CONTRACT BETWEEN THE CITY OF AUSTIN ("City")
AND
INSIGHT PUBLIC SECTOR("Contractor")
For
Public Information Request System Services
MA-5600- NC170000045

This Contract is between INSIGHT PUBLIC SECTOR, having offices at 6820 S. Harl Avenue, Tempe, AZ 85283-4318 and the City, a home-rule municipality incorporated by the State of Texas. Solicitation requirements are met by using Contractor's U. S. Communities Contract No. 4400006644.

1.1 This Contract is composed of the following documents:

1.1.1 U.S. Communities Contract No. 4400006644

1.1.2 This Contract

1.1.3 Exhibit A, Supplemental Terms

1.1.4 Exhibit B, City of Austin, Statement of Work, Addendum 1

1.1.5 Exhibit C, GOVQA Response, Security and Business Continuity, and Foresite Attestation Final

1.1.6 Exhibit D, Insight Public Sector Quote

1.1.7 Exhibit E, Non-Discrimination Certification

1.1.8 Exhibit F, Non-Suspension or Debarment Certification

1.2 **Order of Precedence.** Any inconsistency or conflict in the Contract documents shall be resolved by giving precedence in the following order:

1.2.1 U.S. Communities Contract No. 4400006644

1.2.2 This Contract

1.2.3 Exhibit A

1.2.4 Exhibit B

1.2.5 Exhibit C

1.2.6 Exhibit D

1.3 **Quantity.** Quantity of goods or services as described in Exhibit D.

1.4 Term of Contract.

The Contract shall be in effect for an initial term of 12 months and may be extended thereafter for up to 4 additional 12 month extension option(s), subject to the extension of the cooperative contract (as referenced in Section 1.1.1 above), approval of the Contractor and the City Purchasing Officer or his designee.

1.5 **Compensation.** The Contractor shall be paid a total Not-to-Exceed amount of $ 142,400 for the initial Contract term and $162,563 for the first extension option, $178,204 for the second extension option, $183,550 for the third extension option and $189,057 for the fourth extension option, for a total contract amount not-to- exceed $855,774.

This Contract (including any Exhibits) constitutes the entire agreement of the parties regarding the

subject matter of this Contract and supersedes all prior and contemporaneous agreements and understandings, whether written or oral, relating to such subject matter. This Contract may be altered, amended, or modified only by a written instrument signed by the duly authorized representatives of both parties.

In witness whereof, the City has caused a duly authorized representative to execute this Contract on the date set forth below.

INSIGHT PUBLIC SECTOR	CITY OF AUSTIN
John Brooks	JAMES T. HOWARD
Printed Name of Authorized Person	Printed Name of Authorized Person
Signature	Signature
Senior Director	PROCUREMENT MANAGER/IT
Title:	Title:
7/17/2017	8/18/2017
Date:	Date:

Exhibit Listing

Exhibit A	Supplemental Terms
Exhibit B	City of Austin Statement of Work, Addendum 1
Exhibit C	GOVQA Response, Security and Business Continuity, and Foresite Attestation Final
Exhibit D	Insight Public Sector Quote
Exhibit E	Non Discrimination Certification
Exhibit F	Non Suspension or Debarment Certification

Exhibit A
Supplemental Terms

1. **Designation of Key Personnel.** The Contractor's Contract Manager for this engagement shall be Jessica London, Phone: 630-633-7346, Email jlondon@webqa.net. The City's Contract Manager for the engagement shall be Karen Torres; Phone: 512-974-7752, Email: karen.torres@austintexas.gov .

   Invoices shall be mailed to the below address:

	City of Austin
Department	Communication Technology Management (CTM)
Attention	Accounts Payable
Email Address	CTMAPInvoices@austintexas.gov

2. **TRAVEL EXPENSES**: All travel, lodging and per diem expenses in connection with the Contract for which reimbursement may be claimed by the Contractor under the terms of the Solicitation will be reviewed against the City's Travel Policy as published and maintained by the City's Controller's Office and the Current United States General Services Administration Domestic Per Diem Rates (the "Rates") as published and maintained on the Internet at:

   http://www.gsa.gov/portal/category/21287

   No amounts in excess of the Travel Policy or Rates shall be paid. All invoices must be accompanied by copies of detailed itemized receipts (e.g. hotel bills, airline tickets). No reimbursement will be made for expenses not actually incurred. Airline fares in excess of coach or economy will not be reimbursed. Mileage charges may not exceed the amount permitted as a deduction in any year under the Internal Revenue Code or Regulations.

3. **Equal Opportunity**

   4.1.1 **Equal Employment Opportunity:** No Contractor or Contractor's agent, shall engage in any discriminatory employment practice as defined in Chapter 5-4 of the City Code. No Bid submitted to the City shall be considered, nor any Purchase Order issued, or any Contract awarded by the City unless the Contractor has executed and filed with the City Purchasing Office a current Non- Discrimination Certification. The Contractor shall sign and return the Non-Discrimination Certification attached hereto as Exhibit C. Non-compliance with Chapter 5-4 of the City Code may result in sanctions, including termination of the contract and the Contractor's suspension or debarment from participation on future City contracts until deemed compliant with Chapter 5-4.

   4.1.2 **Americans With Disabilities Act (ADA) Compliance:** No Contractor, or Contractor's agent shall engage in any discriminatory employment practice against individuals with disabilities as defined in the ADA.

4. **Right To Audit**

   5.1.1 The Contractor agrees that the representatives of the Office of the City Auditor or other authorized representatives of the City shall have access to, and the right to audit, examine, or reproduce, any and all records of the Contractor related to t amounts paid by the City to the Contractor under this Contract. Audits may occur one time per each twelve (12) month period. The Contractor shall retain all such records for a period of three (3) years

after final payment on this Contract or until all audit and litigation matters that the City has brought to the attention of the Contractor are resolved, whichever is longer. The Contractor agrees to refund to the City any overpayments disclosed by any such audit.

5.1.2 The Contractor shall include this provision in all subcontractor agreements entered into in connection with this Contract.

5. **Insurance**: Insurance is not required for this contract as Contractor will not carry out on-site work with the City.

5.1.1 **Specific Coverage Requirements.** The Contractor shall at a minimum carry insurance in the types and amounts indicated below for the duration of the Contract, including extension options and hold over periods, and during any warranty period. These insurance coverages are required minimums and are not intended to limit the responsibility or liability of the Contractor.

5.1.1.1 **Commercial General Liability Insurance.** The minimum bodily injury and property damage per occurrence are $500,000 for coverages A (Bodily Injury and Property Damage) and B (Personal and Advertising Injuries). The policy shall contain the following provisions and endorsements.

5.1.1.1.1 Contractual liability coverage for liability assumed under the Contract and all other Contracts related to the project.

5.1.1.1.2 Contractor/Subcontracted Work.

5.1.1.1.3 Products/Completed Operations Liability for the duration of the warranty period.

5.1.1.1.4 Waiver of Subrogation, Endorsement CG 2404, or equivalent coverage.

5.1.1.1.5 Thirty (30) calendar days Notice of Cancellation, Endorsement CG 0205, or equivalent coverage.

5.1.1.1.6 The City of Austin listed as an additional insured, Endorsement CG 2010, or equivalent coverage.

5.1.1.2 **Business Automobile Liability Insurance.** The Contractor shall provide coverage for all owned, non-owned and hired vehicles with a minimum combined single limit of $500,000 per occurrence for bodily injury and property damage. Alternate acceptable limits are $250,000 bodily injury per person, $500,000 bodily injury per occurrence and at least $100,000 property damage liability per accident. The policy shall contain the following endorsements:

5.1.1.2.1 Waiver of Subrogation, Endorsement CA0444, or equivalent coverage.

5.1.1.2.2 Thirty (30) calendar days Notice of Cancellation, Endorsement CA0244, or equivalent coverage.

5.1.1.2.3 The City of Austin listed as an additional insured, Endorsement CA2048, or equivalent coverage.

5.1.1.3 **Worker's Compensation and Employers' Liability Insurance.** Coverage shall be consistent with statutory benefits outlined in the Texas Worker's Compensation Act (Section 401). The minimum policy limits for Employer's Liability are $100,000 bodily injury each accident, $500,000

bodily injury by disease policy limit and $100,000 bodily injury by disease each employee. The policy shall contain the following provisions and endorsements:

5.1.1.3.1 The Contractor's policy shall apply to the State of Texas.

Exhibit B
City of Austin Statement of Work

0500 TABLE OF CONTENTS

1.0 INTRODUCTION

1.1 Purpose of Request for Proposal

The City of Austin is committed to making Austin's city government open and accessible. One particular City responsibility, the management of public information requests, presents an important opportunity to demonstrate that commitment. A digital solution is needed to support members of the public and City staff who participate in the Public Information Request (PIR) process.

The City of Austin (City) is seeking to award a contract agreement to the strongest, most qualified vendor to deliver such a solution.

1.2 Project Scope

1.2.1 General Information

When it comes to Public Information Requests, the City of Austin seeks to provide a customer experience that is efficient, transparent, and compliant with public information laws. This will involve thorough consideration of the needs of system users who submit Public Information Requests (PIRs) to the City, intake PIRs on behalf of the City, and deliver PIR responses back to requestors. For additional information about user roles and responsibilities, refer to Appendix A: Respond to Public Information Request Use Case Specification.

Responders to this RFP should develop an iterative project plan that includes comprehensive user testing and incorporation of user feedback. System users will use the project solution to engage in activities such as:

- Respond to public information request
- Evaluate performance of public information request system
- Publish information released by the PIR process

The City encourages Responders to identify opportunities for integrating the project solution with existing enterprise systems and incorporate the delivery of such integrations into the proposed project plan. For example, the City's open data portal (https://data.austintexas.gov/) could be leveraged to publish information released by the PIR process. In another example, the City sometimes requires and collects payment when responding to public information requests. In this case, the project solution should integrate with the City's existing payment processing systems as described in Requirement #011 of Appendix A.

1.2.2 City's Responsibilities

The City will be responsible for:

- Identifying priority scope implementations
- Setting work hours on City sites and work associated with the City's network
    - Normal City business hours are 7:45 a.m. – 4:45 p.m. CST, Monday through Friday no weekends or City holidays

- Approving all scope of work and or changes in the scope of work, including adds, deletions, and equal changes
- Approving process flows
- Approving implementation schedules
- Approving all measurable project objectives, including but not limited to, milestones and requirement functionality implementation through User Acceptance Testing
- Approving Vendor invoices
- Providing all data entry elements to include forms and sources of information

1.2.3 Vendor's Responsibilities

The Vendor shall be responsible for:

- All system design, software installation, programming, testing, performance tuning, training, updating, data backup, documentation and implementation required for the system.
- If third-party software is required, Vendor shall assume full responsibility for its inclusion in this solution
- Acquiring and installing of any required hardware

Note: The City reserves the right to purchase hardware from other sources

- Providing all technical documents for the proposed system and its components. These documents shall include administrator and end user manuals about product installation and maintenance, including detailed design documents for customized system application and test plans. The supplier shall grant the City the authorization to reproduce any provided documents for internal use.
- Providing detail data backup and restore plan
- Providing disaster recovery and business continuity plan
- Assisting in the development of an acceptance test plans and assist in the performance of testing the entire system. During testing, the Vendor shall be available for assistance and correction of any error detected. Testing shall be successfully performed before the City approves the final sign-off for the acceptance of the system
- Providing a detailed list of the necessary resources and expertise, complete with personnel job descriptions, which shall be required for the City to maintain the system once implemented
- Providing all functional, technical standard, project management/implementation requirements
- Adhering to City of Austin holidays and normal business hours as identified by the City in the approved Project Schedule
- Interfacing with the City Communication Technology Management Staff (CTM) technical staff on related security and network matters through a Project Communication Plan
- Interfacing with PIR staff on related project matters through a Project Communication Plan

2.0 DESCRIPTION OF EXISTING SYSTEM(S)

2.1 Current System

The City currently oversees the functions of an in-house PIR management tool, and any new system under consideration should possess enhanced capabilities from the current tool. Specifications outlined here within reflect the capabilities of a system that would operate at an enhanced level from the current system.

The current system does not provide for the publication of PIR-related information to the City's open data portal (https://data.austintexas.gov/).

Included in this section the current City of Austin Information Request process for the Office of the Chief Information Officer and other city departments.

Table A: Office of the Chief Information Officer Information Request Process Flow Diagram

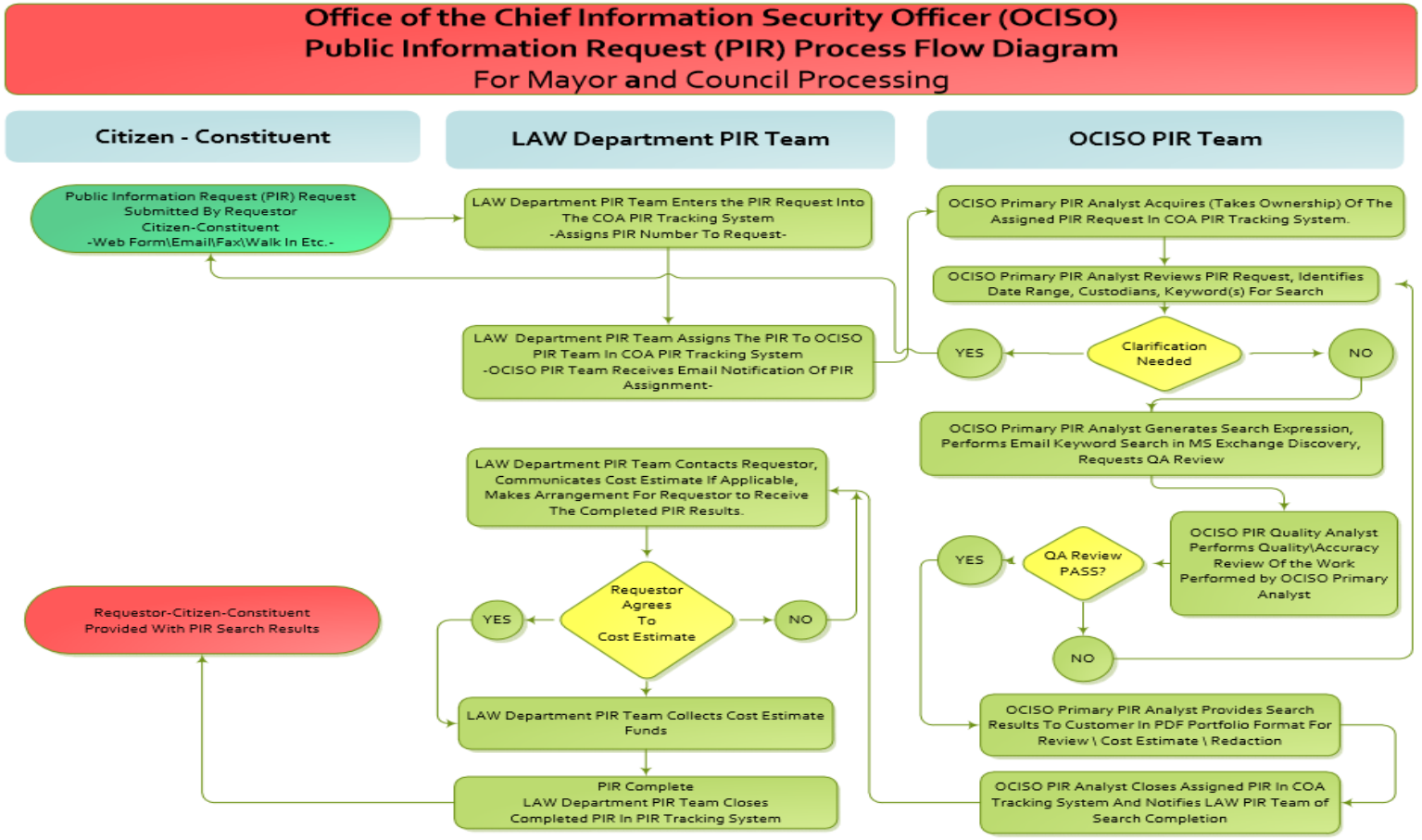
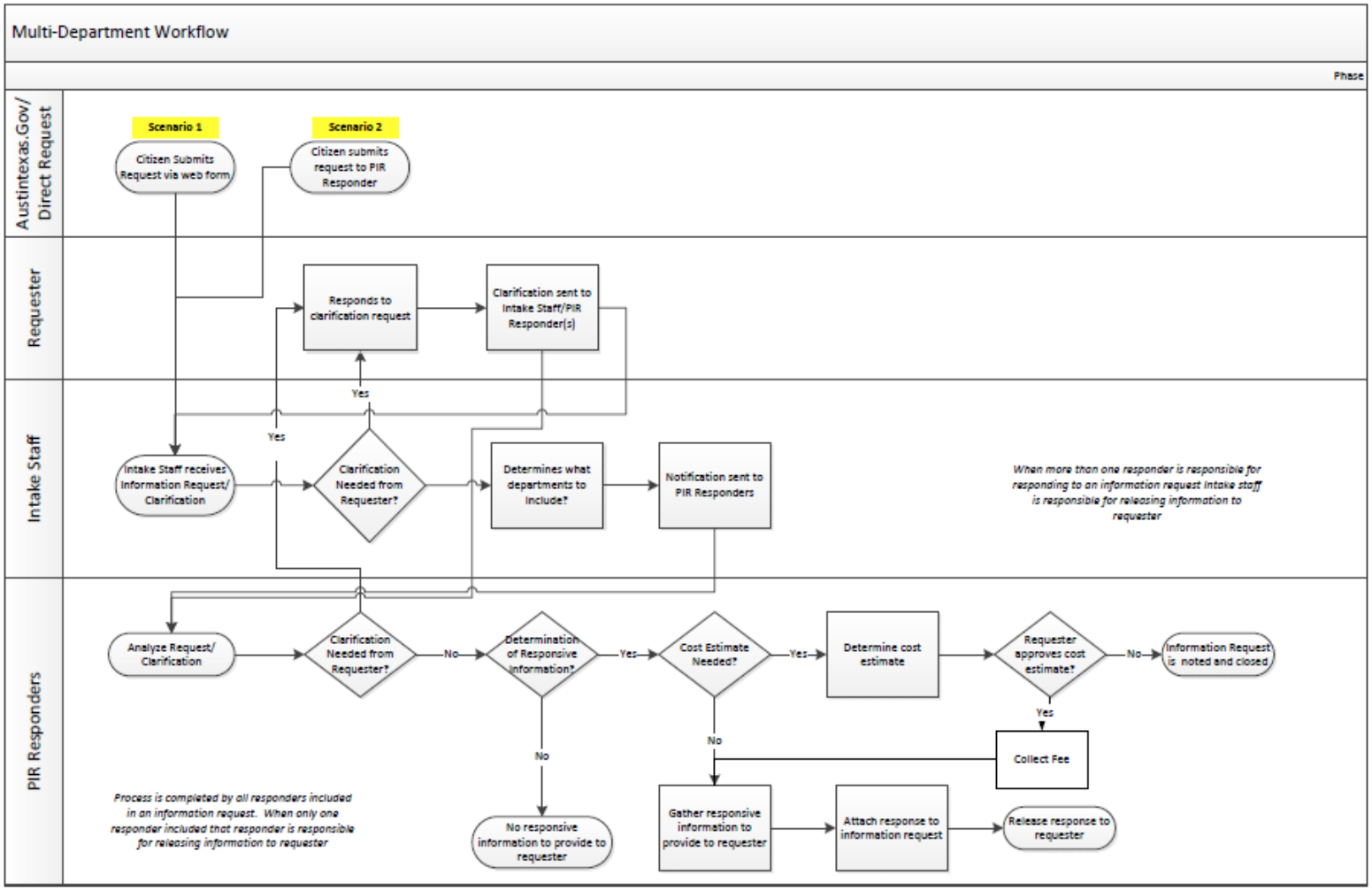


Table B: Information Request Workflow



3.0 REQUIREMENTS INFORMATION

Vendor responses to the requirements are used to evaluate proposals. The Functional and Technical Requirements, and Project Management/Implementation requirements are presented in Sections 4.0, 5.0, and 6.0 of this RFP Scope of Work.

3.1 Organization of Requirements

Requirements are grouped into three (3) areas:

Functional Requirements: These requirements describe product features and functionality requested by end users.
Technical Requirements: Developed by the City's Communication and Technology Management staff, these requirements describe the technical specifications to support the Functional Requirements and the constraints for security and networking.
Project Management/Implementation Requirements: These requirements describe the project management resources, processes, documentation and training that ensure effective product implementation and accomplishment of project objectives.

3.2 Qualifiers for Functional and Technical Requirements

3.2.1 Category Identification (ID)

"Category" ID distinguishes the requirement within each functional, technical, and project management/implementation group. "Category" ID organizes requirements by business process or technical similarity. The "Category" IDs for this RFP are:

"4" for Functional Requirements
"5" for Technical Requirements
"6" for Project Management/Implementation Requirements

3.2.2 Requirement Number

The "Requirement Number" preceded by the "Category ID" provides a unique requirement number for each requirement in the RFP. "Requirement Numbers" begin with 001 are in chronological order by "Category ID".

4 – "001", 4 – "002", 4 – "003", etc. = Functional Requirement
5 – "001", 5 – "002", 5 – "003", etc. = Technical Requirement
6 – "001", 6 – "002", 6 – "003", etc. = Project Management/Implementation Requirement

3.2.3 Type

"Type" is a sub-category providing a brief distinguishing description of the requirement within each category.

3.2.4 Use Case Requirement Number

"Use Case Requirement Number" is only with a Functional requirement These reference callouts are to the Unified Modeling Language (UML) use-case models in Appendix A which identify additional business process and functional processes desired in the Public Information Request (PIR) system and are used *for additional clarity only.*

3.2.5 Required Response

The purpose of the "Required Response" is to guide vendors in describing the item, product feature, or system customization that satisfies the requirements as stated in the "Requirement Description."

Requirement Response Label	What the label means:
Base	Will accomplish this Functional Requirement as part of the basic project solution
Custom	Will accomplish this Functional Requirement, and to do so will dedicate resources to performing custom work. Additional description of the customization and how it will be performed is provided
Not Provided	Will not accomplish this Functional Requirement
Third-Party	Will accomplish this Functional Requirement by engaging a solution developed and or coordinated by a third party. Additional description of the third party engagement is provided

3.2.6 Requirements Rating – Mandatory

Requirements in this Request for Proposal have a rating of **Mandatory** indicating the criticality of the requirements in achieving product and project objectives. All requirements are **Mandatory** unless rated otherwise.

4.0 FUNCTIONAL REQUIREMENTS

4.1 Overview of Functional Requirements

Functional requirements, which describe product features and functionality requested by City of Austin, are grouped in **Section 4.3** according to topics that represent the following business processes:

- Intake of Information Request
- Assign Department and/or Responder
- Determine Fee
- Collect and Disseminate Requested Information
- Generate Reports

Each Functional Requirement is accompanied by a unique identifier. A use case requirement number may also be included. The use case requirement number is a reference to an enumerated requirement in **Appendix A**: Respond to Public Information Request – Use Case Specification. This reference provides additional context to aid the Vendor in understanding business or functional processes that may be related to the requirement.

The City encourages and is open to innovative solutions when Vendors meet the mandatory requirements. The Vendor may propose alternative processes or technologies when relevant.

4.2 Responding To Functional Requirements

To ensure that a proposed solution is thoroughly represented, Vendors should respond to each Functional requirement. Itemized requirements in this section have a rating of Mandatory indicating the criticality of the requirements in achieving product and project objectives. See **Appendix C** for the City's Functional requirements.

Additional reference callouts are to the business process workflow for Intake Staff and PIR Responders in S**ection 2.1**.

Each Vendor response to a Functional Requirement must include the following:

- Indication as to whether or not the Vendor's proposed solution will meet the requirement,
- A narrative description explaining how the Vendor will accomplish the requirement,
- Identification of any involvement of customization or third-party engagement, and
- Additional narrative to explain the need for customization or third-party engagement, when applicable.

