SwiftComply Service Agreement for the City of Everett, WA

This SwiftComply Service Agreement (the ***"Agreement"***) is made and entered into by and between SwiftComply, Inc. (***"SwiftComply"***), a Delaware corporation with its principal offices at 6701 Koll Center Pkwy Suite 250, Pleasanton, CA 94566 and ***Customer*** (as defined in the applicable SwiftComply Service Order) (each a ***"Party"*** and collectively the ***"Parties"***). This Agreement governs the terms and conditions under which Customer may utilize the SwiftComply Service as set forth herein and as specified in one or more applicable SwiftComply Service Order(s) executed by Customer in connection herewith and incorporated herein (the ***"SwiftComply Service Order(s)"***).

WHEREAS SwiftComply owns and operates the SwiftComply Service, a Web-based SaaS solution that includes a variety of SwiftComply Module(s) and provides various features and functionality via such SwiftComply Module(s); and

WHEREAS Customer wishes to utilize the SwiftComply Service in order to help optimize Customer's regulatory programs as well as to leverage the functionality of such SwiftComply Module(s);

NOW THEREFORE, in consideration of the mutual covenants contained herein and other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, SwiftComply and Customer hereby agree as follows:

1) **Definitions.** Capitalized terms used in this Agreement, and not otherwise defined herein, shall have the following meanings:

1.1) ***"Account"*** means an access point for the SwiftComply Service that requires registration by the Customer.

1.2) ***"SwiftComply API"*** means an Application programming interface that provides access to specified content and functionality within certain SwiftComply Modules.

1.3) ***"SwiftComply Modules"*** means collectively all of the Web Applications hosted by SwiftComply and available via the SwiftComply Service, including but not limited to:

a) SwiftComply Backflow: An Application that enables Cross Connection Control Environmental Program Management.
b) SwiftComply Reclaimed Water: An Application that enables Reclaimed/Recycled/Auxiliary Water Program Management.
c) SwiftComply Pretreatment: An Application that enables Industrial Pretreatment Program Management.
d) SwiftComply FOG: An Application that enables Fat, Oils & Greases Environmental Program Management.
e) SwiftComply Stormwater: An Application that enables Stormwater Environmental Program Management.
f) SwiftComply Forms: An Application that provides a workflow automation platform that allows Customer to create web-based forms for their internal operations and for their constituents to transact with Customer.
g) SwiftComply Multi-Modules: An Application that provides dashboards and reporting across multiple SwiftComply Modules.

All features, functionality, reports, etc. for each SwiftComply Module are included as material elements of the applicable SwiftComply Module. SwiftComply may modify, combine, add or delete SwiftComply Modules from the SwiftComply Service from time to time at its sole discretion, provided that in the event that SwiftComply terminates or deletes any SwiftComply Module to which Customer is actively subscribing, SwiftComply shall provide a pro-rata refund for applicable portion of the Subscription Service Fee for the remainder of the then current Service Period.

1.4) ***"SwiftComply Data"*** means any aggregated and normalized key metrics and data collected by SwiftComply for the delivery of the SwiftComply Service.

1.5) ***"SwiftComply Service"*** means the complete set of SwiftComply software and related materials including but not limited to the SwiftComply Modules, SwiftComply Data, SwiftComply Websites, the Documentation and the Software.

1.6) ***"SwiftComply Web Site"*** means the Websites owned and operated by SwiftComply and made available at the following URL: http://customer.swiftcomply.com, https://customer.c3swift.com/, and/or any successor site(s).

1.7) ***"Customer Data"*** means any data provided to SwiftComply by or on behalf of Customer or any data entered or uploaded into the SwiftComply Service by or on behalf of Customer, including Sensitive Data entered or provided by Customer. Customer Data specifically excludes SwiftComply Data as well as any anonymized, customized, modified or derivative works related to the Customer Data.

1.8) ***"Customer State"*** means the state, commonwealth or territory in which the Customer is located.

1.9) ***"Customer Web Site"*** means any Web site owned and operated by Customer.

1.10) ***"Documentation"*** means any accompanying proprietary documentation made available to Customer by SwiftComply for use with the SwiftComply Service, including any documentation available online or otherwise.

1.11) ***"Sensitive Data:*** means any Customer Data that may reasonably be deemed sensitive and/or private in nature, including but not limited to personal wage garnishments, individual healthcare-related expenses, data protected by HIPAA, etc.

1.12) ***"Software"*** means the source code and/or other code which are material elements of the SwiftComply Modules and SwiftComply Service.

2) **Service Usage & Licenses.**

2.1) Account Password and Security. Customer shall protect its passwords and take full responsibility for Customer's own, as well as any third-party, use of the Customer Account(s). Customer is solely responsible for any and all activities that occur under such Customer Account(s), except for any activities performed by SwiftComply as set forth herein. Customer agrees to notify SwiftComply immediately upon learning of any unauthorized use of a Customer Account or any other breach of security. From time to time, SwiftComply's support staff may log in to the Customer Account in order to maintain or improve service, including providing Customer assistance with technical or billing issues. Customer hereby acknowledges and consents to such access.

2.2) SwiftComply License. Subject to the terms and conditions of this Agreement and as specifically set forth in the applicable SwiftComply Service Order(s), SwiftComply grants Customer a limited, revocable, non-exclusive, non-transferable, non-distributable, worldwide license to utilize the SwiftComply Service for the following functionality:

a) Content Delivery. Customer may integrate, link and publish applicable public-facing content from the applicable SwiftComply Modules within one or more Customer Web Site(s);

b) Application Access. Customer may access the SwiftComply Modules via Customer's Account to utilize the functionality provided within such SwiftComply Modules; and

c) API Access. Customer may access the SwiftComply API to share data from the SwiftComply Modules within one or more Customer(s) database(s).

3) Term and Termination.

3.1) Term. The duration of this Agreement shall be defined in accordance with the Term set forth in all applicable Service Order(s). The Term shall commence upon the Start Date set forth in the first SwiftComply Service Order executed between the Parties and shall continue in full force and effect until the termination or expiration of all applicable SwiftComply Service Order(s) (the ***"Term"***).

3.2) Termination. This Agreement and/or any applicable SwiftComply Service Order may be terminated prior to the expiration of the term as follows:

a) Either Party may terminate this Agreement if the other Party fails to cure a material breach of the Agreement within fifteen (15) days after receipt of written notice thereof.

b) Either Party may terminate this Agreement if the other Party is involved in insolvency proceedings, receivership, bankruptcy, or assignment for the benefit of creditors.

3.3) Obligations. Upon expiration or termination of this Agreement:

a) Each Party shall promptly return to the other all of the Confidential Information of the other Party in its possession or control;

b) Customer shall cease use of the SwiftComply Service and shall remove all links from the Customer Web Site(s) to any content provided by the SwiftComply Modules; and

c) Any outstanding fees shall become immediately due and payable, and termination of this Agreement shall not relieve Customer from its obligation to pay to SwiftComply any such fees.

3.4) Survival. Sections 3.3, 3.4 and 4 through 8 inclusive shall survive any termination or expiration of this Agreement.

4) Fees and Billing.

4.1) Fees. Customer shall pay the Fees in accordance with the terms set forth in the applicable SwiftComply Service Order.

4.2) Interest and Collections. Customer will be charged $50 for payments by checks that are returned due to insufficient funds. Any late payments will accrue interest equal to one and one-half percent (1.5%) per month, or the maximum amount allowable under law, whichever is less, compounded monthly. SwiftComply shall be entitled to recover all reasonable costs of collection (including agency fees, attorneys' fees, in-house counsel costs, expenses and costs) incurred in attempting to collect payment from Customer.

