CONSULTANT:	Aspire HR, Inc.
CONTACT PERSON:	Winnie Chu VP Alliances & Regulated Industries
ADDRESS:	5151 Belt Line Road, Suite 1125 Dallas, TX 75254
FEDERAL TAX ID NUMBER/U.B.I. NUMBER:	37-1372385
TELEPHONE/FAX NUMBER:	(972) 372-2815
COUNTY DEPT:	Information Technology
DEPT. CONTACT PERSON:	Matt Crisler
TELEPHONE:	(425) 388-3162
PROJECT:	Absence Management System
AMOUNT:	$366,205.00
FUND SOURCE:	002.5136104101
CONTRACT DURATION:	Five (5) years from contract execution unless extended or renewed pursuant to Section 2 hereof

AGREEMENT FOR PROFESSIONAL SERVICES

THIS AGREEMENT (the "Agreement") is made by and between SNOHOMISH COUNTY, a political subdivision of the State of Washington (the "County") and Aspire HR, Inc. a Texas corporation registered to conduct business in the State of Washington (the "Contractor"). In consideration of the mutual benefits and covenants contained herein, the parties agree as follows:

1. Purpose of Agreement; Scope of Services. The purpose of this Agreement is to provide an absence management system that is geared for the management of state and federally mandated leaves and accommodations. The system shall be used to provide a centralized solution for the County's increasing number of departments and employees and to ensure compliance with state and federal regulations. The scope of services is as defined in Schedule A - Statement of Work, and Schedule C - Partner Order Form – SAAS, attached hereto and by this reference made a part hereof. The software is as defined in Schedule B - Workforce Software Indirect SAAS Agreement, attached hereto and by this reference made a part hereof. This Agreement is the product of County RFP-23-021BC.

The services shall be performed in accordance with the requirements of this Agreement and with generally accepted practices prevailing in the western Washington region in the occupation or industry in which the Contractor practices or operates at the time the services are performed. The Contractor shall perform the work in a timely manner and in accordance with the terms of this Agreement. Any materials or equipment used by the Contractor in connection with performing the services shall be of good quality. The Contractor represents that it is fully qualified to perform the services to be performed under this Agreement in a competent and professional manner.

The Contractor will prepare and present status reports and other information regarding performance of the Agreement as the County may request.

2. Term of Agreement; Time of Performance. This Agreement shall be effective upon contract execution (the "Effective Date") and shall terminate five (5) years from software go-live date, PROVIDED, HOWEVER, that the term of this Agreement may be extended or renewed in additional five (5) year terms, for the duration of the County's use of the system (each a "Renewal Term"), at the sole discretion of the County, by written notice from the County to the Contractor. The Initial Term and the Renewal Terms shall collectively be referred to as the ("Term"). The Contractor shall commence the Services upon the Effective Date, and SaaS Subscriptions shall commence on the Effective Date and conclude after five (5) years from software go-live unless this Agreement is extended or renewed in accordance with section 2 of this Agreement, PROVIDED, HOWEVER, that the County's obligations after December 31, 2023 are contingent upon local legislative appropriation of necessary funds for this specific purpose in accordance with the County Charter and applicable law.

3. Compensation.

a. Services. The County will pay the Contractor for services as and when set forth in Schedule A and Schedule C, and software as described in Schedule B, which is attached hereto and by this reference made a part of this Agreement.

b. Overhead and Expenses. The Contractor's compensation for services set forth in Section 3a above includes overhead and expenses and no separate claims for reimbursement of overhead or expenses will be allowed under this Agreement.

c. Invoices. In accordance with the deliverables set forth in Schedule A and Schedule C, the Contractor shall submit properly executed invoices to the County indicating that the work has been performed and the amount due from the County. Subject to Section 8 of this Agreement, the County will pay such invoices within thirty (30) calendar days of receipt.

d. Payment. The County's preferred method of payment under this contract is electronic using the County's "e-Payable" system with Bank of America. The Contractor is highly encouraged to take advantage of the electronic payment method.

In order to utilize the electronic payment method, the Contractor shall email SnocoEpayables@snoco.org and indicate it was awarded a contract with Snohomish County and will be receiving payment through the County's e-Payable process. The Contractor needs to provide contact information (name, phone number and email address). The Contractor will be contacted by a person in the Finance Accounts Payable group and assisted with the enrollment process. This should be done as soon as feasible after County award of a contract or purchase order, but not exceeding ten (10) business days.

Department approved invoices received in Finance will be processed for payment within seven calendar days for e-Payable contractors. Invoices are processed for payment by Finance two times a week for contractors who have selected the e-Payable payment option.

In the alternative, if the Contractor does not enroll in the electronic ("e-Payable") payment method described above, contract payments will be processed by Finance with the issuance of paper checks or, if available, an alternative electronic method. Alternative payment methods, other than e-Payables, will be processed not more than 30 days from receipt of department approved invoices to Finance.

Upon acceptance of payment, the Contractor waives any claims for the goods or services covered by the Invoice. No advance payment shall be made for the goods or services furnished by Contractor pursuant to this Contract.

e. Contract Maximum. Total charges under this Agreement, all fees and expenses included, shall not exceed $366,205.00 for the initial five-year term of this Agreement.

4. Independent Contractor. The Contractor agrees that Contractor will perform the services under this Agreement as an independent contractor and not as an agent, employee, or servant of the County. This Agreement neither constitutes nor creates an employer-employee relationship. The parties agree that the Contractor is not entitled to any benefits or rights enjoyed by employees of the County. The Contractor specifically has the right to direct and control Contractor's own activities in providing the agreed services in accordance with the specifications set out in this Agreement. The County shall only have the right to ensure performance. Nothing in this Agreement shall be construed to render the parties partners or joint venturers.

The Contractor shall furnish, employ and have exclusive control of all persons to be engaged in performing the Contractor's obligations under this Agreement (the "Contractor personnel"), and shall prescribe and control the means and methods of performing such obligations by providing adequate and proper supervision. Such Contractor personnel shall for all purposes be solely the employees or agents of the Contractor and shall not be deemed to be employees or agents of the County for any purposes whatsoever. With respect to Contractor personnel, the Contractor shall be solely responsible for compliance with all rules, laws and regulations relating to employment of labor, hours of labor, working conditions, payment of wages and payment of taxes, including applicable contributions from Contractor personnel when required by law.

Because it is an independent contractor, the Contractor shall be responsible for all obligations relating to federal income tax, self-employment or FICA taxes and contributions, and all other so-called employer taxes and contributions including, but not limited to, industrial insurance (workers' compensation). The Contractor agrees to indemnify, defend and hold the County harmless from any and all claims, valid or otherwise, made to the County because of these obligations.

The Contractor assumes full responsibility for the payment of all payroll taxes, use, sales, income, or other form of taxes, fees, licenses, excises or payments required by any city, county, federal or state legislation which are now or may during the term of the Agreement be enacted as to all persons employed by the Contractor and as to all duties, activities and requirements by the Contractor in performance of the work under this Agreement. The Contractor shall assume exclusive liability therefor, and shall meet all requirements thereunder pursuant to any rules or regulations that are now or may be promulgated in connection therewith.

5. Ownership. Any and all data, reports, analyses, documents, photographs, pamphlets,

plans, specifications, surveys, films or any other materials created, prepared, produced, constructed, assembled, made, performed or otherwise produced by the Contractor or the Contractor's subcontractors or consultants for delivery to the County under this Agreement shall be the sole and absolute property of the County. Such property shall constitute "work made for hire" as defined by the U.S. Copyright Act of 1976, 17 U.S.C. § 101, and the ownership of the copyright and any other intellectual property rights in such property shall vest in the County at the time of its creation. Ownership of the intellectual property includes the right to copyright, patent, and register, and the ability to transfer these rights. Material which the Contractor uses to perform this Agreement but is not created, prepared, constructed, assembled, made, performed or otherwise produced for or paid for by the County is owned by the Contractor and is not "work made for hire" within the terms of this Agreement.

6. Changes. No changes or additions shall be made in this Agreement except as agreed to by both parties, reduced to writing and executed with the same formalities as are required for the execution of this Agreement.

7. County Contact Person. The assigned contact person (or project manager) for the County for this Agreement shall be:

Name:	Josh Carmichael
Title:	Human Resources Business Partner
Department:	Central Human Resources
Telephone:	(425) 312-0507
Email:	Josh.carmichael@snoco.org

8. County Review and Approval. When the Contractor has completed any discrete portion of the services, the Contractor shall verify that the work is free from errors and defects and otherwise conforms to the requirements of this Agreement. The Contractor shall then notify the County that said work is complete. The County shall promptly review and inspect the work to determine whether the work is acceptable. If the County determines the work conforms to the requirements of this Agreement, the County shall notify the Contractor that the County accepts the work. If the County determines the work contains errors, omissions, or otherwise fails to conform to the requirements of this Agreement, the County shall reject the work by providing the Contractor with written notice describing the problems with the work and describing the necessary corrections or modifications to same. In such event, the Contractor shall promptly remedy the problem or problems and re-submit the work to the County. The Contractor shall receive no additional compensation for time spent correcting errors. Payment for the work will not be made until the work is accepted by the County. The Contractor shall be responsible for the accuracy of work even after the County accepts the work.

If the Contractor fails or refuses to correct the Contractor's work when so directed by the County, the County may withhold from any payment otherwise due to the Contractor an amount that the County in good faith believes is equal to the cost the County would incur in correcting the errors, in re-procuring the work from an alternate source, and in remedying any damage caused by the Contractor's conduct.

9. Subcontracting and Assignment. The Contractor shall not subcontract, assign, or delegate any of the rights, duties or obligations covered by this Agreement without prior express written consent of the County, however Contractor may assign the right, duties and/obligations of this Agreement without prior written notice upon substantial change of control of Contractor, and where substantial change of control will not be considered a breach under this Agreement. Contractors will promptly provide notice to County of substantial change of control. Any attempt by the Contractor to subcontract, assign, or delegate any portion of the Contractor's obligations under this Agreement to another party in violation of the preceding sentence shall be null and void and shall constitute a material breach of this Agreement.

10. Records and Access; Audit; Ineligible Expenditures. The Contractor shall maintain adequate records to support billings. Said records shall be maintained for a period of seven (7) years after completion of this Agreement by the Contractor. The County or any of its duly authorized representatives shall have access at reasonable times to any books, documents, papers and records of the Contractor which are directly related to this Agreement for the purposes of making audit examinations, obtaining excerpts, transcripts or copies, and ensuring compliance by the County with applicable laws. Expenditures under this Agreement, which are determined by audit to be ineligible for reimbursement and for which payment has been made to the Contractor, shall be refunded to the County by the Contractor.

11. Indemnification.

a. Professional Liability.

