City of Kirkland

Request for Proposal

Payment Services for Utility Billing

Job # 41-22-FA

Issue Date: July 20, 2022
Due Date: August 17, 2022 – 3:00 p.m. (Pacific Time)

REQUEST FOR PROPOSALS

Notice is hereby given that proposals will be received by the City of Kirkland, Washington (City), for:

Payment Services for Utility Billing
Job # 41-22-FA

File with Purchasing Agent, Finance Department, 123 - 5th Ave, Kirkland WA, 98033

Proposals received later than **3:00 p.m. PDT on August 17 2022 will not be considered.**

A copy of this Request for Proposal (RFP) may be obtained from City's web site at http://www.kirklandwa.gov/. Click on the Business tab at the top of the page and then click on the "Opportunities" link found under "Doing Business with the City".

The City reserves the right to reject any and all proposals, and to waive irregularities and informalities in the submittal and evaluation process. This RFP does not obligate the City to pay any costs incurred by proposers in the preparation and submission of a proposal. Furthermore, the RFP does not obligate the City to accept or contract for any expressed or implied services.

A response that indicates that any of the requested information in this RFP will only be provided if and when the proposer is selected as the apparently successful Service Provider is not acceptable, and, at the City's sole discretion, may disqualify the proposal from consideration.

The City requires that no person shall, on the grounds of race, religion, color, national origin, sex, age, marital status, political affiliation, sexual orientation, or the presence of any sensory, mental, or physical disability be excluded from participation in, be denied the benefits of, or be otherwise subjected to discrimination under any program or activity. The City further assures that every effort will be made to ensure non-discrimination in all of its programs and activities, whether those programs are federally funded or not.

In addition to nondiscrimination compliance requirements, a Service Provider ultimately awarded a contract shall comply with federal, state and local laws, statutes and ordinances relative to the execution of the work. This requirement includes, but is not limited to, protection of public and employee safety and health; disabilities; environmental protection; waste reduction and recycling; the protection of natural resources; permits; fees; taxes; and similar subjects.

Dated this 20th Day of July, 2022.

Jay Gewin
Purchasing Agent
City of Kirkland

Published in the Daily Journal of Commerce – July 20th and July 27th of 2022.

City Profile

The City is located in the Seattle metropolitan area, on the eastern shore of Lake Washington and approximately 10 miles east of downtown Seattle. It has a population of approximately 92,175, and is the twelfth largest city in the State of Washington and the sixth largest city in King County, Washington. The City manages approximately 24,500 utility accounts for residential, multi-family, and commercial customers for water, sewer, and garbage/recycling services.

Since its incorporation in 1905, Kirkland has grown in geographic size and now occupies 18 square miles.

Current Process

The current lockbox provider processes approximately 3,750 check payments per month, deposits funds daily into the City's bank account, and submits a file to the City each day of the payments recorded that the City imports into its billing software system.

Scope of Work

The City is soliciting requests for proposals from qualified vendors ("Contractors") to provide payment processing services commonly referred to as Lockbox services for its Utility Billing Division.

The ideal Vendor(s) shall have experience in successfully implementing lockbox solutions at local government or utility agencies of similar size to the City and/or in larger agencies. The successful Vendor shall be responsible for the final City approved implementation including development of system integration and connectivity to existing resources.

The Vendor should have staff available to discuss any customer service concerns during the hours City Hall is open (Monday through Friday, 8 A.M. to 5 P.M.).

It should take no more than typically 3 businesses days to receive and deposit check payments mailed to the Vendor's lockbox facility from Kirkland residents and businesses.

If there are any questions about what utility account a payment should be credited, the lockbox provider will reach out to the City for clarification prior to depositing the check.

The City utility bills give customers the opportunity to donate to a charity through a program called "Kirkland Cares". Customers donate funds in addition to their utility bill that is noted by the lockbox contractor so it can be tracked separately in accounting.

General Technical/Information Technology Requirements

The City's Information Technology department will conduct a security review prior to the contract being signed.

The Vendor will be required to adhere to the technological requirements described below, and should describe their technical methodology in their proposal:

- The proposed system meets regulatory requirements such as PCI and other applicable State/Federal laws
- Vendor will provide prompt notice to the City of any confirmed or suspected security breaches. Notice will be provided by e-mail and telephone to the City's primary IT and business contacts.
- The City requires that our data remains our property and must be managed in accordance with the records laws of the State of Washington.
- Vendor's policy for securely managing personal data and sharing of data with any 3rd party sources.
- Describe the process we would follow to get the daily file for import into our utility billing software (Accela – Springbrook).

Supplier agrees to comply with all provisions of the current City of Kirkland security agreements (e.g., IT Cloud Vendor Security Agreement, IT Non-Disclosure Agreement and the IT Vendor/Consultant Network Access Agreement), published by the Department of Information Technology as are pertinent to Supplier's operation. These are shown in Attachment B.

Contract Requirements and Fees

If your proposal is accepted, the following fees and requirements will be due upon award, prior to issuance of a contract:

1. **Compliance with Law/City of Kirkland Business License**
    - Contractor must obtain and provide a copy of a City of Kirkland Business License and otherwise comply with Kirkland Municipal Code Chapter 7.02.
    - The Contractor shall comply with all applicable State, Federal and City laws, ordinances, regulations, and codes.

2. **Insurance**
   Contractor's insurance should be consistent with the requirements found in the sample agreement shown as Attachment A.

Term of Contract

This agreement will be for a period of three (3) years, with a City option to renew for one additional two-year period. The Director of Finance and Administration shall make the determination of contract renewal.

The City reserves the right to cancel the contract upon 60 days written notice to the Contractor.

Contract

The contract shall consist of the following documents: The Request for Proposals (RFP), the accepted proposal, a Professional Services Agreement (see Attachment A), the IT Security Agreements (see Attachment B) and any agreed upon written changes to any of the foregoing documents. The contract documents are complimentary and what is called for in any one document shall be binding as if called for by all.

Process Schedule

The City will attempt to follow this timetable, which should result in the full implementation of an agreement by November 1, 2022.

