com (free tool from Qualys) to confirm their web server is configured securely. Site shall have an A grade for security.

1.2.5 The System shall protect all stored PII information in compliance with all federal, state laws and sector-specific regulations, common law principles, and self-regulatory programs developed by industry groups that regulate the collection, use, processing, and disclosure of PII include but not limited to Consumer protection laws such as the Federal Trade Commission Act (FTC Act), which are used to prohibit unfair or deceptive trade practices involving the collection, use, processing, and disclosure of PII. Some of the laws that apply to specific sectors are:

- Gramm-Leach-Bliley Act (GLBA), which applies to financial institutions
- Health Insurance Portability and Accountability Act (HIPAA), which applies to health care and health plan information.
- Laws that apply to types of activities affecting individual privacy are the following:
    - Telephone Consumer Protection Act (TCPA), applies to telemarketing activities
    - Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM), applies to commercial emails
    - Children's Online Privacy Protection Act (COPPA), which applies to the online collection of information from children under 13
    - Fair Credit Reporting Act (FCRA), which applies to consumer credit and other information; and
    - Electronic Communications Privacy Act (ECPA) and the Computer Fraud and Abuse Act (CFAA), which regulate electronic communications and unauthorized computer use

1.3 **Role-based User Access**

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

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

1.3.3 The System shall provide configuration tools for the District staff to assign and modify users to and from different roles. The 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.

1.4 Application Design

1.4.1 The System shall be designed, developed, deployed, and tested in accordance with and up to industry standards including but not limited to Open Web Application Security Project (OWASP) security principles.

1.5 Audit Trails and Logging

1.5.1 The System shall provide logging for all events, activities, and transactions including but not limited to user activities, internal system activities, scheduled jobs, API calls, interfaces, file transfers, warnings, errors, etc.

1.5.2 Audit trail shall track Date and Time stamp, operator identification and link to Record. Audit trails shall be human readable and shall support user friendly searching, sorting, and filtering functionality.

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

1.5.4 Audit trail data shall not be editable by any user.

1.6 Cloud-based Services

1.6.1 Cloud-based services will comply with accepted industry standards and best practices.

1.6.2 The Vendor shall provide the following details regarding Cloud service ownership:

- Whether the cloud service is public or private.
- If public cloud, how will the Vendor protect each customer's data from access by another customer in the shared environment?
- If private cloud, is it hosted on District-managed hardware or Vendor-managed hardware?
- If the District is asked to host a cloud service on hardware the District manages, what kind of access will the Vendor require including authentication and firewall access?
- Whether the cloud offering is public or private, determine what access privileges will be available to the District IT Systems staff.
- If the Vendor is not the owner of the cloud Infrastructure, who is hosting the infrastructure? How many data centers are in use, and what are their locations?

1.6.3 Cloud-based services, including third party integration if applicable, shall comply with all relevant security standards including ISO/IEC 27001:2013, PCI DSS and NIST 800-53. Ancillary utilities shall be available from the ACH API to make calls for anti-fraud and risk mitigation.

1.6.4 The Vendor shall provide an annual SSAE-18 SOC2 report written by an independent auditor, validating the security controls of the physical, logical, and application environments. This shall include operational procedures that the Vendor is responsible for to manage environments in the public cloud. The Vendor shall continuously monitor the System to timely detect unauthorized activities. The Vendor shall immediately notify the District of any suspected or confirmed security breach and shall take immediate action to remedy such breach.

1.6.5 Cloud-based services shall be available 24 hours per day, seven days per week.

1.6.6 Cloud-based services shall have a 99.9% or better uptime.

2 Usability

2.1 System Performance/Availability

2.1.1 The System shall be available to the District 24 hours a day, 7 days a week.

2.1.2 The System shall provide 99.9 percent availability, including planned outages.

2.1.3 The Vendor shall monitor software application performance to ensure an expected level of service, as measured by performance metrics and user experience. The Vendor shall detect and pinpoint application performance issues before real users are impacted. The Vendor shall promptly notify the District of any outages, degraded performance, or other operating conditions that may adversely affect District operations. Such notifications shall include an estimated time for restoration of normal operating conditions. For incidents lasting longer than 1 hour, the Vendor shall send the District periodic updates. The Vendor shall promptly notify the District when normal operating conditions are restored.