The Contractor agrees to indemnify the County and, if any funds for this Agreement are provided by the State, the State and their officers, officials, agents and employees from damages and liability for damages, including reasonable attorneys' fees, court costs, expert witness fees, and other claims-related expenses, arising out of the performance of the Contractor's professional services under this Agreement, to the extent that such liability is caused by the negligent acts, errors or omissions of the Contractor, its principals, employees or subcontractors. The Contractor has no obligation to pay for any of the indemnitees' defense-related cost prior to a final determination of liability or to pay any amount that exceeds Contractor's finally determined percentage of liability based upon the comparative fault of the Contractor, its principals, employees and subcontractors. For the purpose of this section, the County and the Contractor agree that the County's and, if applicable, the State's costs of defense shall be included in the definition of damages above.

b. All Other Liabilities Except Professional Liability.

To the maximum extent permitted by law and except to the extent caused by the sole negligence of the County and, if any funds for this Agreement are provided by the State, the State, the Contractor shall indemnify and hold harmless the County and the State, their officers, officials, agents and employees, from and against any and all suits, claims, actions, losses, costs, penalties and damages of whatsoever kind or nature arising out of, in connection with, or incidental to the services and/or deliverables provided by or on behalf of the Contractor. In addition, the Contractor shall assume the defense of the County and, if applicable, the State and their officers and employees in all legal or claim proceedings arising out of, in connection with, or incidental to such services and/or deliverables and shall pay all defense expenses, including reasonable attorneys' fees, expert fees and costs incurred by the County and, if applicable, the State, on account of such litigation or claims.

The above indemnification obligations shall include, but are not limited to, all claims against the County and, if applicable, the State by an employee or former employee of the Contractor or its subcontractors, and the Contractor, by mutual negotiation, expressly waives all immunity and limitation on liability, as respects only the County and, if applicable, the State, under any industrial insurance act, including Title 51 RCW, other worker's compensation act, disability benefit act, or other employee benefit act of any jurisdiction which would otherwise be applicable in the case of such claim.

In the event that the County or, if applicable, the State incurs any judgment, award and/or cost including attorneys' fees arising from the provisions of this section, or to enforce the provisions of this section, any such judgment, award, fees, expenses and costs shall be recoverable from the Contractor.

In addition to injuries to persons and damage to property, the term "claims," for purposes of this provision, shall include, but not be limited to, assertions that the use or transfer of any software, book, document, report, film, tape, or sound reproduction or material of any kind, delivered hereunder, constitutes an infringement of any copyright, patent, trademark, trade name, and/or otherwise results in an unfair trade practice.

The indemnification, protection, defense and save harmless obligations contained herein shall survive the expiration, abandonment or termination of this Agreement.

Nothing contained within this provision shall affect or alter the application of any other provision contained within this Agreement.

12. Insurance Requirements. The Contractor shall procure by the time of execution of this Agreement, and maintain for the duration of this Agreement, (i) insurance against claims for injuries to persons or damage to property which may arise from or in connection with the performance of the services hereunder by the Contractor, its agents, representatives, or employees, and (ii) a current certificate of insurance and additional insured endorsement when applicable.

a. General. Each insurance policy shall be written on an "occurrence" form, except that Professional Liability, Errors and Omissions coverage, if applicable, may be written on a claims made basis. If coverage is approved and purchased on a "claims made" basis, the Contractor warrants continuation of coverage, either through policy renewals or the purchase of an extended discovery period, if such extended coverage is available, for not less than three (3) years from the date of completion of the work which is the subject of this Agreement.

By requiring the minimum insurance coverage set forth in this Section 12, the County shall not be deemed or construed to have assessed the risks that may be applicable to the Contractor under this Agreement. The Contractor shall assess its own risks and, if it deems appropriate and/or prudent, maintain greater limits and/or broader coverage.

b. No Limitation on Liability. The Contractor's maintenance of insurance as required by this Agreement shall not be construed to limit the liability of the Contractor to the coverage provided by such insurance, or otherwise limit the County's recourse to any remedy available at law or in equity.

c. Minimum Scope and Limits of Insurance. The Contractor shall maintain coverage at least as broad as, and with limits no less than:

(i) General Liability: $1,000,000 combined single limit per occurrence for bodily injury, personal injury and property damage, and for those policies with aggregate limits, a $2,000,000 aggregate limit. CG 00 01 current edition, including Products and Completed Operations;

(ii) Automobile Liability: N/A combined single limit per accident for bodily injury and property damage. CA 0001 current edition, Symbol 1;

(iii) Workers' Compensation: To meet applicable statutory requirements for workers' compensation coverage of the state or states of residency of the workers providing services under this Agreement;

(iv) Employers' Liability or "Stop Gap" coverage: $1,000,000

(v) Professional Liability/Cyber Liability: an amount not less than $3,000,000 per claim and in the annual aggregate, covering all acts, errors, omissions, negligence, infringement of intellectual property (except patent and trade secret) and network and privacy risks (including coverage for unauthorized access, failure of security, breach of privacy perils, wrongful disclosure of information, as well as notification costs and regulatory defense) in the performance of services for Snohomish County or on behalf of Snohomish County hereunder. Such insurance shall be maintained in force at all times during the term of the agreement and for a period of 3 years thereafter for services completed during the term of the agreement.

If Vendor has access to Confidential Information or Personally Identifiable Information, Vendor shall also carry Privacy and Network Security (also known as Cyber) insurance in the amount of not less than Three Million Dollars ($ 3,000,000) for each claim and in the aggregate. Such policy shall include coverage for all costs incurred to respond to the theft, loss, unauthorized disclosure, wrongful collection or access to information, and all damages resulting from such breach, including fines and penalties imposed.

d. Other Insurance Provisions and Requirements. The insurance coverages required in this Agreement for all liability policies except workers' compensation and Professional Liability, if applicable, must contain, or must be endorsed to contain, the following provisions:

(i) The County, its officers, officials, employees and agents are to be covered as additional insureds as respects liability arising out of activities performed by or on behalf of the Contractor in connection with this Agreement. Such coverage shall be primary and non-contributory insurance as respects the County, its officers, officials, employees and agents. Additional Insured Endorsement shall be included with the certificate of insurance, "CG 2026 07/04" or its equivalent is required.

(ii) The Contractor's insurance coverage shall apply separately to each insured against whom a claim is made and/or lawsuit is brought, except with respect to the limits of the insurer's liability.

(iii) Any deductibles or self-insured retentions must be declared to, and approved by, the County. The deductible and/or self-insured retention of the policies shall not limit or apply to the Contractor's liability to the County and shall be the sole responsibility of the Contractor.

(iv) Insurance coverage must be placed with insurers with a Best's Underwriting Guide rating of no less than A:VIII, or, if not rated in the Best's Underwriting Guide, with minimum surpluses the equivalent of Best's surplus size VIII. Professional Liability, Errors and Omissions insurance coverage, if applicable, may be placed with insurers with a Best's rating of B+:VII. Any exception must be approved by the County.

Coverage shall not be suspended, voided, canceled, reduced in coverage or in limits until after forty-five (45) calendar days' prior written notice has been given to the County.

If at any time any of the foregoing policies fail to meet minimum requirements, the Contractor shall, upon notice to that effect from the County, promptly obtain a new policy, and shall submit the same to the County, with the appropriate certificates and endorsements, for approval.

e. Subcontractors. The Contractor shall include all subcontractors as insureds under its policies, or shall furnish separate certificates of insurance and policy endorsements for each subcontractor. **Insurance coverages provided by subcontractors instead of the Contractor as evidence of compliance with the insurance requirements of this Agreement shall be subject to all of the requirements stated herein.**

13. County Non-discrimination. It is the policy of the County to reject discrimination which denies equal treatment to any individual because of his or her race, creed, color, national origin, families with children, sex, marital status, sexual orientation, age, honorably discharged veteran or military status, or the presence of any sensory, mental, or physical disability or the use of a trained dog guide or service animal by a person with a disability as provided in Washington's Law against Discrimination, Chapter 49.60 RCW, and the Snohomish County Human Rights Ordinance, Chapter 2.460 SCC. These laws protect against specific forms of discrimination in employment, credit transactions, public accommodation, housing, county facilities and services, and county contracts.

The Contractor shall comply with the substantive requirements of Chapter 2.460 SCC, which are incorporated herein by this reference. Execution of this Agreement constitutes a certification by the Contractor of the Contractor's compliance with the requirements of Chapter 2.460 SCC. If the Contractor is found to have violated this provision, or to have furnished false or misleading information in an investigation or proceeding conducted pursuant to this Agreement or Chapter 2.460 SCC, this Agreement may be subject to a declaration of default and termination at the County's discretion. This provision shall not affect the Contractor's obligations under other federal, state, or local laws against discrimination.

14. Federal Non-discrimination. Snohomish County assures that no persons shall on the

grounds of race, color, national origin, or sex as provided by Title VI of the Civil Rights Act of 1964 (Pub. L. No. 88-352), as amended, and the Civil Rights Restoration Act of 1987 (Pub. L. No. 100-259) be excluded from participation in, be denied the benefits of, or be otherwise subjected to discrimination under any County sponsored program or activity. Snohomish County further assures that every effort will be made to ensure nondiscrimination in all of its programs and activities, whether those programs and activities are federally funded or not.

15. Employment of County Employees. SCC 2.50.075, "Restrictions on future employment of County employees," imposes certain restrictions on the subsequent employment and compensation of County employees. The Contractor represents and warrants to the County that it does not at the time of execution of this Agreement, and that it shall not during the term of this Agreement, employ a former or current County employee in violation of SCC 2.50.075. For breach or violation of these representations and warranties, the County shall have the right to terminate this Agreement without liability.

16. Compliance with Other Laws. The Contractor shall comply with all other applicable federal, state and local laws, rules, and regulations in performing this Agreement.

17. Compliance with Grant Terms and Conditions. The Contractor shall comply with any and all conditions, terms and requirements of any federal, state or other grant, if any, that wholly or partially funds the Contractor's work hereunder.

18. Prohibition of Contingency Fee Arrangements. The Contractor warrants that it has not employed or retained any company or person, other than a bona fide employee working solely for the Contractor, to solicit or secure this Agreement and that it has not paid or agreed to pay any company or person, other than a bona fide employee working solely for the Contractor, any fee, commission, percentage, brokerage fee, gifts or any other consideration, contingent upon or resulting from the award or making of this Agreement. For breach or violation of this warranty, the County shall have the right to terminate this Agreement without liability or, in its discretion, to deduct from the Agreement price or consideration, or otherwise recover, the full amount of such fee, commission, percentage, brokerage fee, gift or contingent fee.

19. Force Majeure. If either party is unable to perform any of its obligations under this Agreement as a direct result of an unforeseeable event beyond that party's reasonable control, including but not limited to an act of war, act of nature (including but not limited to earthquake and flood), embargo, riot, sabotage, labor shortage or dispute (despite due diligence in obtaining the same), or governmental restriction imposed subsequent to execution of the Agreement (collectively, a "force majeure event"), the time for performance shall be extended by the number of days directly attributable to the force majeure event. Both parties agree to use their best efforts to minimize the effects of such failures or delays.