Issue RFP	July 20, 2022
Deadline for questions	August 2, 2022 no later than 5PM
Responses to questions posted	August 8, 2022
Deadline for submittal of proposals	August 17, 2022 no later than 3PM
Interviews (if needed) Week of	August 28, 2022
Selection of successful proposal	September 7, 2022
Agreement for services signed	September 21, 2022
Implementation of services	November 1, 2022

These dates are estimates and subject to change by the City.

Requirements of the Proposal

Please include the following broad topics in presenting your proposal, and refer to Attachment C for additional specific information that should be included:

- **Experience** - Summarize experience relevant to the services requested.
- **Method of Service Provision** - Describe method of service delivery, approach, and what makes you unique with respect to providing the identified needs of the City. Please see Attachment C for an inclusive list of the information that should be included.
- **Proposed Fee Structure** - Identify your proposal regarding compensation. Also, describe what expenses would be charged to the City. Please include all items and services that could be utilized by the City on an as-needed basis.
- **Statement of Contract Compliance** - Discuss how your insurance meets the City's requirements as Identified in Attachment A. Also identify any suggested changes in the attached contract.
- **References** - Identify four references who can attest to your experience and capabilities as they relate to services requested. The references must include contact name, address, e-mail address, and telephone number.
- **Acceptance of Terms and Conditions**
- **Non-collusion certificate**
- **Non-disclosure agreement**

Evaluation Procedures

A committee of City Staff will evaluate the submitted proposals. The evaluators will consider how well the proposer's proposed methodology and deliverables meet the needs of the City as described in the proposer's response to each requirement of the proposal. It is important that the responses be clear and complete so that the evaluators can adequately understand all aspects of the proposal. The evaluation process is not designed to simply award the contract to the lowest cost proposer. Rather, it is intended to help the City select the proposer with the best combination of attributes, including price, based on the evaluation factors.

The City will evaluate all proposals received under this solicitation using the following points system:

Completeness of proposal submitted	0-10
References	0-10
Demonstrated ability to provide requested services	0-20
Experience	0-20
Proposed compensation and contract terms	0-40
TOTAL	100

Selection Process

A selection committee will review all proposals, select finalists and may conduct interviews prior to making the final selection of the contractor.

Prior to the commencement of work, the City and the selected contractor will meet to settle contract details. A notice to the consultant of the City's award will constitute notice to proceed. The City is not responsible for any costs incurred by the contractor in the preparation of the proposal. Once submitted to the City, all proposals will become public information.

Proposal Submittal Instructions

Please note: The following general requirements are mandatory for all proposals. Proposals submitted after the deadline date and time or lacking one or more of the following requirements will not be accepted.

1. **Proposals must be submitted by e-mail and be received no later than 3:00 pm PST on August 17, 2022.**
2. E-mailed proposals should include "Payment Services for Utility Billing– Job #41-22-FA" in the subject line and be addressed to purchasing@kirklandwa.gov .
3. All proposals sent electronically must be in the form of a PDF or MS Word document and cannot exceed 20MB.
4. All proposals must include the legal name of the organization, firm, individual or partnership submitting the RFP. Include the address of the principal place of business, mailing address, phone numbers, emails, fax number (if one exists) and primary contact person.

5. To be evaluated, a proposal must address all requirements and instructions contained within.
6. Provide all references and materials required by the RFP instructions within.

Questions: Questions regarding the scope of work or evaluation process must be submitted in writing by 5:00 PM on August 2, 2022 and should be addressed to Tim Hanser, at thanser@kirklandwa.gov.

Questions regarding the RFP process should be addressed to Jay Gewin, Purchasing Agent, at jgewin@kirklandwa.gov.

Terms and Conditions

A. The City reserves the right to reject any and all proposals, and to waive minor irregularities in any proposal.

B. Proposers responding to this RFP must follow the procedures and requirements stated in the RFP document. Adherence to the procedures and requirements of this RFP will ensure a fair and objective analysis of your proposal. Failure to comply with or complete any part of this RFP may result in rejection of your proposal.

C. The City reserves the right to request clarification of information submitted, and to request additional information on any proposal.

D. The City reserves the right to award any contract to the next most qualified agency, if the successful agency does not execute a contract within 30 days of being notified of selection.

E. Any proposal may be withdrawn up until the date and time set above for opening of the proposals. Any proposal not so timely withdrawn shall constitute an irrevocable offer, for a period of one hundred and twenty (120) days to sell to the City the services described in the attached specifications, or until one or more of the proposals have been approved by the City administration, whichever occurs first.

F. The contract resulting from acceptance of a proposal by the City shall be in a form supplied or approved by the City and shall reflect the specifications in this RFP. A copy of the City's standard Professional Services Agreement is available for review (see attachment A). The City reserves the right to reject any proposed agreement or contract that does not conform to the specifications contained in this RFP and which is not approved by the City Attorney's office.

G. The City shall not be responsible for any costs incurred by the agency in preparing, submitting or presenting its response to the RFP.

H. Any material submitted by a proposer shall become the property of the City. Materials submitted after a contract is signed will be subject to the ownership provision of the executed contract.

I. The City reserves the right not to award any portion or all of the project if it finds that none of the proposals submitted meets the specific needs of the project. The City reserves the right to modify the scope of work and award portions of this RFP to the selected vendor. The City reserves the right to award this work to multiple vendors if the scope of work would be best completed by multiple vendors and their associated experience.

Cooperative Purchasing

Chapter 39.34 RCW allows cooperative purchasing between public agencies in the State of Washington. Public agencies which have filed an Intergovernmental Cooperative Purchasing Agreement with the City may purchase from City contracts, provided that the contractor agrees to participate. The City does not accept any responsibility for contracts issued by other public agencies, however.

Public Disclosure

Once submitted to the City, proposals shall become the property of the City, and all proposals shall be deemed a public record as defined in "The Public Records Act," chapter 42 section 56 of the RCW. Any proposal containing language which copyrights the proposal, declares the entire proposal to be confidential, declares that the document is the exclusive property of the proposer, or is any way contrary to state public disclosure laws or this RFP, could be removed from consideration. The City will not accept the liability of determining what the proposer considers proprietary or not. Therefore, any information in the proposal that the proposer claims as proprietary and exempt from disclosure under the provisions of RCW 42.56.270 must be clearly designated as described in the "Proprietary Material Submitted" section above. It must also include the exemption(s) from disclosure upon which the proposer is making the claim, and the page it is found on must be identified. With the exception of lists of prospective proposers, the City will not disclose RFP proposals until a bid selection is made. At that time, all information about the competitive procurement will be available with the exception of: proprietary/confidential portion(s) of the proposal(s), until the proposer has an adequate opportunity to seek a court order preventing disclosure. The City will consider a proposer's request for exemption from disclosure; however, the City will make a decision predicated upon RCW 42.56.