To facilitate this, Vendors should include on the following four labels in each requirement response:

Requirement Response Label	What the label means:
Base	Will accomplish this Functional Requirement as part of the basic project solution
Custom	Will accomplish this Functional Requirement, and to do so will dedicate resources to performing custom work. Additional description of the customization and how it will be performed is provided
Not Provided	Will not accomplish this Functional Requirement
Third-Party	Will accomplish this Functional Requirement by engaging a solution developed and or coordinated by a third party. Additional description of the third party engagement is provided

4.3 Itemized Functional Requirements

4.3.1.1 Intake Information Requests

Functional Requirement Number	Requirement Description	Related Reference in Appendix A
001	Ability to develop an online and knowledge base that will provide requester's the ability to submit request directly into the system	1
002	Ability for City of Austin Law Department's website to transmit submitted Information Request into system	
003	Ability for Intake Staff to input information Request into system	
004	Ability for all Information Request to be completely managed by Intake Staff to complete the following but not limited to: • Assignment of one or more PIR Responders • Final correspondence to requester • Add/Remove templates	
005	Ability to validate requestor email by sending a confirmation code to the Requester email address	1
006	Ability to attach additional documents and videos with an Information Request. Attachment types to include but not limited to the following: • MSG • JPEG • EXCEL • AUDIO and VIDEO • PDF • WORD	1
007	Ability to indicate requesters preferred pickup method such as but not limited to Web portal, physical pickup, mail to postal service address, or email.	1

Functional Requirement Number	Requirement Description	Related Reference in Appendix A
008	Ability to provide requestor confirmation submitted information request with the ability to: • Summarize request • Provide City Contact Information • Anticipated process and/or estimated cost	1
009	Ability to assign unique identifier to each request received (identification number) *Refer to **Section 2.1** for workflow process.*	2
010	Ability to identify duplicate requester and merge	3
011	Ability for internal and external requesters to communicate within the system to complete the following including but not limited to: • Request additional information from requestor • Communicate with requester per preferred communication preference to obtain additional clarity from requester	4, 5

012	Ability to customize unlimited number of rules for automated routing for request and notifications for the following including but not limited to:
	• Adjust requester response timeframe window
	• Notify requestor when response timeframe is expiring
	  o Summary of request
	  o New expected date
	• Send email to PIR Responders
	• Email notification to the assigned PIR Responder for any change or clarification
	• Adjust time out period by administrative users
	• Send additional notification at a set period reminding requester of expected date
	• Override and/or reset expected date
	• Allows Intake Staff to include Multiple instances of Requestors
	• Re-open a closed Information Request to reassign to one more instances of additional requesters by Intake Staff
	• Provide/Request status update notifications to PIR Responders
	• Add customized federal and local business holidays
		5, 6, 7, 8, 12, 13

013	Ability to notify Intake Staff when identified tiered administrative users has completed the following but not limited to: • Information Request creation • Information Request status • Change in status • Notes when added to Information Request	
014	Ability to track and log actions taken within the system to complete the following including but not limited to: • Information request activities throughout the lifecycle of the request	5,7

Functional Requirement Number	Requirement Description	Related Reference in Appendix A
	• Historical dialog between Requester, Intake Staff and other PIR Responders • Activities, dates/time and responsible staff details • Actions by department PIR Responder provides Intake Staff status to the information request • All timing associated with notification, response or other intake Staff or PIR Respondent activities.	
015	Ability to generate email to requestor for clarity request and associate request and response to original request.	5
016	Ability to provide requester the option to include attachments to clarity request	5
017	Ability to provide Intake Staff and PIR Responder the ability to enter and view all notes	5

4.3.1.2 Assign Department and/or Responder

Functional Requirement Number	Requirement Description	Related Reference in Appendix A
018	Ability to align certain users with specific departments and offices	7
019	Ability for approved city staff to create and modify templates to be utilized by PIR responder	7
020	Ability to provide summary guidance for Intake Staff to select the appropriate template based on the type and scope of an Information Request.	7
021	Ability to automate notification to users when Information Request are assigned	8
022	Ability to perform and complete workflow (Information Request) integration	8, 12, 13
023	Ability to provide continuous metering of time of submission and anticipated completion date	8
024	Ability to provide PIR Responders a work queue of open active Information Request	8

4.3.1.3 Determine Fees

Functional Requirement Number.	Requirement Description	Related Reference in Appendix A
025	Ability to calculate, assess and track fees and staff time associated with requests	9
026	Ability to calculate fee estimates and to manage fees associated with routine or frequent Information Requests	9
027	Ability to store historical Information Request fees for use in future cost estimates	9

4.3.1.4 Collect and Disseminate Requested Information

Functional Requirement Number.	Requirement Description	Related Reference in Appendix A
028	Capability to retain large amounts of data within the system	12
029	Ability to search to find documents, issues and user data	12
030	Ability to view common formats by Requestor without specialized applications	12
031	Ability to provide overview of all Information Request task assignment, status and information collected	12
032	Ability to provide Intake Staff continuous status indication throughout the Information Request lifecycle.	12
033	Ability to provide Intake Staff notification when all PIR Responders have provided responses to information request	12
034	Ability to determine PIR Responders responses does not contain sensitive information including but not limited to the following: • Date of Birth • Social Security Number • Driver License Number	12
035	Ability to provide tool(s) to redact information from select information	12
036	Ability to enable data storage and retrieval from achieved data in a manner which is consistent with production data.	13
037	Ability to convert the disseminated information into a machine-readable format for the purpose of facilitating online publication	
038	Ability to send requestor responses via encrypted email. Email encryption must utilize a minimum 256-bit key length.	

4.3.1.5 Generate and Deliver Reports

Functional Requirement Number.	Requirement Description	Related Reference in Appendix A

039	Ability for tier administrative staff to report on the following but not limited to:
	• Dates
	  ○ Submitted/Open Date,
	  ○ Initial 10th Business Day
	  ○ Date Closed
	  ○ Number of days Open
	  ○ PIR Responder Completion Date
	  ○ Date Ranges)
	• Assigned PIR Responders
	• Subject/Topic
	• Status
	• Requester
	• Information Request Description
	• Number of Days Information Request is opened	

040	Ability for PIR Responder to report on the following but not limited to: • Subject/Topic • Status • Open/Active number of Information Request • Assigned Staff	
041	Ability to export information about the status of an individual PIRs in CSV format including but not limited to: • Date Received • Subject/Topic • Current Status • Date Completed	

5.0 TECHNICAL REQUIREMENTS

5.1 Overview of Technical Requirements

Technical requirements, which describe technical specifications to support the Technical Requirements and City of Austin security and networking constraints, are grouped in **Section 5.4** according to the following categories:

- Application Architecture
- Business Continuity and Disaster Recovery
- Data Storage and Archiving
- Database Architecture
- Information Management

Each Technical Requirement is accompanied by a unique identifier.

The City prefers a Cloud (hosted) solution, Software as a Service (SaaS) solution. The Vendor may provide a complete solution or collaborate with Cloud providers to propose the SaaS solution.

The City provides a fully functional IBM Integration Bus (IIB), enterprise service bus (ESB) to include an ESB instance in our demilitarized security zone to interface with internal city applications discussed in our use-case model. The City identified the required performance response in each Functional requirement.

The City encourages and is open to innovative solutions when Vendors meet the mandatory requirements. The Vendor may propose alternative processes or technologies when relevant.

5.2 Responding To Technical Requirements

To ensure that a proposed solution is thoroughly represented, Vendors should respond to each Technical Requirement of the RFP. Itemized requirements in this section have a rating of Mandatory indicating the criticality of the requirements in achieving product and project objectives. See **Appendix D** for the City's Technical Requirements.

If the Vendor requires the City to have technologies not listed in the Technical Requirements, The Vendor shall list those requirements in their RFP responses

Each Vendor response to a Functional Requirement must include the following:

- Indication as to whether or not the Vendor's proposed solution will meet the requirement,
- A narrative description explaining how the Vendor will accomplish the requirement,
- Identification of any involvement of customization or third-party engagement, and
- Additional narrative to explain the need for customization or third-party engagement, when applicable.

To facilitate this, Vendors should include one of the following four labels in each technical requirement response:

Requirement Response Label	What the label means:
Base	Will accomplish this Functional Requirement as part of the basic project solution
Custom	Will accomplish this Functional Requirement, and to do so will dedicate resources to performing custom work. Additional description of the customization and how it will be performed is provided
Not Provided	Will not accomplish this Functional Requirement
Third-Party	Will accomplish this Functional Requirement by engaging a solution developed and or coordinated by a third party. Additional description of the third party engagement is provided

If the Vendor requires the City to have technologies not listed in the Technical requirements, The Vendor shall list those requirements in their RFP responses.

5.3 Itemized Technical Requirements

5.3.1.1 Application Architecture

Technical Requirement Number	Requirement Description
001	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.
002	No requirement to deploy application code to client workstations (note: Java Runtime Environment (JRE) is an exception).
003	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 versions is defined as the manufacturer's latest production point version of the product.
004	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.
005	The application provides built-in application and system configuration tables accessible by all modules.
006	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).
007	The application provides copy, cut, paste, and undo functions from data fields and screens to other applications.

Technical Requirement Number	Requirement Description
008	The application provides ability to perform mass changes to a defined group of transactions with appropriate selection criteria.
009	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.
010	The application provides ability to drill down from a transaction view to the supporting source document or record, regardless of the module source.
011	The system provides ability to restrict free form entry (e.g., require use of drop-down calendar for date field).
012	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.

5.3.1.2 Business Continuity and Disaster Recovery

Technical Requirement Number	Requirement Description
013	The system provides full recovery and system backup capabilities for all online and batch transactions according to City-specified timeframes.
014	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.

5.3.1.3 Data Storage and Archiving

Technical Requirement Number	Requirement Description
015	The solution supports future releases of the application without rendering the archived data unusable.
016	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)
017	The solution ability to work with City of Austin to identify and implement integration additional storage (in-house or another cloud hosted solution such as Amazon Web Services)

5.3.1.4 Database Architecture

Technical Requirement Number	Requirement Description
018	The application provides standardized data extraction Application Program Interface (API) to allow import and export of data to other systems.

019	The application provides ability to encrypt sensitive data when required by federal, state or city compliance (e.g., PII, PCI, HIPAA, etc.).
020	The solution uses the same data validation criteria for bulk data loads as it does for manual data entry.

5.3.1.5 Information Management

Technical Requirement Number	Requirement Description
021	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).
022	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.
023	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.
024	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.
025	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.
026	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.
027	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.

5.3.1.6 Infrastructure

Technical Requirement Number	Requirement Description
028	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.

5.3.1.7 Security and Authentication

Technical Requirement Number	Requirement Description
029	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), Sensitive Personally Identifiable Information (PII).
030	The system provides protection against unauthorized access to data by persons and other software programs.
031	The system masks (i.e., substituting characters with '*') passwords as they are entered into the system.
032	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.
033	The solution provides a method to change the passwords for built-in system accounts (i.e. Administrator, Admin, Super, etc.)
034	Passwords must NOT be included in automated sign-on procedures, stored unencrypted in cache, or transmitted as clear text over the network.
035	The application allows the Application Administrator to restrict generic logins.
036	The system uses Microsoft Active Directory Federated Services (ADFS) for federated identity management.
037	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)
038	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.
039	The system can be configured appropriately to perform according to applicable Federal, State, and Local standards and regulations.

6.0 PROJECT MANAGEMENT / IMPLEMENTATION REQUIREMENTS

6.1 Overview of Project Management / Implementation Requirements

Project Management / Implementation requirements, which describe project management specifications to manage and support the requirements and City of Austin project management office, are grouped according to the following categories:

- Project Management Methodology
- Implementation Methodology
- Training Methodology
- Licensing

Each Project Management/Implementation Requirement is accompanied by a unique identifier. This reference provides additional context to aid the Vendor in understanding project management processes that may be related to the requirement.

The City encourages and is open to innovative solutions when Vendors meet the mandatory requirements. The Vendor may propose alternative processes or technologies when relevant.

6.2 Responding To Project Management / Implementation Requirements

To ensure a proposed solution is thoroughly represented, Vendors should respond to each Project Management / Implementation Requirement. Itemized requirements in this section have a rating of Mandatory indicating the criticality of the requirements in achieving product and project objectives. See **Appendix E** for the City's Project Management/Implementation Requirements.

6.2.1 Vendor's Project Management Methodology

Responding Vendors shall provide documentation describing their proven project management methods. The City recognizes each Vendor shall recommend a project management methodology that demonstrates a commitment to completing the project on time and within budget. Documentation to be included:

- Project Management Methodology (Model) Used
- Explanation of the Methodology
- Explanation of how the Methodology shall be used on this project
- Explanation of how the Vendor shall staff this project for the project's life-cycle, including all specific personnel by name, their technical title, role and responsibilities on the project, and resumes including work experience in related implementations, education and tenure with the Vendor.

6.2.2 Implementation Methodology

Each Implementation requirement shall always indicate explicitly whether or not the Vendor's proposed Services meets the Implementation requirements. Vendors shall describe the format for each document they shall provide and be prepared to deliver selected system documents upon request during the evaluation and selection process outlined in Section 0600. During the project's initiating, designing, implementation and closing phases and prior to system acceptance, the selected Vendor shall profile and maintain updates on the following system documentation:

- Project Schedule(s) based on implementation milestones
    - Schedule Development
    - Baseline Schedule
    - Schedule Updates

6.2.3 Training

The Vendor shall provide the following Training Requirements:

- The Vendor shall develop a long-term Training Program with reproducible Training Materials for conducting training over the solution's life-cycle within the City's PIR Department for:
    - Training for Ten (10) City technical staff

The Vendor shall provide reproducible Training Materials adapted for use by City staff to conduct new end user training and re-training.

6.3 Itemized Project Management / Implementation Requirements

6.3.1.1 Project Management

Project Management Requirement Number	Requirement Description
001	Provide a Project Manager (PM) to represent the Vendor in the management of the Project, interfacing with the City Project Manager (PM) in any decisions relating to the Project
002	Assume and lead all day-to-day management of Vendor personnel, including subcontractor personnel, and associated Deliverables related to the required services
003	Provide a robust project management methodology founded on industry best practices
004	Conduct project management activities through the life of the project and execute the associated plans
005	Document deliverable details, formats, and acceptance criteria in Deliverable Expectation Documents (DEDs) as mutually agreed upon by the City and the Vendor
006	Provide, update, and maintain a Project Schedule (e.g. in MS Project)that includes the following key components:

Project Management Requirement Number	Requirement Description
	• Work breakdown structure • Task and activities required to successfully complete the Project • Schedule/milestone tracking and resource allocation • Critical path identification and dependencies Provide periodic updates (as mutually agreed upon by the City and the Vendor) to Project Schedule which is maintained by the Vendor
007	Provide, update and maintain a formal Project Management Plan (PMP) that includes the following key components: • Project initiation activities • Issues tracking, escalation and resolution • Change request approval, management and tracking • Deliverable/product review and approval and other acceptance criteria • Risk Management, identification, quantification of impact, monitoring, and mitigation plans • Quality management • Vendor and subcontractor resource management • Project success evaluation criteria and Project close-out activities • Status and of the reporting activities • Status reporting templates (including deliverable status reports, issues, risks, plans vs. actual status, etc.)
008	Provide and implement risk mitigation measures, contingency plans and disaster recovery plans as high priority risks are identified and monitored
009	Provide a Communication Plan and Matrix to document the communications with all Project stakeholders throughout the life of the Project as mutually agreed upon by the City of the Vendor communication with internal and external end users
010	Provide Project Status Reports and conduct regularly scheduled status meetings reviewing Project progress, risk, mitigation, issue resolution, deliverable status, and next steps as mutually agreed upon by the City and the Vendor
011	Use the Microsoft Outlook systems provided for all e-mails and scheduling for all Project-related communications
012	Prepare system Change Request as required based on all added, deleted, and/or modified scopes of work
013	Conduct and document Lessons Learned meetings at key intervals with Project Team. Apply Lessons Learned to future design and implementation phases

6.3.1.2 Implementation

Implementation Requirement Number	Requirement Description
014	Test the capability of failover to secondary Disaster Recovery site
015	Provide the Configured Hardware Environments (testing) to test and/or demonstrate all required functionality has been satisfied
016	Provide and document test results in a Documented Successful Testing Results deliverable
017	Validate the system for compliance with the Security Requirements
018	Correct defects found as a result of testing efforts and record all defect in a Defects Log
019	Provide Go/No-go Documentation, including the Production Cutover Plan and the Go-Live Checklist
020	Conduct Go/No-go Meetings with the City's staff and Vendor's technical team

6.3.1.3 Training

Training Requirement Number	Requirement Description
021	Provide formal Project Team Training Plan to document City Project Team training requirements

6.3.1.4 Licensing

Licensing Requirement Number	Requirement Description
022	Provide the licensing model necessary to meet each of the required project objectives
023	Provide cost model for hosting and integration to work with City of Austin hosted solution or working with premise storage solution

7.0 LIST OF APPENDICES FOR THIS SCOPE OF WORK

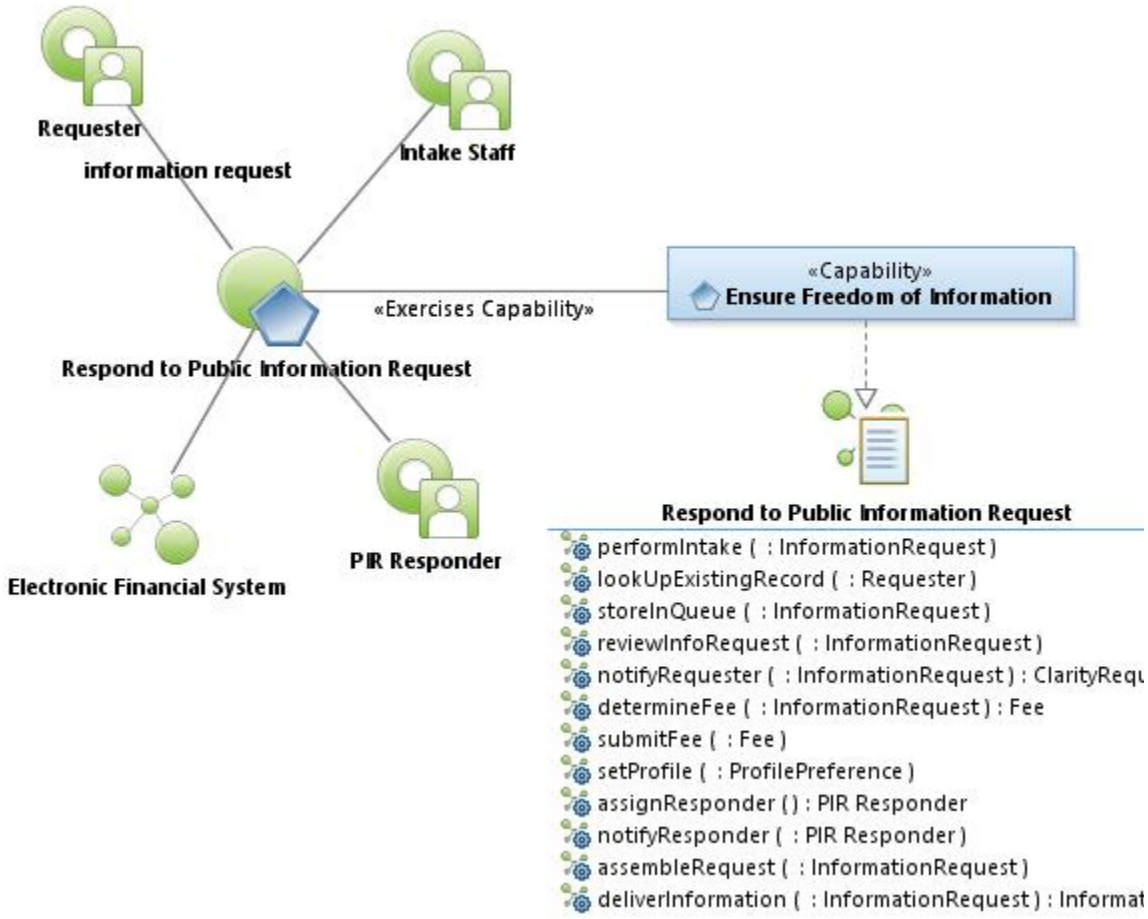
7.1 Appendices

- **Appendix A Use-Cases (References for clarity only)**
- **Appendix B Technical Reference Model**
- **Appendix C Functional Requirements**
- **Appendix D Technical Requirements**
- **Appendix E Project Management/Implementation Requirements**

7.1.1 Appendix A – Use Case Specification

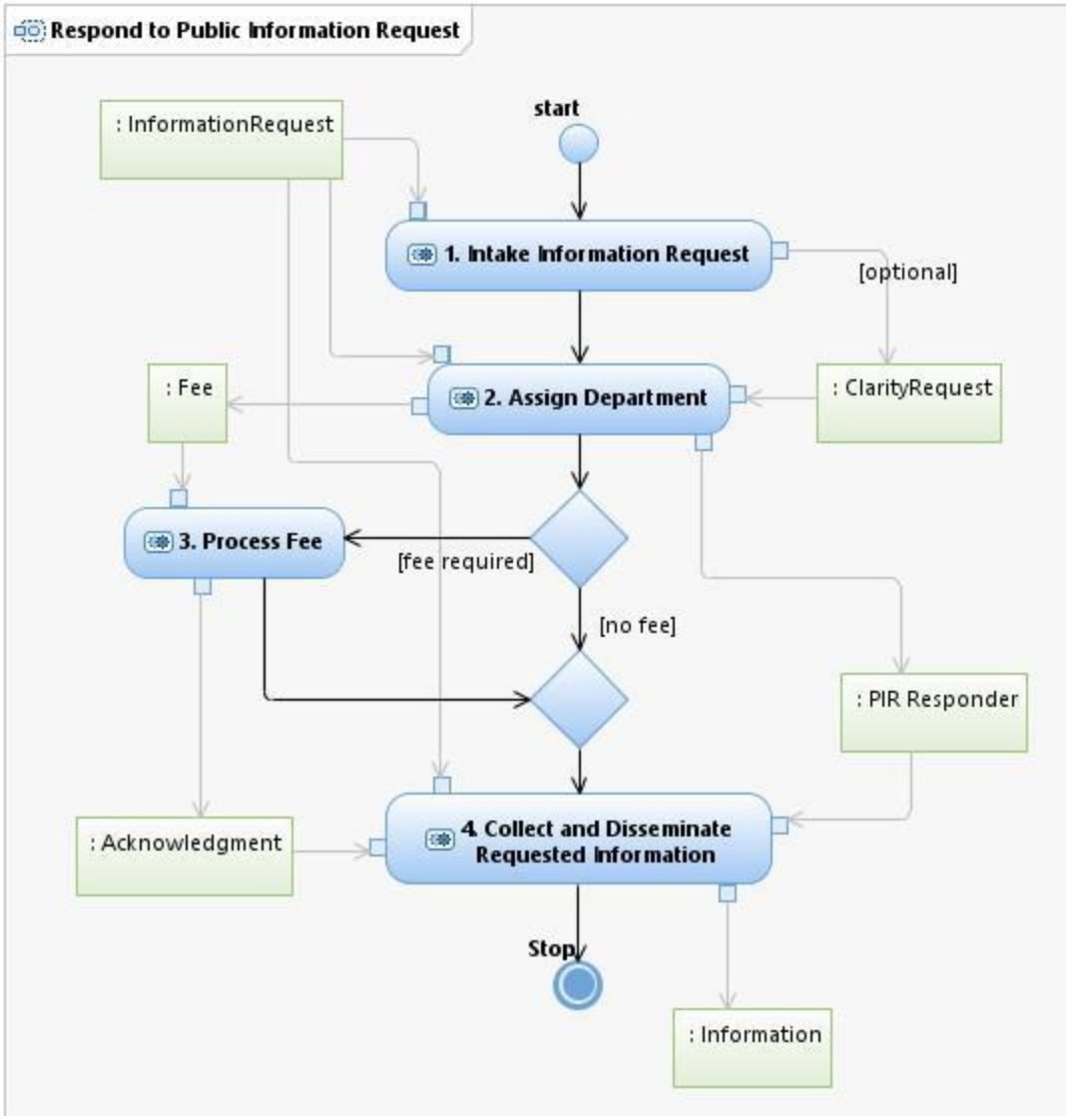
Respond to Public Information Request
Use Case Specification

09/16/2015

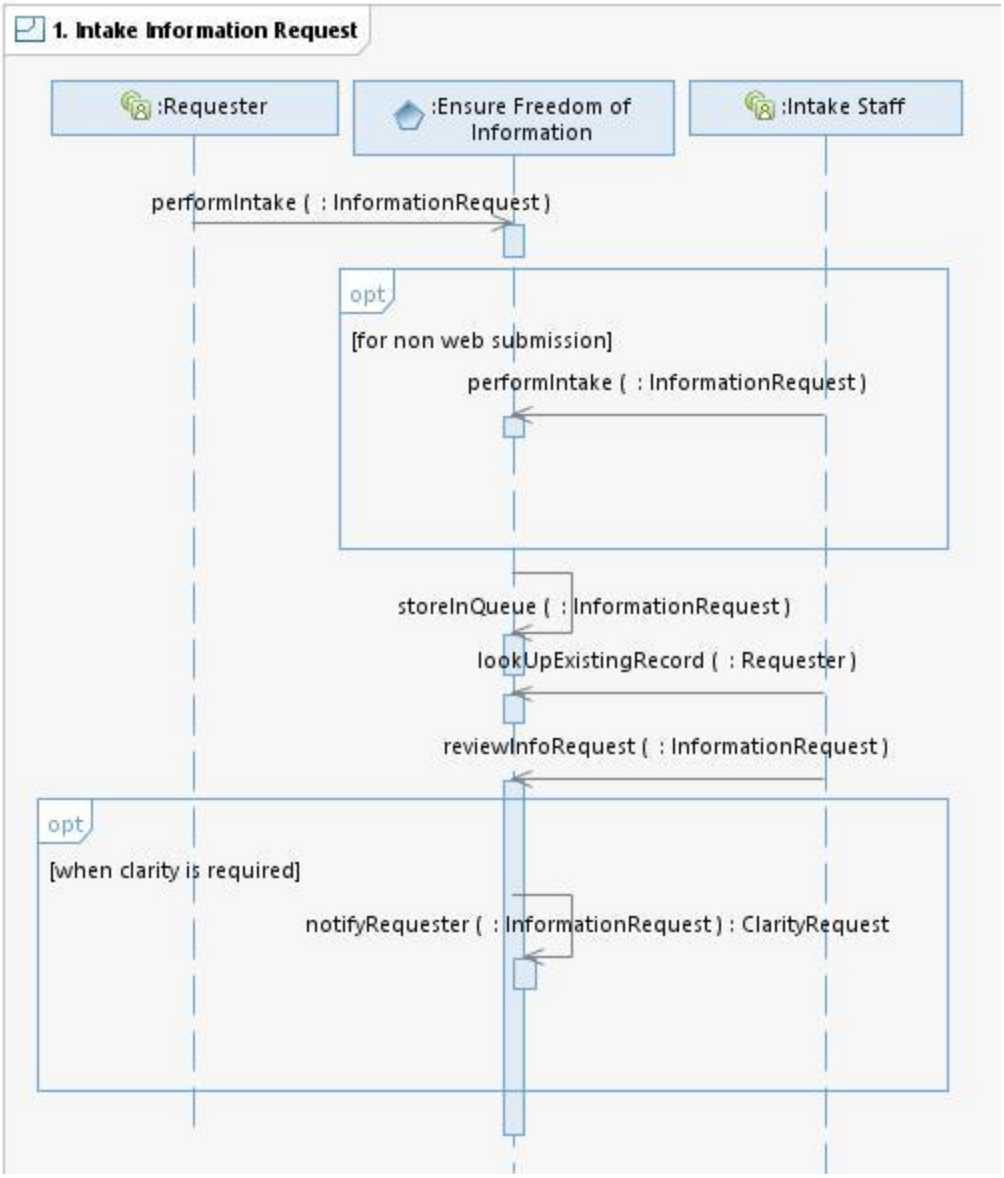


Respond to Public Information Request
Use Case Model

Scope: Intake Staff review Requester Information Request for clarity and completeness. Requester may submit for information using multiple methods to include email, letter or using the city's Web portal. Submissions enter into a queue for review. Intake Staff may contact Requester to seek additional clarification on request. The Intake Staff assign PIR Responders from various departments to collect information. The PIR Responder uses the system to determine fee or fee estimate for complex Information Requests. Requester submits a fee to cover expense for accepted and approved information requests. Simple information requests do not require a fee. Once adjudication of fee occurs (if required), the PIR Responders assemble the Information Request. After review of the material for completeness, the system delivers requested information to the Requester.



