



Request for Proposals # 274-533

Title: Records Management System

Issue Date: October 9th, 2026

Due Date: November 20th, 2026 **no later than 5:00PM EST**

LATE PROPOSALS WILL NOT BE ACCEPTED

Issuing Department: *Raleigh Fire Department*

Direct all inquiries concerning this RFP to:

Daniel Clark

Business Services Manager

Email: RFDContracts@raleighnc.gov

Table of Contents

1.	Introduction	2
1.1	Purpose	2
1.2	Background.....	2
1.3	RFP Timeline	3
1.4	Pre-Proposal Conference	3
1.5	Proposal Question	3
1.6	Proposal Submission Requirements & Contact Information	4
1.7	Business Engagement & Opportunities	5
1.8	Rights to Submitted Material.....	5
1.9	Communications	5
1.10	Lobbying	5
1.11	Conflicts of Interest	5
1.12	Proposer Expenses	7
1.13	Proposer Acceptance	7
2.	Proposals	7
2.1	Request for Proposals Required Document Format	7
2.2	RFP Documents	18
3.	Proposal Evaluation	18
3.1	Proposal Evaluation Criteria (Stage 1).....	19
3.2	Interview/Demonstration (Stage 2)	20
3.3	Final Selection	20
3.4	Notice to Proposers Regarding RFP Terms & Conditions	20
3.5	Contract Term.....	20
4.	Scope of Services	20
	Appendix I – Proposal Cost Form	23
	Appendix II – Proposer Questionnaire	24
	Appendix III – Reference Questionnaire (Instructions)	25
	Appendix III – Reference Questionnaire Form.....	26
	Appendix IV – Sample Contract	28
	Appendix V – Product Requirements Matrix.....	49
	Appendix VI – Sample CoR Vendor Security Questionnaire.....	64

1 INTRODUCTION

1.1 Purpose

The City of Raleigh (COR) is soliciting proposals from one or more firm(s) with which to contract for the following services:

*The City of Raleigh (COR) is soliciting proposals from one or more firm(s) with which to contract for the following services: **The Raleigh Fire Department is seeking a comprehensive Records Management System, with modules that should include at a minimum, functionality for pre-incident planning, fire inspections, incident reporting, scheduling, personnel records, community risk reduction, health and safety, reporting and analytics, Computer-Aided Dispatch (CAD) integration, training, fire investigation, command operations, and asset and inventory management.***

A detailed scope of services is provided in Section 4 of this document.

All information related to this solicitation, including any addenda, will be posted to the North Carolina electronic Vendor Portal (eVP) at <https://evp.nc.gov/>.

All questions related to this solicitation must be submitted in writing (via email) to the following individual – questions submitted via telephone will not be answered:

Contact Name	Email Address
Daniel Clark	RFDContracts@Raleighnc.gov

1.2 Background

The City of Raleigh, the Capital City of North Carolina, remains one of the fastest growing areas in the country. A great economy, top educational institutions, and exceptional health care facilities are some of the characteristics that attract people to the triangle area. The mild climate, diverse work force and proximity to Research Triangle Park combine to make Raleigh a great place to live.

Raleigh is a 21st Century City of Innovation focusing on environmental, cultural, and economic sustainability. The City conserves and protects our environmental resources through best practice and cutting-edge conservation and stewardship, land use, infrastructure and building technologies. The City welcomes growth and diversity through policies and programs that will protect and enhance Raleigh's existing neighborhoods, natural amenities, history, and cultural and human resources for future generations. The City leads to improve quality of life for neighborhoods and standard of living for all citizens. The City works with universities, colleges, citizens, and local partners to promote new technology, create new job opportunities, and encourage local businesses and entrepreneurs. The City enlists and prepares 21st Century staff with the skill sets to carry out the duties of the City through transparent civic engagement and by providing the very best customer service to our citizens.

The City of Raleigh is seeking proposals from qualified vendors to provide a Records Management System for the Raleigh Fire Department. With the current contract approaching expiration, this RFP seeks

to ensure continued access to a system that supports the Department's operational, reporting, and records management needs.

1.3 **Request for Proposal (RFP) Timeline**

Provided below is a list of the anticipated schedule of events related to this solicitation. The City of Raleigh reserves the right to modify and/or adjust the following schedule to meet the needs of the service. All times shown are Eastern Time (EST):

RFP Process	Date and Time
RFP Date	<i>October 9th, 2026 2:00 PM EST</i>
Pre-Proposal Meeting/Site-Visit (if required)	N/A
Deadline for Written Questions	<i>October 30th, 2026 2:00 PM EST</i>
City Response to Questions (anticipated)	<i>November 6th, 2026</i>
Proposal Due Date and Time	<i>November 20th, 2026 by 5:00 PM EST</i>
Evaluation Meeting (anticipated)	<i>December/January</i>
Interviews (if required)	<i>TBD, December 2026-January 2026</i>
Selection Announced (tentative)	<i>TBD, post Interviews</i>

1.4 **Pre-Proposal Conference**

If the City of Raleigh elects to conduct a Pre-Proposal Conference or Site Visit, attendance by prospective proposers is strongly encouraged but is not mandatory. Prospective Proposers are encouraged to submit written questions in advance. Date, time, and location of pre-proposal conference is shown above in the RFP Timeline (Section 1.3).

1.5 **Proposal Questions**

Requests for clarification and questions to this RFP must be received by the City not later than the date shown above in the RFP Timeline (Section 1.3) for the submittal of written inquiries. The firm's failure to request clarification and submit questions by the date in the RFP Timeline above shall be considered to constitute the firm's acceptance of all City's terms and conditions and requirements.

The City shall issue addenda reflecting questions and answers to this RFP, if any, and shall be posted to North Carolina electronic Vendor Portal ([eVP](#)). No information, instruction or advice provided orally or informally by any City personnel, whether made in response to a question or otherwise in connection with this RFP, shall be considered

authoritative or binding. Proposers can only rely on written material contained in an Addendum to this RFP.

It is important that all Proposers submitting to this RFP periodically check [eVP](#) for any Addenda. It is the Proposers responsibility to ensure that all addenda have been reviewed and, if required signed and returned.

All questions related to this solicitation must be submitted in writing (via email) to the following individual – questions submitted via telephone will not be answered:

Contact Name	Email Address
Daniel Clark	RFDContracts@raleighnc.gov

1.6 Proposal Submission Requirements and Contact Information

Proposals must follow the format as defined in Section 2 (PROPOSALS), and be addressed and submitted as follows:

<u>DELIVERED BY US POSTAL SERVICE MAIL:</u>	<u>DELIVERED BY OTHER DELIVERY SERVICES:</u>
City of Raleigh ATTN: Daniel Clark 310 West Martin Street Suite 200 Raleigh, NC 27601 RFP No. 274-533	City of Raleigh ATTN: Daniel Clark 310 West Martin Street Suite 200 Raleigh, NC 27601 RFP No. 274-533

Proposals must be enclosed in an envelope or package and clearly marked with the name of the submitting company, the *RFP number* and the *RFP Title*.

Proposers must submit:

- A. one (1) signed original;
- B. one (1) electronic version of the signed proposal and;
- C. and (1) copies of the signed proposal.

The electronic version of the Proposal must be submitted as a viewable and printable Adobe Portable Document File (PDF) on a USB Flash Drive. Both hard copy and electronic versions must be received by the City on or before the RFP due date and time provided in RFP Timeline (Section 1.3). Proposals received after the RFP due date and time will not be considered and will be returned unopened to the return address on the submission envelope or package.

Proposers must respond to the entire Request for Proposals (RFP). Any incomplete proposal may be eliminated from competition at the discretion of the

City of Raleigh. The City reserves the right to reject any or all proposals for any reason and to waive any informality it deems in its best interest.

Proposals that arrive after the due date and time will not be accepted or considered for any reason whatsoever. If the firm elects to mail in its response, the firm must allow sufficient time to ensure the City's proper receipt of the package by the time specified in the RFP Timeline (Section 1.3). Regardless of the delivery method, it is the responsibility of the firm to ensure that their proposal arrives at the designated location specified in this Section by the due date and time specified in the RFP Timeline (Section 1.3).

1.7 Business Engagement & Opportunities

The City of Raleigh maintains processes to conduct business with all business enterprises, including small, emerging, growing, under-capitalized, and under-resourced firms or organizations.

1.8 Rights to Submitted Material

All proposals and supporting materials, as well as correspondence relating to this RFP, shall become the property of the City. The content of all submittals will be held confidential until the selection of the firm is made. Proposals will be reviewed by the Evaluation Team, as well as other City staff and members of the general public who submit public record requests. ***Any proprietary data must be clearly marked.*** In submitting a Proposal, each Prospective Proposer agrees that the City may reveal any trade secret materials contained in such response to all City staff and City officials involved in the selection process and to any outside consultant or other third party who serves on the Evaluation Team or who is hired by the City to assist in the selection process.

Proposals marked entirely as “confidential”, “proprietary”, or “trade secret” will be considered non-responsive and will be removed from the evaluation process.

1.9 Communications

All communications of any nature regarding this RFP with any City staff, elected City officials, evaluation committee members, are strictly forbidden from the time the solicitation is publicly posted until award. Questions must be submitted in writing to the individual designated in Section 1.1 (Purpose), prior to the deadline provided in the RFP Timeline (Section 1.3). Violation of this provision may result in the firm's proposal being removed from consideration.

1.10 Lobbying

By responding to this RFP, the firm certifies that it has not and will not pay any person or firm to influence or attempt to influence an officer or employee of the City or the State of North Carolina, or any elected official in connection with obtaining a contract as a result of this RFP.

1.11 Conflicts of Interest

City of Raleigh contracts are controlled by three conflict of interest provisions.

First, federal procurement standards provide in 2 CFR 200.318 (c)(1),

No employee, officer, or agent may participate in the selection, award, or administration of a contract supported by a Federal award if he or she has a real or apparent conflict of interest. Such a conflict of interest would arise when the employee, officer, or agent, any member of his or her immediate family, his or her partner, or a firm which employs or is about to employ any of the parties indicated herein, has a financial or other interest in or a tangible personal benefit from a firm considered for a contract. The officers, employees, and agents of the non-Federal entity may neither solicit nor accept gratuities, favors, or anything of monetary value from contractors or parties to subcontracts.

Similarly, the North Carolina General Statutes provides a *criminal* statute for conflicts of interest in public contracting. N.C.G.S. § 14-234(a):

(1) No public officer or employee who is involved in making or administering a contract on behalf of a public agency may derive a direct benefit from the contract except as provided in this section, or as otherwise allowed by law. (2) A public officer or employee who will derive a direct benefit from a contract with the public agency he or she serves, but who is not involved in making or administering the contract, shall not attempt to influence any other person who is involved in making or administering the contract. (3) No public officer or employee may solicit or receive any gift, favor, reward, service, or promise of reward, including a promise of future employment, in exchange for recommending, influencing, or attempting to influence the award of a contract by the public agency he or she serves.

City of Raleigh Charter Section 3.9 regulates private transactions between the City and its officials and employees. The Charter states:

No member of the City Council, official, or employee of the City of Raleigh shall be financially interested, or have any personal beneficial interest, either directly or indirectly, as agent, representative, or otherwise, in the purchase of, or contract for, or in furnishing any materials, equipment or supplies to the City of Raleigh, nor shall any official or employee of the City of Raleigh accept or receive, or agree to accept or receive, directly or indirectly, from any person, firm or corporation to whom any contract may be awarded or from whom any materials, equipment or supplies may be purchased by the City of Raleigh, by rebate, gift, or otherwise, any money or anything of value whatsoever, or any promise, obligation or contract for future reward or compensation, for recommending or procuring the uses of any such materials, equipment or supplies by the City of Raleigh; no member of the City Council, official or employee of the City of Raleigh shall for his own personal benefit operate, directly or indirectly, any concession in any building or on any lands of the City of Raleigh, nor shall any official or employee of the City of Raleigh bid for or be awarded any contract granting concessionary rights of any nature or kind from the City of Raleigh; it shall be unlawful for any member of the City Council, official or employee of the City of Raleigh to bid for or to purchase or to contract to purchase from the City of Raleigh any real estate, equipment, materials, or supplies of any nature or kind whatsoever, either directly or indirectly, at either public or private sale, either singly, or through or jointly with any other person.

1.12 Proposer Expenses

The City of Raleigh will not be responsible for any expenses incurred by any Proposer in the development of a response to this Request for Proposal or any other activities associated with this procurement including but not limited to any onsite (or otherwise) interviews and/or presentations, and/or supplemental information provided, submitted, or given to City of Raleigh and/or its representatives. Further, the City of Raleigh shall reserve the right to cancel the work described herein prior to issuance and acceptance of any contractual agreement/purchase order by the recommended Proposer even if the awarding authority for each entity has formally accepted a recommendation.

1.13 Proposer Acceptance

Submission of any proposal indicates a Proposer's acceptance of the conditions contained in this RFP. Furthermore, the City of Raleigh is not bound to accept a proposal on the basis of lowest price, and further, the City has the sole discretion and reserves the right to cancel this RFP, and to reject any and all proposals, to waive any and all informalities and/or irregularities and reserves the right to re-advertise this RFP with either the identical or revised scope and specifications if it is deemed to be in the best interests of the City to do so.

The City of Raleigh reserves the right to accept or reject any or all of the items in the proposal, and to award the contract in whole or in part and/or negotiate any or all items with individual Proposers if it is deemed in the best interest of the City to do so. Moreover, the City reserves the right to make no selection if proposals are deemed to be outside the fiscal constraint or not in the best interest of the City.

2 PROPOSALS

Submitted proposals must follow the format outlined below. The City may reject as non-responsive at its sole discretion any proposal that does not provide complete and/or adequate responses or departs in any substantial way from the required format.

2.1 Request for Proposals Required Document Format

Proposals should be on 8-1/2" x 11" (A4-sized) paper, printed on both sides, bound with only removable clips or staples (no 3-ring binders), and divided into sections using tabs to easily identify and separate each section as follows:

2.1.1. Section/Tab 1: Cover Letter

Provide an introduction letter summarizing the unique proposal of your firm to meet the needs of this service requirement. This letter should be presented on the firm's official letterhead and signed by an authorized representative who has the authority to enter into a contract with the City on behalf of the firm. Additionally, include the name, address, telephone and email address of the individual who serves as the point of contact for this solicitation.

2.1.2. Section/Tab 2: Corporate Background and Experience

Include background information on the firm and provide detailed information regarding the firm's experience with similar projects. Provide a list of all similar contracts performed in the past (2) number of years, accompanied by at least (3) references (contact persons, firm, telephone number and email address).

Include the total amount invoiced for each listed project, the length of the project, and list of those involved in the project who are also proposed for the subject project named in this solicitation. Failure to provide a list of all similar contracts in the specified period may result in the rejection of the firm's proposal. The evaluation team reserves the right to contact any or all listed references, and to contact other public entities regarding past performance on similar projects.

2.1.3. Section/Tab 3: Financial Information

Review and provide one of the following three (3) financial statement options:

1. Recent audited or reviewed financial statements prepared by an independent certified public accountant (CPA) that shall include, at a minimum, a balance sheet, income statement (i.e., profit/loss statement) and cash flow statement **and**, if the audited or reviewed financial statements were prepared more than six (6) months prior to the issuance of this RFP, the Proposer shall submit its most recent internal financial statements (balance sheet, income statement and cash flow statement or budget with entries reflecting revenues and expenditures from the date of the audited or reviewed financial statements to the end of the most recent financial reporting period (i.e., the quarter or month preceding the issuance date of this RFP)).

OR

2. Recent compiled financial statements prepared by an independent CPA that shall include, at a minimum, a balance sheet, income statement (i.e., profit/loss statement) and cash flow statement **and**, if the compiled financial statements were prepared more than three (3) months prior to the issuance of this RFP, the Proposer shall submit its most recent internal financial statements (balance sheet, income statement and cash flow statement or budget with entries reflecting revenues and expenditures to date), and other evidence of financial stability such as most recently filed income tax return, evidence of a line of credit/loans/other type of financing with statement of amount in use/outstanding balance (e.g., a complete copy commitment letter, loan agreement, billing statement reflecting the line of credit or statement from lender acknowledging the commitment to fund the Proposer's stated financing), personal guaranty with copies of personal income tax filing and statement of net worth or such other evidence that is accurate, reliable and trustworthy regarding the Proposer's financial stability.

OR

3. Include a certified, signed statement from a licensed CPA regularly engaged in the review of the firm's financial information verifying the financial viability of the firm.

All financial information, statements and/or documents provided in response to this solicitation shall be kept confidential provided that EACH PAGE is marked as follows:

“CONFIDENTIAL – DO NOT DISCLOSE EXCEPT FOR THE EXPRESS PURPOSE OF PROPOSAL EVALUATION.”

“**Recent**” shall be defined as financial statements that were prepared within the 12 months preceding the issuance date of this RFP.

Consolidated financial statements of the Proposer’s parent or related corporation/business entity shall not be considered, unless: (1) the Proposer’s actual financial performance for the designated period is separately identified in and/or attached to the consolidated statements, (2) the parent or related corporation/business entity provides the State with a document wherein the parent or related corporation/business entity will be financially responsible for the Proposer’s performance of the contract and the consolidated statement demonstrates the parent or related corporation’s/business entity’s financial ability to perform the contract, financial stability and/or such other financial considerations identified in the evaluation criteria; and/or (3) Proposer provides its own internally prepared financial statements and such other evidence of its own financial stability identified above.

The firm’s failure to provide any of the above-referenced financial statements may result in the proposal being removed from consideration. Proposers are also encouraged to explain any negative financial information, and to provide documentation supporting those explanations and demonstrating the financial strength of the firm.

2.1.4. Section/Tab 4: Project Understanding, Approach and Schedule

Provide a comprehensive narrative, outline, and/or graph demonstrating the firm's understanding and approach to accomplishing the tasks outlined in the Scope of Work section of this RFP. A description of each task and deliverable and the schedule for accomplishing each shall be included.

2.1.5. Section/Tab 5: Team Firm, Experience and Certifications

This section must include the proposed staffing, deployment and firm of personnel to be assigned to this project. The Proposer shall provide information as to the Proposals and experience of all executive, managerial, legal, and professional personnel to be assigned to this project, including resumes citing experience with similar projects and the responsibilities to be assigned to each person. A project-specific firm chart which clearly illustrates the roles, responsibilities, and the reporting relationships of each team member should be included.

2.1.6. Section/Tab 6: Cost

In a separate sealed envelope provide a minimum of *two* (2) complete copies of the Proposal Cost Form and any additional itemized cost breakdown or price schedule. Hourly rates shall be fully burdened to include all costs, all applicable overhead and profit (including lodging, meals, and transportation). Attach any additional pricing details.

2.1.7 Section/Tab 7: Product Requirements Matrix

Fill out the each tab of the product requirement Matrix (Appendix V) answering the ability of the product to meet the described required elements, marking a status code to indicate the capability of the product.

2.1.8 Section/Tab 8: Questionnaire

Answer each of the following questions (1-14) and return with your proposal. Failure to complete and return this tab of the proposal document will be a basis for disqualification. This part of the proposal must include a response to each question.

