City of Kirkland

Request for Proposals

Multi-factor Authentication (MFA) Solution and Professional Services for Implementation

Job # 28-22-IT

Issue Date: April 26th, 2022
Due Date: May 18th, 2022 - 5:00 p.m. (Pacific Time)

REQUEST FOR PROPOSALS

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

Multi-factor Authentication (MFA) Solution and
Professional Services for Implementation
Job # 28-22-IT

File with Financial Operations Manager, Finance Department, 123 - 5th Ave, Kirkland WA, 98033

Proposals received later than **5:00 p.m. on May 18th, 2022 will not** be considered.

A copy of this Request for Proposals (RFP) and supporting documents 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 Request for Proposals link found under "Doing Business with the City".

The City of Kirkland reserves the right to reject 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 respondents 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 Service Provider response that indicates that any of the requested information in this RFP will only be provided if and when the Service Provider 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 of Kirkland assures that no person shall, on the grounds of race, 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 of Kirkland further assures that every effort will be made to ensure non-discrimination in all its programs and activities, whether those programs are federally funded or not.

In addition to nondiscrimination compliance requirements, the Service Provider(s) 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; environmental protection; waste reduction and recycling; the protection of natural resources; permits; fees; taxes; and similar subjects.

Dated this 26th day of April, 2022

Jay Gewin
Purchasing Agent
425-587-3123
City of Kirkland

Published in the Seattle Times on April 26th and May 3rd

Definitions

For the purposes of this RFP, the following definitions apply:

- **Multi-factor Authentication (MFA)** is the practice of requiring multiple means of verifying the identity of a user, such as a combination of a password and a Personal Identification Number (PIN) code taken from an app or a physical token.
- **Cloud Service** or **Cloud Service Subscription** or **Software-as-a-Service (SaaS)** or **SAAS** or **Hosted Vendor** means the subscription to use the MFA Solution functions, data security, data privacy, service level agreements, support, and maintenance including Version Updates.
- **Version Updates** means updates to the MFA Solution whether minor enhancements, major enhancements, planned maintenance, or emergency fixes.
- **API** means Application Programming Interface and is a set of routines, protocols, and tools for building software applications. An API specifies how software components interact. APIs are used with programming graphical user interface (GUI) components for configuring.
- **Customization** means development of software code.
- **Configuration** means setting up data, templates, workflows, screen forms, reports or other parts of the MFA solution and for the avoidance of doubt does not include the development of software code.

Background Information

The City of Kirkland, Washington, is 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 over 92,000 and is the twelfth largest city in the State of Washington and the sixth largest city in King County, Washington.

Since its incorporation in 1905, Kirkland has grown in geographic size and now occupies 18 square miles. The city employs over 600 regular employees.

Kirkland operates under a Council-Manager form of government. The City Council is the policy-making branch of Kirkland's government and consists of seven members elected at large to staggered, four-year terms. The Mayor is elected from within the Council. The City Council is supported by several advisory boards and commissions and the City Manager. The City Manager is appointed by the City Council and serves as the professional administrator of the organization, coordinating its day-to-day activities.

About the IT Department

1. The City is growing an IT Security Program that includes implementing an MFA solution.
2. The IT Department has 25 staff, of which there are 4 network staff (including 1 manager) and 1 Information Systems Security Officer.
3. Total count of technicians administering the MFA solution will be around 10.
4. There are approximately 800 end users that will use this solution.

One of the items on the roadmap for the Security Program is implementing MFA. The primary objectives of an MFA solution include the following:

- Improve the City's cybersecurity posture by reducing the risk of network account breaches.
- Deliver an MFA solution that requires minimal customization and ongoing maintenance.
- Provide knowledge transfer and training to staff administering the MFA system.
- Build meaningful reports and dashboards.

The City's network is comprised of approximately 160 Microsoft Windows servers split between an on-premise environment of redundant HCIs (Hyperconverged Infrastructure) utilizing VMWare and Microsoft's Azure IaaS (Infrastructure as a Service) platform. The two environments are configured as one network and utilize Microsoft's Express Route for connectivity, with a backup VPN connection. The network infrastructure consists of Cisco routers and switches with Palo Alto firewalls on-premise and in Azure. The City uses Microsoft's Office 365 platform for Exchange, SharePoint, OneDrive and Teams.