OWMBE Participation

The City encourages OWMBE firms to submit qualifications and encourages all firms to team with OWMBE firms in their pursuit of this project.

Federal Debarment

The Bidder shall not currently be debarred or suspended by the Federal government. The Bidder shall not be listed as having an "active exclusion" on the U.S. government's "System for Award Management" database (www.sam.gov).

RFP EXCEPTIONS

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

	RFP Section # or Form, Page #	Exception Describe the nature of the Exception	Explanation of Why This is an Issue for You	Your Proposed Alternative to Meet the Needs of the City
1				
2				
3				
4				
5				

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:

Printing, Mailing, and Payment Services – Utility Billing

_____

_____
(Name of Firm)

By: _____
(Authorized Signature)

Title _____

Sworn to before me this_____day of_____,_____ .

Notary Public

CORPORATE SEAL:

The City of Kirkland, Washington, a municipal corporation ("City") and _____, whose address is _____ ("Consultant"), agree and contract as follows.

In consideration of the mutual benefits and conditions set forth below, the parties agree as follows:

I. SERVICES BY CONSULTANT

A. The Consultant agrees to perform the services described in Attachment _ to this Agreement, which attachment is incorporated herein by reference.

B. All services and duties shall be conducted and performed diligently, completely and in accordance with professional standards of conduct and performance.

II. COMPENSATION

A. The total compensation to be paid to Consultant for these services shall not exceed $_____, as detailed in Attachment _____.

B. Payment to Consultant by the City in accordance with the payment ceiling specified above shall be the total compensation for all services performed under this Agreement and supporting documents hereto as well as all subcontractors' fees and expenses, supervision, labor, supplies, materials, equipment or the use thereof, reimbursable expenses, and other necessary incidentals.

C. The Consultant shall be paid on the basis of invoices submitted. Invoicing will be on the basis of percentage complete or on the basis of time, whichever is applicable in accordance with the terms of this Agreement.

D. The City shall have the right to withhold payment to Consultant for any services not completed in a satisfactory manner until such time as Consultant modifies such services to the satisfaction of the City.

E. Unless otherwise specified in this Agreement, any payment shall be considered timely if a warrant is mailed or is available within 45 days of the date of actual receipt by the City of an invoice conforming in all respects to the terms of this Agreement.

III. TERMINATION OF AGREEMENT

The term of this agreement shall commence on the date this agreement is fully executed and shall continue for one (1) year after the date hereof. This agreement shall automatically renew for an additional year unless either party notifies the other in writing at least thirty (30) days prior to such automatic renewal that the party does not wish to renew this agreement. The City may terminate the agreement after the first year with a ninety (90) day written notice.

IV. OWNERSHIP OF WORK PRODUCT

A. Ownership of the originals of any reports, data, studies, surveys, charts, maps, drawings, specifications, figures, photographs, memoranda, and any other documents which are developed, compiled or produced as a result of this Agreement, whether or not completed, shall be vested in the City. Any reuse of these materials by the City for projects or purposes other than those which fall within the scope of this Agreement or the project to which it relates, without written concurrence by the Consultant will be at the sole risk of the City.

B. The City acknowledges the Consultant's plans and specifications as instruments of professional service. Nevertheless, the plans and specifications prepared under this Agreement shall become the property of the City upon completion of the services. The City agrees to hold harmless and indemnify consultant against all claims made against Consultant for damage or injury, including defense costs, arising out of any reuse of such plans and specifications by any third party without the written authorization of the Consultant.

C. Methodology, materials, software, logic, and systems developed under this Agreement are the property of the Consultant and the City, and may be used as either the consultant or the City sees fit, including the right to revise or publish the same without limitation.

D. The Consultant at such times and in such forms as the City may require, shall furnish to the City such statements, records, reports, data, and information as the City may request pertaining to matters covered by this Agreement. All of the reports, information, data, and other related materials, prepared or assembled by the Consultant under this Agreement and any information relating to personal, medical, and financial data will be treated as confidential only as allowed by Washington State laws regarding disclosure of public information, Chapter 42.56 RCW

The Consultant shall at any time during normal business hours and as often as the City may deem necessary, make available for examination all of its records and data with respect to all matters covered, directly or indirectly, by this Agreement and shall permit the City or its designated authorized representative to audit and inspect other data relating to all matters covered by this Agreement. The City shall receive a copy of all audit reports made by the agency or firm as to the Consultant's activities. The City may, at its discretion, conduct an audit, at its expense, using its own or outside auditors, of the Consultant's activities which relate, directly or indirectly, to the Agreement.

Consultant will provide all original operation and maintenance manuals, along with all warranties, from the manufacturer for any equipment or items installed or supplied to the City has part of this contracted project.

The Consultant shall maintain accounts and records, including personnel, property, financial, and programmatic records, which sufficiently and properly reflect all direct and indirect costs of any nature expended and services performed pursuant to this Agreement. The Consultant shall also maintain such other records as may be deemed necessary by the City to ensure proper accounting of all funds contributed by the City to the performance of this Agreement.

The foregoing records shall be maintained for a period of six years after termination of this Agreement unless permission to destroy them is granted by the Office of the Archivist in accordance with RCW Chapter 40.14 and by the City.

V. GENERAL ADMINISTRATION AND MANAGEMENT

The Finance and Administration Department for the City of Kirkland shall review and approve the Consultant's invoices to the City under this Agreement, shall have primary responsibility for overseeing and approving services to be performed by the Consultant, and shall coordinate all communications with the Consultant from the City.

VI. COMPLETION DATE

The estimated completion date for the Consultant's performance of the services specified in Section I is _____.