1. Qualifications and Company Overview

- a) Provide a summary of the company's experience, qualifications, and history supporting fire and emergency services agencies.
- b) Provide a list of fire departments serving metropolitan-sized communities that currently utilize the proposed solution.
- c) Provide a list of current customers that are comparable to the agency in size, population served, call volume, and operational complexity.
- d) Provide a timeline highlighting significant milestones in the company's history.
- e) Provide the company's headquarters and primary business address.
- f) How many employees does the company currently have?
- g) Identify the company's key executives and provide their roles and responsibilities.
- h) How long has the proposed software product been commercially available?
- i) Provide a three-year company outlook and forecast, including information regarding market position, anticipated growth, financial stability, and projected market share.
- j) Describe the company's major strategic initiatives planned for the next three years.
- k) How many customers currently use the proposed product?
- l) What is the company's primary business focus (e.g., Fire, EMS, or both)? Describe the company's experience and level of investment in each area.

2. System and Technical Requirements

- a) Describe the proposed system's technology architecture.
- b) Identify the programming and coding languages used to develop and maintain the system.
- c) Describe the database architecture, including database platform(s), structure, and redundancy.
- d) Describe how the data is encrypted at rest and in transit

- e) Identify the operating systems supported by the system.
- f) Is the proposed solution cloud-based, vendor-hosted, on-premises, or a combination? Describe the hosting model in detail.
- g) Describe all system and network requirements, including recommended and minimum network speeds.
- h) Describe how customers are notified of upcoming system changes, enhancements, releases, and functionality updates.
- i) Describe any hardware requirements for the proposed solution.
- j) Describe how the system integrates with other internal agency systems.
- k) Describe how the system integrates with Computer-Aided Dispatch (CAD) systems.
- l) List all CAD vendors with which the system currently integrates.
- m) Describe how the system integrates with external applications and third-party systems.
- n) Describe the software licensing model, including licensing metrics, user limitations, subscription terms, and any applicable fees.
- o) Describe expected system uptime and availability. Identify all locations where customer data is stored.
- p) Describe the vendor's business continuity and disaster recovery procedures for cloud hosting or cloud vendor outages.
- q) For on-premises deployments, describe the vendor's process for assisting customers during system or infrastructure outages.
- r) Describe how users are added, modified, deactivated, and removed from the system.
- s) Describe the user password reset and account recovery process.
- t) Describe how the system integrates with Microsoft Active Directory (AD) and Microsoft Azure/Entra ID.
- u) Describe how the system interacts with third-party vendor applications.
- v) Describe the support process and responsibilities when an issue involves a third-party vendor application.
- w) What is the typical and guaranteed response time when an issue must be escalated to a third-party vendor?
- x) Describe how photographs, signatures, documents, and other attachments are stored within the system and database.

- y) Describe the user experience and data protection mechanisms when a network connection is lost while a user is working on an incident report, pre-incident plan, or inspection.
 - z) Describe how the system notifies users and administrators about expired or soon-to-expire credentials, certifications, licenses, or other required documentation.
 - aa) Describe how artificial intelligence (AI) has been incorporated into the proposed software.
 - bb) Describe the options and requirements for connecting to the system database using Open Database Connectivity (ODBC).
 - cc) Describe how the system can connect to Microsoft Power BI for reporting and analytics.
-

3. Security

- a) Provide a summary of the proposed system's security architecture, controls, and security practices.
 - b) Describe ownership of all data entered into or generated by the system.
 - c) Describe how customer data is provided to the customer when the customer transitions to another vendor or terminates the contract.
 - d) Describe the hosting architecture, redundancy, disaster recovery capabilities, and off-site backup strategy.
 - e) For cloud-hosted solutions, describe how customers are notified of a confirmed or suspected data breach.
 - f) For cloud-hosted solutions, what is the required and typical timeframe for notifying customers of a data breach?
 - g) Identify who has access to customer data, including vendor employees, contractors, system administrators, and third parties.
 - h) Describe how access to customer data is logged when the data is accessed outside the system's standard user interface.
 - i) Identify the system and security logs that are available to customers.
 - j) Describe how customers can access system, security, audit, and user activity logs.
 - k) Describe how the system supports compliance with applicable state and local data retention requirements.
 - l) Describe how customers can retain data beyond the minimum requirements established by state or local data retention laws.
-

4. Implementation

- a) Provide an overview of the vendor's implementation strategy, methodology, timeline, and process.
 - b) Does the vendor provide customer training during implementation? Describe the training program, delivery methods, duration, and any additional costs.
 - c) Describe how the vendor communicates with customers throughout the implementation process, including project management, status reporting, meetings, and escalation procedures.
 - d) Describe the extent to which customers can configure or customize the software.
 - e) Provide a proposed data migration plan for migrating data from the agency's existing records management system to the proposed platform.
 - f) Describe how the system maintains historical data in National Fire Incident Reporting System (NFIRS) format while supporting new reporting requirements under the National Emergency Response Information System (NERIS).
-

5. Customer Support

- a) What are the vendor's customer support hours? Identify available hours for each support method, including telephone, email, online portal, live chat, and other available methods.
 - b) Describe the customer issue reporting, escalation, tracking, and resolution process, including service-level agreements (SLAs), response times, resolution targets, and guarantees.
 - c) How frequently are system updates and releases deployed?
 - d) Is the system available to users while updates and maintenance are being performed? If not, describe the expected downtime and notification process.
-

6. Pre-Incident Planning

- a) Provide an overview of the system's pre-incident planning capabilities.
- b) Describe how the system integrates with county assessor databases, property records, building department systems, or other online property data sources.
- c) Describe how the system integrates with Esri ArcGIS.
- d) Describe how pre-incident plans can be assigned to stations, apparatus, companies, or individual staff members.
- e) Describe how the system tracks the status of assigned pre-incident plans.
- f) Describe the system's search and query capabilities for pre-incident plan data.
- g) Describe how pre-incident plans are created, assigned, reassigned, and completed.

- h) Describe how company officers can view and track pre-incident plans assigned to them or their company.
 - i) Describe how pre-incident plan information is displayed geographically using GIS maps.
 - j) Describe how the system identifies and notifies staff when pre-incident plans are more than one year old or otherwise due for review.
-

7. Fire Inspections and Fire Prevention

- a) Provide an overview of the system's fire prevention and inspection capabilities.
- b) Describe how the system supports self-inspections, remote inspections, and virtual inspections.
- c) Does the system natively support inspections, permitting, and billing? If so, describe each capability.
- d) Describe the process for creating, scheduling, assigning, and batching inspections.
- e) Describe how the system can create, process, and manage a batch of 5,000 inspections at one time.
- f) Describe how the system interfaces with EnGOV.
- g) Describe how the system interfaces with TCE.
- h) Describe the process for exporting weekly completed inspection data to Microsoft Excel, including the fields that can be exported.
- i) Describe the complete inspection workflow, from inspection creation and assignment through completion, approval, and follow-up.
- j) Describe how inspection schedule cycles are created and maintained.
- k) Describe how inspection schedule cycles can be associated with business classifications or occupancy types.
- l) Describe how users can configure and customize the following:
 - Inspection checklists
 - Codes
 - Fee schedules
 - Forms

8. Incident Reporting

- a) Provide an overview of the system's incident reporting capabilities.
- b) Provide an overview of how fire investigations are initiated, documented, and tracked within the system.
- c) Describe how a Basic Life Support (BLS) agency would use the system to document EMS calls.
- d) Describe the data elements collected in a Patient Care Report (PCR).
- e) Describe the process for completing a medical/sick call.
- f) Describe the process for documenting a cardiac arrest incident.
- g) Describe the process for documenting a multi-vehicle accident involving injuries.
- h) Describe the process for documenting a multi-family structure fire involving exposures.
- i) Describe the process for completing and documenting a fire investigation.
- j) Describe how users can identify incident reports that have not been started, are incomplete, or are awaiting completion.
- k) Describe the Quality Assurance/Quality Improvement (QA/QI) process for incident reports.
- l) Describe how personnel are added to an incident report.
- m) Describe how units and apparatus are added to an incident report.
- n) Describe how equipment used at an incident is documented.
- o) Describe how fields can be designated as mandatory or required.
- p) Describe how custom or user-defined fields are created.
- q) Describe how custom fields can be designated as mandatory or required.
- r) List all CAD vendors with which the incident reporting system integrates.

9. Scheduling and Personnel Management

- a) Provide an overview of the system's scheduling and personnel management capabilities.
- b) Describe how scheduling data flows into and interacts with other modules within the platform.
- c) Describe how staffing rules and minimum staffing requirements are established.
- d) Describe how staffing rules can be overridden, suspended, or stopped when operational circumstances require.
- e) Describe how personnel can be manually assigned to an apparatus or station.

- f) Describe how personnel can be moved to another station or apparatus for part of a shift.
- g) Describe how personnel can be assigned to multiple stations or apparatus throughout the course of a single shift.
- h) Describe the process for requesting and approving leave.
- i) Describe how the system would integrate with the City's enterprise resource planning (ERP) system, including PeopleSoft, for employee time sheets.
- j) Describe how personnel records are initially entered into the system.
- k) Describe how employees can update their own personnel information.
- l) Describe how personnel are assigned to stations.
- m) Describe how personnel are assigned to apparatus.
- n) Describe how historical staffing-level reports can be generated.
- o) Describe the process for retiring or separating an employee from the system.
- p) Describe the process for adding and onboarding a new employee.
- q) Describe the process for hiring and onboarding a large recruit academy class, such as 50 employees.
- r) Describe how the shift dashboard clearly identifies when an apparatus does not meet minimum or required staffing levels.

10. Community Engagement

- a) Provide an overview of the system's community engagement capabilities.
- b) Describe how emergency response agencies can communicate with business and residential constituents through the platform.
- c) Describe the services and functionality included to encourage citizen registration, participation, and engagement.
- d) Describe how a citizen or business owner can view inspection information associated with a specific address.
- e) Describe how a citizen or business owner can view non-EMS incident information associated with a specific address.
- f) Describe how citizens or business owners can subscribe to alerts regarding inspection violations or other compliance issues associated with a business.
- g) Describe how citizens can access public records through the system, including incident listings by address, inspection records by address, and violations associated with an address.

11. Asset and Inventory Management

- a) Provide an overview of the system's asset and inventory management capabilities.
- b) Is asset management natively integrated with the rest of the platform? If so, describe the automation and integration between asset management and other modules.
- c) Describe the system's capabilities for tracking consumable inventory.
- d) Describe the process for adding a gas monitor to the inventory system.
- e) Describe how the system tracks gas monitor testing, calibration, and certification.
- f) Describe how the system tracks gas monitor repairs and maintenance.
- g) Describe how the use of a gas monitor at an incident is documented and associated with the incident.
- h) Describe how hazardous materials (HAZMAT) are tracked within the system.
- i) Describe how the system can generate reports for billing or reimbursement to the state for HAZMAT materials used during an incident.
- j) Describe how inventory item costs are tracked.
- k) Describe how minimum/reorder levels are established and monitored.
- l) Describe how the system notifies users when an item is missing, damaged, broken, expired, or required to be placed out of service.

12. Mobile Application and Artificial Intelligence

- a) Provide an overview of the vendor's mobile application capabilities.
- b) Provide an overview of how artificial intelligence (AI) is currently used within the platform.
- c) Does the vendor provide native mobile applications for both Apple iOS and Android?
- d) List all modules and functionality available through the mobile application.
- e) Does the mobile application provide responder-specific information and functionality? If so, describe the following:
 - a. Dispatch notifications based on selected units or apparatus
 - b. Routing/navigation to the incident
 - c. Notifications regarding updates or changes to an incident
- f) Describe the system's current AI capabilities, including any production functionality and any planned AI enhancements.

- g) Identify which modules currently use or support AI functionality.

13. Incident Command

- a) Provide an overview of the system's incident command capabilities.
- b) Describe how the incident command module supports operations at a structure fire.
- c) Describe how incident command information is shared with personnel operating at the incident.
- d) Describe how the system tracks resources, assignments, personnel, apparatus, and operational activities during an incident.
- e) Describe how incident command information is documented and incorporated into the final incident report.

14. Fire Investigations

- a) Provide an overview of the system's fire investigation capabilities.
- b) Describe how an investigator initiates and completes a fire investigation within the system.
- c) Describe how evidence, photographs, documents, interviews, findings, and other investigative information are captured and associated with an investigation.
- d) Describe how fire investigation data can be searched, reported, exported, and shared.
- e) Describe how fire investigation information is linked to the associated incident report and property/address information.

2.2 RFP Documents

This RFP is comprised of the base RFP document, any attachments, and any addenda released before the contract is awarded. All attachments and addenda released for this RFP in advance of any contract award are incorporated herein by reference.

3 PROPOSAL EVALUATION

3.1 Proposal Evaluation Criteria (Stage 1)

This is not a bid. There will not be a public opening. The proposals received in response to this RFP will be evaluated and ranked by the evaluation committee in accordance with the process and evaluation criteria contained below. Responses will be evaluated in light of the material and substantiating evidence presented in the response and not based on what is inferred. After thoroughly reading and reviewing this RFP, each evaluation committee member shall conduct his or her independent evaluation of the proposals received and grade the responses on their merit in accordance with the evaluation criteria set forth in the following table.

The maximum interview/demonstration points a Proposer can receive is five (5) points. The Proposers selected for interviews/demonstrations under this section will be notified in writing of the date and time. The Proposers' interview/demonstrations shall be based solely upon information provided in each Proposer's original proposal. No new information may be presented.

Criteria	(a) Weight	(b) Score (0-3)	(a) x (b) Weighted Score
Questionnaire Elements (Tab 7)	25		
Product Requirements Matrix (Appendix V)	25		
Corporate Background and Experience	15		
Firm Financial Stability	10		
Project Understanding	10		
Project Approach	5		
Team Firm Experience	5		
Proposed Cost	5		
Total Score (without Interview/Demonstrations)			
Interview/Demonstration (if applicable)	(1-5 points)		
Final Score (with Interview/Demonstrations)			

Score Points

0- Missing or Does Not Meet Expectation 2- Meets Expectation
1- Partially Meets Expectation 3- Exceeds Expectation

Cost Formula: The cost criterion is rated by giving the proposal with the lowest total cost the maximum number of Cost points available. The remaining proposals are rated by applying the following formula:

$$1 - \frac{B - A}{A} \times C = D$$

A—the lowest Proposer's cost.

B—the Proposer's cost being scored.

C—the maximum number of cost points available.

D—Proposer's cost score (points).

Note: If the formula results in a negative number (which will occur when the Offeror's cost is more than twice the lowest cost), zero points shall be assigned.

3.2 Interview/Demonstration (Stage 2)

A short-list of firms may be invited to Stage 2, Interview/Demonstration, step of the evaluation process. Interview/demonstrations are an important aspect of the evaluation

process that offers the City an opportunity to see how the proposer's solution meets the critical components of the RFP.

3.3 Final Selection

Proposals will be evaluated and ranked according to the criteria and weighted values set forth in Section 3.1. Either a final selection for recommendation will be made at this time or the short-list of firms will be invited to participate in Stage 2 of the evaluation process. If Stage 2 is implemented, each firm will be evaluated and assigned a score to determine the best firm for recommendation.

After which negotiations of a contract with the most qualified firm will commence. If negotiations are unsuccessful, the City will then pursue negotiations with the next most qualified firm. All Proposers will be notified of their standing immediately following the City's decision.

The City shall not be bound or in any way obligated until both parties have executed a contract. The City also reserves the right to delay the award of a contract or to not award a contract.

3.4 Notice to Proposers Regarding RFP Terms and Conditions

It shall be the Proposer's responsibility to read the RFP Instructions, the City's contract terms and conditions (within the sample City Service Contract provided in Appendix IV), all relevant exhibits, attachments, and any other components made a part of this RFP and comply with all requirements and specifications herein. Proposers are also responsible for obtaining and complying with all Addenda and other changes that may be issued in connection with this RFP.

3.5 Contract Term

The contract issued by the City to the awarded proposer will define either a completion date by which the services are to be completed and finished, or a term date by which the services will begin and be provided repeatedly over a specific period. The details of the contract term and any options to renew or extend the contract, will be stated in the contract issued by the City. See Appendix IV for a sample-version of the City's contract for services.

4 SCOPE OF SERVICES

Awarded proposer shall provide services, all as set forth in this RFP and more particularly described in this Section 4.

The scope of services shall include but is not limited to the following:

1. System Functionality

Provide an integrated platform supporting incident reporting; pre-incident planning; fire inspections, prevention, and permitting; scheduling and personnel records; training and certification tracking; fire investigations; incident command; community risk reduction and engagement; health and safety; and asset and inventory management.

The system shall support configurable workflows, forms, required fields, approval processes, notifications, and access permissions.

2. Implementation and Configuration

Develop and execute an implementation plan identifying project milestones, schedules, responsibilities, resource needs, and procedures for managing issues. Work with Department and City staff to configure the system to support established business processes and operational requirements. Conduct system testing and user acceptance testing before production deployment and provide transition assistance to maintain continuity of operations.

3. Data Migration and Historical Records

Migrate applicable records and associated attachments from the Department's existing FIREHOUSE/ESO records management environment. Services shall include data mapping, identification of conversion issues, validation, and reconciliation to confirm the completeness and accuracy of migrated records. Preserve access to historical National Fire Incident Reporting System (NFIRS) records and support incident reporting and data submission through the National Emergency Response Information System (NERIS).

4. System Integrations

Provide and configure integrations with Computer-Aided Dispatch (CAD) and applicable City and third-party systems. Integration needs include Microsoft Active Directory or Entra ID, Esri ArcGIS, PeopleSoft, EnGov, TCE, and Microsoft Power BI. Identify supported interfaces, required development, dependencies, and any third-party coordination necessary to implement and maintain each proposed integration.

5. Reporting and Analytics

Provide standard and configurable reports, dashboards, search tools, and data export capabilities supporting operational oversight, administrative reporting, quality assurance, and performance analysis. Authorized staff shall be able to access and analyze current and historical data, including through Microsoft Excel and Power BI.

6. Mobile Access

Provide mobile functionality supporting field activities, including incident documentation, inspections, pre-incident planning, and access to relevant operational information. Identify supported devices and operating systems, functionality available without network connectivity, and procedures for protecting and synchronizing data when connectivity is restored.

7. Security, Availability, and Data Management

Provide role-based access controls, audit logging, data backup, recovery, and business continuity capabilities. Support City data ownership, records retention, and retrieval requirements. Provide procedures for security incident notification and for returning City data and associated attachments in usable formats upon contract termination or transition to another system.

8. Training and Ongoing Support

Provide initial training for system administrators, designated trainers, and end users, together with documentation and training materials. Provide ongoing technical support, software maintenance, updates, and procedures for reporting, escalating, and resolving issues. Establish service levels for system availability and support response, and communicate planned maintenance and changes affecting system functionality.

OPERATING ENVIRONMENT

The Fire Records Management System is intended to serve the City of Raleigh Fire Department. However, the records management system proposed must include capability for handling multiple jurisdictions and multiple agencies.

Figures provided here are annual totals unless otherwise stated.

