INFORMATION PRIVACY AND SECURITY AGREEMENT

This Information Privacy and Security Agreement ("IPSA") is entered into by and between the City of Redmond ("City") and [*insert name and address of contractor*] ("Contractor") as of the date last signed below (the "Effective Date") and hereby amends the attached agreement between City and Contractor (the "Underlying Agreement"). This IPSA shall apply to the extent that the provision of services by Contractor pursuant to the Underlying Agreement, for example including but not limited to, professional services, SAAS, on-premises software, and remote desktop access, involves the processing of City Data, access to City systems, or access to City Data that is subject to privacy laws.

In consideration of the mutual promises in the Underlying Agreement, this IPSA and other good and valuable consideration, the parties agree as follows:

1. **Definitions.**

   a. "Authorized Users" means Contractor's employees, agents, subcontractors and service providers who have a need to know or otherwise access City Data to enable Contractor to perform its obligations under the Underlying Agreement or the IPSA, and who are bound in writing by confidentiality and other obligations sufficient to protect City Data in accordance with the terms and conditions of this IPSA.

   b. "City Data" means any and all information that the City has disclosed to Contractor or that Contractor has created on behalf of the City pursuant to its obligations under the Underlying Agreement. For the purposes of this IPSA, City Data does not cease to be City Data solely because it is transferred or transmitted beyond the City's immediate possession, custody, or control.

   c. "Data Breach" means the unauthorized acquisition, access, use, or disclosure of City Data which compromises the security or privacy of the City Data or associated City software systems.

   d. "Services" means all services, work, activities, deliverables, software or other obligations provided by Contractor pursuant to the Underlying Agreement.

2. **Standard of Care.**

   a. Contractor acknowledges and agrees that, in the course of its engagement by City, Contractor may create, receive, or have access to City Data. Contractor shall comply with the terms and conditions set forth in this IPSA in its creation, collection, receipt, access to, transmission, storage, disposal, use, and disclosure of such City Data and be responsible for any unauthorized creation, collection, receipt, access to, transmission, storage, disposal, use, or disclosure of City Data under its control or in the possession of Authorized Users.

b. Contractor further acknowledges that use, storage, and access to City Data shall be performed with that degree of skill, care, and judgment customarily accepted as sound, quality, and professional practices. Contractor shall implement and maintain safeguards necessary to ensure the confidentiality, availability, and integrity of City Data. Contractor shall also implement and maintain any safeguards required to be implemented by applicable state and federal laws and regulations.

3.   User Access to City Data.

a. Contractor shall not access, use or disclose City Data in any manner that would constitute a violation of state or federal law, the terms of the Underlying Agreement, or the terms of this IPSA. Contractor may only provide access to Authorized Users who have a legitimate business need to access, use or disclose City Data in the performance of Contractor's duties to City.

b. If Contractor requires access to a City software system, then each Authorized User must have a unique sign-on identification and password for access to City Data on City systems. Authorized Users are prohibited from sharing their login credentials, and may only receive such credentials upon execution of the Authorized User Access Agreement, attached hereto as Exhibit A.   Contractor shall notify City within one (1) day of the departure of any Authorized User, so that City may terminate such Authorized User's access to City software systems.

4.   Use of Subcontractors or Agents.

a. Contractor may disclose City Data to a subcontractor and may allow the subcontractor to create, receive, maintain, access, or transmit City Data on its behalf, provided that Contractor obtains satisfactory assurances that the subcontractor will appropriately safeguard the information. Without limiting the generality of the foregoing, Contractor shall require each of its subcontractors that create, receive, maintain, access, or transmit City Data on behalf of Contractor to execute a written agreement obligating the subcontractor to comply with all terms of this IPSA and to agree to the same restrictions and conditions that apply to Contractor with respect to the City Data.

b. Contractor shall be responsible for all work performed on its behalf by its subcontractors and agents involving City Data as if the work was performed by Contractor. Contractor shall ensure that such work is performed in compliance with this IPSA, the Underlying Agreement and applicable law.