2.1.4 The Vendor shall provide a Service Level Agreement (SLA) that specifically identifies the System uptime and performance guarantees as delineated in this document.

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

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

2.2 Accessibility

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

2.2.2 The System shall be accessible from current versions of Edge, Chrome, Firefox, Safari, and any other commonly used web browser.

2.2.3 The System shall be compliant with Section 508 of the Rehabilitation Act of 1973, the Americans with Disabilities Act, and any other applicable law and regulation. The System shall have any website or web-based tool meet WCAG 2.0 AA or above level compliance.

2.2.4 The System shall support internationalization (I18N).

2.3 **Design**

2.3.1 The System shall incorporate well established User Interface patterns to facilitate a good user experience, e.g., provide tips for form fields, drop down menus for fields, and incremental search for users who may not know the correct terminology to type in, etc.

2.3.2 The System shall have the ability to match EBMUD.com's look and feel.

2.3.3 The System shall have the ability to modify its look and feel to match EBMUD's look and feel, should EBMUD's look and feel change.

2.3.4 The System shall use responsive Web Design so that the solution displays and functions well on mobile devices.

2.3.5 The System shall have the ability to sign into the System from the EBMUD.com home page.

2.4 **Scalability / Flexibility**

2.4.1 The District user profile for the System will likely change in the future.

- The System shall accommodate a minimum of 30 concurrent users and be flexible with increasing the number up to 50 without any degradation in performance.
- The System has at least 60000 visitors per year and issues at least 5500 certificates with increases of up to 4% projected each year. As of last year, there's over 600 visits to customer portal eastbaypsl.com each day. The System shall accommodate these without any degradation in performance.
- The System shall perform at its optimal level 24 x 7 and accommodate peak usage (7am – 7pm Pacific Time Monday-Friday) without any degradation in performance.
- The System shall accommodate interactions with the District's new systems through standard interfaces (details below in section Interfaces and Integrations).

2.4.2 The System shall accommodate a phased approach to implementation defined by the District without major system re-configuration or extended system down time.

2.5 Online Help and Database Schema

2.5.1 The System shall provide multiple methods of online, interactive help including but not limited to context-sensitive, topical searches of documentation, reference documents, tutorial videos, and specific, clear, non-technical error messages.

2.5.2 The Vendor shall provide documentation for the database including schema and data model.

2.6 Web Analytics to Measure Customer Engagements

The System shall utilize Web Analytics tools and monitor system performance. Performance shall be measured in a meaningful way and reported to the District monthly.

2.6.1 For each functionality, record:

- Page Hits
- Time it takes to complete the functionality.
- Time spent on each web page in the functionality.
- Visitor Flow Path to get to the functionality. I.e., the web pages the customer visited before executing a functionality.
- Abandonment rate and a list of pages on which a visitor abandoned a process.

2.7 Mobility

2.7.1 The District requires that all mobile functions are accomplished in a web browser, not an App. The System shall be mobile friendly, and no app download required for customer booking inspection appointment and pay fees through mobile device.

2.7.2 The System shall provide access to all major functions through a mobile device web browser running on Android, Windows, or iOS operating systems. Please state which kinds of devices and browser the System supports.

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

2.7.4 The System shall use responsive, mobile-friendly user interface.

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

2.7.6 Mobile devices shall have ability to store data offline and upload automatically when connection is available.

2.7.7 The System shall be able to send text messages to mobile devices. The System shall be able to configure the text message with embedded web page links.

2.7.8 The Vendor shall provide and maintain a list of supported mobile operating systems and browsers.

2.8 Communications

2.8.1 The System shall utilize internet standard communication protocol for electronic mail and text transmission.

3 Interfaces and Integrations

3.1 **The District utilizes numerous custom-built, commercial off-the-shelf, 3rd party, and cloud-based software solutions. The System will need to exchange data with these applications in batch or real time. The System shall provide standard interfaces to the District's existing and future systems/applications for incoming and outgoing data. A brief description of some of the applications/vendors with which the System may need to interface is included in Appendix A.**

3.1.1 The System shall use standard interface technologies to exchange data with other applications. This includes but is not limited to JSON for data exchange, REST as messaging design, industry-standard web services with HTTPS, and secure bi-directional file transfer via SFTP. The System shall support REST API with HTTPS from single source IP. The Vendor shall develop and support API and all the selected methods.