Interaction Overview

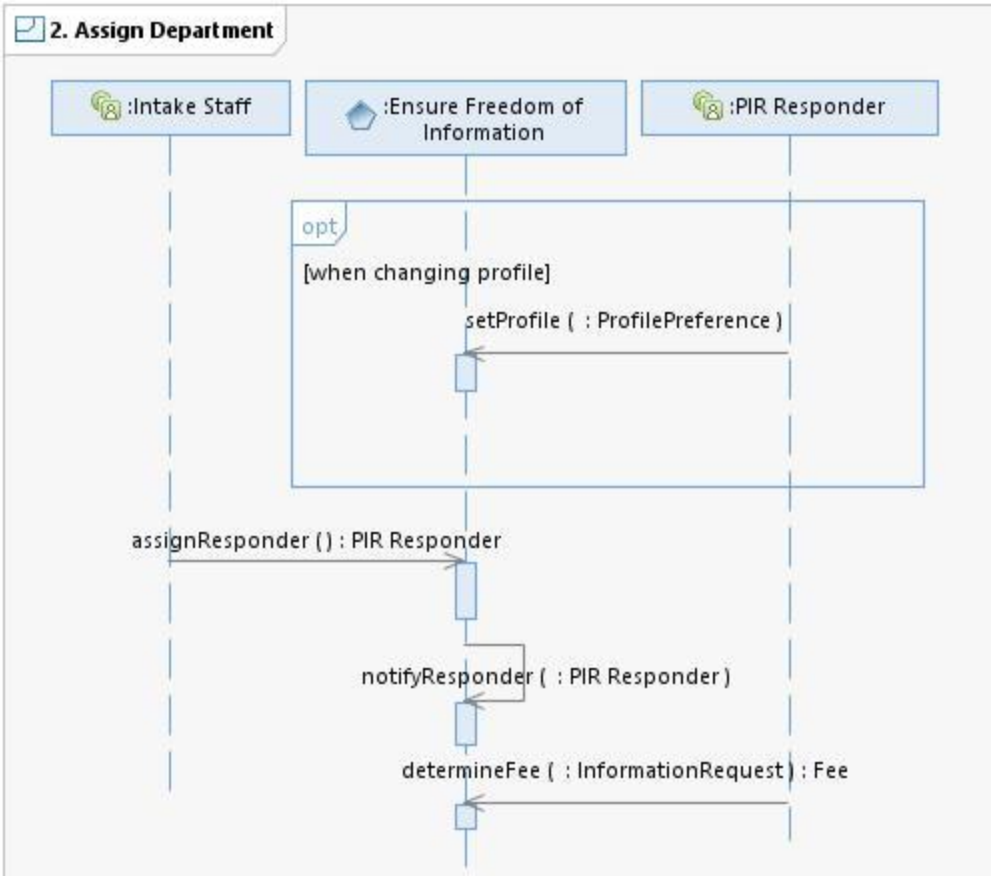


1. Intake Information Request
Sequence Diagram

Req#	Type/Interface - Requirement Description	Performance
001	**Ensure Freedom of Information/performIntake**	3.1.6 Ability to develop an online and knowledgebase that will provide requester's the ability to submit requests directly
	When a Requester makes an Information Request using the city's Web portal, the Requester completes the entry form to include name, address, email address and phone number. The system allows for incomplete entries (ex., organizational affiliation, business, name, address, phone, etc. are not required) for the Information Request. When using the Web portal, however, the system requires	

Req#	Type/Interface - Requirement Description	Performance
	a valid email address for an anonymous submission. The system validates Requester email by sending a confirmation code to the Requester email address - the Requester must use the system to validate email ownership. The system provides ability to attach additional documents with the Information Request. The Requester uses the Web portal to make an Information Request and indicate preferred delivery method (ex., Web portal, hard copy, or other media such as compact disc). The system defaults to deliver Information Request items electronically through the Web portal or emailed with attachments depending on the requested item. The volume of some Information Request items necessitate electronic delivery such a video files. The system provides the Requester the ability to indicate pickup method such as Web portal, physical pickup, mail to postal service address, or email. For non-Web submission such as written letter, other paper submission or email, the Intake Staff uses the system to complete the entry form on behalf of the Requester. Intake Staff use the system for all Intake Request items no matter the source. Intake Staff enters all the text information into the system, scans or converts the submission (ex., email) to Portable Document Format (PDF) and uses the system to attach the PDF document to the Information Request entry. To manage Requester expectation, the system provides confirmation using a system generated email or letter summarizing city contact information, anticipated process and/or any associated costs.	into the system.
002	**Ensure Freedom of Information/storeInQueue** Once complete, the Requester uses the Web portal to submit the Information Request. The system assigns a unique identifier and stores the Information Request in a queue for completeness check review by the Intake Staff.	3.2.4 Unique identifier for each request processed (identification numbers).
003	**Ensure Freedom of Information/lookUpExistingRecord** The Intake Staff use the system to identify if existing Requester demographic record exists in the system using identification information provided by the Information Request. The system assists the Intake Staff in merging duplicative Requester records while maintaining the integrity of associated historic Information Request items.	No requirement identified.
004	**Ensure Freedom of Information/reviewInfoRequest** The Intake Staff use the system to review the Information Request for completeness and clarity. When required, the Intake Staff use the system to request additional information from the Requester. The Intake Staff enters the clarity description into the system - depending on the Requester communication preference, the system generates an email or paper letter requesting clarity from the Requester.	3.3.10 Ability for internal and external requesters to communicate within the system.

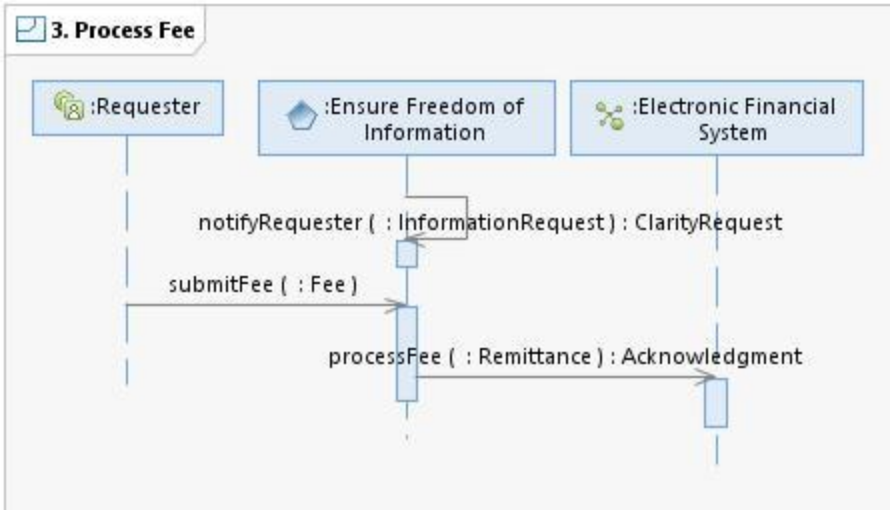
Req#	Type/Interface - Requirement Description	Performance
005	**Ensure Freedom of Information/notifyRequester** For Web portal submissions, the system generates an email containing the Information Clarity Request. Within the email, the system provides a URL link to direct the Requester to a form to add clarity description associated with the original request. The Web link expires after set period adjustable by approved city staff. At some adjustable set period, the system sends a secondary notice to the Requester prior to link expiration. The original Web submission remains intact while the added submission acts as an additional submission (addendum to the request). The system provides the Requester an option to include document attachments to the Clarity Request. There are no limits to the number of additional Clarity Requests by the system. Clarity requests may occur anytime during the PIR Responder activity. At any phase in the Information Request process, the PIR Responder may request additional clarity. The system identifies and stores with the Information Request the identity of the requesting city staff. Clarity descriptions are visible to all PIR Responders and Intake Staff assigned to the Information Request task. The Requester may respond in writing or by email to a clarity request - in this situation, the Intake Staff enters the clarity response into the system and attaches a PDF version of the original. Approved staff members use the system to observe the historic dialog between Requester, Intake Staff and other PIR Staff clarity dialog. The system provides Intake Staff and PIR Responder the ability to enter viewable notes shared among the task participants, but not viewable or released to the Requester. The Notification informs Requester of a required fee and informs Requester when Information Request is ready for pickup or delivery.	3.3.10 Ability for internal and external requesters to communicate within the system. 3.2.8 Unlimited number of customizable rules for automated routing of requests and notifications. 3.2.3 Tracking and logging features of actions taken within the system.



2. Assign Department
Sequence Diagram

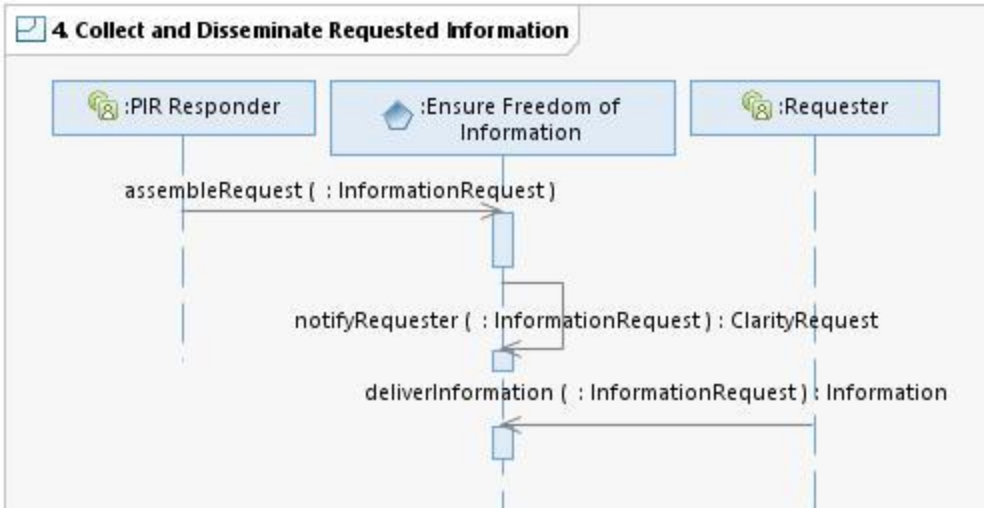
Req#	Type/Interface - Requirement Description	Performance
006	**Ensure Freedom of Information/setProfile** The PIR Responder and Intake Staff use the system to set desired notification elements such as (but not limited to) update to Requester Clarity Request, Intake Staff or PIR Responder Information Request comment, flagged interest in a particular Information Request not currently assigned, etc. All Notifications are by email. Intake Staff control some profile items.	3.1.4 Automated receipt and routing of requests and notifications, as well as customizable rules for those automated features. 3.3.5 Automated status-update notification to users (email).
007	**Ensure Freedom of Information/assignResponder** The Intake Staff use the system to assign department PIR Responder(s) to an Information Request. Only authorized Intake Staff may add or remove department PIR Responder reviews. The	3.1.4 Automated receipt and routing of requests and notifications, as

Req#	Type/Interface - Requirement Description	Performance
	system tracks Information Request activities using a log or similar method to indicate Information Request activity throughout the lifecycle of the request. Information log include activities, dates/time and responsible staff details, etc. The system provides commonly used PIR Responder templates modifiable by approved city staff. The system provides summary guidance for the Intake Staff to select the appropriate template based on the type and scope of the Information Request. The Intake Staff use the system to add or remove department PIR Respondent on selected templates as needed. Once satisfied with the PIR Responder list, the Intake Staff use the system to submit PIR Responder tasks. The system log file activity tracking actions by department PIR Responder provides Intake Staff status to the parent Information Request.	well as customizable rules for those automated features. 3.3.2 Ability to align certain users with specific departments and offices. 3.3.8 Tiered administrative settings for top-level users. 3.2.3 Tracking and logging features of actions taken within the system.
008	**Ensure Freedom of Information/notifyResponder** The system sends an email to the PIR Responder, which contains a URL link to the assigned Information Request. The PIR Responder selects the system provided URL to load and observe the Information Request. The system provides email notification to the assigned PIR Responder for any change or clarification to a request or other selectable profile items. The system logs all timing associated with notification, response or other Intake Staff or PIR Respondent activities. The system provides continuous metering of time of submission and anticipated completion date.	3.2.8 Unlimited number of customizable rules for automated routing of requests and notifications. 3.3.4 Automated notification to users when requests are assigned. 3.3.12 Workflow integration.
009	**Ensure Freedom of Information/determineFee** Some information requests require fees to pay for supplies and labor to assemble the requested information. The PIR Responder use the system to calculate fee estimates and to manage fees associated with routine or frequent Information Requests. The system stores historical Information Request fees for use in future cost estimates. Requester must submit fees or initial fee estimate prior to Information Request activities. For some complex, labor-intensive requests, there may be additional charges prior to receiving the information requested.	3.1.2 The ability to calculate, assess, and track fees and staff time associated with requests.



3. Process Fee
Sequence Diagram

Req#	Type/Interface - Requirement Description	Performance
010	**Ensure Freedom of Information/submitFee**	No requirement specified.
	The Requester uses the Web portal to submit required fee.	
011	**Ensure Freedom of Information/processFee**	No requirement specified.
	Interface to the city's online financial credit card, debit card, and automated clearinghouse (ACH) service provider.	



4. Collect and Disseminate Requested Information Sequence Diagram

Req#	Type/Interface - Requirement Description	Performance
012	**Ensure Freedom of Information/assembleRequest** Departments gather information based on the Information Request and clarity response in various formats. The system aids in delivering common formats viewable by the Requester without specialized applications - good examples include Portable Document Format (PDF). In some circumstances, Intake Staff and/or PIR Responder print hardcopy or copy media to CD ROM for Requester pickup. The PIR Responder uses the system to attach the information requested to the assigned information request task (by unique identifier). The system allows for links (i.e., Uniform Resource Locator - URL) for information sources visible and accessible to the Requester when released. The system ensures all Information Request tasks are associated and reported in consistent form using a unique identification relationship to include status of department assignments. PIR Requester gathered information is visible to the unique identification Information Request while maintaining visible relationship with other department PIR Requester responses. The system provides overview of all Information Request task assignment status and information collected. The system provides Intake Staff continuous status indication throughout the Information Request lifecycle. Assembly is where material is reviewed for releasability, personal identification information, and confidentiality, etc. - for sensitive material, the system tracks approving official when indicated or non-releasable material. The system provides tools to redact select information.	3.2.2 Capable of retaining large amounts of data within the system. 3.3.2 Ability to align certain users with specific departments and offices. 3.2.6 Search functionality to find documents, issues, and user data. 3.3.12 Workflow integration.

013	**Ensure Freedom of Information/deliverInformation**	3.3.12 Workflow integration. 4.4.1 The solution should enable data storage and retrieval from archived data in a manner which is constant with production data.
	Guided by a URL link in a Notification, the system provides the Requester a URL link to a Web portal containing additional URL(s) referencing the information requested. Similar to a Clarity Request, the Notification of delivery times out after a prescribed period. The time out period is adjustable by approved city staff. In addition, the system sends additional Notification at a set period reminding Requester of expiration date. The system provides Intake Staff the ability to override and/or reset expiration. The system allows Intake Staff to include multiple instances of Requester. The system does not expose multiple instances to other requesters. At any time, the Intake Staff may use the system to resurrect a closed Information Request reassign to one more instances of additional requesters. For hand delivery option, the Intake Staff use the system to create paper copies of the Information Request or digital copies on Requester desired media. The Intake Staff use the system to close the Information Request when warranted or the closure occurs during period end.	

7.1.2 Appendix B – Technical Reference Model

The Technical Reference Model is based on the September 24, 2015 model provided by the Office of the Chief Enterprise IT Architect. It is the City of Austin's component-based technical framework used for standards, specification and technologies that support and enable the delivery of service to City departments.

Area	Category	Standard
Application Technology		
Development Tools	Analysis, Design and Modeling	Unified Modeling Language (UML)
	Requirements Management	Rational Software Architect (RSA)
	Software Change and Configuration Management Tools	GitHub
	Web Authoring Tools	Drupal (outward)
	Application Development Tools	Visual Studio
		PL/SQL Developer
		Notepad++
		Java
		Cold Fusion
Software Engines	Search Engines	Solr
	Geographic Information System (GIS) Engines	ESRI Current minus 2 versions (10.1-10.3)
		ArcGIS for Desktop current minus 2 versions (10.1-10.3)
		ArcGIS for Server current minus 2 versions (10.1-10.3)
		ArcGIS Online current minus 2 versions (10.1-10.3)
		Smallworld Electronic Office (AE only)
		ArcSDE current minus 2 versions (10.1-10.3)
		FME current minus 2 versions (10.1-10.3)
	Business Rules Engines	BPM
		BPMN
	Business Process Management Engines	Websplore
Application and Web Server Software	Application Server Software	ArcGIS Server (includes server extensions) current minus 2 versions (10.1-10.3)
		FME Server current minus 2 versions (10.1-10.3)
	Web Server Software	Apache current minus 2 versions

Area	Category	Standard
		Internet Information Services (IIS) current minus 1 version
		IBM WebSphere
Integration Software	Enterprise Service Bus (ESB)	IBM Integration Bus (IIB)
Application Testing Software	Debugging Test Tools	PL/SQL Developer
		Fiddler
		Firebug (Firefox plugin)
		IE Developer Tools
	Function Testing Tools	PL/SQL Developer
	Load and Performance Testing Tools	PL/SQL Developer
		Visual Studio
		Jmeter
	System Testing Tools	Visual Studio
		PL/SQL Developer
	Unit Testing Tools	Visual Studio
		PL/SQL Developer
Information Management Technologies		
Business Intelligence and Data Warehouse Platforms	Business Intelligence Platforms	MicroStrategy
	Web Reporting Tools	Google Analytics
		DBNetGrid
		CADReports
		Microcall
	Dashboard/Scorecard Tools	MicroStrategy
	Data Mining Tools	Oracle Discoverer
		PL/SQL Developer
	Data Warehouses	Oracle
		SQL Server
	Geospatial Tools	ArcGIS Desktop current minus 2 versions (10.1-10.3)
	Data Analytics (Statistical Analytics, Prediction, and Modeling)	ERWin
		Visio
	Unstructured Data/Natural Language Processing	EDIMS
		OS File
		CIFS
Data Management	Database Connectivity	PL/SQL Developer
		Oracle SQL Developer
		Oracle SQL *Net
	Object Oriented DBMS	Oracle
	Relational DBMS	Oracle
		SQL Server
		Oracle

Area	Category	Standard
		SQL Server
	Database Related Management Tools	IDERA
		PL/SQL Developer
Data Integration	Database Replication and Clustering	PL/SQL Developer
		FME
		Oracle Real Applications Cluster (RAC)
		SQL Server Cluster
	Data at Rest	EMC
		NetApp Storage
		Tintri
		Nimble
		Pure
	Data Synchronization	GeoWorx Sync
		DFS
	Extract, Transform, Load (ETL)	FME Server
		FME Desktop
		Informatica
	Data in Motion (Common Message Terminology and Semantics)	SQL *Net
		TCP/IP
		BigIP
Collaboration and Electronic Workplace		
Collaboration Software	Content Management	Sharepoint
		GIThub
		Drupal CMS
	Electronic Messaging	Microsoft Exchange
	Unified Messaging	Lync/Skype
	Email and Calendaring	Microsoft Outlook
	Real Time and Team Collaboration	Sharepoint
		GoToMyPC
		Cisco VPN
		NetMotion
		Citrix
		Adobe Connect
		Vidyo
		Cleo
		Lync/Skype
	Shared Whiteboard	SmartBoard
		BMC Service Desk Express
	Process and Schedule Synchronization	Tivoli
		Airwatch
	Computer Based Training (CBT)	Adobe Connect
Productivity Software	Accounting and Finance	Advantage

Area	Category	Standard
	Desktop Publishing	Microsoft Publisher
	File Manager and Viewer	EDIMS (Opentext)
		Adobe Acrobat
	Enterprise Faxing	Captaris Rightfax
	Graphics Design Software	Adobe Creative Suite
	Multimedia Software	Adobe Creative Suite
	Standard Office Suite	Microsoft Office 2013
	Miscellaneous Productivity Tools and Utilities	Windows Snipping Tool
	Web Browsers	Internet Explorer current minus 1 (IE 11 and 10)
		Firefox current minus 1
		Chrome current minus 1
	Case Management	AMANDA
		BMC Magic Service Desk Express
		FDM
		Versadex
		LIMS
	Surveys	Survey Monkey
		Survey Builder
		Sharepoint
System Management		
System Management Tools	Alert Management	Orion Solarwinds
		Puppet
		Microsoft SCCM
		Idera
		Trend IWSVA
		Netbotz
		ISX Environmental Monitoring
		Avaya ASA
		Avaya Session Manager
		ADV NMS
	Application Management	Tivoli
	Asset Management and Work Order	Maximo
		BMC Magic Service Desk Express
		Mobile Workforce Manager
	Data Center Automation Software	Appsense
		Idera
		Microsoft SCCM
		EMC Networker
		APC Structureware
		Active Directory
	Disaster Recovery	NetApp VSC

Area	Category	Standard
	Monitoring	Orion Solarwinds
	Remote Desktop Management	Dameware
		MS RDP
	System Change and Configuration Management	Puppet
		Microsoft SCCM
Network Infrastructure	Switching and Routing	Cisco
		Brocade
		ADVA
	Load Balancing and Failover	F5 Big IP
	Network Name and Address	Windows DHCP
		Windows DNS
		IP - IPv6 (not used yet)
		Ipsec
		WINS
		BIND DNS
Network and Telecommunications		
Transport	Local/Campus Area Network (LAN/CAN)	Cisco
		Brocade
	Wide Area Network (WAN)	City Owned Fiber
		AT&T Connections
		Avaya Equipment
		Nortel Equipment
		TimeWarner Cable
	Cabling	BICSI
Wireless and Mobile Networks	Cellular Networks	AT&T (Public Safety)
		Verizon (Public Safety)
		AT&T (AVL- Public Safety)
		Verizon (AVL)
		Sprint (AVL)
	Secure WiFi	Cisco WAP
	Public WiFi	Cisco WAP
		Meraki WAP
	Radio	P25
		Motorola
	Pagers	USA Mobility
	Aircards	Sprint
		Verizon
		AT&T
End User Computer Devices	Personal Computers (PCs)	Dell Workstations/Laptops
	Mobile Hardware	iPad current minus 1
		iPhone current minus 1
		Android current minus 1
	Hardened Laptops	Panasonic
		Dell

Area	Category	Standard
Platforms and Storage		
Operating Systems	Desktop/Laptop	Win 7 current minus 1
		Win 8 current minus 1
	Mainframe	AIX current minus 2
	Mobile Device	Android current minus 1
		iOS current minus 1
	Server	Windows Server current minus 1
		AIX current minus 2
		Linux (Redhat) current minus 1
Cloud Services/ Virtualization	Cloud Technologies	ArcGIS Online current minus 2
	Virtualization Software	VMWare
		Citrix Xen Server
		VirtualBox
Storage	Long Term Back-up	EMC Networker
		NetApp
		Avamar
	Operational Recovery	EMC Networker
		NetApp
		Avamar
	Production	EMC Networker
		NetApp
		Avamar
System Management Tools	Network Performance Optimization	Microsoft SCCM
		Trend Antivirus
		Puppet
		GitHub
		PKI
		GPO
		IBM HMC
		Trend IWSVA
	Logging	Splunk
	Patch Management	WSUS
		Microsoft SCCM
Enterprise Architecture		
Employment	Application	Rational Software Architect (RSA)
		MS Picture Manager
		HTML-Kit
		SnagIt
		FTP
		Subversion
	Framework	Eclipse
		Unified Modeling Language (UML)
		IBM UPIA

7.1.3 Appendix C – Functional Requirements

Vendor Product/Service: Vendor shall indicate if the Product/Services meets the functional requirement and/or describes how the proposed Product/Services shall accomplish each Functional requirement. Vendors shall indicate if the accomplished requirement is:

Category	Req. No.	Topic	Requirement Description	Use Case Req. No.	Vendor Product/Service*	Vendor Response
4	001	Intake Information Request	Ability to develop an online and knowledge base that will provide requester's the ability to submit request directly into the system	1	□ BASE □ CUSTOM □ THIRD PARTY □ NOT PROVIDED	
4	002	Intake Information Request	Ability for City of Austin Law Department's website to transmit submitted Information Request into system		□ BASE □ CUSTOM □ THIRD PARTY □ NOT PROVIDED	
4	003	Intake Information Request	Ability for Intake Staff to input information Request into system		□ BASE □ CUSTOM □ THIRD PARTY □ NOT PROVIDED	

Category	Req. No.	Topic	Requirement Description	Use Case Req. No.	Vendor Product/Service*	Vendor Response
4	004	Intake Information Request	Ability for all Information Request to be completely managed by Intake Staff to complete the following but not limited to: • Assignment of one or more PIR Responders • Final correspondence to requester • Add/Remove templates		□ BASE □ CUSTOM □ THIRD PARTY □ NOT PROVIDED	
4	005	Intake Information Request	Ability to validate requestor email by sending a confirmation code to the Requester email address	1	□ BASE □ CUSTOM □ THIRD PARTY □ NOT PROVIDED	
4	006	Intake Information Request	Ability to attach additional documents and videos with an Information Request. Attachment types to include but not limited to the following: • MSG • JPEG • EXCEL • AUDIO and VIDEO • PDF • WORD	1	□ BASE □ CUSTOM □ THIRD PARTY □ NOT PROVIDED	

Category	Req. No.	Topic	Requirement Description	Use Case Req. No.	Vendor Product/Service*	Vendor Response
4	007	Intake Information Request	Ability to indicate requesters preferred pickup method such as but not limited to Web portal, physical pickup, mail to postal service address, or email.	1	□ BASE □ CUSTOM □ THIRD PARTY □ NOT PROVIDED	
4	008	Intake Information Request	Ability to provide requestor confirmation submitted information request with the ability to: • Summarize request • Provide City Contact Information • Anticipated process and/or estimated cost	1	□ BASE □ CUSTOM □ THIRD PARTY □ NOT PROVIDED	
4	009	Intake Information Request	Ability to assign unique identifier to each request received (identification number) *Refer to **Section 2.1** for current workflow process.*	2	□ BASE □ CUSTOM □ THIRD PARTY □ NOT PROVIDED	
4	010	Intake Information Request	Ability to identify duplicate requester and merge	3	□ BASE □ CUSTOM □ THIRD PARTY □ NOT PROVIDED	

Category	Req. No.	Topic	Requirement Description	Use Case Req. No.	Vendor Product/Service*	Vendor Response
4	011	Intake Information Request	Ability for internal and external requesters to communicate within the system to complete the following including but not limited to: • Request additional information from requestor • Communicate with requester per preferred communication preference to obtain additional clarity from requester	4, 5	□ BASE □ CUSTOM □ THIRD PARTY □ NOT PROVIDED	
4	012	Intake Information Request	Ability to customize unlimited number of rules for automated routing for request and notifications for the following including but not limited to: • Adjust requester response timeframe window • Notify requestor when response timeframe is expiring o Summary of request o New expected date • Send email to PIR	5, 6, 7, 8, 12, 13	□ BASE □ CUSTOM □ THIRD PARTY □ NOT PROVIDED	

Category	Req. No.	Topic	Requirement Description	Use Case Req. No.	Vendor Product/Service*	Vendor Response
			Responders • Email notification to the assigned PIR Responder for any change or clarification • Adjust time out period by administrative users • Send additional notification at a set period reminding requester of expected date • Override and/or reset expected date • Allows Intake Staff to include Multiple instances of Requestors • Re-open a closed Information Request to reassign to one more instances of additional requesters by Intake Staff • Provide/Request status update notifications to PIR Responders • Add customized federal and local business holidays			

Category	Req. No.	Topic	Requirement Description	Use Case Req. No.	Vendor Product/Service*	Vendor Response
4	013	Intake Information Request	Ability to notify Intake Staff when identified tiered administrative users has completed the following but not limited to: • Information Request creation • Information Request status • Change in status • Notes when added to Information Request		□ BASE □ CUSTOM □ THIRD PARTY □ NOT PROVIDED	

Category	Req. No.	Topic	Requirement Description	Use Case Req. No.	Vendor Product/Service*	Vendor Response
4	014	Intake Information Request	Ability to track and log actions taken within the system to complete the following including but not limited to: • Information request activities throughout the lifecycle of the request • Historical dialog between Requester, Intake Staff and other PIR Responders • Activities, dates/time and responsible staff details • Actions by department PIR Responder provides Intake Staff status to the information request • All timing associated with notification, response or other intake Staff or PIR Respondent activities.	5,7	□ BASE □ CUSTOM □ THIRD PARTY □ NOT PROVIDED	
4	015	Intake Information Request	Ability to generate email to requestor for clarity request and associate request and response to original request	5	□ BASE □ CUSTOM □ THIRD PARTY □ NOT PROVIDED	

Category	Req. No.	Topic	Requirement Description	Use Case Req. No.	Vendor Product/Service*	Vendor Response
4	016	Intake Information Request	Ability to provide requester the option to include attachments to clarity request	5	□ BASE □ CUSTOM □ THIRD PARTY □ NOT PROVIDED	
4	017	Intake Information Request	Ability to provide Intake Staff and PIR Responder the ability to enter and view all notes	5	□ BASE □ CUSTOM □ THIRD PARTY □ NOT PROVIDED	
4	018	Assign Department	Ability to align certain users with specific departments and offices	7	□ BASE □ CUSTOM □ THIRD PARTY □ NOT PROVIDED	
4	019	Assign Department/ Responder	Ability for approved city staff to create and modify templates to be utilized by PIR responder	7	□ BASE □ CUSTOM □ THIRD PARTY □ NOT PROVIDED	
4	020	Assign Department/ Responder	Ability to provide summary guidance for Intake Staff to select the appropriate template based on the type and scope of an Information Request.	7	□ BASE □ CUSTOM □ THIRD PARTY	

Category	Req. No.	Topic	Requirement Description	Use Case Req. No.	Vendor Product/Service*	Vendor Response
					□ NOT PROVIDED	
4	021	Assign Department/ Responder	Ability to automate notification to users when Information Request are assigned	8	□ BASE □ CUSTOM □ THIRD PARTY □ NOT PROVIDED	
4	022	Assign Department/ Responder	Ability to perform and complete workflow (Information Request) integration	8, 12, 13	□ BASE □ CUSTOM □ THIRD PARTY □ NOT PROVIDED	
4	023	Assign Department/ Responder	Ability to provide continuous metering of time of submission and anticipated completion date	8	□ BASE □ CUSTOM □ THIRD PARTY □ NOT PROVIDED	
4	024	Assign Department/ Responder	Ability to provide PIR Responders a work queue of open active Information Request	8	□ BASE □ CUSTOM □ THIRD PARTY □ NOT PROVIDED	

Category	Req. No.	Topic	Requirement Description	Use Case Req. No.	Vendor Product/Service*	Vendor Response
4	025	Determine Fee	Ability to calculate, assess and track fees and staff time associated with requests	9	□ BASE □ CUSTOM □ THIRD PARTY □ NOT PROVIDED	
4	026	Determine Fee	Ability to calculate fee estimates and to manage fees associated with routine or frequent Information Requests	9	□ BASE □ CUSTOM □ THIRD PARTY □ NOT PROVIDED	
4	027	Determine Fee	Ability to store historical Information Request fees for use in future cost estimates	9	□ BASE □ CUSTOM □ THIRD PARTY □ NOT PROVIDED	
4	028	Collect and Disseminate Requested Information	Capability to retain large amounts of data within the system	12	□ BASE □ CUSTOM □ THIRD PARTY □ NOT PROVIDED	
4	029	Collect and Disseminate Requested Information	Ability to search to find documents, issues and user data	12	□ BASE □ CUSTOM □ THIRD PARTY	

Category	Req. No.	Topic	Requirement Description	Use Case Req. No.	Vendor Product/Service*	Vendor Response
					□ NOT PROVIDED	
4	030	Collect and Disseminate Requested Information	Ability to view common formats by Requestor without specialized applications	12	□ BASE □ CUSTOM □ THIRD PARTY □ NOT PROVIDED	
4	031	Collect and Disseminate Requested Information	Ability to provide overview of all Information Request task assignment, status and information collected	12	□ BASE □ CUSTOM □ THIRD PARTY □ NOT PROVIDED	
4	032	Collect and Disseminate Requested Information	Ability to provide Intake Staff continuous status indication throughout the Information Request lifecycle.	12	□ BASE □ CUSTOM □ THIRD PARTY □ NOT PROVIDED	
4	033	Collect and Disseminate Requested Information	Ability to provide Intake Staff notification when all PIR Responders have provided responses to information request	12	□ BASE □ CUSTOM □ THIRD PARTY □ NOT PROVIDED	

Category	Req. No.	Topic	Requirement Description	Use Case Req. No.	Vendor Product/Service*	Vendor Response
	034	Collect and Disseminate Requested Information	Ability to determine PIR Responders responses does not contain sensitive information including but not limited to the following: • Date of Birth • Social Security Number • Driver License Number	12	□ BASE □ CUSTOM □ THIRD PARTY □ NOT PROVIDED	
4	035	Collect and Disseminate Requested Information	Ability to provide tool(s) to redact information from select information	12	□ BASE □ CUSTOM □ THIRD PARTY □ NOT PROVIDED	
4	036	Collect and Disseminate Requested Information	Ability to enable data storage and retrieval from achieved data in a manner which is consistent with production data.	13	□ BASE □ CUSTOM □ THIRD PARTY □ NOT PROVIDED	
4	037	Collect and Disseminate Requested Information	Ability to convert the disseminated information into a machine-readable format for the purpose of facilitating online publication		□ BASE □ CUSTOM □ THIRD PARTY □ NOT PROVIDED	

Category	Req. No.	Topic	Requirement Description	Use Case Req. No.	Vendor Product/Service*	Vendor Response
4	038	Collect and Disseminate Requested Information	Ability to send requestor responses via encrypted email. Email encryption must utilize a minimum 256-bit key length.		□ BASE □ CUSTOM □ THIRD PARTY □ NOT PROVIDED	

Category	Req. No.	Topic	Requirement Description	Use Case Req. No.	Vendor Product/Service*	Vendor Response

4	039	Reporting	Ability for tier administrative staff to report on the following but not limited to:
			• Dates
			  o Submitted/Open Date,
			  o Initial 10th Business Day
			  o Date Closed
			  o Number of days Open
			  o PIR Responder Completion Date
			  o Date Ranges)
			• Assigned PIR Responders
			• Subject/Topic
			• Status
			• Requester
			• Information Request Description
			• Number of Days Information Request is opened
					□ BASE
					□ CUSTOM
					□ THIRD PARTY
					□ NOT PROVIDED	

Category	Req. No.	Topic	Requirement Description	Use Case Req. No.	Vendor Product/Service*	Vendor Response
4	040	Reporting	Ability for PIR Responder to report on the following but not limited to: • Subject/Topic • Status • Open/Active number of Information Request • Assigned Staff		□ BASE □ CUSTOM □ THIRD PARTY □ NOT PROVIDED	
4	041	Reporting	Ability to export information about the status of an individual PIRs in CSV format including but not limited to: • Date Received • Subject/Topic • Current Status • Date Completed		□ BASE □ CUSTOM □ THIRD PARTY □ NOT PROVIDED	

7.1.4 Appendix D – Technical Standards (Requirements)

Vendor Product/Service: Vendor shall indicate if the Product/Services meets the functional requirement and/or describes how the proposed Product/Services shall accomplish each Functional requirement. Vendors shall indicate if the accomplished requirement is:

Category	Req No	Topic	Description	Vendor Product/Service*	Vendor Response
5	001	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.	□ BASE □ CUSTOM □ THIRD PARTY □ NOT PROVIDED	
5	002	Application Architecture	No requirement to deploy application code to client workstations (note: Java Runtime Environment (JRE) is an exception).	□ BASE □ CUSTOM □ THIRD PARTY □ NOT PROVIDED	

Category	Req No	Topic	Description	Vendor Product/Service*	Vendor Response
5	003	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 versions is defined as the manufacturer's latest production point version of the product.	□ BASE □ CUSTOM □ THIRD PARTY □ NOT PROVIDED	
5	004	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.	□ BASE □ CUSTOM □ THIRD PARTY □ NOT PROVIDED	

Category	Req No	Topic	Description	Vendor Product/Service*	Vendor Response
5	005	Application Architecture	The application provides built-in application and system configuration tables accessible by all modules.	□ BASE □ CUSTOM □ THIRD PARTY □ NOT PROVIDED	
5	006	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).	□ BASE □ CUSTOM □ THIRD PARTY □ NOT PROVIDED	
5	007	Application Architecture	The application provides copy, cut, paste, and undo functions from data fields and screens to other applications.	□ BASE □ CUSTOM □ THIRD PARTY □ NOT PROVIDED	
5	008	Application Architecture	The application provides ability to perform mass changes to a defined group of transactions with appropriate selection criteria.	□ BASE □ CUSTOM □ THIRD PARTY □ NOT PROVIDED	
5	009	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.	□ BASE □ CUSTOM □ THIRD PARTY □ NOT PROVIDED	

Category	Req No	Topic	Description	Vendor Product/Service*	Vendor Response
5	010	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.	□ BASE □ CUSTOM □ THIRD PARTY □ NOT PROVIDED	
5	011	Application Architecture	The system provides ability to restrict free form entry (e.g., require use of drop-down calendar for date field).	□ BASE □ CUSTOM □ THIRD PARTY □ NOT PROVIDED	
5	012	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.	□ BASE □ CUSTOM □ THIRD PARTY □ NOT PROVIDED	

Category	Req No	Topic	Description	Vendor Product/Service*	Vendor Response
5	013	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.	□ BASE □ CUSTOM □ THIRD PARTY □ NOT PROVIDED	
5	014	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.	□ BASE □ CUSTOM □ THIRD PARTY □ NOT PROVIDED	
5	015	Data Storage and Archiving	The solution supports future releases of the application without rendering the archived data unusable.	□ BASE □ CUSTOM □ THIRD PARTY □ NOT PROVIDED	
5	016	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)	□ BASE □ CUSTOM □ THIRD PARTY □ NOT PROVIDED	

Category	Req No	Topic	Description	Vendor Product/Service*	Vendor Response
5	017	Data Storage and Archiving	The solution ability to work with City of Austin to identify and implement integration additional storage (in-house or another cloud hosted solution such as Amazon Web Services)	□ BASE □ CUSTOM □ THIRD PARTY □ NOT PROVIDED	
5	018	Database Architecture	The application provides standardized data extraction Application Program Interface (API) to allow import and export of data to other systems.	□ BASE □ CUSTOM □ THIRD PARTY □ NOT PROVIDED	
5	019	Database Architecture	The application provides ability to encrypt sensitive data when required by federal or state compliance (e.g., PII, PCI, HIPAA, etc.).	□ BASE □ CUSTOM □ THIRD PARTY □ NOT PROVIDED	
5	020	Database Architecture	The solution uses the same data validation criteria for bulk data loads as it does for manual data entry.	□ BASE □ CUSTOM □ THIRD PARTY □ NOT PROVIDED	

Category	Req No	Topic	Description	Vendor Product/Service*	Vendor Response
5	021	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).	□ BASE □ CUSTOM □ THIRD PARTY □ NOT PROVIDED	
5	022	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.	□ BASE □ CUSTOM □ THIRD PARTY □ NOT PROVIDED	

Category	Req No	Topic	Description	Vendor Product/Service*	Vendor Response
5	023	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.	□ BASE □ CUSTOM □ THIRD PARTY □ NOT PROVIDED	

Category	Req No	Topic	Description	Vendor Product/Service*	Vendor Response
5	024	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.	□ BASE □ CUSTOM □ THIRD PARTY □ NOT PROVIDED	

Category	Req No	Topic	Description	Vendor Product/Service*	Vendor Response
5	025	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.	□ BASE □ CUSTOM □ THIRD PARTY □ NOT PROVIDED	

Category	Req No	Topic	Description	Vendor Product/Service*	Vendor Response
5	026	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.	□ BASE □ CUSTOM □ THIRD PARTY □ NOT PROVIDED	

Category	Req No	Topic	Description	Vendor Product/Service*	Vendor Response
5	027	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.	□ BASE □ CUSTOM □ THIRD PARTY □ NOT PROVIDED	
5	028	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.	□ BASE □ CUSTOM □ THIRD PARTY □ NOT PROVIDED	

Category	Req No	Topic	Description	Vendor Product/Service*	Vendor Response
5	029	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), Sensitive Personally Identifiable Information (PII).	□ BASE □ CUSTOM □ THIRD PARTY □ NOT PROVIDED	
5	030	Security and Authentication	The system provides protection against unauthorized access to data by persons and other software programs.	□ BASE □ CUSTOM □ THIRD PARTY □ NOT PROVIDED	
5	031	Security and Authentication	The system masks (i.e., substituting characters with '*') passwords as they are entered into the system.	□ BASE □ CUSTOM □ THIRD PARTY □ NOT PROVIDED	

Category	Req No	Topic	Description	Vendor Product/Service*	Vendor Response
5	032	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.	□ BASE □ CUSTOM □ THIRD PARTY □ NOT PROVIDED	
5	033	Security and Authentication	The solution provides a method to change the passwords for built-in system accounts (i.e. Administrator, Admin, Super, etc.)	□ BASE □ CUSTOM □ THIRD PARTY □ NOT PROVIDED	
5	034	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.	□ BASE □ CUSTOM □ THIRD PARTY □ NOT PROVIDED	
5	035	Security and Authentication	The application allows the Application Administrator to restrict generic logins.	□ BASE □ CUSTOM □ THIRD PARTY □ NOT PROVIDED	

Category	Req No	Topic	Description	Vendor Product/Service*	Vendor Response
5	036	Security and Authentication	The system uses Microsoft Active Directory Federated Services (ADFS) [current version minus 1] for federated identity management.	□ BASE □ CUSTOM □ THIRD PARTY □ NOT PROVIDED	
5	037	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)	□ BASE □ CUSTOM □ THIRD PARTY □ NOT PROVIDED	
5	038	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.	□ BASE □ CUSTOM □ THIRD PARTY □ NOT PROVIDED	

Category	Req No	Topic	Description	Vendor Product/Service*	Vendor Response
5	039	Security and Authentication	Ability to send requestor responses via encrypted email. Email encryption must utilize a minimum 256-bit key length.	□ BASE □ CUSTOM □ THIRD PARTY □ NOT PROVIDED	

7.1.5 Appendix E – Project Management Requirements

Category	Req. No.	Topic	Requirement Description	Vendor Response
6	001	Project Management Methodology	Provide a Project Manager (PM) to represent the Vendor in the management of the Project, interfacing with the City Project Manager (PM) in any decisions relating to the Project	
6	002	Project Management Methodology	Assume and lead all day-to-day management of Vendor personnel, including subcontractor personnel, and associated Deliverables related to the required services	
6	003	Project Management Methodology	Provide a robust project management methodology founded on industry best practices	
6	004	Project Management Methodology	Conduct project management activities through the life of the project and execute the associated plans	
6	005	Project Management Methodology	Document deliverable details, formats, and acceptance criteria in Deliverable Expectation Documents (DEDs) as mutually agreed upon by the City and the Vendor	
6	006	Project Management Methodology	Provide, update, and maintain a Project Schedule (e.g. in MS Project)that includes the following key components: • Work breakdown structure • Task and activities required to successfully complete the Project • Schedule/milestone tracking and resource allocation	

Category	Req. No.	Topic	Requirement Description	Vendor Response
			• Critical path identification and dependencies Provide periodic updates (as mutually agreed upon by the City and the Vendor) to Project Schedule which is maintained by the Vendor	
6	007	Project Management Methodology	Provide, update and maintain a formal Project Management Plan (PMP) that includes the following key components: • Project initiation activities • Issues tracking, escalation and resolution • Change request approval, management and tracking • Deliverable/product review and approval and other acceptance criteria • Risk Management, identification, quantification of impact, monitoring, and mitigation plans • Quality management • Vendor and subcontractor resource management • Project success evaluation criteria and Project close-out activities • Status and of the reporting activities • Status reporting templates (including deliverable status reports, issues, risks, plans vs. actual status, etc.)	
6	008	Project Management Methodology	Provide and implement risk mitigation measures, contingency plans and disaster recovery plans as high priority risks are identified and monitored	

Category	Req. No.	Topic	Requirement Description	Vendor Response
6	009	Project Management Methodology	Provide a Communication Plan and Matrix to document the communications with all Project stakeholders throughout the life of the Project as mutually agreed upon by the City of the Vendor communication with internal and external end users	
6	010	Project Management Methodology	Provide Project Status Reports and conduct regularly scheduled status meetings reviewing Project progress, risk, mitigation, issue resolution, deliverable status, and next steps as mutually agreed upon by the City and the Vendor	
6	011	Project Management Methodology	Use the Microsoft Outlook systems provided for all e-mails and scheduling for all Project-related communications	
6	012	Project Management Methodology	Prepare system Change Request as required based on all added, deleted, and/or modified scopes of work	
6	013	Project Management Methodology	Conduct and document Lessons Learned meetings at key intervals with Project Team. Apply Lessons Learned to future design and implementation phases	
6	014	Implementation Methodology	Test the capability of failover to secondary Disaster Recovery site	
6	015	Implementation Methodology	Provide the Configured Hardware Environments (testing) to test and/or demonstrate all required functionality has been satisfied	
6	016	Implementation	Provide and document test results in a Documented	

Category	Req. No.	Topic	Requirement Description	Vendor Response
		Methodology	Successful Testing Results deliverable	
6	017	Implementation Methodology	Validate the system for compliance with the Security Requirements	
6	018	Implementation Methodology	Correct defects found as a result of testing efforts and record all defect in a Defects Log	
6	019	Implementation Methodology	Provide Go/No-go Documentation, including the Production Cutover Plan and the Go-Live Checklist	
6	020	Implementation Methodology	Conduct Go/No-go Meetings with the City's staff and Vendor's technical team	
6	021	Training Methodology	Provide formal Project Team Training Plan to document City Project Team training requirements	
6	022	Licensing	Provide the licensing model necessary to meet each of the required project objectives	
6	023	Licensing	Provide cost model for hosting and integration to work with City of Austin hosted solution or working with premise storage solution	

ADDENDUM
CITY OF AUSTIN, TEXAS

Solicitation: DIR Compete -PIR Addendum No: 1 Date of Addendum: 5/18/17

This addendum is to incorporate the following changes to the above referenced solicitation:

I. Clarifications:

Section 0500, 3.26, Remove "mandatory"

Section 0500, 4.1, 2nd to last sentence: remove "mandatory"

Section 0500, 4.2, 2nd sentence: remove "Itemized requirements in this section have a rating of Mandatory indicating the criticality of the requirements in achieving product and project objectives."

Section 0500, 5.1, Second to last sentence: remove "mandatory"

Section 0500, 5.2, second sentence: remove "Itemized requirements in this section have a rating of Mandatory indicating the criticality of the requirements in achieving product and project objectives."

Section 0500, 6.1, 2nd to last sentence: remove "mandatory"

Section 0500, 6.2, remove "Itemized requirements in this section have a rating of Mandatory indicating the criticality of the requirements in achieving product and project objectives."

Section 0500, APPENDICES A-E, strike all references to mandatory. Simply "requirements."

Note: No requirements in this solicitation are mandatory. See attached 0500 with corrections.

II. Questions:

1. **Submittals must come with an approved Texas DIR quote. May other cooperatives be use to obtain quotes?**

   ANSWER: Yes. Any one of the following Cooperatives may be used for the provision of a quote: U.S. Communities Government Purchasing Alliance; Texas Multiple Award Schedule (TXMAS), Houston-Galveston Area Council of Governments (HGAC); Texas Procurement and Support Services (TPASS), Texas Local Government Purchasing Cooperative (Buyboard); The Cooperative Purchasing Network (TCPN).

2. **How will vendors be evaluated?**

ANSWER: Evaluation will be conducted by a group of end-users and technical experts. Am

Among other items, the team will look at: Prior Experience and References (20 points), Personnel and Project Management Structure (20 points), Functional and Technical Requirements (30 points) and Total Price Proposed (30 points).

III. **ALL OTHER TERMS AND CONDITIONS REMAIN THE SAME.**

Please let us know if you have any further questions.

APPROVED BY: _____ 15.18.17

Paula Barriffe, Procurement Specialist I
Purchasing Office, 512-974-2031

Date

ACKNOWLEDGED BY:

John Brooks _____ 9/7/2017

Name Authorized Signature Date

RETURN ONE COPY OF THIS ADDENDUM TO THE PURCHASING OFFICE, CITY OF AUSTIN, WITH YOUR RESPONSE OR PRIOR TO THE SOLICIATION CLOSING DATE. FAILURE TO DO SO MAY CONSTITUTE GROUNDS FOR REJECTION.

