City of Kirkland

Request for Proposals

Managed Detection and Response (MDR) Solution and Professional Services for Implementation and Security Services

Job # 09-26-IT

Issue Date: March 11, 2026
Due Date: March 30, 2026

REQUEST FOR PROPOSALS

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

Managed Detection and Response (MDR) Solution and Professional Services for Implementation and Security Services

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

Proposals received later than **4:00 p.m. on March 30, 2026 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". Certain supporting documents contain sensitive information and will only be released upon receipt of a fully executed Non-Disclosure Agreement (NDA). The NDA template is provided as Attachment B to this RFP. Proposers must submit a signed NDA to Duy (Bobby) Huynh, Technical Project Manager, at bhuynh@kirklandwa.gov, and copy Jacinda Guild, Purchasing Agent, at jguild@kirklandwa.gov, prior to accessing these materials.

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.

If the proposer omits the requested information, at the City's sole discretion, the City may disqualify the proposal from consideration.

The City of Kirkland assures that no person shall, on the grounds of race, color, national origin, or sex 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 11th day of March 2026

Jacinda Guild
Purchasing Agent
City of Kirkland

Background Information

The City of Kirkland is located on the eastern shore of Lake Washington. It is a suburban city, surrounded by other suburban cities and pockets of unincorporated King County. The City is near several major transportation routes including Interstate 405, State Route 520, and Interstate 5. These routes connect the City economically and socially to the greater Seattle area.

At the time of incorporation in 1905, the City of Kirkland's population was approximately 530. The current population is 97,850 and Kirkland is the thirteenth largest city in the State of Washington and the sixth largest in King County.

Since its incorporation, Kirkland has grown in geographic size to eighteen square miles - approximately twenty times its original size. This growth occurred primarily through the consolidation of the cities of Houghton and Kirkland in 1968, the annexations of Rose Hill and Juanita in 1988 and the annexation of North Juanita, Finn Hill, and Kingsgate areas in 2011.

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 a new MDR solution.
2. The IT Department has 32 staff, of which there are 3 network staff and one security analyst.
3. Total count of technicians using the MDR solution will be around 5.
4. There are approximately 1500 IT configuration items/nodes.

The City's network is comprised of 1GB and 10GB ethernet with fiber service to all city buildings, approximately 180 Microsoft Windows servers, a small amount of LINUX and is split between an on-premises 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-premises and in Azure. The City uses Microsoft 365 platform for Email, SharePoint, OneDrive, Copilot and Teams. We use Microsoft defender EDR.

The City's telephony system is a Cisco VoIP solution supporting over 800 telephony devices (phone, ATAs, voice gateways, etc.). It includes voice mail, ACD queues, and E911.

Purpose of Request

The purpose of this request is to learn how well suited your firm's commercial MDR Solution meets the City's requirements and implementation needs. The City expects to evaluate solution for Managed Detection and Response (MDR) combined with services which include, but not limited to, PCI Compliance Assessment, Penetration Testing, Tabletops Exercise, IT Policy Review, etc. At the City's sole discretion, the City may or may not award a contract from this RFP process.

Definitions

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

- **Managed Detection and Response (MDR**) is a managed cyber security service for intrusion detection that provides intrusion detection of malware and malicious activity in your network, and assists in rapid incident response to eliminate those threats with succinct remediation actions.
- **Cloud Service** or **Cloud Service Subscription** or **Software-as-a-Service (SaaS)** or **SAAS** or **Hosted Vendor** means the subscription to use the ITOM Solution functions, data security, data privacy, service level agreements, support, and maintenance including Version Updates.
- **Version Updates** means updates to the MDR Solution whether minor enhancements, major enhancements, planned maintenance, or emergency fixes.
- **EDR (Microsoft Defender)** is a security technology that monitors endpoint devices to detect, investigate, and respond to malicious or suspicious activity.
- **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 MDR solution and for the avoidance of doubt does not include the development of software code.

Minimum Qualifications

- Firm
  - Previous experience as a commercial provider for a MDR Solution, government experience preferred.
  - Professional services experience in implementing the MDR Solution.
- Project Manager
  - Previous professional services experience implementing a similar sized MDR Solution for a City similar in size to Kirkland within the last 3 years.
- Solution
  - The MDR Solution must ensure that the City's data is not hosted offshore or transmitted unencrypted.

