**Technical Standards**

06/10/2016

**SaaS/PaaS** - Solutions using Software as a Service (SaaS) or Platform as a Service (PaaS).  
**Internal** - Solutions hosted within City of Austin infrastructure.

Mandatory - Essential requirement  
Expected - Anticipated or presumed requirement  
\_\_\_\_\_ - No preference

| **ID#** | **Topic** | **Description** | **Internal** | **SaaS/PaaS** |
| --- | --- | --- | --- | --- |
| 1 | Application Architecture | The application provides Web-enabled components to meet the Rehabilitation Act of 1973 Section 503, W3C and industry standards for graphics and design; speed; reliability; and security for dynamic content and user interaction. | Mandatory | Mandatory |
| 2 | Application Architecture | Ensure compatibility of software with the current version of the following: iOS, Windows and Android mobile devices - Chrome, Safari, IE and Firefox browsers (within 12 months); Windows and Apple operating systems - Office productivity (within 18 months); Oracle and MS SQL databases (within 24 months). Current version is defined as the manufacturer's latest production point version of the product. | Mandatory | Mandatory |
| 3 | Application Architecture | No requirement to deploy application code to client workstations (note: Java Runtime Environment (JRE) is an exception). | Mandatory | Mandatory |
| 4 | Application Architecture | The application provides the ability to automate the deployment of software and updates to user workstations including, but not limited to Web-based deployment tools to push/pull software to the desktop (note: applicable only to run-time environment, like Java). Unless the contractor provides an alternative solution, users do not require administrative privileges. | Mandatory | Mandatory |
| 5 | Application Architecture | The application provides built-in application and system configuration tables accessible by all modules. | Mandatory | Mandatory |
| 6 | Application Architecture | The application provides (if needed) ability to manage automatic job scheduling (i.e., batch jobs, billing) including, but not limited to, the interface with external job schedulers and automatic notification capabilities when a job abnormally terminates. The City currently support UNIX CRON, Tivoli work Scheduler, Oracle DBMS\_JOBS, and MS SQL DTS. | Mandatory | \_\_\_\_\_ |
| 7 | Application Architecture | The application provides forms-based data validation (field level validation) and displays error messages when validation fails (i.e., user enters text in a numeric field). | Mandatory | Mandatory |
| 8 | Application Architecture | The application provides copy, cut, paste, and undo functions from data fields and screens to other applications. | Mandatory | Mandatory |
| 9 | Application Architecture | The application provides ability to perform mass changes to a defined group of transactions with appropriate selection criteria. | Mandatory | Mandatory |
| 10 | Application Architecture | The application provides ability to effective date transactions and table updates including, but not limited to future and retroactive changes, based on user-defined criteria. | Mandatory | Mandatory |
| 11 | Application Architecture | The application provides ability to drill down from a transaction view to the supporting source document or record, regardless of the module source. | Mandatory | Mandatory |
| 12 | Application Architecture | The system provides ability to restrict free form entry (e.g., require use of drop-down calendar for date field). | Mandatory | Mandatory |
| 13 | Application Architecture | The system meets Web Accessibility standards including, but not limited to, ability to support ADA and compliant with Section 508 of the Federal Rehabilitation Act (see http://www.access-board.gov/sec508/summary.htm). Web based applications must be compliant following the specifications of 508c of the Americans with Disabilities Act. If compliance is not possible, reasonable alternatives may be considered. | Mandatory | Mandatory |
| 14 | Application Architecture | The application provides ability to apply upgrades and patches without impact to existing user interface customizations (e.g., user-defined forms/fields, Web interface, etc.). | Expected | Expected |
| 15 | Application Architecture | The solution supports Distributed File System (DFS) shares for file access. | Expected | \_\_\_\_\_ |
| 16 | Audit | The system provides user-defined audit features for all transactions in solution including, but not limited to, all historical changes, date, time, and user ID of the person making the change. | Expected | Expected |
| 17 | Audit | The system provides ability to prevent audit records from being deleted or altered, except as part of a system administration archival process. | Expected | Expected |
