GRAVITY™
IGM Technology Corp.

Customer:	City of Redmond - Washington	**Service Provider:**	IGM Technology Corp
Address:	15670 NE 85th St Redmond, WA USA	**Address:**	207 W Plant St Winter Garden, FL
Billing Contact:	Wanda Norman Technology Project Manager 425-556-2176 wnorman@redmond.gov	**IGM Contact:**	Isaac Yermus, Account Executive iyermus@igm.technology 647-996-2140

ORDER DETAILS

Order Form #:	O-05149 – 2025		**Subscription Start Date:**	
Created on:	Mar 28, 2025		**Subscription End Date:**	
Quote Valid for:	60 days		**Contract length:**	36 months
Billing Frequency	Annual		**Payment Terms:**	Net 30

SOFTWARE SERVICES

Products / Modules:	**Description**	**Start Date**	**End Date**	**Annual Fee:**
● **ACFR Automation** ● **Direct Connection Integration**	Includes environment setup, provisioning, administrator, interface configuration, and user training. Access includes up to 10 named users.			$28,000

PROFESSIONAL SERVICES

Products / Modules:	**Description**	**Total One-Time Fee:**
● IGM Gravity Implementation	*See details in SOW in Exhibit A*	$28,000

BILLING TABLE

Period	Date	Software Services	Professional Services	Total Services	Notes
Year 1		$28,000	$28,000	$56,000	*Initial Service Term of three (3) years. Annual rate increases are set at 5%.*
Year 2		$29,400			
Year 3		$30,870			

This SaaS Services Agreement ("Agreement") is entered into on this ________ day of __________________, 2025 (the "Effective Date") between **IGM Technology Corp**. with a place of business at 207 W Plant St. Winter Garden, FL ("Company"), and the Customer listed above ("Customer"). Each of Customer and Company is referred to herein as a "party" and collectively as the "parties". This Agreement includes and incorporates the attached Terms and Conditions, and referenced Exhibits to such, and contains, among other things, warranty disclaimers, liability limitations and use limitations. There shall be no force or effect to any different terms of any related purchase order or similar form even if signed by the parties after the date hereof.

Any ambiguity, conflict or inconsistency between the documents comprising this Agreement shall be resolved according to the following order of precedence: (1) Gravity Terms and Conditions (2) Exhibit D (3) Exhibit A (4) Exhibit B (5) Exhibit C.

IGM Technology Corp.:		**City of Redmond, Washington:**	
By:	______________________	By:	______________________
Name:	______________________	Name:	______________________
Title:	______________________	Title:	______________________
Email:	______________________	Email:	______________________
Address:	______________________	Address:	______________________
	______________________		______________________

TERMS AND CONDITIONS

1. SAAS SERVICES AND SUPPORT

1.1 Subject to the terms of this Agreement, Company will use commercially reasonable efforts to provide Customer the Services, as defined in the Statement of Work, attached hereto as Exhibit A, in accordance with the Service Level Terms attached hereto as Exhibit B.

1.2 Subject to the terms hereof, Company will provide Customer with reasonable technical support services in accordance with the Support Terms attached hereto as Exhibit C.

2. RESTRICTIONS AND RESPONSIBILITIES

2.1 Customer will not, directly or indirectly: reverse engineer, decompile, disassemble or otherwise attempt to discover the source code, object code, or underlying structure, ideas, know-how, or algorithms relevant to the Services, including any associated software, documentation, or data; modify, translate, or create derivative works based on the Services or any associated materials (except to the extent expressly permitted by Company or authorized within the Services); use the Services or any associated materials for timesharing or service bureau purposes or otherwise for the benefit of a third party; or remove any proprietary notices or labels.

2.2 Each party represents, covenants, and warrants that it will use the Services and perform its obligations under this Agreement in compliance with all applicable laws and regulations.

Customer Indemnification: Customer agrees to indemnify, defend, and hold harmless Company and its officers, directors, employees, and agents from and against any and all damages, losses, liabilities, settlements, and expenses (including without limitation reasonable attorneys' fees and costs) arising from (i) Customer's use of the Services in violation of this Agreement or applicable law; or (ii) claims alleging that Customer's data, content, or use infringes any third-party rights.