Security and Business Continuity Information

Table of Contents

Document Change Management (changes since last full revision)

Last full revision created January 9th, 2017 by Jim Cassan, Director of Infrastructure and Security

Change Date	Changed By	Change Type	Change
2/20/2017	JMC (DOS)	update	Training, updated internal and formal training content
3/16/2017	JMC (DOS)	update	Access management, updated and replaced cloud region diagram
4/2/2017	JMC (DOS)	update	Access management, updated IT management access list
4/12/2017	JMC (DOS)	update	Disaster recovery, updated cloud region processes
4/27/2017	JMC (DOS)	update	CJIS and HIPAA sections, added content

Introduction

The purpose of this document is to define the WebQA/GovQA Data Security Policy. Data is considered a primary asset and as such must be protected in a manner commensurate with its value. Security and privacy must focus on controlling unauthorized access to data. Security compromises and/or privacy violations could jeopardize our ability to provide service; lose revenue through fraud or destruction of proprietary or confidential data; violate business contracts, trade secrets, and customer privacy; or reduce credibility and reputation with its customers, shareholders and partners. This policy therefore discusses:

- Data content
- Data classification
- Data ownership
- Data security
- Data storage, transmission and disposal
- Disaster recovery
- Data center and cloud processing environments
- Incident reporting and escalation
- Staff training and certification

The main objective of this policy is to ensure that data is protected in all of its forms, on all media, during all phases of storage and transmission and throughout all stages of its life cycle, from unauthorized or inappropriate access, use, modification, disclosure, or destruction. This policy applies to all existing data assets, whether owned by WebQA/GovQA, a customer or vendor and in any and all of our processing environments. The processing environment is considered to be, collectively, all applications, systems, and networks that we own or operate or that are operated by our agents.

This policy defines the WebQA/GovQA overall security and risk control objectives that we endorse. The premise for the policy can be stated as:

"Other than data defined as public, which is accessible to all identified and authenticated users and possibly anonymous users, all data and processing resources are only accessible on a need to know basis to specifically identified, authenticated, and authorized entities."

This document forms part of WebQA/GovQA's conditions of employment for employees, a part of the contractual agreement for vendors, suppliers, and third party processors or agents, hereafter referred to as "vendors". All parties must read the policy completely, and confirm that they understand the contents of the policy and agree to abide by it. When deemed necessary, authorized written agreements to this policy may be required.

Breach of Policy and Enforcement

A breach of this policy could have severe consequences to WebQA/GovQA, its ability to provide services, or maintain the integrity, confidentiality, or availability of services.

Intentional misuse resulting in a breach of any part of this policy will result in disciplinary action at the discretion of WebQA/GovQA senior management. Severe, deliberate or repeated breaches of the policy may be considered grounds for instant dismissal; or in the case of a WebQA/GovQAvendor, termination of their contracted services. Without exception, all employees and vendors are ound by these policies and are responsible for their strict enforcement.

Scope of the Policy

This policy applies to all WebQA/GovQA and customer data assets that exist in any WebQA/GovQA processing environment, on any media and during any part if its lifecycle. The following entities or users are covered by this policy:

- Full or part-time employees of WebQA/GovQA who have access to WebQA/GovQA or customer data.
- WebQA/GovQA vendors, contractors and/or other processors who have access to WebQA/GovQA or customer data.
- Other persons, entities, or organizations that have access to WebQA/GovQA or customer data.

Data Life Cycle

The security of data can be understood through the use of a data life cycle. The typical life cycle of data is: generation, use, storage and disposal. The following sections provide guidance as to the application of this policy through the different life cycle phases of data.

All users of data assets are personally responsible for complying with this policy. All users will be held accountable for the accuracy, integrity, and confidentiality of the information to which they have access. Data must only be used in a manner consistent with this policy.

Data Usage

All users that access WebQA/GovQA or customer data must do so only in conformance to this policy. Only uniquely identified, authenticated and authorized users may access data. Each user must ensure that WebQA/GovQA data assets under their direction or control are properly labeled and safeguarded according to their sensitivity, proprietary nature, and criticality. Access control mechanisms must also be utilized to ensure that only authorized users can access data to which they have been granted explicit access rights. Where the data access and/or usage includes Criminal Justice Information (CJI), Healthcare provider (HIPAA) and other sensitive information, additional compliance requirements exist and must be met. See the CJIS and HIPAA sections of this document for further details.

Data Transmission

All users that access WebQA/GovQA or customer data to enable its transmission must do so only in conformance to this policy. Where necessary, data transmitted must be secured via cryptographic mechanisms. This may include the use of confidentiality and/or integrity mechanisms as well. Where the data transmission includes Criminal Justice Information (CJI), Healthcare provider (HIPAA) and other sensitive information, additional compliance requirements exist and must be met. See the CJIS and HIPAA sections of this document for further details.

Data Storage

All users that are responsible for the secure storage of WebQA/GovQA or customer data must do so only in conformance to this policy. Where necessary, data stored must be secured via cryptographic mechanisms. This may include the use of confidentiality and/or integrity mechanisms. Access control mechanisms must also be utilized to ensure that only authorized users can access data to which they have been granted explicit access rights. Where the data storage includes Criminal Justice Information (CJI), Healthcare provider (HIPAA) and other sensitive information, additional compliance requirements exist and must be met. See the CJIS and HIPAA sections of this document for further details.

Data Disposal

Access control mechanisms must also be utilized to ensure that only authorized users can access data to which they have been granted explicit access rights during the disposal process.

The Information Technology Group has developed and implemented procedures to ensure the proper disposal of various types of data. These procedures are made available to all users with access to data that requires special disposal techniques. Where required, WebQA/GovQA will return all data to the originating client as the data owner. When data return is not required, data will be destroyed in compliance with existing contracts, local, state and federal laws as applicable. Where the data storage includes Criminal Justice Information (CJI), Healthcare provider (HIPAA) and other sensitive information, additional compliance requirements exist and must be met. Without exception, disposal of such data will be performed in compliance with all applicable legal requirements. See the CJIS and HIPAA sections of this document for further details.

Data Access and Restrictions (authorized users, review periods)

System	Allowed Personnel	Authorized By	Review Period
Firewalls / IDS/P	CTO, DOS	CEO, CTO, DOS	90 Days
Routers/switches	CTO, DOS	CEO, CTO, DOS	90 Days
Web Servers (Prod)	CTO, DOS, DOT. DAS	CEO, CTO, DOS	90 Days
Database Servers (Prod)	CTO, DOS, DOT, DAS	CEO, CTO, DOS	90 Days
Development Servers	CTO, DOS, DOT, DAS, DEV	CTO, DOT, DOS	90 Days
NAS and SAN Storage	CTO, DOS, DOT, DAS	CTO, DOT, DOS	90 Days
PC, Printers, FAX	ALL	MAN, DOS	90 Days
Client data for implementation and maintenance duties	Appropriately trained and certified staff	CTO, DOS	30 Days
CJIS, HIPAA and FEDRAMP systems	CJIS Level 4 and HIPAA certified staff only	CTO, DOS	30 Days
CJIS, HIPAA and FEDRAMP data	Appropriately trained and certified staff	CTO, DOS	30 Days

- Legend

CEO = Chief Executive Officer

CTO = Chief Technology Officer

DOS = Manager/Director of Infrastructure and Security

DOT = Manager/Director of Technology

DAS = Manager/Director of Application Security

DEV = Developer(s)

DIMP = Manager/Director of Implementation

IMP = Implementation team

MAN = Department head or manager

USR = One or more internal users

CJIS/HIPAA/FEDRAMP = Systems accessible only by properly trained and certified staff and from within a secure/compliant environment Refers to CJI, PHI, PII and other sensitive data.

Data Center and Connectivity Diagram

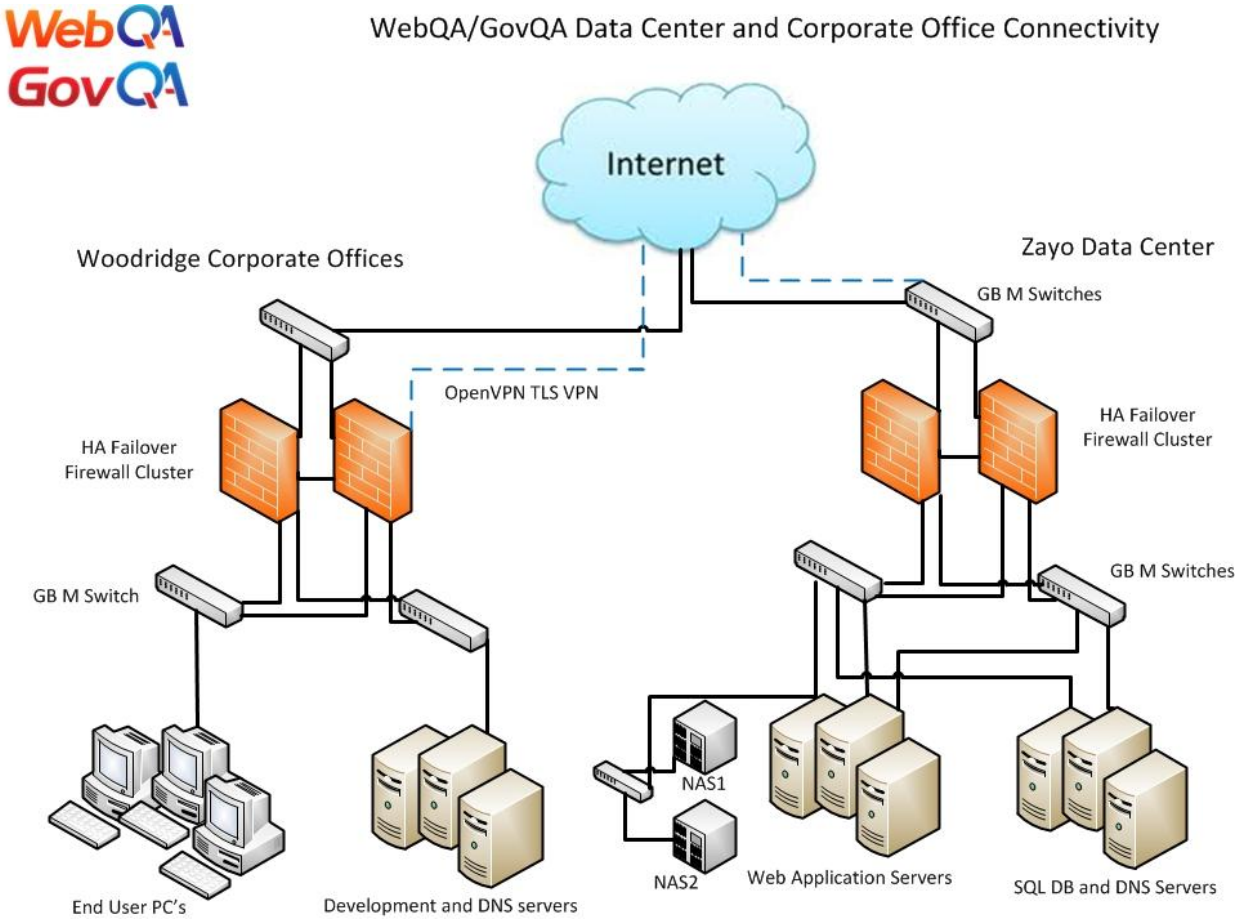


Figure 1: Primary data center design and corporate office connectivity

Network and Access Management Diagrams

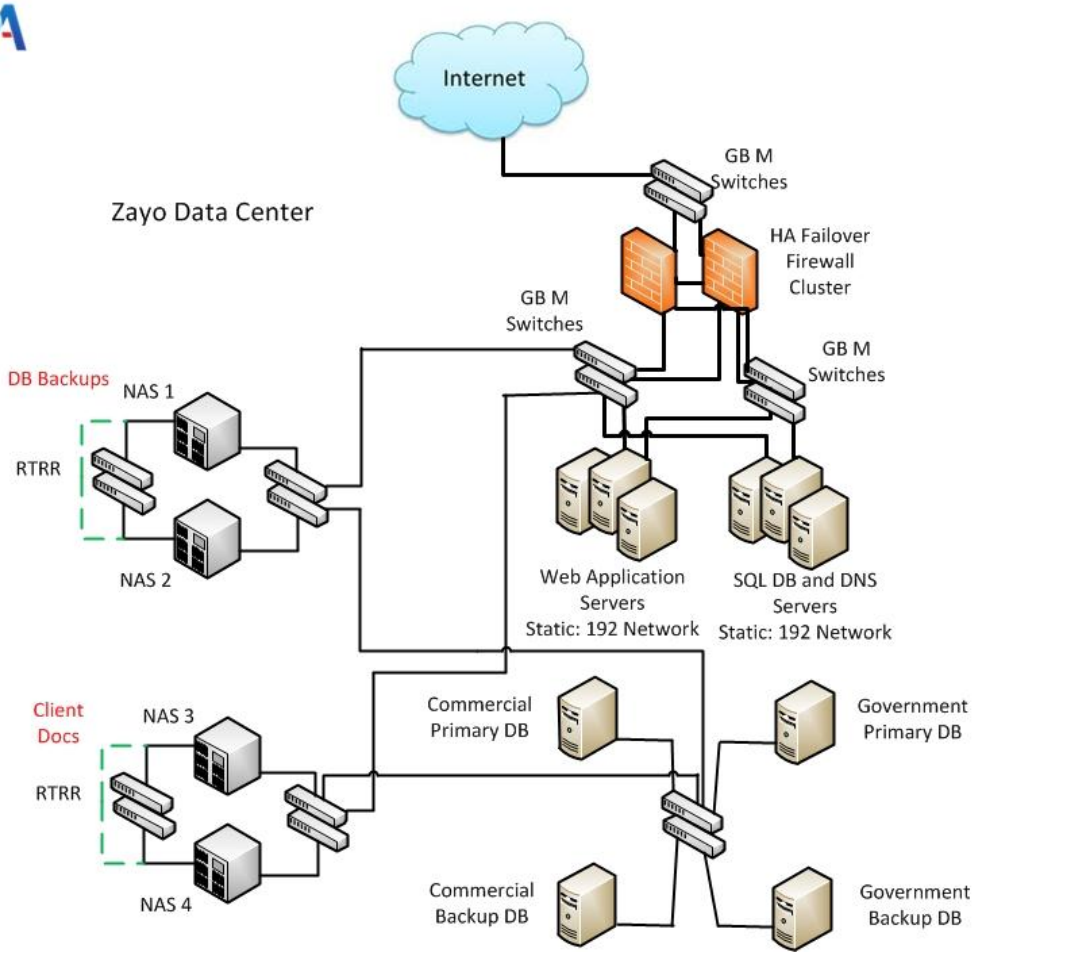


Figure 2: Primary data center network diagram including HA failover and redundancy implementations

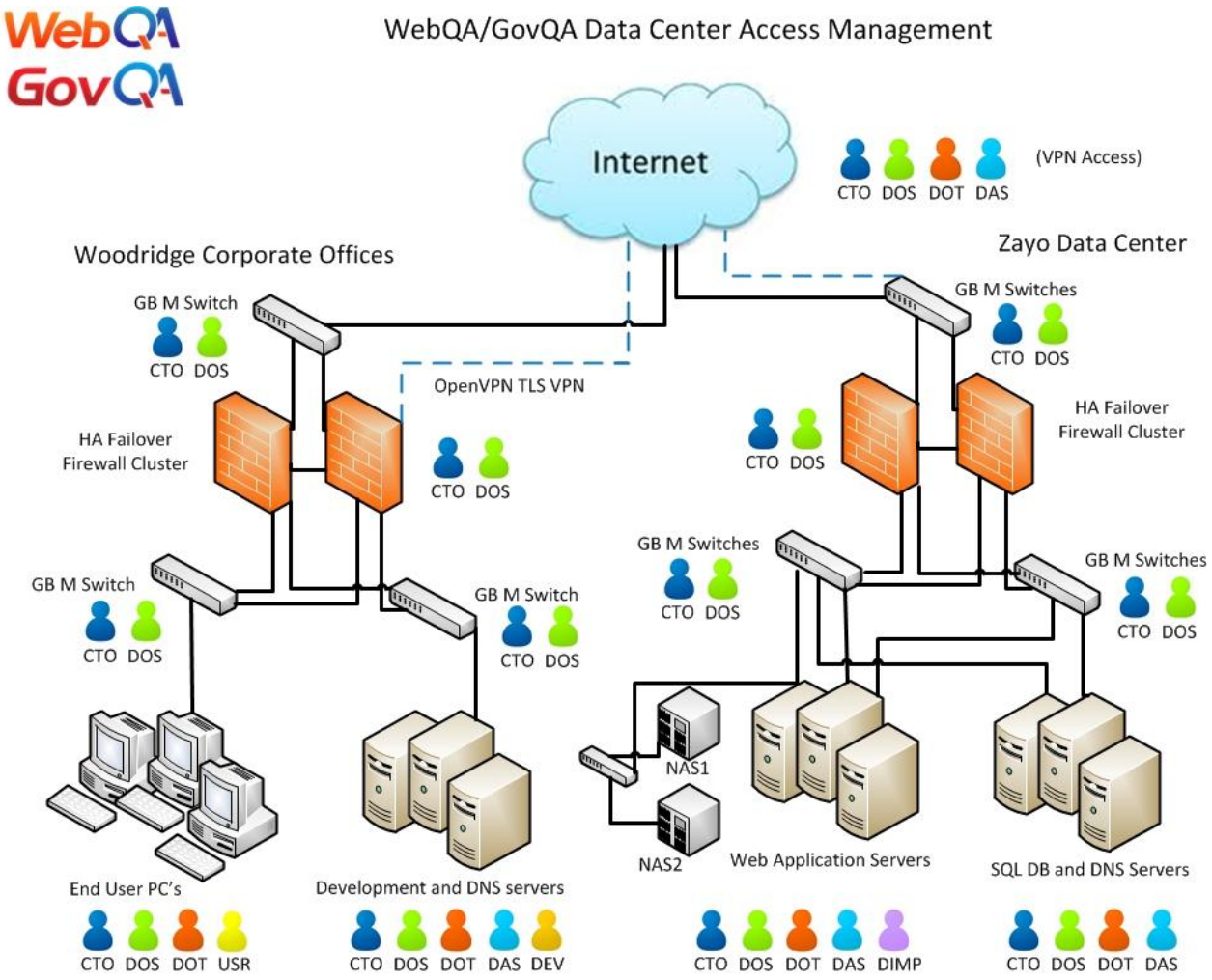


Figure 3: Data center access management diagram (excludes CJI, HIPAA and other sensitive systems/data)

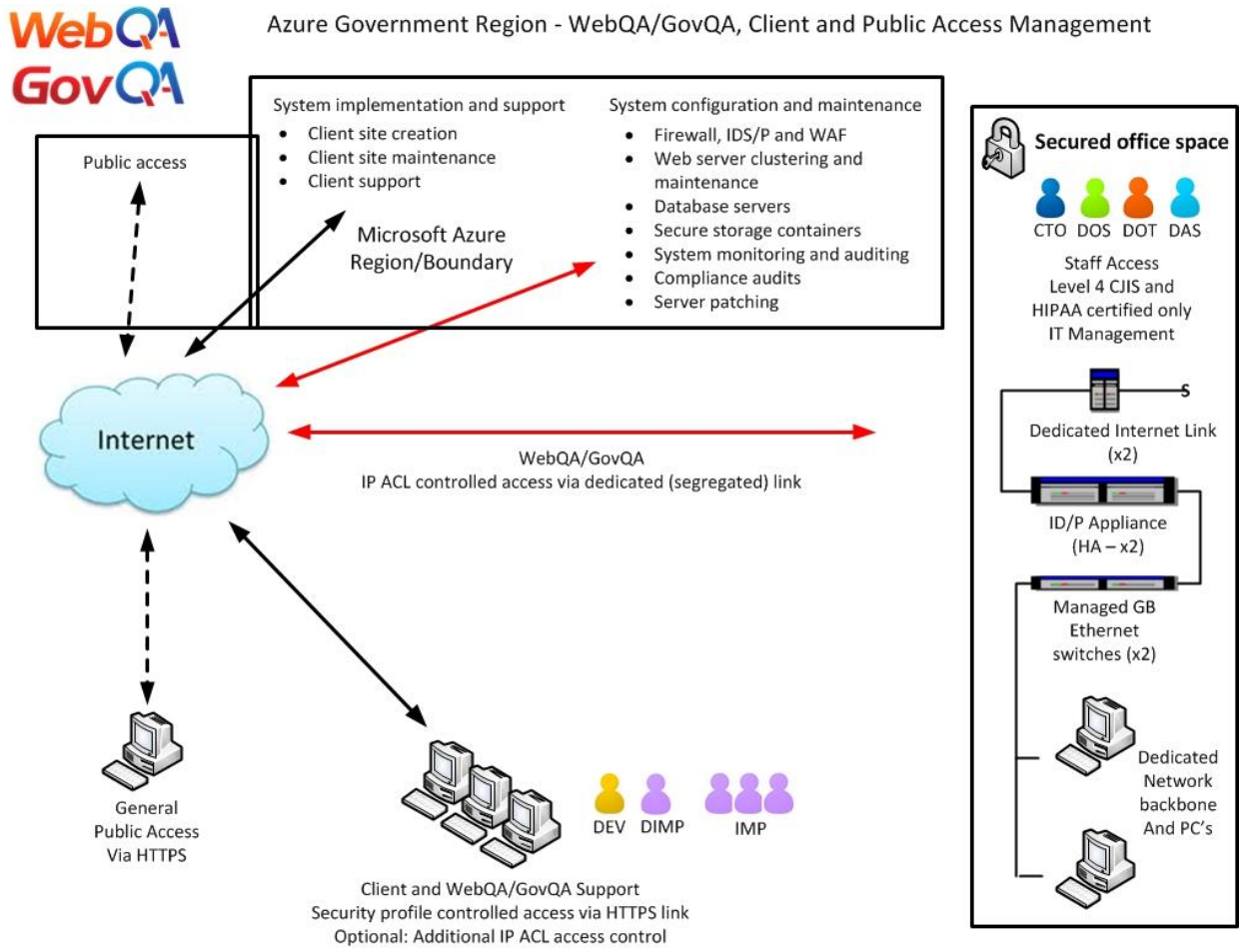


Figure 4: WebQA/GovQA access to unencrypted CJI, HIPAA and other sensitive information is restricted to only CJIS Level 4 and HIPAA certified personnel and only from the WebQA/GovQA secured space, utilizing a dedicated, network backbone. Client access is restricted by mandatory security profiles and optionally by IP controlled access lists (ACL). Public access (non-sensitive data) is via HTTPS.

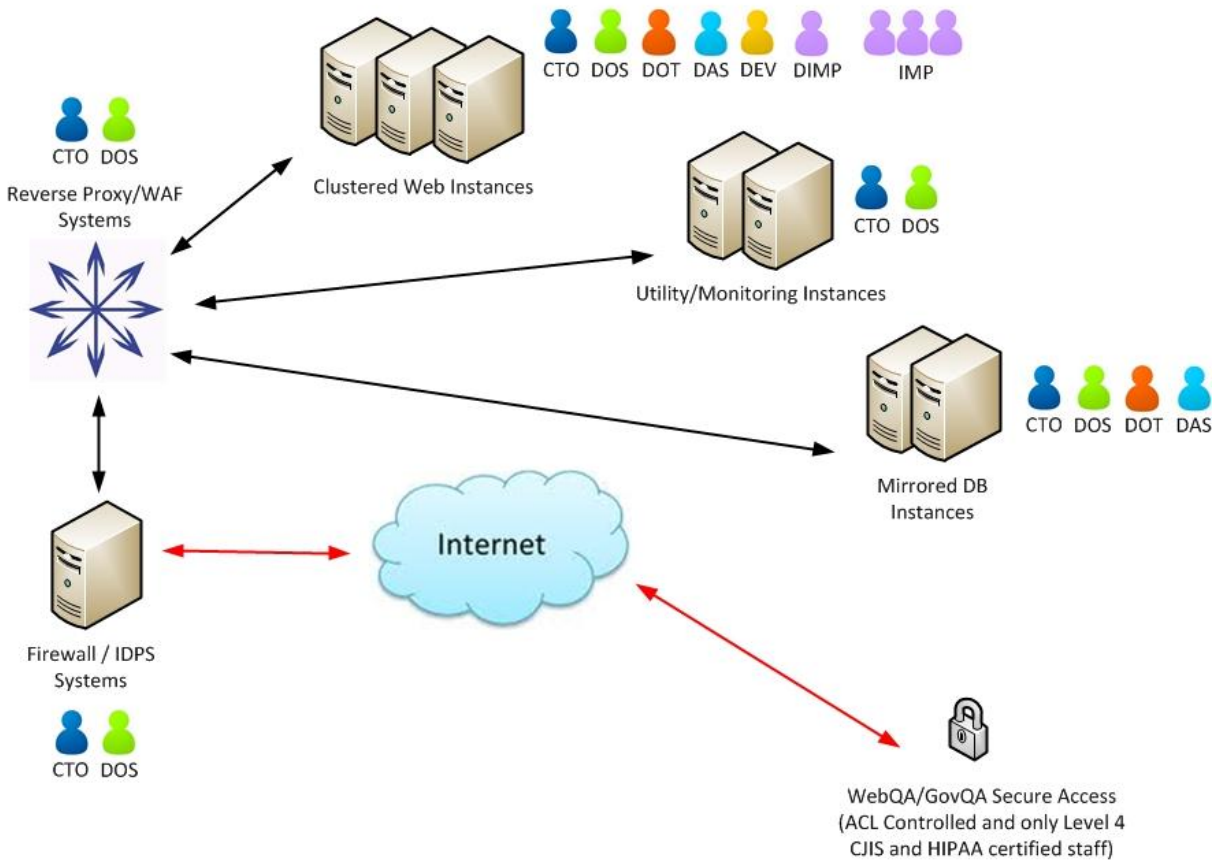


Figure 5: WebQA/GovQA Azure Government region access restrictions to/by IT Management and Implementation staff.