Scope

The scope includes the MDR Solution and professional services for implementation assistance. The City has limited funding and expects using the MDR Solution out of the box with minimal configuration and customization. The City is planning on providing a project manager, 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, APIs, etc. Further, the City expects the commercial provider to provide overall guided implementation 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 MDR Solution. The City expects to prepare the IT staff for the change. The approach is to deploy minimum viable operational capacity and iterate improvements after production launches. The City expects professional services assistance to be remote using online methods.

Out of Scope for Commercial Provider

- Traditional project management.
- Extensive customization to MDR Solution. Any customization beyond standard configuration may be subject to further discussion and agreement between the City and the selected Proposer.
- Low priority or requirements not approved.
- IT business processes, customized business rules, standard operating procedure documentation, or the City's performance metrics.

In Scope for Commercial Provider

- Overall implementation consultation and guidance.
- General Configuration and Knowledge Transfer.
- Platform Single Sign On (SSO) with the City's Microsoft Entra.
- Functional Configuration (based) and Knowledge Transfer.
- Reporting, dashboards, and Configuration and Knowledge Transfer.
- MDR 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 normalizing, analysis, alerting and dashboards.
- Support plan with thirty (30) day stabilization period with daily minor configuration corrections.
- Performance testing of MDR Solution including the City's setup, configuration, alerting and dashboards.
- Responsible for readiness, transition, production launch and handover to support.
- The items listed below represent the City's current in-scope MDR and security services. Please refer to Appendix A for additional details on the high-level service items.
    - Managed Detection & Response (MDR) Solution
    - On-Premises Data Collectors
    - Incident Response Retainer
    - Professional Security Services, including but not limited to:
        - Internal Vulnerability Scanning (Quarterly)
        - Security Governance & Policy Advisory
        - Vulnerability Intelligence
        - External Penetration Testing (Quarterly)
        - Incident Response Tabletop Exercises (Semi-Annual)

- PCI Compliance Support Services

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.

TIMELINE

The City's target service go-live is **July 2026**. The City anticipates completing vendor selection and onboarding activities in advance of this date. Proposers should include an implementation approach that enables the deployment, configuration, and validation of services prior to go-live. The City expects proposers to describe their standard onboarding process and estimated timeframe for achieving operational readiness. The timeline represents the City's current target schedule and may be adjusted during the procurement or contract negotiation process.

EVALUATION PROCESS AND SELECTION OF PROPOSALS

Proposals are evaluated for the MDR Solution based on the MDR solution's ability to meet the City's requirements response in Appendix A. If the City chooses to include orals (interviews and demonstrations), the evaluation is further based on the MDR 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 MDR 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 (if conducted).

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

- MDR Solution Requirements and Agreement Suitability – 30%
- Implementation Methodology Plan and other Security Services – 25%
- Price – 25%
- References and professional expertise – 20%

A selection committee will evaluate each submitted written proposal and each oral session (if necessary), 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.

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 Appendix A
5. Submit implementation methodology and plan for the phases in the scope section. Provide improvements to the phased approach as your firm would implement.
6. Provide a firm, fixed price cost proposal based on the proposed implementation methodology and deliverables.
    - Year 1 pricing to include a detailed, itemized breakdown of procurement and implementation costs.
    - Identify and describe any alternative pricing structures (e.g., Year 1 front-loaded costs, distributed three-year pricing, or other options, if applicable).

	Year 1	**Year 2**	**Year 3**
Managed Detection and Response Solution	$	$	$
Professional Services			
Implementation Assistance	$	$	$
Additional Professional Services • Included, but not limited to:	$	$	$

• Incident Response Retainer • Internal Vulnerability Scanning • Penetration Testing • Incident Response Tabletop Exercise • PCI Assessment and Annual Review • Governance and Policy Advisory • Etc.			

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

SUBMISSION INSTRUCTIONS

Proposals must be received by no later than **4:00 PM PST on March 30, 2026.**
We encourage that proposals be submitted by email. Emailed proposals should include "Proposal - Job# 09-26-IT" in the subject line and be addressed to: purchasing@kirklandwa.gov. (Emailed proposals must be in PDF format and cannot exceed 20MB).

As an alternate to email, proposals can be mailed or delivered to:

City of Kirkland
Attn: Jacinda Guild – Job #09-26-IT
123 5th Avenue
Kirkland, WA 98033

If submitting a paper proposal, the original plus four (4) copies of all proposals in printed form must be submitted in a sealed envelope or box with the following words clearly marked on the outside of the envelope, City Response Managed Detection and Response **(MDR) Solution and Professional Services for Implementation and Security Services**. The supplier's name and address must be clearly indicated on the envelope.