Company Indemnification: Company agrees to indemnify, defend, and hold harmless Customer (including its officers, employees, and agents) from and against any and all damages, losses, liabilities, settlements, and expenses (including without limitation reasonable attorneys' fees and costs) arising from claims that the Services infringe any valid third-party intellectual property rights.

2.3 Customer shall be responsible for obtaining and maintaining any equipment and ancillary services needed to connect to, access or otherwise use the Services, including, without limitation, modems, hardware, servers, software, operating systems, networking, web servers and the like (collectively, "Equipment"). Customer shall also be responsible for maintaining the security of the Equipment and the administrative and user passwords.

3. CONFIDENTIALITY; PROPRIETARY RIGHTS

3.1 Each party (the “Receiving Party”) understands that the other party (the “Disclosing Party”) has disclosed or may disclose business, technical or financial information relating to the Disclosing Party’s business (hereinafter referred to as “Proprietary Information” of the Disclosing Party). Proprietary Information of Company includes non-public information regarding features, functionality and performance of the Service. Proprietary Information of Customer includes non-public data provided by Customer to Company to enable the provision of the Services (“Customer Data”). The Receiving Party agrees: (i) to take reasonable precautions to protect such Proprietary Information, and (ii) not to use (except in performance of the Services or as otherwise permitted herein) or divulge to any third person any such Proprietary Information. The Disclosing Party agrees that the foregoing shall not apply with respect to any information after five (5) years following the disclosure thereof or any information that the Receiving Party can document (a) is or becomes generally available to the public, or (b) was in its possession or known by it prior to receipt from the Disclosing Party, or (c) was rightfully disclosed to it without restriction by a third party, or (d) was independently developed without use of any Proprietary Information of the Disclosing Party or (e) is required to be disclosed by law.

3.2 Customer shall own all right, title and interest in and to the Customer Data. Company shall own and retain all right, title and interest in and to (a) the Services and Software, all improvements, enhancements or modifications thereto, (b) any software, applications, inventions or other technology developed in connection with Implementation Services or support, and (c) all intellectual property rights related to any of the foregoing.

3.3 No rights or licenses are granted except as expressly set forth herein.

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

4. PAYMENT OF FEES

4.1 Customer will pay Company the then applicable fees described in the Order Form for the Services and Implementation Services in accordance with the terms therein (the “Fees”). If Customer’s use of the Services exceeds the Service Capacity set forth on the Order Form or otherwise requires the payment of additional fees (per the terms of this Agreement), Customer shall be billed for such usage and Customer agrees to pay the additional fees in the manner provided herein. For purposes of this Agreement, the Initial Service Term shall mean the first three (3) years following the Effective Date, unless otherwise specified in the Order Form.

Company reserves the right to increase the Service Fees to reflect inflation and ongoing enhancements applied to the software platform; however, any such increase shall not exceed five percent (5%) over the Service Fees charged in the immediately preceding Term (Initial or Renewal), unless otherwise agreed in writing by the parties. Company may also change the Fees or applicable charges and institute new charges and Fees at the end of the Initial Service Term or any subsequent renewal term, subject to the 5% cap.

If Customer believes that Company has billed Customer incorrectly, Customer must contact Company no later than sixty (60) days after the closing date on the first billing statement in which the error or problem appeared, in order to receive an adjustment or credit. Inquiries should be directed to Company’s customer support department. First-year Software Service Fees and Implementation Fees are payable net thirty (30) days after the Effective Date of this agreement. Annual fees are payable net thirty (30) days after the renewal date.

4.2 Company will bill through an invoice. Full payment for invoices issued in any given month must be received by Company within thirty (30) days after the mailing date of the invoice. Unpaid amounts are subject to a finance charge of 1% per month on any outstanding balance, or the maximum permitted by law, whichever is lower, plus all expenses of collection and may result in immediate termination of Service. Customer shall be responsible for all taxes associated with Services other than taxes based on Company's net income.

5. TERM AND TERMINATION

5.1 Subject to earlier termination as provided below, this Agreement is for the Initial Service Term as specified on the Quote, and shall be automatically renewed for an unlimited number of one-year periods, each a "Renewal Term" (collectively, the "Term"), unless either party requests termination at least thirty (30) days prior to the end of the then-current term.