4.3) Taxes. Customer is solely responsible for all applicable sales, use and other taxes and similar charges based on or arising from this Agreement or any SwiftComply Service Order. In the event that Customer is exempt from sales tax, Customer will provide SwiftComply with a tax-exempt certificate upon request.

5) Intellectual Property.

5.1) General. Both Parties may only use the other Party's intellectual property as expressly set forth herein. Nothing in this Agreement shall be construed in any manner to affect or modify either Party's ownership rights in any pre existing or future works, trademarks, copyrights or technologies developed or created by either Party, including without limitation, their respective proprietary software used in connection with the development and provision of their respective Websites, databases, systems, products and/or services. Unless specifically agreed by the Parties in writing, all intellectual property, including without limitation information that could become the subject of a patent, copyright or trade secret, developed by a Party in the context of performing its obligations under this Agreement shall be exclusively owned by that Party and the other Party shall cooperate with any reasonable requests to execute documents confirming such ownership.

5.2) Data Ownership and License.

a) Customer represents and warrants that it has obtained all data subjects' consent or otherwise has the full legal right necessary to provide the Customer Data to SwiftComply for SwiftComply's use as contemplated by this Agreement. Customer acknowledges that SwiftComply shall have no legal liability for its use and/or the display of the Customer Data as contemplated by this Agreement.

b) Customer represents and warrants that Customer shall not provide or enter Sensitive Data to be displayed in any publicly available element of the SwiftComply Service. To the extent that Customer enters or uploads any Sensitive Data into the SwiftComply Service, Customer shall assume full responsibility for the disclosure of such Sensitive Data. SwiftComply is under no obligation to review and/or verify whether or not Customer Data includes Sensitive Data.

c) Customer Data shall remain the property of Customer, and Customer hereby grants SwiftComply a limited, perpetual, irrevocable and royalty-free right to use, copy, modify, and display the Customer Data within any SwiftComply Module(s) and for the purpose of providing the SwiftComply Service.

5.3) Proprietary Rights Notice. The SwiftComply Service and all intellectual property rights in the SwiftComply Service are, and shall remain, the property of SwiftComply. All rights in and to the SwiftComply Service not expressly granted to Customer in this Agreement are hereby expressly reserved and retained by SwiftComply without restriction, including, without limitation, SwiftComply's right to sole ownership of the SwiftComply API, SwiftComply Modules, SwiftComply Data, SwiftComply Websites, Documentation and Software. Without limiting the generality of the foregoing, Customer agrees not to (and to not allow any third party to): (a) sublicense, copy, distribute, rent, lease, lend or use the SwiftComply Service outside of the scope of the license granted herein or make the SwiftComply Service available to any third party or use the SwiftComply Service on a service bureau time sharing basis; (b) copy, modify, adapt, translate, prepare derivative works from, reverse engineer, disassemble, or decompile the SwiftComply Service or otherwise attempt to discover or reconstruct any source code, underlying ideas, algorithms, file formats, program interfaces or other trade secrets related to the SwiftComply Service; (c) use the trademarks, trade names, service marks, logos, domain names and other distinctive brand features or any copyright or other proprietary rights associated with the SwiftComply Service for any purpose without the express written consent of SwiftComply; (d) register, attempt to register, or assist anyone else to register any trademark, trade name, service marks, logos, domain names and other distinctive brand features, copyrights or other proprietary rights associated with SwiftComply other than in the name of SwiftComply; or (e) modify, remove, obscure, or alter any notice of copyright, trademark, or other proprietary right or legend appearing in or on any item included with the

SwiftComply Service. If the use of the SwiftComply Service is being purchased by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), in accordance with 48 C.F.R. 227.7202-4 (for Department of Defense (DOD) acquisitions) and 48 C.F.R. 2.101 and 12.212 (for non-DOD acquisitions), the Government's rights in the SwiftComply Service, including its rights to use, modify, reproduce, release, perform, display or disclose any elements of the SwiftComply Service, will be subject in all respects to the commercial license rights and restrictions provided in this Agreement.

6) Representations, Warranties, Indemnification and Liability.

6.1) By SwiftComply. SwiftComply represents and warrants that: (i) the SwiftComply Service shall be provided in accordance with, and shall not violate applicable laws, rules or regulations; and (ii) by using the SwiftComply Service, Customer will not violate or in any way infringe upon the personal or proprietary rights of any third party, (iii) to SwiftComply's knowledge, the SwiftComply Service does not contain any virus, worm, Trojan horse, time bomb or similar contaminating or destructive feature; and (iv) SwiftComply holds all necessary rights to permit the use of the SwiftComply Service and all components thereof provided to Customer under this Agreement.

6.2) By Customer. Customer represents and warrants that: (i) it has all right, title, and interest in and to the Customer Data necessary for its use in connection with the SwiftComply Service; and (ii) it shall not use the SwiftComply Service in a manner or in connection with any activity that would violate this Agreement or any law, rule or regulation or rights of any third party.

6.3) By Both. SwiftComply and Customer both represent and warrant that (i) each has full power and authority to enter into and perform its obligations under this Agreement; (ii) this Agreement is a legal, valid and binding obligation, enforceable against each Party in accordance with its terms; and (iii) entering into this Agreement will not knowingly violate the Agreement or any laws, regulations or third-party contracts.

6.4) Indemnification by SwiftComply. At SwiftComply's cost, SwiftComply agrees to indemnify, hold harmless and defend Customer against any cost, loss or expense (including attorney's fees) resulting from any claims by third parties for loss, damage or injury (each, a ***"Claim"***) arising out of or relating to (i) SwiftComply's breach of any term, condition, representation or warranty of this Agreement, (ii) SwiftComply's violation of any third party rights in connection with the SwiftComply Service or (iii) SwiftComply's violations of applicable laws, rules or regulations in connection with the SwiftComply Service. In such a case, Customer will provide SwiftComply with written notice of such Claim. Customer shall cooperate as fully as reasonably required in the defense of any Claim. Customer reserves the right, at its own expense, to assume the exclusive defense and control of any matter subject to indemnification by SwiftComply. Notwithstanding the foregoing, unless the settlement involves no cost, loss or continuing liability to Customer, SwiftComply shall not settle any Claim, without the written consent of Customer, such consent not to be unreasonably withheld.

6.5) Limited Warranty. SwiftComply warrants that the SwiftComply Service will be delivered in a professional and workmanlike manner substantially in accordance with the statement of work set forth in the applicable SwiftComply Service Order and that the SwiftComply Service will operate in all material respects as described in its product descriptions and/or documentation. EXCEPT FOR THE EXPRESS WARRANTIES STATED IN THIS AGREEMENT, INCLUDING ANY applicable SwiftComply SERVICE ORDER, SwiftComply MAKES NO ADDITIONAL WARRANTY, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, GUARANTEES, REPRESENTATIONS, PROMISES, STATEMENTS, ESTIMATES, CONDITIONS, OR OTHER INDUCEMENTS.