Proposals should be prepared simply and economically, providing a straightforward, concise description of provider capabilities to satisfy the requirements of the request. Special bindings, colored displays, promotional materials, etc. are not required or desired. Emphasis should be on completeness and clarity of content. Use recycled paper for responses and any printed or photocopied material created pursuant to a contract with the City whenever practicable. Use both sides of the paper for any submittal to the City whenever practicable.

Submittal Deadlines

March 11, 2026	Release RFP
March 19, 2026 (4:00 PM PT)	Proposer questions due by **(4:00 PM PDT)**
March 26, 2026	Answers to RFP questions posted on website
March 27, 2026	Signed NDA due, if required for protected information
March 30, 2026	Proposals Due by **4:00 PM PDT**
If the City decides to proceed: April 10, 2026	Notify proposers of orals
Week of April 20, 2026	Orals (remote)
April 27, 2026	Submission Evaluation Period
If the City decides to proceed: May 13, 2026	Selected Submission Notified

Questions

Upon release of this RFP, all proposer communications concerning the RFP should be directed to the City's RFP Coordinator listed below via email. Unauthorized contact regarding this RFP with any other City employees may result in disqualification. Any oral communications will be considered unofficial and non-binding on the City. Service Providers should rely only on written statements issued by the RFP Coordinator. The City's RFP Coordinator for this project is:

Name: Jacinda Guild
Address: City of Kirkland, Finance and Administration
123 5th Avenue, Kirkland, Washington 98033
E-mail: jguild@kirklandwa.gov

Terms and Conditions

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

2. 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.

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

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

5. 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.

6. 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.

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

8. 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.

9. The City reserves the right not to award any portion of this RFP or the project in entirety 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 vendor 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 (Disadvantaged Business Enterprise) 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 vendor 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).

PROFESSIONAL SERVICES AGREEMENT **Attachment A**

Managed Detection and Response (MDR) Solution and Professional Services for Implementation and Security Services

The City of Kirkland, Washington, a municipal corporation ("City") and _____, whose address is _____ ("Consultant"), in consideration of the mutual benefits and conditions set forth below, the parties agree and contract as follows.

I. SERVICES BY CONSULTANT

A. The Consultant agrees to perform the services for the City's _____ project, as such services were described and detailed in the City's Request for Proposal (RFP) Job #___ and all documents submitted by Consultant in response, which are hereby fully incorporated herein as part of this Agreement as if set forth herein, and as such services are further described in the following attachments to this Agreement:

1. Attachment A – Professional Services Statement of Work; and
2. [If applicable] Attachment __ – Consultant's _____ Agreement.

Unless specifically noted in this Agreement, the terms of this Professional Services Agreement supersede any conflicting provisions contained within these attachments.

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

C. [Remove if not applicable based on IS review] In addition, in providing the services, Consultant shall agree to and comply with the following:

1. Attachment _B_ (Non-Disclosure Agreement); and
2. Attachment _C_ (Vendor Network Access Agreement).

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 30 days of the date of actual receipt by the City of an invoice conforming in all respects to the terms of this Agreement.

III. GENERAL ADMINISTRATION AND MANAGEMENT

The _____ 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.

IV. COMPLETION DATE AND/OR DURATION OF AGREEMENT

For the Consultant's performance of the [installation/configuration/etc.] services specified in Section I, the estimated completion date is _____ [or is described in Attachment X].

[Also, include if applicable] For [software licensing and/or maintenance and/or support services], this Agreement expires _____ [or as stated in Attachment X].

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.

V. 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.

VI. 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, including chapter 42.56 RCW.

E. The Consultant will 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.

F. 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.

G. 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.

H. The foregoing records shall be maintained for a period of six (6) 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.

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

A. To the greatest extent allowed by law the Consultant shall defend, indemnify, and hold harmless the City and its officers, officials, employees, and volunteers ("Indemnified Parties") 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 Indemnified Parties.

B. 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.

C. It is further specifically and expressly understood that the indemnification provided herein constitutes the Consultant's waiver of immunity under Title 51 RCW, Washington's industrial insurance law, solely for the purpose of this indemnification. This waiver has been mutually negotiated by the parties.