5.2 Termination for Non-Appropriation of Funds: If the term of this Agreement extends into fiscal years subsequent to that in which it is approved, such continuation of the Agreement is contingent on the appropriation and availability of funds for such purpose, as determined in good faith by the City. If funds to effect such continued purpose are not appropriated or available as determined in good faith by the City, this Agreement shall automatically terminate and the City shall be relieved of any further obligation.

5.3 In addition to any other remedies, it may have, either party may also terminate this Agreement upon thirty (30) days' written notice to the other party of a material breach, provided that such breach is not cured within such thirty (30) day period (or without notice in the case of nonpayment). Customer will pay in full all undisputed fees for the Services up to and including the last day on which the Services are provided. Upon any termination, Company will comply with its obligations outlined in Section 14(c) of the Customer's Information Privacy and Security Agreement regarding the return, retention, and destruction of City Data. All sections of this Agreement which by their nature should survive termination will survive termination, including, without limitation, accrued rights to payment, confidentiality obligations, warranty disclaimers, and limitations of liability.

6. WARRANTY AND DISCLAIMER

6.1 Company shall use reasonable efforts consistent with prevailing industry standards to maintain the Services in a manner which minimizes errors and interruptions in the Services and shall perform the Professional Services in a professional and workmanlike manner. Services may be temporarily unavailable for scheduled maintenance or for unscheduled emergency maintenance, either by Company or by third-party providers, or because of other causes beyond Company's reasonable control, but Company shall use reasonable efforts to provide advance notice of any scheduled service disruption. HOWEVER, COMPANY DOES NOT WARRANT THAT THE SERVICES WILL BE UNINTERRUPTED OR ERROR FREE; NOR DOES IT MAKE ANY WARRANTY AS TO THE RESULTS THAT MAY BE OBTAINED FROM USE OF THE SERVICES. EXCEPT AS EXPRESSLY SET FORTH IN THIS SECTION, THE SERVICES AND IMPLEMENTATION SERVICES ARE PROVIDED "AS IS" AND COMPANY DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT.

7. LIMITATION OF LIABILITY

7.1 NOTWITHSTANDING ANYTHING TO THE CONTRARY, EXCEPT FOR BODILY INJURY OF A PERSON, COMPANY AND ITS SUPPLIERS (INCLUDING BUT NOT LIMITED TO ALL EQUIPMENT AND TECHNOLOGY SUPPLIERS), OFFICERS, AFFILIATES, REPRESENTATIVES, CONTRACTORS AND EMPLOYEES SHALL NOT BE RESPONSIBLE OR LIABLE WITH RESPECT TO ANY SUBJECT MATTER OF THIS AGREEMENT OR TERMS AND CONDITIONS RELATED THERETO UNDER ANY CONTRACT, NEGLIGENCE, STRICT LIABILITY OR OTHER THEORY: (A) FOR ERROR OR INTERRUPTION OF USE OR FOR LOSS OR INACCURACY OR CORRUPTION OF DATA OR COST OF PROCUREMENT OF SUBSTITUTE GOODS, SERVICES OR TECHNOLOGY OR LOSS OF BUSINESS; (B) FOR ANY INDIRECT, EXEMPLARY, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES; (C) FOR ANY MATTER BEYOND COMPANY'S REASONABLE CONTROL; OR (D) FOR ANY AMOUNTS THAT, TOGETHER WITH AMOUNTS ASSOCIATED WITH ALL OTHER CLAIMS, EXCEED THE FEES PAID BY CUSTOMER TO COMPANY FOR THE SERVICES UNDER THIS AGREEMENT IN THE 12 MONTHS PRIOR TO THE ACT THAT GAVE RISE TO THE LIABILITY, IN EACH CASE, WHETHER OR NOT COMPANY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