The City's telephony system is a Cisco VoIP solution supporting over 700 telephony devices (phone, ATAs, voice gateways, etc.) It includes voice mail, ACD queues, and E911.

Purpose and Background

The purpose of this request is to learn how well suited your firm's commercial MFA Solution meets the City's requirements and implementation needs. The City expects to evaluate on-premise MFA Solutions and Cloud Service (SaaS) MFA Solutions. At the City's sole discretion, the City may or may not award a contract from this RFP process.

Minimum Qualifications

- For the Firm:
  - Previous experience as a commercial provider for an MFA Solution.
  - Professional services experience in implementing the MFA Solution.
- For the Project Manager:
  - Previous professional services experience implementing a similar sized MFA Solution for a City similar in size to Kirkland within the last 3 years.
- For the MFA Solution:
  - The MFA Solution must ensure single sign-on with Active Directory and Azure Active Directory.
  - The MFA Solution must ensure that the City's data is not hosted offshore or transmitted unencrypted.

Scope of Work

The scope includes the MFA Solution and professional services for implementation assistance. The City has limited funding and expects using the MFA Solution out of the box with minimal

configuration and customization. The City is planning on providing an implementation manager and a technical lead. Other City staff may be utilized as needed. The implementation assistance includes guidance and knowledge transfer using out of the box configuration, templates, workflows, and APIs. Further, the City expects the commercial provider to provide overall guided assistance, configuration (including, but not limited to altering, reporting and dashboards), training, readiness, production launch support, focused 30-day stabilization, and ongoing service/support for the MFA Solution. The City expects to prepare the IT staff for the change. The approach is to deploy to all City staff, vendors and contractors with network login accounts. The City expects professional services assistance to be remote using online methods.

In Scope for Commercial Provider

- Overall implementation consultation and guidance.
- General Configuration and Knowledge Transfer.
- Single Sign On (SSO) with the City's Active Directory Configuration and Azure Active Directory.
- Functional Configuration (based on Attachment A requirements) and Knowledge Transfer.
- Reporting, dashboards, and Configuration and Knowledge Transfer.
- MFA Solution Orientation/Overview, Online Help, and Training.
- Guides, formats and consultation for preparation for configuration or API.
- Collect all appropriate data from the City's technical infrastructure, and setup and configure alerting and dashboards.
- Support plan with thirty (30) day stabilization period with daily minor configuration corrections.
- Performance testing of MFA Solution including the City's setup, configuration, alerting and dashboards.
- Responsible for readiness, transition, production launch and handover to support.

Out of Scope for Commercial Provider

- Traditional project management.
- Extensive customization to MFA Solution.
- IT business processes, customized business rules, standard operating procedure documentation, service level agreement documentation, or the City's performance metrics.
- Onsite presence or travel expenses.

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 B.

Budget and Timeline

- The proposer should propose what scope is possible with a budget of up to $350K (including tax). Items in this budget include, but are not limited to, the following:
  - First year MFA solution costs and recurring fees or annual maintenance fees for a period of 3 years.
  - Hardware tokens.
  - Professional services assistance for implementation during the first year after contract execution.
- The proposer should include an implementation timeline/schedule.

Evaluation Process and Selection of Proposals

Proposals are evaluated for the MFA Solution based on the MFA solution's ability to meet the City's requirements response in Attachment A. If the City chooses to include orals (interviews and demonstrations), the evaluation is further based on the MFA Solution demonstration, which shall be unscripted.

Proposals are evaluated for professional services based on both the firm and individual team member's experience and expertise on similar projects. Further, the team/firm's capacity (personnel and other resources) to complete the project within the proposed schedule. Factors considered in the evaluation of the Scope submitted include:

1. Responsiveness of the written proposal to the purpose and scope;
2. Qualifications of key individuals in terms of what personnel will be committed to this project and what their qualifications are in implementing the MFA solution;
3. Cost/Budget;
4. Ability and history of successfully completing contracts of this type, meeting projected deadlines and experience in similar work;
5. Orals.

The City selects based on the evaluation of the written proposals and orals. The City may elect to interview some or all proposers. Written proposals and orals will be evaluated based on the following criteria:

- MFA Solution Requirements and Agreement Suitability – 30%
- Implementation Methodology Plan – 25%
- Price – 25%
- References and professional expertise – 20%

A selection committee will evaluate each submitted written proposal and each oral session, to determine the proposal that is most advantageous to the City based on the evaluation process

and evaluation criteria outlined in this RFP. Should the City decide to contract, the contract award is to the highest ranked proposer for the solution type selected by the City.