| 18 | Audit | The system provides ability for audit-tracking reports including, but not limited to user access and usage logs. | Expected | Expected |
| 19 | Audit | The system provides ability to archive and restore audit logs. | Expected | Expected |
| 20 | Business Continuity and Disaster Recovery | The system provides full recovery and system backup capabilities for all online and batch transactions according to City-specified timeframes. | Mandatory | Mandatory |
| 21 | Business Continuity and Disaster Recovery | The system provides software redundancy including, but not limited to, integrity checking capability to identify the existence of program and/or system discrepancies and issue an alert to the appropriate systems operations team. | Mandatory | Mandatory |
| 22 | Business Continuity and Disaster Recovery | The system provides ability to alert specified users when key components are unavailable (e.g., DBMS, servers, interfaces, network transport, etc.). | Mandatory | Preferred |
| 23 | Business Continuity and Disaster Recovery | The system provides ability to restore transactions from the database transaction log. | Expected | \_\_\_\_\_ |
| 24 | Business Continuity and Disaster Recovery | The system provides software redundancy including, but not limited to, software crash tolerance (i.e., server and client software shall maintain its integrity in case of power failures and abrupt shutdowns); redundancy in the application server tier with automated cut-over; redundancy in the database server tier with automated cut-over; restart and recovery capability after system/server failure with no loss of data or software components; and roll-back. | Expected | Expected |
| 25 | Business Continuity and Disaster Recovery | The system provides software redundancy including, but not limited to, file protection capability to limit the types of operations (e.g. read, write, delete, and data dictionary modification) that individual users on given data or program files can perform. | Expected | Expected |
| 26 | Business Continuity and Disaster Recovery | The system provides software redundancy including, but not limited to, incremental, differential, and full backups and restores of the database, core and customized software, software and database configuration options, user preferences and rights, etc. This includes the ability to recover specific data records and/or files from backup and/or near-line storage. | Expected | \_\_\_\_\_ |
| 27 | Data Storage and Archiving | The solution supports future releases of the application without rendering the archived data unusable. | Mandatory | Mandatory |
| 28 | Data Storage and Archiving | The solution utilizes storage area network (SAN). | Mandatory | \_\_\_\_\_ |
| 29 | Data Storage and Archiving | The system provides online access to the current year plus unlimited previous years of all types of data retained in the system, and provides archive capabilities thereafter. | Expected | Expected |
| 30 | Data Storage and Archiving | The system provides ability to archive data to external storage media and support partitions, based on user-defined including, but not limited to, number of years. | Expected | Preferred |
| 31 | Data Storage and Archiving | The system allows the City to accurately plan for storage and backup requirements, both for initial implementation and for future growth. | Expected | \_\_\_\_\_ |
| 32 | Data Storage and Archiving | The contractor provides the City a complete copy of current and archived data hosted by an ASP provider in the event of contract termination within a month of notification in one of the required formats listed above. (ASP Hosted) | \_\_\_\_\_ | Mandatory |
| 33 | Database Architecture | The application provides standardized data extraction Application Program Interface (API) to allow import and export of data to other systems. | Mandatory | Mandatory |
| 34 | Database Architecture | The application provides ability to encrypt sensitive data when required by federal or state compliance (e.g., PII, PCI, HIPAA, etc.). | Mandatory | Mandatory |
| 35 | Database Architecture | The application provides use of Structured Query Language (SQL) for database queries. | Mandatory | \_\_\_\_\_ |
| 36 | Database Architecture | The solution uses the same data validation criteria for bulk data loads as it does for manual data entry. | Mandatory | Mandatory |
| 37 | Database Architecture | The application provides ability to exchange database information using industry accepted standards and formats including Extensible Markup Language (XML). | Expected | Expected |
| 38 | Database Architecture | The application provides ability to copy, archive and retrieve data to external storage media (e.g., tape, DVD, SAN) based on user-defined selection criteria. | Expected | \_\_\_\_\_ |