8. MISCELLANEOUS

8.1 If any provision of this Agreement is found to be unenforceable or invalid, that provision will be limited or eliminated to the minimum extent necessary so that this Agreement will otherwise remain in full force and effect and enforceable. This Agreement is not assignable, transferable or sub-licensable by Customer except with Company's prior written consent. Company may transfer and assign any of its rights and obligations under this Agreement without consent. This Agreement is the complete and exclusive statement of the mutual understanding of the parties and supersedes and cancels all previous written and oral agreements, communications and other understandings relating to the subject matter of this Agreement, and that all waivers and modifications must be in a writing signed by both parties, except as otherwise provided herein. No agency, partnership, joint venture, or employment is created as a result of this Agreement and Customer does not have any authority of any kind to bind Company in any respect whatsoever. In any action or proceeding to enforce rights under this Agreement, the prevailing party will be entitled to recover costs and attorneys' fees. All notices under this Agreement will be in writing and will be deemed to have been duly given when received, if personally delivered; when receipt is electronically confirmed, if transmitted by facsimile or e-mail; the day after it is sent, if sent for next day delivery by recognized overnight delivery service; and upon receipt, if sent by certified or registered mail, return receipt requested. The address for such notices and communications shall be as set forth on the signature page attached hereto.

EXHIBIT A
Statement of Work

The Company will provide the following "Services" and comprehensive training to the following modules:

- **ACFR Automation**
- **Direct Connection Integration**
- **Single Sign-On**

Company's deployment methodology uses an iterative approach to guide our customers through the successful implementation of our products. Drawing on years of experience working with and leading government entities, as well as best practices from both the public and private sectors, we ensure a successful implementation. This methodology demands a high level of focus and engagement from both parties to achieve the desired results

Company will take a similar approach for each module through the implementation.

Phase 1: Discovery and Planning

During the Discovery and Planning phase of the project, Company and the Customer will work together to design a project plan and configuration guide to meet the goals of the Customer.
Some of the tasks to be completed during the Discovery and Planning Phase are:

- Contract Signed and Reviewed with Customer
- Agree upon starting date of project
- Kick off of project
- Review current system and identify configuration within Gravity
- Identify any Gaps and proposed solution
  Deliverables: Project Plan, Gap Analysis & Resolution Document

After Company and the Customer have agreed on the design of the solution, the configuration can begin. During the configuration phase of the project, Company will take on the task of configuring the system based on the agreed upon design. When questions or concerns arise it will be important for Company and the Customer to review and agree upon updated configuration.
Some of the tasks to be completed during the Configuration phase include:

- Data elements, tables, roles, reports, data file extracts, data file import configurations, active directory integration, etc. are configured to meet the Customer's requirements
- Configuration settings have been loaded and system tested
- Configuration settings are available for UAT and Training purposes

- Data will be loaded

Deliverables: A fully operational system that is ready for UAT Testing.

Phase 3: Testing/Training

After the system has been configured and the project leaders feel it is ready for testing, the implementation will move into the testing and training phase. During the testing phase Company and the Customer will prepare a testing plan to ensure the system is working to the design that was agreed upon in phase 1 and configured in phase 2. The Customer will provide Company with a list of any areas that need to be updated to ensure the software is ready to Go-Live.

Phase 2: Configuration

Once the system has been tested and approved, the training of end users can occur. Company will work collaboratively with the Customer on the training needs and develop training materials. Company and/or the Customer will deliver training to end users.

Some of the tasks to be completed during the Testing/Training phase include:

- A User Acceptance Testing (UAT) plan will be created and reviewed in collaboration with the customer.
- The customer will conduct UAT and provide any needed changes or concerns.
- Company will update to ensure successful UAT
- A training plan will be developed and reviewed with the Customer.
- Training will be completed.
- Training materials provided to the Customer

Deliverables: Training Material and UAT Acceptance

The last phase of the project is to Go-Live. Once the configuration has been tested and training complete, the Customer can schedule a Go-Live date. During the Go-Live event Company will support the users with any questions that may arise. Following Go-Live, ongoing support will be provided by the Company's standard support team through its established support channels. Go-Live is expected to be completed within five (5) months from the project start date, contingent upon the Customer providing all required documentation, feedback, and approvals within a reasonable timeframe. The Customer will also provide Company with a list of any areas that need to be updated to ensure the software is ready for Go-Live. Some of the tasks to be completed during the Testing/Training phase include:

- Company and the Customer will agree on a Go-Live Date.
- Communication plan developed for end users
- Company supports the Customer in initial Go-Live and questions answering