The contract shall be firm/fixed based on the deliverables of each phase. A cost proposal is required as part of the submission. During the final selection process, the City will discuss available project funds and a firm scope of work that will obtain the City's objectives within the funds available.

Submission Criteria

All proposals must include the following items as related to the scope of this RFP:

1. Submit your firm's size, total revenue, background and experience.
2. Submit individual team member resumes.
3. Submit three (3) professional references.
4. Complete the requirements response in Attachment A.
5. Submit implementation methodology and plan for the phases in the scope section. Optional: provide improvements to the phased approach your firm would implement.
6. Submit current SOC 2 Compliance report.
7. Provide a cost proposal based on the implementation methodology and deliverables in a firm/fixed format. Include on-going support/maintenance.

	Year 1	**Year 2**	**Year 3**
Select one or more solutions for pricing			
On-Premise Solution	$	$	$
Cloud Service Subscription	$	$	$
Hybrid Solution (On-Premise/Cloud)	$	$	$
Professional Services			
Implementation Assistance	$	$	$

8. Provide your firms licensing/subscription agreement(s).
9. Provide your recommended statement of work for professional services assistance using the proposed methodology and with clearly defined responsibilities.

Proposal Submission 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 received no later than 5:00 PM on May 18, 2022 (Pacific Time).**
2. Emailed proposals should include, "MFA Solution and Professional Services – Job # 28-22-IT" 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. If paper proposals are being submitted, they must consist of four copies in a sealed envelope or box. The City must receive any paper submittal by 5:00 PM on May 18, 2022, and any delivery received after the deadline will be rejected. These can be mailed or delivered to:

   City of Kirkland
   ATTN: Purchasing staff – MFA Solution Job # 28-22-IT
   123 5th Avenue
   Kirkland, WA 98033
5. 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, phone numbers, emails, fax number (if one exists) and primary contact person.
6. Complete, sign and submit all RFP forms provided by the Department.
7. To be evaluated, a proposal must address all requirements and instructions contained within.
8. 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 and should be addressed to Donna Gaw, Information Systems Security Officer, at dgaw@kirklandwa.gov . Questions regarding the RFP process should be addressed to Purchasing staff, at purchasing@kirklandwa.gov. Questions must be submitted before 5:00 PM on May 6, 2022

Submittal Deadlines

April 26th, 2022	Release RFP
May 6th, 2022	Proposer questions due – 5:00 PM PDT
May 12th, 2022	Answers to RFP questions posted on website
May 18th, 2022	Proposals Due by 5:00 PM PDT
If the City decides to proceed:	
June 3rd, 2022	Notify proposers of demonstrations and orals
Week of June 20th, 2022	Demonstrations and Orals (remote)

If the City decides to proceed:
June 29th, 2022 Notify selected proposer

Contract

The Consultant and the City will execute an Agreement for Multi-factor Authentication (MFA) Solution and Professional Services for Implementation (Attachment B).

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 B). 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.

J. The City will require the successful respondent sign a Nondisclosure Agreement (Attachment C).

K. The City will require the successful respondent sign a Vendor Network Access Agreement (Attachment D).

L. The following City policies that are referenced in Attachment D to this RFP, are attached as follows – the Technology Resource Usage Policy (Attachment E) and the Technology Security Policy (Attachment F).

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 consultant 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.

DBE Participation

The City encourages DBE firms to submit qualifications and encourages all firms to team with DBE 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).

Attachment A

Requirements

The City has documented its requirements for the MFA solution. The City desires a right-sized solution and will establish a priority based on responses. **Please complete a response for each requirement in the spreadsheet associated with this RFP called "RFP_MFA Requirements".**

Response and Instructions

The response columns are C through G.

- Column C ("Response")
  - Complete a brief description indicating how the solution meets the requirement.
  - If the requirement is met by custom development, note the impact to support and version updates.
- Columns D thru G ("How the Requirement is Met")
  - Place an X in accordance with the definitions below. Put one single X for each requirement. If the requirement is both Current Capability or Configurable Item AND Custom, explain in column C.
  - Mark an X for every requirement.
  - If there is no X indicated for the requirement, the City will assume 'Not Available'.