Consultant will diligently proceed with the services contracted for, but consultant shall not be held responsible for delays occasioned by factors beyond its control which could not reasonably have been foreseen at the time of the execution of this Agreement. If such a delay arises, Consultant shall forthwith notify the City.

VII. SUCCESSORS AND ASSIGNS

The Consultant shall not assign, transfer, convey, pledge, or otherwise dispose of this Agreement or any part of this Agreement without prior written consent of the City.

VIII. NONDISCRIMINATION

Consultant shall, in employment made possible or resulting from this Agreement, ensure that there shall be no unlawful discrimination against any employee or applicant for employment in violation of RCW 49.60.180, as currently written or hereafter amended, or other applicable law prohibiting discrimination, unless based upon a bona fide occupational qualification as provided in RCW 49.60.180 or as otherwise permitted by other applicable law. Further, no person shall be denied or subjected to discrimination in receipt of the benefit of any services or activities made possible by or resulting from this Agreement in violation of RCW 49.60.215 or other applicable law prohibiting discrimination.

IX. HOLD HARMLESS/INDEMNIFICATION

To the greatest extent allowed by law the Consultant shall defend, indemnify and hold the City, its officers, officials, employees and volunteers harmless from any and all claims, injuries, damages, losses or suits including attorney fees, arising out of or in connection with performance of this Agreement, except for injuries and damages caused by the sole negligence of the City.

Should a court of competent jurisdiction determine that this Agreement is subject to RCW 4.24.115, then, in the event of liability for damages arising out of bodily injury to persons or damages to property caused by or resulting from the concurrent negligence of the Consultant and the City, its officers, officials, employees, and

volunteers, the Consultant's liability hereunder shall be only to the extent of the Consultant's negligence. It is further specifically and expressly understood that the indemnification provided herein constitutes the Consultant's waiver of immunity under Industrial Insurance, Title 51 RCW, solely for the purpose of this indemnification. This waiver has been mutually negotiated by the parties. The provisions of this section shall survive the expiration or termination of this Agreement.

X. LIABILITY INSURANCE COVERAGE

The Consultant shall procure and maintain for the duration of the Agreement, insurance against claims for injuries to persons or damage to property which may arise from or in connection with the performance of the work hereunder by the Consultant, its agents, representatives, or employees. A failure to obtain and maintain such insurance or to file required certificates and endorsements shall be a material breach of this Agreement.

Consultant's maintenance of insurance as required by the agreement shall not be construed to limit the liability of the Consultant to the coverage provided by such insurance, or otherwise limit the City's recourse to any remedy available at law or in equity.

A. Minimum Scope of Insurance

Consultant shall obtain insurance of the types described below:

1. Automobile Liability insurance covering all owned, non-owned, hired and leased vehicles. Coverage shall be as least as broad as Insurance Services Office (ISO) form CA 00 01 or a substitute form providing equivalent liability coverage. If necessary, the policy shall be endorsed to provide contractual liability coverage.

2. Commercial General Liability insurance shall be as least as broad as ISO occurrence form CG 00 01 and shall cover liability arising from premises, operations, stop-gap independent contractors and personal injury and advertising injury. The City shall be named as an additional insured under the Consultant's Commercial General Liability insurance policy with respect to the work performed for the City using an additional insured endorsement at least as broad as ISO CG 20 26.

3. Workers' Compensation coverage as required by the Industrial Insurance laws of the State of Washington.

4. Professional Liability insurance appropriate to the Consultant's profession.

5. Network Security (Cyber) and Privacy Insurance shall include, but not be limited to, coverage, including defense, for the following losses or services:

   Liability arising from theft, dissemination, and/or use of City confidential and personally identifiable information, including but not limited to, any information about an individual maintained by or on behalf of the City, including (i) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place

of birth, mother's maiden name, or biometric records; and (ii) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information regardless of how or where the information is stored or transmitted.

Network security liability arising from (i) the unauthorized access to, use of, or tampering with computer systems, including hacker attacks; or (ii) the inability of an authorized Third Party to gain access to supplier systems and/or City Data, including denial of service, unless caused by a mechanical or electrical failure; (iii) introduction of any unauthorized software computer code or virus causing damage to the City or any other Third Party Data.

Lawfully insurable fines and penalties resulting or allegedly resulting from a Data breach.

Event management services and first-party loss expenses for a Data breach response including crisis management services, credit monitoring for individuals, public relations, legal service advice, notification of affected parties, independent information security forensics firm, and costs to re-secure, re-create and restore Data or systems.

For purposes of this insurance subsection, the terms Third Party and Data are defined in Section XI.

B. **Minimum Amounts of Insurance**

Consultant shall maintain the following insurance limits:

1. Automobile Liability insurance with a minimum combined single limit for bodily injury and property damage of $1,000,000 per accident.

2. Commercial General Liability insurance shall be written with limits no less than $1,000,000 each occurrence, $2,000,000 general aggregate.

3. Professional Liability insurance shall be written with limits no less than $1,000,000 per claim and $1,000,000 policy aggregate limit.

4. Network Security (Cyber) and Privacy Insurance shall be written with limits no less than $1,000,000 per claim, $2,000,000 policy aggregate for network security and privacy coverage, $100,000 per claim for regulatory action (fines and penalties), and $100,000 per claim for event management services

C. **Other Insurance Provisions**

The insurance policies are to contain, or be endorsed to contain, the following provisions for Automobile Liability and Commercial General Liability insurance:

1. The Consultant's insurance coverage shall be primary insurance as respects the City. Any insurance, self-insurance, or self-insured pool coverage

maintained by the City shall be excess of the Consultant's insurance and shall not contribute with it.

2. The Consultant shall provide the City and all Additional Insureds for this services with written notice of any policy cancellation, within two business days of their receipt of such notice.

D. **Acceptability of Insurers**

Insurance is to be placed with insurers with a current A.M. Best rating of not less than A:VII.

E. **Verification of Coverage**

Consultant shall furnish the City with original certificates and a copy of the amendatory endorsements, including but not necessarily limited to the additional insured endorsement, evidencing the insurance requirements of the Consultant before commencement of the services.