3.1.2 The System will provide a central location for all data to be consumed by existing and future EBMUD systems/applications. The Vendor shall provide an SFTP server for bi-directional file transfers for this purpose. The System will validate all outgoing data prior to placement in the central location.

3.1.3 The System will provide the ability to call web service APIs with HTTPS to consume data from EBMUD systems and applications.

3.1.4 The System shall encrypt all data that traverses public computer networks and protect that data from fraudulent activity, unauthorized disclosure, or modification.

3.1.5 The System shall provide logging with sufficient details to facilitate troubleshooting of interfaces.

3.1.6 The System shall have geospatial functionalities which can display APN parcel data, utility data, and PSL inspection data by parcel on geospatial maps. The District utilizes ArcGIS Server software (version 10.9.1) from ESRI.

3.1.7 The Vendor shall have strong experience with ERP integration and close partnership with Oracle Fusion ERP system. The District utilizes the Oracle Fusion Cloud Financial system (ERP)—"Elsie". The Vendor should be familiar with ERP data importing and exporting utilities.

- The System shall interface with current release of Oracle Fusion Cloud Financials and update accounting information from PSL in a defined schedule (i.e., nightly, weekly, or immediately)
- The Vendor shall develop the interface with Elsie per functional requirements. The Vendor shall develop an automated process to import data to Elsie daily from the System.
- The Vendor shall generate a file in the format of Oracle's import template (Appendix C is an example: 06_PSL_TECH_APP_C_JournalImportTemplate.xlsm) with PSL data mapped to Elsie data for the District to download from a designated SFTP location or District internal network The Vendor shall have good knowledge of ERP data model and be able to map PSL data with ERP as required in Oracle import template.
- The Vendor should develop reports with data from multiple sources - Cloud applications and internal data sources including the System, Elsie, District APN database, or third-party software etc. in real time with Secured Webservice API.
- The Vendor should be able to extract data in a format (i.e., csv or SQL statement) can be consumed by EBMUD applications or databases.
- The Vendor shall provide detailed event log file accessible by the District.
- The System shall call the Oracle API from known static IP address. No dynamic IP shall be used.
- Intermedia data should not be saved outside of PSL. Temporary data should be cleared up once transaction is validated, committed, logged, and done.

3.1.8 The District utilizes DocuSign Enterprise/Business version software-as-a-service (SAAS). The System shall have integration or ability to integrate with current release of DocuSign for web browser and mobile device.

3.1.9 The System shall be able to query the District APN parcel database with REST API.

3.1.10 To facilitate the District customers in applying payments both from the web site or a mobile device, including via ACH, Authorize.net or a third party, the System shall follow Micro-Entries rules, which are used by some ACH Originators as a method of account validation. The System shall meet all PCI compliance standards.

- The System shall integrate with the latest release of ACH on web browsers and mobile devices.
- The System shall integrate with latest release of Authorize.net both on web browsers and mobile devices.
- The Vendor shall provide seamless transactions utilizing Authorize.net SDKs, or other method approved by the District.
- The Vendor shall provide the resources to design, implement, and support EBMUD's look and feel on the frontend web pages and mobile devices including payment web site of any third party.

3.1.11 The System shall be able to consume data and export data in file formats including, but not limited to the following: Adobe PDF, CSV, HTML/XML, MS Access, MS Excel, MS Word. The System shall be able to edit documents in MS Word.

3.2 **The District-preferred methods of data exchange are listed below in the order of higher to lower preference:**

3.2.1 REST services using HTTPS.

3.2.2 Flat file – the data in the file will be encrypted both in transit via SFTP and PGP at rest.

3.3 **For new and existing interfaces, the Vendor shall provide specifications including but not limited to the following within the District timeline specified in the functional requirements:**

3.3.1 Authentication and authorization

3.3.2 Data fields, data types, source system, and destination systems

3.3.3 Frequency

3.3.4 Communication protocol

3.3.5 How interface errors and recovery are handled

3.3.6 How transactions are logged

3.3.7 SLA requirements for incoming and outgoing interface transactions.

3.3.8 All web service API documentation

4 Data Management

4.1 Data Security

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

4.1.2 The System shall retrieve Personally Identifiable Information (PII) only on an as-needed basis using the District-specified interfaces. System shall not store PII unless authorized by the District in writing.