6.6) Limitation of Liability. NEITHER SwiftComply NOR CUSTOMER WILL BE LIABLE TO THE OTHER PARTY FOR ANY INDIRECT, SPECIAL, PUNITIVE, CONSEQUENTIAL (INCLUDING, WITHOUT LIMITATION, LOST PROFITS), OR INCIDENTAL DAMAGES, WHETHER BASED ON A CLAIM OR ACTION OF CONTRACT, WARRANTY, NEGLIGENCE, STRICT LIABILITY, OR OTHER TORT, BREACH OF ANY STATUTORY DUTY, INDEMNITY OR CONTRIBUTION, OR OTHERWISE, EVEN IF THE PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE EXCLUSION CONTAINED IN THIS PARAGRAPH SHALL apply REGARDLESS OF THE FAILURE OF THE EXCLUSIVE REMEDY PROVIDED IN THE FOLLOWING SENTENCE. BOTH PARTIES' TOTAL CUMULATIVE LIABILITY TO THE OTHER PARTY FOR ANY LOSS OR DAMAGES RESULTING FROM ANY CLAIMS, DEMANDS OR ACTIONS ARISING OUT OF OR RELATING TO THIS AGREEMENT SHALL NOT EXCEED THE CUMULATIVE FEES PAID BY CUSTOMER TO SwiftComply IN THE PRECEDING TWELVE (12) MONTHS. THE FOREGOING SHALL NOT LIMIT A PARTY'S (A) PAYMENT OBLIGATIONS UNDER THE AGREEMENT; (B) LIABILITY FOR INDEMNIFICATION OBLIGATIONS UNDER SECTION 6.3; (C) LIABILITY FOR ANY BREACH OF ITS CONFIDENTIALITY OBLIGATIONS UNDER SECTION 7; OR (D) LIABILITY FOR ITS INFRINGEMENT OR MISAPPROPRIATION OF ANY PROPRIETARY RIGHTS OF THE OTHER PARTY. NOTHING IN THIS AGREEMENT SHALL BE CONSTRUED AS EXCLUDING OR LIMITING A PARTY'S LIABILITY FOR FRAUD OR ITS LIABILITY FOR DEATH OR PERSONAL INJURY ARISING FROM ITS NEGLIGENCE.

6.7) Essential Element. The provisions of this Section 6 are an essential element of the benefit of the consideration reflected in this Agreement.

7) Confidentiality.

7.1) Subject to any applicable open public records laws in the Customer State, each Party will keep the specific terms of this Agreement confidential, including the contents of the schedules and exhibits, and not disclose any portion of them to any third party (other than to its attorneys, accountants, advisors and potential investors who are bound to keep such information confidential) without the other Party's prior written consent, except as required by law, including but not limited to open public record laws.

7.2) In addition, in connection with the negotiation and performance of this Agreement, a Party (the ***"Receiving Party"***) may receive information from the other Party (the ***"Disclosing Party"***) which is confidential or proprietary in nature, including without limitation information about a Party's products, systems and services (***"Confidential Information"***). The Receiving Party agrees that, during the term of this Agreement and for a period of three (3) years thereafter, it will keep the Confidential Information in strictest confidence and protect such Confidential Information by similar security measures as it takes to protect its own Confidential Information of a similar nature, but in no event shall the Receiving Party take less than reasonable care with the Confidential Information of the Disclosing Party. The Receiving Party also agrees that it will not use any Confidential Information for any purpose other than in connection with the performance of its obligations under this Agreement.

7.3) The term ***"Confidential Information***" shall not include information which A) is or becomes generally available to the public without breach of this Agreement, B) is in the possession of the Receiving Party prior to its disclosure by the Disclosing Party, C) becomes available from a third party not in breach of any obligations of confidentiality, D) is independently developed by the Receiving Party, or E) is required to be disclosed by the Receiving Party pursuant to law, rule, regulation, subpoena or court order, including but not limited to open public record laws.

7.4) The Parties recognize that the disclosure or use of a Disclosing Party's Confidential Information by the Receiving Party in violation of the provisions of this Section 7 may cause irreparable injury to the Disclosing Party; therefore, in the event either Party breaches the provisions of this Section 7, the other Party, in addition to any other remedies it may have, shall be entitled to seek preliminary and permanent injunctive relief without the necessity of posting a bond.

8) Miscellaneous.

8.1) General. If any provision of this Agreement is held to be unenforceable for any reason, such provision shall be reformed to the extent necessary to make it enforceable to the maximum extent permissible so as to implement the intent of the Parties, and the remainder of this Agreement shall continue in full force and effect. A waiver of any default is not a waiver of any subsequent default. The relationship between SwiftComply and Customer is one of independent contractors, not partnership, joint venture or agency. This Agreement shall be binding upon and inure to the benefit of the respective successors and permitted assigns of the Parties hereto. The United Nations Convention on Contracts for the International Sale of Goods and the Uniform Computer Information Transactions Act shall not apply to this Agreement. The Software is controlled by U.S. Export Regulations, and it may not be exported to or used by embargoed countries or individuals.

8.2) Entire Agreement. This Agreement and the accompanying SwiftComply Service Order(s), together, constitute a valid and binding agreement between the Parties and are intended to be the Parties' complete, integrated expression of the terms of their agreement with respect to the SwiftComply Service, and any prior agreements or understandings with respect to such subject matter are superseded hereby and fully merged herein.

8.3) Assignment. Neither Party will assign this Agreement in whole or in part to any third party without the prior written consent of the other Party; provided, however, either Party may assign this Agreement without such consent to any subsidiary or parent company of such Party or to any successor by way of any merger, consolidation or other corporate reorganization of such Party or sale of all or substantially all of the assets of such Party or to an entity that assumes, by sale, license or otherwise, the business activities that are the subject of this Agreement, provided that such subsidiary or parent company or successor assumes or is otherwise fully bound by all of the obligations of the assigning Party under this Agreement.

8.4) Marketing Materials. Customer agrees that SwiftComply may utilize Customer's name solely to identify it as a SwiftComply Customer on the SwiftComply Web site, in client lists and other marketing materials. Any other uses of Customer's name and/or logo (other than as included in the content and/or other items furnished to SwiftComply by Customer) shall require Customer's prior written consent.

8.5) Insurance. SwiftComply shall maintain commercial general liability insurance, cybersecurity insurance, professional liability insurance and auto liability insurance in amounts that are consistent with industry standards. SwiftComply shall maintain Worker's Compensation insurance as required by law.

8.6) No Boycott of Israel. SwiftComply hereby certifies that SwiftComply is not currently engaged in and shall not, for the duration of the Term of this Agreement, engage in a boycott of goods or services from the State of Israel; companies doing business in or with the State of Israel or authorized by, licensed by or organized under the laws of the State of Israel; or persons or entities doing business in the State of Israel.

8.7) Jurisdiction. This Agreement shall be governed by the applicable laws in the Customer State, without regard to conflict of laws rules. Any dispute, claim or controversy arising out of or relating to this Agreement or the breach, termination, enforcement, interpretation or validity thereof, including the determination of the scope or applicability of this agreement to arbitrate, shall be determined by arbitration in the Customer State before a panel of three arbitrators. Such arbitration shall be administered by JAMS pursuant to JAMS' Streamlined Arbitration Rules and Procedures. Judgment on an award, if any, may be entered in any court having jurisdiction. This clause shall not preclude parties from seeking provisional remedies in aid of arbitration from a court of appropriate jurisdiction. The Parties acknowledge that this Agreement evidences a transaction involving interstate commerce. Notwithstanding the provision with respect to applicable substantive law, any arbitration conducted pursuant to the terms of this Agreement shall be governed by the Federal Arbitration Act (9 U.S.C., Secs. 1-16).

8.8) Modification. SwiftComply shall have the right to modify this Agreement at any time by posting revised terms and conditions at the following URL: http://www.SwiftComply.com/terms-and-conditions. In the event that such modifications involve a material change to the Agreement, SwiftComply will seek approval from Customer via email. Changes will be binding on the date they are approved by Customer.