City of Raleigh Fire Department

Incidents in 2025	61,886
Incidents in 2024	58,166
Estimated Incidents in 2026	63,000
Estimated Incidents in 2027	65,000
Estimated Incidents in 2028	67,000
Number of sworn members	553
Number of fire stations	28
Number of other fire facilities	2
Number of engines	29
Number of ladders	9
Number of rescue units	0
Number of squads	2
Number of heavy rescue units	1
Number of light & air units	2
Number of HazMat Units	5
Number of water rescue units	1
Number of reserve engines	10
Number of reserve trucks	2
Number of arson units	1
Number of other units	2

The City of Raleigh Fire Department use these services for computers and internet:

- Spectrum Business Class Internet service 300M x 20M at most fire stations, other stations have city provided fiber.
- Each station has 3 -5 computers. These are standard Windows 11 mini desktop units.
- MDTs are Dell Rugged 7220-7220 models connected to a Sierra Wireless MP70 in the apparatus using Verizon 4G.
- We are looking to add another Dell Rugged device connected to LTE to start data collection in the field.

APPENDIX I

PROPOSAL COST FORM

The awarded proposer shall perform the services to be performed as set forth in this RFP and more particularly described in Section 4 for a not to exceed total amount of:

\$_____.

Attach proposal cost itemization or breakdown to this Appendix I Proposal Cost Form.

Proposer/Company Name: _____

Authorized Signature _____ Date _____

Signed by: _____
[Type or Print Name]

Title of Signer: _____

APPENDIX II PROPOSER QUESTIONNAIRE

The following questions must be answered, and data given must be clear and comprehensive. If necessary, questions may be answered on separate sheets. The Proposer may submit any additional information desired.

Company Name:		d/b/a (if applicable)	
Street / PO Box:			
City:		State:	Zip:
Phone:		Fax:	E-Mail:
Website (if applicable):			
☐ Sole Proprietor ☐ Partnership ☐ Corporation ☐ Other			
Number of years in business under company's present name:			
Fed Tax ID #:		DUNS #	
Are you registered with the North Carolina Secretary of State to conduct business (if required)? (Check One) YES: ☐ NO: ☐ Not Applicable: ☐			
Are you properly licensed/certified by the Federal and/or State of North Carolina to perform the specified work? YES: ☐ NO: ☐ Not Applicable: ☐ ATTACH COPY OF ALL APPLICABLE LICENSING/CERTIFICATION DOCUMENTS			
Are/will you be properly insured to perform the work? YES: ☐ NO: ☐			
Contact for this Contract:		Title:	
Phone:		Fax:	E-Mail:
Have you ever defaulted or failed on a contract? (If yes, attach details) YES: ☐ NO: ☐			
List at least three (3) references for which you have provided these services (same scope/size) in the past three years - preferably government agencies. Do not include City of Raleigh as a reference to meet the requirement of listing at least (3) references. PROPOSERS ARE RESPONSIBLE FOR SENDING REFERENCE QUESTIONNAIRE (APPENDIX III) TO THEIR REFERENCES.			
1.	Company:		
	Contact Person:	Title:	
	Phone:	Fax:	E-Mail:
Describe Scope of Work:			
2.	Company:		
	Contact Person:	Title:	
	Phone:	Fax:	E-Mail:
Describe Scope of Work:			
3.	Company:		
	Contact Person:	Title:	
	Phone:	Fax:	E-Mail:
Describe Scope of Work:			
4.	Company:		
	Contact Person:	Title:	
	Phone:	Fax:	E-Mail:
Describe Scope of Work:			
5.	Company:		
	Contact Person:	Title:	
	Phone:	Fax:	E-Mail:
Describe Scope of Work:			
The undersigned swears to the truth and accuracy of all statements and answers contained herein:			
Authorized Signature:		Date:	

APPENDIX III
REFERENCE QUESTIONNAIRE
(Instructions)

274-533 Records Management System

The City of Raleigh, as a part of the RFP, requires proposing companies to submit a minimum of three (3) business references as required within this document. The purpose of the references is to document the experience of the proposer relevant to the scope of services and assist in the evaluation process.

- The Proposer is required to send the reference form (the following two pages) to each business reference listed on Proposer Questionnaire.
- The business reference, in turn, is requested to submit the Reference Form directly to the City of Raleigh Point of Contact identified on the Reference Questionnaire form for inclusion in the evaluation process.
- The form and information provided will become a part of the submitted proposal. The business reference may be contacted for validation of the response.
- It is the Proposer's responsibility to verify their references have been received by the City of Raleigh Point of Contact by the date indicated on the reference form.

APPENDIX III

REFERENCE QUESTIONNAIRE FORM

274-533 Records Management System

(Name of Business Requesting Reference)

This form is being submitted to your company for completion as a business reference for the company listed above.

This form is to be returned to the City of Raleigh, **Daniel Clark**, via email to ***RFDContracts@raleighnc.gov*** no later than **5:00 p.m. EST, November 20th, 2026** and **MUST NOT** be returned to the company requesting the reference.

For questions or concerns regarding this form, please contact the City of Raleigh, Point of Contact above.

Company Providing Reference

Contact Name and Title/Position

Contact Telephone Number

Contact Email Address

Questions:

1. In what capacity have you worked with this company in the past? If the company was under a contract, please acknowledge and explain briefly whether or not the contract was successful.

Comments:

2. How would you rate this company's knowledge and expertise?

☐ 3= Excellent

☐ 2= Satisfactory

☐ 1= Unsatisfactory

☐ 0= Unacceptable

Comments:

3. How would you rate the company's flexibility relative to changes in the scope and timelines?

☐ 3= Excellent

☐ 2= Satisfactory

☐ 1= Unsatisfactory

☐ 0= Unacceptable

Comments:

4. What is your level of satisfaction with hard-copy materials, e.g. reports, logs, etc. produced by the company?
☐ 3= Excellent ☐ 2= Satisfactory ☐ 1= Unsatisfactory ☐ 0= Unacceptable

Comments:

5. How would you rate the dynamics/interaction between the company and your staff?
☐ 3= Excellent ☐ 2= Satisfactory ☐ 1= Unsatisfactory ☐ 0= Unacceptable

Comments:

6. Who were the company's principle representatives involved in providing your service and how would you rate them individually? Would you comment on the skills, knowledge, behaviors or other factors on which you based the rating?

(3= Excellent; 2= Satisfactory; 1= Unsatisfactory; 0= Unacceptable)

Name: _____	Rating: _____
Name: _____	Rating: _____
Name: _____	Rating: _____
Name: _____	Rating: _____

Comments:

7. With which aspect(s) of this company's services are you most satisfied?

Comments:

8. With which aspect(s) of this company's services are you least satisfied?

Comments:

9. Would you recommend this company's services to your organization again?

Comments:

APPENDIX IV

SAMPLE CONTRACT

NORTH CAROLINA
WAKE COUNTY

AGREEMENT FOR SOFTWARE AS A SERVICE

THIS SOFTWARE AS A SERVICE AGREEMENT (“Agreement”) is entered into by and between the City of Raleigh, a North Carolina municipal corporation, (hereinafter, the “City”), and [Keywords], a [add vendor’s state of incorporation] [add vendor’s corporate structure (Corporation, LLC, Partnership, etc.)] (hereinafter, the “Contractor”). This Contract is effective as of the date of the City’s signature below (“Effective Date”).

Now, in consideration of sums to be paid by the City to the Contractor, and other good and valuable consideration, the Contractor and City do contract and agree as follows:

1. Description of Services

Contractor hereby grants to the City a nonexclusive, worldwide license to access and use [add number of copies or seats] licenses of Contractor’s software titled [add name of software] version [add version of software] as may be updated (the “Software”), a more detailed description of which is contained in **Exhibit A** and incorporated herein by reference. Contractor’s provision and licensing of the Software under this Agreement, and the scope of work or additional description contained in **Exhibit A**, shall be referred to as the “Services”.

[All the services related to the software that will or can be provided by the Contractor (like training, monitoring, or cloud storage) and are intended to be provided by the Contractor, must be stated and described on Exhibit A.]

2. Definitions

- 2.1. **“Documentation” means all materials provided by the vendor that describe the features, functionality, performance standards, service levels, or specifications of the SaaS product, including user guides, service descriptions, and technical manuals. Documentation establishes the baseline for service expectations and shall be attached to this Agreement. The vendor may not materially reduce the described services or functionality without prior written approval from the City.**
- 2.2. **“City Data” means (a) any information, documents, data, instruments, records, or reports created or possessed by the City and provided to Contractor, (b) information or data provided to Contractor from the City’s residents, customers, employees, agents, or other contractors by virtue of this Agreement, and (c) any information or data derived from the processing, storage, or analysis of any other City Data provided to Contractor.**
- 2.3. **“Acceptance” means the written approval from the City of the services or work received by the City for the consideration as provided in Section 10, below.**

- 2.4. “Commencement Date” means the date to which the Contractor shall begin the work and services, but no earlier than the last of the parties to sign.
- 2.5. “Completion Date” means the date by which the work and services must be complete.
- 2.6. “Deliverables” means the tasks, reports, information, documents and other items, which the Contractor is required to complete and deliver to the City in accordance to Exhibit A.
- 2.7. “Effective Date” means the date of the last of the parties to sign.
- 2.8. “Expiration Date” means the date by which the term or period of time the work and services are to be provided ends. And the date by which work, and services can no longer be provided by the Contractor.
- 2.9. “Notice to Proceed” is City’s written notice and authorization for the Contractor to begin the work and services in accordance to Exhibit A.
- 2.10. “Project” means the work or services as defined in Exhibit A to be performed by the Contractor for the consideration as provided in Section 10, below.
- 2.11. “Services” (or “Work”) means the work or services including any deliverables which the Contractor is to perform for City as set forth in Exhibit A.
- 2.12. “Communications” is any public or City employee facing information presented in channels such as, but not limited to, a website, mobile applications, social media, printed materials, vehicles, billboards, and videos.

3. Time and Period of Performance

- 3.1. Initial Term. The term of this Agreement shall be for *[add number of years/quarters/months of the services-the written number followed by the numeral in parenthesis]* from the Effective Date, unless earlier terminated by the parties (“Initial Term”).
- 3.2. Renewal Term. On or before the expiration of the Initial Term, and then on or before the expiration of any Renewal Term as defined herein, this Agreement may be renewed by City for up to *[add number of renewal terms]* additional one-year terms (“Renewal Term”). Each Renewal Term shall run for one (1) year from the expiration of the previous Initial or Renewal Term and shall be subject to the same terms and conditions as the Initial Term unless earlier terminated or amended in writing by the parties.

[Note: In certain situations that warrant the change, a department may request a change to the renewal term language above for “automatic renewals” from IT Client Services during planning and approval phases of contract development.]

4. Compensation

The City shall pay the Contractor \$ *[add dollar amount]* for the Services to be performed hereunder. The total amount payable to the Contractor by the City under this Agreement shall not exceed \$ *[add dollar amount]* unless changed by a duly authorized amendment.

5. Invoices

- 5.1. Contractor shall submit invoice(s) to the CITY stating the nature and quantity of the Services performed and accompanied by proper supporting documentation as the CITY may require. The Contractor may submit invoices using ONE of the following options:**

5.1.1. The Contractor shall email all invoices to: accountspayable@raleighnc.gov; or

5.1.2. The Contractor shall mail all invoices to:

City of Raleigh
Accounts/Payable
P.O. Box 590
Raleigh, NC 27602-0590

5.1.3. Each invoice must contain the following information:

- 5.1.3.1. Contractor name
- 5.1.3.2. Invoice Number
- 5.1.3.3. Current and Valid City of Raleigh Purchase Order Number
- 5.1.3.4. City of Raleigh Contract Number
- 5.1.3.5. Description of Services Performed
- 5.1.3.6. Date Services were performed
- 5.1.3.7. Address to which the Payment Should Be Sent

5.2. CITY will pay accurate, undisputed, properly submitted invoices within thirty (30) days after the CITY's Contract Manager has approved each invoice. An undisputed, properly submitted invoice is defined as an invoice that indicates only the Services that have been satisfactorily completed and accepted by the CITY pursuant to the terms of this Contract.

5.3. As a condition of payment, the Contractor must submit an invoice to the CITY no later than sixty (60) days after the applicable Services have been provided, access to licensed software has been activated, or deliverables have been made available for use—whichever is most applicable to the nature of the work. Any Services or deliverables not invoiced within this 60-day period shall be deemed waived, and the CITY shall have no obligation to pay for them. Exceptions may be granted in writing at the CITY's sole discretion.

5.4. The Contractor waives the right to payment for any work and services that have not been invoiced to the CITY within 60 days after such work and services were performed.

5.5. All invoices must include the following Purchase Order Number: _____. Invoices submitted without the correct purchase order number will result in delayed payment. New Purchase Order numbers will be generated as needed for annual encumbrances.

6. Quality Of Services

6.1. The Software provided under this Agreement shall be furnished in a stable and "general availability" format, to the reasonable satisfaction of the City, and shall materially conform to the Documentation, and all prevailing industry and professional standards.

6.2. If this Agreement relates to sensitive data: Contractor shall assure that all support, if any, is performed by appropriately qualified and licensed personnel, eligible to work in the United States, who shall exercise the degree of skill, and possess the credentials and knowledge normally possessed by members of their profession in good standing in the community.

7. Time is of the Essence

The parties acknowledge and agree that time is of the essence with respect to Contractor's performance of the Services under this Agreement and that Contractor will respond within five (5) business days.

Contractor shall deliver services and Deliverables on or before the assigned dates in the Exhibits for City's consideration of acceptance.

8. Termination

- 8.1. Termination for Convenience.** The City may terminate this Agreement at any time by providing thirty (30) days written notice to the Contractor ("Termination for Convenience"). In the event of a Termination for Convenience, all undisputed fees already paid by the City during the current Initial or Renewal Term shall be non-refundable and are forfeited. Contractor shall be entitled to receive just and equitable compensation for the Services provided to the City as of the date of termination. Notwithstanding the foregoing, in no event will the total amount due to Contractor under this section exceed the total amount due Contractor under this Agreement (or any subsequent Amendments). In the event of termination, the Contractor will be required to return and destroy the City's data with 5 business days.
- 8.2. Termination for Cause without Opportunity to Cure.** The City may terminate the Contract if the Contract violates or fails to perform any covenant, provision, obligation, term or condition contained in the Contract, provided that, unless otherwise stated in the Contract, such failure or violation shall not be cause for termination if both of the following conditions are satisfied:
- 8.2.1. Such default is reasonably susceptible to cure; and,
 - 8.2.2. Contractor cures such default within thirty (30) days of receipt of written notice of default from the City.
 - 8.2.3. Contractor shall cease performance immediately upon receipt of such notice. In the event of a Termination for Cause all previously paid fees will be refunded to the City on a pro-rata basis. The pro-rated refund will be provided starting from the date Contractor receives notice of the City's Termination for Cause.
 - 8.2.4. Notwithstanding the above, the Contractor shall not be relieved of liability to the City for damages sustained by the City by virtue of any breach of this Agreement, and the City may withhold any payment due to the Contractor for the purpose of setoff until such time as the City can determine the exact amount of damages due the City because of the breach.

9. Remedies

- 9.1. Right to Cover.** If the Contractor fails to meet the Completion Date or resolution time set forth in this Contract (including the exhibits), the City may take any of the following actions with or without terminating this Contract, and in addition to and without limiting any other remedies it may have:
- 9.1.1. Employ such means as it may deem advisable and appropriate to perform itself or obtain the Services from a third party until the matter is resolved and the Contractor is again able to resume performance under this Contract; and,
 - 9.1.2. Deduct any and all expenses incurred by the City in obtaining or performing the Services from any money then due or to become due the Contractor and, should the CITY's cost of obtaining or performing the services exceed the amount due the Contractor, collect the amount due from the Contractor.
- 9.2. Right to Withhold Payment.** If the Contractor breaches any provision of this Contract, the CITY shall have a right to withhold all payments due to the Contractor until such breach has been fully cured.
- 9.3. Specific Performance and Injunctive Relief.** The Contractor agrees that monetary damages are not an adequate remedy for the Contractor failure to provide the Services as required by this Contract, nor could monetary damages be the equivalent of the performance of such obligation. The City has the right to seek specific performance and injunctive relief from a court of competent jurisdiction should the Contractor breach, or attempt to breach, the Contract.

Accordingly, the Contractor hereby consents to an order granting specific performance of such obligations of the Contractor in a court of competent jurisdiction within the State of North Carolina. The Contractor further consents to the City obtaining injunctive relief (including a temporary restraining order) to assure performance in the event the Contractor breaches the Contract.

- 9.4. **Setoff.** The City shall be entitled to setoff and deduct from any amounts owed to the Contractor pursuant to this Contract all damages and expenses incurred or reasonably anticipated as a result of the Contractor's breach of this Contract.
- 9.5. **Other Remedies.** Upon breach of this Contract, the City may seek all legal and equitable remedies to which it is entitled. The remedies set forth herein shall be deemed cumulative and not exclusive and may be exercised successively or concurrently, in addition to any other available remedy.

10. Indemnification

- 10.1. Except to the extent caused by the sole negligence or willful misconduct of the City, the Contractor shall indemnify, defend, and hold harmless the City, including its officers, agents, and employees, from liability of any kind, including all claims, costs (including defense), and losses accruing or resulting to any other person, firm, or corporation furnishing or supplying work, services, materials, or supplies in connection with the performance of this Agreement, and from any and all claims, costs (including defense) and losses accruing or resulting to any person, firm, or corporation that may be injured or damaged by the Contractor in the performance of this Agreement. This representation and warranty shall survive the termination or expiration of this Agreement.
- 10.2. The Contractor shall indemnify, defend, and hold harmless the City, its officers, agents and employees from liability of any kind, including claims, costs (including defense) and expenses, on account of any copyrighted material, patented or unpatented invention, articles, device, or appliance manufactured or used in the performance of this Agreement.
- 10.3. The Contractor shall indemnify, defend, and hold the Customer harmless from any damages, costs, or claims arising from a security breach, unauthorized disclosure, or failure to adhere to the cybersecurity and privacy obligations outlined in this Agreement.

11. Insurance

- 11.1. **Additional Insured.** Contractor agrees to endorse the City as an additional insured on the Commercial General Liability Policies, Auto Liability Policies, and Umbrella Liability Policies if being used to meet the standard of the General Liability and Automobile Liability. The Additional Insured shall read as follows:
City of Raleigh is named additional insured as their interest may appear.
- 11.2. **Certificate of Insurance.** Contractor shall provide to the City a Certificate of Insurance evidencing that all coverages, limits and endorsements required herein are maintained and in full force and effect. Said Certificates of Insurance shall provide a minimum thirty (30) day endeavor to notify duty by Contractor's insurer, when available. If Contractor receives a non-renewal or cancellation notice from an insurance carrier affording coverage required herein, or receives notice that coverage no longer complies with the insurance requirements herein, Contractor agrees to notify the City within five (5) business days with a copy of the non-renewal or cancellation notice, or written specifics as to which coverage is no longer in compliance. The Certificate Holder address should read:
City of Raleigh, Post Office Box 590, Raleigh, NC 27602-0590

11.3. Minimum Coverage Requirements. Contractor agrees to maintain at all times during the life of this Agreement, on a primary basis and at its sole expense, the following coverages and limits. The requirements contained herein, as well as City's review or acceptance of insurance maintained by Contractor is not intended to and shall not in any manner limit or qualify the liabilities or obligations assumed by Contractor under this Agreement. All insurance companies must be authorized to do business in North Carolina and be acceptable to the City of Raleigh's Risk Manager.