Deliverables: Final acceptance from the Customer

Phase 4: Go-Live

EXHIBIT B
Service Level Terms

The Services shall be available 99.9%, measured monthly, excluding holidays and weekends and scheduled maintenance. If Customer requests maintenance during these hours, any uptime or downtime calculation will exclude periods affected by such maintenance. Further, any downtime resulting from outages of third-party connections or utilities or other reasons beyond Company's control will also be excluded from any such calculation. Customer's sole and exclusive remedy, and Company's entire liability, in connection with Service availability shall be that for each period of downtime lasting longer than one hour, Company will credit Customer 5% of Service fees; provided that no more than one such credit will accrue per day. Downtime shall begin to accrue as soon as Customer (with notice to Company) recognizes that downtime is taking place, and continues until the availability of the Services is restored. In order to receive downtime credit, Customer must notify Company in writing within 24 hours from the time of downtime, and failure to provide such notice will forfeit the right to receive downtime credit. Such credits may not be redeemed for cash. Company will apply any credits accumulated in the prior Term, towards the Service Fees in the next term.

Company will use commercially reasonable efforts to respond to all Helpdesk tickets within one (1) business day.

Emergency customer support is available outside of Support hours and can be initiated by calling IGM's customer support line or emailing support@igm.technology

EXHIBIT C
Support Terms

IGM will provide Technical Support to customer via both telephone and electronic mail Monday – Friday between 6am – 8pm Eastern Time ("Support Hours").

Customer may initiate a helpdesk ticket during Support Hours by calling IGM's customer support line or any time by emailing support@igm.technology

EXHIBIT D
INFORMATION PRIVACY, SECURITY AND ACCESS AGREEMENT

This Information Privacy, Security, and Access Agreement ("IPSA") is entered into by and between the City of Redmond ("City") and [*insert name and address of Consultant*] ("Consultant") as of the date last signed below (the "Effective Date") and hereby supplements the attached agreement between City and Consultant (the "Underlying Agreement"). This IPSA shall apply to the extent that the provision of services by Consultant 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 exemption from disclosure under Chapter 42.56 RCW.

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

1. Definitions.

a. "Authorized Users" means Consultant's employees, agents, subconsultants and service providers who have a need to know or otherwise access City Data to enable Consultant 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 Consultant or given Consultant access to, or that Consultant 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 accessed by, or is transferred or transmitted beyond the City's immediate possession, custody, or control.

c. "City software systems" means the systems, solutions (COTS and custom developed), applications and platforms used to support the management, operation and development of City activities.

d. "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.

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

2. Standard of Care.

a. Consultant acknowledges and agrees that, in the course of its engagement by City, Consultant may create, receive, or have access to City Data. Consultant 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. Consultant 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. Consultant shall implement and maintain safeguards necessary to ensure the confidentiality, availability, and integrity of City Data. Consultant 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. Consultant 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. Consultant may only provide access to Authorized Users who have a legitimate business need to access, use or disclose City Data in the performance of Consultant's duties to City.

b. If Consultant 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. Consultant 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 Subconsultants or Agents.

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

b. Consultant shall be responsible for all work performed on its behalf by its subconsultants and agents involving City Data as if the work was performed by Consultant.

Consultant 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. Consultant 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, Consultant 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 Consultant has access to City protected health information, then Consultant must also execute the City's Business Associate Agreement.

b. Consultant may store City Data on servers housed in datacenters owned and operated by third parties, provided the third parties have executed confidentiality agreements with Consultant and subject to Section 5.c.

c. Unless specifically authorized in writing by City, Consultant shall not (i) access, store, process, transmit, or create City Data at locations outside the fifty (50) United States of America; (ii) permit viewing access to City Data by Consultant or any of its agents (including any subconsultants) or any other person outside the fifty (50) United States of America through any screen sharing technology such as Remote Desktop Protocol or VMware Remote Console ("VMRC"), or other current or future protocols designed to provide similar functionality; or (iii) provide City Data received from, created, or received by Vendor on behalf of City to any employee or agent, including a subconsultant, if such employee, agent, or subconsultant receives, processes, or otherwise has access to such City Data outside of the fifty (50) United States of America. The prohibitions set forth in this Section 5.c apply not only to Consultant's data center locations and personnel primarily involved with providing the contracted Services, but equally to any and all data centers and personnel used for resilience or redundancy, backups, log storage, after-hours support, and any downstream partners that may access, store, process, transmit, or create City Data.