| 39 | Database Architecture | The application provides ability to perform database maintenance including, but not limited to, backup and upgrades without requiring system downtime during core business hours. | Expected | Expected |
| 40 | Database Architecture | The solution includes a method of purging record data from the database(s) ensuring referential integrity with master/child records. | Expected | Expected |
| 41 | Database Architecture | The system provides ability to set up log event triggers to automatically notify the system administrator when user-defined database conditions are met. (Note: If hosted solution, provide access to configurable alerts.) | Expected | \_\_\_\_\_ |
| 42 | Information Management | The system prevents the loss or unauthorized deletion of records before the expiration of their retention period as authorized by an approved records control schedule or with the written permission of the Texas State Library and Archives Commission. Texas Local Government Records Act §202.001(a). | Mandatory | Mandatory |
| 43 | Information Management | The system prevents the unauthorized alteration of records before the expiration of their retention period. The system provides logs or audit trails that document edits and views of records. This is a requirement for records governed by HIPAA; and, depending on the type of record, there may be additional integrity requirements governed by Texas House Bill 300. | Mandatory | Mandatory |
| 44 | Information Management | The system provides systematic deletion of records upon expiration of their retention period as authorized by an approved records control schedule or with the written permission of the Texas State Library and Archives Commission. Texas Local Government Records Act §202.001(a) and §201.003(16), Austin City Code §2-11-11. Sufficient metadata must be present to identify records eligible for disposition based on defined triggering events and dates. | Mandatory | Mandatory |
| 45 | Information Management | Upon expiration of the retention period, the system ensures destruction of all duplicate records to include convenience copies. Texas Rules of Evidence, Rule 1003. The system's back-up strategy ensures retention of backup records doesn't excessively exceed destruction of originals. System procedures must ensure retention rules apply to copies of production data used to develop, test, or train. | Mandatory | Mandatory |
| 46 | Information Management | The system ensures records are retrievable and available until the expiration of their approved retention period. Texas Local Government Records Act §205.008(b). Records stored on contractor, outsourced, cloud, or hosted platforms remain the property and responsibility of the City. When contacted by an authorized City employee or when the contract ends or is terminated, contractors must deliver records, in all requested formats and media, along with all finding aids and metadata, to the City at no cost. Austin City Code §2-11-15. | Mandatory | Mandatory |
| 47 | Information Management | Until expiration of retention period, hardware and software must be available to access records and sufficient metadata must be present to facilitate timely retrieval of records. Contracts with hosted solution providers must specify the contractor's duties with respect to management of records as required by Austin City Code §2-11-15. The system ensures retention of specific records - even if their retention period has expired - if they are the subject of known or reasonably anticipated litigation, public information request, audit or other legal action. Texas Local Government Records Act §202.002, Austin City Code § 2-11-11. The system maintains a log of litigation and other holds allowing release of holds after resolution of litigation, audit, or public information requests. | Mandatory | Mandatory |
| 48 | Information Management | The system creates records/logs of destruction activity. Texas Local Government Records Act §203.046, Austin City Code §2-11-11. Destruction logs must (a) show a minimal set of metadata sufficient to uniquely identify the records purged; (b) show who approved and who executed the destruction, and the dates on which these events took place; (c) reflect compliance with an approved, written standard operating procedure; and (d) be retained permanently. | Mandatory | Mandatory |
| 49 | Infrastructure | The system uses industry standard virtualization infrastructure to support load balancing. | Mandatory | \_\_\_\_\_ |
| 50 | Infrastructure | If the system is Simple Network Management Protocol (SNMP V.3) compliant, the contractor provides standard Management Information Base (MIB) files for all SNMP-enabled components. | Mandatory | \_\_\_\_\_ |