5.   Use, Storage, or Access to, City Data.

a. Contractor shall only use, store, or access City Data in accordance with, and only to the extent permissible under this IPSA and the Underlying Agreement. Further, Contractor shall comply with all laws and regulations applicable to City Data (for example, in compliance with the Health Insurance Portability and Accountability Act ["HIPAA"] or the FBI Criminal Justice

Information Services requirements). If Contractor has access to City protected health information, then Contractor must also execute the City's Business Associate Agreement.

b. Contractor may store City Data on servers housed in datacenters owned and operated by third parties, provided the third parties have executed confidentiality agreements with Contractor. Any transmission, transportation, or storage of City Data outside the United States is prohibited except with the prior written authorization of the City.

6. Privacy.

a. Contractor represents and warrants that in connection with the Services provided by Contractor:

i. All use of City Data by Contractor shall be strictly limited to the direct purpose of performing the Services, except to the extent that City expressly grants permission in writing for such additional uses.

ii. Collection of data which identifies individuals shall be limited to the minimum required by the Services.

iii. If the Services, in whole or part, involves access or delivery of information pertaining to the City via a public-facing web site, then Contractor represents and warrants that its current privacy policy is published online, and is accessible from the same web site as any web-hosted application that is a part of the Services. Contractor's privacy policy will provide end-users with a written explanation of the personal information collected about end-users, as well as available opt-in, opt-out, and other end-user privacy control capabilities.

iv. If Contractor creates technical system log information, aggregated technical usage or traffic data, and/or statistically measured technical usage or traffic data that contains or originated (in whole or part) from City Data, then Contractor's use of such data shall be strictly limited to the direct purpose of the Services and Contractor's technical security operations and systems maintenance. Contractor is prohibited from using such data that personally identifies an individual for secondary commercial purpose (including but not limited to marketing to such individuals, or disclosing data to third parties for reasons unrelated to the primary purpose for originally collecting the data), nor may Contractor solicit consent from the identified individual to do so unless the Underlying Agreement defines a means to do so that does not unduly burden individual privacy rights.

b. Contractor shall maintain the confidentiality of City Data. Confidential information shall not be deemed to include information which (a) is or becomes publicly known through no fault of Contractor; (b) is a publicly available document; or (c) disclosure of which is required by court order or legal requirement. If disclosure of City Data is required by court order or legal requirement the Contractor shall notify City, unless such notification is prohibited by court order or legal requirement. City may take such legally available measures as it chooses to limit or prevent disclosure of the City Data.

7. **Information Security.** This Section 7 applies to the extent that Contractor owns, supports, or is otherwise responsible for host(s), network(s), environment(s), or technology products (including hardware or software) which may contain City Data.

a. Contractor represents and warrants that the design and architecture of Contractor's systems (including but not limited to applications and infrastructure) shall be informed by the principle of defense-depth; controls at multiple layers designed to protect the confidentiality, integrity and availability of data.

b. Contractor shall make appropriate personnel vetting/background checks, have appropriate separation of duties, and undertake other such workflow controls over personnel activities as necessary to safeguard City Data.

c. Contractor shall implement appropriate procedures to monitor and deploy security patches and prevent unintended or unauthorized system configuration changes that could expose system vulnerability or lead to a Data Breach.

d. To the extent that the Services include software that was developed, in whole or part, by Contractor, then Contractor shall ensure that all such Services were developed within a software development life cycle (SDLC) process that includes security and quality assurance roles and control process intended to eliminate existing and potential security vulnerabilities.

e. Contractor shall have appropriate technical perimeter hardening. Contractor shall monitor its system and perimeter configurations and network traffic for vulnerabilities, indicators of activities by threat actors, and/or the presence of malicious code.

f. Contractor shall have access, authorization, and authentication technology appropriate for protecting City Data from unauthorized access or modification, and capable of accounting for access to City Data. The overall access control model of Contractor systems shall follow the principal of least privileges.

g. Contractor shall collaborate with City to safeguard electronic City Data with encryption controls over such City Data both stored and in transit. Contractor shall discontinue use of encryption methods and communication protocols which become obsolete or have become compromised. All transmissions of City Data by Contractor shall be performed using a secure transfer method.

h. Contractor shall maintain a process for backup and restoration of data with a business continuity and disaster recovery plan.

i. Contractor facilities will have adequate physical protections, commensurate with leading industry practice to secure business facilities, data centers, paper files, servers, backup systems, and computing equipment, including, but not limited to, all mobile devices and other equipment with information storage capability.