20. Intentionally Removed.

21. Non-Waiver of Breach; Termination.

a. The failure of the County to insist upon strict performance of any of the covenants or agreements contained in this Agreement, or to exercise any option conferred by this

Agreement, in one or more instances shall not be construed to be a waiver or relinquishment of those covenants, agreements or options, and the same shall be and remain in full force and effect.

b. If the Contractor breaches any of its obligations hereunder, and fails to cure the same within fourteen (14) calendar days of written notice to do so by the County, the County may terminate this Agreement, in which case the County shall pay the Contractor only for the services fully or partially completed up to and including the date of written notice, and corresponding reimbursable expenses, if any, accepted by the County in accordance with Sections 3 and 8 hereof.

c. The County may terminate this Agreement upon sixty (60) calendar days' written notice to the Contractor for any reason other than stated in subparagraph b above, in which case payment shall be made in accordance with Sections 3 and 8 hereof for the services fully or partially completed up to and including the termination date, and corresponding reimbursable expenses, if any, reasonably and directly incurred by the Contractor in performing this Agreement prior to receipt of the termination notice.

d. Termination by the County hereunder shall not affect the rights of the County as against the Contractor provided under any other section or paragraph herein. The County does not, by exercising its rights under this Section 21, waive, release or forego any legal remedy for any violation, breach or non-performance of any of the provisions of this Agreement. At its sole option, the County may deduct from the final payment due the Contractor (i) any damages, expenses or costs arising out of any such violations, breaches or non-performance and (ii) any other set-offs or credits including, but not limited to, the costs to the County of selecting and compensating another contactor to complete the work of the Agreement.

22. LIMITATION OF LIABILITY

22.1 Liability Exclusion. NEITHER PARTY WILL BE LIABLE TO THE OTHER PARTY (NOR TO ANY PERSON CLAIMING RIGHTS DERIVED FROM SUCH OTHER PARTY'S RIGHTS) FOR CONSEQUENTIAL, INCIDENTAL, INDIRECT, PUNITIVE, OR EXEMPLARY DAMAGES OF ANY KIND (INCLUDING, WITHOUT LIMITATION, LOST REVENUES OR PROFITS, OR LOSS OF GOODWILL OR REPUTATION) WITH RESPECT TO ANY CLAIMS BASED ON CONTRACT, TORT OR OTHERWISE (INCLUDING NEGLIGENCE AND STRICT LIABILITY) ARISING OUT OF OR RELATING TO THIS AGREEMENT, REGARDLESS OF WHETHER THE PARTY LIABLE OR ALLEGEDLY LIABLE WAS ADVISED, HAD OTHER REASON TO KNOW, OR IN FACT KNEW OF THE POSSIBILITY THEREOF.

22.2 Limitation of Damages. EACH PARTY'S MAXIMUM LIABILITY ARISING OUT OF OR RELATING TO THIS AGREEMENT, REGARDLESS OF THE CAUSE OF ACTION (WHETHER IN CONTRACT, TORT, BREACH OF WARRANTY, OR OTHERWISE), WILL NOT EXCEED THE AGGREGATE AMOUNT OF THE FEES PAID TO CONTRACTOR BY COUNTY UNDER THE THIS AGREEMENT DURING THE 6 MONTH PERIOD IMMEDIATELY PRECEDING THE INCIDENT GIVING RISE TO THE APPLICABLE CAUSE OF ACTION.

22.3 Exceptions. THE FOREGOING EXCLUSIONS AND LIMITATIONS OF LIABILITY SET FORTH IN SECTION 22.3 AND SECTION 22.2 SHALL NOT APPLY TO (I) THE FAILURE OF COUNTY TO MAKE PAYMENTS, OR (II) LIABILITY RESULTING FROM THE GROSS NEGLIGENCE OR WILLFUL MISCONDUCT OF A PARTY.

23. Notices. All notices and other communications shall be in writing and shall be sufficient if given, and shall be deemed given, on the date on which the same has been mailed by certified mail, return receipt requested, postage prepaid, addressed as follows:

If to the County:
Snohomish County Information Technology
3000 Rockefeller Avenue, M/S 709
Everett, Washington 98201
Attention: Dee White
Senior IT Contract Specialist

and to:
Snohomish County Purchasing Division
3000 Rockefeller Avenue, M/S 507
Everett, Washington 98201
Attention: Purchasing Manager

If to the Contractor:
Aspire HR, Inc.
5151 Belt Line Road, Suite 1125
Dallas, TX 75254
Attention: Winnie Chu
VP Alliances and Regulated Industries

The County or the Contractor may, by notice to the other given hereunder, designate any further or different addresses to which subsequent notices or other communications shall be sent.

24. Confidentiality. The Contractor shall not disclose, transfer, sell or otherwise release to any third party any confidential information gained by reason of or otherwise in connection with the Contractor's performance under this Agreement. The Contractor may use such information solely for the purposes necessary to perform its obligations under this Agreement. The Contractor shall promptly give written notice to the County of any judicial proceeding seeking disclosure of such information.

25. Public Records Act. This Agreement and all public records associated with this Agreement shall be available from the County for inspection and copying by the public where required by the Public Records Act, Chapter 42.56 RCW (the "Act"). To the extent that public records then in the custody of the Contractor are needed for the County to respond to a request under the Act, as determined by the County, the Contractor agrees to make them promptly available to the County. If the Contractor considers any portion of any record provided to the County under this Agreement, whether in electronic or hard copy form, to be protected from disclosure under law, the Contractor shall clearly identify any specific information that it claims to be confidential or proprietary. If the County receives a request under the Act to inspect or copy the information so identified by the Contractor and the County determines that release of the information is required by the Act or otherwise appropriate, the County's sole obligations shall be

to notify the Contractor (a) of the request and (b) of the date that such information will be released to the requester unless the Contractor obtains a court order to enjoin that disclosure pursuant to RCW 42.56.540. If the Contractor fails to timely obtain a court order enjoining disclosure, the County will release the requested information on the date specified.

The County has, and by this section assumes, no obligation on behalf of the Contractor to claim any exemption from disclosure under the Act. The County shall not be liable to the Contractor for releasing records not clearly identified by the Contractor as confidential or proprietary. The County shall not be liable to the Contractor for any records that the County releases in compliance with this section or in compliance with an order of a court of competent jurisdiction.

26. Interpretation. This Agreement and each of the terms and provisions of it are deemed to have been explicitly negotiated by the parties. The language in all parts of this Agreement shall, in all cases, be construed according to its fair meaning and not strictly for or against either of the parties hereto. The captions and headings of this Agreement are used only for convenience and are not intended to affect the interpretation of the provisions of this Agreement. This Agreement shall be construed so that wherever applicable the use of the singular number shall include the plural number, and vice versa, and the use of any gender shall be applicable to all genders.

27. Complete Agreement. The Contractor was selected through the County's RFP identified in Section 1. The RFP and the Contractor's response are incorporated herein by this reference. To the extent of any inconsistency among this Agreement, the RFP, and the Contractor's response, this Agreement shall govern. To the extent of any inconsistency between the RFP and the Contractor's response, the RFP shall govern.

28. Conflicts between Attachments and Text. Should any conflicts exist between any attached exhibit or schedule and the text or main body of this Agreement, the text or main body of this Agreement shall prevail.

29. No Third Party Beneficiaries. The provisions of this Agreement are for the exclusive benefit of the County and the Contractor. This Agreement shall not be deemed to have conferred any rights, express or implied, upon any third parties.

30. Governing Law; Venue. This Agreement shall be governed by the laws of the State of Washington. The venue of any action arising out of this Agreement shall be in the Superior Court of the State of Washington, in and for Snohomish County.

31. Severability. Should any clause, phrase, sentence or paragraph of this agreement be declared invalid or void, the remaining provisions of this Agreement shall remain in full force and effect.

32. Authority. Each signatory to this Agreement represents that he or she has full and sufficient authority to execute this Agreement on behalf of the County or the Contractor, as the case may be, and that upon execution of this Agreement it shall constitute a binding obligation of the County or the Contractor, as the case may be.

33. Survival. Those provisions of this Agreement that by their sense and purpose should survive expiration or termination of the Agreement shall so survive.

34. Execution in Counterparts. This Agreement may be executed in counterparts, each of which shall constitute an original and all of which shall constitute one and the same Agreement.

35. Entire Agreement and Order of Precedence. This written Agreement and its corresponding Exhibits and Schedules constitutes the entire agreement between the parties with respect to the subject matter contained herein, superseding all previous agreements, statements or understandings pertaining to such subject matter. In the event of any conflict between this Master Document and any of the attached Exhibits or Schedules, the precedence of Documents shall be as follows:

1. Agreement
2. Schedule A Statement of Work and attachments
3. Schedule B Workforce Software Indirect SAAS Agreement and attachments
4. Schedule C Partner Order Form - SAAS
5. RFP-23-021BC and Contractor's Response to RFP-23-021BC

SNOHOMISH COUNTY:

Klein, Ken Digitally signed by Klein, Ken
Date: 2024.04.10 13:09:09
-07'00'

County Executive Ken Klein
Executive Director Date

Approved as to insurance
and indemnification provisions:

Barker, Sheila Digitally signed by Barker, Sheila
Date: 2024.03.14 10:01:49 -07'00'

Risk Management Date

ASPIRE HR, INC.:

Joe Chevalier

3/13/2024 | 14:01 CDT Date

~~CFO~~

Approved as to form only:

Legal Counsel to the Contractor Date

COUNCIL USE ONLY

Approved 4/10/2024

ECAF # 2024-0323

MOT/ORD Motion 24-133

Schedule A

Statement of Work

Developed for:
Snohomish County Government

Prepared by:
Aspire HR, LLC

Date:
September 25, 2023

This Statement of Work is made part of and incorporated by this reference into the Professional Services Agreement (“Agreement “) between Snohomish County (“County”) and Aspire HR, Inc. (“ASPIREHR” or “AHR” or “Contractor”) (“Agreement”). In the event of any inconsistency or conflict between the terms and conditions of this SOW and the Agreement, the Agreement shall control. In areas where the Agreement refers to the SOW to provide additional clarity or detail, the SOW shall control. Capitalized terms used but not defined herein shall have the meaning given in the Agreement.

1. Contract Information

Contract Information	
Statement of Work Type	Time & Material
Invoice Address and Billing Contact	DIS.Admin@co.snohomish.wa.us
Aspire HR Key Contacts	**Aspire HR Account Executive:** Winnie Chu, VP Alliances and Regulated Industries wchu@aspirehr.com; 972-372-2815 **Aspire HR Professional Services Contacts:** Jennifer Adams, VP Delivery jadams@aspirehr.com; 972-372-2876
County Key Contacts	**Snohomish Executive Sponsor:** Rhea Reynolds, HR Director Rhea.Reynolds@snoco.org; 425 388-3932 **Snohomish Stakeholder:** Joshua Carmichael, HRBP Leaves and Accommodations Josh.Carmichael@snoco.org; 425-312-0507 Mandy Iverson, Project Coordinator (HRIS & People Analytics) Mandy.Iverson@snoco.org; 425-312-0709

2. Project Scope

AspireHR, Inc. is a value-added reseller of WorkForce Absence software developed by WorkForce Software, LLC and is reselling licensing and ongoing support to the County as detailed in Schedule B, the WorkForce Software Indirect SaaS Agreement and Schedule C, the Partner Order Form – SaaS. In addition to reselling licensing and software manufacturer support, AspireHR shall provide configuration and implementation services to the County as detailed in this Statement of Work (SOW). The County desires to obtain a license to use such software and have the Contractor guide the County through implementation, software configuration and provide initial support through go-live. The Contractor desires to license such software to the County and perform the services on the terms and conditions set forth herein.