11.3.1. Commercial General Liability – Combined single limit of no less than \$1,000,000 per occurrence and \$2,000,000 aggregate. Coverage shall not contain any endorsement(s) excluding nor limiting Product/Completed Operations, Contractual Liability, or Cross Liability.

11.3.2. Automobile Liability – Limits of no less than \$1,000,000 Combined Single Limit. Coverage shall include liability for Owned, Non-Owned, and Hired automobiles. In the event that Contractor does not own automobiles, Contractor agrees to maintain coverage for Hired and Non-Owned Auto Liability, which may be satisfied by way of endorsement to the Commercial General Liability policy or separate Auto Liability policy. Automobile coverage is only necessary if vehicles are used in the provision of Services under this Agreement or are brought on City property.

11.3.3. Cyber Liability Insurance – Including first-party and third-party coverage, with limits no less than \$1,000,000 per occurrence and \$3,000,000 in the aggregate for all claims each policy year. The policy maintained to satisfy this provision shall not contain terms limiting or excluding coverage for ransomware, malware, intellectual property, or data breach claims.

11.3.4. Worker's Compensation & Employer's Liability – Contractor agrees to maintain Worker's Compensation Insurance in accordance with North Carolina General Statute Chapter 97 with statutory limits and employer's liability of no less than \$1,000,000 per occurrence.

11.3.5. Umbrella or Excess Liability – Contractor may satisfy the minimum liability limits required above under an Umbrella or Excess Liability policy, provided that if the Umbrella or Excess Liability policy is being used to satisfy the Cyber Liability policy requirement above, then said policy shall not contain terms limiting or excluding coverage for ransomware, malware, intellectual property, or data breach claims. There is no minimum Per Occurrence limit of liability under the Umbrella or Excess Liability, however, the Annual Aggregate limits shall not be less than the highest 'Per Occurrence' limit for required policies. Contractor agrees to endorse City of Raleigh as an 'Additional Insured' on the Umbrella or Excess Liability unless the Certificate of Insurance states the Umbrella or Excess Liability provides coverage on a 'Follow-Form' basis.

11.3.6. Professional Liability – Limits of no less than \$1,000,000 for each claim and \$3,000,000 aggregate coverage limit. A Professional Liability policy is only required if Support is being provided as part of the Services under this Agreement.

12. Communications

12.1. If communications to the public and/or City employees are required as part of the Contractor's scope of work under this Contract, then the Contractor shall work with the City in the development of a communications plan ("Communications Plan") that must first be approved by the City in writing before any such communications are delivered to the public and/or City employees.

12.1.1. For the avoidance of doubt, this Section does not apply to communications with City employees who are authorized users of the Services. The City's current brand and communications guidelines are incorporated into this Contract by reference.

12.2. Communications Plan Approval. Any public marketing materials, or public outreach from the Contractor related to the service or effort under this Contract that references the City of Raleigh, must first be reviewed and approved by the City's Communications Department. This is to ensure that the Communications Plan: (i) complies with the City's brand and communication guidelines; (ii) integrates with the City's other communications channels and digital strategy; (iii) meets accessibility guidelines; and (iv) conforms to communications best practices with respect to general user experience.

12.2.1. For the avoidance of doubt, this section does not apply to communications within the application to [Keywords] authorized users, existing [Keywords] documentation or help articles or resources, or content and communication is that is broadly available to all [Keywords] customers without naming specific customers.

12.3. Accessibility Requirements: All HTML web materials made available to the general public conform with World Wide Web Consortium's (W3C) Web Content Accessibility Guidelines (WCAG), version 2.1, level AA.

12.3.1. Languages: HTML content made available for the general public Webpages that are public will be available for use with publicly available translation tools (e.g. G-translate).

12.4. Advertising. Contractor shall not use the existence of this Contract, or the name of the City of Raleigh, as part of any advertising without the prior written approval of the Customer. This includes granting and rescinding permission - which shall be provided at the discretion of the Communications Director of the Customer.

12.5. Trademarks. Any trademarks and service marks ("Trademarks") adopted by the Contractor to identify the Services. Documentation and other products and services, belong to the Contractor. Nothing herein grants, or shall be construed to grant, to Customer any rights to such Trademarks.

13. Trademark

13.1. Acknowledgement of City Brand and Tree Logo Ownership and Restrictions. The City of Raleigh has developed proprietary branding (the "City Brand") centered around the Raleigh tree mark logo (the "Tree Logo"). The City's exclusive rights and ownership in and to the Tree Logo are protected under trademark and copyright, including U.S. Copyright Reg. No. VAu1-322-896, N.C. State Trademark Registration Reg. No. T-23070 and Federal Trademark Registration Reg. No. 5,629,347, as well as under other federal and state laws.

- 13.1.1. Contractor acknowledges and understands that the City is not conferring any license to Contractor under this Agreement to use or depict the Tree Logo or other aspects of the City Brand. Contractor shall not make any use or depiction of the Tree Logo or other aspects of the City Brand without the prior express written approval of the City. In this regard, should any materials being produced by Contractor for the City under this Agreement contemplate use or depiction of the Tree Logo, including, but not limited to, printed materials, digital media, signage and/or display materials, Contractor shall proceed under the auspices and direction of the City's Communications Department and shall comply with all guidelines and restrictions governing use or depiction of the Tree Logo.

14. Cybersecurity and Privacy

- 14.1. As is necessary to comply with Section 22 below, City Data does not include this Agreement or any internal information, documents, data, instruments, records, or reports created by and originating solely with Contractor or its licensors that, while pertaining to this Agreement, do not otherwise contain City Data as defined above.
- 14.1.1. As between the City and Contractor only, City Data shall remain the exclusive property of the City, and the City retains the right, title, and interest in all City Data unless specifically relinquished in writing. "Authorized Persons" means City employees or agents. "Contracted Persons" means Contractor's employees who are currently engaged in the provision of Services under this Agreement, and Contractor's subcontractors who comply with Section 14.6 below.
- 14.2. Permissible Use of City Data. Contractor may use any City Data in its possession only as is necessary to provide the Services under this Agreement or to comply with any applicable law or court order. Contractor otherwise prevents and shall contractually prohibit the access, copying, or use of City Data in Contractor's possession by any third-party, Contractor's other customers, or Contractor's subcontractors, provided that Contractor may disclose City Data to Contractor's subcontractors as is necessary to provide the Services under this Agreement only if:
- 14.2.1. Contractor's contract with such subcontractor contains terms reasonably consistent with this Agreement; and,
- 14.2.2. Such subcontractor has acknowledged in writing, either independently or in its contract with Contractor, that the City Data shall remain the exclusive property of the City and that the subcontractor will maintain an industry standard information security program.
- 14.3. Data Security & Protection. The Contractor shall implement and maintain appropriate administrative, technical, logical, and physical safeguards to ensure the security, confidentiality, integrity, and availability of Customer Data and prevent anyone other than authorized City employees or designees from monitoring, using, or gaining access to City Data.
- 14.3.1. The Contractor will employ industry best practices and regulatory requirements for cybersecurity and data in the collection, transmission, storage and access of City Data and will make all reasonable attempts to prevent the loss, corruption, or unauthorized

alteration of City Data. These measures shall be consistent and comply with the following frameworks:

14.3.1.1. NIST Cybersecurity Framework (CSF) 2.0

14.3.1.2. CIS Controls (latest version)

14.3.1.3. ISO/IEC 27001 and 27701 (if applicable to privacy and security management)

14.3.2. Data Storage, Transmission, and Access. The Contractor will store, collect, and process City data solely on servers physically located within the continental United States of America in a climate-controlled environment which includes: (i) fire and security hazard detection and suppression systems, and (ii) network and electrical redundancy systems, for instance automatic fail-over standby generators or backup Uninterruptable Power Supply.

14.3.3. Utilize, at a minimum and if applicable, Multi-Factor Authentication, updated network security certificates, Transport Layer Security v1.2 or later, or other like transmission security, end-to-end and at rest encryption using AES-256 at a minimum, in accordance with the Federal Information Processing Standard Publication 140 as applicable and as amended from time to time, and other similar security measures commonly utilized in the storage, transmission, and access of data.

14.4. Data Security and Privacy Documentation. Contractor shall provide the City a copy of the following documents, or attestation as outlined, within three business days of the City's request for such documents.

14.4.1. Attestation of the industry standard compliance framework(s) used as the basis for the creation of the Contractor's security-related documents and artifacts:

14.4.1.1. Data Classification policy;

14.4.1.2. Privacy policy;

14.4.1.3. Security Training and Awareness policy;

14.4.1.4. Incident response plan;

14.4.2. The Contractor shall attest that the Incident Response Plan follows industry standard practices, such as those that at a minimum are consistent with the contingency planning requirements of NIST Special Publication 800-61 Rev. 2, NIST Special Publication 800-53 Rev. 5, and the incident response requirements of NIST Special Publication 800-53 Rev. 4, as those standards may be amended. Contractor will adhere to each of its established policies to the extent such policies do not conflict with this Agreement or violate any laws, rules, or regulations.

14.4.2.1. If Contractor does not possess or maintain one of the foregoing policies, Contractor shall notify the City of this deficiency prior to the execution of this Agreement:

- 14.4.2.1.1. Mobile Device Management policy;
- 14.4.2.1.2. Disaster Recovery plan;
- 14.4.2.1.3. Business Continuity plan;
- 14.4.2.1.4. Audit and testing schedules;
- 14.4.2.1.5. Security requirements for third-party business partners and contractors;
- 14.4.2.1.6. Background Check policy;
- 14.4.2.1.7. Summary of all previous data breaches; and
- 14.4.2.1.8. Any other relevant information regarding security policies or procedures.

14.5. Data Privacy & Compliance. The Contractor shall comply with the latest version of all applicable federal, state, and local laws, including but not limited to:

- 14.5.1. North Carolina Identity Theft Protection Act, N.C.G.S. § 75-60 et seq;
- 14.5.2. The Payment Card Industry Data Security Standard (PCI-DSS) (if applicable);
- 14.5.3. The General Data Protection Regulation (GDPR) (if applicable);
- 14.5.4. The Health Insurance Portability and Accountability Act (HIPAA) (if applicable);
- 14.5.5. The Criminal Justice Information Services (CJIS) Security Policy (if applicable).

14.6. Subcontractors & Third-Party Service Providers. If the Contractor engages any subcontractors or third-party services or service providers that process Customer Data, the Contractor shall:

- 14.6.1. Ensure subcontractors and third-party services or service providers adhere to the same security and privacy requirements set forth in this agreement;
- 14.6.2. Conduct security assessments of subcontractors and third-party services or service providers before engaging their services;
- 14.6.3. Provide the City with an annual updated list of subcontractors and third-party services or service providers and attest that these entities are continuing to adhere to the same security and privacy requirements set forth in this agreement;
- 14.6.4. Remain fully liable for any actions or omissions of subcontractors and third-party services or service providers related to Customer Data security.

- 14.7. Notification of Security Incident: Contractor shall promptly notify the City in writing of any actual or suspected security incident, data breach, unauthorized access, or other cybersecurity event that compromises City Data, systems, or services. The notification must occur:
- 14.7.1. Within 24 hours of detecting a confirmed breach affecting City Data;
 - 14.7.2. Within 48 hours of detecting a suspected security incident requiring further investigation.
 - 14.7.3. This does not include pings and other broadcast attacks on Contractor's firewall, port scans, unsuccessful log-on attempts, denials of service, and any combination of the above, so long as no such incident results in a data security incident related to City Data. The initial notification shall be sent to the City's Chief Information Security Officer (CISO) and include:
 - 14.7.3.1. A summary of the incident and affected data;
 - 14.7.3.2. The date, time, and nature of the incident;
 - 14.7.3.3. Steps taken to contain and mitigate the breach;
 - 14.7.3.4. A timeline for corrective action and root cause analysis.
- 14.8. Security Investigation. The Contractor must cooperate with the City's request to investigate and resolve the incident in a timely manner, promptly implement necessary remedial measures, and document all responsive actions and measures related to the security incident to include all post-incident review or after-action reports and actions that will be taken to prevent a reoccurrence of the data breach. If a Data Security Incident occurs in which City Data is accessed, viewed, copied, altered, or deleted, Contractor must, at its sole cost and expense:
- 14.8.1. Investigate, identify, and remediate the root cause of the incident;
 - 14.8.2. Bear any costs associated with the investigation and resolution of the incident;
 - 14.8.3. Prevent the public disclosure of the Data Security Incident except as required by law or with the City's permission;
 - 14.8.4. If applicable, pay the reasonable costs to City for sending notification to individuals whose personal information is City Data, as required by the North Carolina Identity Theft Protection Act, N.C.G.S. § 75-60 et seq.;
 - 14.8.5. If applicable, engage the services of a credit monitoring or identity protection service;
 - 14.8.6. If applicable, publish a website or toll-free number and call center for affected individuals as required by North Carolina and federal law;
 - 14.8.7. Complete all remedial and corrective actions in accordance with information security industry best practices; and

- 14.8.8. Provide City within 10 business days the written findings of any investigation and access to remedial measures as they may be relevant to end users or consumers of Contractor's SaaS products.
- 14.9. Business Continuity and Disaster Recovery Plan: Contractor shall establish and maintain a comprehensive business continuity and disaster recovery plan that covers the restoration of both technology and business operations in the event of an unplanned event. Upon the City's request, the Contractor shall provide the City access to Contractor's business continuity and disaster recovery plans for the City's review, including the frequency and last utilization of any such plan. The Contractor agrees to review and update its BC/DR plan on at least an annual basis.
- 14.9.1. The planning process for the business continuity and disaster recovery plan shall include risk analysis, business impact analysis, and recovery strategies for different scenarios to include cyberattacks, geographic/regional events, pandemics, and natural disasters (e.g., tornado, hurricane, flooding, fire, power outage). The business continuity and disaster recovery plan shall cover, among other things, Contractor's operations associated with its activities under the Agreement. Contractor shall utilize geographically diverse data centers to ensure availability in the event of a disaster or Data Security Incident.
- 14.10. Data Retrieval. For the duration of this Agreement and for forty-five (45) days following this Agreement's expiration or termination, Contractor shall provide the City with a method for accessing, retrieving, and downloading all City Data in a nonproprietary, industry standard format, and shall assist the City in accessing, retrieving, or downloading all City Data held by any of Contractor's subcontractors who qualify as Contracted Persons, to the extent that such City Data has not been removed or otherwise already deleted by Contracted Persons, City, or its Authorized Persons.
- 14.11. Data Return at the City's request. Contractor shall:
- 14.11.1. Return all City Data to the City in a nonproprietary, industry standard machine-readable format within forty-five (45) days of such a request, except as required by applicable law or to defend itself in any legal action, proceeding or investigation, including all data held by the Contractor's subcontractors;
- 14.11.2. Permanently delete all Customer Data from Contractor and subcontractor systems, unless otherwise required by law, and not retain any City Data following the above forty-five (45) day period and must remove, delete, purge, overwrite or otherwise render City Data inaccessible.
- 14.11.3. Upon the removal, deletion, or purging of such data, the Contractor will ensure that destruction of the data was performed securely and in accordance with the latest revision of NIST Special Publication 800-88;
- 14.11.4. Contractor will provide to the City an attestation of destruction once data has been destroyed.
- 14.12. Data Deletion. City may, in its sole discretion and upon written notice to Contractor, instruct Contractor to delete City Data instead of returning such City Data. Contractor will not delete

any City data without prior written consent from the City and not before a copy of such data has been provided to the City. Notwithstanding the foregoing, Contractor will have no obligation to maintain City Data more than forty-five (45) days after the effective date of termination of this Agreement.

- 14.12.1. For the purposes of this Subsection 13.3 and as is necessary to comply with Section 14.8 below, City Data does not include this Agreement or any internal information, documents, data, instruments, records, or reports created by and originating solely with Contractor or its licensees that, while pertaining to this Agreement, do not otherwise contain City Data as defined above.
- 14.13. Data Backups: The Contractor shall implement and maintain a comprehensive data backup strategy to ensure the security, integrity, and availability of City Data. At a minimum, the backup solution shall:
 - 14.13.1. Include automated, regularly scheduled backups of all City Data;
 - 14.13.2. Maintain at least one offsite or geographically separate backup to prevent data loss due to localized incidents;
 - 14.13.3. Utilize encrypted backups both in transit and at rest;
 - 14.13.4. Support versioning and recovery of previous data states to protect against accidental deletions or corruption.
- 14.14. Backup Frequency and Retention. The Contractor shall adhere to the following backup schedule and retention policy:
 - 14.14.1. Backup Frequency: Critical data (e.g., databases, configurations, customer records) shall be backed up at least once every 24 hour; Full system backups shall occur weekly.
 - 14.14.2. Retention Policy: Daily backups shall be retained for at least 30 days; Weekly backups shall be retained for at least 90 days; Monthly backups shall be retained for at least one year, unless otherwise agreed upon.
- 14.15. Disaster Recovery and Restoration. The Contractor shall implement a disaster recovery plan that ensures timely data restoration in the event of a cybersecurity incident (e.g., ransomware, data breach); a system failure or hardware malfunction; a natural disaster or force majeure event. The Contractor shall:
 - 14.15.1. Ensure that data restoration can be completed within 3 hours of an outage (Recovery Time Objective – RTO);
 - 14.15.2. Guarantee that no more than 1 hour of data loss occurs in the worst-case scenario (Recovery Point Objective – RPO);
 - 14.15.3. Test backup and recovery processes at least quarterly and provide reports upon request.

14.16. Customer Access to Backups. The Contractor shall provide the City with Access to self-service backup recovery options (if applicable);

14.16.1. The ability to request a full data export in a machine-readable format;

14.16.2. A process to verify the integrity of backed-up data upon request.

14.17. Data Ownership and Compliance. All backup copies of City Data shall remain the sole property of the City. The Contractor shall ensure that backup and recovery procedures comply with all applicable data protection laws and regulations (e.g., NIST CSF, GDPR, HIPAA, ISO 27001).

14.18. Security and Encryption. All backup data shall be encrypted using industry-standard encryption protocols (e.g., AES-256). Backups shall be protected against unauthorized access through strict access controls. Any third-party backup service providers used must comply with the same security and compliance requirements as the Contractor.

14.19. Backup Failure and Notification. If a backup failure occurs, the Contractor shall notify the City within 24 hours and provide:

14.19.1. A detailed report of the failure, including root cause analysis.

14.19.2. Immediate steps taken to remediate the issue.

14.19.3. An updated timeline for ensuring proper backup restoration.

14.20. Security Audits & Assessments. The City agrees to work closely and collaboratively with the Contractor in the event an audit of records is required. The Contractor and the City shall mutually agree on the scope and schedule of the audit to ensure minimal disruption to operations. Both parties commit to transparent communication and cooperation to successfully complete the audit in compliance with applicable regulations and contractual obligations. The Contractor shall:

14.20.1. Maintain detailed security logs and monitoring systems to detect unauthorized access or anomalous activity;

14.20.2. Conduct annual third-party security audits (e.g., SOC 2 Type II, ISO 27001, or equivalent) and provide results to the Customer upon request;

14.20.3. Allow the Customer to perform security assessments, penetration testing, or compliance audits upon reasonable notice.