F. **Failure to Maintain Insurance**

Failure on the part of the Consultant to maintain the insurance as required shall constitute a material breach of agreement, upon which the City may, after giving five business days' notice to the Consultant to correct the breach, immediately terminate the agreement or, at its discretion, procure or renew such insurance and pay any and all premiums in connection therewith, with any sums so expended to be repaid to the City on demand, or at the sole discretion of the City, offset against funds due the Consultant from the City.

G. **City Full Availability of Consultant Limits**

If the Consultant maintains higher insurance limits than the minimums shown above, the City shall be insured for the full available limits of Commercial General and Excess or Umbrella liability maintained by the Consultant, irrespective of whether such limits maintained by the Consultant are greater than those required by this agreement or whether any certificate of insurance furnished to the City evidences limits of liability lower than those maintained by the Consultant.

XI. SAFEGUARDING OF PERSONAL INFORMATION

A. **Definitions.** The following definitions shall have the assigned meaning for this section.

1. "Data" means all information, whether in oral or written (including electronic) form, created by or in any way originating with City and End Users, and all information that is the output of any computer processing, or other electronic manipulation, of any information that was created by or in any way originating with City and End Users, in the course of using and configuring the Services provided under this Agreement as described in Attachment A, and includes City Data, End User Data, and Personal Information.

2. **"Data Compromise"** means any actual or reasonably suspected unauthorized access to or acquisition of computerized Data that compromises the security, confidentiality, or integrity of the Data, or the ability of City to access the Data.
3. **"End User"** means the individuals (including, but not limited to employees, authorized agents, students and volunteers of City; Third Party consultants, auditors and other independent contractors performing services for City; any governmental, accrediting or regulatory bodies lawfully requesting or requiring access to any Services; customers of City provided services; and any external users collaborating with City) authorized by City to access and use the Services provided by Consultant under this Agreement.
4. **"Third Party"** means persons, corporations and entities other than Consultant, or any of their employees, contractors or agents.

B. The Consultant shall not use or disclose Personal Information, as defined in RCW 19.255.010, in any manner that would constitute a violation of federal law or applicable provisions of Washington State law. Consultant agrees to comply with all federal and state laws and regulations, as currently enacted or revised, regarding Data security and electronic Data interchange of Personal Information.

The Consultant shall ensure its directors, officers, employees, subcontractors or agents use Personal Information solely for the purposes of accomplishing the services set forth in the Agreement.

The Consultant shall protect Personal Information collected, used, or acquired in connection with the Agreement, against unauthorized use, disclosure, modification or loss.

The Consultant and its sub-consultants and agents agree not to release, divulge, publish, transfer, sell or otherwise make Personal Information known to unauthorized persons without the express, prior written consent of the City or as otherwise authorized by law.

The Consultant agrees to implement physical, electronic, and managerial policies, procedures, and safeguards to prevent unauthorized access, use, or disclosure of Personal Information.

The Consultant shall make the Personal Information available to amend as directed by the City and incorporate any amendments into all the copies maintained by the Consultant or its subcontractors and agents. Consultant shall certify its destruction after ninety (90) calendar days and the Consultant shall retain no copies. If Consultant and City mutually determine that return or destruction is not feasible, the Consultant shall not use the Personal Information in a manner other than those permitted or authorized by state and federal laws.

The Consultant shall notify the City in writing immediately upon becoming aware of any unauthorized access, use, or disclosure of Personal Information. Consultant shall take necessary steps to mitigate any harmful effects of such use or disclosure. Consultant is financially responsible for notification of any unauthorized access, use or disclosure. The details of the notification must be approved by the City. Any breach of this clause may result in immediate termination of the Agreement by the City and the demand for return of all Personal Information.

Consultant agrees that prior to the Effective Date of this Agreement, Consultant will, at its expense, conduct or have conducted within the last 12 months, the following, and thereafter, Consultant will at its expense conduct or have conducted the following at least once per year, and immediately after any actual or reasonably suspected Data Compromise:

- A PCI, SOC 2 or other mutually agreed upon audit of Consultant's security policies, procedures and controls;
- A vulnerability scan, performed by a Third Party scanner, of Consultant's systems and facilities that are used in any way to deliver services under this Agreement as described in Attachment A; and,
- A formal penetration test, performed by a process and qualified personnel, of Consultant's systems and facilities that are used in any way to deliver services under this Agreement as described in Attachment A.

The same will be evidenced by providing the City a copy of the Successful Audit Letter and a Scope of Audit Document (outlining what is included in the audit). Audit Report will not include "private" information, defined as proprietary environment/infrastructure detail not specific to systems that process or transmit City Data.

Consultant to comply with PII (Personally Identifiable Information) or SPI (Sensitive Personal Information) by signing **Attachment B** 'IT Cloud Vendor Security Agreement' agreeing to follow security best practices.

XII. COMPLIANCE WITH LAWS/BUSINESS LICENSE

The Consultant shall comply with all applicable State, Federal, and City laws, ordinances, regulations, and codes. Consultant must obtain a City of Kirkland business license or otherwise comply with Kirkland Municipal Code Chapter 7.02.

XIII. FUTURE SUPPORT

The City makes no commitment and assumes no obligations for the support of Consultant activities except as set forth in this Agreement.

XIV. INDEPENDENT CONTRACTOR

Consultant is and shall be at all times during the term of this Agreement an independent contractor and not an employee of the City. Consultant agrees that he or she is solely responsible for the payment of taxes applicable to the services performed under this Agreement and agrees to comply with all federal, state, and local laws regarding the reporting of taxes, maintenance of insurance and records, and all other requirements and obligations imposed on him or her as a result of his or her status as an independent contractor. Consultant is responsible for providing the office space and clerical support necessary for the performance of services under this Agreement. The City shall not be responsible for withholding or otherwise deducting federal income tax or social security or for contributing to the state industrial insurance of unemployment compensation programs or otherwise assuming the duties of an employer with respect to the Consultant or any employee of Consultant.

XV. EXTENT OF AGREEMENT/MODIFICATION

This Agreement, together with all attachments and addenda, represents the final and completely integrated Agreement between the parties regarding its subject matter and supersedes all prior negotiations, representations, or agreements, either written or oral. This Agreement may be amended only by written instrument properly signed by both parties.

