## Introduction

## Completion of the Fairfax County Technology Requirements Response Matrix must be included in the response to the technology requirements outlined in the Banking RFP. It is intended to assist Fairfax County with assessing the vendor responses to the technology requirements. The clear identification of each element is required by Fairfax County in order to sustain and ensure a solid foundation for the development and implementation of secure information technology practices within Fairfax County Government. Elements are also included for issues relative to HIPAA Privacy and Security compliance. Vendors with access to Fairfax County information resources are required to abide by all policies and procedures of Fairfax County Government.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Standards** | **Offerors Response** | **Where in Your Proposal is the Specification Described?** |
|  | **Description of System/Service** |  |  |
|  | **Bank Name** |  |  |

|  | **STANDARDS** | **DOES SYSTEM COMPLY?****OR****CAN SERVICE BE DELIVERED?** | **WHERE IN YOUR PROPOSAL IS THE SOLUTION DESCRIBED?** | **COMMENTS/PLANS FOR MEETING COMPLIANCE** |
| --- | --- | --- | --- | --- |
|  | **Technology Requirements** | **(Yes/No/Alternative Solution)** |  |  |
| 23.11.1. | **MAINTAIN AN INFORMATION SECURITY PROGRAM** |  |  |  |
| a. | Offeror/Contractor should maintain a formal information security technology program that identifies management, operational, and technical controls to ensure the confidentiality, integrity, and availability of information systems and data and validates those controls. |  |  |  |
| b. | Offeror/Contractor should maintain an active vulnerability management program to protect systems from known vulnerabilities. |  |  |  |
| 23.11.2. | **TRANSMISSION SECURITY** |  |  |  |
| a. | Offeror shall identify data transmission techniques used to transfer information securely between (i.e., 2-way) their Information Systems and the County's. The System Security procedures and practices, which protect the data during and after the transmission shall be submitted for evaluation. |  |  |  |
| b. | Offeror/Contractor should use strong cryptography and security protocols (for example, SSL/TLS, IPSEC, etc.) to safeguard sensitive financial information data during transmission between networks. |  |  |  |
| 23.11.3. | **PROTECTION OF STORED DATA** |  |  |  |
| a. | Offeror/Contractor should maintain a defense-in-depth security architecture incorporating intrusion detection, firewalls, and other network security monitoring and access control mechanisms. |  |  |  |
| b. | Offeror/Contractor should protect financial data by implementing access control mechanisms to limit access to data to personnel whose job requires such access. |  |  |  |
| c. | Offeror/Contractor should protect financial data by implementing an auditing and systems monitoring program to identify and alert of unauthorized access or transactions. |  |  |  |
| d. | Offeror/Contractor should restrict physical access to systems housing customer financial data. |  |  |  |
| e. | Offeror/Contractor should implement data retention and disposal policies, procedures and processes, by limiting data storage amount and retention time to that which is required for legal, regulatory, and business requirements |  |  |  |
| 23.11.4. | **HARDWARE REQUIREMENTS** |  |  |  |
| a. | System hardware requirements should be listed in detail to include make, model and number of devices required for the full implementation of the application. Hardware proposed should be consistent with County standards as outlined in the County IT Plan. |  |  |  |
| 23.11.5. | **BACKUP AND RECOVERY** |  |  |  |
| a. | All vendor solutions must have an appropriate automated backup capability for system and application backup and recovery. Backup media shall be in a format suitable for convenient off-site storage. The system must provide differential backup schedules for various system components configurable by the system administrator. Incremental and full backup capabilities must be provided. All backup and recovery processes must be subject to auditing and reporting. System backups must be accomplished without taking the application out of service and without degradation of performance or disruption to operations |  |  |  |
| b. | Offeror to describe the backup and recovery processes that are in place that allows for the continuation of operations in the event of a disaster where the County will continue to maintain operations. |  |  |  |
| c. | Offeror/Contractor to provide emergency backup plan to receive payment information. The County currently provides payment information to the originating/receiving bank via secured internet transmission. The emergency backup plan must be available to initiate payments when needed. The file specifications for County are:- Record length: 94 characters, fixed- EBCDIC alphanumeric set- Standard labels (date set name ACHTAP) |  |  |  |