Outlined below are the solution modules for SuccessFactors, providing core features and definition summary. Additional clarity and precision of scope detail, requirements and assumptions are identified in Appendix A of this SOW. References to Diamond Client is installation of a standard technical solution. References to Sapphire Methodology are WFS standard 3 iterations approach for building requirements and unit testing.

2.0 Project Scope Overview	
Release Scope	• Absence Compliance Tracker Implementation • Diamond Client Accelerators o Diamond Client Configuration (if applicable*) is AspireHR prebuilt solution using best practices and key features. o Diamond Supporting Documentation & Tools (Editable Samples) ▪ Diamond Business Processes for supported modules ▪ Diamond Training Plans for Training Communications & Change Management ▪ Diamond Test Scenarios/Scripts for supported modules ▪ Diamond QRGs for supported modules ▪ Diamond Train the Trainer Deck ▪ Pre-written test script templates constructed from the Diamond Client Configuration have been prepared and will be transitioned *Note: Diamond Client may not be available for all modules/products
Implementation Duration	• 12 weeks
Languages Supported	• US English
Countries & Currency Supported	• United States (US Dollar)
Sapphire Client Implementation	• All modules listed above shall be preconfigured by AspireHR and delivered with the Diamond Client accelerator (where applicable) with iterative unit testing including a round of User Acceptance Testing (UAT) ("Iteration"). o Up to 3 Iterations of unit testing and 1 cycle of UAT. o Refer to the accompanying Appendix A for module specific scope details.

	o Implementation and deployment tasks shall be conducted in up to 2 environments: Test or Development and Production tenants. A third instance shall be supported for Payroll and Employee Central implementations only. o AspireHR consultants shall capture initial requirements within the guidelines of the attached Appendix A in a Business Requirements Document, which shall subsequently be used for requirements approval and Unit testing. o During UAT and Hypercare, defects will reference the requirement number as documented and signed off by Customer at completion of Realization from the Business Requirements Document. Items not identified as requirements will be treated as changes and may incur additional costs, as documented through the change request process. o AspireHR consultants shall provide a completed workbook at production cutover/go-live that captures the technical configuration. o 1 medium complexity demographic integration from HRIS to Workforce Software is in scope
Consulting Team	• Certified AspireHR resources shall be assigned and shall conduct all work virtually
Post Go-Live Support	*Hypercare:* • Hypercare is two (2) weeks of Post Go-Live support as part of the project timeline • Hypercare Support includes: o Configuration defect resolution i.e., configuration does not reflect the final Business Requirements Document • Hypercare Support excludes: o Design changes – configuration and XML changes outside of a configuration defect or an approved change request o Application defect management
Additional Items	• Enhancements or new functionality delivered via SuccessFactors system releases that occur after the effective date of this Statement of Work are not in scope. Pricing for any new enhancements or new functionality can be provided upon request. • Consulting by AspireHR resources to be provided for the in-scope deliverables only. Additional items and functionality requests shall be captured in a change log to be assessed and implemented on a time and materials basis in accordance with section 14 of this SOW, Change Process. • Changes to configuration scope identified after the last Iteration (final requirements gathering) shall be completed after go-live, either through a support services transaction or a separate project after go-live that is subject to approval through the Change Process and may incur additional costs. • This Statement of Work describes the delivery of professional services only. The software licensing and support related to this implementation is detailed in Schedules B and C. Any software, subscription service, tools or hardware required by County for the operation of the SuccessFactors hosted service or other related

	integration software in addition to Schedules B and C are not supplied under this Statement of Work and must be acquired and licensed separately by County.

3. Definitions

- “Acceptance” means (i) the work and/or deliverables substantially satisfy the functions and specifications agreed to by both parties and as described herein; and (ii) the work and/or deliverables shall be deemed delivered and acceptable by the County, following completion of any acceptance testing with written acknowledgement from the County testifying of acceptance if applicable, after the rendering of work and the acceptance of deliverables as described in this SOW and the Agreement.
- “Final Acceptance” means the point when County acknowledges that the Contractor has performed the entire work product in accordance with the Contract, or the entire product has been used in a production environment for 3 months.
- “Defect” means (1) any failure of the Software to operate in accordance with the documentation, functional specifications, or performance standards; and/or (2) any failure of the Contractor to perform the services in accordance with the service level standards.
- “Material Defect” means any Defect that (1) severely impacts the County’s ability to use the software or the system or the Contractor’s ability to provide services, or (2) has a significant financial impact on the County.

4. Assumptions

The following assumptions apply to the AspireHR implementation:

- This Statement of Work shall represent a continuous single event without delays. AspireHR has the right to reassign project resources if project delays or suspension extends beyond 4 weeks at any point within the project. Pauses of work at County request beyond 2 weeks shall incur delay fees for project extension as defined in section 12.
- This Statement of Work is based on current application features only as outlined under Configuration Scope above. Configuration of future enhancements, or enhancements released during the duration of the project, are not included. A Change Request can be initiated to add or remove scope from the project.
- Consultant will not provide legal advice and it is the County’s responsibility to validate the system meets any legal requirements with their qualified legal advisors. This Statement of Work describes the delivery of professional services only. Any software, subscription service, tools or hardware required by County for the operation of the SuccessFactors hosted service or other related integration software are not supplied under this Statement of Work and must be acquired or licensed separately by County.
- All module configuration and deployment shall be in up to 2 instances: Beginning in Test or Development and moving to Production tenants unless otherwise specified in Appendix A. The applicable Development or Test environment shall be updated by the County with all existing production configuration (if applicable) prior to the start of the project.
- County is responsible for all migration of employee data (if applicable) into the system. AspireHR shall provide guidance on the formatted templates for County to populate and assist with their import into the WorkForce Software system. County is responsible for all third-party data integration, data cleansing, data mapping, and transformation of data into provided templates and validation of data accuracy once imported into the Workforce Software system.

- AspireHR Resources shall conduct work virtually using AspireHR equipment.

5. Scope Exclusion

The following are exclusions from this project scope and shall not be provided or configured:

- Custom Report Development
- Custom Training Services
- Custom Test Scripts, Scenarios, and Dashboards
- Custom Change Management services
- Data Conversion, Migration, Transformation, or Historical Data Loads
- Integrations not described in Appendix A
- Other services not exclusively called out in this document

6. Project Management Services

AspireHR Project Management Services are included as a part of this implementation agreement.

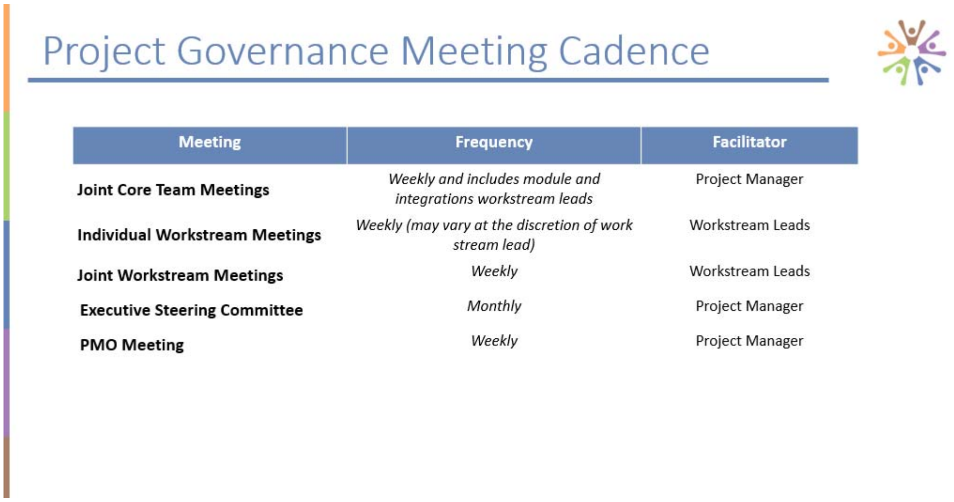
AspireHR project management responsibilities include the following activities throughout the implementation project life cycle:

- Develop and manage overall project plan in Smartsheet Workspace
- Maintain and clarify project scope
- Communicate and drive key milestones
- Communicate any timeline delays to key milestones and execution of the change request process
- Communicate Roles and responsibilities of the project team utilizing the contact list in Smartsheet workspace
- Communicate Milestone Completion and execute deliverable Acceptance procedures
- Create and provide updates to supporting project documentation in Smartsheet workspace (IE: RAID log, Change Log, Testing Log) throughout the implementation
- Schedule weekly or biweekly County/AspireHR team meeting, PMO Meeting, and monthly Steering Committee Meeting
- Create, maintain, and provide access to MS Teams channel for documentation repository throughout implementation
- Project Charter and vision in collaboration with the County

AspireHR project management incorporates measuring, evaluating and correcting project progress throughout the project timeline:

- Create & Maintain Project Plan. AspireHR utilizes Smartsheet to allow web-based access to the project plan for all parties. Use of Smartsheet as the primary tracking tool is mandatory. Use of additional or different project management tools shall incur additional cost. Collaboration with SAP and County Project Manager for any additional internal tasks to be added to the project plan
- Collaborate with County Project Manager to jointly conduct status meeting (meeting up to one (1) hour) to discuss action items and tasks scheduled for completion in the upcoming weeks
- Develop monthly status reports to summarize progress, highlight and track risks and issues, define next steps and County action items; seek County Project Manager approval and updates
- Weekly functional calls shall be scheduled by the AspireHR Project Manager or the AspireHR team leads in accordance with the Project Plan and above specified deliverables. Up to five (5) collaborative calls (one hour each) per week shall be scheduled with project team.
- Project Manager shall schedule all predefined calls stated in SOW and Project Plan.

Please see meeting cadences throughout the implementation:



Project Governance Meeting Cadence

Meeting	Frequency	Facilitator
Joint Core Team Meetings	*Weekly and includes module and integrations workstream leads*	Project Manager
Individual Workstream Meetings	*Weekly (may vary at the discretion of work stream lead)*	Workstream Leads
Joint Workstream Meetings	*Weekly*	Workstream Leads
Executive Steering Committee	*Monthly*	Project Manager
PMO Meeting	*Weekly*	Project Manager

AspireHR PMO Toolkit includes the following tools:

- AspireHR Smartsheet Workspace (Project Plan, RAID Log , Change Log, Testing Log, Contact List, Dashboard for Testing and Project. Any custom reports or metrics added to the dashboard shall need requirement sessions and additional build discussions through a change request and may incur additional costs. AspireHR Microsoft Teams for Project collaboration, document sharing, and project organization and links to Smartsheet
- Zoom or Microsoft Teams shall be used for all project meetings and meetings shall be recorded and stored in a central location for access by all parties – assuming personal information is not shared in recorded sessions.

