Section III: Exhibits

Exhibit A – Key Functional and Technical Requirements

Exhibit B – Pricing Proposal

Exhibit C – Customer References

Exhibit D – Acceptance of Terms and Conditions of RFP

Exhibit E – Non-Collusion Certificate

Exhibit F – Non-Disclosure Agreement

Exhibit G – City of Kirkland IT Vendor Security Policy and IT Cloud Security Policy

Exhibits

Exhibit A – Key Functional and Technical Requirements

This section includes the Requirements to be evaluated in this RFP. This document will become Section 3 of your RFP response. **Use the electronic format provided with this RFP package**. This is not a comprehensive list of all of the City's requirements, but includes the key requirements that will be used to evaluate the RFPs and will be included as part of the signed contracts. Each item has been provided a ranking of R, I, N or E. A ranking of "R" indicates a feature is preferably Required, "I" indicates the feature is Important to the final decision, a ranking of "N" indicates the feature would be Nice to Have in a solution, and a ranking of "E" represents areas to Explore in the overall solution. Software applications that are missing a significant number of required features and technology preferences may be eliminated from consideration.

Vendors must provide a rating for every item for Core Modules. If the requirement does not pertain to the proposal being submitted, enter "N/A". In addition, **each line item should include a brief explanation of how the required item is supported**. Do not modify the format, font, numbering, etc. of this section. If a submitted RFP includes blank responses the document may be considered in violation and rejected. Vendors are encouraged to respond by either providing a response to requirements based on Vendor-offered solutions, or by identifying third party partnership solutions.

Use the following rating system to evaluate each requirement:

Rating	Definition
3	**Standard and available in the current release**. Software supports this requirement and can be implemented with minimal configuration at no additional cost. No source code modification is required.
2	**Meet requirement with minor modification**. Modification maintains application on upgrade path. Testing and production of modifications will be completed by implementation date. Include an estimate for the cost of the modification.
1	**Available with 3rd party software application.** Indicate name of the application recommended and number of installs jointly completed.
0	**Not available.** Software will not meet requirement.
F	**Future Release.** Requirement will be available in future release. Indicate anticipated release date: month and year.

Sample Response Format: Please use the format below when completing your response. The rating should be on one line and the comment should follow on the second line. Comments such as "Standard Functionality" or "In the CRM system" are not acceptable comments.

	General	Rating and Comment
R	1. Audit Trail with user, date, time stamp throughout all modules. Before/after values is Important.	3 System logs all transactions and stamps them with user, date, time and before/after values.

Exhibits

R = Required
I = Important
N = Nice to have
E = Explore

City of Kirkland

CRM Software Requirements

Rating	Vendor Background	Comments
	1. **Company**	
	▪ Company Name	
	▪ Contact Person Name and Title	
	▪ Contact Address, Phone, Email	
	2. **Company Information**	
	▪ Public vs. Private	
	▪ Year Founded	
	▪ Revenue and Income: Current and Prior Year	
	▪ Office Locations: Headquarters, Implementation, Support, Development	
	▪ Nearest regional office to Kirkland, WA	
	▪ Website	
	▪ Employee Count	
	▪ Data center location and provider (owned vs. leased)	
	3. **Number of Customers**	
	▪ Total Customers	
	▪ Total Customers on Proposed Application	
	▪ Total Cities	
	▪ Total Washington Cities	
	▪ Total Customers Our Size	
	4. **Target Customer Profile**	
	▪ Target Industries	
	▪ Sizing - Users and Population	
	5. **Version Schedule**	
	▪ Current version and Release Date	
	▪ Proposed Version and Release Date	