XVI. ADDITIONAL WORK

The City may desire to have the Consultant perform work or render services in connection with the project other than provided for by the express intent of this Agreement. Any such work or services shall be considered as additional work, supplemental to this Agreement. This Agreement may be amended only by written instrument properly signed by both parties.

XVII. NON-ENDORSEMENT

As a result of the selection of a consultant to supply services to the City, the consultant agrees to make no reference to the City in any literature, promotional material, brochures, sales presentation or the like without the express written consent of the City.

XVIII. NON-COLLUSION

By signature below, the Consultant acknowledges 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 or submission of a proposal to the City for consideration in the award of a contract on the specifications contained in this Agreement.

XIX. WAIVER

Waiver by the City of any breach of any term or condition of this Agreement shall not be construed as a waiver of any other breach.

XX. ASSIGNMENT AND SUBCONTRACT

The Consultant shall not assign or subcontract any portion of the services contemplated by this Agreement without the prior written consent of the City.

XXI. DEBARMENT

Recipient certifies that it is not suspended, debarred, proposed for debarment, declared ineligible or otherwise excluded from contracting with the federal government, or from receiving contracts paid for with federal funds.

XXII. SEVERABILITY

Any provision or part of the Agreement held to be void or unenforceable under any law or regulation shall be deemed stricken. Unless such stricken provision goes to the essence of the consideration bargained for by a party, all remaining provisions

shall continue to be valid and binding upon the parties, and the parties agree that the Agreement shall be reformed to replace such stricken provision or part thereof with a valid and enforceable provision that comes as close as possible to expressing the intention of the stricken provision.

XXIII. GOVERNING LAW AND VENUE

This Agreement shall be interpreted in accordance with the laws of the State of Washington. The Superior Court of King County, Washington, shall have exclusive jurisdiction and venue over any legal action arising under this Agreement.

XXIV. DISPUTE RESOLUTION

All claims, counterclaims, disputes, and other matters in question between City and Consultant arising out of or relating to this Agreement shall be referred to the City Manager or a designee for determination, together with all pertinent facts, documents, data, contentions, and other information. The City Manager or designee shall consult with Consultant's representative and make a determination within thirty (30) calendar days of such referral. No civil action on any claim, counterclaim, or dispute may be commenced until thirty (30) days following such determination.

XXV. EFFECTIVE DATE

This Agreement shall be deemed effective on the last date signed below.

IN WITNESS WHEREOF, the parties hereto have executed this Agreement on the dates written below:

CONSULTANT:	CITY OF KIRKLAND:
Signature: _____	Signature: _____
Printed Name: _____	Printed Name: _____ (Type City Staff Name)
Title: _____	Title: _____
Date: _____	Date: _____

Attachment B

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 SOC2 and 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 incidents 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 enabled 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

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.	City of Kirkland
Signature	Signature
Printed Name	Printed Name
Title	Title
Date	Date

NON-DISCLOSURE 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/partnership/limited liability company, etc.> ("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 ("Confidential Information[1]") 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 or complete the project>, the sufficiency of such consideration being hereby acknowledged, the 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, 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 who have agreed to be bound the terms of this Agreement or a similar agreement that is at least as protective of the Confidential Information as provided for herein.

[1] "Confidential Information" means the information the City has provided the Vendor by or at the direction of the City, or to which access was provided to the Vendor by or at the direction of the City, in the course of the Vendor's wish to submit a proposal or complete this project.

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 destroy or 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 Vendor, its officers, agents and employees, agrees to hold harmless, indemnify and defend at its own expense the City, its officers, agents and employees, from and against any and all claims of any kind whatsoever arising out of the Vendor's intentional acts or negligent failure to perform any of its obligations under this Agreement.

8. 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.

9. 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.

10. 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.

11. 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.

12. 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.

13. 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>

By:_____ By:_____

Its:_____ Its:_____

VENDOR NETWORK ACCESS AGREEMENT

This Agreement ("Agreement") related to network access is made between the City of Kirkland, Washington, a municipal corporation ("City") and _____, ("Vendor"), whose address is _____, and shall be effective upon the date last signed below.

WHEREAS, the Vendor requires access to the City's network to perform certain pre-approved network operations services through separate contract, which may include product installation, updates, configuration, and troubleshooting; and;

WHEREAS, the Vendor will be provided a City network login account(s) for Authorized Employees[2] for pre-approved City work.

NOW, THEREFORE, in consideration of the mutual commitments contained herein, and in support of those included within the separate contract between the City and the Vendor providing for the provision of such pre-approved City work, attached hereto as Attachment __, the parties agree as follows:

1. The Vendor agrees that all Authorized Employees will abide by the City's Technology Resource Usage Policy, Attachment __ to this Agreement and the City's Technology Security Policy, Attachment __ to this Agreement.
2. The Vendor agrees that if an account is assigned to a single or multiple Authorized Employee(s), all those with access to this account are held accountable under this Agreement.
3. The Vendor agrees that all remote access will be monitored by the responsible City staff member for the duration of the Vendor login session unless other City-approved arrangements have been made.
4. The Vendor agrees that remote access into systems with City data is conducted from IT systems which have the latest security patches, anti-virus updates, and malware signatures using a secure connection (e.g., VPN (using GlobalProtect), Microsoft Teams).
5. The Vendor agrees that they should only expect to be provided levels of access as required and appropriate for the assigned tasks, as determined by City staff.
6. The Vendor agrees that they must report all security incidents to the appropriate City of Kirkland IT personnel, including any serious security breaches on their own network during the time they have user-id/password access to the City's network, within 2 hours of identifying the security incident.
7. The Vendor agrees that, depending on the City systems and/or data they are working with, formal background checks may be required. This includes but is not limited to all systems that fall under the purview of the Criminal Justice Information Services (CJIS) policies.