7. Testing Scope

AspireHR shall provide the sample testing guidance documentation/templates for the project to guide the County HR team members in leading and executing test cases and scenarios/scripts during User Acceptance Testing. Unless otherwise specified above, the County is responsible for fulfilling the Test Lead role.

Test Type	Description	Owner
Iterative Module Unit Testing	• Execute transactions in the system to validate configuration matches Business Requirements • Feedback sessions • No formal test scripts • All unit test must occur during the planned time period in order to meet project schedule	County
User Acceptance Testing (UAT)	• Country Leads and executes UAT to verify the end-to-end business process (forms, workflow, site, permissions, email notifications, reports, etc.) • AspireHR will document any new requirements and shall be tracked for future configuration and implementation.	

	• AspireHR will correct defects as noted during UAT and referenced back to the business requirement document. • UAT Completion and defect resolution of all Critical/High defects shall indicate readiness to move configuration to production. • Medium/Low defects will be resolved during the hypercare/warranty period. • AspireHR to provide recommended *sample* test cases/scripts as a starting point for County to create its overall end to end test plan and test cases. • AspireHR to provide defect resolution during UAT and Hypercare.	

8. GoLive Support

AspireHR shall provide [Company] up to two (2) weeks of remote post implementation Go-Live support from the technical Go-Live date per module. County shall provide first-tier support to end-users. AspireHR shall provide support to County. Support includes: Configuration defect resolution (i.e., configuration does not reflect the final configuration workbooks) Go Live Support excludes: Design changes – configuration and XML changes outside of a configuration defect or an approved change request. Application defect management

9. Training

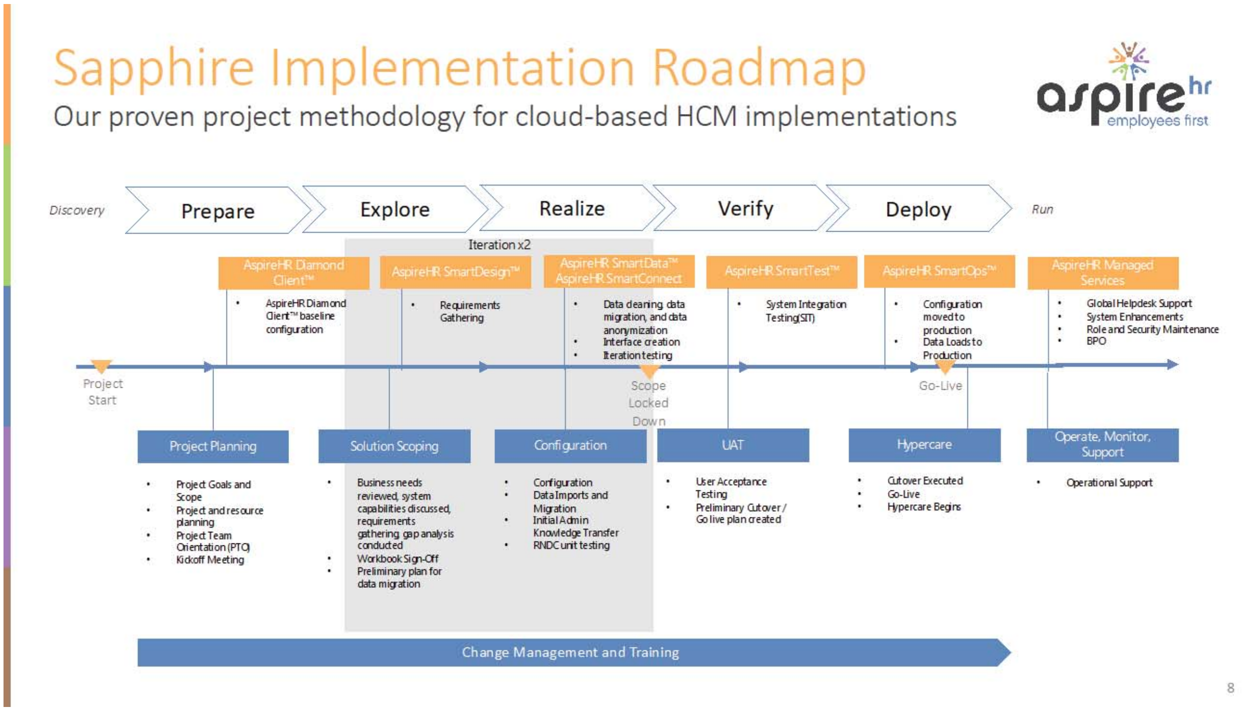
Knowledge transfer shall occur during implementation to step system admins through system settings. These knowledge transfer sessions will be recorded and the recordings provided to the County for future reference.

County shall be provided with editable Diamond Client Training materials.

10.Sapphire Implementation Approach

Based on SAP's Activate and Launch Methodologies, AspireHR has developed an updated implementation methodology which places more of an emphasis on a best practice preconfigured deployment with ready-to-go supporting documents. The AspireHR Sapphire Methodology is comprised of five phases: Prepare, Explore, Realize, Verify, and Deploy. Each phase has a specific set of deliverables designed to ensure the successful implementation of a well-designed system.

AspireHR consultants shall be 100% virtual throughout the project lifecycle. During the project the consultants' activities include but are not limited to the project kick-off and initial workshops, initial solution playback (County validation) sessions, testing kickoff, and go-live. The following graphic depicts the release cycles for AspireHR module (s).



Sapphire Implementation Roadmap

Our proven project methodology for cloud-based HCM implementations

Discovery

Prepare

Explore

Realize

Verify

Deploy

Run

Iteration x2

AspireHR Diamond Client™

- AspireHR Diamond Client™ baseline configuration

AspireHR SmartDesign™

- Requirements Gathering

AspireHR SmartData™ AspireHR SmartConnect

- Data cleaning, data migration, and data anonymization
- Interface creation
- Iteration testing

AspireHR SmartTest™

- System Integration Testing(SIT)

AspireHR SmartOps™

- Configuration moved to production
- Data Loads to Production

AspireHR Managed Services

- Global Helpdesk Support
- System Enhancements
- Role and Security Maintenance
- BPO

Project Start

Scope Locked Down

Go-Live

Project Planning

- Project Goals and Scope
- Project and resource planning
- Project Team Orientation (PTO)
- Kickoff Meeting

Solution Scoping

- Business needs reviewed, system capabilities discussed, requirements gathering, gap analysis conducted
- Workbook Sign-Off
- Preliminary plan for data migration

Configuration

- Configuration
- Data Imports and Migration
- Initial Admin Knowledge Transfer
- RNDC unit testing

UAT

- User Acceptance Testing
- Preliminary Cutover / Go live plan created

Hypercare

- Cutover Executed
- Go-Live
- Hypercare Begins

Operate, Monitor, Support

- Operational Support

Change Management and Training

8

10.1. Project Deliverable Ownership

Below is a table of project deliverables for the combined AspireHR and County team. The table notes the phase of the project implementation lifecycle, the deliverable description, and denotes the primary owner of the tasks.

	Responsibility	County	AHR	
Section 1.0	Prepare Phase			
1.1	Coordinates and leads implementation		Y	
1.2	Imports Diamond Client User Test Data (if applicable)		Y	
1.3	Coordinates and leads formal Project Kickoff		Y	
1.4	Leads and manages internal County project team, SMEs and external stakeholders and vendors	Y		
1.5	Creates & communicates project plan and schedule		Y	
1.6	Manages project scope		Y	
1.7	Monitors other projects that could impact success criteria/timeline	Y		
1.8	Provides Diamond Documentation BPMs, Test Scenarios, Knowledge Transfer Documentation, and Completed Workbooks.		Y	
1.9	Audit 3rd party implementation vendor tasks (if applicable)	Y		
1.10	Ensures AHR project deliverables are provided on or prior to the date communicated in the project plan		Y	
1.11	Coordinates all County-requested meetings on the AHR side		Y	
1.12	Completes Project Team Orientation & Administrative Training from SAP	Y		
1.13	Confirms Access to all Diamond Client Documentation in AHR Teams	Y		

1.14	Ensures project deliverables are provided on time		Y	
Section 2.0	Explore Phase			
2.1	Attend Module Orientation	Y		
2.2	Attend Knowledge Transfer Sessions (Administrative)	Y		
2.3	Provide Business Requirements, review and approve in Business Requirements Document	Y		
2.4	Attend Test Script Knowledge Transfer Meetings	Y		
2.5	Prepare Testing Strategy	Y		
2.6	Diamond Data Imports (if needed)	Y		
2.7	Prepares Change Management Strategy using delivered materials	Y		
2.8	Prepare Training Strategy using delivered materials	Y		
2.9	Create an Issues Log for use throughout the project		Y	
2.10	Conducts solution walkthroughs and business requirements gathering sessions		Y	
Section 3.0	Realize			
3.1	Execute Unit Testing	Y		
3.3	Conduct testing support calls		Y	
3.4	Conduct final Knowledge Transfer		Y	
3.5	Communicate Production Transition Strategy (Cutover Plan)		Y	
3.6	Reviews and approves Production Transition \ Strategy	Y		
Section 4.0	Verify			
4.1	Execute User Acceptance Testing	Y		
4.2	Distributes end – user communication & training	Y		
4.3	Develops go live plan and checklist		Y	
4.4	Cutover configuration to production		Y	
4.5	Validate Cutover via testing	Y		
Section 5.0	Deploy Phase			
5.1	Communicate process for tracking go-live and post go-live support issues		Y	
5.2	Addresses functional issues (go-live/post go-live support)		Y	
5.3	Addresses integration issues (go-live/post go-live support)		Y	

The AspireHR Project Manager shall provide notifications to County for Milestone Recognition.

Deliverable Type	Criteria
Documentation	County shall receive access to a Diamond Teams site that shall contain all of the ready-to-go template documentation including Business Process Maps, Test Scripts, Workbooks, Business Requirements Documents and product documentation workbooks.

11. Testing and Acceptance Criteria

Upon completion of each milestone described in Section 13.2 of this SOW, AspireHR shall notify County and the Acceptance testing process will commence. County Acceptance of each milestone shall be based on conformance with all associated tasks and deliverables as described in this SOW. When AspireHR completes a milestone, AspireHR shall submit a Milestone Acceptance Form – Attachment 2 to the County for review and approval.

If the County rejects any of the key deliverables in the milestone, AspireHR shall have 5 business days to either correct items documented in the County's notification of rejection, or to provide a correction plan. Following the delivery of AspireHR's notice that the work has been corrected the Acceptance test will start again and the County will either issue a written notice of Acceptance or provide AspireHR with a notification of rejection, which will include documentation of the specific grounds for the rejection, outlining work not in compliance with the phase or milestone. If the work fails to comply with the phase or milestone after AspireHR's attempt to correct the work and no clear plan can be agreed upon between the County Sponsor and AspireHR's Project Director, the County will determine the appropriate corrective action(s), up to and including declaring a material breach of Contract.