Exhibits

Rating	**Pricing Summary - Details in RFP Pricing Section 4**	**Comments**
	All Costs – Required Modules	
	6. **Software License :**	
	▪ Named vs. Concurrent licensing ▪ Mobile licensing (if different)	
	7. **Implementation:** Total cost for implementation, data conversion, training, report development, integration, travel, etc.	
	8. **Maintenance:** Total cost - Years 1-10.	
	9. **Other Costs**	
	10. **Total First Year Cost – Required Modules**	
	11. **Total Ten year Cost – Required Modules**	
Rating	**Technology**	**Rating/Comments**
R	12. Integration across all modules in the system; enter data once, updates all records.	
R	13. For web clients: Web-enabled or Web-based architecture with published open API's and browser and platform agnostic. List of current browsers supported and the version you support.	
R	14. Describe functions supported by mobile technology, e.g. workflow approvals, data look-up's, etc. Include what devices and mobile OS's are support (iPads vs Surfaces, iOS vs. Android)	
R	15. Available SaaS and hosted options which allow more than one environments, e.g. production, test	
R	16. Role-level security to menu and screen level.	
I	17. Provide the ability to translate information into multiple languages. Please explain you method.	
I	18. Comply with ADA WCAG 2.0 AA or higher or have a roadmap for this.	
R	19. Comply with institutional data security requirements including: a. PHI security	
R	20. Single sign-on: MS Active Directory; LDAP compatible.	
R	21. Microsoft Outlook and Exchange Server integration for Email and workflow approval.	
R	22. Office 365 integration.	
R	23. Import/Export to Microsoft Word, Access and Excel; ability to filter data for export.	
R	24. List integration technologies, e.g. Web Services, SOA, XML, etc. Flat file not preferred.	

Rating	Technology	Rating/Comments
I	25. Describe compliance with Service Oriented Architecture (SOA).	
I	26. Indicate experience integrating and proposed method to other City applications and services (e.g. Web Services, API, etc.):	
	a. Tyler Munis	
	b. Tyler EnerGov	
	c. Lucity	
	d. REC1	
	e. VueWorks	
	f. Accela Springbrook	
	g. GovQA WebQA	
	h. Esri Enterprise ArcGIS Platform	
	i. Assetworks Fleet FocusFA	
	j. HP TRIM	
	k. City Website http://www.kirklandwa.gov	
	l. SharePoint Online	
	m. Latitude Geographics Geocortex	
	n. HP Omega	
	o. Social Media	
R	27. Scan and attach PDF, JPEG, wav, MP3, TIF, etc. and MS Office files to records throughout all modules. System provides the capability for the requester to attach photos or other files from an external source when submitting a service request. Specify what image types are supported. Is there a file size limit?	
R	28. Online Readable Data Dictionary or database schema.	
I	29. Indicate tools and utilities available for data purge, archiving processes and retention rule implementation.	
I	30. Ability to use special characters (including keyboard [`|!@#$%^&*”] vs. non-keyboard①☺🖃🗁) in notes, emails approvals, passwords, etc.	
Rating	**General Requirements**	**Rating/Comments**
I	31. Configurable role-based dashboards to present reports, tasks, notifications.	
R	32. Audit Trail with user, date and time stamp throughout all modules, with before/after history.	
I	33. User configurable menus, screens, and fields, e.g. hide unused fields, set tab order, define mandatory fields, etc.	

I	34. Flexible description field widths throughout the system. Describe what is supported.	
R	35. User-defined fields that can be used in queries and reports; indicate where available and limitations.	
I	36. Configurable electronic forms that can be filled in, routed online for approval and update the database.	
I	37. Context sensitive field help.	
R	38. Rules-based workflow routing to multiple approvers that can be concurrent or consecutive with prioritization, alerts.	
R	39. Visibility to Workflow queue.	
R	40. Activity or date triggered alerts, flags, and messages.	
R	41. Effective dating of transactions throughout all modules; input change today that is effective at a future or past date.	
N	42. Searchable notes fields by key word across records and modules.	
I	43. Indicate strategy for document management within the application including retention.	
R	44. Ability to group contacts	
N	45. Generate letters, mailing labels, emails, faxes, consolidate communications.	
Rating	**Core Business Functionality**	**Rating/Comments**
R	46. Provide a web portal for submission of customer requests. Proposed solution is a “software as a service” (SaaS) licensing and delivery model. This must be integrated with the City Website.	
R	47. Provide native smart device applications for submission of customer requests. Specify platforms the applications are available in.	
R	48. Software is a web-based solution and allows staff to access the organization’s data from anywhere at any time with just a browser, internet connection, and user ID and password.	
R	49. The customer interface is obvious, intuitive, user friendly, and easy to navigate by the requestor.	
R	50. Relational Database for storage and maintenance of requests / cases / activities / requestors / responders.	
R	51. Ability to inactivate a service request category and related data without deleting any previously created requests/cases.	
R	52. Provides a back end application that allows staff to manage and support the applications and users.	