14.21. Ongoing Security Improvements: The Contractor shall continuously monitor industry trends, emerging threats, and regulatory updates to ensure security measures remain effective. Any material changes to security protocols must be communicated to the Customer in a timely manner.

15. Amendments

This Contract may be amended only by written agreement of the parties executed by their authorized representatives.

16. **Applicability of North Carolina Public Records Law**

Notwithstanding any other provisions of this Agreement, this Agreement and all materials submitted to the City by the Contractor are subject to the public records laws of the State of North Carolina and it is the responsibility of the Contractor to properly designate materials that may be protected from disclosure as trade secrets under North Carolina law as such and in the form required by law prior to the submission of such materials to the City. Contractor understands and agrees that the City may take any and all actions necessary to comply with federal, state, and local laws and/or judicial orders and such actions will not constitute a breach of the terms of this Agreement. To the extent that any other provisions of this Agreement conflict with this paragraph, the provisions of this Section shall control.

17. **Assignment**

This Agreement may not be assigned without the express written consent of the City.

18. **City Property**

The Contractor shall be responsible for the proper custody and care of any property furnished or purchased by the City and provided to Contractor for use in connection with the performance of this Agreement and will reimburse the City for the replacement value of its loss or damage.

19. **Companies Boycotting Israel Divestment Act Certification**

Contractor certifies that it has not been designated by the North Carolina State Treasurer as a company engaged in the boycott of Israel pursuant to N.C.G.S. § 147-86.81.

20. **Compliance with Laws**

Contractor understands and agrees that the City may take any and all actions necessary to comply with federal, state, and local laws and judicial orders and such actions will not constitute a breach of the terms of this Agreement. To the extent that any other provisions of this Agreement conflict with this paragraph, the provisions of this Section shall control.

21. **Compliance with Safety Standards**

Contractor shall comply with all laws, ordinances, codes, rules, regulations, safety standards and licensing requirements that are applicable to the conduct of its business, including those of federal, state, and local agencies having jurisdiction and authority. Contractor shall familiarize itself with any building regulations applicable to any City worksite where Contractor is performing Services.

22. **Confidentiality**

Contractor shall protect the confidentiality of any and all individuals and will not discuss, transmit, or narrate in any form other information, medical or otherwise, received in the course of providing services hereunder except as authorized by the individual, a legally responsible person for the individual, or as otherwise permitted or required by law.

23. **Contracting Authority**

Contractor represents and warrants that it has full authority to enter into this Agreement and that each party has obtained all necessary consents in connection with the execution and delivery of this Agreement. The persons executing this Agreement on behalf of the parties warrant that they are duly authorized to execute this Agreement on behalf of their party. This Agreement constitutes a valid and legally binding obligation on each party, enforceable in accordance with its terms.

24. Entire Agreement / Incorporation of Documents

This Agreement, and any documents incorporated herein by reference, constitute the complete Agreement between the parties and supersedes all prior oral or written statements or agreements between the parties concerning the subject matter of this Agreement. In cases of conflict between this Agreement and any of the above-incorporated documents, the terms of this Agreement shall prevail.

25. E-Verify

Contractor shall comply with E-Verify, the federal E-Verify program operated by the United States Department of Homeland Security and other federal agencies, or any successor or equivalent program used to verify the work authorization of newly hired employees pursuant to federal law and as in accordance with N.C.G.S. § 64-25 et seq. In addition, to the best of Contractor's knowledge, any subcontractor employed by Contractor as a part of this Agreement shall be in compliance with the requirements of E-Verify and N.C.G.S. § 64-25 et seq.

26. Force Majeure

Except as otherwise provided in any environmental laws, rules, regulations or ordinances applicable to the parties and the services performed under this Agreement, neither party shall be deemed to be in default of its obligations hereunder if and so long as it is prevented from performing such obligations by an act of war, hostile foreign actions, nuclear explosion, earthquake, hurricane, tornado, controlling governmental order issued pursuant to a public health crisis, or other catastrophic natural event or act of God. Either party to the Agreement must take reasonable measures and implement reasonable protections when a weather event otherwise defined as a force majeure event is forecast to be eligible to be excused from the performance otherwise required under this Agreement by this provision.

27. Governing Law

Both the City and the Contractor, for themselves and their respective agents, officials, employees, and servants, hereby acknowledge and agree that this Contract shall be governed and construed in accordance with the applicable laws of the State of North Carolina, without regard to its choice of law provisions, and no other.

The proper, sole, and exclusive venue for any civil action arising out of or in any way related to this Contract shall be the federal or state courts sitting in Wake County, North Carolina.

28. Health Insurance Portability and Accountability Act (HIPAA)

In the event that the Services include the collection, processing, storage, or handling of Protected Health Information as that phrase is defined within Contractor shall comply with any and all laws and subsequent amendment thereof relating to the privacy and security of healthcare information, including the Health Insurance Portability and Accountability Act of 1996 (45 C.F.R. Parts 160, 162 & 164 and 42 C.F.R. Part 2), as further expanded by the Health Information Technology for Economic and Clinical Health Act, which was adopted as a part of the American Recovery and Reinvestment Act of 2009, and any subsequent modification thereof. Pursuant to 45 C.F.R. § 164.506, the parties may share an individual's Protected Health Information for the purposes of treatment, payment, or health care operations without the individual's consent.

29. Immunity

Nothing in this Agreement shall be construed to mandate purchase of insurance by the City pursuant to N.C.G.S. § 160A-485 or in any way waive the City's defense of sovereign or governmental immunity from any cause of action alleged or brought against any party for any reason if otherwise available as a matter of law. No officer, agent or employee of the City shall be subject to any personal liability by reason of the execution of this Agreement or any other

documents related to the transactions contemplated hereby. Such officers, agents, or employees shall be deemed to execute this Agreement in their official capacities only, and not in their individual capacities. This Section shall not relieve any such officer, agent, or employee from the performance of any official duty provided by law.

30. Iran Divestment Act Certification

Contractor certifies that, as of the date listed below, it is not on the Final Divestment List as created by the State Treasurer pursuant to N.C.G.S. § 147-86.55, et seq. In compliance with the intent of the Iran Divestment Act and N.C.G.S. § 147-86.60, Contractor shall not utilize in the performance of the Agreement any subcontractor that is identified on the Final Divestment List.

31. Non-Appropriation of Funds

The City of Raleigh is a governmental entity, and this Agreement's validity is based upon the availability of public funding under the authority of its statutory mandate. In the event that funds are not available and not appropriated to the program specified in this Agreement, then this Agreement shall automatically expire without penalty to either party. In the event of a legal change in the City's statutory authority, mandate, and mandated functions which adversely affects the authority to continue performing obligations under this Agreement, then this Agreement shall automatically expire without penalty to either party.

32. Non-Discrimination

To the extent permitted by North Carolina law, the parties for themselves, their agents, officials, directors, officers, members, representatives, employees, and contractors agree not to discriminate in any manner or in any form based on actual or perceived age, mental or physical disability, sex, religion, creed, race, color, sexual orientation, gender identity or expression, familial or marital status, economic status, veteran status or national origin in connection with this Agreement or its performance.

The parties agree to conform with the provisions and intent of Raleigh City Code § 4-1004 in all matters related to this Agreement. This provision is incorporated into the Agreement for the benefit of the City of Raleigh and its residents and may be enforced by an action for specific performance, injunctive relief, or any other remedy available at law or equity. This section shall be binding on the successors and assigns of all parties with reference to the Agreement.

33. Notices

All notices, requests for payment, or other communications arising under this Agreement shall be in writing, shall include an auditable receipt, and sent to the following individuals:

City of Raleigh

Attn:

Title:

Address 1: P.O. Box 590

Address 2: Raleigh, NC 27602

Telephone:

Email:

Contractor

Attn:

Title:

Address 1:

Address 2:

Telephone:

Email:

All notices required or permitted under this Agreement shall be sufficient if sent by personal delivery, electronic mail, or certified mail. The parties may update their addresses for notice from time to time by notice to the other party in conformance with this Section. Except as otherwise provided in this Agreement, notice is effective only upon receipt by the receiving party.

34. Relationship of the Parties

The Contractor shall be considered an independent contractor and as such shall be wholly responsible for the work to be performed and for the supervision of its employees. Nothing herein is intended or will be construed to establish any agency, partnership, or joint venture. Contractor represents that it has, or will secure at its own expense, all personnel required in performing the Services under this Agreement. Such employees shall not be employees of or have any individual contractual relationship with the City.

35. Right to Audit and Access to Records

The City may conduct an audit of any services performed and fees paid subject to this Agreement. The City or its designee may perform such an audit throughout the Term of the Agreement and for three (3) years after termination thereof or longer if otherwise required by law. The Contractor and its agents shall maintain all internal books, documents, papers, accounting records, contract records and such other evidence as may be appropriate to substantiate costs incurred under this Agreement. "Records" shall be defined as data of every kind and character, including but not limited to books, documents, papers, accounting records, contract documents, information, and materials that, in the City's sole discretion, relate to matters, rights, duties or obligations of this Agreement. Records and employees shall be available during normal business hours upon advanced written notice. Electronic mail shall constitute written notice for purposes of this section. The City or its designee shall have the right to: (i) review and copy records; (ii) interview current and former employees; (iii) conduct such other investigation to verify compliance with Agreement terms; and (iv) conduct such other investigation to substantiate costs incurred by this Agreement. The Contractor shall provide the City or its designee reasonable access to facilities and adequate and appropriate workspace for the conduct of audits. The rights established under this section shall survive the termination of the Agreement, and shall not be deleted, circumvented, limited, confined, or restricted by contract or any other section, clause, addendum, attachment, or the subsequent amendment of this Agreement. The Contractor shall reimburse the City for any overcharges identified by the audit within ninety (90) days of written notice of the City's findings. Contractor shall, upon request, provide any records associated with this engagement to the North Carolina State Auditor that are necessary to comply with the provisions of N.C.G.S. § 147-64.7.

36. Severability

To the extent permitted by applicable law, the parties hereby waive any provision of law that would render any clause of this Agreement invalid or otherwise unenforceable in any respect. In the event that a provision of this Agreement is held to be invalid or otherwise unenforceable, such provision will be interpreted to fulfill its intended purpose to the maximum extent permitted by applicable law, and the remaining provisions of this Agreement will continue in full force and effect.

37. Third-Party Beneficiary

This Agreement is not intended for the benefit of any third party. The rights and obligations contained herein belong exclusively to the parties hereto and shall not confer any rights or remedies upon any person or entity other than the parties hereto.

38. Public Records Obligations; Trade Secrets

Notwithstanding any other provisions of this Agreement, this Agreement and all materials submitted to the City by the Contractor are subject to the public records laws of the State of North Carolina and it is the responsibility of the Contractor to properly designate materials that may be protected from disclosure as trade secrets under North Carolina law as such and in the form required by law prior to the submission of such materials to the City. Regardless of what Contractor may label as a trade secret, determination as to whether it is or is not entitled to protection will be determined by the City, in its sole discretion, in accordance with N.C.G.S. § 132-1.2 and any other applicable law.

39. Survival

The provisions of this Agreement related to intellectual property, the City's public records obligations, confidentiality, the right to audit, City Data, indemnification, and insurance survive the termination or expiration of this Agreement.

The remainder of this page remains blank intentionally.

IN WITNESS WHEREOF, the parties have executed this Agreement by digital signature, under seal, on the respective dates below, and this Agreement shall be effective upon the date of the City's signature (the "Effective Date") or as of the Effective Date set forth on page one of this Agreement.

CONTRACTOR:

[Keywords]

By:

Signature (SEAL)

Name

Title

Date of Signature

CITY:

CITY OF RALEIGH
a North Carolina municipal corporation

By:

Signature

Name

Choose an item.

Title

Choose an item.

Department

Date of Signature

ATTEST:

Signature

Name

Title

ATTEST:

_____(SEAL)
City Clerk (or designee)

This instrument has been pre-audited in the manner required by the Local Government Budget and Fiscal Control Act.

Chief Financial Officer (or designee)

City of Raleigh Contract Number xxxxxxxxxx

Appendix V - Product Requirements Matrix

DIRECTIONS

Using the table below, indicate the ability of the product to meet the described required elements. Using the the following "status code" criteria, indicate the capability of each item in the "Capability" column:

E - Requirement is fully and completely met by proposed system and can be demonstrated in the proposed software package.

M - Requirement will be provided by proposed modifications to the base software package in the total price proposed. These modifications will be maintained in the base software package in future releases of the software package.

O - Requirement will be provided by a standard option. The cost of these options must be provided in the cost section of the proposal.

X - Requirement is not being proposed.

For items needing comments or explanation, indicate using the "Vendor Comments/Explanation" column. In the event additional space is required for additional comments or explanation, use a separate sheet to further describe the method in which the proposed records system meets the specific requirement, making sure to reference the associated element number.

Failure to complete all tabs and return this section of the RFP will be a basis for disqualification. This section is to be returned on the original forms provided; in no case shall the requirements be retyped or altered in any way from those provided within.

Spec ID	Description of Requirement	Availability	Vendor Comments/Explanation
GR-1	System is cloud-based.	Select from Drop Down List	
GR-2	All interfaces are cloud-based.	Select from Drop Down List	
GR-3	All interfaces are accessible with customers user account.	Select from Drop Down List	
GR-4	All data is hosted within the United States.	Select from Drop Down List	
GR-5	Database is in its own instance.	Select from Drop Down List	
GR-6	Database is encrypted.	Select from Drop Down List	
GR-7	The ability for customers to access or download a copy of the database schema	Select from Drop Down List	
GR-8	Have an on-premises copy of the database that is synced with cloud solution	Select from Drop Down List	
GR-9	Administrators can define roles and permissions through the user interface.	Select from Drop Down List	
	Administrators can limit access to different modules with the system(ie can have access to NFRIS but no access to fire inspections).	Select from Drop Down List	
GR-10	The software supports a data-sharing capability to allow other agencies who use the solution to easily share data between accounts.	Select from Drop Down List	
GR-11	The software is mobile responsive and can be accessed on any browser on any device.	Select from Drop Down List	
GR-12	iOS and Android applications at not additional cost.	Select from Drop Down List	
GR-13	Regular system upgrades with new functionality are deployed.	Select from Drop Down List	
GR-14	Upgrades, maintenance and support are included.	Select from Drop Down List	
GR-15	The software is compatible with ArcGIS and Google Maps.	Select from Drop Down List	
GR-16	The software can export data to be used with ArcGIS and Google Maps.	Select from Drop Down List	
GR-17	The software offers easy account-specific customization.	Select from Drop Down List	
GR-18	The ability to import data from different formats into different modules (NFIRS reports, NERIS reports,Inventory Data, etc).	Select from Drop Down List	
GR-19	The ability to export data in different formats (text, csv, excel,PFD, SQL, SQL to SQL).	Select from Drop Down List	
GR-20	The software allows users to tab through fields to complete forms.	Select from Drop Down List	
GR-21	The software saves data when user tabs or move to another form.	Select from Drop Down List	
GR-22	The software has the ability to track changes to all fields in the system.	Select from Drop Down List	
GR-23	The software integrates with Microsoft's AD and Microsoft Azure	Select from Drop Down List	
GR-24	The software has single sign On (SSO) ability	Select from Drop Down List	
		Select from Drop Down List	
GR-25	Is the software in escrow? (if the company goes bankrupt the cutomers obtain all the code to make the system run)	Select from Drop Down List	
GR-26	The system has the ability to track subpoena requests and the data provide for that request	Select from Drop Down List	
GR-27	The system has the ability to track all items associated accreditation (CFAI)	Select from Drop Down List	
GR-28	The system has the ability to provide reports for accreditation (CFAI)	Select from Drop Down List	
GR-29	The system has a dashboard that provide your status on accreditation (CFAI)	Select from Drop Down List	
GR-30	The system should have a separate daily test sute(production data is bumped into a testing site daily)	Select from Drop Down List	
GR-31	The ssytem shoud jhave a 30 day test site.(productiono data is dumped into a separate testing site every 30 days)	Select from Drop Down List	
GR-32	The System allows ODBC connection to the production database	Select from Drop Down List	
GR-33	The System allows ODBC connectionf from the database to Power BI	Select from Drop Down List	
GR-34		Select from Drop Down List	