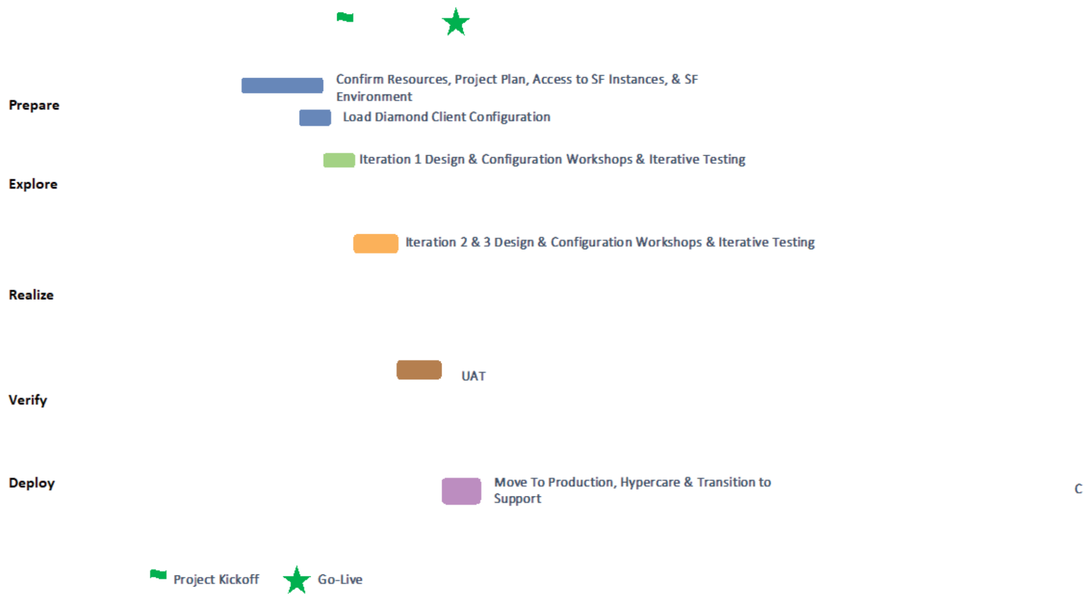
Written Final Acceptance shall be provided by the County to AspireHR when the full system supplied by AspireHR (including all software, custom configurations, training, and support agreements) has been installed or delivered to County, all activities described in this SOW, and all milestones described in Section 13.2 of this SOW are fully functional and proven to be satisfactory to the project sponsor without Material Defect. All requirements found in this and all other project documentation (including those documents submitted by AspireHR) must be satisfactorily met by AspireHR products/services for each milestone, as well as tested (at the discretion of County) and accepted by County.

12.Project Timeline

The following section defines the procedures and expected durations for acceptance of deliverables. AspireHR and County shall work together to define a project schedule with these durations in mind. Once the project schedule is mutually agreed upon, delays caused by County that result in a longer overall project timeline or period of performance shall require a change order.

The high-level timeline for the project is estimated in weeks from the time AspireHR's Professional Services engages with the County on each module to the completion of the module. Note that the project team will take up to 4 weeks from signature in order to obtain access to the County SuccessFactors/Workforce Software environments, implement Diamond Client accelerators, and prepare for Kickoff. The project plan and timeline shall be finalized at Iteration 1.

Sample Timeline



The project timeline is estimated as follows for each phase: Prepare, 2 weeks; Explore /Iteration 1 3 weeks; Realization Iteration 2&3 3 weeks; Verify 3 weeks; Deploy 3 weeks (includes 2 weeks Hypercare). If a module is extended beyond the estimated duration, the County may incur additional fees for the extension of the project timeline. Delays by SAP SuccessFactors or Workforce Software, LLC that impact the ability to achieve timelines shall not be considered as a delay by the County.

The timelines above assume County has sufficient project team availability for all work streams in order to stay on schedule. Any project delays as a result of County project team availability, County progress on County responsibilities, or County decision making shall result in a Change Order.

After the project is kicked off and an agreed upon project plan is created, AspireHR shall hold a project timeline review and obtain County's agreement that:

- There is sufficient project team availability from all work streams in order to stay on schedule.

12.1. Project Milestone Explanations

The following chart outlines the key milestones during the project which shall trigger an invoice.

Milestone	Description
Project Start (Prepare)	SOW has been signed, AspireHR resources have been allocated, AspireHR Project Managers have aligned with County PMO or Project Lead on next steps
Module Kickoff (Explore)	Project has been kicked off and County has received module orientation
IT1 Configuration Updates (Realize)	Iteration 1 Configuration Changes have been completed. Sample County data has been loaded to system (if applicable) using provided templates to

	the County. Data must be populated in format provided on the templates for upload.
UAT Preparation (Verify)	All Iterative Configuration Changes are completed. AspireHR has provided editable Diamond test scripts and testing guidance.
Cutover Initiation (Deploy)	AspireHR has prepared cutover checklists with County and is ready to begin cutover tasks.

*If applicable

13. Pricing

13.1. Release 1 Pricing Price per Module

The pricing below reflects the cost of implementation per module. Pricing reflects project management per the included schedule. Actual invoicing shall be done on a milestone basis as reflected in section 13.2 below.

Solution/Role	Amount
Workforce Software Absence Management	$ 87,205
Integration – 1 medium complexity demographic file from HRIS system to WorkforceSoftware	included
Total	$87,205

AspireHR shall perform all work remotely.

If scope exceeds what is defined in this Statement of Work, and technical enhancements are needed, it shall be executed post technical go-live, working with Support or conducted in a separate initiative in order to maintain the Diamond Client timeline.

Notes:

- Expansion of timeline greater than 4 weeks total resulting from County delays, lack of County resources to perform County activities, or suspension of work due to County action will result in a weekly fee of $8000 and potential change of AspireHR resource.

13.2. Release 1 Fees Milestones

AspireHR's total fixed fees for in scope Consulting Services (excluding expenses) are AspireHR's Consulting Fee is a representation of the cost for services, risk, and assumptions as identified in this Statement of Work.

The below Consulting Fee Schedule is provided on a Fixed Bid/Fixed Scope basis:

Absence Management Milestone Invoice Table		
Milestone	Estimated Date	Amount
1. Module Kick-off		$7,268
2. IT1 Workbook Sign-off for configuration		$14,534
3. IT2 / Workbook Sign-off for configuration		$14,534
4. IT3 / Final Workbook Sign-off for configuration		$14,534
5. IT3 / Unit Testing Completed		$14,534
6. SIT Initiated		$7,267
7. UAT Initiated		$7,267
8. Production Release for Go-Live		$7,267
	TOTAL	$87,205

14. Period of Performance

The Project Start deliverable shall begin no more than six (6) months from the execution of this Statement of Work.

15. Change Control

Throughout a project, new information may surface that may necessitate a change in business requirements or a change in the technical environment. These changes may result in a change in project scope and therefore impact the estimated level of effort or project timeline. Any identified potential new changes must follow the County Change Management Process (also "Change Process"). Approved changes resulting from this process shall require a Change Order, which either AspireHR or County shall complete and provide to the other party. Change Orders may result in additional fees. AspireHR shall advise County of the estimate if additional fees shall apply. All changes must be tracked in the County Change Control Log in Smartsheet.

A completed Change Order form includes the requested change, impact on the current engagement and resources, time, and fees to implement the Change Order. AspireHR shall submit the completed Change Order form to the other party for review and written approval. Work on the requested change shall not commence until written approval has been received. Impacts to project timelines for delayed approvals may necessitate additional costs.

Estimates shall remain valid for a period of ten (10) business days from the date of submission. If County does not approve the Change Order form within ten (10) business days, and AspireHR has not extended the period of validity in writing, the change estimate shall automatically expire. Upon receipt of written approval, the AspireHR team shall begin work on the requested change according to the agreed-upon schedule.

16. Project Completion Criteria

The full Absence Management solution supplied by the Contractor (including all hardware, software, custom configurations, training, and support agreements) has been installed or delivered to the County and are fully functional and proven to be satisfactory to the project sponsor. All requirements found in this and all other project documentation (including those documents submitted by the Contractor) must be satisfactorily met by the Contractor products/services, tested by the County, and accepted through testing (at the discretion of the County).

17. Rolling Estoppel

County assumes responsibility for providing the resources as indicated in the SOW. County shall be conclusively deemed to have fulfilled its obligations, unless it receives a deficiency report from Contractor by the fifteenth (15th) day of the month following the month of the alleged deficiencies and Contractor identifies specific deficiencies in County's fulfillment of its obligations in that report. Deficiencies must be described in terms of how they have affected the specific performance requirement of Contractor.

Contractor is estopped from claiming that a situation has arisen that might otherwise justify changes in the project timetable, the standards of performance under the contract or the contract price, if Contractor knew of that problem and failed to include it in the applicable report.

In the event Contractor identifies a situation wherein County is impairing Contractor's ability to perform for any reason, Contractor's deficiency report should contain Contractor's suggested solutions to the situation(s). These suggestions should be in sufficient detail so that County project managers can make a prompt decision as to the best method of dealing with the problem and continuing the project in an unimpeded fashion.

If the problem is one that allows Contractor (within the terms of the contract) to ask for changes in the project timetable, the standards of performance, the project price or all of these elements, the report should comply with the change order procedures.

18. Security Requirements

The County does not offer unlimited Contractor access to servers housed in the County Data Center. The County shall create a Contractor access account, as needed. Server access shall be coordinated against internal change control request and access is facilitated via Citrix. No other Contractor access application use is supported by the County.

The Contractor shall instruct its employees, agents, and subcontractors that they shall comply with the County's security, access, and safety requirements for the protection of the County's facilities and employees while on the County's premises.

19. Data Rights

Ownership. County Data is and shall remain the sole and exclusive property of County and all right, title, and interest in the same is reserved by County. This Section shall survive the termination of this Agreement.

Contractor Use of County Data. Contractor is provided a limited license to County Data for the sole and exclusive purpose of providing the Services, including a license to collect, process, store, generate, and display County Data only to the extent necessary in providing the Services. Contractor shall: (a) keep and maintain County Data in strict confidence, using such degree of care as is appropriate and consistent with its obligations as further described in this Agreement and applicable law to avoid unauthorized access, use, disclosure, or loss; (b) use and disclose County Data solely and exclusively for the purpose of providing the Services, such use and disclosure being in accordance with this Agreement and applicable law; and (c) not use, sell, rent, transfer, distribute, or otherwise disclose or make available County Data for Contractor's own purposes or for the benefit of anyone other than County without County's prior written consent. This Section shall survive the termination of this Agreement.

