Appendix D.4 - Technical Requirements Form

| **ID** | **Requirement** |
| --- | --- |
| System Monitoring |
| TR-1 | Ability to provide routine system monitoring reports to the City regarding the performance, availability and status of all services provided by the Proponent. Provide a list of monitoring reports that will be provided to the City. Describe how the requirement is supported. |
| Response: |
| TR -2 | Ability to monitor information sources for emerging threats (e.g. newly disclosed vulnerabilities in the versions of software used). Describe how the requirement is supported. |
| Response: |
| TR -3 | Ability to integrate with external Security Information and Event Monitoring tools (SIEM). Describe how the requirement is supported. |
| Response: |
| Degradability, Interoperability, and Integration |
| TR -4 | Ability to support message queuing in the event the system is down or experiencing abnormal load conditions. Describe how the requirement is supported. |
| Response: |
| TR -5 | Ability to support a single sign-on approach. For example, can the solution allow an asset to remain in context when moving from one application to another. Describe how the requirement is supported. |
| Response: |
| TR -6 | Ability to leverage Web services to push and pull data via standard secure Web Protocols (SOAP, REST, etc.). Describe how the requirement is supported. Indicate if imports and exports are possible with Microsoft Office applications. |
| Response: |
| TR -7 | Ability to work with Active Directory or cloud-based directory services (Azure Directory Services). Describe how the requirement is supported. |
| Response: |
| TR -8 | Ability to provide tools to support data import/export processes (e.g. ETL process). Describe how the requirement is supported. |
| Response: |
| TR -9 | Ability to integrate to an electronic signature solution (e.g. PactSafe, Adobe, DocuSign etc.). Describe how the requirement is supported. |
| Response: |
| TR-10 | Ability to have data objects in the solution accessible via an API, vendor developed scripts, sftp sites, or other protocols which may be necessary. Describe how the requirement is supported. |
| Response: |
| TR-11 | Ability to trace a release to a version control system label and be able to roll back to a specific version, based on a tag or a point in time. Describe how the requirement is supported. |
| Response: |
| Mobile Applications |
| TR-12 | Mobile Applications should continue to operate when wireless network connectivity is lost. Describe how the requirement is supported. |
| Response: |
| TR-13 | Mobile Applications should be capable of presenting pre-loaded data. Describe how the requirement is supported. |
| Response: |
| TR-14 | Mobile Applications should automatically synchronize with central servers as wireless network availability is restored with no impact to workflow. Describe how the requirement is supported. |
| Response: |
| TR-15 | Mobile Applications should let users capture data when wireless network connectivity is lost. Describe how the requirement is supported. |
| Response: |
| TR-16 | Ability to secure connections between entities or devices. Describe how the requirement is supported. |
| Response: |
| Audit Tracking, Security |
| TR-17 | Ability to track who created/updated/deleted each data element. Auditing parameters should be configurable. Describe how the requirement is supported. |
| Response: |
| TR-18 | Ability to support distributed denial of service mitigation (e.g. be compatible with services like Cloudflare, Akamai, etc.). Describe how the requirement is supported. |
| Response: |
| TR-19 | Ability to support Automated Audit Log Analysis for detecting unauthorized access by credentialed users. |
| Response: |
| TR-20 | The contents of a cookie should be encrypted using a published, widely used encryption algorithm. Cookies should not contain any personal or otherwise sensitive information. Cookies should apply to the hosting domain only. Describe how the requirement is supported. |
| Response: |
| TR-21 | Ability to configure inactivity timeout for users. Describe how the requirement is supported. |
| Response: |
| TR-22 | Ability to protect any data in transit and at rest, using encryption or equivalent mechanism. Describe how the requirement is supported. |
| Response: |
| TR-23 | Ability to provide node authentication between client and Proponent systems for all types of transactions is required. Describe how the requirement is supported. |
| Response: |
| TR-24 | Ability to allow an admin to create roles with granular application permissions. When an Active Directory User accesses the application, they are granted the privileges of the corresponding role(s) of their associated Group(s). Privileges are always “allow”, never “deny” – by default, all privileges are denied.  |