R	53. Ability to identify a responsible person, department and/or workgroup for each case/request.	
R	54. Must have a locked-out, read only and other field level specific access control features based on individual user ID and password.	
R	55. Ability to send pre-programmed or template responses to individual requests based on the category or type of request. System can provide automated feedback to the requester regarding acknowledgement of the contact.	
R	56. Ability to send/receive emails to City of Kirkland staff from within the application and have this data captured within the request/case. (Replies to system emails are added to case).	
R	57. The ability to establish response times, with email reminders to assigned staff if cases are not closed. Ability for staff to respond back to email and details will be captured within the case.	
R	58. Individuals using the application can submit requests without registering and creating a profile.	
R	59. Ability to record geolocation of a case and view data geographically.	
I	60. Ability for City Staff to modify and provide and accurate GIS location if the request is inaccurate.	
R	61. The ability to establish the escalation to additional staff members if the request/case has not been closed within the approved timeline window.	
R	62. The ability for individuals to see in a geographical way issues that have already been reported. As well as seeing the status of communications on the issue.	
R	63. The ability for individuals to see what has been reported and the status of those items. (non map view)	
I	64. System allows the customer to view/recall any past request and/or response.	
R	65. System can provide automated feedback to the requester at various stages in the workflow process.	
I	66. Ability to provide knowledge base of frequently requested topics.	
N	67. The ability to use voice for keyword searches.	
R	68. System provides for notes/alerts/etc. to be tagged to a customer account, such that upon next staff access of that account the customized alert is displayed.	
R	69. Ability to define and configure validation lists and categories.	
R	70. System is compliant with Washington State Public Records laws.	

Exhibits

Rating	Reporting	Rating/Comments
R	71. Non-proprietary open reporting tools. List tools offered that are integrated with the system.	
I	72. User-level query and reporting tools that allow for presentation ready formatting of data, headers, graphs, charts, etc.	
R	73. Filterable date-range or point-in-time reporting and queries. Drop down lists or drag and drop criteria selection preferred.	
R	74. Define queries and save with refresh capabilities.	
R	75. Deliver library of prebuilt reports.	
I	76. Modify standard report and save with permissions.	
R	77. User-level security to field level flows through to queries and reports.	
I	78. Schedule generation of reports and distribute via e-mail, to a shared folder, dashboard, or portal.	
I	79. Generate reports in multiple formats, e.g. HTML, PDF, Excel, Word, etc. Please specify the formats you support.	

Exhibits

Exhibit B – Pricing Proposal

Use the Pricing Summary forms for pricing information (hours and $) for proposed solutions. This form will become Section 4 of your RFP response. Additional documents can be provided as supporting information to the summarized information on these pages. Pricing must be fully comprehensive, complete and list any available discounts.

City of Kirkland Pricing Summary			
CRM Software			
Software	**Hours**	**$**	**Assumptions/Comments**
Sub-Total Software			
Implementation			**Assumptions/Comments**
Implementation			
Project Management			
Training			
Design and Configuration			
Report Development			
Integration			
Travel			
Other Costs			
Sub-Total Implementation			
On-Going			**Assumptions/Comments**
Year 1			
Years 2 through 5			
Years 6 through 10			
Sub-Total On-Going			
Total – All Costs			

Exhibits

Exhibit C – Customer References

Using the template provided, provide references for each software solution proposed, including three current customers. Please include at least three references where your client has integrated this product with back-end systems such as work order or service request systems, GIS, and websites.