20.SAML 2.0 Compliance

Annual Certificate Updates

If the solution integrates with County's Active Directory Federation Services (ADFS) then SAML2.0 compliance is required. The Contractor shall ensure compliance with SAML 2.0 for end user authentication during the term of this Agreement. If the Contractor has not implemented the full SAML 2.0 standard to include monitoring of federation metadata, County shall provide Contractor with advance notice of a token-signing certificate replacement and shall provide Contractor with the new certificate prior to the scheduled change. The Contractor shall be solely responsible for ensuring the County users are provided uninterrupted access to the Software by managing the Software's certificate renewal during annual updates. Coordination of certificate updates shall be between the following points of contact that may be updated from time to time by notification to the other party in writing.

If solution is an Azure Enterprise application, County prefers that the application is published to the Azure Gallery. Any standard protocol Azure AD supports may be used.

Contractor Contact for Certificate Coordination:

Name Broderick Martin
Phone
Email bmartin@aspirehr.com

County Contact for Certificate Coordination:

Todd Ryden
425.388.3867
ADFS-support@co.snohomish.wa.us (preferred)

21.Attachments

- Attachment 1 – Technical Standards RFP Questions
- Attachment 2 – Milestone Acceptance Form Sample
- Attachment 3 – Snohomish County Employee Groups

Appendix A – Scope

Absence Compliance Tracker (ACT)

Summary:

ACT is an intake, evaluation, and case management tool for leave and ADA accommodation cases governed by federal and state laws within the United States. ACT assists employers in evaluating the circumstances of an employee request and determining which laws provide leave and/or job protection or accommodation requirements. ACT helps Human Resource professionals manage tasks, documents, and due dates for an absence or accommodation case from the time an employee submits a request for leave until the employee returns to work or the accommodation is provided.

By default, ACT includes federal and state leave programs that cover a breadth of common leave types (such as pregnancy or military leave) as well as specific leave situations, such as for crime victims and organ donation. Additionally, ACT contains a set of standard documents that comply with the applicable federal and state standards. ACT automatically fills in the documents with case-specific information when a leave case is initiated. ACT includes a leave workflow based on best practices that is designed to help an organization comply with the required timing and content of communication, and a workflow to process ADA accommodation requests.

Leave Types:

ACT recognizes three different leave types: *continuous, intermittent,* and *reduced schedule*. When an employee has a continuous leave case, the application assumes the employee is on leave all day, every day and automatically generates the Leave of Absence (LOA) pay code on the employee's timesheet in the amount of the employee's *standard daily hours* for the duration of the case. If the employee is on intermittent or reduced schedule leave, the employee's manager or case manager must manually enter the Leave of Absence (LOA) pay code on the employee's timesheet.

Regardless of the leave type, ACT determines if the Leave of Absence requested by the employee is covered by the federal and state leave programs, based on the remaining balances for the approved leaves on the case. If the Leave of Absence is covered with any distributed federal or state leave program, then the leave is considered Protected Leave in ACT. If the Leave of Absence is not covered then the leave is considered Unprotected Leave.

Functional Behavior:

1. Included Leave Programs: Jurisdictions and Leave Programs within the U.S.
2. Calendar Definition: County may select the appropriate calendar definition which becomes the basis for computing leave usage and availability for year-based leave programs. *See decision points.*

3. Employer Sectors and Category Types: includes sector-specific regulations for a variety of public and private sectors. Most organizations fall into one of the basic Public Sector or Private Sector categories.
4. Employee Self-Service Leave Requests: allows an employee to request leave, such as medical or family type leave, without having to know anything about leave programs or their eligibility for such programs. The application guides the employee through a series of questions that collects the necessary information, which the application and an HR case administrator use to determine eligibility.
5. Intake and Case Management Workflow: provides case management workflow that is based on best practices and is designed to help case managers efficiently manage leave and accommodation cases and their associated deadlines.
6. Documents and Email Messages: comes with a set of standard documents that comply with the applicable federal and state standards.
7. Timesheet display**: The timesheet displays the leave time an employee takes related to an ACT Case. The Pay Code used for all leave events is LOA (Leave of Absence).
8. On-Screen Messages**: Messages appear on the Messages tab of the timesheet to alert employees of invalid entries. Messages prevent erroneous or unacceptable entries, such as an employee or case manager entering negative hours. Some messages are solely informational and draw attention to a condition on the timesheet, such as when an employee's location has changed.
9. Security Levels and Roles: The application uses role-based security to make sure that ACT users only have rights to information and functionality they need to perform their required tasks.
10. Reports: comes with several standard reports which are listed in the AFD.
11. HR Import: There are key employee fields that need to be imported to support the application.
    ** Timesheet features require WorkForce Time and Attendance module.

Required Imports:

The following interfaces are **required** processes for the County when implementing.

- **Employee Management/Employee import**: Importing employee information required for ACT.

Definition of Medium Import (HRIS demographic included)

- Up to 4 Target Connections/Files
- Up to 50 Fields
- Includes value mapping, limited to simple logic, such as remove dashes from SSN, format date substring)

Optional Imports:

The following additional interfaces are **optional** one-time processes for the County when implementing ACT. Data must be provided in the format defined in the *ACT Functional Description* document).

- Work History Import: Transfers work history for one or more employees into ACT. ACT uses the information to determine an employee's eligibility for leave when the prior year's work history is needed for the initial launch of the application. The work history import is optional, although strongly recommended because it is a key part of the ability of ACT to automatically determine an employee's eligibility for leave. Note: this interface has a standard format, this is the format that is assumed for this implementation, changes or customizations shall require a change to the project scope.

- Leave History Import: Loads historical leave usage into ACT during initialization of the application. This essential information allows ACT to determine an employee's leave availability immediately following the launch of the application. Like the work history import, the leave history import is optional, although generally recommended because it is a key part of the ability of ACT to automatically determine an employee's remaining leave balances. Note: this interface has a standard format. This is the format that is assumed for this implementation. Changes or customizations shall require a change to the project scope and may incur additional costs.

- Open Case Import: Allows current, open approved leave cases to be imported into ACT for continued use after the implementation startup. This functionality is convenient during a transition to ACT from another leave management tool or process. After the import, case managers can update additional case information and continue managing the case going forward. *THE OPEN CASE IMPORT IS ASSUMED OUT OF SCOPE UNLESS SPECIFICALLY REQUESTED AND LISTED IN THE MAIN BODY SOW.*

County Decision Points:

1. One calendar definition must be selected to become the basis for computing FMLA.
   - Rolling from today
   - Calendar date
   - Employee anniversary (based on ACT Hire Date)
   - From first usage

2. The following additional interfaces are available for optional use by the County:
   - Work History Import
   - Leave History Import
   - Open Case Import (Out of Scope)

3. ACT Employee Self-Service Leave Request option: County decides during the definition phase if the employees are allowed to initiate their own leave of absence case.

County Responsibilities:

The following items must be performed by the County to execute this model accurately:

1. Ensure the employee import data has the appropriate data fields required for ACT.
2. Ensure data is available if optional data imports are being implemented.

Limitations & Restrictions

1. Distributed documents are restricted from being tailored with County specific logos or declarations in this model. They become custom documents and, therefore, are not updated during future ACT rule updates.
2. Multiple documents attached in a single email is not supported.
3. Implementation of this model does not include changes to the standard workflow defined in the ACT Functional Description document. Changes to the standard workflow require a custom solution approach.
4. This model does not cover supplementing Leave of Absences with custom leave or paid leave.
5. Configuration of workflow for the Employee Groups listed in Schedule A, Attachment 3 Snohomish County Employee Groups are included in the scope. Additional Employee Group configuration will be subject to written agreement only, in accordance with section 14 of this SOW, Change Process.
6. Work History Import: If data is not imported then case managers must continue to manually determine leave eligibility for up to one full year after ACT go-live. After one year and if using Workforce Time, ACT has enough work history to determine leave eligibility based on the number of hours worked in the previous twelve months.
7. Leave History Import: If data is not imported, then case managers must continue to manually determine available balances for FMLA and other distributed leaves for one full year after ACT go-live. After one year, ACT has enough leave history to determine available balances for FMLA and other distributed leaves.
8. Open Case Import: If data is not imported then any open leave cases from a previous leave management tool or process cannot be managed in ACT.
9. Special considerations for holidays are not included in this model. LOA is generated to timesheets on holidays in continuous cases.
10. County implementations using the SAP Time and Attendance Management by WorkForce Software do not include links to leave summaries within ACT cases nor the link to the Leave Regulations Map on the Home screen.
11. All employee characteristics must be at the employee record level. This is true even in a multiple assignment implementation.

Attachment 1

Snohomish County Technical Standard

Questions RFP-23-021BC

Company Name: Aspire HR

Common Criteria

These criteria apply to both On-Premise and Vendor Hosted (SaaS) solutions being proposed.

For each Common Criteria requirement below, please respond by entering the appropriate codes (described below) in the Response Code fields. In addition to providing a code, vendor must provide a separate narrative explanation in the Vendor Response fields.

When any proposed solution does not Comply ("C") with county technical standards, vendor must provide the following:

- specific details describing how the solution deviates,
- steps that must be taken for the solution to work in the county system, and
- any costs associated with the deviation from standard/steps to be taken.

Vendor must also provide cost information in the cost section of the proposal.

Full, direct, and substantive responses that explain how the solution would perform the function are required. Non-specific responses or omitted information may be considered non-responsive. Any question where the Vendor Response section is left blank will receive a zero score, regardless of the response code given.

Response Codes

"C" Comply – The proposed system will fully meet the requirement. It is a standard feature or function in the base application of the software. Vendor shall explain how the proposed solution fully meets the requirement.

"D" Does not comply – The proposed solution does not comply with this requirement; the software/ system will not meet this requirement in its entirety. Vendor shall explain if and how the proposed solution may meet the requirement. Be sure to use this code if the question is not applicable and state "not applicable" in the vendor response section.

"WC" With Conditions – The following are applicable for this response code:

- The solution can meet this requirement by providing a unit of software or a software module that is separate from the base application. This required unit of software or module ***must*** be included and clearly identified in the Vendor's Cost Proposal.
- The requirement can be met by altering the proposed software to meet the requirements and specifications. Costs for customizing software ***must*** be included and clearly identified

in Vendor’s Cost Proposal. Vendor must also commit to completion of customization as part of the initial installation / implementation.

- The requirement can be met by purchase of additional hardware (such as servers) to meet the requirements and specifications. Cost for additional hardware ***must*** be included and clearly identified in the Vendor’s Cost Proposal.