| 51 | Infrastructure | The solution uses an accurate, NIST time source for traceable time stamp. If back-end components use date/time stamping, client-side components synchronize with back-end servers. | Mandatory | Mandatory |
| 52 | Infrastructure | If the solution includes electronic hardware such as servers or network devices, all network-enabled hardware supports auto-negotiation of network speeds and duplex settings, including 10 mbps, 100 mbps and Gigabit Ethernet, if applicable. | Expected | \_\_\_\_\_ |
| 53 | Infrastructure | If applicable, all portable devices (laptops, hand-held units, etc.) provide display screens readable in conditions ranging from darkness to direct sunlight. | Expected | Expected |
| 54 | Infrastructure | If applicable, all supplied portable devices (laptops, hand-held units, etc.) are resistant to heat, cold, moisture, dust and shock. | Expected | Expected |
| 55 | Infrastructure | If applicable, all supplied portable devices (laptops, hand-held units, etc.) are capable to receive program or firmware updates via network connections. | Expected | Expected |
| 56 | Infrastructure | System server components use standard Domain Name Services (DNS). | Expected | \_\_\_\_\_ |
| 57 | Integration Architecture | The system provides the ability to set up appropriate approval, audit trail, and reconciliation procedures for all inbound and outbound interfaces. | Mandatory | Mandatory |
| 58 | Integration Architecture | If application requires integration with other City data, the application must integrate using an enterprise service bus. | Expected | Expected |
| 59 | Security and Authentication | If applicable, the system provides adequate protection of data covered by regulatory or other compliance requirements (e.g., U.S. Health Insurance Portability and Accountability Act (HIPAA), Family Educational Rights and Privacy Act (FERPA), Payment Card Industry (PCI). | Mandatory | Mandatory |
| 60 | Security and Authentication | The system authenticates with multiple internal Microsoft Active Directories. | Mandatory | \_\_\_\_\_ |
| 61 | Security and Authentication | The application provides encryption for data exchanged between the front-end user application and the back-end servers - federal or state compliance required (e.g., PII, PCI, HIPAA, etc.). | Mandatory | Mandatory |
| 62 | Security and Authentication | The system provides protection against unauthorized access to data by persons and other software programs. | Mandatory | Mandatory |
| 63 | Security and Authentication | The system masks (i.e., substituting characters with '\*') passwords as they are entered into the system. | Mandatory | Mandatory |
| 64 | Security and Authentication | The system is PCI-compliant when handling credit card transactions. | Mandatory | Mandatory |
| 65 | Security and Authentication | The solution does not require operating system administrator privileges on the client workstation(s) to run or receive application updates or the vendor must provide another solution for updates. | Mandatory | Mandatory |
| 66 | Security and Authentication | The solution provides a method to change the passwords for built-in system accounts (i.e. Administrator, Admin, Super, etc.) | Mandatory | Mandatory |
| 67 | Security and Authentication | When the contractor is connected to the City's Virtual Private Network (VPN) for solution support purposes, the contractor uses single tunneling, which means the contractor disconnects from their local network during the VPN session. | Mandatory | \_\_\_\_\_ |
| 68 | Security and Authentication | Passwords must NOT be included in automated sign-on procedures, stored unencrypted in cache, or transmitted as clear text over the network. | Mandatory | Mandatory |
| 69 | Security and Authentication | The application allows the Application Administrator to restrict generic logins. | Mandatory | Mandatory |
| 70 | Security and Authentication | When applicable, the system provides 128-bit SSL or higher or TLS, between the client browser and application modules. | Expected | Expected |
| 71 | Security and Authentication | The system allows an approved administrator to inactivate user access. | Expected | Expected |
| 72 | Security and Authentication | The system provides ability to manage user permissions centrally for all modules of the applications. | Expected | Expected |
| 73 | Security and Authentication | The system provides ability to use tokens and/or passwords for user logons. | Expected | Expected |
| 74 | Security and Authentication | The system provides users the ability to change password, users to change their password on set period and password expiration. | Expected | Expected |
| 75 | Security and Authentication | The system provides ability to configure passwords including, but not limited to the following: minimum password length of at least eight characters; case sensitive, contain numbers, alphanumeric characters, and special characters; and complex passwords based on user-defined criteria. | Expected | Expected |