8.9) Force Majeure. If the performance of this Agreement or any obligations hereunder is prevented or interfered with by reason of fire or other casualty or accident, strikes or labor disputes, war or other violence, any law, proclamation, regulation, or requirement of any government agency, or any other act or condition beyond the reasonable control of a Party hereto, that Party upon giving prompt notice to the other Party shall be excused from such performance during such occurrence.

8.10) Notices. All notices, requests, or other communications between the Parties that are required or permitted hereunder will be in writing and will be given by: (a) delivery in person or by prepaid courier service with a nationally recognized courier company, (b) delivery by registered or certified mail, postage prepaid, return receipt requested, (c) by confirmed fax, or (d) email to the address and/or fax number set forth in the applicable SwiftComply Service Order. A Party may change the street or email address or fax number to which notice is to be sent by giving written notice of such change. Notices will be deemed given when received as evidenced by verification from the courier company, the mail or confirmation of email receipt or fax confirmation.

8.11) Titles & Subtitles. The titles and subtitles in this Agreement are used for convenience only and are not to be considered in construing it.

Service Order

6701 Koll Center Pkwy Suite 250, Pleasanton, CA 94566 - 619.304.6022 - www.swiftcomply.com

SWIFT COMPLY

Created by	Reilly Kirk	**Create Date**	9/28/2023
Contact Phone	503-522-3544		
Contact Email	reilly.kirk@swiftcomply.com	**Order Date**	

Customer Information

Customer	City of Everett	**Contact**	Sam Pann	**Billing Contact**	
Street Address	2930 Wetmore Avenue	**Title**	Application Business Systems Analyst	**Email**	accountspayable@everettwa.gov
City, St, Zip	Everett, WA, 98201	**Email**	spann@everettwa.gov	**Phone**	
Phone	425-257-8700	**Phone**	425.257.6415	**PO # (If any)**	

SwiftComply will provide your Services according to this schedule...

Period	Start Date	Description
Setup	3 weeks/signed	Setup Services
Initial	upon implementation	Subscription Services

The Services you will receive and the Fees for those Services are...

SKU	Set up Services	Standard/Non*	Quantity	Service Fees
C-3-502	Services-Advanced Implementation-data migration, training, CSV Billing Sync setup	S	1	$7,500.00
Total SwiftComply Setup Service Fee - Billed ONE-TIME				**$7,500.00**

SKU	Subscription Services	Standard/Non*	Quantity	Service Fees
C-1-203	Saas-Backflow-unlimited users & ongoing support	S	1	$9,875.00
Total SwiftComply Subscription Service Fee - Billed ANNUALLY IN ADVANCE				**$9,875.00**

To be clear, you will initially be billed as follows...

	Billing Date(s)	Amount(s)	Notes
Invoice #1	30 days/order date	$7,500.00	
Invoice #2	upon implementation	$9,875.00	

Billing Terms and Conditions

Valid Until	12/31/2023	Pricing set forth herein is valid only if SwiftComply Service Order is executed on or before this date.
Payment	Net 30	All invoices are due Net 30 days from the date of invoice.
Rate Increase	5.0% per annum	After the Initial Service Period, the Annual Subscription Service Fee shall automatically increase by this amount.
Renewals	Annual	Additional subscription years and/or renewals will be billed annually in accordance with pricing and terms set forth herein.
XC2 Credit	Conditional	Any overlap of XC2 annual contract and SwiftComply annual contract will be credited into first annual SwiftComply cost.
Tester Portal	Possioble waiver justification	At any time, Everett can require that all backflow tests be submitted via the Tester Online Portal for $5.00/passing test paid directly to SwiftComply via credit card. This would waive annual SaaS fee to City. Alternatively they may include the tester portal for an additional cost

General Terms & Conditions

Taxes	The Service Fees and Billing amounts set forth above in this SwiftComply Service Order **DO NOT** include applicable taxes. In accordance with the laws of the applicable state, in the event that sales, use or other taxes apply to this transaction, SwiftComply shall include such taxes on applicable invoices and Customer is solely responsible for such taxes, unless documentation is provided to SwiftComply demonstrating Customer's exemption from such taxes.
Customer Deliverables	Customer shall provide all deliverables and respond to all approval requests within three (3) business days of such requests. Any delay by Customer in meeting these deliverable requirements may result in a delayed launch of the applicable Service(s), but such delay shall not affect or change the Service Period(s) as set forth in this Service Order.
Term & Termination	Subject to the termination rights and obligations set forth in the SwiftComply Service Agreement, this SwiftComply Service Order commences upon the Order Date set forth herein and shall continue until the completion of the Service Period(s) for the Service(s) set forth herein. Each Service shall commence upon the Start Date set forth herein and shall continue until the completion of the applicable Service Period.
Auto-Renewal	After the Initial Period, the Service Period for any SwiftComply Annual Subscription Services shall automatically renew for successive annual periods (each an ***"Annual Term"***), unless either Party provides written notice of its desire not to renew at least sixty (60) days prior to the end of the then current Annual Term.
Non Standard Items (*)	Based on approved scope of work. Timeline for deliverables is not committal. Subscription Services billed is based on standard deliverables.
Agreement	This SwiftComply Service Order shall become binding upon execution by both Parties. The signature herein affirms your commitment to pay for the Service(s) ordered in accordance with the terms set forth in this SwiftComply Service Order and also acknowledges that you have read and agree to the terms and conditions set forth in the SwiftComply Service Agreement included alongside this document. This Service Order incorporates by reference the terms of such SwiftComply Service Agreement.

Customer		SwiftComply	
Signature		**Signature**	Reilly Kirk
Name	Cassie Franklin	**Name**	Reilly Kirk
Title	Mayor	**Title**	Account Executive

Please e-mail signed Service Order to Sales@SwiftComply.com

Attest

ADDENDUM
(CLOUD/OFFSITE HOSTING)

Vendor:	SwiftComply
Agreement:	SwiftComply Service Agreement and Service Order(s)

The City of Everett (City) and Vendor are parties to the Agreement as shown in the table above. Regardless of anything to the contrary in the Agreement, the Vendor agrees as follows:

1. **Compliance Requirements**: Vendor must maintain System and Organization Controls 2 (SOC2) compliance and provide annual SOC2 reports to demonstrate Vendor's compliance with the Trust Services Criteria. Vendor must ensure that all systems and services provided to the City meet or exceed the SOC2 requirements. Vendor will also promptly notify the City of any changes in its SOC2 compliance.

2. **Data Ownership**: The City shall own all right, title and interest in its data related to the Agreement. Vendor shall not access City User accounts, or City Data, except (i) in the course of data center operations, (ii) response to service or technical issues, (iii) as required by the express terms of the Agreement, or (iv) at City's written request.

3. **Confidentiality**: Vendor shall protect the confidentiality of City data and shall not disclose any City data to any third party without the City's prior written consent. Vendor shall maintain appropriate security measures to protect City data from unauthorized access, use, or disclosure.

4. **Data Protection**: Protection of personal privacy and sensitive data shall be an integral part of the business activities of Vendor to ensure that there is no inappropriate or unauthorized use of City data at any time. To this end, Vendor shall safeguard the confidentiality, integrity, and availability of City data and comply with the following conditions:

    a. All data obtained by Vendor from the City or from affiliates of the City under the Agreement shall become and remain property of the City.

    b. At no time shall any data or processes which either belongs to or are intended for the use of City or its officers, agents, or employees, be copied, disclosed, or retained by Vendor or any party related to Vendor for subsequent use unless such use is authorized by the City in writing.