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

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

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

4.1.6 The Vendor shall create a Data Management plan and review it with the District annually.

4.2 Archiving Data

4.2.1 The System shall provide mechanisms for the archival of PSL data to external storage for access, deletion, and auditing; and retain it for a minimum of 12 years. Such storage shall be immutable, and no changes can occur. Records are readable and accessible for authorized users. A file can be read as many times as necessary, but it cannot be overwritten, deleted, or modified in any way. Both content and indexes shall be maintained with replicas. Archived data or documents shall be able to migrate/import/export.

4.2.2 The Vendor shall provide a full database export once a month that can be imported into the District's Oracle database. The Vendor shall place database backup file in a secure location and grant the District access to download.

4.2.3 The System will have configurable data archive (online) criteria.

4.2.4 The System will have a configurable data archive (online) schedule.

4.2.5 The System will have configurable rules for data purging.

4.2.6 The System will retain data up to a configurable number of years.

4.3 Data Availability

4.3.1 All data entered or uploaded into the System shall remain the property of the District and shall not to be disclosed or used without the District's written permission.

4.3.2 The System shall be able to associate data to predefined retention schedules. Retention schedules shall be permanently tied to the data but a retention schedule, itself, can be subject to change.

4.3.3 The Vendor shall grant the District technical staff read-only access to the System's database to query data.

5 Business Continuity and Disaster Recovery

5.1 The Vendor shall provide a Business Continuity and Disaster Recovery plan.

5.2 The System shall provide full data back-ups on a predetermined schedule.

5.3 The System shall provide recovery capabilities with data recovery back as soon as possible but no more than 12 hours.

5.4 The System shall be able to recover all committed transactions as of the time point immediately preceding the disaster and no more than 15 minutes.

5.5 The System shall have its business continuity plan tested at a minimum of once a year. The Vendor shall specifically test its ability to restore the System data from backups no less than annually.

6 Patches and Releases

6.1 The Vendor shall provide at least 10 days advance notice for minor changes and 30 business days for major changes and releases/patch release. The Vendor shall coordinate with the District to deploy changes and current production data to test instances specified by the District.

6.2 The Vendor shall perform system maintenance and upgrades outside of business hours (business hours: 7am – 5pm Pacific Time Monday through Sunday, 7 days a week including holidays) e.g., weekend nights. The Vendor shall notify the District at least 10 business days in advance for system offline maintenance.

6.3 The Vendor shall provide at least 8 weeks for testing and training for every major system upgrade.

6.4 The Vendor shall provide the option to opt out of software upgrades.

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

6.6 The Vendor shall notify the District at least 90 business days in advance of any changes which will potentially affect APIs or require the District to modify its interfaces. All such notifications shall be accompanied by documentation describing the changes, the affected APIs and interfaces, and suggested solutions.

6.7 The Vendor shall provide options to go back to the previous version of the System if issues are encountered in the new upgrade.

7 Implementation Plan and Schedule

7.1 Implementation Approach

7.1.1 **Standard Implementation** – The Vendor shall provide their standard Implementation plan and schedule that fulfills all functional and technical requirements set forth in this document.

7.1.2 **Phased Implementation** – The Vendor shall be flexible for a phased implementation plan and schedule for phases in the various integration components with the District's applications based on functional requirements. This allows the District to get core functionality sooner and not wait for all the integrations to happen in order to start using the Vendor solution. Potential phases include but are not limited to:

- Core functionalities:
  - Configuration of the Software.
  - Integrations with geospatial maps and the District APN database.
  - Integration with District's Single Sign-On.
  - Mobile device setup.
  - Integration with ACH and Authorize.net.
  - Integration with Oracle Fusion Cloud Financial system (ERP)—"Elsie"
  - Historic PSL Data Migration from current PSL system.
- Integrations with the District systems including SharePoint and ERP.
- Migration of all the District historical PSL documents not stored in the current PSL system, e.g., on network drives, into the System.
- Potential other system integrations.