Data Security Policy Statement

Goals

This policy has been written with the following goals in mind:

- To educate WebQA/GovQA users and vendors about their obligation for protection of all data assets.
- To ensure the security, integrity, and availability of all WebQA/GovQA and customer data.
- To establish the WebQA/GovQA baseline data security stance and classification schema.
- Where applicable, to define compliance requirements, policies and procedures

Processing Environment

The WebQA/GovQA/GovQA processing environment that this policy applies to is comprised of:

- **Applications –** Application software is system or network-level routines and programs designed by (and for) system users and customers. It supports specific business-oriented processes, jobs, or functions. It can be general in nature or specifically tailored to a single or limited number of functions.
- **Systems –** A system is an assembly of computer hardware (e.g., sub-networks, application servers, file servers, workstations, data, etc.) and application software configured for the purpose of processing, handling, storing, transmitting, and receiving data that is used in a production or support environment to sustain specific applications and business organizations in their performance of tasks and business processes.
- **Networks –** A network is defined as two or more systems connected by a communication medium. It includes all elements (e.g., routers, switches, bridges, hubs, servers, firewalls, controllers, and other devices) that are used to transport information between systems.

Data Security Responsibilities

The *Information Technology Group* within WebQA/GovQA is responsible for:

- Defining the security requirements, controls and mechanisms applicable to all data assets.
- Defining the methods and guidelines used to identify and classify all data assets.
- Defining the procedures for identifying data owners for all data assets.
- Defining the labeling requirements for all data assets.
- Defining all other data security usage, processing, transmission, storage and disposal processes and procedures.
- Defining the procedures necessary to ensure compliance to this policy by all WebQA/GovQA users and vendors.
- Defining and enforcing policies and procedures for maintaining compliance with CJIS, HIPAA and other special requirements
- Facilitating the evaluation of new regulatory, legal, and also best practice requirements as they are mandated or become recognized in our industry.

Management Responsibilities

Other organizations within WebQA/GovQA also have various responsibilities for ensuring compliance with this policy, such as:

- All individual organizations must ensure that staff complies with this policy.
- The *Systems Administration Group* must ensure that adequate logs and audit trails are kept of all data access.
- The *Security Administration Group* must ensure the activation and maintenance of all security mechanisms.
- The *Risk Management Group* is responsible for communicating business requirements and issues for business processes and the data those include, ensuring their correct data classification.

- The internal audit area is responsible for regularly evaluating the data classification schema for consistent application and use.

Other Responsibilities

Other organizations have responsibilities to comply with this policy, such as:

- All WebQA/GovQA agents, vendors, content providers, and third party providers that process customer data must have and be willing to provide a documented security policy that clearly identifies those data and other resources and the controls that are being imposed upon them.
- All WebQA/GovQA agents, vendors, content providers, and third party providers that access the WebQA/GovQA processing environment and its data or provide content to it must have a security policy that complies with and does not contradict the WebQA/GovQA security policy.
- All agents, vendors, content providers, and third party providers must agree not to bypass any of our security requirements.

Policy Review

It is the responsibility of the Information Technology Group to facilitate the review of this policy on a regular basis. Due to the dynamic nature of the Internet, this policy should be reviewed at least annually or whenever an addition or modification is warranted. Senior management, Systems administration, and Legal should, at a minimum, be included in the annual review of this policy. In addition, security related changes are to be reviewed and accepted by both the IT Security Team and Change Advisory Board (CAB). CJIS and HIPAA systems may have additional review requirements and must and will be reviewed per those compliance requirements. See the CJIS and HIPAA section for additional details.

Data Content

The nature of specific data content that exists in the processing environment, and the controls that should apply to these, is dependent upon various factors. This policy does not mandate or endorse particular data content. Rather, the business decision process used to evaluate the inclusion or exclusion of particular data content should consider the following items.

Regardless of the specific data content that exists in the environment, all aspects of this policy must be enforced. Considerations for evaluating data content include:

- Legal and regulatory obligations in the locales in which we operate.
- Can privacy, confidentiality, security, and integrity of the data be ensured to the satisfaction of customers, compliance requirements and legal authorities?
- Is it in line with our business goals and objectives?
- Do customers require or demand access to specific data content?
- What rules govern the movement across international boundaries of different data content, and do we have in place controls to enforce these rules?

- Does the data in question require special consideration such as CJIS, HIPAA, FEDRAMP or other compliance factors?

Data Classification

Data classification is necessary to enable the allocation of resources to the protection of data assets, as well as determining the potential loss or damage from the corruption, loss or disclosure of data.

To ensure the security and integrity of all data the default data classification for any data asset is either Confidential Customer Data or Proprietary Company Data. The Information Technology Group is responsible for evaluating the data classification schema and reconciling it with new data types as they enter usage. It may be necessary, as we enter new business endeavors, to develop additional data classifications.

All data found in the processing environment must fall into one of the following categories:

- ***Public WebQA/GovQA Data –*** Public WebQA/GovQA data is defined as data that any entity either internal or external to *WebQA/GovQA* can access. The disclosure, use or destruction of Public company data will have limited or no adverse effects on WebQA/GovQA nor carry any significant liability. (Examples of Public WebQA/GovQA data include readily available news, press releases, or company location.)
- ***Proprietary WebQA/GovQA Data –*** Proprietary WebQA/GovQA data is any information that derives its economic value from not being publicly disclosed. It includes information that WebQA/GovQA is under legal or contractual obligation to protect. The value of proprietary company information to WebQA/GovQA would be destroyed or diminished if such information were disclosed to others. Most WebQA/GovQA sensitive information should fall into this category. Proprietary company information may be copied and distributed within WebQA/GovQA only to authorized users. Proprietary company information disclosed to authorized external users must be done so under a non-disclosure agreement. (Examples of Proprietary WebQA/GovQA data include company policies, sales plans, and application source code.)
- ***Confidential WebQA/GovQA Data –*** Confidential WebQA/GovQA Data is information that is not to be publicly disclosed, regardless of its economic value. The disclosure, use, or destruction of Confidential Company Data can have adverse effects on WebQA/GovQA and possibly carry significant civil, fiscal, or criminal liability. This designation is used much less frequently. It is used for highly sensitive information whose access is restricted to selected, authorized employees and agents. The recipients of confidential information have an obligation not to reveal the contents to another individual unless that person has a valid need to know and has proper authorization. Company confidential information must not be copied without authorization from the identified owner. (Examples of Confidential WebQA/GovQA Data include company strategic plans or cryptographic keys.)
- ***Public Primary Customer Data –*** Public customer data is defined as data that any entity either internal or external to WebQA/GovQA can access. The disclosure, use, or destruction of Public primary customer data will have limited or no adverse effects on WebQA/GovQA or the customer, and carry no significant liability. Public customer data is entrusted to, and may transit or be stored by WebQA/GovQA (and others) over which they have custodial responsibility but do not have

ownership. (Examples of Public customer data include public knowledge base items, publicly available documents or other customer data that is readily available through other public channels or records.)

- ***Confidential Primary Customer Data –*** Confidential primary customer data is defined as data that only authorized internal WebQA/GovQA entities or specific authorized external entities can access. The disclosure, use, or destruction of confidential customer data can have adverse effects on WebQA/GovQA and their relationship with their customers, and possibly carry significant liability for both. Confidential customer data is entrusted to and may transit or is stored by WebQA/GovQA (and others) over which they have custodial responsibility but do not have ownership. (Examples of Confidential Primary customer data include customer employee resources, employee handbook, or other data considered private.)
- ***Public Custodial Customer Data –*** Public custodial customer data is defined as data that any reseller customer or partner stores within the WebQA/GovQA system, which any entity either internal or external to WebQA/GovQA can access. Public Custodial Customer Data is treated exactly as Public Primary Customer Data.
- ***Confidential Custodial Customer Data –*** Confidential custodial customer data is defined as data that any reseller customer or partner stores within the WebQA/GovQA system, that only authorized internal WebQA/GovQA entities or specific authorized external entities can access. Confidential Custodial Customer Data is treated exactly as Confidential Primary Customer Data.
- ***Confidential CJIS (CHRI, PII, etc.) Data –*** Confidential CJIS data is defined as data that originated from or exists within a state or federal law enforcement agency and/or their designees. Data may include, but not be limited to; arrest and conviction records, court case information, etc. and must be protected at all times. Such data is considered highly sensitive in nature and the access, handling, dissemination, transmission and disposal of such data must be performed in accordance with strict standards. Where necessary, such data will be encrypted and unescorted, unencrypted access available only to individuals properly trained and certified.
- ***Confidential HIPAA (PHI, PII, etc.) Data*** – Confidential HIPAA data is defined as data that originated from or exists within a health insurance, health services provider, medical services organization, etc. and/or their designees. Data may include, but not be limited to; health and other medical records, insurance claims, etc. and must be protected at all times. Such data is considered highly sensitive in nature and the access, handling, dissemination, transmission and disposal of such data must be performed in accordance with strict standards. Where necessary, such data will be encrypted and unescorted, unencrypted access available only to individuals properly trained and certified.

Data Ownership

In order to classify data it is necessary that an owner be identified for all data assets. The owner of the data is responsible for classifying their data according to the classification schema noted in this policy. If an owner cannot be determined for a WebQA/GovQA data asset, the Information Technology Group will act as its custodian.

The default classification for all data not classified by its owner must be Confidential Primary Customer Data, Confidential Custodial Customer Data or Proprietary WebQA/GovQA Data.

The Information Technology Group is responsible for developing, implementing, and maintaining procedures for identifying all data assets and associated owners. The owner of all customer data is the individual owner who generates or is assigned ownership of that data. (Data such as public key certificates generated by an external Certificate Authority but assigned to a specific customer are considered owned by that customer)

Non-disclosure Agreements

On occasion, data assets may need to be released to entities outside of WebQA/GovQA. When a legitimate business reason exists for releasing sensitive information, a written Non-Disclosure Agreement (NDA), requiring the data recipient's agreement to maintain that data in confidence and restrict its use and dissemination, must be obtained before disclosing the data.

Data Security Principles

WebQA/GovQA's business goals, objectives, and needs for security can be derived from three principles: accountability, authorization, and availability. These three principles emphasize the need for security to function properly in WebQA/GovQA's processing environment, which is comprised of applications, network, and system resources. Non-compliance with these principles can have serious, adverse, and deleterious effects on WebQA/GovQA.

In the context of this policy, the following provides the overall concepts or security principles for which all users and vendors are responsible. It is the responsibility of the Information Technology Group to define the specific mechanisms necessary to support these principles.

Accountability

All network, system, and application events must be attributable to a specific and unique individual. It should be possible to attribute a responsible individual to every event through an identification service and to verify that the individual so assigned has been properly identified through an authentication process. It must also be possible to trace any event so as to reconstruct the time, place, and circumstances surrounding it through an audit process.

In this context identification refers to a security process that recognizes a claim of identity by comparing a user id offered with stored security information.

Authentication refers to a security process that verifies the claimed identity of the user, for example a password. Auditability refers to a security process that records information of potential security significance.

Authentication is limited to the specific user id, and in the case of the external application, this may be an anonymous web user. No static or persistent information is stored for these users, other than standard web server logs. Any interpretation of this user information would require a proactive effort by a privileged user of the system.

Authorization

All network, system, and application events must only result from allowable actions through access control mechanisms. Permission may be derived directly from an individual's identity, or from a job classification or administrative privilege based on that individual's identity. The principle of "least privilege" specifies that individuals only be granted permission for actions needed to perform their assigned duties.

Limiting actions to those properly authorized protects the confidentiality and integrity of data within the WebQA/GovQA processing environment. In this context access control refers to a security process that allows or denies a user request based on privilege, group information, or context. Confidentiality refers to a security process that prevents disclosure of information to unauthorized parties while the information is in use or transit, or being stored or destroyed.

Availability

All permitted activity should operate with reliability. The data necessary to carry out such events must be readily retrieved and correct with high confidence. All results of an event must be completed, unless the event is aborted in its entirety. The results of an event should not depend in unexpected ways on other concurrent events. The security services themselves must be documented and readily administered.

In this context integrity refers to a security process that guarantees data has not been altered, deleted, repeated, or rearranged during transmission, storage, processing, or recovery.

Security Implementation

The following items describe the actual implementation plan, where applicable, for the aforementioned security guidelines.

Data and Resource Access

Customer and other critical data resides on clustered, load balanced servers, which are hot-failover redundant. The web and database servers are behind and protected by hot-failover redundant firewalls, using a masked IP scheme.

Physical Security and Connectivity

Concerning non-Government (CJIS and HIPAA) processing, the WebQA/GovQA servers are homed in a state-of-the-art data center. Some of the specifics include:

An 86,000 square foot facility, one of the largest Tier III+ data centers in North America. It has been specifically built to safeguard mission critical data and accommodate future growth and change. The building envelope was designed and constructed to withstand extreme temperatures, high winds, floods, fire, impact, pollution, and electro-magnetic interference.

Connectivity: 2 OC-48s from Chicago, Illinois and 2 OC-12's to Fort Worth, Texas and Tukwilla, Washington provide more than 6.2 GB of aggregate connectivity.

Security: Generation Five infrastructure, outfitted with 2 access portals and biometric hand-scanners.

Electrical:

- The IDC has a distributed electrical system - providing a multiple path distribution system, thereby maximizing redundancy
- 10 High-Voltage Distribution Panel (HDP) switch boards, containing 10 Automatic Transfer Switches (ATS).
- 12 Diesel Generators, 2,000 kW each. The distributed system is comprised of 5 primary units, and 1 backup unit. Each generator has a 2,000 gallon fuel belly storage tank, with an additional (top off tank) holding 80,000 gallons, shared.
- 24 500kW primary UPS modules.
- 6 500kW reserve parallel-redundant UPS modules.
- 15 165kva power management modules (PMM).

Mechanical:

- 34 Train rooftop split system air conditioning units @ 120 ton each.
- 2 Liebert systems for NOC/NODE/Power room @ 22 ton each.
- 5 Administrative air conditioning units @ 15 ton each.
- 2 Liebert systems for SubNodes @ 15 ton each.
- VESDA Fire Detection System (Very Early Smoke Detection Annunciation)
- Pressurized, dry-pipe, pre-action fire suppression system

Cloud:

- Amazon AWS or Microsoft Azure instances
- Amazon S3 buckets and Azure storage containers, featuring industry-standard encryption mechanisms
- Key management systems such as KMS and/or Key Vault

- Government compliant regions for CJIS, HIPAA, FEDRAMP and other sensitive systems

Handling of Customer Information

All information systems containing Primary or Custodial Customer Information will display banners that alert any user, whether authorized or not, of the presence of Customer Information. All Customer Information that is no longer needed will be returned to the customer or destroyed as necessary and per required compliance processes. No Customer Information will be disclosed to third parties without written customer consent.

Any media or storage mechanism containing customer information will have a generic name that does not allow a reader to infer the customer identity.

A logical separation will be maintained between all customer information and any other customer's information.

Remote Access

All remote access will comply with the WebQA/GovQA authentication policy. This type of access will require two factor authentication (e.g., VPN and Server). Access to Government regions (Amazon GovCloud and Azure Government) will be restricted to secure office space, requiring additional access controls and available to only properly trained and certified staff. Unescorted access to the secure space is not permitted.

Security Review and Update process

All servers will be reviewed regularly to make sure they are up to date. New patches are reviewed on a case by case basis to determine if they will be applied - Based upon risk, type, impact, etc. Before any significant outage/patch/upgrade all partners & customers are to be notified.

All key logs are reviewed daily. Service interruptions (potentially due to security issues) send out automated notifications that are escalated promptly as necessary. For the Azure Government region, automatic server patches are applied by means of a autonomous, controlled rollout.

Firewall Implementation and Management

Firewalls utilize current, recommended security processes, with the following features or attributes:

- Run the latest OS, firmware and rule sets

- Are hot-failover redundant, regularly tested and verified
- Employ stateful inspection
- Log all intrusion attempts, reviewed daily
- Provide DoS and DDoS protection
- Offer Gigabit (or greater) performance

Virus Prevention and Protection

The Information Technology Group will guard against viruses that disrupt or threaten the viability of all systems. Virus scanning software will be installed on all servers. Users and operators shall not knowingly introduce a computer virus into a WebQA/GovQA computer. Anti-virus and anti-malware protection will be enforced by domain group policy on all user's computers and servers.

Identification and Authentication

All servers and secure access computers will be set to blank their screen (or display a screen saver) after a reasonable period of time and require an authorized user to enter a password to establish or re-establish a session.

No person's identification or authentication information can be used to originate simultaneous processes from multiple physical locations.

Any user identification that has been inactive for an extended period of time will be disabled. If such user identification remains inactive, it will be purged from the system and not reassigned until an appropriate and compliant period of time has elapsed.

Password Usage

The following password policies will be enforced on all servers:

- Users will not disclose their passwords or share passwords.
- Users will not document passwords in any readily perceivable manner.
- Newly-issued passwords will expire on the first use.
- The system's password file will be encrypted.
- Passwords will have an adequate minimum length (e.g. 8 digits) and must be distinctive (e.g., contain both alpha and numeric or symbolic characters), meeting complexity requirements.
- Passwords will automatically expire after an appropriate maximum life (e.g. 90 days, or less where required).
- The system will prevent re-use of recently used passwords (e.g. within the last 365 days and/or the last 10 passwords used).
- The authentication system must limit the number of attempts to enter a password before enforcing a lock-out for the user. (e.g. 3)
- The password change process will force re-authentication.

Utilization of Encryption

An approved encryption method (e.g. minimum 256 bit encryption) will be used when transmitting any information over a network that is not trusted. Furthermore, any information stored on the customer computers by the web application, in the form of cookies, will also be encrypted. AES256 encryption is utilized on all network communications, backups and storage by default. This applies to all data at rest and in motion and also to data center and cloud systems alike.

Records Retention and Backup

Nightly incremental database backups are performed to a separate network attached storage device (NAS) at each data center or secure storage container for each cloud region. These are also replicated via RTRR on a near real time basis. Full weekly database backups are also performed to separate, redundant NAS devices or secure storage containers (as applicable). In addition, client supplied or attached documents are also backup up nightly to redundant NAS devices or secure storage containers and can optionally, be replicated to redundant storage containers. Each secure container (AWS bucket or Azure container) is individual to only that client and is encrypted utilizing AES256 encryption.

Infrastructure Security

Service interruptions (potentially due to security issues) send out automated notifications that are escalated promptly as necessary.

All Windows servers are hardened according to Microsoft certified hardening documents. All other servers and systems are hardened per the recommended procedures by the publisher. Various internal and external monitoring tools are utilized to ensure uptime and event notification.

Disaster Recovery

The Information Technology Group within WebQA/GovQA has recognized the need for and importance of disaster recovery and continuity of operations and has prepared the organization and its information systems accordingly. This process will be tested on a quarterly basis or other level of frequency where specific compliance requirements exist. See the Disaster Recovery section for additional details.

WebQA/GovQA Application Security

The WebQA/GovQA software is homed within our data center (non-Government) processing environment and has specific security parameters which are discussed in the following sections. All software accessing or processing CJIS, HIPAA, FEDRAMP and other sensitive data is homed within an Azure Government region and meets or exceeds all required compliance standards.

Note: CJIS, HIPAA and FEDRAMP systems are entirely cloud-based and reside within compliant Microsoft Azure Government instances. The following sections refer to and/or describe non-CJIS/HIPAA/FEDRAMP systems. See CJIS and HIPAA sections for additional details.

System Architecture

- Each application utilizes its own completely independent database (single-tenant).
- Each database has one non-administrator role that provides read only access via stored procedures.
- The aforementioned non-administrator role is specific to that database and cannot access any other databases.
- The associated user id and password is encrypted and compiled into the COM+ DLL on the application server.
- The system architecture is tiered so that the web site only accesses the business layer objects, which only access that data access objects. The data access objects contain the encrypted user id and password in compiled code. This is then used to access data in the database (via stored procedures only). No direct access from the application to the database is possible.
- Since HTTP and HTTPS is stateless, state is stored within the database. Furthermore, all information passed via URL (e.g., item rights) is validated on both sides of the transaction.

Coding Methodology

All development takes into account potential security holes. In this effort, the following tenets apply:

- Assumptions about the size of user input are not made.
- No unchecked user input is to be processed.
- Specific data validation (form field, SQL injection, etc) apply to all input

System Configuration

The following items describe the actual implementation plan, where applicable, for the aforementioned security guidelines.

Data Restoration - All data can be restored from local backup, separate server backup or remote backup. Two types of items need to be restored - content and data. Each is kept in separate stores. Each database/application implementation contains separate security authentication information. Furthermore, application accessibility is based upon the site name, compiled security ids, encrypted passwords, and server location. Therefore, even if a database was restored incorrectly, the application would not be able to access the data.

Patch management – In general, WebQA/GovQA will adhere to a quarterly (or seasonal) release schedule. The type of release can be either a patch or a level increase. Each version will undergo quality assurance testing by WebQA/GovQA development and quality assurance (QA) testing staff.

All software accessing or processing CJIS, HIPAA, FEDRAMP and other sensitive data is homed within an Azure Government region. The entire system and processing environment was designed and implemented, taking into account all compliance requirements including, but not limited to, security, encryption, access controls and auditing.

Other sections within this document cover these topics in greater detail. In addition, supplemental documents provide further detail.

Service Level Goals

WebQA/GovQA will provide, on a case by case basis, service level goals similar to the following:

Scheduled Maintenance – All necessary, Scheduled Maintenance will occur outside of normal business hours of 7am to 7pm (CT) whenever possible. This will typically also include weekends (Saturday and Sunday).

Internet Connection – WebQA/GovQA's goal is to have its production systems connected to the Internet and available to be accessed by WebQA/GovQA, Resellers, Customers and Reseller's Customers 99.0% of the time, measured in minutes, on a monthly basis, excluding scheduled maintenance. This is a general overall goal for all systems collectively and does not refer to the individual SLA quoted within a client contract.