D. 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 this Agreement, insurance against claims for injuries to persons or damage to property that may arise from or in connection with the performance of the work hereunder by the Consultant and/or 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 this Agreement shall not be construed to limit the liability of the Consultant to the coverage provided by such insurance or to 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:

    a. 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.

    b. 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 the City's 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.

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

    d. 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 the 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 the City and/or 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 the City and/or End Users, in the course of using and configuring the Services provided under this Agreement, and includes the City's Data, End User's 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.

C. 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 and for no other purposes.

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

E. 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.

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

G. The Consultant shall make 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.

H. 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.

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

- 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; and,
- A formal penetration test of Consultant's systems and facilities that are used in any way to deliver services under this Agreement, with such test performed by qualified personnel consistent with an established process.

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), or equivalent as determined acceptable to the City. The audit report should not include "private" information, defined as proprietary environment/infrastructure detail not specific to systems that process or transmit 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 Chapter 7.02 of the Kirkland Municipal Code.

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. The terms of this Agreement supersede any conflicting provisions contained in any attachments and/or addenda.

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 Managed Detection and Response (MDR) Solution and Professional Services for Implementation and Security Services; and

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

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

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

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

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

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

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

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

6. Notwithstanding other provisions of this Agreement, the Agreement does not restrict the Vendor with respect to the use of information that is already legally in its possession, that is available to the Vendor from other sources without violating this Agreement or the

intellectual property rights of the City or that is in the public domain. Notwithstanding other provisions of this Agreement, this Agreement also shall not restrict the Vendor from providing, making, using or selling services, devices or other products so long as the Vendor does not breach this Agreement, violate the City's intellectual property rights or utilize any of the Confidential Information.

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

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

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

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

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

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

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

CITY OF KIRKLAND

_____
<Company Name>

By:_____ By:_____

Its:_____ Its:_____

VENDOR NETWORK ACCESS AGREEMENT Attachment C

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

IT Cloud Vendor Security Agreement **Attachment D**

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

Attachment E – Network Diagram

Attachment withheld pending execution of the Non-Disclosure Agreement (Attachment B).

Appendix A

Requirements

The City has documented its requirements for the ITOM 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 MDR Requirements".** The requirements listed represent the City's current desired capabilities and are not exhaustive. They may evolve during the evaluation, contract negotiation, and implementation phases of the project. Each requirement has the following attributes:

<table>
<tr><th>Column</th><th>Meaning</th></tr>
<tr><td>Requirement Category</td><td>The category organizes the requirements at the highest level. The City desires an understanding on your firm's capabilities across all the requirement categories.
<table>
<tr><th>Requirement Category</th></tr>
<tr><td>00-Performance</td></tr>
<tr><td>01-Security</td></tr>
<tr><td>02-Stability</td></tr>
</table></td></tr>
<tr><td>Priority</td><td>The priority provides the material needed for trade-offs and decision making.
<table>
<tr><th>Priority</th><th>Description</th></tr>
<tr><td>01-Must Have</td><td>Evaluated as pass/fail.</td></tr>
<tr><td>02-Nice to Have</td><td>Important, but not mandatory.</td></tr>
<tr><td>03-Should Have</td><td>Expected as part of the solution.</td></tr>
</table></td></tr>
<tr><td>Requirement Description</td><td>This is a description of the requirement for the solution being proposed.</td></tr>
</table>

Response Instructions

The response columns are F through K.

- **Response** - Column F
  - Complete a brief description indicating how the Service Provider's solution meets the requirement.
  - If the requirement is met by custom development, note the impact to support and Version Updates in column K.
- **How the Requirement is Met** - Columns G through K
  - Place an X in the column if the solution includes the requirement in accordance with the column definitions below. If the requirement is both Current Capability or Configurable Item AND Custom, explain in column K.
  - If there is no X indicated for the requirement, the City will assume 'Not Available'.

Column	Definition
Current Capability or Configurable Item - Column G	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.

Future Release - Column H	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).
Custom Development - Column I	Requirement will be met by packaged software currently under development, in beta test, or not yet released. This is an additional cost. Explain in column G.
Not Available - Column J	Requirement cannot be provided either as part of the baseline solution or as a future enhancement.

- **Indicate Module or Product Offering Associated to Requirement and Pricing** - Column K
    - Indicate the module or product used to meet the requirement.
    - Ensure the module or product used to meet the requirement is included in the pricing.