j. Contractor shall, at its own expense, conduct an information security and privacy risk assessment, no less than annually, in order to demonstrate, substantiate, and assure that the security and privacy standards and practices of Contractor meet or exceed the requirements set out in this IPSA. Upon written request, Contractor shall furnish City with an executive summary of the findings of the most recent risk assessment. In lieu of providing an executive summary, Contractor may provide evidence of privacy and security certification from an independent third party.

 i. City reserves the right to conduct or commission additional tests, relevant to the Services, in order to supplement Contractor's assessment. Contractor shall cooperate with such effort.

 ii. If the findings of the risk assessment identify either: a potentially significant risk exposure to City Data, or other issue indicating that security and privacy standards and practices of Contractor do not meet the requirements set out in this IPSA, then Contractor shall notify City to communicate the issues, nature of the risks, and the corrective active plan.

8. Data Breach Procedures and Liability.

 a. Contractor shall maintain a data breach plan in accordance with the criteria set forth in Contractor's privacy and security policy and shall implement the procedures required under such data breach plan on the occurrence of a Data Breach, in compliance with the requirements of Washington's data breach notification law codified at RCW 19.255.010. Contractor shall report, either orally or in writing, to City any Data Breach involving City Data including any reasonable belief that an unauthorized individual has accessed City Data. The report shall identify the nature of the event, a list of the affected individuals and the types of data, and the mitigation and investigation efforts of Contractor. Contractor shall make the report to the City immediately upon discovery of the Data Breach, but in no event more than forty-eight (48) hours after discovery of the Data Breach. Contractor shall provide investigation updates to the City. If such Data Breach contains protected health information, as defined by HIPAA, Contractor shall comply with the breach requirements contained in the Business Associate Agreement.

 b. Notwithstanding any other provision of the Underlying Agreement, and in addition to any other remedies available to the City under law or equity, Contractor shall promptly reimburse the City in full for all costs incurred by the City in any investigation, remediation or litigation resulting from any Data Breach. Contractor's duty to reimburse the City includes but is not limited to, reimbursing to the City its cost incurred in doing the following:

 i. Notification to third parties whose information may have been or were compromised and to regulatory bodies, law- enforcement agencies or other entities as may be required by law or contract;

ii.   Establishing and monitoring call center(s) and credit monitoring and/or identity restoration services to assist each person impacted by a Data Breach of a nature that, in City's sole discretion, could lead to identity theft; and

iii.   Payment of legal fees and expenses, audit costs, fines and penalties, and other fees imposed upon the City by a regulatory agency, court of law, or contracting partner as a result of the Data Breach.

c.   Upon a Data Breach, Contractor is not permitted to notify affected individuals without the express written consent of City. Unless Contractor is required by law to provide notification to third parties or the affected individuals in a particular manner, City shall control the time, place, and manner of such notification.

9.   No Surreptitious Code. Contractor warrants that, to the best of its knowledge, its system is free of and does not contain any code or mechanism that collects personal information or asserts control of the City's system without City's consent, or which may restrict City's access to or use of City Data. Contractor further warrants that it will not knowingly introduce, via any means, spyware, adware, ransomware, rootkit, keylogger, virus, trojan, worm, or other code or mechanism designed to permit unauthorized access to City Data, or which may restrict City's access to or use of City Data.

10.   Public Records Act. Contractor recognizes that City is a municipal entity subject to the Public Records Act, Chapter 42.56 RCW, and that City is obligated to disclose records upon request unless a specific exemption from disclosure exists. Nothing in this IPSA is intended to prevent City's compliance with the Public Records Act, and City shall not be liable to Contractor due to City's compliance with any law or court order requiring the release of public records.

11.   City Control and Responsibility. City retains all ownership, title, and rights to the City Data. City has and will retain sole responsibility for: (a) all City Data; and (b) City's information technology infrastructure, including computers, software, databases, electronic systems (including database management systems) and networks, whether operated directly by City or through the use of third-party services.