7.2 **Implementation methodology**

7.2.1 Agile development process by the Vendor is required so that the District can get frequent deliverables weekly or bi-weekly for testing. This shortens the feedback cycle and helps detects major problems and issues sooner in the project.

7.3 **Data Migration**

7.3.1 The Vendor shall migrate all historical data including documents from the current PSL system to the new system and validate all the migrated data. Table and field name details are attached in Appendix B.

7.3.2 The System shall provide service to migrate historical documents from external storage including those stored on network drives in formats of PDF, MS Word, MS Excel, etc. into the new system.

7.3.3 The Vendor shall support the District's use of third-party ETL tools or other automated tools as necessary.

7.4 Development, Test, Training, and Staging Instances

7.4.1 The Vendor shall provide the below instances during the implementation period as well as post go-live for the life of the contract. Each instance shall include all required components, such as application servers and databases, add-ons, and current data sets for periodic and ongoing system upgrades and testing.

- The Vendor shall provide a development instance in order to do software development and unit testing.
- The Vendor shall provide a test instance to verify patches and upgrades and perform user testing before implementation in production.
- The Vendor shall provide a training instance to allow the District staff to train on the System.
- The Vendor shall provide a staging instance to allow the District to test integrations with other applications. The staging environment shall be as similar as possible to the production environment.

7.4.2 The System will support scripted configuration moves, allowing automated transfer from one environment to another or from the configuration repository.

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

7.4.4 Upon request by the District, the Vendor shall add or delete instances with 30-day notice without affecting the production system. The Vendor shall update and perform testing as required. Examples of updates are stopping scheduled jobs and email notifications, changing user permission, etc.

8 Exit Strategy

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

8.2 After providing the District with a current copy of Production data, the Vendor and all its subcontractors will securely destroy all copies of the District data within 30 business days and attest to this destruction. A written attestation of data destruction from the Vendor is required.

8.3 If the Vendor goes out of business or ends support for the product used by the District, the Vendor shall provide information required to set up the system and its environment from scratch, including but not limited to, source code, configurations, data, documentation (installation and operation), production database export, etc. The District shall have access to all information for

maintaining the System and its functionality. It is mandatory that the Vendor set up escrow for this and keep the contents of escrow up to date with the current release. The Vendor shall notify the District by email when code or other material is updated in escrow. The District may periodically modify the list of parties to be notified.

8.4 The Vendor shall provide service and support to the District to migrate all PSL data to a new destination shall the District decide to switch to a different product. The Vendor shall provide the service and support for no less than 90 days for the District to complete data migration.

8.5 The Vendor shall keep escrow updated after each patch release.

9 Preliminary Security Information Gathering (PSIG)

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

The Vendor shall complete the Preliminary Security Information Gathering (PSIG) document in Attachment C of PSL RFP package.

10 Technology Stack

General - The System shall be web enabled and have web access to 100% of its functionality. In case any functions perform better with external installations, or additional software/add-on is required to be installed in the local PC, or additional hardware/instrument is required, the Vendor shall list upfront any solution components that the District needs to purchase, host, or install. The Vendor shall provide detailed information for the functionalities of each component and system requirement including, but not limited to software versions, hardware manufacturer and model, and network requirement for all components. Data flow/communication between each component shall all be secured and clearly explained.

The System shall be HTML5 compliant and support all modern browsers in current release cycles, including Microsoft Edge, Chrome, Firefox, and Safari. The System, including the software, architecture, and environment, shall use modern technology that meets accepted industry standards and best practices. The technology stack shall be able to function on VMWare VCenter. The System shall provide tools for monitoring the System health and performance. The technology stack to support the System will be made up of the following parts (Please state your solution support for each requirement in the RFP Excel Response Spreadsheet):

10.1 Operating System – The System shall run on an operating system that is designed for enterprise applications, and it shall be patchable and maintainable into the future. The OS shall be in a

current maintenance and release cycle for both web and mobile devices. The System will be required to run on Windows Server 2022 or newer or Red Hat Linux Release 8.x or newer, or current release of iOS. Other operating systems may be considered at the District's discretion. OS shall be under mainstream support by the OS vendor.