| Response: |
| TR-25 | Ability to leverage a virus scanning solution to inspect files attached in by the application (e.g OPSWAT). Describe how the requirement is supported. |
| Response: |
| TR-26 | Ability to provide a secure, scheduled, and audited patching process based upon release cycles or in the instance of a security breach. Describe the audit patching process. |
| Response: |
| TR-27 | Ability to support user authentication to/from applications via SAML and Open ID Connect (OIDC) authentication integration. Describe what user authentications are supported.  |
| Response: |
| TR-28 | Ability to support multi-factor authentication schemes. Describe what schemes are supported. |
| Response: |
| TR-29 | Ability to support logout from the application which triggers a global sign-out from any other SAML supported application. Describe how the requirement is supported. |
| Response: |
| TR-30 | Ability to avoid displaying technical details about the internal operation of the system to users through error messages. Describe how the requirement is supported. |
| Response: |
| Availability, Scalability |
| TR-31 | Ability to alert users of an unplanned outage. Describe how the requirement is supported. |
| Response: |
| TR-32 | Have measures in place to mitigate the impact of outages on dependent systems/interfaces. Describe how the requirement is supported. |
| Response: |
| TR-33 | The solution should be available 24 hours per day, 7 days per week, 365 days per year at 99.99% or better. This excludes the City-owned networks. Describe how the requirement is supported. |
| Response: |
| TR-34 | The solution should provide disaster recovery capabilities for the entire system to ensure the continuation of business by having adequate and appropriate backups of all data, and built-in error checking and recovery capabilities. Provide your disaster recovery processes including how backs-ups are structured and stored. Indicate if there is a requirement for the City to backup any part of the solution or provide storage. |
| Response: |
| TR-35 | Compatible with the Microsoft Windows 10 operating system. |
| Response: |
| TR-36 | Ability to deploy 'on demand' in a non-production environment, such as, a test, development, QA, Training, or staging environments. |
| Response: |
| TR-37 | Ability to support User Interface rendering response times of 3 seconds or less. |
| Response: |
| TR-38 | Ability to notify users when delays exceed acceptable response times. Describe how the requirement is supported. |
| Response: |
| TR-39 | Ability to scale system resources and user accounts on demand. Describe how the requirement is supported. |
| Response: |
| Accessibility, Configurability, Dependability, Maintainability |
| TR-40 | Core functionalities offered to the users should be compatible with the following Web Browsers.Supported web browsers are:- Microsoft Internet Explorer 11 +- Google Chrome 70+- Apple Safari 12 + |
| Response: |
| TR-41 | Ability to support the following accessibility guidelines: - Web Content Accessibility Guidelines (WCAG) 2.0 |
| Response: |
| TR-42 | Ability to enforce a data retention policy based on data classification and type. Describe how the requirement is supported. |
| Response: |
| TR-43 | Ability to allow for delegated administrative access to selected staff for appropriate oversight and admin functions, such as viewing user accounts properties, error logs, application configurations. Describe how the requirement is supported. |
| Response: |
| TR-44 | Ability to ensure data currency is maintained with multiple users accessing the same record. Describe how the requirement is supported. |
| Response: |
| TR-45 | Timestamps in events log files set to UTC time. Standardizing to UTC simplifies log correlation within the organization and with external parties no matter what time zone the device being synchronized is located in. Describe how the requirement is supported. |
| Response: |
| TR-46 | Ability to support time synchronization for concurrency of timestamps for stored records, events, and messages exchanged between external systems. Describe your time synchronization architecture, including what Stratum Level is supported for time synchronization of system clocks. |
| Response: |
| TR-47 | The solution should provide automated notifications to the City's operations team in the event of a critical system events or errors. Describe how this can be supported. |
| Response: |
| TR-48 | User interface components should implement a responsive design that supports access from a range of devices including smartphones, tablets, and desktop computers. |
| Response: |