Spec ID	Description of Requirement	Availability	Vendor Comments
IR-1	Incident reporting integrates seamlessly with Comptuer Aided Dispatch(CAD) vendor.	Select from Drop Down List	
IR-2	CAD import is it own module.	Select from Drop Down List	
IR-3	CAD import has user permissions.	Select from Drop Down List	
IR-4	CAD import fields can be updated by customers at anytime without vendor assistance.	Select from Drop Down List	
IR-5	CAD import allows fields to be added to the import process without vendor assistance.	Select from Drop Down List	
IR-6	CAD import allows customers to to change when the import happens.	Select from Drop Down List	
IR-7	CAD import allows customers to select date range for one time run import(dueto possible missed incidents).	Select from Drop Down List	
IR-8	The system can import CAD data when the incident is closed.	Select from Drop Down List	
IR-9	The system can import CAD data live as the incident is happening.	Select from Drop Down List	
IR-10	Users can change all data entered by CAD.	Select from Drop Down List	
IR-11	The system datatime stamps all activity by CAD import.	Select from Drop Down List	
IR-12	Vendor appears on both the NFIRS/NERIS and NEMSIS vendor sites as approved. Vendor agrees to update incident reporting to meet new standards as NFIRS/NERIS and NEMSIS evolve in a timely manner.	Select from Drop Down List	
IR-13	Incident Report meets the NFIRS 5.0 standard for historical data and NERIS for 2026 and future.	Select from Drop Down List	
IR-14	Incident Report directly connect to NERIS and includes North Carolina requirements.	Select from Drop Down List	
IR-15	Data collection for Incident Reports can be customized to determine what data points are requested.	Select from Drop Down List	
IR-16	Incident Report meets the NEMSIS standard.	Select from Drop Down List	
IR-17	Incident Report for EMS are contained in a separate tables.	Select from Drop Down List	
IR-18	Patient data is contained in a separate tables and HIPPA rules are applied.	Select from Drop Down List	
IR-19	Data collection for EMS Incident Reports can be customized to determine what data points are requested.	Select from Drop Down List	
IR-20	Incident Report that are not part of the NFIRS export can be exported according to state-specified EMS rules and schematron.	Select from Drop Down List	
IR-21	Incident reports are available for use with iOS, Windows, and Android devices.	Select from Drop Down List	
IR-22	The incident report works in all major internet browsers, including Chrome, Edge, Safari, and Firefox.	Select from Drop Down List	
IR-23			
IR-24	The incident historical report is one report meeting NFIRS and NEMSIS requirements. Users do not need to fill out two different run forms. The system is dynamic based upon data supplied by the user to drive completion.	Select from Drop Down List	
IR-25	The incident report is one report meeting NERIS requirements	Select from Drop Down List	
IR-26	The incident report has the ability to add equipment used from the inventoru module to an incident.	Select from Drop Down List	
IR-27	The incident report exports to billing software or company with all signatures and attachments.	Select from Drop Down List	
IR-28	The incident report has a full audit trail from creation of report.	Select from Drop Down List	
IR-29	The audit trail of incidents contains all original and changed values along with username and datetime stamp.	Select from Drop Down List	
IR-30	The audit trail contains the name of users who print records at any time.	Select from Drop Down List	
IR-31	Printing of ePCR or NFIRS/NERIS can be limited by user permissions.	Select from Drop Down List	
IR-32	Printing of ePCR or NFIRS/NERIS are printed in standard formats of NRIFS and PCR.	Select from Drop Down List	
IR-33	Printing of ePCR or NFIRS/NERIScan be printed to PDF.	Select from Drop Down List	
IR-34	Printing of ePCR or NFIRS/NERIS can be printed to local printer attached to computer.	Select from Drop Down List	
IR-35	Users can print ePCR or NFIRS/NERIS data separately.	Select from Drop Down List	
IR-36	ePCR data complies with HIPAA.	Select from Drop Down List	
IR-37	The system has permissions to limit access to NFIRS/NERIS data.	Select from Drop Down List	
IR-38	The system has permissions to limit access to fields within the NFIRS/NERIS data.	Select from Drop Down List	
IR-39	The system has permissions to limit access to ePCR data.	Select from Drop Down List	
IR-40	The system has permissions to limit access to fields within the ePCR data.	Select from Drop Down List	
IR-41	The incident report allows for multiple users to supply needed information.	Select from Drop Down List	
IR-42	The incident report allows for live signature capture.	Select from Drop Down List	
IR-43	The incident report allows for unlimited signatures.	Select from Drop Down List	
IR-44	The incident report allows the record to be locked(no edits)	Select from Drop Down List	
IR-45	Locking incident report are not automatic.	Select from Drop Down List	
IR-46	Locking incident report can be set by user.	Select from Drop Down List	
IR-47	A locked incident can be unlocked based on permissions. The act of locking and unlocking incident reports are logged as part of the audit trail for the incident report.	Select from Drop Down List	
IR-48	Audit records for locked incident reports will include username and datetime stamp.	Select from Drop Down List	
IR-49	Signatures allow for language translations.	Select from Drop Down List	
IR-50	The officer in charge can sign the incident report.	Select from Drop Down List	
IR-51	Incident reports can be saved and accessed later for completion.	Select from Drop Down List	
IR-52	The system has an easy way for users to locate records that are incomplete.	Select from Drop Down List	
IR-53	System provides statuses on each incident report.	Select from Drop Down List	
IR-54	The status of the report can be changed by users based upon permission level	Select from Drop Down List	
IR-55	Data must be shared between modules of the system to eliminate redundant information. As an example, if the address's pre-incident value is known, the data is pulled into the incident report without user intervention.	Select from Drop Down List	
IR-56	Required fields can be added to enhance local data collection.	Select from Drop Down List	
IR-57	Picklist can be modified to meet local standards.	Select from Drop Down List	
IR-58	Plus-One codes can be used locally to enhance data collection.	Select from Drop Down List	
IR-59	Incident reporting has the NFIRS/NERIS dataset available.	Select from Drop Down List	
IR-60	Incident reporting has the ability to export data to NFIRS/NERIS.	Select from Drop Down List	
IR-61	Incident reporting has exposure tracking of all employees for both medical and fire reasons.	Select from Drop Down List	
IR-62	The system integrates with all major cardiac monitors, including Philips, Zoll, and Stryker.	Select from Drop Down List	
IR-63	Integration with cardiac monitors is done through the cloud	Select from Drop Down List	
IR-64	Integration with cardiac monitors is done through USB/IR from a device	Select from Drop Down List	
IR-65	The incident report allows users to merge existing patients and contacts of occupancies into the report	Select from Drop Down List	
IR-66	All data collected via the incident is statistically available.	Select from Drop Down List	
IR-67	The system allows for the creation of unlimited custom fields.	Select from Drop Down List	
IR-68	The incident form is dynamic, displaying only needed fields to reduce clicks and scrolling by the user.	Select from Drop Down List	
IR-69	The system integrates with scheduling platforms to eliminate the need to add personnel to incident reports.	Select from Drop Down List	
IR-70	Incident reporting easily returns incorrect reports to users for correction.	Select from Drop Down List	
IR-71	Incident reports have an easy-to-read flow chart of vitals and treatments.	Select from Drop Down List	
IR-72	Incident Report flow is intuitive and matches the chronology of an incident - response, scene, actions, information, investigation, wrap-up.	Select from Drop Down List	
IR-73	The system allows for connectivity with local EMS and hospital software to provide seamless transfer of information.	Select from Drop Down List	
IR-74	The system allows for transfer of care and HER to local EMS in real-time.	Select from Drop Down List	
IR-75	The system allows for patient outcomes to be reported back.	Select from Drop Down List	
IR-76	The system allows for the ability to chart patient care with appcalbe fields(procedures, medications, affected area)	Select from Drop Down List	
IR-77	The system allows for EMS Q/QI modules to flag specific calls, fields for review.	Select from Drop Down List	
IR-78	The system allows for customizalbe forms within charting to allow for extra infomration or special studies.	Select from Drop Down List	
IR-79	The system allows for customizalbe reports for trends and data on patient reportable fields.	Select from Drop Down List	
IR-80	The system has a data portal for active data monitoring to identify trends.	Select from Drop Down List	
IR-81	The system allows for staffing from the staffing module to be pulled into an incident report	Select from Drop Down List	

IR-82 The system allows for units that were disaptched to be pulled in from CAD vendor
IR-83 The system allows to pull updated from a CAD vendor

Select from Drop Down List
Select from Drop Down List

Spec ID	Description of Requirement	Availability	Vendor Comments
FI-1	Fire Investigation has the ability to pull CAD data into a fire investigation report	Select from Drop Down List	
FI-2	Fire Investigation can be imported from the NERIS/NFRIS module	Select from Drop Down List	
FI-3	Fire Incident data in the fire investigation report can be modified(all fields)	Select from Drop Down List	
FI-4	Fire Investigation need to have property loss data	Select from Drop Down List	
FI-5	Fire Investigation report need to contain weather conditions that are pulled from the internet	Select from Drop Down List	
FI-6	Fire Investigation report need to contain weather conditions that can be updated by investigator	Select from Drop Down List	
FI-7	Fire Investigation report need to have the ability to have unlimited people involved	Select from Drop Down List	
FI-8	Fire Investigation report need to have the ability to collect personal information of all people involved	Select from Drop Down List	
FI-9	Fire Investigation report need to have the ability to document observations	Select from Drop Down List	
FI-10	Fire Investigation report need to have the ability to track evidence	Select from Drop Down List	
FI-11	Fire Investigation report need to have the ability for chain of custody	Select from Drop Down List	
FI-12	Fire Investigation report need to have the ability for unlimited hypothesis	Select from Drop Down List	
FI-13	Fire Investigation report need to have the ability for unlimited narratives	Select from Drop Down List	
FI-14	Fire Investigation report need to have the ability for unlimited attachments	Select from Drop Down List	
FI-15	Fire Investigation report need to have the ability to tie associated records to the fire investigation report	Select from Drop Down List	
	Fire Investigation report need to have the ability to document unlimited activities that the investigator performed at the scene	Select from Drop Down List	
FI-16	Limit the ability of who can print	Select from Drop Down List	
FI-17	Limit the ability of who can access the module	Select from Drop Down List	
FI-18	Add custom fields to fire investigation module	Select from Drop Down List	
FI-19	The ability to print the custom fields on a report	Select from Drop Down List	
FI-20	Print a report that meets NFPA 921 form standard	Select from Drop Down List	
FI-21			

Spec ID	Description of Requirement	Availability	Vendor Comments
SP-1	There is a shift dashboard with the ability to show specific information for users including upcoming assignments, call shifts and announcements.	Select from Drop Down List	
SP-2	The software inclues a 'My Shifts' calendar for personnel to see shifts.	Select from Drop Down List	
SP-3	Personnel can mark their availability on a central calendar.	Select from Drop Down List	
SP-4	The software includes a 'drag and drop' shift board to visualize assignments and vacancies.	Select from Drop Down List	
SP-5	Users can change the shift board view from one to seven days.	Select from Drop Down List	
SP-6	The shift board can be quickly filtered, including by shifts.	Select from Drop Down List	
SP-7	The tool offers vacancy recommendations based on ranks and availability.	Select from Drop Down List	
SP-8	The software pre-fills base shift/rotation and assignments for employees.	Select from Drop Down List	
SP-9	The software has the ability to limit the amount of hours staff can do callback.	Select from Drop Down List	
SP-10	The software has the ability to select staff based number of hours worked and certification to fill open positions.	Select from Drop Down List	
SP-11	Automated call shift functionality exists.	Select from Drop Down List	
SP-12	Call shifts by SMS are available.	Select from Drop Down List	
SP-13	Call shifts by email are available.	Select from Drop Down List	
SP-14	Call shifts by phone call are available.	Select from Drop Down List	
SP-15	Call shift history and audit log is available.	Select from Drop Down List	
SP-16	The software offers messaging functionality to all individuals.	Select from Drop Down List	
SP-17	Targeted messaging to pre-configure groups is available.	Select from Drop Down List	
SP-18	Messaging by SMS is available.	Select from Drop Down List	
SP-19	Messaging by email is available.	Select from Drop Down List	
SP-20	Messaging history and audit log are available.	Select from Drop Down List	
SP-21	Employees can make shift-trade requests.	Select from Drop Down List	
SP-22	Employees can review shift-trade requests.	Select from Drop Down List	
SP-23	A shift-trade history and audit log are available.	Select from Drop Down List	
SP-24	A shift trade register to view owed, earned and balance hours is available.	Select from Drop Down List	
SP-25	Employees can make time-off requests through a time-off module.	Select from Drop Down List	
SP-26	Admins can review time-off requests.	Select from Drop Down List	
SP-27	A time-off history and audit log is available.	Select from Drop Down List	
SP-28	Admins can create, edit, and manage assignments.	Select from Drop Down List	
SP-29	Admins can create, edit, and manage ranks.	Select from Drop Down List	
SP-30	Admins can create, edit and manage groups.	Select from Drop Down List	
SP-31	Admins can create, edit and manage shifts.	Select from Drop Down List	
SP-32	Admins can create, edit, and manage work types.	Select from Drop Down List	
SP-33	Admins can create, edit and manage time-off types.	Select from Drop Down List	
SP-34	The system stores personnel-related information and admins can easily search and filter a personnel list.	Select from Drop Down List	
SP-35	The Software has unlimted staffing rules.	Select from Drop Down List	
SP-36	The software has the ability to change staffing rules on the fly.	Select from Drop Down List	
SP-37	Users with permission have the ability to disable minimum staffing rules.	Select from Drop Down List	
SP-38	Users with permission have the ability to manually add/remove staff from the schedule.	Select from Drop Down List	
SP-39	The Software has the ability to track promotion(dates and locations).	Select from Drop Down List	
SP-40	The Software has the ability to track station and unit locations of staff as their primary assignment.	Select from Drop Down List	
SP-41	The Software has the ability to track station and unit locations of staff as their callback assignments.	Select from Drop Down List	
SP-42	The Software has the ability to track personnel data and track chagnes to:(home address, DOB,hire date, adjused hire date, end of service date, rank, status, location,FDID number,age, contact,qualification, certifications, education level, track injuies and vechile accidents, track activies personnel was invoiced with).	Select from Drop Down List	
SP-43	The Software can limit user access to personal records and schdueling based on user permission.	Select from Drop Down List	
SP-44	The Software has the ability to track discipline issues.	Select from Drop Down List	
SP-45	The Software has the ability to use AI to assist with minuium staffing.	Select from Drop Down List	

Spec ID	Description of Requirement	Availability	Vendor Comments
FI-1	User-customizable checklists and inspection types are included.	Select from Drop Down List	
FI-2	The software has the ability to have different checklists for different inspection types.	Select from Drop Down List	
FI-3	Codes are tied to inspection checklist items, allowing for automatic creation of violation upon item failure.	Select from Drop Down List	
FI-4	Customizable checklist item responses are included.	Select from Drop Down List	
FI-5	Pre-planning and mapping are integrated while completing inspection.	Select from Drop Down List	
FI-6	Software has the ability to modify occupancy information during inspection.	Select from Drop Down List	
FI-7	Software has the ability to modify contact information during inspection.	Select from Drop Down List	
FI-8	Software has the ability to assign inspections to users, teams, apparatus, and stations.	Select from Drop Down List	
FI-9	Software has the ability to add remarks for a specific violation.	Select from Drop Down List	
FI-10	Users can add photos / attachments for specific violations.	Select from Drop Down List	
FI-11	Users can duplicate violations on the fly.	Select from Drop Down List	
FI-12	Users can search all codes and add ad-hoc violations on the fly.	Select from Drop Down List	
FI-13	Users can view current AND historic violations during the inspection.	Select from Drop Down List	
FI-14	The software can auto-generate an inspection report.	Select from Drop Down List	
FI-15	Customizable inspection reports are available.	Select from Drop Down List	
FI-16	Users can set an automated reminder to schedule re-inspection if failures exist.	Select from Drop Down List	
FI-17	Users can send inspection reports automatically to inspection contacts.	Select from Drop Down List	
FI-18	The software automatically groups past violations on re-inspection for easy resolution.	Select from Drop Down List	
FI-19	The software has virtual Inspection functionality with camera and location sharing during inspection.	Select from Drop Down List	
FI-20	An inspection timer with the ability to manually modify is included.	Select from Drop Down List	
FI-21	A searchable list of all violations is included.	Select from Drop Down List	
FI-22	An easy way to view violation history across re-inspections exists.	Select from Drop Down List	
FI-23	Fees and invoicing into the inspection are integrated.	Select from Drop Down List	
FI-24	The software includes integrated permitting functionality into the inspection.	Select from Drop Down List	
FI-25	Permits can be printed at the time of the inspection is completed.	Select from Drop Down List	
FI-26	A code organizer for managing agency-specific fire and building codes, code research and searching is included.	Select from Drop Down List	
FI-27	The tool is a fully responsive web inspections app for use on any device.	Select from Drop Down List	
FI-28	An iPad inspections app for offline inspection functionality is available.	Select from Drop Down List	
FI-29	Users can record plan review activities against permits.	Select from Drop Down List	
FI-30	Users can add and modify custom fee schedules.	Select from Drop Down List	
FI-31	Is there a QC process in your system? If so will it automatically email the officer that completed the report	Select from Drop Down List	
FI-32	The ability to share data with ESRI	Select from Drop Down List	
FI-33	Is this software capable of building queries and saving them for future use	Select from Drop Down List	
FI-34	Does this software have built in analytics	Select from Drop Down List	
FI-35	Can I select the email from the inspection record and it automatically attach the inspection report?	Select from Drop Down List	
FI-36	Can the system accept photos and attachments?	Select from Drop Down List	
FI-37	Are you able to create a mapped route for daily inspection schedule?	Select from Drop Down List	
FI-38	Can the system accept payments?	Select from Drop Down List	
FI-39	Can the user batch over 5,000 inspections at a time?	Select from Drop Down List	
FI-40	Does the system integrate with EnerGov?	Select from Drop Down List	
FI-41	Does the system integrate with Bryer's compliance engine?	Select from Drop Down List	

Spec ID	Description of Requirement	Availability	Vendor Comments
PI-1	Connectors to County Assessor site, Building Department and GIS for automated pre-plans on every structure	Select from Drop Down List	
PI-2	The software includes geospatial pre-plan mapping with drag and drop NFPA-standard map markers.	Select from Drop Down List	
PI-3	The software includes hazardous material mapping and collection with a searchable ERG field.	Select from Drop Down List	
PI-4	The software includes the ability to add custom map markers through the user interface.	Select from Drop Down List	
PI-5	Map markers are related to occupancy ID.	Select from Drop Down List	
PI-6	The software has the ability to add annotations including text, lines, shapes and measurements.	Select from Drop Down List	
PI-7	The software has the ability to modify map marker locations while in Google street view.	Select from Drop Down List	
PI-8	Users can easily add attachments and photos to an occupancy.	Select from Drop Down List	
PI-9	Users can easily add attachments and photos to a specific map marker.	Select from Drop Down List	
PI-10	Pre-Plan standards and custom forms for data collection in the field are available on any device.	Select from Drop Down List	
PI-11	The software has easy-to use high-rise/multi-level pre-incident planning for both data collection and visualization, including the ability add/remove/edit levels per building.	Select from Drop Down List	
	Users can auto-create physical pre-plan, hazmat units, and map markers for easy mapping after data migration.	Select from Drop Down List	
PI-12		Select from Drop Down List	
PI-13	Special Event / IAP pre-planning for specific events or incidents is available.	Select from Drop Down List	
PI-14	Users can easily edit pre-plans on mobile devices.	Select from Drop Down List	
PI-15	Users can edit pre-plans on Google Maps.	Select from Drop Down List	
PI-16	Users can edit pre-plans on Esri ArcGIS maps.	Select from Drop Down List	
PI-17	Permissions exist to allow some users to require approval before publishing pre-plans.	Select from Drop Down List	
PI-18	The software includes history tracking of pre-plans with audit logs.	Select from Drop Down List	
PI-19	The software has an occupancy organizer that allows users to filter occupancies by several attributes.	Select from Drop Down List	
	The software includes pre-plan management that allows admins to change pre-plan cycles, assign pre-plans, and mark target hazards.	Select from Drop Down List	
PI-20	Users have the ability to create ArcGIS feature services for pre-plan and occupancy data by County Users	Select from Drop Down List	
PI-21	without help from the vendor.	Select from Drop Down List	
PI-22	The system can limit access to map layers based on groups or users.	Select from Drop Down List	
PI-23	The system can limit access to an Incident Action Plan that has been attached to a occupancy	Select from Drop Down List	
PI-24	The system can quickly show what building have been pre-plan in a give data range.	Select from Drop Down List	
PI-25	The system can generate a heat map showing what building have been pre-planned.	Select from Drop Down List	
PI-26	The system can query per-plan data by station, apprautus, user, schedule date, completed date	Select from Drop Down List	
PI-27	The system has the ability to schudule pre-plans to stations, appratus, users.	Select from Drop Down List	
PI-28	The system has the ability to display pre-plans data based on dispatched incidents.	Select from Drop Down List	