| 76 | Security and Authentication | The system provides ability to record the date and time of changed password. | Expected | Expected |
| 77 | Security and Authentication | The system provides ability to deny user access after a definable number of unsuccessful attempts to logon. | Expected | Expected |
| 78 | Security and Authentication | The system provides ability to log, based on user-defined criteria, each authorized and/or unauthorized access attempt. Log information includes, but is not limited to, user identification, IP address, date, time, transaction type, and type of access (e.g., read, modify). | Expected | Expected |
| 79 | Security and Authentication | The system provides ability to assign application access rights for the entire suite of applications at a single point of entry. | Expected | Expected |
| 80 | Security and Authentication | The system provides ability to control access to all activities (e.g., online transactions, batch processing, report writer, query, system utilities) including, but not limited to the following levels: system, database, module, field, inquiry, approval, report, transaction, table, individual, group, organization (e.g., department, division), user role, user site, time period, and position across all functional areas. | Expected | Expected |
| 81 | Security and Authentication | The system provides ability to create and maintain security profiles to control access including, but not limited to the following: employee level, module, field, transaction type, employee group, standard report, and ad hoc report. | Expected | Expected |
| 82 | Security and Authentication | The system provides ability to automatically log users off the system when there has been no activity for a definable (pre-defined) period. | Expected | Expected |
| 83 | Security and Authentication | The system provides ability to generate summary and detail reports including, but not limited to user access, usage logs, audit logs, failed and/or unauthorized access attempts based on user defined parameters (e.g., audit requirements). The system provides ability to alert the application administrator when any of these events exceed a specific, definable threshold. | Expected | Expected |
| 84 | Security and Authentication | The system provides ability to utilize session encryption methods necessary to ensure the secure electronic transfer of sensitive information. | Expected | Expected |
| 85 | Security and Authentication | If the system requires bulk data loads via the Internet, the system uses a secure network transport method. | Expected | Expected |
| 86 | Security and Authentication | New user permissions default to least privileges security permissions. | Expected | Expected |
| 87 | Security and Authentication | The application provides a transaction log related to changes made to security (roles, groups, and permissions). | Expected | Expected |
| 88 | Security and Authentication | To help enforce City's security policies, the solution allows the application administrator to disconnect a particular user and to lock out a user during an active session. | Expected | Expected |
| 89 | Security and Authentication | The system provides ability to restrict remote access to the application by client IP address or network address range. | \_\_\_\_\_ | Expected |
| 90 | Security and Authentication | The system uses Microsoft Active Directory Federated Services (ADFS) [current version minus 1] for federated identity management. | \_\_\_\_\_ | Mandatory |
| 91 | Security and Authentication | The system ensures the City's data is not made available to any other parties not specifically authorized to view or access the data. (ASP Hosted) | \_\_\_\_\_ | Mandatory |
| 92 | Security and Authentication | For systems with sensitive data (personally identifiable information (PII), city confidential data, or data covered by a federal security standard), the contractor conducts an annual security assessment of all tiers of its hosting facility, including application servers and network devices. Provide summary copies of the security audit reports to the City of Austin annually. We prefer an annual 3rd party security assessment, which we may require depending on the data being hosted. | \_\_\_\_\_ | Mandatory |
| 93 | System Flexibility | The system provides the ability to define business rules based on user-defined criteria (e.g., organizational level, account code, bargaining unit, location, program, grant, etc.). | Mandatory | Expected |
| 94 | System Flexibility | The system solution is compatible with Citrix for client server configurations. | Expected | Expected |