5. **Data Location**: Vendor shall not store or transfer non-public City data outside of the United States. This includes backup data and disaster recovery locations. Vendor will permit its personnel and contractors to

access City data remotely only as required to provide technical support.

6. **Encryption**:

    a. Vendor shall encrypt all non-public data in transit regardless of the transit mechanism.

    b. For engagements where Vendor stores sensitive personally identifiable or otherwise confidential information, this data shall be encrypted at rest. Examples of such information include without limitation: social security number, date of birth, driver's license number, financial data, federal/state tax information, and hashed passwords. Vendor's encryption shall be consistent with validated cryptography standards as specified in National Institute of Standards and Technology FIPS140-2, Security Requirements. The key location and other key management details will be agreed to by City and Vendor technical staffs. **When Vendor cannot maintain encryption at rest, Vendor must maintain, for the duration of the Agreement, cyber security liability insurance coverage for any loss resulting from a data breach in accordance with Supplier shall procure and maintain insurance as required under cyber liability insurance requirements at: https://www.everettwa.gov/319/Procurement. Additionally, where encryption of data at rest is not possible, Vendor must provide to the City a description of its existing security measures that provide a similar level of protection.**

7. **Breach Notification and Recovery**: The City requires public breach notification when citizens' personally identifiable information is lost or stolen. Additionally, unauthorized access or disclosure of non-public data is considered to be a breach. Vendor will provide notification without unreasonable delay and all communication shall be pre-coordinated with the City. When Vendor or Vendor's subcontractors are responsible for the loss, Vendor shall bear all costs associated with the investigation, response and recovery from the breach, including without limitation credit monitoring services with a term of at least three years, mailing costs, website, and toll free telephone call center services. The City rejects any limitation on liability that purports to relieve a vendor from its own negligence or to the extent that it purports to creates an obligation on the part of the City or State of Washington to hold a vendor harmless.

8. **Notification of Legal Requests**: Vendor shall notify the City upon receipt of any electronic discovery, litigation holds, discovery searches, and expert testimonies related to, or which in any way might reasonably require access to, the data of the City. Vendor shall not respond to subpoenas, service of process, and other legal requests

related to the City without first notifying the City and providing the City a reasonable opportunity to respond, unless prohibited by law from providing such notice and opportunity.

9. **Termination and Suspension of Service**: In the event of termination or expiration of the Agreement, Vendor shall implement an orderly return of City data in CSV or XML or another mutually agreeable format. Vendor shall guarantee the subsequent secure disposal of City data.

    a. *Suspension of services*: During any period of suspension or contract negotiation or disputes, Vendor shall not take any action to intentionally erase any City data.

    b. *Termination or Expiration of any Services or Agreement in entirety*: In the event of termination or expiration of any services or the Agreement in entirety, Vendor shall not take any action to intentionally erase any City data for a period of 90 days after the effective date of the termination/expiration. After such 90-day period, Vendor shall have no obligation to maintain or provide any City data and shall thereafter, unless legally prohibited, dispose of all City data in its systems or otherwise in its possession or under its control as specified in section 9.d below. Within this 90-day period, Vendor will continue to secure and back up City data covered under the Agreement.

    c. *Post-Termination Assistance*: The City shall be entitled to any post-termination assistance generally made available with respect to the services provided under the Agreement unless a unique data retrieval arrangement has been established as part of the Agreement or otherwise agreed in writing by Vendor and the City.

    d. *Secure Data Disposal*: When requested by the City or when required under section 9.b above, Vendor shall destroy all requested data in all of its forms, for example: disk, CD/DVD, backup tape, and paper. Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST) approved methods, and certificates of destruction shall be provided to the City.

10. **Background Checks**: Vendor shall conduct criminal background checks and not utilize any staff, including subcontractors, to fulfill the obligations of the Agreement who have been convicted of any crime of dishonesty, including, but not limited to, criminal fraud. Vendor shall promote and maintain awareness of the importance of securing the City's information among Vendor's contractors, employees and agents.

11. **Data Dictionary**: Prior to go-live, Vendor shall provide to the City a data dictionary.

12. **Security Logs and Reports**: Vendor shall allow the City access to system security logs that affect the engagement under the Agreement, its data and or processes. This includes the ability for the City to request a report of the records that a specific user accessed over a specified period of time.

13. **Contract Audit**: Vendor shall allow the City to audit conformance to Agreement terms, system security and data centers as appropriate. The City may perform this audit or contract with a third party at its discretion at the City's expense. Such reviews shall be conducted with at least 30 days advance written notice and shall not unreasonably interfere with Vendor's business.

14. **Subcontractor Disclosure**: Vendor shall identify to City technical staff all of its strategic business partners related to services provided under the Agreement, including, but not limited to, all subcontractors or other entities or individuals who may be a party to a joint venture or similar agreement with Vendor, who will be involved in any application development and/or operations.

15. **Third-Party Vendors**: Vendor may use third-party vendors to provide services to City. Vendor must ensure that any third-party vendor is also SOC2 compliant and must provide to the City evidence of compliance upon City request.

16. **Business Continuity**: Vendor will maintain a comprehensive continuity of operations plan consistent with SOC2 requirements and will regularly review and update the plan as necessary. Vendor will provide the City with notice of any changes to the continuity of operations plan that may impact the City's use of the services under the Agreement.

    a. In the event of a disruption of Vendor's operations, Vendor will use commercially reasonable efforts to restore service as soon as possible, consistent with SOC2 requirements.

    b. Vendor will conduct regular tests of its continuity of operations plan to ensure that it is effective and up-to-date.

17. **Operational Metrics**: Vendor and the City technical staffs shall reach agreement on operational metrics and document these metrics in the Agreement or elsewhere in writing. Examples include, but are not limited to:

    a. Advance notice and change control for major upgrades and system changes

    b. System availability/uptime guarantee/agreed-upon maintenance downtime

    c. Recovery time objective/recovery point objective

    d. Security vulnerability scanning

18. **Third Party Supplier Access to City Data**: Vendor will provide an initial list of suppliers with access to City data and maintain the list for the duration of the Agreement. Vendor will notify the City within 90 days of any change to the supplier list.

This Addendum is part of the Agreement. In the event of any inconsistency between provisions of the Agreement and this Addendum, the provisions most stringent on Vendor shall control.

Signature on this Addendum may be by ink, pdf, email, fax, electronic signature or other electronic means, or any combination thereof, in which case such signature(s) will deemed an original signature.

VENDOR:

By: Reilly Kirk

Printed Name: Reilly Kirk

Title: Account Executive

Email Address of Signer: reilly.kirk@swiftcomply.com

ADDENDUM
(CAT 3 AND/OR CAT 4 DATA SHARING)

Receiving Party:	SwiftComply
Agreement:	SwiftComply Service Agreement and Service Order(s)
Short Description of Confidential Information to be Shared	The data stored in this applications contains the following: PII of customers, to include name & address. Maintenance records of sewer backflow prevention devices.
Authorized Use of Confidential Information	For the sole benefit of the City of Everett

Receiving Party and the City of Everett agree as follows:

1. Definitions

"Agreement" means agreement(s) between the City and Receiving Party as shown in the table above. An Agreement may be in the form of a contract, a work order, a statement of work, or any other document under which the City is to share or otherwise allow Receiving Party use of Confidential Information**.**

"Authorized Use" means the use of the Confidential Information set forth in the table above.

"**Authorized User**" means persons or classes of persons in Receiving Party's workforce who need access to Confidential Information to carry out their duties.