12.   Term and Termination.

a.   Term. The term of this IPSA is the same as the term in the Underlying Agreement.

b.   Termination.   In addition to the termination rights in the Underlying Agreement, City may terminate this IPSA and the Underlying Agreement as follows:

i.   In the event of a material breach of this IPSA by the Contractor, provided that City first sends the Contractor written notice describing the breach with reasonable specificity, including any steps that must be taken to cure the breach. If Contractor fails to cure the breach to the reasonable satisfaction of City within thirty (30) days after receipt of the written

notice, this IPSA and the Underlying Agreement may be terminated at the end of the 30-day period; provided, that if a cure cannot be completed within the thirty (30) day period, the cure period shall be extended so long as Contractor shall initiate the cure within the thirty (30) day period and thereafter diligently pursue it to completion, and provided further, that the cure period shall not be extended more than ninety (90) days after receipt of the notice of the breach; or

ii.   Immediately upon a Data Breach by Contractor or Contractor's Authorized Users.

c.   Effect of Expiration or Termination.

i.   If City terminates the Underlying Agreement or this IPSA due to a material breach or Data Breach described in Section 12.b above, City shall not be obligated to pay any early termination fees or penalties.

ii.   Within thirty (30) days following the expiration or termination of the Underlying Agreement, Contractor shall return to City all City Data in a format and structure acceptable to City and shall retain no copies of such City Data, unless City requires destruction of the City Data. As applicable, Contractor shall comply with any transition service requirements described in the Underlying Agreement.

iii.   Contractor is permitted to retain City Data in its backups, archives and disaster recovery systems until such City Data is deleted in the ordinary course of Contractor's data deletion practices; and all City Data will remain subject to all confidentiality, security and other applicable requirements of this IPSA and as otherwise required by law.

13.   Insurance. In addition to the insurance requirements of the Underlying Agreement, Contractor will maintain at its sole cost and expense at least the following insurance covering its obligations under this IPSA.

a.   Cyber Liability Insurance: With coverage of not less than Two Million Dollars ($2,000,000) in the aggregate which shall include at a minimum coverage for (i) unauthorized access, which may take the form of a "hacker attack" or a "virus" introduced by a third party or cyber extortion; (ii) crisis management, response costs and associated expenses (e.g. legal and public relations expenses); (iii) breach of the City Data; and (iv) loss of data or denial of service incidents.

b.   If Contractor's Services include professional services, then Contractor shall maintain Professional Liability or Errors and Omissions Coverage of not less than Two Million Dollars ($2,000,000) per claim and in the aggregate.

c.   Contractor's insurance shall be primary to any other insurance or self-insurance programs maintained by City. Contractor shall provide to City upon execution a certificate of insurance and blanket additional insured endorsement (if applicable for the Cyber

Liability Insurance). Receipt by City of any certificate showing less coverage than required is not a waiver of Contractor's obligations to fulfill the requirements.

d.   Upon receipt of notice from its insurer(s), Contractor shall provide City with thirty (30) days prior written notice of any cancellation of any insurance policy, required pursuant to this Section 13. Contractor shall, prior to the effective date of such cancellation, obtain replacement insurance policies meeting the requirements of this Section 13. Failure to provide the insurance cancellation notice and to furnish to City replacement insurance policies meeting the requirements of this Section 13 shall be considered a material breach of this IPSA.

e.   Contractor's maintenance of insurance as required by this Section 13 shall not be construed to limit the liability of Contractor to the coverage provided by such insurance, or otherwise limit the City's recourse to any remedy available at law or equity. Further, Contractor's maintenance of insurance policies required by this IPSA shall not be construed to excuse unfaithful performance by Contractor.

14.   Cumulative Rights and Remedies. All City rights and remedies set out in this IPSA are in addition to, and not instead of, other remedies set out in the Underlying Agreement, irrespective of whether the Underlying Agreement specifies a waiver, limitation on damages or liability, or exclusion of remedies. The terms of this IPSA and the resulting obligations and liabilities imposed on Contractor shall supersede any provision in the Underlying Agreement purporting to limit Contractor's liability or disclaim any liability for damages arising out of Contractor's breach of this IPSA.

15.   Indemnification. Contractor shall indemnify, defend and hold harmless City and City's officers, directors, employees, volunteers and agents (each, a "City Indemnitee") from and against any and all third party loss, cost, expense, claims, suit, cause of action, proceeding, damages or liability incurred by such City Indemnitee arising out of or relating to (i) a breach of this IPSA by Contractor; (ii) a violation by Contractor of any information security and privacy statute or regulations; or (iii) any Data Breach by Contractor.