[2] "Authorized Employees" means the Vendor's employees who need to access the City's network to perform work (including, but not limited to product installation, updates, configuration, troubleshooting, etc.) requested by the City

8. The Vendor agrees that, except in the case of an approved security audit and with prior written permission from the City, the Vendor must not test, or compromise City computer or communication system security measures by any means, including but not limited to unapproved system cracking (hacking), password cracking (guessing), file decryption, software copying, or similar unauthorized attempts. Such measures may be unlawful as well as serious violations of City 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 prior approval from the City, the Vendor is prohibited from using "sniffers" or any other hardware or software that monitors the traffic on a network or the activity on a computer.
9. The City agrees that they will provide an IT point of contact for the Vendor. This point of contact will liaise with the Vendor to help ensure they are in compliance with these policies and respond to other issues that may arise related to remote access.
10. The City agrees to provide the Vendor with the required remote access to the City's network.

IN WITNESS WHEREOF, the parties hereto have executed this Agreement on the dates written below:

_____	_____
Signature	Signature
_____	_____
Name	Name
_____	_____
City of Kirkland	Organization
_____	_____
Date	Date

Technology Resource Usage Policy
Chapter 7, Records & Information
Policy 7-1

Effective Date: May 11, 2016

PURPOSE:

This policy is designed to protect the integrity and security of the City of Kirkland's information technology resources and the data which is in the City's care. The City of Kirkland authorizes the use of computing and network resources by City officials, staff, contractors, volunteers and others to carry out legitimate City business. All users of City computing and network resources shall do so in an ethical, legal, and responsible manner. All use of technology resources must be consistent with all City policies and work rules.

GOAL:

To establish and document the acceptable and appropriate use of computer and information systems, networks and other technology resources at the City of Kirkland, and to address the protection of data in the City's possession. This policy describes the appropriate use of technology provided by the City.

SCOPE:

Defines appropriate use of the City of Kirkland network, computers, all related peripherals, software, electronic communications, and Internet access, whether accessed directly from the City's network or from another location. Applies to use of the City's network and technology resources at any location, from any City-owned device or personal device that has been granted access to the City's network. Applies to all users of City technology resources regardless of employment status.

In order to be granted access to networks and related resources, staff must be familiar with this policy and associated work rules.

Technology Security Policy
Chapter 7, Records & Information
Policy 7-4
Effective Date: February 10, 2014 (Revised)

PURPOSE:

This policy is designed to protect the integrity, availability, and confidentiality of information held by the City of Kirkland and to protect Information Technology (IT) assets from unauthorized use or modification and from accidental or intentional damage or destruction. It includes the security of IT facilities and off-site data storage; computing, telecommunications, city data, and applications related services purchased from other government agencies or commercial concerns; and internet-related applications and connectivity.

GOAL:

To be effective, information security must be a team effort involving the participation and support of every individual who deals with City of Kirkland information and/or information systems.

SCOPE:

This policy applies to all city offices, departments, officials, employees and all system users (such as contractors, consultants, temporary employees, interns and volunteers).

This policy applies to all computer and network systems (portable and fixed) owned by and/or administered by the City of Kirkland. Similarly, this policy applies to all platforms (operating systems), all computer sizes (smart-phones through mainframes), and all application systems (whether developed in-house or purchased from third parties).

DEFINITIONS:

Information security is defined as the ability to manage access to and rights related to City of Kirkland systems, data, and technology assets. This includes access by city staff, IT department staff, vendors, citizens, and unrelated actors such as people attempting to gain unauthorized access for any reason.

REFERENCES:

This Technology Security Policy is complemented by Administrative Policy 7-1: Technology Use Policy.

POLICY:

Security

1. Onsite Network Access

a. Direct network access may be provided to staff, volunteers, on-call employees, and elected or appointed officials as needed to allow them to perform their work duties.
b. All staff provided such access must read and agree to follow this policy.
c. The following permissions are required for access to specific systems:
    i. General network and email access for staff or volunteers must be approved by a direct Supervisor, Manager, or Director. For Directors, Elected or Appointed Officials, permission must be granted by the City Manager's Office. Permission may be requested via email to helpdesk@kirklandwa.gov.
    ii. Requests for access to business systems must also be approved by the associated business system owner.
d. Changes in permission require the same approval as initial granting of permission.
e. Direct access by any other party (such as a vendor) is generally not allowed except as needed to maintain IT systems or for the performance of city business. Such access requires the permission of a Manager or Director in the IT Department.
f. All accounts will be audited at by IT at least once a year.

2. Remote Network Access for Staff

a. Remote access includes any network access that requires a username/password including network access via virtual private network from a city or an approved and appropriately licensed personal computer and access from mobile devices including tablet devices and mobile phones.It is preferred that city staff use a maintained, city owned computer (check out laptops) to access the city network.
b. Remote access to the city network via staff's personal computer may be provided to staff for short or long-term periods. Approval is required

from the staff member's manager and from the IT department. Only IT approved hardware/software VPN connections will be allowed.

c. Any employee connecting to the city network on their personal devices via VPN must have current anti-virus software installed on their device that is appropriate to the device. This is the employee's responsibility as the city has no direct way to audit this.
d. User-owned mobile devices, such as cellular telephones or tablets, will not be granted access to any city systems except those provided by Outlook such as email and calendaring.
e. Devices that are lost or stolen must be reported to the IT Service Desk as soon as possible. Such devices may be wiped (all data may be remotely removed from the device). This applies to personal and city-owned devices that access City data. If the City wipes a device, personal data and information may also be lost.

3. Vendor Access

If a vendor desires remote access they must be referred to the IT department, and their access will be governed by the IT Security Policy for Vendors.

4. Connection to External Networks

City of Kirkland system users must not establish any connections between the City of Kirkland network and external networks (including Internet Service Providers) unless these connections have been approved by IT.

5. Password Controls

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 as authorized by IT.
e. Passwords must not be shared.
f. Personnel with Administrative accounts must use a different password from their regular user account.
g. Users should not use the same passwords for city and personal needs.

h. Other systems with their own internal password controls will comply with above network login password policy when technically possible.

6. Physical Access Controls

Users of individual and shared PC's are responsible to make sure that no unauthorized users may access the PC. That means that when leaving a PC for any length of time, users are required to place that PC into a state where an approved City of Kirkland network username and password are required to use the PC. Two ways to achieve this are to lock the PC using "Ctrl-Alt-Del" and selecting "Lock Computer" or logging off the PC. This applies to desktop and portable PC's.