"**City**" means the City of Everett.

"City Data Security Requirements" means the requirements in the attached EXHIBIT A**:** CITY DATA SECURITY REQUIREMENTS**.**

"**Category 3 Confidential Information**" means information that is specifically protected from disclosure by law. It may include but is not limited to

- Personal Information about individuals, regardless of how that information is obtained;
- Information concerning employee personnel records, or

- Information regarding IT infrastructure and security of computer and telecommunications systems.

"**Category 4 Confidential Information**" means information that is specifically protected from disclosure by law and for which:

- Especially strict handling requirements are dictated, such as by statutes, regulations, or agreements; or
- Serious consequences could arise from unauthorized disclosure, such as threats to health and safety, or legal sanctions.

"**Confidential Information**" means information of any kind that is (1) categorized as Category 3 Confidential Information and/or Category 4 Confidential Information and (2) is disclosed by the City to Receiving Party.

"Confidential Data Breach" means the unauthorized acquisition, access, use, or disclosure of Confidential Information shared under this Agreement that compromises the security, confidentiality or integrity of the Confidential Information.

"Department" means the City's Information Technology Department.

"Director" means the City's Director of Information Technology**.**

"Disclosure" or "Disclose" means the disclosure, release, transfer, provision of, access to, or divulging information in any manner from one person to another person.

"Personal Information" means information identifiable to any person, including, but not limited to, information that relates to a person's name, health, finances, education, business, use or receipt of governmental services or other activities, addresses, telephone numbers, Social Security Numbers, driver license numbers, other identifying numbers, and any financial identifiers.

"**Receiving Party**" means the person set forth in the table above. Unless the specifically stated otherwise in this Addendum, "Receiving Party" includes the Receiving Party's owners, members, officers, directors, partners, employees, and/or agents. For purposes of any permitted subcontract, "Receiving Party" includes any subcontractor and its owners, members, officers, directors, partners, employees, and/or agents.

"Use" includes assessing or sharing data or the employment, application, utilization, examination, or analysis of data.

"**Washington OCIO Security Standard**" means the Washington Office of the Chief Information Officer Standard, 141.10 (https://ocio.wa.gov/policies/141-securinginformation-technology-assets/14110-securing-informationF-technology-assets), as such standard may be hereafter amended or superseded.

2. Purpose

The purpose of this Addendum is to provide terms and conditions under which the City will allow the restricted use of its Confidential Information to the Receiving Party, and under which the Receiving Party may receive and use the Confidential Information. This Addendum ensures that City Confidential Information is provided, protected, and used only for purposes authorized by this Addendum and state and federal law governing such use.

The Confidential Information to be shared under this Addendum is shared to help the City fulfill its functions as municipal corporation under the laws of the State of Washington.

3. Confidential Information Use Requirements

a. Receiving Party acknowledges that the City is providing City Confidential Information to Receiving Party under this Addendum.

b. The City does not provide Confidential Information for Receiving Party's discretionary use. Receiving Party must use the Confidential Information only for the Authorized Use.

c. Receiving Party shall not access or use the Confidential Information for any commercial purpose except as necessary for the Authorized Use or for any personal purpose.

d. Unless the Agreement specifically states otherwise, the Confidential Information may not be linked with other data sources without prior written agreement of the Director.

e. Unless the Agreement specifically states otherwise, the Receiving Party is not authorized to update or change any Confidential Information on any City system without prior written agreement of the Director.

4. Confidential Information Security

a. Receiving Party shall take due care and take reasonable precautions to protect the City's data from unauthorized physical and electronic access. Receiving Party certifies that it complies with the requirements of the Washington OCIO Security Standard's policies and standards for data security and access controls to ensure the confidentiality, integrity and availability of all data shared.

b. Receiving Party must protect and maintain all Confidential Information against unauthorized use and disclosure. This duty requires Receiving Party to employ reasonable security measures in accordance with Washington OCIO Security Standard. Receiving Party will restrict access to the Confidential Information by:

- Allowing access only to Authorized Users that have an authorized business requirement to view the Confidential Information; and
- Physically securing any computers, documents, or other media containing the Confidential Information.

c. Receiving Party for all Confidential Information must comply with the City Data Security Requirements (EXHIBIT A: CITY DATA SECURITY REQUIREMENTS).

5. **Confidential Information Non-Disclosure.**

a. Receiving Party shall not disclose, in whole or in part, the Confidential Information provided by City to any individual or entity, unless this Addendum specifically authorizes the disclosure. Confidential Information may be disclosed only to persons and entities that have the need to use the data to achieve the Authorized Use and only when such disclosure is in accordance with this Addendum.

b. Receiving Party shall not use, publish, transfer, sell, or otherwise disclose any Confidential Information for any purpose that is not directly connected with the Authorized Use, except:

- As required by law in accordance with Section 8; or
- With the prior written consent of the Director; or
- In the case of Confidential Information including Personal Information, with the prior written consent of the Director and the prior written consent of the person or personal representative of the person who is the subject of the Confidential Information.

c. Receiving Party must identify to the City:

- Authorized Users, which are those persons or classes of persons in its workforce who need access to Confidential Information to carry out their duties; and
- For each such person or class of persons, the types of information to which access is needed and any conditions appropriate to such access.

d. Authorized Users may access Confidential Information only for the Authorized Use. For each Authorized User:

- Receiving Party shall instruct the Authorized User on the requirements of this Addendum. This means that the Receiving Party shall ensure that all staff with access to the Confidential Information are aware of the use and disclosure requirements of this Addendum, will advise new staff of the provisions of this Addendum, and will provide an annual reminder to staff of these requirements. will access
- Receiving Party shall require the Authorized User to read and sign an agreement to comply with the non-disclosure requirements of this Addendum prior to being granted access to Confidential Information. This written agreement must be (i) maintained by Receiving Party for a minimum of six years from

the date the Authorized User's access to Confidential Information ends and (ii) provided to the City upon request.

e. Receiving Party must implement policies and procedures that limit the Confidential Information disclosed to Authorized Users to the amount reasonably necessary to achieve the purpose of the disclosure as described in this Addendum.

f. Any disclosure of Confidential Information contrary to this Addendum is unauthorized and is subject without limitation to penalties identified in law.

6. Confidential Information Disposal.

a. Receiving Party shall promptly dispose of Confidential Information and Confidential Information Products upon the occurrence of any of the following:

- Written request from the Department; or
- At the end of the term of the Agreement; or
- When no longer needed for the Authorized Use, or
- Six years have elapsed from the date the Confidential Information was received from the City, unless otherwise directed by the Department.

b. All Confidential Information and Confidential Information Product disposal must be in accordance with the City Data Security Requirements (EXHIBIT A: CITY DATA SECURITY REQUIREMENTS). Receiving Party will provide written certification of disposition at the Department's request in a form reasonably acceptable to the Department.

c. Receiving Party may retain Confidential Information as necessary for compliance or accounting purposes with the prior written consent of the Department, which will not be unreasonably withheld.

d. Paper documents with Confidential Information may be recycled through a contracted firm, provided the contract with the recycler specifies that the confidentiality of information will be protected, and the information destroyed through the recycling process. Paper documents containing Category 4 Confidential Information must be destroyed on-site through shredding, pulping, or incineration.