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

10.3 Database – The database shall be an enterprise relational database system of type Oracle or Microsoft SQL Server and shall be in a current maintenance and release cycle (Oracle 19c or above, SQL Server Std 2019 version 15 or above). Other database systems may be considered at the District's discretion and shall be under mainstream support by database vendor.

10.4 Programming Language – The programming language shall be a modern web enabled programming language that is either object oriented, or object based. The list includes Ruby, Java, Python, PHP, JavaScript, and C#. Other programming languages may be considered at the District's discretion.

10.5 Reporting Engine – The reporting engine shall be modern, flexible, and robust. Acceptable reporting engines are Crystal Reports and Jasper, or similar as approved by the District. Custom reporting engines shall be approved as functionally and technically robust by the District.

- Report engine shall allow automatic report generation and distribution based on a schedule (Daily, Monthly, Weekly, etc.). Distribution methods include but are not limited to email or saving to an EBMUD network location.
- Reports shall be exportable to common formats including PDF, CSV, and MS Excel.
- Report should be able to access from multiple data sources. i.e., third-party cloud solutions, District internal data sources.

10.6 Ad hoc reporting tool – the System shall provide reporting tools that are easy to use by non-technical users. Access to run or configure reports shall be based on user roles.

10.7 Whitelisting – the System shall support IP whitelisting so people outside of the United States can't access the System. The Vendor is required to use only staff and systems based in the United States.

By signing below, I acknowledge that I have read and understand the requirements as set forth in this document. My signature also certifies that documentation will be provided wherever the System does not fully meet any of the requirements set forth in this document.

_____

Print Name

_____ _____

Sign Name Date

11 Appendix A.

The table below lists all systems that the PSL will need to integrate with at the discretion of the District:

Current Systems				
System/Integration Name	**Description**	**Interface Type**	**Location**	**Must have/ Nice to have**
Single Sign On	Azure AD Sign On Protocols	REST Web Service API	Cloud	Must have
DocuSign	System used to obtain digital signatures for external legal documents. https://account.docusign.com/	REST Web Service API	Cloud	Must have
APN	EBMUD District Enterprise Parcel database (custom-built, on-premises)	REST Web Service API	On Premises	Must have
ACH	Application Programming Interface which allows debiting and crediting of checking and savings accounts via the ACH network.	REST Web Service API	Cloud	Must have
Authorize.net	Third-party payment processing system, manually, on your website, or through a mobile app.	REST Web Service API	Cloud	Must have
Elsie (Financial System)	Financial System with Oracle Fusion Cloud (ERP)	Web Service API or XSLM file	Cloud	Must have
SharePoint	Microsoft SharePoint	Web Service API	Cloud	Nice to have

12 Appendix B.

Inspection_laterals:

COLUMN_NAME	DATA_TYPE
PSL_INSP_RESULTS_NUM_GN	NUMBER
PSL_LAT_CD_NUM	NUMBER
PSL_LAT_NUM	NUMBER
PSL_LAT_INSP_LAT_LEN_FT	FLOAT
PSL_LAT_INSP_PIPE_DIA_IN	FLOAT
PSL_INSP_STNDPIPE_HGT_IN	FLOAT
PSL_RPLC_CD_NU	NUMBER
PSL_PIPE_MAT_NU	NUMBER
PSL_RPLC_MTHD_CD_NU	NUMBER
PSL_OLD_MAT_CD_NU	NUMBER
PSL_GG_AUDIT_CD_NU	NUMBER
PSL_SETUP_RESULTS_CD_NU	NUMBER
PSL_CONN_CD_NU	NUMBER
PSL_LWR_CLNOUT_CD_NU	NUMBER
PSL_TEST_TYPE_NU	NUMBER
PSL_LAT_INSP_ST_PSI_NU	FLOAT
PSL_LAT_INSP_END_PSI_NU	FLOAT
PSL_WTR_LOSS_CD_NU	NUMBER
PSL_RESULTS_CD_NU	NUMBER
PSL_LAT_INSP_VER_NU	NUMBER
PSL_LAT_INSP_CMNT_TX	VARCHAR2(4000 BYTE)
ROW_CREATN_DM	TIMESTAMP(6)
ROW_MOD_DM	TIMESTAMP(6)
ROW_MOD_BY	VARCHAR2(10 BYTE)