Response Option	Definition
Column D: Current Capability or Configurable Item	Requirement will be met by using a feature that is installed and operational in other agencies or businesses and can be demonstrated to the City of Kirkland and is included in the cost of the base package.
Column E: Future Release	Requirement will be met by a future release of the product and is included in the cost of the base package (if not please indicate in the Response column).
Column F: Custom Development	Requirement will be met by packaged software currently under development, in beta test, or not yet released. This is an additional cost.
Column G: Not Available	Requirement cannot be provided either as part of the baseline solution or as a future enhancement.

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 City or the Consultant may terminate or suspend this Agreement at any time, with or without cause, by giving ten (10) days' notice to the other in writing. In the event of termination, all finished or unfinished reports, or other material prepared by the Consultant pursuant to this Agreement, shall be provided to the City. In the event the City terminates prior to completion without cause, consultant may complete such analyses and records as may be necessary to place its files in order. Consultant shall be entitled to receive just and equitable compensation for any satisfactory services completed on the project prior to the date of termination, not to exceed the payment ceiling set forth above.

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 seven 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 Information Systems Security Officer 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 November, 2022.

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 Contractor 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 Contractor and the City, its officers, officials, employees, and volunteers, the Contractor's liability hereunder shall be only to the extent of the Contractor's negligence. It is further specifically and expressly understood that the indemnification provided herein constitutes the Contractor'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 CITY DATA

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 ___, 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 Contractor 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 notify the City in writing immediately upon becoming aware of any unauthorized access, use, or disclosure of City Data. 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 City Data.

C. 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 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 ___; and,
- A formal penetration test, performed by a process and qualified personnel, of Contractor's systems and facilities that are used in any way to deliver services under this Agreement as described in Attachment ___.

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.

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: _____

This Non-Disclosure Agreement ("the Agreement") is made this _____ day of _____, 20__, 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 for the Multi-Factor Authentication (MFA) Solution and Professional Services for Implementation; and

Whereas, the Vendor will need to review confidential information ("the Confidential Information") belonging to the City in order to implement the MFA Solution, which the City does not want disclosed; and

Whereas, in consideration for being allowed to see the Confidential Information so that it can implement the MFA Solution, 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>

By:_____ By:_____

Its:_____ Its:_____

VENDOR NETWORK ACCESS AGREEMENT Attachment D

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[1] 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

[1] "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

systems that fall under the purview of the Criminal Justice Information Services (CJIS) policies.

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 **Attachment E**
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.

REFERENCES:

Administrative Policy 7-4. Technology Security Policy (Attachment F to this document)

POLICY:

Summary

1. The City provides network, communications systems, software, equipment and devices ("technology resources") to carry out legitimate City business. By using the City's technology resources, an employee or other user granted access via being given a user name and user-selected/password to the system understands they are required to disclose the contents of any data files, information and communications created on, stored on, transmitted, received or exchanged via the City's network, communications systems, equipment or devices.

2. There is no right to privacy in the use of City technology resources. By using the City's technology resources an employee understands the City will monitor, record, and review the use of that technology resource.

3. Users are expected to act lawfully, ethically and professionally, and to exercise common sense.

4. Users granted access to critical and/or sensitive data are responsible for its protection.

5. Incidental use for personal needs is allowed as long as that activity does not interfere with City business or conflict with any City policy or work rule. This does not confer a right to download software for personal use, or to load or use personal entertainment such as music files on City computers. Users are expected to respect the business need for available Internet bandwidth and not to run streaming sites steadily across the City's network for non-business purposes such as music, news, sports, or interactive online gaming.

6. Transmission, distribution, or storage of any information or materials in violation of federal, state or municipal law is prohibited. Software that is copyrighted or licensed may not be shared or illegally distributed. Copyright violations are federal offenses that may result in civil and criminal penalties to employees and the City of Kirkland.

7. Users must manage their electronic documents in accordance with records retention policies and procedures as defined and identified by the City Clerk's Office. Documents past their retention schedules should be deleted from the network to save space and eliminate the need to backup unnecessary files.

Personal Use

Technology resources may be used for incidental personal needs as long as such use does not result in or subject the City to additional cost or liability, interfere with business, productivity or performance, pose additional risk to security, reliability or privacy, cause or tend to cause damage to the City's reputation or credibility, or conflict with the requirements of any City policy or work rule. Personal usage should generally conform to limits typically associated with personal phone calls. This document does not attempt to address every possible situation that may arise. Professional judgment, etiquette, and common sense shall be exercised while using City technology resources. Technology resources may not be used to facilitate operation of a private business, consulting, to promote religious causes or non-City sanctioned charitable solicitations, or for political activity.