Spec ID	Description of Requirement	Availability	Vendor Comments
TR-1	The system has the ability to track ISO training hours.	Select from Drop Down List	
TR-2	The system has the ability to categorize ISO training hours. (To include the ability to rollover from category to category)	Select from Drop Down List	
TR-3	The system has the ability to deliver video content to over 600 staff member at the same time.	Select from Drop Down List	
TR-4	The sytem has the ability to upload video content.	Select from Drop Down List	
TR-5	The sytem has the ability to email staff of pending assignments. (To include reoccurring reminders of overdue assignments)	Select from Drop Down List	
TR-6	The sytem has the ability for supervisors to view their staffs progress on assignments.	Select from Drop Down List	
TR-7	The sytem has the ability to track who has read departments polices.	Select from Drop Down List	
TR-8	The sytem has a document repository. (To include the ability to stack versions of documents, with the newest document being the one viewable)	Select from Drop Down List	
TR-9	The sytem has a way to easily search for documents in the repository.	Select from Drop Down List	
TR-10	The sytem has a way to search for words within the documents in the repository.	Select from Drop Down List	
TR-11	The system has the ability to be used a Learning Management System(LMS).	Select from Drop Down List	
TR-12	The system has the ability to build activities (class)	Select from Drop Down List	
TR-13	The system has the ability to watch a videos within a class (To include the ability to require staff to watch in entirety before being able to complete class)	Select from Drop Down List	
TR-14	The system has the ability to require staff to open an attachment within a class.	Select from Drop Down List	
TR-15	The system has the ability to track progress of task type work books.	Select from Drop Down List	
TR-16	The system has the ability to track staff credentials.	Select from Drop Down List	
TR-17	The system has the ability for staff to self assign courses.	Select from Drop Down List	
TR-18	The system has a home page dash board for ease of access to regularly used items and notifications.	Select from Drop Down List	
TR-19	The system has the ability to assign access at multiple levels.	Select from Drop Down List	
TR-20	The system has the ability to generate, view, and export reports from activity (class) completions	Select from Drop Down List	
TR-21	The system has the ability to bulk upload users, test banks, etc.	Select from Drop Down List	
TR-22	TThe LMS system has the ability to assign skills	Select from Drop Down List	
TR-23	TThe LMS system has the ability to assign skills for yearly fitnet tests	Select from Drop Down List	
TR-24	TThe LMS system has the ability to quickly complete skill evaluations via desktop and tablet	Select from Drop Down List	

Spec ID	Description of Requirement	Availability	Vendor Comments
HS-1	The system has the ability to add injury reports not related to a fire.	Select from Drop Down List	
HS-2	The system has the ability to add vehicle accident reports not related to a incident report.	Select from Drop Down List	
HS-3	The system has the ability to trace exposures not related to an incident.	Select from Drop Down List	
HS-4	The system has a dashboard that tracks injury reports	Select from Drop Down List	
HS-5	The system has a Quality and Assurance(QA) process for injury and vehicle accident.	Select from Drop Down List	
HS-6	The system has the ability to track outcomes of investigation into a injury.	Select from Drop Down List	
HS-7	The system has the ability to track outcomes of investigation into a vehicle accident.	Select from Drop Down List	
HS-8	The system has the ability to limit access to injury reports by user permissions.	Select from Drop Down List	
HS-9	The system has the ability to limit access to vehicle accident reports by user permissions.	Select from Drop Down List	
HS-10	The system has the ability to limit access to exposures by user permissions.	Select from Drop Down List	
HS-11	The system has the ability to track injuries based on part of the body.	Select from Drop Down List	
HS-12	The system has the ability to track vehicle accident based on if the apparatus was responding.	Select from Drop Down List	
HS-13	The system has the ability to track vehicle accident based on who was responsible.	Select from Drop Down List	
HS-14	The system has built in workflow for staff injury reports not at an incident.	Select from Drop Down List	
HS-15	The system has built in workflow for vehicle accident reports not at an incident.	Select from Drop Down List	
HS-16	The system has dashboard to track status of vehicle and staff injuries.	Select from Drop Down List	
HS-17	The system allows customers to create a report that track status of vehicle and staff injuries.	Select from Drop Down List	

Spec ID	Description of Requirement	Availability	Vendor Comments
R-1	The system has the ability to create custom reports at no cost to the customer.	Select from Drop Down List	
R-2	The system has the ability to allow customers to modify/copy existing reports at no cost to the customer	Select from Drop Down List	
R-3	The system can schedule reports.	Select from Drop Down List	
R-4	The system can email scheduled reports.	Select from Drop Down List	
R-5	The sytem can send a report to a SharePoint site.	Select from Drop Down List	
R-6	The system can email up to 100 reports per minute.	Select from Drop Down List	
R-7	Reports can be be viewed in excel.	Select from Drop Down List	
R-8	Reports can be be viewed in common delimited text format.	Select from Drop Down List	
R-9	Reports can be be viewed in PDF.	Select from Drop Down List	
R-10	The system can run SQL queries.	Select from Drop Down List	
R-11	The system has query capabilities in all modules.	Select from Drop Down List	
R-12	User with the permission can save their own custom queries in all modules.	Select from Drop Down List	
R-13	User with the permission can save their own custom reports in all modules.	Select from Drop Down List	
R-14	User with the permission can save their data to ArcGIS online.	Select from Drop Down List	
R-15	User with the permission can save their data to be imported google maps.	Select from Drop Down List	

Spec ID	Description of Requirement	Availability	Vendor Comments
AS-1	The platform includes an assets dashboard with the ability to show specific information for users, including upcoming checks, work orders, and system logs.	Select from Drop Down List	
AS-2	An apparatus-specific dashboard with basic information about apparatus is available.	Select from Drop Down List	
AS-3	Quick links to create work orders and fuel requests are available.	Select from Drop Down List	
AS-4	A quick button to mark vehicles out of service is included.	Select from Drop Down List	
AS-5	Apparatus is grouped by station.	Select from Drop Down List	
AS-6	Platform can start scheduled vehicle checks.	Select from Drop Down List	
AS-7	Platform can start scheduled equipment checks.	Select from Drop Down List	
AS-8	Platform can start scheduled inventory checks.	Select from Drop Down List	
AS-9	Users can easily view checklist history.	Select from Drop Down List	
AS-10	Customizable checklists for daily, weekly, and monthly checks are available.	Select from Drop Down List	
AS-11	Users can auto-generate work orders from checklist item failures.	Select from Drop Down List	
AS-12	Users can add remarks and photos to checklist issues.	Select from Drop Down List	
AS-13	Users can relate equipment and inventory to compartments.	Select from Drop Down List	
AS-14	Compartment checks are included in the main vehicle check.	Select from Drop Down List	
AS-15	A searchable and filterable apparatus list is available.	Select from Drop Down List	
AS-16	A searchable and filterable equipment list is available.	Select from Drop Down List	
AS-17	A searchable and filterable inventory list is available.	Select from Drop Down List	
AS-18	Quantity control for inventory exists.	Select from Drop Down List	
AS-19	Expiration dates on inventory are included.	Select from Drop Down List	
AS-20	There is solid integration with vehicles to automatically import engine diagnostics and other vehicle data.	Select from Drop Down List	
AS-21	The system has the ability to track gas monitors.	Select from Drop Down List	
AS-22	The system has the ability to track HAZMAT consumables.	Select from Drop Down List	
AS-23	The system has the ability to track tests of equipment.	Select from Drop Down List	
AS-24	The system has the ability to track all changes to an asset by username and datetime stamp	Select from Drop Down List	
AS-25	Check Sheet or equipment list for 5 Battalions and/or 29 Stations so unified ordering system to prevent duplicating efforts.	Select from Drop Down List	
AS-26	Track Lot numbers and expiration	Select from Drop Down List	
AS-27	Check-out/Check-in equipment and training aides	Select from Drop Down List	
AS-28	Issue (sell) stock to individual locations- apparatus, Batt Stations, fire stations, people	Select from Drop Down List	
AS-29	Track perishable items	Select from Drop Down List	
AS-30	Easily receive inventory against purchase orders and transfer stock between supply rooms.	Select from Drop Down List	
AS-31	Easily create reports to see quantities on hand in warehouse, and what has been issued to a given location/person in a specified period.	Select from Drop Down List	
AS-32	Track assets- location, warranty, serial number, maintenance, maintenance performed, and preventative maintenance	Select from Drop Down List	
AS-33	Point of sale system that allows customers to request supply items from warehouse(s) within the same system	Select from Drop Down List	
AS-34	Ability to use with mobile application/software to manage inventory and assets in the field at satellite warehouse locations and apparatus	Select from Drop Down List	
AS-35	Barcode scanning consumables and assets that have the manufactures barcode	Select from Drop Down List	
AS-36	Fields within the system designed for use in medical field, current system is designed for vehicle maintenance with nomenclature that reflects maintenance needs	Select from Drop Down List	

Spec ID	Description of Requirement	Availability	Vendor Comments
CE-1	A resident-facing marketing page customized with county colors and themes is available.	Select from Drop Down List	
CE-2	Information pages can be translated into multiple languages	Select from Drop Down List	
CE-3	There is a portal for residents and business owners to sign up to add critical information about their occupancy.	Select from Drop Down List	
CE-4	There is a portal for residents and business owners to search for non EMS incident reports.	Select from Drop Down List	
CE-5	There is a portal for residents and business owners to search for fire inspections reports.	Select from Drop Down List	
CE-6	There is a portal for residents and business owners to search for fire inspections reports and invoices.	Select from Drop Down List	
CE-7	There is a portal for residents and business owners to search for fire inspections reports, listed violations, and invoices	Select from Drop Down List	
CE-8	Community portal users can provide pet and livestock information.	Select from Drop Down List	
CE-9	Community portal users can provide door/gate access codes.	Select from Drop Down List	
CE-10	Community portal users can provide access and utility information.	Select from Drop Down List	
CE-11	Community portal users can provide hazardous material.	Select from Drop Down List	
CE-12	Community portal users can provide fire systems.	Select from Drop Down List	
CE-13	Community portal users can provide attachments.	Select from Drop Down List	
CE-14	Residents can apply for a burn permit online with burn permit workflow and burn bans.	Select from Drop Down List	
CE-15	The tool can send automated emails to remind community portal users to update information	Select from Drop Down List	
CE-16	The tool will automatically remove account information if not reconfirmed after multiple opportunities within a department-configurable time period.	Select from Drop Down List	
CE-17	Downloadable marketing resources to send or print to help drive sign-ups are available.	Select from Drop Down List	
CE-18	The provider offers the regular creation of social media posts that customers can download and use to drive sign-ups.	Select from Drop Down List	
CE-19	Data provided by residents and business owners is automatically imported into the pre-plan	Select from Drop Down List	
CE-20	Automated emergency SMS notifications to commercial community portal users when units are dispatched to their occupancy are available.	Select from Drop Down List	

Spec ID	Description of Requirement	Availability	Vendor Comments
AI-1	Does your system us AI	Select from Drop Down List	
AI-2	AI part of your incident documenation module	Select from Drop Down List	
AI-3	AI part of your eCPR module	Select from Drop Down List	
AI-4	AI helps fill out fileds in incident documenation module	Select from Drop Down List	
AI-5	AI helps fill out fileds in ePCR module	Select from Drop Down List	
AI-6	AI helps fill staffing shortages	Select from Drop Down List	
AI-7	AI helps create AD-HOC reports	Select from Drop Down List	
AI-8	Report of AI audit trail	Select from Drop Down List	

Spec ID	Description of Requirement	Availability	Vendor Comments
AI-1	Does the system have an intergrated Incident Command Module	Select from Drop Down List	
AI-2	Incident Command Module was create by you	Select from Drop Down List	
AI-3	Incident Command Module was purchased or obtained by merger	Select from Drop Down List	
AI-4	Incident Command is intergated with schedule module	Select from Drop Down List	
AI-5	Incident Command is intergated with CAD vendor	Select from Drop Down List	
AI-6	Incidetn Command is intergated with NERIS reporting module	Select from Drop Down List	
AI-7	Incident Command is all drag and drop	Select from Drop Down List	
AI-8	Incident Command pulls units from CAD	Select from Drop Down List	
AI-9	Incident Command can create division on the fly	Select from Drop Down List	
AI-10	Incident Command can be view by several users at once	Select from Drop Down List	
AI-11	Incident Command can transfer command	Select from Drop Down List	

APPENDIX VI

Vendor Security Questionnaire

The City requires vendors to complete a Vendor Security Questionnaire (VSQ) as part of the City's Vendor Risk Assessment Program. This evaluation helps ensure that vendors meet the City's cybersecurity, privacy, and data protection standards.

The VSQ requirement is applicable when a vendor will access City systems or data; provide technical support; host, process, or store City information; integrate with City networks or applications; or perform any work that could impact the security or availability of City information systems.

The VSQ is used to assess a vendor's security controls, data handling practices, and compliance posture. Vendors who do not meet minimum security expectations may not be eligible for award. Finalist vendors will be notified if they need to complete the official VSQ after evaluation.

City of Raleigh – Vendor Security Questionnaire

Version 6 | Effective June 2026 | City of Raleigh Information Security

PURPOSE

The City of Raleigh, North Carolina, employs this Vendor Security Questionnaire (VSQ) to evaluate vendors' information security posture and risk management practices. This form includes sections on asset management, access controls, incident response, data governance, artificial intelligence, quantum computing readiness, and other critical cybersecurity areas. All technology and data-related vendors are required to complete and submit this form to assess and mitigate potential risks associated with access to the City's systems and data.

INSTRUCTIONS

- Third-party vendors and companies should complete and return this form to their designated City representative.
- Please complete the Vendor Identification section on Tab #2 before responding to all questions.
- Use the dropdown lists in the 'Vendor Response' column; add context in the 'Vendor Comments' column as needed.
- If a SOC 2, ISO 27001, CMMC, or HITRUST certification is available, send it via encrypted email marked CONFIDENTIAL. See Question 1.1 for skip-logic instructions.
- The City of Raleigh is unable to enter into a Non-Disclosure Agreement (NDA) for access to documentation due to public records law.
- Failure to fully complete this form and/or provide required documentation may result in delayed contract processing.

REVIEW PROCESS

Upon receipt, the City's IT Security group will review responses and provide feedback to the sponsoring business department. For questions, contact your City of Raleigh representative or the appropriate Enterprise IT Business Relationship Partner.

IMPORTANT NOTICES

- Risk Baseline ratings (HIGH / MEDIUM / LOW) indicate the City's baseline risk classification for each control area. HIGH-rated items require YES responses or documented compensating controls.
- Responses of 'Partial (Please explain)' or 'No' on HIGH-risk items will be escalated for additional review.
- This questionnaire is updated periodically. Version 6 adds modernized AI governance controls, supply chain transparency requirements, and quantum-readiness alignment with NIST IR 8413.

City of Raleigh Vendor Security Questionnaire – v6				
Version 6 Effective June 2026 Complete all required fields. Use dropdowns in the Vendor Response column (Column E) to respond. Add Notes and Comments to Column F.				
VENDOR IDENTIFICATION				
Company Legal Name:				
Company Address:				
Security Officer Name & Email:				
Completed By (Name & Title):				
Date Completed:				
Product(s) / Services Covered by this Questionnaire:				
#	Question	Risk Baseline	Vendor Response (select from dropdown)	Vendor Comments
1 INFORMATION REQUESTS				
Identifies and gathers key certification and documentation artifacts that may enable streamlined review.				
1.1 (UPDATED)	Does your organization hold a SOC 2 Type I, SOC 2 Type II, SOC 3 Type II, ISO 27001, or HITRUST certification? • SOC 2 Type I: Provide report via encrypted email and mark it CONFIDENTIAL; answer 1.5–1.7; skip to Section 4. • SOC 2 Type II: Provide report via encrypted email and mark it CONFIDENTIAL; answer 1.5–1.7; skip to Section 11. • SOC 3 Type II: Provide report via encrypted email and mark it CONFIDENTIAL; answer 1.5–1.7; skip to Section 9. • ISO 27001: Provide certificate and Statement of Applicability via encrypted email and mark the document CONFIDENTIAL; answer 1.5–1.7; skip to Section 14. • HITRUST CSF: Provide Certification Report via encrypted email and mark the document CONFIDENTIAL; answer 1.5–1.7; skip to Section 14. • CMMC: Provide Certification Report via encrypted email and mark the document CONFIDENTIAL; answer 1.5–1.7; skip to Section 14. • If none of these options can be provided: Completion of the full questionnaire is Mandatory.	N/A		
1.2	Please provide a copy of your information security policy and mark it CONFIDENTIAL. We recommend providing this document via encrypted email.	N/A		
1.3	Please provide a copy of any relevant audit reports covering information security controls (e.g., NIST CSF assessment, NIST 42001:2023, etc.). Mark the document(s) CONFIDENTIAL and provide the document(s) via encrypted email.	N/A		
1.4	Please provide a copy of your most recent penetration test and/or vulnerability assessment report. Mark the document(s) CONFIDENTIAL and provide the document(s) via encrypted email.	N/A		
1.5 (UPDATED)	If your services are offered as Software as a Service (SaaS) or cloud-based, are they provided in a FedRAMP-authorized, GovRAMP-authorized, or equivalent government-grade cloud environment? If Yes, provide: authorization type (e.g., FedRAMP Moderate/High, GovRAMP), authorization level, sponsoring agency, and scope of covered services.	HIGH		
1.6 (UPDATED)	Please describe any significant security incidents or breaches within the last 5 years, including size, scope, impact, remediation actions taken, and whether regulatory or legal notification was triggered. Significant incidents include: compromise of sensitive data, disruption of critical services, regulatory/legal notification triggered, significant financial or reputational impact, or confirmed lateral movement or persistent threat activity.	HIGH		
1.7 (UPDATED)	Please describe any lawsuits, legal actions, or regulatory investigations your organization has been involved in within the past five years that may be relevant to your cybersecurity practices, data protection responsibilities, or service delivery obligations.	HIGH		
2 ASSET MANAGEMENT				
Identifies, tracks, and safeguards hardware, software, and data assets throughout their lifecycle.				
2.1	Do you maintain an inventory of all hardware and software assets, including ownership and lifecycle status?	HIGH		
2.2	Do you have an information classification scheme designed to ensure data is protected according to its sensitivity and confidentiality requirements?	HIGH		
2.3	Do you maintain an inventory or map of data flows between internal and external information systems, including cross-border transfers?	HIGH		
2.4 (NEW)	Do you maintain a software bill of materials (SBOM) for software products or services delivered to the City?	MEDIUM		
3 GOVERNANCE				
Establishes policies, procedures, and oversight to ensure alignment between security practices and organizational goals.				
3.1	Do you have an information security policy approved by management and communicated to all applicable personnel and contractors?	HIGH		
3.2	Do you have a formal security policy exception process that includes documented risk acceptance by the appropriate risk owner?	HIGH		
3.3	Do you review and update your information security policy at least annually?	MEDIUM		
3.4	Do you regularly perform security threat and risk assessments on critical information systems using an industry-standard methodology (e.g., NIST RMF, ISO 27005, FAIR)?	HIGH		
3.5	Have you designated an individual at manager level or above who is responsible for information security activities (e.g., CISO or equivalent)?	HIGH		
3.6	Do you have a process to monitor regulatory and legal changes and ensure ongoing compliance with applicable security requirements?	MEDIUM		
3.7 (NEW)	Do you maintain a formal records retention and disposal schedule that addresses security and privacy requirements, including data belonging to the City of Raleigh?	MEDIUM		
4 SUPPLY CHAIN RISK MANAGEMENT				
Evaluates and mitigates risks associated with third-party vendors, suppliers, and partners.				
4.1	Do you perform security assessments on potential suppliers prior to entering into agreements with them?	MEDIUM		
4.2	Do your supplier agreements include appropriate security requirements and assign shared responsibility for data protection?	MEDIUM		
4.3	Do you regularly evaluate suppliers to ensure they are meeting their contractual security obligations?	MEDIUM		
4.4 (NEW)	Do you require your critical subprocessors and suppliers to carry cyber liability insurance? If yes, please specify minimum coverage amounts.	MEDIUM		
4.5 (NEW)	Do you have a process to vet and monitor open-source software components used in your products or services for known vulnerabilities (e.g., using SCA tooling)?	HIGH		
5 IDENTITY MANAGEMENT, AUTHENTICATION, AND ACCESS CONTROL				
Manages user identities and ensures only authorized individuals have access to systems and data.				
5.1	Is all access to information systems formally approved by the appropriate asset owner?	MEDIUM		
5.2	Can all access to information systems be traced to unique, identified individuals (no shared accounts)?	HIGH		
5.3	Are all access rights reviewed at least annually for appropriateness by asset owners?	MEDIUM		
5.4	Are all access rights immediately revoked upon employee or contractor termination or change of role?	HIGH		