Certificates:

COLUMN_NAME	DATA_TYPE
PSL_CERT_GN	NUMBER
APN_DATA_APN_TX	VARCHAR2(32 BYTE)
APN_ADDR_BLDG_NU	NUMBER
APN_ADDR_FRACT_NU	VARCHAR2(3 BYTE)
APN_ADDR_PFIX_CD	VARCHAR2(2 BYTE)
APN_ADDR_ST_NM	VARCHAR2(25 BYTE)
APN_ADDR_SFIX_CD	VARCHAR2(4 BYTE)

COLUMN_NAME	DATA_TYPE
APN_ADDR_APT_NU	VARCHAR2(10 BYTE)
CITY_NM	VARCHAR2(20 BYTE)
APN_ZIP_CD	VARCHAR2(5 BYTE)
PSL_CERT_TYPE_CD	NUMBER
PSL_PYMT_NU	NUMBER
PSL_CERT_ISSUE_DM	TIMESTAMP(6)
PSL_CERT_EXPIR_DM	TIMESTAMP(6)
PSL_CERT_CLAWBACK_EXPIR_DM	TIMESTAMP(6)
PSL_CERT_CMNT_TX	VARCHAR2(4000 BYTE)
PSL_CERT_VER_NU	NUMBER
ROW_CREATN_DM	TIMESTAMP(6)
ROW_MOD_DM	TIMESTAMP(6)
ROW_MOD_BY	VARCHAR2(10 BYTE)

Inspections:

COLUMN_NAME	DATA_TYPE
PSL_INSP_RESULTS_NUM_GN	NUMBER
PSL_INSP_RESULTS_INSPCTR_ID_NU	NUMBER
APN_DATA_APN_TX	VARCHAR2(32 BYTE)
PSL_APN_TYPE_CD	NUMBER
PSL_INSP_RESULTS_TEST_DM	TIMESTAMP(6)
PSL_TEST_TYPE_NUM	NUMBER
PSL_CONN_CD_NU	NUMBER
PSL_INSP_RESULTS_LEN_FT	FLOAT
PSL_INSP_RESULTS_START_PSI_NU	FLOAT
PSL_INSP_RESULTS_END_PSI_NU	FLOAT
PSL_INSP_PIPE_DIA_IN_NU	FLOAT
PSL_PIPE_MAT_NU	NUMBER
PSL_WTR_LOSS_CD_NU	NUMBER
PSL_SETUP_RESULTS_CD	NUMBER
PSL_RESULTS_CD	NUMBER
PSL_INSP_CTRTR_LCNSE_TX	VARCHAR2(32 BYTE)
PSL_INSP_RESULTS_TESTER_TX	VARCHAR2(32 BYTE)
PSL_INSP_RESULTS_TESTER_PH	VARCHAR2(32 BYTE)
PSL_RPLC_CD	NUMBER
PSL_GG_AUDIT_CD_NU	NUMBER

COLUMN_NAME	DATA_TYPE
PSL_INSP_RESULTS_CMNT_TX	VARCHAR2(4000 BYTE)
PSL_INSP_RESULTS_SUBMT_FG	NUMBER(10,0)
PSL_INSP_RESULTS_SPARE1_TX	VARCHAR2(64 BYTE)
PSL_INSP_RESULTS_SPARE2	VARCHAR2(4000 BYTE)
PSL_INSP_RESULTS_VER_NU	NUMBER
ROW_CREATN_DM	TIMESTAMP(6)
ROW_MOD_DM	TIMESTAMP(6)
ROW_MOD_BY	VARCHAR2(10 BYTE)
PSL_INSP_RESULTS_UL_LEN_FT	FLOAT
PSL_INSP_RESULTS_LL_LEN_FT	FLOAT
PSL_INSP_RESULTS_TL_LEN_FT	FLOAT
PSL_UL_TEST_TYPE_NU	NUMBER
PSL_TLLL_TEST_TYPE_NU	NUMBER
PSL_INSP_RESULTS_UL_ST_PSI_NU	FLOAT
PSL_INSP_RESULTS_UL_END_PSI_NU	FLOAT
PSL_UL_WTR_LOSS_CD_NU	NUMBER
PSL_TLLL_ST_PSI_NU	FLOAT
PSL_TLLL_END_PSI_NU	FLOAT
PSL_TLLL_WTR_LOSS_CD_NU	NUMBER
PSL_UL_RESULTS_CD_NU	NUMBER
PSL_TL_RESULTS_CD_NU	NUMBER
PSL_INSP_CITY_HERE_CD	NUMBER
PSL_INSP_CITY_ISSUE_CD	NUMBER
PSL_INSP_MAIN_LOC_TX	VARCHAR2(400 BYTE)
PSL_INSP_OFFHOUR_START_TIME	VARCHAR2(10 BYTE)
PSL_INSP_OFFHOUR_END_TIME	VARCHAR2(10 BYTE)