| 23.11.6 | **DISASTER RECOVERY** |  |  |  |
| a. | Contractor should maintain disaster recovery procedures to assist in preventing interruption of system use. |  |  |  |
| b. | Contractor should maintain high availability of resources available to customers. |  |  |  |
| c. | Offeror should describe the backup and recovery processes that are in place that allows for the continuation of operations in the event of a disaster where the County will continue to maintain operations. |  |  |  |
| 23.11.7. | **INCIDENT RESPONSE AND HANDLING** |  |  |  |
| a. | Contractor should maintain an incident response plan including strategy for notifying customers in the event of a breach and compromise of customer information. |  |  |  |
| 23.11.8. | **SYSTEM ADMINISTRATION** |  |  |  |
| a. | The proposed solution must provide a suite of system administration tools to support the effective ongoing operation of the systems. The full suite of system administration tools native to the operating system and database utilized shall be available to appropriate County personnel. |  |  |  |
| b. | System administration capabilities, at a minimum, must include the ability to: |  |  |  |
| - | Create and maintain user accounts |  |  |  |
| - | Manage security |  |  |  |
| - | Manage backup and recovery processes |  |  |  |
| - | Monitor and tune system performance |  |  |  |
| - | Install and configure hardware |  |  |  |
| - | Install and configure software/updates |  |  |  |
| - | Import new or updated geofiles, including addresses and street centerlines (when applicable) |  |  |  |
| - | Monitor and maintain interfaces |  |  |  |
| - | Schedule procedures |  |  |  |
| - | Manage disaster recovery procedures |  |  |  |
| - | Configure alerts  |  |  |  |
| - | Organize and maintain system documentation |  |  |  |
| - | Perform remote management |  |  |  |
| c. | The system administrator or other authorized user must also be able to add a report, macro, or function to the application menu and add new data elements to forms or to report formats. |  |  |  |
| d. | All system administration procedures must be supported by a detailed logging, auditing and reporting capability. |  |  |  |
| 23.11.9. | **SYSTEM DOCUMENTATION** |  |  |  |
|  | The Offeror/Contractor will supply documentation in printed and electronic format (MS Word Format and/or .pdf format at the County’s option). The proposed solution must include complete documentation including, at a minimum: |  |  |  |
| a. | Technical Documentation (2 printed copies plus a CD/DVD/USB Drive) - must describe the technical architecture of the product as installed, configured and customized. The technical documentation must include information regarding the relational database design (data dictionary), record or table layouts, file schemas and use of application programs interfaces (API’s), program description, and report manual. The Offeror must compile and provide to the County complete documentation for all COTS and customized including: |  |  |  |
| - | Data dictionary |  |  |  |
| - | Database table layouts |  |  |  |
| - | Interface specifications |  |  |  |
| - | Data conversion processes |  |  |  |
| - | Programs |  |  |  |
| - | XML schema |  |  |  |
| - | Stored queries and procedures |  |  |  |
| - | Canned Reports List and Report layouts.  |  |  |  |
| b. | Systems Administration Documentation 2 printed copies plus a CD/DVD/USB Drive) - must describe the steps and procedures needed to operate the product as installed, configured and customized, on a day-to-day basis. It must include information relating to procedures for system start-up and shut down, batch job submission procedures, security procedures, table maintenance procedures, etc. |  |  |  |
| c. | User Documentation (2printed copies plus a CD/DVD/USB Drive) - must describe the operation of the products, as installed, configured and customized from the perspective of the end user. The documentation must cover sign-on and sign-off sequences, menu operation, screen descriptions, means of invoking online help facilities, report generation, etc., and must be targeted to specific user groups. |  |  |  |
| d. | The Contractor shall, at no additional charge to the County, provide updated technical, System Administrator, and user documentation when major system changes or updates occur such as Versions or Releases. Documentation will be provided in electronic format with permission for the County to distribute internally as needed. All new versions and releases must be accompanied by a document clearly explaining the new functionality, features, corrections, etc., addressed by the release or version. |  |  |  |