5.5	Do you restrict and control the use of privileged accounts using a Privileged Access Management (PAM) system or equivalent controls?	HIGH		
5.6	Do you enforce least privilege and separation of duties principles in access permission management?	HIGH		
5.7	Do you require multi-factor authentication (MFA) for all remote access to organizational data, including email?	HIGH		
5.8	Do you require MFA for all administrative access to cloud-based information systems?	HIGH		
5.9 (NEW)	Do you enforce phishing-resistant MFA (e.g., FIDO2/WebAuthn, PIV/CAC) for privileged and remote access?	HIGH		
5.10 (NEW)	Do you have a formal Identity Governance and Administration (IGA) program or process that enforces role-based access control (RBAC) and periodic access certification?	MEDIUM		
6 HUMAN RESOURCE SECURITY				
<i>Ensures employees, contractors, and third parties understand and adhere to security responsibilities.</i>				
6.1	Do you have a security awareness program requiring all employees and contractors to complete role-appropriate training at least annually?	HIGH		
6.2	Do you conduct regular phishing simulation tests of your employees?	HIGH		
6.3	Do you conduct appropriate background checks on all new employees based on the sensitivity of their role?	HIGH		
6.4	Do you require all new employees and contractors to sign confidentiality agreements prior to accessing organizational systems or data?	MEDIUM		
6.5 (NEW)	Do you provide role-specific security training for personnel with elevated privileges or access to sensitive data (e.g., developers, system administrators, data custodians)?	MEDIUM		
7 DATA SECURITY				
<i>Protects sensitive data from unauthorized access, loss, or alteration through encryption, classification, and controls.</i>				
7.1	Do you require that all removable media that may contain organizational data is encrypted?	MEDIUM		
7.2	Do you require that all media, including hardcopies, containing organizational data is disposed of securely when no longer required?	HIGH		
7.3	Have you implemented data loss prevention (DLP) tools to detect and prevent unauthorized data exfiltration?	HIGH		
7.4	Do you employ full disk encryption on all laptops and portable computing devices?	MEDIUM		
7.5	Do you encrypt databases at rest? If yes, specify the encryption standard used (e.g., AES-256).	HIGH		
7.6	Is data encrypted data in transit using industry-standard protocols (e.g., TLS 1.2 or higher)?	HIGH		
7.7 (NEW)	Do you have a formal data classification policy that governs how City of Raleigh data is labeled, handled, stored, and transmitted?	HIGH		
7.8 (NEW)	Do you perform regular data discovery scans to identify unauthorized or unclassified sensitive data stores?	MEDIUM		
8 SYSTEM ACQUISITION, DEVELOPMENT, AND MAINTENANCE				
<i>Incorporates security requirements into the procurement, development, and maintenance of IT systems.</i>				
8.1	Are information security requirements defined for all new information systems, whether acquired or developed?	MEDIUM		
8.2	Are development, testing, and staging environments separated from the production environment?	HIGH		
8.3	Is data used for development and testing protected through anonymization, pseudonymization, or synthetic data?	HIGH		
8.4 (UPDATED)	Are information security requirements tested to verify they function as designed (e.g., security acceptance testing)?	HIGH		
8.5	Are your applications developed with secure coding practices, including mitigations for the OWASP Top 10 Most Critical Web Application Security Risks?	HIGH		
8.6	Are your web applications and APIs protected by a Web Application Firewall (WAF)?	HIGH		
8.7	Do you incorporate threat modeling into application design and architecture reviews?	MEDIUM		
8.8	Is application source code tested for vulnerabilities using automated static analysis (SAST) and/or dynamic analysis (DAST) tooling?	HIGH		
8.9	Are new information systems scanned for vulnerabilities and security misconfigurations prior to production deployment?	HIGH		
8.10	Do you monitor and restrict the installation of unauthorized software on organizational endpoints?	HIGH		
8.11 (NEW)	Do you perform software composition analysis (SCA) to identify and remediate known vulnerabilities in third-party and open-source libraries?	HIGH		
8.12 (NEW)	Do you have a secure software development lifecycle (SSDLC) policy that includes mandatory security gates (e.g., code review, security testing) before deployment?	MEDIUM		
9 PHYSICAL AND ENVIRONMENTAL SECURITY				
<i>Safeguards physical infrastructure and facilities against unauthorized access and environmental threats.</i>				
9.1	Are physical security perimeter controls implemented at sensitive locations such as data centers (e.g., badge access, CCTV, mantraps)?	HIGH		
9.2	Are all visitors appropriately identified, logged, and escorted while in sensitive locations?	HIGH		
9.3 (NEW)	Are your primary and disaster-recovery data centers geographically separated and protected against environmental threats (e.g., flood, fire, power)?	MEDIUM		
9.4 (NEW)	Does your organization store or process City of Raleigh data in a third-party hosted data center (e.g., AWS, Microsoft Azure, Google Cloud)? If Yes, provide: • Primary data center name and geographic location(s) • Backup / disaster-recovery data center name and geographic location(s) • Any applicable data residency or sovereignty restrictions governing where City data is stored or processed.	HIGH		
10 INFORMATION PROTECTION PROCESSES AND PROCEDURES				
10.1	Do you segment your network into zones based on trust levels and control traffic flows between zones (e.g., DMZ, micro-segmentation)?	MEDIUM		
10.2	Do you control the transfer of information to external parties through authentication and encryption?	HIGH		
10.3	Are all changes to information systems recorded, risk-assessed, planned, and tested prior to deployment (e.g., via a Change Approval Board process)?	HIGH		
10.4	Are all information systems susceptible to malware protected by up-to-date endpoint detection and response (EDR) or anti-malware software?	HIGH		
10.5	Do you have a backup and recovery process ensuring data can be recovered in the event of unexpected loss, and are backups tested at least annually?	HIGH		
10.6	Do you segregate wireless network access for BYOD and guest devices from your production network?	MEDIUM		
10.7	Do you enforce containerization or mobile device management (MDM) on all mobile devices that may contain organizational data, including email, regardless of ownership?	MEDIUM		
10.8	Do you have the capability to remotely wipe all organizational data from laptops and mobile devices in the event of loss or theft?	HIGH		
10.9	Do you monitor external sources (e.g., vendor bulletins, CISA KEV, NVD) for newly identified vulnerabilities and patches applicable to your systems?	MEDIUM		
10.1	Do you evaluate, prioritize, and apply information system patches in a timely manner commensurate with their risk level (e.g., critical patches within 14 days)?	HIGH		

10.11 (NEW)	Do you have a formal vulnerability management program that tracks open vulnerabilities from discovery to remediation with defined SLAs by severity?	HIGH		
11 PROTECTIVE TECHNOLOGY				
<i>Utilizes tools and technologies to defend systems and data from cyber threats.</i>				
11.1	Have security event logging requirements been defined and are all information systems configured to generate logs meeting those requirements?	MEDIUM		
11.2	Are security event logs protected from tampering and retained per defined logging requirements (specify retention period in comments)?	MEDIUM		
11.3	Have you deployed intrusion detection or prevention systems (IDS/IPS) at the network perimeter and/or internally?	MEDIUM		
11.4	Have you deployed DNS filtering or web proxy controls to restrict access to known malicious or unauthorized URL categories?	MEDIUM		
11.5	Have you deployed controls to detect and mitigate Distributed Denial of Service (DDoS) attacks?	HIGH		
11.6 (NEW)	Have you deployed email security controls including anti-phishing, anti-spoofing (DMARC/DKIM/SPF), and sandboxing capabilities?	HIGH		
11.7 (NEW)	Do you employ a Zero Trust Architecture (ZTA) or equivalent approach that continuously validates identity and device posture before granting access to resources?	MEDIUM		
12 SECURITY CONTINUOUS MONITORING				
<i>Continuously monitors systems and networks to identify vulnerabilities and detect potential security incidents.</i>				
12.1	Have you deployed a Security Information and Event Management (SIEM) or equivalent platform to collect, correlate, and analyze security events from multiple sources?	MEDIUM		
12.2	Do you monitor privileged user activity to detect potential misuse or security incidents?	MEDIUM		
12.3	Do you monitor user and entity behavior analytics (UEBA) or equivalent controls to detect anomalous activity?	HIGH		
12.4	Are security alerts monitored 24x7 by a Security Operations Center (SOC) or equivalent capability?	HIGH		
12.5	Do you employ automated tools to scan information systems for vulnerabilities on a regular basis (specify frequency in comments)?	HIGH		
12.6	Do you perform penetration tests on all web applications and services at least annually, using standard methodologies (e.g., PTES, OWASP Testing Guide)?	HIGH		
12.7 (NEW)	Have you deployed threat intelligence feeds that are operationalized to detect and respond to indicators of compromise (IOCs) and threat actor TTPs?	MEDIUM		
12.8 (NEW)	Do you conduct threat hunting activities on a periodic basis to proactively identify attacker presence within your environment?	MEDIUM		
13 INFORMATION SECURITY INCIDENT MANAGEMENT				
<i>Prepares for, detects, and responds to security incidents to minimize impact and facilitate recovery.</i>				
13.1	Do you have a formal, documented security incident response plan (IRP)?	HIGH		
13.2	Do you conduct regular tabletop exercises or simulation tests of your incident response plan (at least annually)?	HIGH		
13.3	Are all security incidents recorded, classified by severity, and tracked through to resolution?	HIGH		
13.4	Are forensic investigations conducted as part of incident response to preserve evidence and support root-cause analysis?	HIGH		
13.5 (NEW)	Do you have a defined process for notifying the City of Raleigh of security incidents that involve City data, including target notification timelines (e.g., within 24 hours of discovery)?	HIGH		
13.6 (NEW)	Do you maintain a formal business continuity plan (BCP) and disaster recovery plan (DRP) that are tested at least annually?	HIGH		
14 PRIVACY				
<i>Ensures the ethical and legal handling of personal and sensitive information to protect individual rights.</i>				
14.1	Do you have a data retention policy and process designed to meet applicable privacy regulations (e.g., GDPR, CCPA, North Carolina Identity Protection Act)?	HIGH		
14.2	Do you maintain an inventory and map of where all personal data is stored, including cross-border data flows and legal basis for transfer?	HIGH		
14.3 (NEW)	Do you have a documented process for responding to data subject access requests (DSARs) and privacy rights requests within regulatory timeframes?	HIGH		
14.4 (NEW)	Do you perform Data Protection Impact Assessments (DPIAs) or Privacy Impact Assessments (PIAs) for new processing activities involving personal data?	MEDIUM		
15 ARTIFICIAL INTELLIGENCE GOVERNANCE				
<i>Manages the security, privacy, and ethical risks of AI and ML technologies, including GenAI, NLP, and autonomous systems.</i>				
15.1 (UPDATED)	Does your software, platform, or service incorporate any form of Artificial Intelligence (AI) or Machine Learning (ML), including Large Language Models (LLMs), Natural Language Processing (NLP), Generative AI (GenAI), or autonomous decision-making components? If Yes, describe the AI components and their function.	HIGH		
15.2 (UPDATED)	Do you have a formal AI governance policy or framework (e.g., aligned to NIST AI RMF 1.0, ISO 42001, or EU AI Act requirements) that governs development, deployment, and monitoring of AI systems?	HIGH		
15.3 (UPDATED)	Do you provide role-specific AI security and responsible AI training to staff who develop, deploy, or operate AI systems?	HIGH		
15.4 (UPDATED)	Do your AI systems have documented transparency mechanisms, including model cards, audit logs, explainability features, or regular third-party audits?	HIGH		
15.5 (UPDATED)	Do your AI components enforce data privacy and security controls, including data minimization, access controls, and encryption of training data and model artifacts?	HIGH		
15.6 (UPDATED)	Do your AI systems have documented bias detection and mitigation protocols? Please briefly explain the methodology used.	HIGH		
15.7 (NEW)	Will City of Raleigh data — including prompts, documents, or outputs — be used to train, fine-tune, or improve your AI models for use with other customers? If Yes, describe the opt-out mechanism, data segregation controls, and privacy safeguards in place.	HIGH		
15.8 (NEW)	Do you implement controls to prevent AI-specific attacks such as prompt injection, model inversion, data poisoning, or adversarial inputs?	HIGH		
15.9 (NEW)	Do you perform regular adversarial testing (red teaming) of your AI systems to identify safety, reliability, and security risks prior to deployment and on an ongoing basis?	HIGH		
15.10 (NEW)	Do you have a process to detect, log, and respond to AI system misuse, hallucinations, or harmful outputs in production environments?	HIGH		
15.11 (NEW)	If your AI system makes or influences decisions that affect individuals, do you provide a human-in-the-loop review mechanism and a process for individuals to contest automated decisions?	HIGH		
15.12 (NEW)	Which AI features make autonomous actions versus recommendations requiring human approval?	HIGH		
16 QUANTUM COMPUTING READINESS				
<i>Prepares for the security implications of quantum computing, including post-quantum cryptography migration.</i>				
16.1 (UPDATED)	Does your organization have a Quantum Computing Readiness or Cryptographic Agility Plan that addresses migration to NIST-approved post-quantum cryptographic (PQC) algorithms (e.g., CRYSTALS-Kyber, CRYSTALS-Dilithium, SPHINCS+)? If Yes, provide your target migration timeline.	MEDIUM		
16.2 (NEW)	Have you inventoried your cryptographic assets (algorithms, key lengths, protocols, certificates) to identify those vulnerable to quantum attack (e.g., RSA, ECC, DH)?	MEDIUM		

16.3 (NEW)	Do you monitor NIST, CISA, and NSA guidance on post-quantum cryptography to ensure timely adoption of approved standards?	LOW		
17 SUBPROCESSORS				
<i>Ensures transparency and accountability for third-party subprocessors that handle or process City data.</i>				
17.1 (UPDATED)	Please provide a complete list of all subprocessors your organization engages that may have access to City of Raleigh data. Include for each: • Subprocessor name and country of incorporation • Services provided • Location(s) where City data is processed or stored • Legal basis for any cross-border data transfer • Security certifications or safeguards in place If the list is extensive, attach as a separate document labeled 'Subprocessor Register – [Company Name] – [Date]'.	HIGH		
17.2 (NEW)	Do you notify the City of Raleigh prior to engaging new subprocessors or making material changes to existing subprocessor arrangements that may affect City data?	HIGH		
17.3 (NEW)	Do you contractually require your subprocessors to maintain security and privacy standards equivalent to those required of you under your agreement with the City of Raleigh?	HIGH		
18 OFFSHORE RESOURCES AND CROSS-BORDER DATA				
<i>Identifies the use of non-U.S. personnel with access to City data or systems, and ensures appropriate controls govern data crossing U.S. boundaries.</i>				
18.1 (NEW)	Does your organization employ, contract, or otherwise engage personnel located outside of the United States who have access to City of Raleigh data or supporting systems? If Yes, identify the countries where offshore personnel are located and describe the nature of their access.	HIGH		
18.2 (NEW)	If offshore or non-U.S. personnel have access to City data or systems, what controls are in place to govern, monitor, and restrict that access? Describe applicable controls such as role-based access control, VPN enforcement, data residency restrictions, enhanced audit logging, and contractual data handling obligations.	HIGH		
18.3 (NEW)	Does City of Raleigh data ever leave U.S. boundaries for any purpose, including processing, storage, support, development, or analytics? If Yes, identify all countries involved, the legal basis for the cross-border transfer (e.g., Standard Contractual Clauses, data processing agreements), and the safeguards in place to protect the data.	HIGH		
18.4 (NEW)	Do you provide advance notice to the City of Raleigh before engaging non-U.S. personnel who will have access to City data, or before routing or storing City data outside the United States?	HIGH		
19 CYBER LIABILITY INSURANCE				
<i>Verifies that the vendor maintains adequate cyber liability insurance to address cybersecurity incidents, data breaches, and associated third-party liability.</i>				
19.1 (NEW)	Does your organization carry cyber liability insurance coverage?	HIGH		
19.2 (NEW)	Please provide the following details for your cyber liability insurance policy if you carry a policy: • Insurer name • Policy effective and expiration dates • First-party coverage limit (e.g., breach response, forensics, ransomware, business interruption) • Third-party liability coverage limit (e.g., regulatory fines, customer notification costs, litigation defense) • Whether the City of Raleigh can be listed as an additional insured If you do not have a policy, please indicate N/A.	HIGH		
19.3 (NEW)	What is the minimum aggregate cyber liability insurance coverage amount maintained by your organization? Please specify the amount in USD in the Vendor Comments column.	HIGH		
19.4 (NEW)	Do you contractually require your critical subprocessors and key third-party vendors to maintain cyber liability insurance at minimum coverage levels equivalent to those you carry or as specified in your vendor agreements? If Yes, specify minimum required amounts in Vendor Comments.	MEDIUM		
20 OPERATIONAL RESILIENCE				
<i>Assesses the vendor's capacity to maintain or rapidly restore critical service delivery in the face of disruptions, including technical failures, natural disasters, and cyberattacks. Complements incident response and BCP/DRP coverage in Section 13.</i>				
20.1 (NEW)	Do you have formally documented Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) for services provided to the City of Raleigh? If Yes, specify the RTO and RPO targets in Vendor Comments.	HIGH		
20.2 (NEW)	Do you maintain redundant infrastructure (e.g., active-active or active-passive failover, hot/warm/cold standby environments) to ensure continuity of services provided to the City of Raleigh in the event of a primary system failure?	HIGH		
20.3 (NEW)	Are your Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) tested through tabletop exercises, simulations, or full technical failover tests at least annually? If Yes, describe the most recent test type and date in Vendor Comments.	HIGH		
20.4 (NEW)	Do you maintain formal Service Level Agreements (SLAs) specifying uptime guarantees, availability commitments, and remediation timelines for disruptions to services delivered to the City of Raleigh? If Yes, specify the SLA targets (e.g., 99.9% uptime) in Vendor Comments.	HIGH		
20.5 (NEW)	Do you perform regular capacity planning and load testing to ensure your infrastructure can sustain service availability under both normal and peak demand conditions?	MEDIUM		
20.6 (NEW)	Do you have defined communication procedures to notify the City of Raleigh of service disruptions, outages, or degraded performance that may affect City operations, including target notification timelines and designated points of contact?	HIGH		