# IT Cloud Vendor Security Agreement

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

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

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

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

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

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

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

**Definitions:**

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

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

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

**Options:**

Option 1: A vendor can verify that they have a high level of security certification that is satisfactory to the City of Kirkland. Examples include but may not be limited to SOC2 and FedRamp.

If this option is selected, print the mutually agreed upon certification level below and attach appropriate documentation.

---

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

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

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

Any deviation from the above best practices must be described here and mutually agreed upon (Signatures on this policy will constitute mutual agreement).

Description of any area where vendor is requesting a waiver, an agreement to a different method, or any other change to this policy:

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

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

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________

___

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

City business person responsible for contract and vendor management:

| | | |
|---|---|---|
| Name | Title | Department |

City IT person responsible for contract and vendor management:

| | | |
|---|---|---|
| Name | Title | Department |

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

| | |
|---|---|
| VENDOR NAME. | City of Kirkland |
| Signature | Signature |
| Printed Name | Printed Name |
| Title | Title |
| Date | Date |

# NON-DISCLOSURE AGREEMENT

This Non-Disclosure Agreement (“the Agreement”) is made this _____ day of ________, 202__, by and between the City of Kirkland, a municipal corporation of the State of Washington (the “City”), and _______________________ , a __ <Corporation/partnership/limited liability company, etc.> (“the Vendor”).

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

Whereas, the Vendor will need to review confidential information (“Confidential Information[1]”) belonging to the City in order to be able to <prepare its proposal/complete this project>, which the City does not want disclosed; and

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

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

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

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

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

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

similar agreement that is at least as protective of the Confidential Information as provided for herein.

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

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

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

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

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

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

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

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

persons or entities in violation of this Agreement to the same extent as if said conduct were by the Vendor.

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

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

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

CITY OF KIRKLAND

___________________________
<Company Name>

By:_______________________________ By:_______________________________

Its:_______________________________ Its:_______________________________