CUSTOMER REFERENCES - EXISTING LIVE CUSTOMERS

Item	Vendor Response
Client Reference No. 1 - Existing	
Name	
Number of Employees	
Population	
Contact Name	
Contact Title	
Contact Telephone Number	
Contact E-mail Address	
Products, Modules, Services Provided by Vendor	
First Date of Business Relationship with Vendor	
Go Live Date	
Rationale for including the specific reference	
Client Reference No. 2 - Existing	
Name	
Number of Employees	
Population	
Contact Name	
Contact Title	
Contact Telephone Number	
Contact E-mail Address	
Products, Modules, Services Provided by Vendor	
First Date of Business Relationship with Vendor	
Go Live Date	
Rationale for including the specific reference	
Client Reference No. 3 - Existing	
Name	
Number of Employees	
Population	
Contact Name	
Contact Title	
Contact Telephone Number	
Contact E-mail Address	
Products, Modules, Services Provided by Vendor	
First Date of Business Relationship with Vendor	

Exhibits

Go Live Date	
Rationale for including the specific reference	

Exhibits

Exhibit D – Acceptance of Terms and Conditions of RFP

ACCEPTANCE OF TERMS AND CONDITIONS

It is the intent of the City to contract with a private Vendor. All Vendor representations, whether verbal, graphical or written, will be relied on by the City in the evaluation of the responses to this Request for Proposal. This reliance on the Supplier's represented expertise is to be considered as incorporated into any, and all, formal Agreements between the parties.

PRINT THE WORDS "NO EXCEPTIONS" HERE ______________________________________IF THERE ARE NO EXCEPTIONS TAKEN TO ANY OF THE TERMS, CONDITIONS, OR SPECIFICATIONS OF THESE REQUEST FOR PROPOSAL DOCUMENTS.

IF THERE ARE EXCEPTIONS TAKEN TO ANY OF THESE TERMS, CONDITIONS, OR SPECIFICATIONS OF THESE REQUEST FOR PROPOSAL DOCUMENTS, THEY MUST BE CLEARLY STATED IN THE TABLE BELOW ("RFP EXCEPTIONS") AND RETURNED WITH YOUR PROPOSAL IN THE APPROPRIATE SECTION.

IF YOU PROVIDED A SAMPLE COPY OF YOUR CONTRACT(S) YOU STILL NEED TO IDENTIFY IN THIS DOCUMENT ("RFP EXCEPTIONS") ANY AND ALL EXCEPTIONS YOU HAVE TO THE CITY'S TERMS AND CONDITIONS.

Company	
Authorized Individual Name and Title	
Telephone	
Email	
Address	

AUTHORIZED SIGNATURE

____

DATE ____

<u>OTHER NOTES:</u>

Exhibits

RFP EXCEPTIONS

Add any additional line items for exceptions as necessary and reference any explanatory attachments within the line item to which it refers.

	Reference	Exception	Reason	Alternate Approach
1				
2				
3				
4				
5				

Exhibit E – Non-Collusion Certificate

NON-COLLUSION CERTIFICATE

STATE OF ______________________________)
ss.
COUNTY OF ______________________________)

The undersigned, being duly sworn, deposes and says that the person, firm, association, co-partnership or corporation herein named, has not, either directly or indirectly, entered into any agreement, participated in any collusion, or otherwise taken any action in restraint of free competitive bidding in the preparation and submission of a proposal to the City of Kirkland for consideration in the award of a contract on the improvement described as follows:

CRM Software

____

____
(Name of Firm)

By: ______________________________________
(Authorized Signature)

Title ______________________________________

Sworn to before me this______day of_____________,____ .

Notary Public

CORPORATE SEAL:

Exhibits

Exhibit F – Non-Disclosure Agreement

NONDISCLOSURE AGREEMENT

This Non-Disclosure Agreement ("the Agreement") is made this _____ day of ________, 201__, by and between the City of Kirkland, a municipal corporation of the State of Washington (the "City"), and ________________________ , a __ corporation ("the vendor").