| e. | The Contractor shall, at no additional charge to the County, provide documentation for any system configurations and integrations. System documentation must be provided in a MS Word format. Any content within the documentation which is considered proprietary in nature shall be so marked. |  |  |  |
| f. | The Contractor shall be responsible for providing updated documentation for the application environment on an ongoing basis.  |  |  |  |
| 23.11.10. | **OWNERSHIP OF AND ACCESS TO DATA AND ASSOCIATED PRODUCTS** |  |  |  |
|  | The application data is and must remain the sole property of the County. Therefore, all tools and capabilities native to the database/OS environment, either Oracle/SQL Server, Unix/Windows, as proposed, should be available to the County to allow for full access to that data. All tables, layouts, queries, stored procedures, XML schema and other content developed to support the operation of the database and the application in the Fairfax environment become the property of the County, and shall be available to the appropriate County personnel as needed and upon request. Database query, extract and download capabilities into external formats such as MS Excel must be completely operational and available for appropriate County personnel to access using County standard access mechanisms |  |  |  |
| b. | The above is not meant to include -proprietary programs or other intellectual property unique to the Offeror’s solution. However, such claim to proprietary content cannot intrude on the County’s right to access its data without undue interference or additional cost. Any such proprietary materials must be clearly marked and/or disclosed. |  |  |  |
| c. | Data owned by Fairfax County may not be used by the Offeror for any purposes without the express written consent of the appropriate County representative. |  |  |  |
| 23.11.11. | **SOFTWARE UPGRADES AND PATCHES** |  |  |  |
|  | The Contractor shall make available to the County at no additional charge all upgrades and patches to the software as they are released so long as the County is currently under the Offeror’s software maintenance agreement. If the County opts to take advantage of the patch or updated version, the Offeror shall install and support it under the on-site maintenance agreement. |  |  |  |
| b. | To ensure that documentation is consistent with the operating environment, Contractor must deliver updated documentation concurrently with the software update. Upgrades and patches will be applied in accordance with change management procedures. |  |  |  |
| 23.11.12. | **Data Communications** |  |  |  |
| a. | For purposes of information exchange, Offeror shall identify their preferred data formats. The County has a preference for adopting non-proprietary formats associated with standards commonly used in the Banking and Finance industry. The County maintains discretion to not adopt formats suggested by the Contractor. |  |  |  |
| b. | Contractor shall identify data transmission techniques used to transfer information securely between (i.e., 2-way) their Information Systems and the County's. The System Security procedures and practices, which protect the data during and after the transmission shall be submitted for evaluation. All standards and regulations followed by the Offeror for compliance must be listed.Details such as supported transmission protocols, transmission rates, access and availability must be provided with sufficient technical details for evaluating compatibility and capability. This includes standards followed to protect the content during transmissions such as authentication, encryption, audit and non-repudiation.Process automation is important to the County. Offeror is encouraged to identify the work process that is initiated upon receipt of data transmissions from the County. |  |  |  |
| c. | Offeror shall identify its ability to acknowledge County transmissions. Upon further processing of the contents of the transmission, its ability to communicate status updates and/or handle exceptions and errors shall be identified. This may be included in the same section that identifies the workflow associated with the County's data.Offeror shall identify the operational aspects of its data handling. This includes the County's ability to receive notifications upon the occurrence of systems and application errors/exceptions or updates on progress/status. The timeliness of the notification with its severity must be identified.Contractor/Offeror shall submit an Operations Guide for the County to reference to identify and fix the erroneous condition. The Guide must elaborate on means to overcome the error in a timely and automated manner. |  |  |  |