7. Confidential Data Breach

a. The compromise or potential compromise of Confidential Information that may be a breach that requires notice to affected individuals under RCW 42.56.590, RCW 19.255.010, or any other applicable breach notification law or rule must be reported to the Director within one (1) business day of discovery.

b. If the Receiving Party does not have full details about the incident, it will report what information it has and provide full details within 15 business days of discovery. To the extent possible, these initial reports must include at least:

   - The nature of the unauthorized use or disclosure, including a brief description of what happened, the date of the event(s), and the date of discovery;
   - A description of the types of information involved;
   - The investigative and remedial actions the Receiving Party or its subcontractor took or will take to prevent and mitigate harmful effects and protect against recurrence;
   - Any details necessary for a determination of whether the incident is a breach that requires notification under RCW 19.255.010, RCW 42.56.590, or any other applicable breach notification law or rule; and
   - Any other information City reasonably requests.

c. Receiving Party must also take actions to mitigate the risk of loss and comply with any notification or other requirements imposed by law or the City.

d. If notification to individuals must, <u>in the sole judgement of City</u>, be made, the Receiving Party will further cooperate and facilitate notification to required parties, which may include notification to affected individuals, the media, the Attorney General's Office, or other authorities based on applicable law. At the City's sole discretion, Receiving Party may be required to directly fulfill notification requirements, or if the City elects to perform the notifications, the Receiving Party must reimburse the City for all associated costs.

e. Receiving Party is responsible for all costs incurred in connection with a security incident, privacy breach, or potential compromise of Confidential Information, including:

   - Computer forensics assistance to assess the impact of a Confidential Data Breach, determine root cause, and help determine whether and the extent to which notification must be provided to comply with breach notification laws;
   - Notification and call center services for individuals affected by a security incident or privacy breach, including fraud prevention, credit monitoring, and identify theft assistance; and
   - Regulatory defense, fines, and penalties from any claim in the form of a regulatory proceeding resulting from a violation of any applicable privacy or security law(s) or regulation(s).

f. Receiving Party's obligations regarding breach notification survive any termination of this Addendum and continue for as long as Receiving Party maintains the Confidential Information and for any breach or potential breach, at any time.

8. Legally Required Disclosure of Confidential Information

Receiving Party shall provide Formal Notice to the City within five days after receipt of any of the following:

- A public records request under Chapter 42.56 RCW or any other public disclosure law;
- A subpoena for disclosure of Confidential Information; or
- Any other request for disclosure of Confidential Information that Receiving Party believes may legally bind Receiving Party to disclose Confidential Information.

Receiving Party shall cooperate with the City in redacting or withholding Confidential Information from disclosure in accordance with applicable law. If Receiving Party determines that it must disclose Confidential Information, Receiving Party shall provide the City at least fifteen (15) days prior Formal Notice of the date of such disclosure, so that the City may seek an injunction against disclosure.

9. Subcontractors

Receiving Party will not enter into any subcontract that discloses Confidential Information to a subcontractor not identified in the Agreement without written approval of the Director in the Director's sole discretion. If such disclosure is so approved, then (A) such disclosure will only be for the specific purpose and uses authorized by City and (B) Receiving Party must include all requirements of this Addendum (including its Data security terms, conditions and requirements) in any such subcontract. In no event will the existence of a subcontract operate to release or reduce any responsibility or liability of Receiving Party to the City for any Confidential Data Breach, breach of this Addendum or violation of applicable law.

10. HIPAA/Business Associate Agreement

If the Confidential Information includes protected health information (as defined under 45 CFR §§164.501 and 160.103), then the City and Receiving Party will execute a separate Business Associate Agreement as required by applicable law.

11. Insurance.

Receiving Party shall maintain the insurance set forth in the City Cyber-liability Insurance Requirements, available at https://www.everettwa.gov/319/Procurement.

12. Term and Termination

This Addendum remains in effect for as long as Receiving Party has access to or otherwise uses Data. This Addendum may remain in effect for a longer term than the Agreement.

13. Monitoring

Receiving Party agrees that City will have the right, at any time, to monitor, audit, and review activities and methods in implementing this Agreement in order to assure compliance.

At the City's request or in accordance with Washington OCIO Security Standard, Receiving Party shall obtain third-party audits covering Data Security and Permissible Use. Receiving Party may cover both the Permissible Use and the Data Security Requirements under the same audit, or under separate audits.

Receiving Party must maintain records related to compliance with this Addendum for six (6) years after expiration or termination of this Addendum. The City and its designee will have the right to access those records during that six-year period for purposes of audit.

14. General Provisions

a. **Amendments:** The City Data Security Requirements (EXHIBIT A: CITY DATA SECURITY REQUIREMENTS) may be modified by written agreement between the Director and an authorized representative of Receiving Party. All other provisions of this Addendum may be modified only by a written amendment signed by the Mayor of the City and by an authorized representative of Receiving Party.

b. **Assignment**: Receiving Party shall not assign this Addendum without the prior written consent of the Director, which may be withheld at the Director's sole discretion.

c. **Governing Law and Venue**: This Addendum is governed by, and will be construed and enforced in accordance with, the laws of the State of Washington. Snohomish County Superior is the exclusive venue for any lawsuit regarding this Addendum.

d. **Waiver**: Waiver of any breach or default on any occasion will not be deemed to be a waiver of any subsequent breach or default. Any waiver will not be construed to be a modification of the terms and conditions of this Addendum.

e. **Formal Notice**: When "Formal Notice" to the City is required under this Addendum, notice is only effective if in writing and the notice is delivered in accordance with either of the following:

- ➢ Delivered by email to the Director, and the Director specifically acknowledges receipt of the notice in writing; or
- ➢ The notice is physically delivered to <u>both</u> of following persons at the following physical addresses:

  Director of Information Technology
  2930 Wetmore Ave
  Everett, WA 98201

  City Clerk
  2930 Wetmore Ave
  Everett, WA 98201

f. **Indemnification**:

(1) Receiving Party shall be responsible for and shall indemnify, defend, and hold the City harmless from any and all claims, costs, charges, penalties, demands, losses, liabilities, damages, judgments, or fines, of whatsoever kind of nature, arising out of or relating to (i) Receiving Party or any of its subcontractor's performance or failure to perform this Addendum, or b) the acts or omissions of Receiving Party or any of its subcontractors.

(2) Receiving Party's duty to indemnify, defend, and hold the City harmless from any and all claims, costs, charges, penalties, demands, losses, liabilities, damages, judgments, or fines shall include the City's personnel-related costs, reasonable attorney's fees, court costs, and all related expenses.

(3) Receiving Party waives its immunity under Title 51 RCW to the extent it is required to indemnify, defend, and hold harmless the City and its officials, agents, or employees.

(4) Nothing in this section shall be construed as a modification or limitation on Receiving Party's obligation to procure insurance in accordance with this Addendum or the scope of such insurance.

g. **Public Records Act**. Receiving Party acknowledges that the City is subject to the Public Records Act (Chapter 42.56 RCW). This Addendum is a "public record" as defined in Chapter 42.56 RCW. Any documents or information submitted to the City by Receiving Party may also be construed as "public records" and therefore subject to public disclosure.

h. **Signatures:** The parties may execute this Addendum in multiple counterparts, each of which is deemed an original and all of which constitute only one Addendum. Signature on this Addendum may be by pdf, email, fax or other electronic means, in which case such signature(s) will have the same effect as an original ink signature.

h. **Coordination of Agreement and Addenda**: This Addendum is part of the Agreement. In the event of any inconsistency between provisions of the

Agreement and this Addendum, the provisions most stringent on Receiving Party shall control.