Whereas, the Vendor <is the successful candidate/wishes to submit a proposal>for the <project name>; and

Whereas, the Vendor will need to review confidential information ("the Confidential Information") belonging to the City in order to be able to <prepare its proposal/complete this project>, which the City does not want disclosed; and

Whereas, in consideration for being allowed to see the Confidential Information so that it can prepare a proposal, the sufficiency of such consideration being hereby acknowledged, Vendor is willing to enter into this Non-Disclosure Agreement,

Now therefore, as evidenced by their signatures below, the parties hereby agree as follows:

1. The Vendor shall maintain and protect the confidentiality of the Confidential Information, the Vendor shall not disclose the Confidential Information to any person or entity and shall not challenge, infringe or permit or assist any other person or entity to disclose the Confidential Information or challenge or infringe any of the City's license rights, trade secrets, copyrights, trademarks or other rights respecting the Confidential Information.

2. Except pursuant to a written agreement between the parties, the Vendor shall not directly or indirectly, i) provide, make, use or sell, or permit or assist any other person or entity to provide, make, use or sell any services, devices or products incorporating any protected feature embodied in any of the Confidential Information; ii) apply for or seek to register, or otherwise attempt to create, establish or protect any patents, copyrights or trademarks with respect to any of the Confidential Information; or iii) use any name used by the other party, whether or not subject to trademark protection, or any confusingly similar name.

3. The Vendor shall not disclose the Confidential Information except to those persons employed by the Vendor, or its affiliates or subsidiaries, who have reasonable need to review the Confidential Information under the terms of this Agreement.

4. Vendor shall not make any copies, drawings, diagrams, facsimiles, photographs or other representations of any of the Confidential Information.

5. Upon request by the City, Vendor shall immediately return any Confidential Information in its possession, including all copies thereof.

6. Notwithstanding other provisions of this Agreement, the Agreement does not restrict the Vendor with respect to the use of information that is already legally in its possession, that is available to the Vendor from other sources without violating this Agreement or the intellectual property rights of the City or that is in the public domain. Notwithstanding other provisions of this Agreement, this Agreement also shall not restrict the Vendor from providing, making, using or selling services, devices or other products so long as the Vendor does not breach this Agreement, violate the City's intellectual property rights or utilize any of the Confidential Information.

7. The covenants in this Agreement may be enforced a) by temporary, preliminary or permanent injunction without the necessity of a bond or b) by specific performance of this Agreement. Such relief shall be in addition to and not in place of any other remedies, including but not limited to damages.

8. In the event of a suit or other action to enforce this Agreement, the substantially prevailing party shall be entitled to reasonable attorneys' fees and the expenses of litigation, including attorneys' fees, and expenses incurred to enforce this Agreement on any appeal.

9. The Agreement shall be governed by and construed in accordance with Washington law. The King County Superior Court or the United States District Court for the Western District of Washington at Seattle (if federal law is applicable) shall have the exclusive subject-matter jurisdiction of matters arising under this Agreement, shall have personal jurisdiction over the parties and shall constitute proper venue for any litigation relating to this Agreement.

10. For purposes of this Agreement, all covenants of the Vendor shall likewise bind the officers, directors, employees, agents, and independent contractors of the Vendor, as well as any direct or indirect parent corporation of the Vendor, direct or indirect subsidiary corporations of the Vendor and any other person or entity affiliated with or related to the Vendor or to any of the foregoing persons or entities. The Vendor shall be liable to the City for conduct of any of the foregoing persons or entities in violation of this Agreement to the same extent as if said conduct were by the Vendor.

11. The Vendor shall not directly or indirectly permit or assist any person or entity to take any action which the Vendor would be barred by this Agreement from taking directly.

12. This Agreement shall bind and inure to the benefit of the heirs, successors and assigns of the parties.

IN WITNESS WHEREOF, the parties have duly executed this Agreement on the day and year first written above.

CITY OF KIRKLAND

____
<Company Name>

Exhibits

By:______________________________

Its:______________________________

By:______________________________

Its:______________________________

Exhibits

Exhibit G – City of Kirkland IT Vendor Security Policy and IT Cloud Vendor Security Policy

IT Vendor Security Policy

Scope: This policy applies to all vendors who do any form of work with the City of Kirkland that requires them to log into and utilize networked city systems. This is regardless of who the vendor is and which department they are working for or with. It also applies to staff with other municipal, county, state or federal entities.