6. Privacy.

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

i. All use of City Data by Consultant 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 Consultant 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. Consultant'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 Consultant 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 Consultant's use of such data shall be strictly limited to the direct purpose of the Services and Consultant's technical security operations and systems maintenance. Consultant 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 Consultant 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. Consultant 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 Consultant; (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 Consultant 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 Consultant 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. Consultant represents and warrants that the design and architecture of Consultant'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. Consultant 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. Consultant 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 Consultant, then Consultant 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. Consultant shall have appropriate technical perimeter hardening. Consultant 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. Consultant 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 Consultant systems shall follow the principal of least privileges.

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

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

i. Consultant 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. Consultant 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 Consultant meet or exceed the requirements set out in this IPSA. Upon written request, Consultant shall furnish City with an executive summary of the findings of the most recent risk assessment. In lieu of providing an executive summary, Consultant 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 Consultant's assessment. Consultant 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 Consultant do not meet the requirements set out in this IPSA, then Consultant shall notify City to communicate the issues, nature of the risks, and the corrective active plan.

8. Data Breach Procedures and Liability.

a. Consultant shall maintain a data breach plan in accordance with the criteria set forth in Consultant'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 laws codified at RCW 19.255.010 and RCW 42.56.590. Without limiting the generality of the foregoing, Consultant 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 Consultant. Consultant 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. Consultant shall provide investigation updates to the City. If such Data Breach contains protected health information, as defined by HIPAA, Consultant 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, Consultant 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. Consultant'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, Consultant is not permitted to notify affected individuals without the express written consent of City. Unless Consultant 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. Consultant 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. Consultant 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. Consultant 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 Consultant 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 Consultant, provided that City first sends the Consultant written notice describing the breach with reasonable specificity, including any steps that must be taken to cure the breach. If Consultant 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 Consultant 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 Consultant or Consultant'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, Consultant 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, Consultant shall comply with any transition service requirements described in the Underlying Agreement.

iii. Consultant 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 Consultant'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.

iv. Consultant agrees to certify that City Data, including City Data held by subconsultants, has been returned, deleted, or destroyed from its systems, servers, off-site storage facilities, office locations, and any other location where Consultant or subconsultants, maintain City Data within 45 days of receiving City's request that the City Data be returned, deleted, or destroyed. Consultant shall document its verification of data removal, including tracking of all media requiring cleaning, purging or destruction.

13. Insurance. In addition to the insurance requirements of the Underlying Agreement, Consultant 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 Consultant's Services include professional services, then Consultant 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. Consultant's insurance shall be primary to any other insurance or self-insurance programs maintained by City. Consultant 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 Consultant's obligations to fulfill the requirements.

d. Upon receipt of notice from its insurer(s), Consultant shall provide City with thirty (30) days prior written notice of any cancellation of any insurance policy, required pursuant to this Section 13. Consultant 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. Consultant’s maintenance of insurance as required by this Section 13 shall not be construed to limit the liability of Consultant to the coverage provided by such insurance, or otherwise limit the City’s recourse to any remedy available at law or equity. Further, Consultant’s maintenance of insurance policies required by this IPSA shall not be construed to excuse unfaithful performance by Consultant.

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 Consultant shall supersede any provision in the Underlying Agreement purporting to limit Consultant’s liability or disclaim any liability for damages arising out of Consultant’s breach of this IPSA.

15. Indemnification. Consultant 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 Consultant; (ii) a violation by Consultant of any information security and privacy statute or regulations; or (iii) any Data Breach by Consultant.

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 Consultant'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: ISAdministration@redmond.gov, or phone number: 425-556-2929. 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.

Consultant	**City of Redmond**
______________________________	
______________________________	
By: __________________________	By: ___________________________
Name: ________________________	Name: ________________________
Title: ________________________	Title: _________________________
Date: ________________________	Date: _________________________

EXHIBIT A
AUTHORIZED USER ACCESS AGREEMENT

Name of Individual: ___________________________ Name of Consultant: ______________________

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 ________________ ("Consultant").

I agree that I may use the City Data for the sole purpose of Consultant'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 Consultant'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 Consultant'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 Consultant.

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