City staff may use their own personal computers and/or phones to access the public side of our wireless network and connect to the Internet for reasonable personal use. Examples of reasonable use include accessing social network sites at lunch or checking email. The public network is NOT secure and thus there is risk associated with using it for online transactions like banking (similar to the risks associated with using any free public Internet connection for the same thing). The wireless network does not have adequate resources for constant streaming media use like Internet radio. Such connections should be intermittent and in keeping with professional standards.

Internet/Intranet Usage

1. Access to reporting is provided to Directors to help them monitor their staff's use of the Internet as circumstances warrant.

2. Use of the Internet, as with use of all technology resources, should conform to all City policies and work rules. Filtering software will be actively used by the City to preclude access to inappropriate web sites

unless specific exemptions are granted as a requirement of work duties (e.g., police have the ability to access sites on criminal activity, weapons, etc.). Attempts to alter or bypass filtering mechanisms are prohibited.

3. Downloading and installing software (for City business use) from the Internet requires permission from staff on the Information Technology Service Desk, in the Applications Division, or from an IT Manager. Downloading and installing software for personal use is prohibited.

4. Except for City business related purposes (such as police investigations), visiting or otherwise accessing the following types of sites is prohibited:

    a. "Adult" or sexually-oriented web sites.

    b. Sites associated with hate crimes or violence.

    c. Sites that would create discomfort to a reasonable person in the workplace.

    d. Any gaming sites including gambling sites.

5. Social media may be an effective tool to promote community engagement and employees may want to participate in social media via blogging, discussion forums, wikis, mashups, social networking, message boards, e-mail groups and other media.

6. Employees may not set up or brand any Web 2.0 technologies as belonging to, supported by, or approved by the City of Kirkland (for example, a social networking site for a Board or Commission) without express written permission from IT and from their own Department Director and meeting all of the expectations defined by Policy 7-5.

7. Due to band-width limitations, use of the City's network to download *non-business* related multimedia information is prohibited.

Examples include streaming video of baseball games, streaming audio of radio programs, MP3 files and on-line games. Specific examples include Pandora, Google Play, and iTunes software, unless approved for use with a City-owned iPhone (and loading of iTunes music libraries on City computers is prohibited for any personal use). These items should also not be saved on City network drives.

8. E-mail content must be consistent with the same standards expected in any other form of written or verbal communication occurring in a business setting where documents are subject to public disclosure.

9. Electronic communication systems are best suited for routine topics, not for high-level policy issues. Avoid use of electronic communication for sensitive personnel-related or legal matters when possible.

10. Members of bargaining units should not use electronic communications for confidential bargaining unit messages or to transact internal bargaining unit business other than for incidental use as approved by the Human Resources Director.

11. Users must manage their e-mail in accordance with records retention policies and procedures as defined and identified by the City Clerk's Office.

12. Retention of personal email should be minimized, and no data restores or IT resources will be engaged to recover personal email "lost" in City systems.

13. It is the obligation of the user to guard against copyright infringement by paying careful attention to what is received and sent by means of file attachments. If materials are received which may constitute copyright infringement, do not distribute the file or execute associated programs. Contact the Information Technology Service Desk immediately and report the possible copyright infringement.

14. Staff communicating to distribution lists of 50 or more recipients should utilize an approved listserv technology. Even if the email addresses are posted in the "bcc" section, email with a large number of recipients typically gets caught in spam filters and may not reach its intended audience.

15. The City provides staff access to and support for the Exchange/Outlook messaging (e-mail) system. Access or usage of any other messaging system is not allowed unless it is web-based. Subject to the personal use limitations explained above, staff may access web-based personal email *but should not download personal documents or attachments from these sites*. Employees may not install client based software for Internet service on City equipment. Examples: AOL, Instant Messaging.

16. The City provides the ability to send secure (encrypted) email messages to email recipients outside of the organization. Staff may use secure email with approval from IT Management and from their own Department Director or Manager. The use of secure email is restricted to messages that would be prohibited from disclosure by law.

17. Users should be attentive to emails that have unusual or questionable subject lines or an unknown sender. This helps to mitigate spam, phishing and script born viruses that come into the network through email attachments or by clicking on links that lead to hostile web sites. If you suspect phishing or script born viruses in email attachments, delete the email. If you do open any email or attachments which raise suspicions, please contact the Service Desk immediately.