16.   Miscellaneous.

a.   Order of Precedence. This IPSA shall survive the expiration or earlier termination of the Underlying Agreement. In the event the provisions of this IPSA conflict with any provision of the Underlying Agreement, or Contractor's warranties, support contract, or service level agreement, the provisions of this IPSA shall prevail.

b.   Entire Agreement. This IPSA, including its exhibits, constitutes the sole and entire agreement of the Parties with respect to the subject matter of this IPSA and supersedes all prior and contemporaneous understandings, agreements, representations and warranties, both written and oral, with respect to such subject matter.

c.   No Third-Party Beneficiaries. This IPSA is for the sole benefit of the parties hereto and their respective permitted successors and permitted assigns and nothing herein,

express or implied, is intended to or shall confer upon any other person any legal or equitable right, benefit or remedy of any nature whatsoever under or by reason of this IPSA.

d.   Notices. All notices required to be given by either party to the other under this IPSA shall be given to the Technology and Information Systems Service Desk at the following email address: _____, or phone number: _____. All other notices shall be governed by the requirements of the Underlying Agreement.

e.   Amendment and Modification; Waiver. No amendment to or modification of this IPSA is effective unless it is in writing, identified as an amendment to or modification of this IPSA and signed by an authorized representative of each party. The waiver of any breach of any provision of this IPSA will be effective only if in writing. No such waiver will operate or be construed as a waiver of any subsequent breach.

f.   Severability. If a provision of this IPSA is held invalid under any applicable law, such invalidity will not affect any other provision of this IPSA that can be given effect without the invalid provision. Further, all terms and conditions of this IPSA will be deemed enforceable to the fullest extent permissible under applicable law and, when necessary, the court is requested to reform any and all terms or conditions to give them such effect.

g.   Governing Law; Submission to Jurisdiction.   This IPSA is governed exclusively by the laws of the State of Washington, excluding its conflicts of law rules. Exclusive venue for any action hereunder will lie in the state and federal courts located in Seattle, King County, Washington and both parties hereby submit to the jurisdiction of such courts.

h.   Counterparts. This IPSA may be executed in counterparts and by facsimile or electronic pdf, each of which is deemed an original, but all of which together are deemed to be one and the same agreement. A signed copy of this IPSA delivered by facsimile, e-mail or other means of electronic transmission is deemed to have the same legal effect as delivery of an original signed copy of this IPSA.

[Signature Page to Follow]

IN WITNESS WHEREOF, the parties hereto have executed this agreement as of the date first above written.

Contractor   **City of Redmond**

_____

_____

By: _____   By: _____

Name: _____   Name: _____

Title: _____   Title: _____

Date: _____   Date: _____

AUTHORIZED USER ACCESS AGREEMENT

Name of Individual: _____ Name of Contractor: _____

I understand and agree that I am being provided electronic access to a system containing confidential and or proprietary data (the "City Data") owned and operated by the City of Redmond ("City") due to my employment by or contractual relationship with _____ ("Contractor").

I agree that I may use the City Data for the sole purpose of Contractor's obligations to City and in a manner that complies with City's Information Technology Usage Policy. I understand that under no circumstances shall I attempt to impermissibly access, download, read, alter, use or disclose any City Data.

In the event I inadvertently access City Data not related to Contractor's obligations to City, I agree that I will not use, copy, alter or disclose such data and will immediately delete all such data from my records and notify City.

I understand that my user identification, password and profile (collectively, "Authorized User ID") will allow me to access the City Data. I acknowledge that I will keep my Authorized User ID confidential and will not divulge such information to any other individual or entity. I agree to take appropriate measures to protect the privacy of any City Data and to comply with Contractor's privacy and security policies and procedures. I agree that if I suspect that my Authorized User ID has been obtained by another individual, I will immediately inform City so that appropriate action may be taken.

I understand that my access to City Data may be monitored. I understand that all actions used in connection with the City Data may be saved, searched and audited for compliance. I understand that I do not have any personal privacy rights related to my access of the City Data. I further understand that the City has the right to revoke my access at any time.

I agree that I will not use City Data for any other purpose, including personal use, solicitation for outside business ventures, or clinical or research studies. I understand that unauthorized use or disclosure of certain types of City Data may subject me to civil liability under state and/or federal law, and that improper use or disclosure may constitute a crime.

I understand that should I violate any provision of this Authorized User Access Agreement, City will discontinue my access to the City Data and may terminate access of Contractor.

I acknowledge that I have read, understand and agree with the conditions above. Further, I agree to immediately notify City at _____ of any conflict with or violation of the above conditions.

_____   _____
Authorized User Signature   Date