Disaster Recovery

Data Center

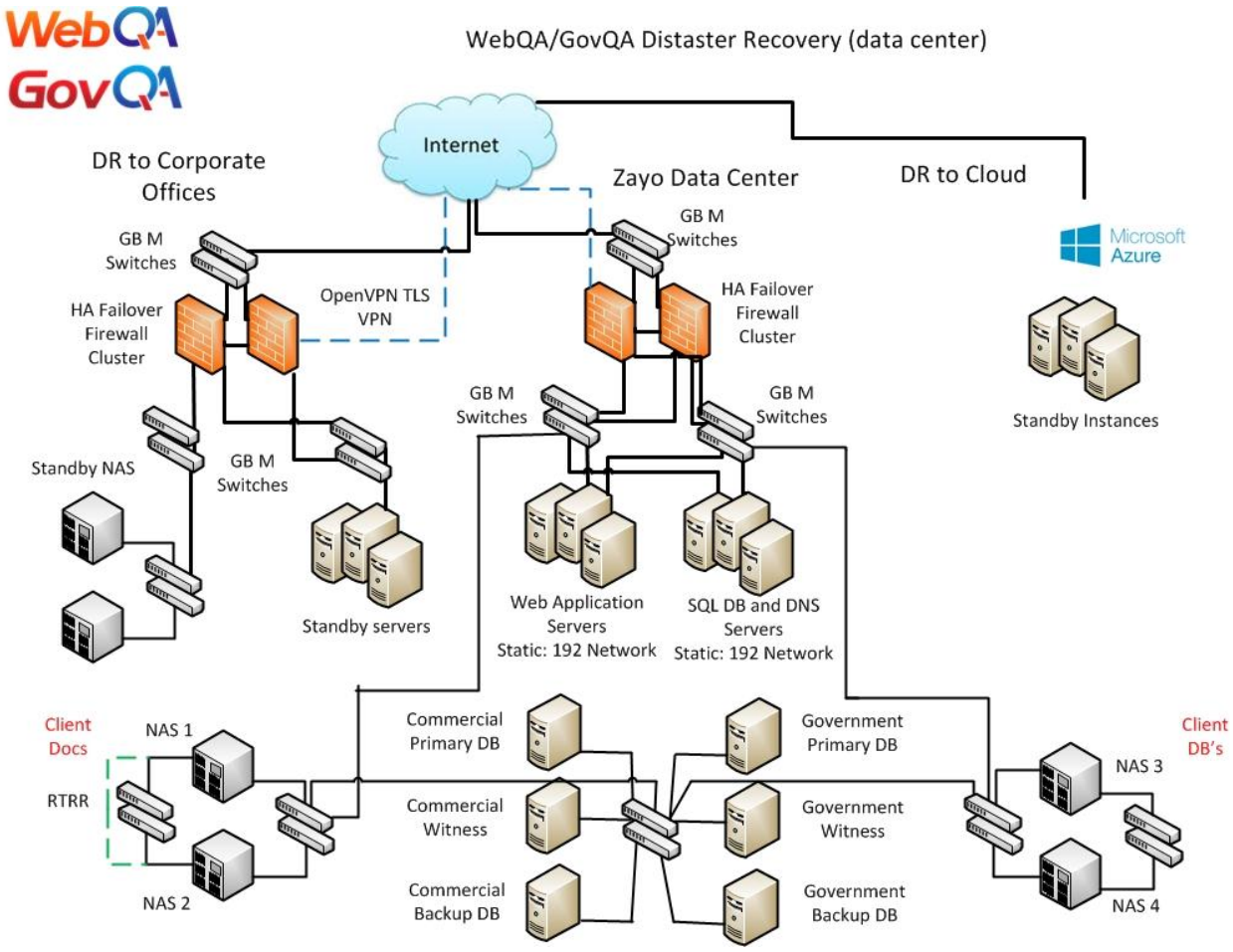


Figure 6: WebQA/GovQA data center disaster recovery diagram

Azure region

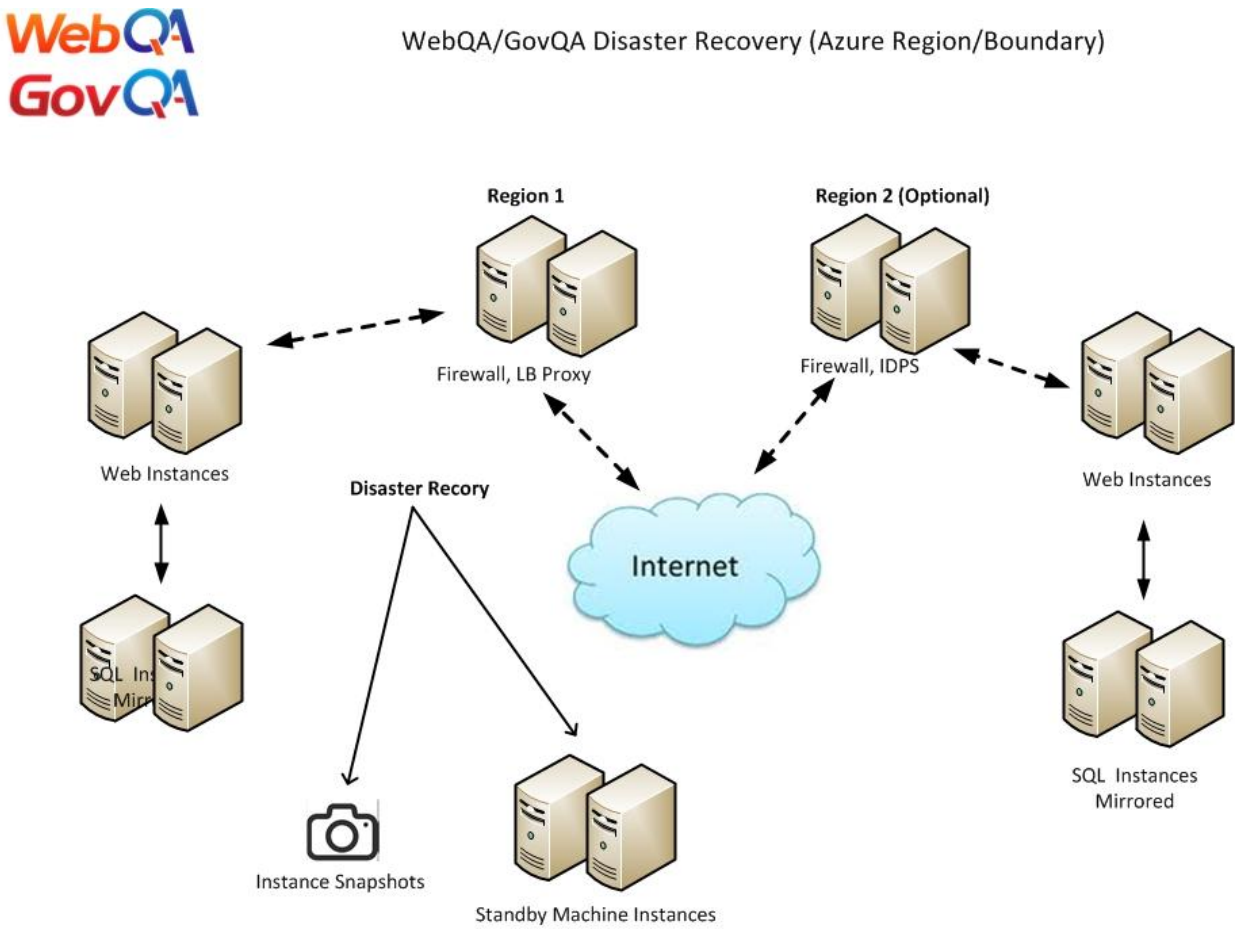


Figure 7: WebQA/GovQA Azure cloud disaster recovery diagram

Disaster Recovery

In the event of a natural disaster, which either crippled or completely destroyed the main data center, services would be automatically rerouted via dynamic DNS to cloud-based systems including Azure or Amazon AWS. Mirrored database instances and identically duplicated and clustered web servers hosted by our cloud providers would provide all services until our own hosted systems could be restored. This not only provides immediate failover for customers, but also cloud system and storage redundancy as well. With this scenario, WebQA/GovQA could continue to deliver services for an indefinite period of time.

In having a secondary hosted data center, critical systems could also be brought up there from backups and run temporarily as the primary data center was restored.

Lastly, the WebQA/GovQA corporate offices provide suitable rack space, power and air conditioning systems to run additional systems temporarily.

High Availability Failover (local failures)

Each WebQA/GovQA location (Corporate office, data centers) each utilize current industry-standard practices to ensure proven (and thoroughly tested) high availability failover mechanisms.

Each location utilizes clustered HA failover firewalls, each capable of assuming inspection, routing and load balancing duties as required. All data communication switches are gigabit managed switches and each has a redundant spare dedicated to it. All servers and NAS units have multiple (minimum two) NIC adapters and an alternate route to network resources in the event of adapter failure.

Each location has multiple provider feeds ensuring continuous bandwidth availability. Automatic failover groups are defined and will reroute provider links upon gateway failure.

The main data center provides fully redundant power circuits, generator backups, air conditioning and provider feeds All are tested at regular intervals. A minimum of once monthly, typically more frequently.

Web servers are clustered and load balanced by purpose. Lower priority clusters will have a minimum of two servers per cluster and higher priority clusters have a minimum of three servers per cluster. Higher priority clusters also have content duplicated across multiple clusters to ensure further protection against failure and data loss.

Database servers are mirrored for redundancy. Each database is backed up nightly to two separate NAS units, utilizing a “full” backup strategy. Nightly backups are saved for seven (7) days. In addition, each database is also backed up weekly to two separate NAS units, utilizing the “full” backup strategy. Weekly backups are saved for eight (8) weeks.

Spare web and database servers are racked at each data center, awaiting service. In addition, spare servers are also built and stored at the WebQA/GovQA corporate offices should they be needed.

Client documents, provided as uploads or attachments, are backed up to one specific NAS device, which runs a live Real Time Remote Replication (RTRR) job to a second, identical NAS device.

All backup jobs, as well as NAS space availability is verified daily as are all sync, rsync and rtrr jobs.

Secure, TLS/SSL VPN tunnels connect each WebQA/GovQA location to each other. These VPN connections require two-step authentication and are only permit site-to-site and management access to remote resources. Each link is verified daily for availability and error-free operation.

Offsite Storage

To finalize WebQA/GovQA DR and HA failover systems, offsite storage for application code, team development projects, source code and critical customer data is saved offsite from each location in the form of secure NAS, server and/or cloud storage. Backup sets are reviewed frequently to verify availability and data integrity. Access to these backup sets is limited to only those IT management staff members who require it, as listed previously in this document.

Disaster Recovery (government cloud)

WebQA/GovQA leverages the compliance and redundancy of the Azure Government platform for all government, CJIS, HIPAA and other sensitive systems.

The Azure platform provides and WebQA/GovQA leverages several key redundancy and disaster recovery features including:

- Server clustering (web servers)
- Instance mirroring (database mirroring)
- Standby machine instances (rapid activation and service restoration)
- Machine/instance snapshots (rapid recovery and restoration)
- Multiple regions for entire system redundancy

All cloud systems are thoroughly verified and tested immediately following activation and in an ongoing quarterly schedule thereafter. Where required for compliance purposes, more frequent testing is performed.

Incident Response and Escalation

WebQA/GovQA utilizes the following security incident response and escalation process (subject to change depending on the actual nature of the incident):

1. Incident or threat is detected
2. WebQA/GovQA security team alerted and begins immediate investigation and collects all available forensics information including logs, files, etc.
3. WebQA/GovQA security team notifies company management team immediately
4. WebQA/GovQA notifies clients and proper authorities within 24 hours (default), sooner if impact may/will be severe or as required by compliance standards/requirements
5. WebQA/GovQA security team remediates the threat as quickly as possible
6. WebQA/GovQA send “all clear” notification to client(s), management team and authorities, including a full report of the threat, remediation actions, impact and future preventative steps

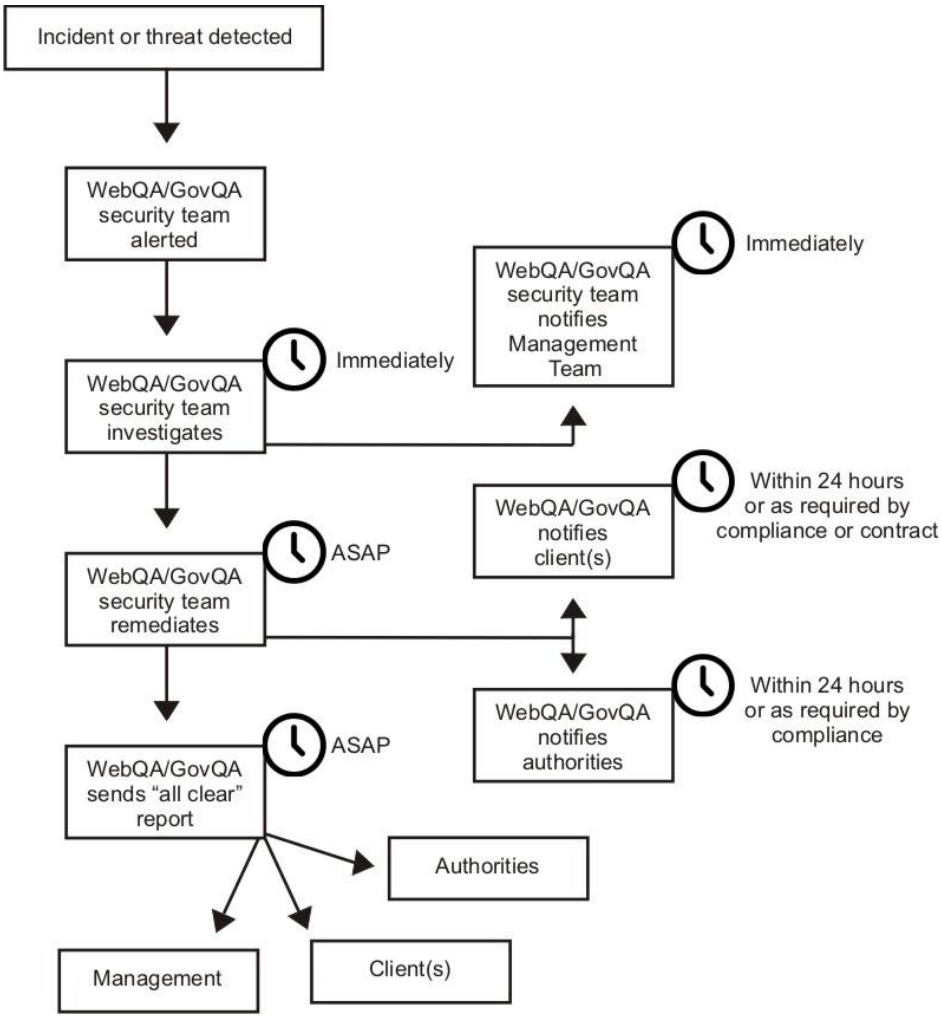


Figure 8: WebQA/GovQA incident response and escalation diagram

Criminal Justice Information Services (CJIS) Compliance

Information Exchange Agreements (CJIS Policy 5.1 Requirements)

WebQA/GovQA recognizes the requirement of information exchange agreements where Criminal Justice Information (CJI) is involved. Where exchange agreement documents exist and are provided by any client or agency engaging the products and/or services of WebQA/GovQA, they will be reviewed and negotiated as appropriate prior to the execution of a contract and the delivery of the intended products and/or services. In the event no such documentation/agreement can be provided by the client or agency, WebQA/GovQA will draft appropriate/compliant documentation and will negotiate and execute the agreement prior to the delivery of products and/or services. The agreement shall include all required terms and conditions including, but not limited to data security, access controls, information handling, data storage, etc. Where required, a CJIS Security Addendum will be signed by WebQA/GovQA.

Monitoring, Review and Delivery of Services (CJIS Policy 5.1.2 Requirements)

WebQA/GovQA will, as required, provide detailed reporting regarding all vulnerability monitoring, detection and remediation; as well as all security incident reporting, tracking and responses. Where required and applicable, WebQA/GovQA will log the transfer or other dissemination of CJI information.

Security Awareness Training (CJIS Policy 5.2 Requirements)

As required and without exception, WebQA/GovQA will conduct and maintain CJIS Security Awareness training. Level 4 CJIS Online training and certification will be held by all WebQA/GovQA personnel who will have access to unencrypted CJI. Other levels will be maintained as appropriate. All formal CJIS Online training and certification will be completed prior to access to CJI being permitted.

In addition to formal CJIS Online training and certification, WebQA/GovQA provides as internal training both general security and CJIS training to all employees and includes this training as part of the new hire employment process. This training must also be completed, with a signed document of acknowledgment prior to access to CJI being permitted.

Detailed records of all security awareness training will be maintained by WebQA/GovQA and will be provided upon request.

Incident Response (CJIS Policy 5.3 Requirements)

WebQA/GovQA maintains various vulnerability and threat scanning, monitoring, prevention, reporting, tracking and remediation systems as follows:

- Intrusion detection and prevention systems
- Perimeter and Web Application Firewalls (WAF)
- Reverse proxy system separation
- Internal and external system vulnerability scanning
- SSL scanning

As required and without exception, WebQA/GovQA will report all security incidents within the required timeframe and format. A director of security (ISO) will actively participate in the deployment, implementation and ongoing management of all systems. Likewise, the security director will actively participate in all incident review and reporting, remediation and recovery events. In addition, the security director will be directly involved with all escalation processes and procedures.

Auditing and Accountability (CJIS Policy 5.4 Requirements)

As required, WebQA/GovQA maintains compliant access control mechanisms and auditing systems as follows:

- File and directory change monitoring and logging
- Detailed access control management and logging
- Detailed change management control and logging
- Autonomous compliance monitoring and logging

In addition to the automated utilities, applications and other systems listed above, the WebQA/GovQA Security Team closely monitors all systems (security, access control and auditing) ensuring all Policy 5.4 requirements are maintained.

Access Control and Management (CJIS Policy 5.5 and 5.6 Requirements)

As required, WebQA/GovQA will closely restrict, manage, monitor and track access to all systems. Various automated systems are utilized to manage access. Strict least-privileged access is always implemented and maintained. In addition, the WebQA/GovQA Security Team closely manages all access

permissions, enforcement, logs and reports to ensure strict compliance with all section 5.5 and 5.6 requirements. WebQA/GovQA restricts access to unencrypted CJI by means of a secured office space and only by Level 4 CJIS trained and certified staff.

Configuration Management (CJIS Policy 5.7 Requirements)

As required, WebQA/GovQA will closely restrict, manage, monitor and track all change management events. Various systems are utilized to manage and track configuration changes as follows:

- Detailed configuration management control and logging
- Autonomous compliance monitoring and logging

In addition, WebQA/GovQA has a change management board (CAB), consisting of the following staff members:

Chief Technology Officer (CTO)

Director of Security (CISO, ISO)

Directory of Technology

Director of Application Security

Infrastructure Support Engineer

All configuration changes with CJIS relevancy requires the review and approval of the CAB.

Media Protection (CJIS Policy 5.8 Requirements)

As required, WebQA/GovQA will protect all media (where applicable) and data both at rest and in motion, conforming to all prescribed/required encryptions methods. Where required and possible, NIST, FIPS 140-2 and other required compliance standards will be strictly implemented and maintained. Compliance with all section 5.8 requirements will be met as applicable.

Physical Protection (CJIS Policy 5.9 Requirements)

As required, WebQA/GovQA will provide suitable physical access mechanisms and control to protect CJIS data. WebQA/GovQA limits access to unencrypted CJIS data to a secured office space and by only Level 4 trained and certified staff. WebQA/GovQA leverages the CJIS compliant facilities and platforms

provided by Microsoft Azure Government. Letters of compliance are available directly from the Microsoft Azure Government site.

System and Communications Protection and Information Integrity (CJIS Policy 5.10 Requirements)

WebQA/GovQA maintains various vulnerability and threat scanning, monitoring, prevention, reporting, tracking and remediation systems as follows:

- Intrusion detection and prevention systems
- Perimeter and Web Application Firewalls (WAF)
- Reverse proxy system separation
- Internal and external system vulnerability scanning
- SSL scanning
- Antivirus / Antimalware
- Automated server patching

As required and without exception, WebQA/GovQA will protect all CJIS data both at rest and in motion. All CJIS and other sensitive data will be stored in either single-tenant SQL databases or encrypted storage containers. All stored and transmitted data will utilize AES256 encryption and will meet all other section 5.10 requirements as possible and applicable.

Formal Audits (CJIS Policy 5.11 Requirements)

WebQA/GovQA utilizes an experienced third party vendor to conduct CJIS compliance audits, including a full review of all policies, procedures and documentation. The audit reports are available to clients and agencies upon request.

In addition, WebQA/GovQA will cooperate with any and all applicable audits by client agencies and other state and federal authorities as required.

Personnel Security (CJIS Policy 5.12 Requirements)

WebQA/GovQA performs a federal background check on all prospective employees prior to offering employment. Once hired, new hires receive both internal general security and CJIS security awareness training as well as CJIS Online training and certification at an appropriate level prior to be granted access to CJIS data. All IT staff members receive Level 4 training and certification.

In addition, all staff members who will be granted access to CJIS and other sensitive data are live-scan finger printed and background checks run at the state (State of Illinois) and Federal (FBI) levels prior to accessing CJI. Where required, other state background checks are also performed to satisfy the needs of the client or agency.

Mobile Devices (CJIS Policy 5.13 Requirements)

WebQA/GovQA maintains compliance with all mobile device requirements as defined in section 5.13. Specific details and additional information will be provided where required and applicable.

Health Insurance Portability and Accountability Act (HIPAA) Compliance

Security, Privacy, Transaction and Code Sets, Unique Identifiers and Enforcement Rules

WebQA/GovQA leverages the Azure Government platform to protect Electronic Protected Health Information (ePHI) and Personal Health Information (PHI) in general during all phases of access, transmission, storage and disposal. As applicable, WebQA/GovQA utilizes various systems, utilities, policies and procedures as follows to meet or exceed the defined HIPAA rules.

Monitoring and Risk Analysis

WebQA/GovQA will, as required, provide detailed reporting regarding all vulnerability monitoring, detection and remediation; as well as all security incident reporting, tracking and responses. Where required and applicable, WebQA/GovQA will log the transfer or other dissemination of ePHI or PHI information.

Security Awareness Training

As required and without exception, WebQA/GovQA will conduct and maintain HIPAA Security Awareness training. Appropriate training and certification will be held by all WebQA/GovQA personnel who will have access to ePHI and PHI. In addition to formal HIPAA training and certification, WebQA/GovQA provides as internal training both general security and HIPAA training to all employees and includes this training as part of the new hire employment process. This training must also be completed, with a signed document of acknowledgment prior to access to ePHI and PHI being permitted.

Detailed records of all security awareness training will be maintained by WebQA/GovQA and will be provided upon request.

Incident Response and Reporting

WebQA/GovQA maintains various vulnerability and threat scanning, monitoring, prevention, reporting, tracking and remediation systems as follows:

- Intrusion detection and prevention systems
- Perimeter and Web Application Firewalls (WAF)

- Reverse proxy system separation
- Internal and external system vulnerability scanning
- SSL scanning

As required and without exception, WebQA/GovQA will report all security incidents within the required timeframe and format. A designated HIPPA compliance officer (CO) will actively participate in the deployment, implementation and ongoing management of all systems. Likewise, the compliance officer will actively participate in all incident review and reporting, remediation and recovery events. In addition, the compliance officer will be directly involved in the creation of all policy creation, procedure definitions and with all escalation processes and procedures.

Auditing and Accountability

As required, WebQA/GovQA maintains compliant access control mechanisms and auditing systems as follows:

- File and directory change monitoring and logging
- Detailed access control management and logging
- Detailed change management control and logging
- Autonomous compliance monitoring and logging

In addition to the automated utilities, applications and other systems listed above, the WebQA/GovQA Security Team closely monitors all systems (security, access control and auditing) ensuring all HIPAA Rule requirements are maintained.

Access Control and Management

As required, WebQA/GovQA will closely restrict, manage, monitor and track access to all systems. Various automated systems are utilized to manage access. Strict least-privileged access is always implemented and maintained. In addition, the WebQA/GovQA Security Team closely manages all access permissions, enforcement, logs and reports to ensure strict compliance with all HIPAA Security Rule requirements. WebQA/GovQA restricts access to ePHI and PHI by means of a secured office space and only by properly trained and certified staff.

Configuration Management

As required, WebQA/GovQA will closely restrict, manage, monitor and track all change management events. Various systems are utilized to manage and track configuration changes as follows:

- Detailed configuration management control and logging
- Autonomous compliance monitoring and logging

In addition, WebQA/GovQA has a change management board (CAB), consisting of the following staff members:

Chief Technology Officer (CTO)

Director of Security (CISO, ISO, CO)

Directory of Technology

Director of Application Security

Infrastructure Support Engineer

All configuration changes with HIPAA relevancy requires the review and approval of the CAB.

Note: WebQA/GovQA employs a full-time security and compliance officer.

Media Protection

As required, WebQA/GovQA will protect all media (where applicable) and data both at rest and in motion, conforming to all prescribed/required encryptions methods. Where required and possible, NIST, FIPS 140-2 and other required compliance standards will be strictly implemented and maintained.

Physical Protection

As required, WebQA/GovQA will provide suitable physical access mechanisms and control to protect ePHI and PHI data. WebQA/GovQA limits access to ePHI and PHI data to a secured office space and by only properly trained and certified staff. WebQA/GovQA leverages the HIPAA compliant facilities and platforms provided by Microsoft Azure Government. Letters of compliance are available directly from the Microsoft Azure Government site.

System and Communications Protection and Information

WebQA/GovQA maintains various vulnerability and threat scanning, monitoring, prevention, reporting, tracking and remediation systems as follows:

- Intrusion detection and prevention systems
- Perimeter and Web Application Firewalls (WAF)
- Reverse proxy system separation
- Internal and external system vulnerability scanning
- SSL scanning
- Antivirus / Antimalware
- Automated server patching

As required and without exception, WebQA/GovQA will protect all ePHI and PHI data both at rest and in motion. All ePHI, PHI and other sensitive data will be stored in either single-tenant SQL databases or encrypted storage containers. All stored and transmitted data will utilize AES256 encryption and will meet all other required data encryption standards.

Formal Audits

WebQA/GovQA utilizes an experienced third party vendor to conduct HIPAA compliance audits, including a full review of all policies, procedures and documentation. The audit reports are available to clients and agencies upon request.

In addition, WebQA/GovQA will cooperate with any and all applicable audits by client agencies and other state and federal authorities as required.

Personnel Security

WebQA/GovQA performs a federal background check on all prospective employees prior to offering employment. Once hired, new hires receive both internal general security and HIPAA security awareness training as well as formal online HIPAA training and certification at an appropriate level prior to being granted access to ePHI and PHI data. All IT staff members receive formal HIPAA security training and certification.

In addition, all staff members who will be granted access to ePHI and PHI and other sensitive data are live-scan finger printed and background checks run at the state (State of Illinois) and Federal (FBI) levels prior to accessing ePHI or PHI. Where required, other state background checks are also performed to satisfy the needs of the client or agency.

NIST and FIPS Compliance

With compliance in mind, for all CJIS, HIPAA, FEDRAMP and other sensitive data processing systems, WebQA/GovQA adheres to NIST Catalog and FIPS compliance standards where applicable and possible. Each key component and/or system within the WeQA/GovQA access boundary has been carefully designed and reviewed to comply with recommended and/or required standards per CJIS, HIPAA, FISMA, FEDRAMP and other requirements, as applicable.

Appendix A

Glossary of Terms

A

ACL	Access control list, a list of attributes, often IP addresses, used to restrict access within a system or to an object.
ANSI	American National Standards Institute
Azure Government	Cloud hosting platform offered by Microsoft, providing FEDRAMP, CJIS, HIPAA and other compliant systems and services

C

CAB	Change Advisory Board, a committee of members who propose, review and approve or deny changes to policies, procedures and systems.
CJIS	Criminal Justice Information Services is a division of the United States Federal Bureau of Investigation (FBI), serves to provide timely and relevant criminal justice information to qualified law enforcement, criminal justice, civilian, academic, employment, and licensing agencies.
Client	Any existing or prospective customer of WebQA/GovQA
CSP	Cloud service provider, a hosting provider such as Amazon (AWS) or Microsoft (Azure)who provides a platform for creating virtual machine environments.
Company	Alias for WebQA, GovQA and WebQA/GovQA collectively

E

ePHI	Electronic Personal Health Information, electronically transferred Personal Health Information. See PHI.

F

FBI	Federal Bureau of Investigations
FEDRAMP	Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.
FIPS	Federal Information Processing Standards, a set of standards that

	describe document processing, encryption algorithms and other information technology standards for use within non-military government agencies and by government contractors and vendors who work with the agencies.
FISMA	Federal Information Security Management Act, United States legislation that defines a comprehensive framework to protect government information, operations and assets against natural or man-made threats.

H

HIPAA	Health Insurance Portability and Accountability Act, United States law designed to provide privacy standards to protect patients' medical records and other health information provided to health plans, doctors, hospitals and other health care providers

N

NIST	National Institute of Standards and Technology is a measurement standards laboratory, and non-regulatory agency of the United States Department of Commerce. Defines and publishes technology standards used by many organizations to form standards-based policies.