Provision: When possible, this policy should be an addendum to existing contracts that require access to City of Kirkland networked systems. It may be signed separately when necessary.

Duration: This policy applies from the time a vendor signs its contract with the city through project completion or support contract termination.

1. Vendors with access to City data or systems shall provide their services in manner consistent with this policy and with standard security and related compliance policies such as PCI and/or HIPPA. If vendors have remote access into systems with City data, vendors shall ensure that the remote access is conducted from IT systems which have the latest security patches, anti-virus updates, and malware signatures using a secure connection (e.g. VPN).

2. Vendors should only expect to be provided with the minimum security levels required for the particular tasks that they are responsible for. Vendors should not anticipate an "always on" connection, and in most cases will have to request that any connection to the city's network be turned on when they need to gain access.

3. Except in the case of an approved security audit and with prior written permission, vendors must not test, or attempt to compromise computer or communication system security measures. Incidents involving unapproved system cracking (hacking), password cracking (guessing), file decryption, software copying, or similar unauthorized attempts to compromise security measures may be unlawful, and will be considered serious violations of City of Kirkland policy. This includes hardware or software tools that could be employed to evaluate or compromise information systems security. Examples of such tools include, but are not limited to, those that defeat software copy protection, discover secret passwords, keyloggers, identify security vulnerabilities, or decrypt encrypted files. Similarly, without this type of approval, vendors are prohibited from using "sniffers" or any other hardware or software that monitors the traffic on a network or the activity on a computer.

4. Vendors shall abide by the following policies for passwords:

   a. Network login passwords must be at least 8 characters long and include at least one number and one capital letter.
   b. Passwords must be changed every 90 days.
   c. The same password cannot be re-used within twenty password changes.

d. Passwords must not be written down or stored in systems except in encrypted applications designed to store passwords.
e. Passwords must not be shared among vendor staff.
f. Vendors should not use the same passwords for city and personal needs.
g. Other password protected systems will comply with above network login password policy when technically possible.

5. Vendors must report all security incidences to the appropriate City of Kirkland IT personnel, including any serious security breaches on their own network during the time they have userid/password access to the City of Kirkland's network within 24 hours of identifying the security incident.

6. City of Kirkland IT will provide an IT point of contact for vendors. This point of contact will liaise with the vendor to ensure they are in compliance with these policies.

7. Vendors working on certain types of systems or with certain data will need to have formal background checks completed. This includes but is not limited to all systems that fall under the purview of the Criminal Justice Information Services policies. It is the responsibility of the City of Kirkland IT to notify vendors who need a background check.

The following signature block must be completed any time that this agreement stands alone and is not a formal addendum to a current contract.

______________________________	______________________________
Signature	Signature
______________________________	______________________________
Name	Name
______________________________	______________________________
City of Kirkland	Organization
______________________________	______________________________
Date	Date

Exhibits

IT Cloud Vendor Security Agreement

This IT Cloud Vendor Security Agreement ("Security Agreement") is entered into by and between the City of Kirkland, ("City"), and __________________ ("Vendor")

Scope: This policy applies to all Vendors who do any form of work ("Contract") with the City of Kirkland that includes possession, storage, processing, or transmission of Personally Identifiable Information (PII), Sensitive Personal Information (SPI) or Personal Health Information (PHI) for City of Kirkland employees, volunteers, contractors, and/or citizens in any location that is outside of the City of Kirkland Firewalls. This includes public and private cloud infrastructures and Vendor's own infrastructure on their premises. This is regardless of who the Vendor is and which department they are working for or with, and it applies to all locations where the Vendor stores information.

If this Contract covers only PII or SPI, then only this addendum must be signed.

If this Contract covers PHI, then this addendum must be signed and a HIPAA Business Associates Agreement must also be signed and incorporated as an addendum to this document or as an addendum to the Contract.

This policy does NOT apply to CJIS data (criminal justice data). There is a separate federally mandated addendum that covers protection of CJIS data, which must also be signed if the Contract includes such information.

Provision: When possible, this policy should be an addendum to existing contracts with vendors. It may be signed separately when necessary.