[signatures on following pages]

RECEIVING PARTY:

By: Reilly Kirk

Printed Name: Reilly Kirk

Title: Account Executive

Email Address of Signer: reilly.kirk@swiftcomply.com

CITY OF EVERETT:

By: ____________________

Cassie Franklin, Mayor

EVERETT

STANDARD DOCUMENT
APPROVED AS TO FORM
OFFICE OF THE CITY ATTORNEY
JULY 28, 2023

ATTEST:

____

OFFICE OF THE CITY CLERK

EXHIBIT A: CITY DATA SECURITY REQUIREMENTS

1. Definitions

In addition to the definitions set out in the Addendum, the definitions below apply to this Exhibit.

A) "Hardened Password" means a string of characters containing at least one (1) capital letter, one (1) lowercase letter, one (1) number, one (1) non-alphanumeric or special character.
   1) Minimum password length is 9 characters.
   2) Users may not use their previous ten (10) passwords.
   3) Cannot be a dictionary word or a proper name.
   4) Cannot be the same as a User ID or contain the User ID string.

B) "Portable/Removable Media" means any data storage device that can be detached or removed from a computer and transported, including but not limited to: optical media (e.g. CDs, DVDs); USB drives; or flash media (e.g. CompactFlash, SD, MMC). **Confidential Information is forbidden from being stored on, transported on, copied to or backed up on portable/removable media.**

C) "Portable/Removable Devices" means any small computing device that can be transported, including but not limited to: handhelds/PDAs/Smartphones; Ultramobile PC's, flash memory devices (e.g. USB flash drives, personal media players); and laptops/notebook/tablet computers.

D) "Secured Area" means an area to which only Authorized Users have access. Secured Areas may include buildings, rooms, or locked storage containers (such as a filing cabinet) within a room, as long as access to the Data is not available to unauthorized personnel.

E) "Transmitting" means the transferring of data electronically, such as via email, SFTP, etc.

F) "Trusted System(s)" means the following methods of physical delivery:
   1) hand-delivery by a person authorized to have access to the Confidential Information with written acknowledgement of receipt;
   2) United States Postal Service ("USPS") first class mail, or USPS delivery services that include Tracking, such as Certified Mail, Express Mail or Registered Mail; (3) commercial delivery services (e.g. FedEx, UPS, DHL) which offer tracking and receipt confirmation; and (4) City interoffice mail system, using a privacy envelope.

G) "Unique User ID" means a string of characters that identifies a specific user and which, in conjunction with a password, passphrase, or other mechanism, authenticates a user to an information system.

2. Data Transmission

A) When transmitting City's Confidential Information electronically, including via email, the Data must be encrypted using NIST 800-series approved algorithms (http://csrc.nist.gov/publications/PubsSPs.html). This includes transmission over the public internet.

B) When transmitting City's Confidential Information via paper documents, the Receiving Party must use a Trusted System.

3. Protection of Confidential Information

A) Confidential Information will be encrypted with NIST 800-series approved algorithms. Encryption keys will be stored and protected independently of the Confidential Information. Access to the Confidential Information will be restricted to Authorized Users through the use of access control lists, a Unique User ID, and a Hardened Password, or other authentication mechanisms which provide equal or greater security. Systems which contain or provide access to Confidential Information must be located in an area that is accessible only to authorized personnel, with access controlled through use of a key, card key, combination lock, or comparable mechanism.

B) Confidential Information may not be stored on Portable/Removable Media or Devices.

C) Any paper records containing Confidential Information must be protected by storing the records in a Secured Area that is accessible only to authorized personnel. When not in use, such records must be stored in a locked container, such as a file cabinet, locking drawer, or safe, to which only authorized persons have access.

4. Confidential Information Segregation

City's Confidential Information received under this MDSA must be segregated or otherwise distinguishable from non-City data. This is to ensure that when no longer needed by the Receiving Party, all of City's Confidential Information can be identified for return or destruction. It also aids in determining whether City's Confidential Information has or may have been compromised in the event of a security breach.

a. City's Confidential Information must be kept in one of the following ways:

i. on media (e.g. hard disk, tape, etc.) which will contain only City Confidential Information; or

ii. in a logical container on electronic media, such as a partition or folder dedicated to City's Confidential Information; or

iii. in a database that will contain only City Confidential Information; or

iv. within a database and will be distinguishable from non-City data by the value of a specific field or fields within database records; or

v. when stored as physical paper documents, physically segregated from non-City data in a drawer, folder, or other container.

b. When it is not feasible or practical to segregate City's Confidential Information from non-City data, then both City's Confidential Information and the non-City data with which it is commingled must be protected as described in this Exhibit.

5. Confidential Information Disposition

When the Confidential Information is no longer needed, except as noted below, the Confidential Information must be returned to City or destroyed. Media are to be destroyed using the US Department of Defense 5220.22-M Standard.

For City's Confidential Information stored on network disks, deleting unneeded Confidential Information is sufficient as long as the disks remain in a Secured Area and otherwise meet the requirements listed in Section 3, above. Destruction of the data as outlined in this section of this Exhibit may be deferred until the disks are retired, replaced, or otherwise taken out of the Secured Area.

EVERETT

ADDENDUM
(WASHINGTON STATE TRANSPARENCY LAWS)

Vendor:	SwiftComply
Agreement:	SwiftComply Service Agreement and Service Order(s)

The City of Everett and the above Vendor are parties to the above Agreement. Regardless of anything to the contrary in the Agreement, Vendor agrees as follows:

1. The Agreement does not require the City to keep confidential or otherwise refrain from disclosing anything that is determined by the City Clerk to be subject to disclosure under the Washington Public Records Act, chapter 42.56 RCW.

2. The Agreement does not require the City to destroy or return anything that is subject to retention requirements established by the Washington Secretary of State or established by applicable law.

3. The Agreement does not require the City to have any City employee sign any agreement.

4. The Agreement itself (and its related amendments, purchase orders, scopes of work, service orders or similar documents stating work to be done for the City or pricing for the City) are never confidential and may at any time be posted to the City's public website.

Signature on this Addendum may be by ink, pdf, email, fax, electronic signature or other electronic means, any of which is fully effective.

VENDOR:

By: Reilly Kirk

Printed Name: Reilly Kirk

Title: Account Executive

Email Address of Signer: reilly.kirk@swiftcomply.com

SwiftComply_SD

Final Audit Report 2023-10-10

Created:	2023-10-10
By:	Marista Jorve (mjorve@everettwa.gov)
Status:	Signed
Transaction ID:	CBJCHBCAABAAqvgBilyNCyifrGUec0fR9-mU3GqcTf2X

"SwiftComply_SD" History

Document created by Marista Jorve (mjorve@everettwa.gov)
2023-10-10 - 3:12:08 PM GMT

Document emailed to Cassie Franklin (cfranklin@everettwa.gov) for signature
2023-10-10 - 3:13:32 PM GMT

Email viewed by Cassie Franklin (cfranklin@everettwa.gov)
2023-10-10 - 3:33:27 PM GMT

Document e-signed by Cassie Franklin (cfranklin@everettwa.gov)
Signature Date: 2023-10-10 - 3:33:42 PM GMT - Time Source: server

Document emailed to Marista Jorve (mjorve@everettwa.gov) for signature
2023-10-10 - 3:33:44 PM GMT

Email viewed by Marista Jorve (mjorve@everettwa.gov)
2023-10-10 - 3:34:01 PM GMT

Document e-signed by Marista Jorve (mjorve@everettwa.gov)
Signature Date: 2023-10-10 - 3:34:24 PM GMT - Time Source: server

Agreement completed.
2023-10-10 - 3:34:24 PM GMT