P

PHI	Protected health information, includes such items as medical records, insurance claim information, etc.
PII	Personally identifiable information, any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another, includes such items as social security and telephone numbers, home address, etc.

Appendix B

WebQA/GovQA Technology Team Organizational Chart

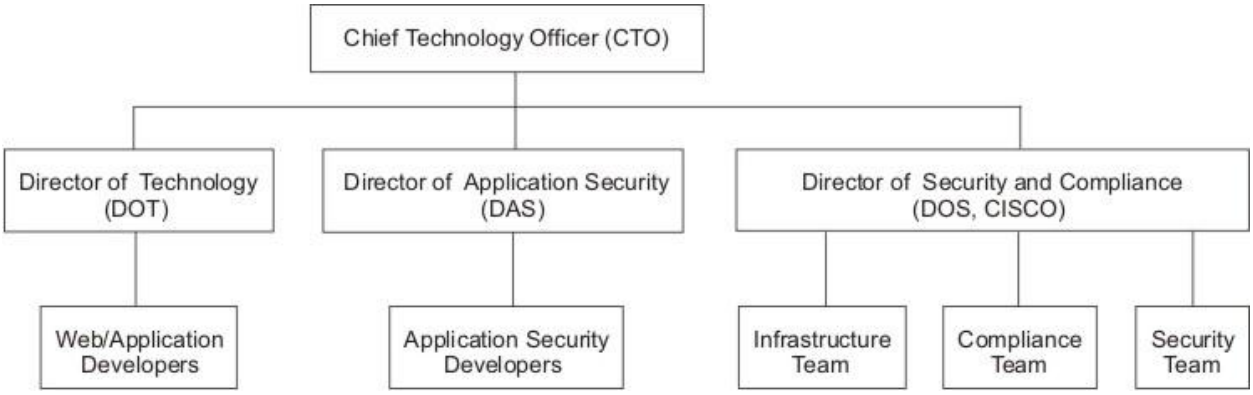


Figure B1: WebQA/GovQA technology management and security team organizational chart

Exhibit E

City of Austin, Texas
NON-DISCRIMINATION AND NON-RETALIATION CERTIFICATION

City of Austin, Texas

Equal Employment/Fair Housing Office

To: City of Austin, Texas,

I hereby certify that our firm complies with the Code of the City of Austin, Section 5-4-2 as reiterated below, and agrees:

(1) Not to engage in any discriminatory employment practice defined in this chapter.

(2) To take affirmative action to ensure that applicants are employed, and that employees are treated during employment, without discrimination being practiced against them as defined in this chapter, including affirmative action relative to employment, promotion, demotion or transfer, recruitment or recruitment advertising, layoff or termination, rate of pay or other forms of compensation, and selection for training or any other terms, conditions or privileges of employment.

(3) To post in conspicuous places, available to employees and applicants for employment, notices to be provided by the Equal Employment/Fair Housing Office setting forth the provisions of this chapter.

(4) To state in all solicitations or advertisements for employees placed by or on behalf of the Contractor, that all qualified applicants will receive consideration for employment without regard to race, creed, color, religion, national origin, sexual orientation, gender identity, disability, sex or age.

(5) To obtain a written statement from any labor union or labor organization furnishing labor or service to Contractors in which said union or organization has agreed not to engage in any discriminatory employment practices as defined in this chapter and to take affirmative action to implement policies and provisions of this chapter.

(6) To cooperate fully with City and the Equal Employment/Fair Housing Office in connection with any investigation or conciliation effort of the Equal Employment/Fair Housing Office to ensure that the purpose of the provisions against discriminatory employment practices are being carried out.

(7) To require of all subcontractors having 15 or more employees who hold any subcontract providing for the expenditure of $2,000 or more in connection with any contract with the City subject to the terms of this chapter that they do not engage in any discriminatory employment practice as defined in this chapter

For the purposes of this Offer and any resulting Contract, Contractor adopts the provisions of the City's Minimum Standard Non-Discrimination and Non-Retaliation Policy set forth below.

City of Austin
Minimum Standard Non-Discrimination and Non-Retaliation in Employment Policy

As an Equal Employment Opportunity (EEO) employer, the Contractor will conduct its personnel activities in accordance with established federal, state and local EEO laws and regulations.

The Contractor will not discriminate against any applicant or employee based on race, creed, color, national origin, sex, age, religion, veteran status, gender identity, disability, or sexual orientation. This policy covers all aspects of employment, including hiring, placement, upgrading, transfer, demotion, recruitment, recruitment advertising, selection for training and apprenticeship, rates of pay or other forms of compensation, and layoff or termination.

The Contractor agrees to prohibit retaliation, discharge or otherwise discrimination against any employee or applicant for employment who has inquired about, discussed or disclosed their compensation.

Further, employees who experience discrimination, sexual harassment, or another form of harassment should immediately report it to their supervisor. If this is not a suitable avenue for addressing their compliant, employees are advised to contact another member of management or their human resources representative. No employee shall be discriminated against, harassed, intimidated, nor suffer any reprisal as a result of reporting a violation of this policy. Furthermore, any employee, supervisor, or manager who becomes aware of any such discrimination or harassment should immediately report it to executive management or the human resources office to ensure that such conduct does not continue.

Contractor agrees that to the extent of any inconsistency, omission, or conflict with its current non-discrimination and non-retaliation employment policy, the Contractor has expressly adopted the provisions of the City's Minimum Non-Discrimination Policy contained in Section 5-4-2 of the City Code and set forth above, as the Contractor's Non-Discrimination Policy or as an amendment to such Policy and such provisions are intended to not only supplement the Contractor's policy, but will also supersede the Contractor's policy to the extent of any conflict.

UPON CONTRACT AWARD, THE CONTRACTOR SHALL PROVIDE THE CITY A COPY OF THE CONTRACTOR'S NON-DISCRIMINATION AND NON-RETALIATION POLICIES ON COMPANY LETTERHEAD, WHICH CONFORMS IN FORM, SCOPE, AND CONTENT TO THE CITY'S MINIMUM NON-DISCRIMINATION AND NON-RETALIATION POLICIES, AS SET FORTH HEREIN, **OR** THIS NON-DISCRIMINATION AND NON-RETALIATION POLICY, WHICH HAS BEEN ADOPTED BY THE CONTRACTOR FOR ALL PURPOSES WILL BE CONSIDERED THE CONTRACTOR'S NON-DISCRIMINATION AND NON-RETALIATION POLICY WITHOUT THE REQUIREMENT OF A SEPARATE SUBMITTAL.

Sanctions:

Our firm understands that non-compliance with Chapter 5-4 and the City's Non-Retaliation Policy may result in sanctions, including termination of the contract and suspension or debarment from participation in future City contracts until deemed compliant with the requirements of Chapter 5-4 and the Non-Retaliation Policy.

Term:

The Contractor agrees that this Section 0800 Non-Discrimination and Non-Retaliation Certificate of the Contractor's separate conforming policy, which the Contractor has executed and filed with the City, will remain in force and effect for one year from the date of filling. The Contractor further agrees that, in consideration of the receipt of continued Contract payment, the Contractor's Non-Discrimination and Non-Retaliation Policy will automatically renew from year-to-year for the term of the underlying Contract.

Dated this 17 day of July, 2017

CONTRACTOR [signature]

Authorized Signature [signature]

Title [signature]

Exhibit F

City of Austin, Texas
Section 0805
NON-SUSPENSION OR DEBARMENT CERTIFICATION

The City of Austin is prohibited from contracting with or making prime or sub-awards to parties that are suspended or debarred or whose principals are suspended or debarred from Federal, State, or City of Austin Contracts. Covered transactions include procurement contracts for goods or services equal to or in excess of $25,000.00 and all non-procurement transactions. This certification is required for all Vendors on all City of Austin Contracts to be awarded and all contract extensions with values equal to or in excess of $25,000.00 or more and all non-procurement transactions.

The Offeror hereby certifies that its firm and its principals are not currently suspended or debarred from bidding on any Federal, State, or City of Austin Contracts.

Contractor's Name: Insight Public Sector

Signature of Officer or Authorized Representative: [signature] Date: 7/17/2017

Printed Name: Todd Brooks

Title: Services Director

County of Fairfax, Virginia

To protect and enrich the quality of life for the people, neighborhoods and diverse communities of Fairfax County

FEB 2 3 2016

Insight Public Sector, Inc.
6820 South Harl Avenue
Tempe, Az 85283

Attention: Erica Falchetti

Reference: RFP 2000001701, Technology Products, Services, Solutions & Related Products and Services

Dear Ms. Falchetti:

Acceptance Agreement

Contract Number: 4400006644

This acceptance agreement signifies a contract award for Technology Products, Services, Solutions and Related Products and Services. The period of the contract shall be from May 1, 2016 through April 30, 2019, with four one-year renewal options or any combination of time equally not more than four years.

The contract award shall be in accordance with:

1) This Acceptance Agreement;

2) The Attached Memorandum of Negotiations.

Please note that this is not an order to proceed. A Purchase Order constituting your notice to proceed will be issued to your firm. Please provide your Insurance Certificate according to Section 17 of the Fairfax County Contract, within 10 days after receipt of this letter. All questions in regards to this contract shall be directed to the Contract Specialist, Lonnette Robinson, at 703-324-3281 or via e-mail at Lonnette.Robinson@fairfaxcounty.gov.

Sincerely,

Cathy A. Muse, CPPO
Director/County Purchasing Agent

Department of Purchasing & Supply Management
12000 Government Center Parkway, Suite 427
Fairfax, VA 22035-0013
Website: www.fairfaxcounty.gov/dpsm
Phone 703-324-3201, **TTY:** 1-800-828-1140, **Fax:** 703-324-3228

MEMORANDUM OF NEGOTIATIONS
RFP2000001701

The County of Fairfax (hereinafter called the County) and Insight Public Sector, Inc., (hereinafter called the "Contractor") agree to the following negotiated issues. The issues listed below shall be part of any subsequent contract.

a. The County's Request for Proposal RFP2000001701 and all Addenda;
b. The Contractor's Technical and Cost Proposals dated September 21, 2015;
c. The Contractor's Functional Roles per Labor Category dated December 2, 2015
d. The Geographic Market Tiers dated 12/10/2015;
e. This Memorandum of Negotiation;
f. County purchase order;
g. Any amendments subsequently issued.

In addition, the County and the Contractor agree to the following:

1. Insight is awarded a contract for the following sections of the RFP:
   - 3.1.1 Technology Products
   - 3.1.2 Technology Services and Solutions
   - 3.1.3 Cisco Products, Services and Solutions
   - 3.1.4 HP Products, Services and Solutions
   - 3.1.5 Dell Products, Services and Solutions
   - 3.1.6 Panasonic Products, Services and Solutions
   - 3.1.7 EMC² Products, Services and Solutions
   - 3.1.8 CommVault Products, Services and Solutions
   - 3.1.9 Symantec Products, Services and Solutions
   - 3.1.10 Veritas Products, Services and Solutions
   - 3.1.11 VMWare Products, Services and Solutions
   - 3.1.12 Apple Products, Services and Solutions
   - 3.1.15 Microsoft Products, Services and Solutions
   - 3.1.16 Citrix Products, Services and Solutions
   - 3.1.17 NetApp Products, Services and Solutions
   - 3.1.18 Related Products, Services and Solutions

2. Participating Public Agencies reserve the right to request pricing with both service pricing methodologies: Service Category Rates and Time and Material Rates.

3. Pricing discount for Cisco hardware/software is 36% off MSRP for both government and education. Discounts are minimum discounts.

4. Any discounts are minimum discounts and any rates are not-to-exceed rates.

5. Contractor will offer Public Agencies the lowest possible price for which they are eligible under any contract available to the customer through this contract award. Insight will check for lowest possible price when an order is placed.

6. Any End User License Agreements (EULA's) referenced in Contractor's proposal is not incorporated as a part of the contract.

7. The Lead Public Agency acknowledges for itself and on behalf of each Participating Public Agency electing to procure under the Master Agreement that it may be required to execute one or more applicable Contractor standard contract documents if and when it orders one or more technology product, service/solution. At the time that an order for a technology product, service/solution is placed by a Public Agency, the Public Agency will review the applicable standard contract document(s) and, if acceptable to each particular Public Agency, complete and sign such document(s). Contractor agrees and acknowledges that if and when an order for one or more technology product, service/solution is placed by Lead Public Agency, Contractor may be required to execute a Contract Addendum substantially in the form attached hereto as License Agreement Addendum.

8. In the event that additional third-party products are procured under the Contract, the Contractor agrees to provide a copy of any and all applicable third-party agreements for review by the County. The County reserves the right to negotiate the terms and conditions of the third-party agreements associated with the use of the third-party products prior to issuing the purchase order for additional products.

9. The parties agree that any Statement/Scope of Work (SOW) and/or Service Level Agreement will be subject to negotiations and will be binding upon the parties and set forth in a written amendment to the Contract signed by the County Purchasing Agent and the Contractor.

ACCEPTED BY:

Kenneth Lamneck, Chief Executive Officer
Insight Public Sector, Inc.

2/9/16
Date

Cathy A. Muse, CPPO, Director
Department of Purchasing and Supply Management

2/22/16
Date

LICENSE AGREEMENT ADDENDUM

Fairfax County (hereinafter referred to as "the County") and Insight Public Sector, Inc. ("Supplier"), a business incorporated in Illinois, F.E.I.N. 36-3949000, having its principal place of business at 6820 S. Harl Ave.,Tempe, Arizona 85283 are this day entering into a contract and, for their mutual convenience, the parties are using the standard form contracts provided by Supplier. This addendum, duly executed by the parties, is attached to and hereby made a part of Supplier's standard form contracts and together shall govern the use of any and all Technology Product, Services and Solutions licensed by the County whether or not specifically referenced in the order document.

As used herein, the term "contract" shall mean Supplier's standard form contract(s) and any and all exhibits and attachments thereto, and any additional terms and conditions incorporated or referenced therein. The term(s) "Customer," "You," and/or "you," as used in the contract(s), shall mean, as applicable, Fairfax County, or any of its officers, directors, agents or employees.

Supplier's standard form contracts are, with the exceptions noted herein, acceptable to the County. Nonetheless, because certain standard clauses that may appear in, or be incorporated by reference into, Supplier's standard form contract(s) cannot be accepted the County, and in consideration of the convenience of using those forms, and this form, without the necessity of specifically negotiating a separate contract document, the parties hereto specifically agree that, notwithstanding any provisions appearing in the attached Supplier's standard form contract(s), none of the following shall have any effect or be enforceable against the County or any of its officers, directors, employees or agents:

1. Requiring the application of the law of any state other than the Commonwealth of Virginia in interpreting or enforcing the contract or requiring or permitting that any dispute under the contract be resolved in any court other than a circuit court of the Commonwealth of Virginia;

2. Requiring any total or partial compensation or payment for lost profit or liquidated damages by the County, or its officers, directors, employees or agents if the contract is terminated before its ordinary period;

3. Imposing any interest charge(s) contrary to that specified by § 2.2-4352 of the Code of Virginia;

4. Requiring the County to maintain any type of insurance either for the benefit of the County or for Supplier's benefit;

5. Granting Supplier a security interest in property of the County or the Commonwealth or any of their officers, directors, employees or agents;

6. Requiring the County or any of its officers, directors, employees or agents to indemnify or to hold harmless Supplier for any act or omission;

7. Limiting or adding to the time period within which claims can be made or actions can be brought (Reference *Code of Virginia* §8.01 et seq.);

8. Limiting selection and approval of counsel and approval of any settlement in any claim arising under the contract and in which the County or any of its officers, directors, employees or agents is a named party;

9. Binding the County or any of its officers, directors, employees or agents to any arbitration or to the decision of any arbitration board, commission, panel or other entity;

10. Obligating the County, or any of its officers, directors, employees or agents, to pay costs of collection or attorney's fees;

11. Requiring any dispute resolution procedure(s) other than those in accordance with the Fairfax County Purchasing Resolution and the Code of Virginia;

12. Permitting Supplier to access any County records or data, except pursuant to court order, or as required by law;

13. Permitting Supplier to use any information provided by the County except for Supplier's own internal administrative purposes, or as required by law;

14. Requiring the County to limit its rights or waive its remedies at law or in equity, including the right to a trial by jury; and

15. Bestowing any right or incurring any obligation that is beyond the duly granted authority of the undersigned representative of the County to bestow or incur on behalf of the County.

16. Establishing a presumption of severe or irreparable harm to Supplier by the actions or inactions of the County;

17. Limiting the liability of Supplier for property damage or personal injury;

18. Permitting Supplier to assign, subcontract, delegate or otherwise convey the contract, or any of its rights and obligations thereunder, to any entity without the prior written consent the County except as follows: Supplier may assign all or any of its rights and obligations to a third party as a result of a merger or acquisition or sale of all or substantially all of its assets to such third party provided assignee agrees in writing to be bound by the terms and conditions set forth in the contract and provided such third party is a U.S.-based entity or maintains a registered agent and a certification of authority to do business in Virginia, or to an affiliate of Supplier, provided Supplier remains liable for affiliate's compliance with the terms and conditions set forth in this Contract;

19. Not complying with contractual provisions 1, 8, 10, 11, 12, and 13 at the following URL, which are mandatory provisions, required by law or by the Fairfax County Purchasing Resolution, which are hereby incorporated by reference: http://www.fairfaxcounty.gov/purchasing/po/termsandcondition.htm.

    The terms and conditions in documents posted to the aforereferenced URL are subject to change pursuant to action by the legislature of the Commonwealth of Virginia or a change in the Fairfax County Purchasing Resolution as adopted by the Fairfax County Board of Supervisors. Software Publisher is advised to check the URL periodically;

20. Not complying with the contractual claims provision of the Fairfax County Purchasing Resolution which is also incorporated by reference;

21. Enforcing the United Nations Convention on Contracts for the International Sale of Goods and all other laws and international treaties or conventions relating to the sale of goods. They are expressly disclaimed. UCITA shall apply to this contract only to the extent required by § 59.1-501.15 of the Code of Virginia;

22. Not complying with all applicable federal, state, and local laws, regulations, and ordinances;

23. Requiring that the County waive any immunity to which it is entitled by law;

24. Requiring that the County, which is tax exempt, be responsible for payment of any taxes, duties, or penalties;

25. Requiring or construing that any provision in this contract conveys any rights or interest in County data to Supplier;

26. Obligating the County beyond approved and appropriated funding. All payment obligations under this contract are subject appropriations by the Fairfax County Board of Supervisors for this purpose. In the event of non-appropriation of funds for the items under this contract, the County may terminate, in whole or in part, this contract or any order, for those goods or services for which funds have not been appropriated. This may extend to the renewal of maintenance services for only some of the licenses granted by Supplier. Written notice will be provided to the Supplier as soon as possible after legislative action is completed. There shall be no time limit for termination due to termination for lack of appropriations;

27. Permitting unilateral modification of the contract by Supplier;

28. Permitting unilateral termination by Supplier of the contract or the licenses granted thereunder, or permitting suspension of services by Supplier, except pursuant to an order from a court of competent jurisdiction, or as required by law;

29. Requiring or stating that the terms of the Supplier's standard form contract shall prevail over the terms of this addendum in the event of conflict;

30. Renewing or extending the contract beyond the initial term or automatically continuing the contract period from term to term;

31. Requiring that the contract be "accepted" or endorsed by the home office or by any other officer subsequent to execution by an official of the County before the contract is considered in effect;

32. Delaying the acceptance of the contract or its effective date beyond the date of execution;

33. Defining "perpetual" license rights to have any meaning other than license rights that exist in perpetuity unless otherwise terminated in accordance with the applicable provisions of the contract;

34. Permitting modification or replacement of the contract pursuant to any new release, update or upgrade of Software or subsequent renewal of maintenance. If Supplier provides an update or upgrade subject to additional payment, the County shall have the right to reject such update or upgrade;

35. Requiring purchase of a new release, update, or upgrade of Software or subsequent renewal of maintenance in order for the County to receive or maintain the benefits of Supplier's indemnification of the County against any claims of infringement on any third-party intellectual property rights;

36. Prohibiting the County from transferring or assigning to any entity the contract or any license pursuant to the contract;

37. Granting Supplier or an agent of Software Publisher the right to audit or examine the books, records, or accounts of the County other than as may be required by law;

The parties further agree as follows:

38. Supplier warrants that it is the owner of the Software or otherwise has the right to grant to the County the license to use the Software granted hereunder without violating or infringing any law, rule, regulation, copyright, patent, trade secret or other proprietary right of any third party.

39. Supplier agrees to indemnify, defend and hold harmless the County or its officers, directors, agents and employees ("County's Indemnified Parties") from and against any and all third party claims, demands, proceedings, suits and actions, including any related liabilities, obligations, losses, damages, fines, judgments, settlements, expenses (including attorneys' and accountants' fees and disbursements) and costs (each, a "Claim" and collectively, "Claims"), incurred by, borne by or asserted against the County's Indemnified Parties to the extent such Claims in any way relate to, arise out of or result from: (i) any intentional or willful conduct or negligence of any employee or subcontractor of Supplier, (ii) any act or omission of any employee or subcontractor of Supplier, (iii) breach of any representation, warranty or covenant of Supplier contained herein, (iv) any defect in the Software, or (v) any actual or alleged infringement or misappropriation of any third party's intellectual property rights by any of the Software. Selection and approval of counsel and approval of any settlement shall be accomplished in accordance with all applicable laws, rules and regulations. In all cases the selection and approval of counsel and approval of any settlement shall be satisfactory to the County against whom the claim has been asserted. This indemnification provision shall supersede any infringement indemnification provision set forth Supplier's standard form contract(s). No limitation of liability provision included in the contract shall apply to Supplier's indemnification obligations under this paragraph.

40. The County shall not be required to maintain as confidential any information, data, or records that have not been properly designated as trade secret or proprietary information pursuant to Va. Code Ann. § 2.2-4342(F) and are not otherwise exempted from the provisions of the Virginia Freedom of Information Act, Va. Code Ann. § 2.2-3700, *et seq*.

41. All information provided by the County pursuant to the contract shall be treated as confidential information and shall not be disclosed by Supplier, its employees, agents or subcontractors, except as specifically set forth in the contract documents. The County's confidential information shall include, but shall not be limited to: (a) Protected Health Information, as defined in HIPAA, which shall be subject to the County Business Associate Agreement, if applicable; and (b) any personally identifiable information included in information provided by the County.

    Supplier shall indemnify and hold the County harmless including, its officers, trustees, employees, and agents, from any and all claims, penalties, fines, costs, liabilities or damages, including but not limited to reasonable attorney fees, incurred by the County as a direct result of the acts or omissions of Supplier, its employees, officials, agents, or subcontractors that cause a failure to maintain confidentiality of information as required under the contract and applicable law, including but not limited to breach of HIPAA requirements and unauthorized access to, or failure to maintain confidentiality of, personally identifiable information. Supplier will promptly provide notice to the County of any breach of security or confidentiality of information provided by the County and shall be responsible for actions required to cure such breach resulting from Supplier's action or inaction. This indemnity obligation is supplemental to any other indemnification obligation set forth in this Addendum. No limitation of liability provision included in the contract shall apply to Supplier's indemnification obligations under this paragraph.

This contract, consisting of this Fairfax County License Agreement Addendum and the Supplier's standard form contract and any and all exhibits and attachments thereto, and any additional terms and conditions incorporated or referenced therein, constitute the entire agreement between the parties and may not be waived or modified except by written agreement between the parties.

IN WITNESS WHEREOF, the parties have caused this contract to be duly executed as of the last date set forth below by the undersigned authorized representatives of the parties, intending thereby to be legally bound.

Insight Public Sector, Inc.

By: _____
(Signature)

Name: _Kenneth Lamneck_____
(Print)

Title: _Chief Executive Officer_____

Date: _2/8/2016_____

Fairfax County

By: Cathy A Muse
(Signature)

Name: Cathy A. Muse
(Print)

Title: Director/County Purchasing Agent

Date: 2/22/16

CERTIFICATE OF INTERESTED PARTIES

FORM 1295

Complete Nos. 1 - 4 and 6 if there are interested parties.
Complete Nos. 1, 2, 3, 5, and 6 if there are no interested parties.

OFFICE USE ONLY
CERTIFICATION OF FILING

Certificate Number:
2017-237429

Date Filed:
07/17/2017

Date Acknowledged:

1 Name of business entity filing form, and the city, state and country of the business entity's place of business.
Insight Public Sector, Inc.
Tempe, AZ United States

2 Name of governmental entity or state agency that is a party to the contract for which the form is being filed.
City of Austin

3 Provide the identification number used by the governmental entity or state agency to track or identify the contract, and provide a description of the services, goods, or other property to be provided under the contract.
MA-5600-NC170000045
U.S. Communities Contract No. 4400006644, Reseller of IT products and services

4 Name of Interested Party	City, State, Country (place of business)	Nature of interest (check applicable)	
		Controlling	Intermediary

5 Check only if there is NO Interested Party. [X]

6 AFFIDAVIT

I swear, or affirm, under penalty of perjury, that the above disclosure is true and correct.

SHERRI L WEST
Notary Public – Arizona
Maricopa County
My Comm. Expires Jun 25, 2021

Signature of authorized agent of contracting business entity

AFFIX NOTARY STAMP / SEAL ABOVE

Sworn to and subscribed before me, by the said Lisanne Steinheiser, this the 17 day of July, 20 17, to certify which, witness my hand and seal of office.

Signature of officer administering oath | Sherri L. West — Printed name of officer administering oath | Notary Public — Title of officer administering oath