18. The use of e-mail to send or solicit the receipt of inappropriate content such as sexually oriented materials, hate mail, content that a reasonable person would view as obscene, harassing or threatening and having no legitimate or lawful purpose, or contents falling within the inappropriate categories for Internet usage is prohibited, regardless of whether such email is humorous or attempting to be humorous.

19. The use of City email for engaging in political campaigns or activities is prohibited.

20. The City maintains an email group called "ALL" which will send email to all regular users of the City's email system. This should be used sparingly, and according to the guidelines below:

    a. In general, "ALL" email should not include pictures or graphics. If there is a graphic component to a message, post the actual information on Kirknet in the HUB or in Announcements (whichever is appropriate), and include a link in your "ALL" email.

    b. "ALL" emails should generally only be sent twice for each City sponsored event such as diversity and wellness events and transportation programs:

        i. Once to announce the event (including a link to more information available on the Intranet or to where people can subscribe for more information).

        ii. Once on the day of the event as a reminder.

    c. Post-event information such as winners or drawings etc. should be posted on Kirknet. Emails should only be sent to the affected individuals.

    d. Directors or the City Manager's Office may authorize the use of "ALL" email at any time. "ALL" email thus authorized should contain information that might be of use to all City employees. For example, announcements of all-City meetings from the CMO.

    e. IT will use "ALL" emails for systems outages that may require some action by the users in order to save their data, such as an email or file server or major system outage that occurs during normal working hours (other system related information should

be posted on the Intranet in Announcements).

f. "ALL" emails may be used for emergency management purposes at the direction of any Director, the PIO, the OEM, or the Incident Commander.

g. "ALL" emails may be sent to announce training that all employees are expected to attend.

h. Inappropriate uses of "ALL" Email include:

   i. Lost and found, available food, tickets or other items for sale, and car lights-on messages. Instead, use the appropriate alternative group. For example, the CITY HALL group is appropriate for light-on outside the City Hall building. For-sale items should be posted in the Moss Bay section of the Intranet, and shouldn't be advertised through use of email at all.

   ii. General information or compassionate causes should not be sent using email outside of your own department (employees are encouraged to post this kind of information on the HUB, which is a section of our Intranet).

   iii. Jokes and other information not related to City business.

   iv. Publishing vacation schedules.

   v. Forwarding warnings about computer viruses or attacks that have not been verified by IT.

i. Do not use "Reply All" when replying to an "ALL" email.

Systems and Data Security

All City staff with access to systems or data owned by the City are expected to abide by the Information Systems Technology Security Policy (Attachment F).

Administration, Reporting and Violations/Discipline

The Information Technology Department, all City Departments, and Human Resources Department share responsibility for enforcing the Technology Resource Usage Policy.

1. Information Technology Department Responsibilities:
    a. The Information Technology Department is responsible for recommending policy guidelines.

    b. The Information Technology Department is responsible for enterprise monitoring of technology resources using security and monitoring tools. This includes running the software which provides the Internet usage monitoring and reporting to departments that Directors can access at will. The Information Technology Department is not responsible for actual review of the report data on any regular basis, but may randomly and reasonably review this reporting to ensure organizational compliance with these policies.

    c. If, in the normal course of business activities, the Information Technology Department discovers violations of this policy, the Information Technology Department will report the activities to the employee's supervisor, Director of HR, and/or to the City Manager depending upon the severity of the infraction.

    d. The Information Technology Department will make training on these policies available periodically and anytime on request.

2. Department Responsibilities:
    a. Departments assist in the development, adoption, and update of this policy through the Information Technology Steering Team.

    b. If, in the course of normal business activities, department management suspects an employee has or is violating this policy, such a violation may be the subject of evaluation and progressive discipline up to and including termination.

3. Human Resources Department Responsibilities
    a. Human Resources is responsible for integrating this policy into new hire orientation and training.

    b. In conjunction with the Department, Human Resources is responsible for the coordination of any progressive disciplinary actions in response to violations.

    c. As with any set of policies or rules, exceptions may be granted and documented on a case-by-case basis. These require authorization from the Department involved as well as from the Information Technology Department. Some exceptions may also require City Manager approval.

Technology Security Policy **Attachment F**
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 Resource Usage Policy (Attachment E to this document)

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.