Automatic Screen Locking – All City computers (including but not limited to PC's, laptops and workstations) automatically go into a password-protected screen lock mode after fifteen (15) minutes of inactivity. Mobile devices also require a screen-lock; the timing may vary due to device or business limitations.

7. External Data Storage Media

External data storage is defined as physical media such as CD's, thumb drives, portable drives, portable backup units, and internet-based or "cloud" based storage (e.g. dropbox).

a. In general, no City data shall be stored on external data storage except to such extent that it is required to perform a job function and has been approved by IT. An example of approved use is that IT carries thumb drives to support software installations in certain cases, or a PowerPoint presentation may need to be delivered to the place where it will be presented.
b. City data must only be stored on devices that are owned and managed by the city. For example:
    i. An internet-based storage account may be set up with a city email account and used for city data as needed with IT approval.
    ii. A thumb drive may be purchased with City funds and used as needed or checked out from the IT department for short-term needs.
c. In no case should City and personal data be comingled except as allowed under the Technology Use Policy. .

d. External data storage is only to be used for backup and recovery purposes with IT permissions.

All data must be wiped from external storage media as soon as it is no longer required (in accordance with public records retention laws).

8. Miscellaneous other security provisions

a. Access to critical and/or sensitive information must be physically and/or logically restricted to those with a need-to-know.
b. Paper documents that contain information that could jeopardize system security must be locked away in appropriate containers (safes, file cabinets, etc.) when not in use and properly disposed of (shredded) when deemed out of date or no longer required by retention requirements.
c. System users 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. Likewise, short-cuts bypassing systems security measures, as well as pranks and practical jokes involving the compromise of systems security measures are absolutely prohibited. This also 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, identify security vulnerabilities, or decrypt encrypted files. Similarly, without this type of approval, system users are prohibited from using "sniffers" or any other hardware or software that monitors the traffic on a network or the activity on a computer.
d. Staff will not provide vendors access to the network via their own network login accounts.

Procedures

1. Information Technology Steering Team

a. Review proposed changes to organization-wide information security standards, guidelines, and procedures and provide input to the Information Technology Department.
b. Assist in adherence to security policies within departments.

2. Information Technology Department

a. Review all IT security policies at least once every two years and recommend appropriate updates to the Information Technology Steering Team.
b. Communicate security policies to City offices and departments.
c. Manage the IT infrastructure in accordance with best practice security policies for items like SPAM control and virus protection.
d. Offer training for City staff on adopted security policies through regularly scheduled security awareness training.
e. Review logs and perform other maintenance and monitoring to ensure that attacks against City systems are identified, tracked, avoided and defeated.
f. Investigate system intrusions and other information security incidents. Report out on investigations as appropriate.
g. Patch server operating systems and desktop operating systems as prudent to avoid significant and verified security holes in applications or systems.

3. System Owners

All system owners (includes IT staff and department/office staff that have specific duties as business system owners) will:

a. Approve all access to data, processes, and utilities in systems that they own.
b. Refine and evaluate system security at least once a year, including review of all levels of access for all users of the system.
c. Inform system users of security requirements for each specific system.

d. Provide any training necessary or answer questions to make sure end users understand the security policy and make recommendations to IT and/or department directors to improve security.

ENFORCEABILITY:

The City of Kirkland Information Technology Department reserves the right to revoke the system privileges of any user at any time for violation of this policy. Violations of this policy may result in discipline up to and including termination.

Attachment C

Lockbox Services Questions/Statements to be Included in Proposals

This RFP process seeks to find the best overall lockbox solution for the City for this investment. The award shall be made to the qualified Vendor whose proposal is most advantageous to the City with price and other factors considered. Other factors that may contribute to the selection process include but are not limited to the following:

- Project approach and understanding of the City's objectives and requirements
- Supplier's implementation methodology and implementation success
- Vendor's experience providing lockbox services for customers of similar size to Kirkland
- Feedback from customer references
- Compliance with the City's terms and conditions
- Ability to integrate with other City systems and adhere to City's technological requirements
- Cost and quality of ongoing maintenance and support

Responses Requested (in the same numerical format)

1. Provide the names of individuals, with phone numbers and e-mail addresses, who will be working on the proposed services and their areas of responsibility including their specific experience relative to the request for proposal requirements.

2. Submit at least four (4) references (preferably from current local government or utility customers) who can attest to the lockbox provider's experience as it relates to providing lockbox services. The references must include contact name, title, address, e-mail address, telephone number and services used.

3. Provide a description of the following key items:
   A. Time and frequency of pickups
   B. Turn-around processing time
   C. Deposit deadlines
   D. Ability to provide images of remittance documents and checks via web and/or CD ROM.
   E. Acceptance criteria for payments
   F. Rejection criteria for payments
   G. Method and time of data transmissions
   H. Location of post office box
   I. Location of lockbox office
   J. Ability to return original documents of all business license and false alarm submissions
   K. Method and time of delivery for returning original documents to the City
   L. Ability for the City to determine appropriate batch size and batch numbering system
   M. Treatment of exceptions (non-standard) items

N. Ability to handle payments containing multiple remittance advices
O. Technical specifications of transmission of data to the City
P. Error tolerance of lockbox personnel and subcontractors
Q. Bonding requirements of lockbox personnel and subcontractors

4. Describe how inquires requiring research and adjustments are handled by the institution. Are there established turn-around times for research and adjustment items? If yes, specify.

5. Security/Protection Measures: What security features are in place to minimize the risk of unauthorized transactions?

6. Service Enhancements: Describe any enhancements, technological or otherwise, that we should consider to improve operational or cash management efficiencies.

7. Discuss your use of the internet in providing services to your municipal/business customers.

8. Provide information on how your institution plans to keep your product line competitive. Describe what approach you are taking in the development of new services.

9. Disaster Recovery:
    a. Describe your institution's formal disaster recovery plan.
    b. How quickly will back-up facilities be activated?
    c. Describe your institution's operating capabilities to assist the City in the event of a disaster or declared emergency.

10. Implementation Plan: Describe the implementation plan you would coordinate with the City, including timetable.

11. List the address and hours of operation at your lockbox office.

12. Discuss any special conditions, other fees, other services, or deviations from the requested scope.