Enforcement:

COLUMN_NAME	DATA_TYPE
PSL_APN_GN	NUMBER
APN_DATA_APN_TX	VARCHAR2(32 BYTE)
APN_ADDR_BLDG_NU	NUMBER
APN_ADDR_FRACT_NU	VARCHAR2(3 BYTE)
APN_ADDR_PFIX_CD	VARCHAR2(2 BYTE)
APN_ADDR_ST_NM	VARCHAR2(25 BYTE)
APN_ADDR_SFIX_CD	VARCHAR2(4 BYTE)
APN_ADDR_APT_NU	VARCHAR2(10 BYTE)

COLUMN_NAME	DATA_TYPE
CITY_NM	VARCHAR2(20 BYTE)
APN_ZIP_CD	VARCHAR2(5 BYTE)
PSL_OWNER_NM	VARCHAR2(64 BYTE)
PSL_MAIL_ADDR_LINE1_TX	VARCHAR2(40 BYTE)
PSL_MAIL_CITY_NM	VARCHAR2(40 BYTE)
PSL_MAIL_STATE_NM	VARCHAR2(25 BYTE)
PSL_MAIL_ZIP4_CD	VARCHAR2(10 BYTE)
PSL_LAND_USE_TX	VARCHAR2(25 BYTE)
PSL_APN_TYPE_CD_NU	NUMBER
PSL_APN_CMNT_TX	VARCHAR2(4000 BYTE)
PSL_ENFORCE_CD	NUMBER
PSL_ENFORCE_DM	TIMESTAMP(6)
PSL_ENFORCE_TRIGGER_DM	TIMESTAMP(6)
PSL_LST_EVENT_NU	NUMBER
PSL_NEXT_DUE_DATE_DM	TIMESTAMP(6)
PSL_APN_VER_NU	NUMBER
ROW_CREATN_DM	TIMESTAMP(6)
ROW_MOD_DM	TIMESTAMP(6)
ROW_MOD_BY	VARCHAR2(10 BYTE)

Fees:

COLUMN_NAME	DATA_TYPE
PSL_APN_FEE_GN	NUMBER
APN_DATA_APN_TX14	VARCHAR2(32 BYTE)
PSL_PYMT_TYPE	NUMBER
PSL_APN_FEE_QT	FLOAT
PSL_PYMT_NU	NUMBER
PSL_APN_FEE_PAID_FG	NUMBER(10,0)
PSL_APN_FEE_VER_NU	NUMBER
ROW_CREATN_DM	TIMESTAMP(6)
ROW_MOD_DM	TIMESTAMP(6)
ROW_MOD_BY	VARCHAR2(10 BYTE)
PSL_FEE_DM	TIMESTAMP(6)
PSL_APN_FEE_TX	VARCHAR2(4000 BYTE)

Payments:

COLUMN_NAME	DATA_TYPE
PSL_PYMT_GN	NUMBER
APN_DATA_APN_TX	VARCHAR2(32 BYTE)
PSL_PYMT_TYPE_NU	NUMBER
PSL_PYMT_DM	TIMESTAMP(6)
PSL_PYMT_RCPT_TX	VARCHAR2(4000 BYTE)
PSL_PYMT_STAT_CD	NUMBER
PSL_PYMT_VER_NU	NUMBER
ROW_CREATN_DM	TIMESTAMP(6)
ROW_MOD_DM	TIMESTAMP(6)
ROW_MOD_BY	VARCHAR2(10 BYTE)