Duration: This policy applies from the time a vendor signs its Contract with the city through such point in time that all data which was in the vendor's control is returned to the city and destroyed at the city's request, including but not limited to backups, test sites, and disaster recovery sites.

Definitions:

Personally Identifiable Information (PII), or **Sensitive Personal Information (SPI)**: Information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context.

Protected Health Information (PHI): any information about health status, provision of health care, or payment for health care that can be linked to a specific individual, which is more particularly defined under HIPAA (Title 45, CFR) and the Health Care Information Act (RCW Chapter 70.02).

Vendor: Includes owners and employees, volunteers, subsidiaries, and any subcontractors who might reasonably have access to this data.

Options:

Option 1: A vendor can verify that they have a high level of security certification that is satisfactory to the City of Kirkland. Examples include but may not be limited to FedRamp. If this option is selected, print the mutually agreed upon certification level below and attach appropriate documentation:

____

Option 2: Vendors can agree to follow the following security best practices:

1. All customer data will be stored on servers physically located in the United States.
2. All customer data will be stored in a location with reasonable physical controls where data will not be visible to anyone not covered by this policy.
3. Access to data will only be provided on a need to know basis in order for the vendor to complete this work.
4. Data will not be shared with an outside third party without explicit written consent of the city.
5. Data will be encrypted prior to and during any transfer from one location to another.
6. Data will be disposed of appropriately, including shredding or burning of any printed versions and destruction or secure erasure of any electronic medium on which data has been stored.
7. Vendor agrees to the appropriate internal certification for vendor staff who access the data (for example, PHI must only be handled by vendors who have HIPPA training).
8. Vendor staff with access to City of Kirkland data covered by this policy must pass a criminal background check prior to accessing that data.
9. Vendors must perform internal and/or external security auditing on a regular basis that is no less common than once per year.
10. Vendors shall abide by the following policies for passwords:
    a. Network login passwords must be at least 8 characters long and include at least one number and one capital letter.
    b. Passwords must be changed every 90 days.
    c. The same password cannot be re-used within twenty password changes.
    d. Passwords must not be written down or stored in systems except in encrypted applications designed to store passwords.
    e. Passwords must not be shared among vendor staff.
    f. Vendors should not use the same passwords for city and personal needs.
    g. Other password protected systems will comply with above network login password policy when technically possible.
11. Vendors must report all security incidences to the appropriate City of Kirkland IT personnel, including any serious security breaches on their own network, within 24 hours of identifying the security incident.
12. In the event of a data breach, Vendor must have an internal policy to provide for timely forensic investigation of affected and related servers and must follow all state, local, and federal requirements for notifying individual's whose PII or PHI has been or may have been breached.

13. Vendor’s servers must be patched on a regular and timely basis with all security-related patches from application and infrastructure vendors.
14. Data must be kept in at least two different physical locations. One location can be in a compressed format (e.g. as a backup file).
15. Vendor must enable logging as follows:
    a. Logs are enables for common third party applications
    b. Logs are active by default
    c. Logs are available for review by the City of Kirkland for up to one year
    d. Logs are retained for up to one year

Any deviation from the above best practices must be described here and mutually agreed upon (Signatures on this policy will constitute mutual agreement).
Description of any area where vendor is requesting a waiver, an agreement to a different method, or any other change to this policy:

A breach of this Security Agreement also constitutes a breach of any agreement to which it is appended and the City may terminate either or both because of such breach as soon as it must to mitigate that breach or others that may then be apparently forthcoming. The City agrees to work with the Vendor to avoid such termination if reasonably possible but protection of the information held by the Vendor cannot be compromised in the process.

Description of data in the Vendor’s care (attach additional sheets if necessary):

____

____

____

Is this an addendum to an existing or new contract (Y/N): ___
If yes, name and duration of contract: ____

City business person responsible for contract and vendor management:

Name Title Department

City IT person responsible for contract and vendor management:

Name Title Department

Exhibits

The following signature block must be completed. By signing this agreement, vendor warrants that they are responsible for the security of the PII, SPI, and/or PHI in their care.

VENDOR NAME.

Signature

Printed Name

Title

Date

City of Kirkland

Signature

Printed Name

Title

Date