#	Common Criteria	Response Code
2.2	The proposed solution is compatible with all standard County desktop hardware configurations.	C
Vendor Response: Since this is a SaaS solution, it requires no infrastructure other than • An internet connection• A modern browser enabled with JavaScript, cookies, and SSLEmpLive supports the two most recent stable versions of the following browsers: Chrome, Firefox, Internet Explorer and Safari.		
2.3	The proposed solution is compatible with all standard County laptop configurations.	C
Vendor Response: Since EmpLive is a SaaS solution, it requires no infrastructure other than• An internet connection• A modern browser enabled with JavaScript, cookies, and SSLEmpLive supports the two most recent stable versions of the following browsers: Chrome, Firefox, Internet Explorer and Safari.		
2.4	The proposed solution is compatible with all standard County PC software.	C
Vendor Response: Since EmpLive is a SaaS solution, it requires no infrastructure other than• An internet connection• A modern browser enabled with JavaScript, cookies, and SSLEmpLive supports the two most recent stable versions of the following browsers: Chrome, Firefox, Internet Explorer and Safari.		
2.6	The proposed solution is compatible with smart phone devices. In the Vendor Response field, specify the smart phone operating systems (iOS, Android, etc.) and versions for which the proposed solution is compatible.	C
Vendor Response: Mobile capabilities are a complimentary extension of the WorkForce Suite. The WorkForce Suite is designed as mobile-first and responsive, making it easily accessible across desktops, smart phones, and tablets. Android phone or tablet using the default browser or Chrome, OS version 7.0 and above. iPhone using iOS 12 or above. iPad using iOS 12, or accessed through any mobile browser. Employees use the web interface (i.e., self service) or a mobile device to submit time-off requests. However, leave of absence (LOA) requests can only be entered via the web interface.		
2.7	The proposed solution is compatible with or will not have any performance limitations as a result of County security configurations. Please explain all incompatibilities, noting item number and specific incompatibility and/or performance impacts.	C
Vendor Response: The proposed solution is compatible with or will not have any performance limitations as a result of County security configurations.Please explain all incompatibilities, noting item number and specific incompatibility and/or performance impacts.		

<table>
<tr><th>#</th><th>Common Criteria</th><th>Response Code</th></tr>
<tr><td>2.9</td><td>The proposed solution will run through a remote desktop (RDP) connection/session.</td><td>C</td></tr>
<tr><td colspan="3"><i>The actually response is “Not Applicable”. We are offering a SaaS solution that is accessed by a browser or mobile app</i></td></tr>
<tr><td>2.9.1</td><td>If the application expects or relies on remote access email, calendar, documents, etc., will the application perform as expected using Office 365?</td><td>C</td></tr>
<tr><td colspan="3"><i>Vendor Response:</i> The WorkForce Suite is compatible with Windows 10. Furthermore, Microsoft systems can be used to access or exchange data with WorkForce Suite. We support the ability to export reports to Word or Excel. We also support calendar integration (employee syncs calendar for shifts, absences, holidays). Emails are generated for various notifications. Time-off request emails support the ability for the manager to approve requests directly from the email.</td></tr>
<tr><td>2.10</td><td>The proposed solution is fully-functional when utilized over a wireless (Wi-Fi) connection.</td><td>C</td></tr>
<tr><td colspan="3"><i>Vendor Response:</i> The WorkForce Suite is web-based and is accessible via the internet from a browser, mobile app, or data collection device.</td></tr>
<tr><td>2.11</td><td>The proposed solution is fully-functional when utilized over VPN (specifically NetMotion).</td><td>C</td></tr>
<tr><td colspan="3"><i>Vendor Response:</i> The actually response is “Not Applicable”. We are offering a SaaS solution that is accessed by a browser or mobile app.</td></tr>
<tr><td>2.16</td><td>If applicable, the proposed solution is capable of exchanging data with other Snohomish County application via automated processes.
Explain how the proposed solution will source and/or consume data from a county application, the requirements for county applications to participate in data exchange, and identify any deviations from a RESTful exchange system and the associated mechanisms.</td><td>C</td></tr>
<tr><td colspan="3"><i>Vendor Response</i>: We have both REST APIs and SOAP web services. We also support file transfers over SFTP.</td></tr>
</table>

2.17	If applicable, the proposed solution is compatible with OneSpan's digital signature solution. If proposed solution is dependent on digital signature workflows for processing, explain the mechanism used to ensure workflow items are not frozen or orphaned when a named user or users become unavailable.	C
Vendor Response: The actual answer is "Not Applicable". Workflows and "signatures" are built into the solution.		
2.18	If applicable, the proposed solution meets all County records management requirements. Explain how the solution meets or does not meet all of the requirements listed in the technical standard document.	C
Vendor Response: Click here to enter text.		
2.19	If applicable, the proposed solution meets all County security requirements. Explain how the solution meets or does not meet all the requirements listed in the technical standard document.	C
Vendor Response: WorkForce Suite is ISO 27001, ISO 27017, ISO 27018, and ISO 27701 Certified (https://www.schellman.com/certificate-directory?certificateNumber=1736251-7) and we perform annual SOC 1 Type II, SOC 2 Type II, and ISO 27001, ISO 27017, ISO 27018, and ISO 27701 audits. Controls include:Physical SecurityEach of our global SaaS facilities require a key card, PIN and/or biometrics to enter, and are monitored 24x7 with video surveillance. Facilities have perimeter barriers. Each facility has at least N+1 redundant power, air conditioning systems, and generators, with at least 24 hours of fuel and Priority 1 refueling (the same priority as hospitals and police). All processing is performed in a private cloud (dedicated hardware) in Oracle Cloud Infrastructure. WorkForce Software maintains and supports all systems and applications.Perimeter SecurityDDoS services protect against Distributed Denial of Service attacks, web application firewalls protect applications, while firewalls secure traffic in a DMZ and between key subnets. Intrusion detection systems continuously monitor the SaaS environment.Data EncryptionThe WorkForce Suite SaaS platform support the strongest HTTPS (TLS 1.2 or higher) encryption available for use by browsers and web services. Data from clock terminals is encrypted over the Internet, and secure protocols are used for bulk file transfers. Data at rest, including backups, are encrypted with AES-256 encryption at the storage layer. Oracle transparent database encryption is enabled with AES-128 encryption.Security TestingWe perform weekly internal and external vulnerability scans, and contract with third-party security firms to perform independent vulnerability scans, annual data center penetration tests, and annual web application security tests. Our software development teams use a variety a security testing tools and follow OWASP methodologies that include SAST, DAST and SCA testing. WorkForce Software proactively analyzes security logs to identify security threats.User AuthenticationClients can customize password rules within WorkForce Suite's native authentication systems and/or can use Single Sign-On (SSO) over SAML to authenticate against your directory services. Customers can use Multifactor Authentication (MFA). On the back end, our staff use VPN with MFA to remotely access our data centers.Database SecurityDatabase access is strictly controlled and monitored. Database entitlements are audited monthly.Internal System SecurityWe use non-routable IP addressing, port-redirection, network address translation and other mechanisms to protect systems within the firewalls. We use SE Linux with with the		

Center for Internet Security Benchmarks fully configured. Systems are routinely patched for security. Servers have AES-256 encrypted storage, centrally managed anti-virus/anti-malware, host-based intrusion detection, file integrity checking, root kit detection, host-based firewalls.Redundancy and Disaster RecoveryAll network components, load balancers, proxy servers, application servers and database servers have redundant hardware. WorkForce Software has multiple redundant Internet providers. We maintain complete disaster recovery facilities with infrastructure and Internet connectivity. Your data is replicated to standby servers at both the Primary Site and the Disaster Recovery Site. Failover testing is performed annually.Backups and RestoresWorkForce Software performs full database backups weekly and incremental backups daily and stores these encrypted backups at both our Primary and Disaster Recovery Sites. Routine restores are used to verify that backed-up data is accessible.Operating ProceduresWorkForce Software adheres to documented Change Management Procedures. All changes require approval from the Change Approval Board. Access to the SaaS environment is strictly limited, and access must be approved in advance by our Change Approval Board.

Vendor-Hosted (SaaS) Only

For each vendor hosted requirement below, please respond by entering the appropriate codes (described below) in the Response Code fields. In addition to providing a code, vendor must provide a separate narrative explanation in the Vendor Response fields.

When any proposed solution does not Comply ("C") with county technical standards, vendor must provide the following:

- specific details describing how the solution deviates,
- steps that must be taken for the solution to work in the county system, and
- any costs associated with the deviation from standard/steps to be taken.

Vendor must also provide cost information in the cost section of the proposal.

Full, direct, and substantive responses that explain how the solution would perform the function are required. Non-specific responses or omitted information may be considered non-responsive. Any question where the Vendor Response section is left blank will receive a zero score, regardless of the response code given.

Response Codes

"C" Comply – The proposed system will fully meet the requirement. It is a standard feature or function in the base application of the software. Vendor shall explain how the proposed solution fully meets the requirement.

"D" Does not comply – The proposed solution does not comply with this requirement; the software/ system will not meet this requirement in its entirety. Vendor shall explain if and how the proposed solution may meet the requirement. Be sure to use this code if the question is not applicable and state "not applicable" in the vendor response section.

"WC" With Conditions – The following are applicable for this response code:

- The solution can meet this requirement by providing a unit of software or a software module that is separate from the base application. This required unit of software or module ***must*** be included and clearly identified in the Vendor's Cost Proposal.
- The requirement can be met by altering the proposed software to meet the requirements and specifications. Costs for customizing software ***must*** be included and clearly identified in Vendor's Cost Proposal. Vendor must also commit to completion of customization as part of the initial installation / implementation.

The requirement can be met by purchase of additional hardware (such as servers) to meet the requirements and specifications. Cost for additional hardware ***must*** be included and clearly identified in the Vendor's Cost Proposal.

#	Vendor-Hosted (SaaS) Only	Response Code
VH1	Is the application hosted as software as a service (SAAS) or a cloud-based solution? • If "Yes," are all requirements listed above met by the vendor and the application? • If "No," list the requirements not met by the proposed application. • Does your proposed solution and cost estimate include both a test/staging environment and a production environment? • If "No," describe the steps necessary to acquire a secondary (test/staging) environment and include associated costs in the cost section.	C
Vendor Response: The WorkForce Suite provides all customers with development, test, and production environments.		
VH2	Is the solution compatible with the hosted data storage standards listed? If the answer to any of the above is "No," list and explain the requirements not met.	C
Vendor Response: Really, not applicable: We are not providing a storage solution nor are we offering a file or document management system. We are providing a SaaS solution which happens to use storage. That storage is maintained by WorkForce Software. All storage is encrypted with AES-256 encryption. Data is stored in a dedicated Oracle Pluggable Database that used Oracle AES-128 Transparent Database Encryption.		
VH3	The proposed solution can provide single sign-on capability utilizing ADFS. If the Response Code is not "C" explain how the application integrates with AD but does not use ADFS for single sign-on and if the purchase of a third party tool is required.	C
Vendor Response: The WorkForce Suite can be configured to authenticate users through a single sign-on (SSO) mechanism. When using SSO, information is passed to the WorkForce Suite via an authentication server or cookies, and the user is seamlessly authenticated. This option is ideal if users are already into an existing HR portal or other system. If server authentication is used, the server can be an IIS web server, a portal server, or a database server.The solution can automatically authenticate a user based on an established logon, such as a Windows domain session or corporate portal, without entering an ID/password. The WorkForce Suite can be configured to integrate with nearly any access management system or portal, such as Active Directory, SiteMinder, or PeopleSoft Portal. Assuming Active Directory is configured to act as a SAML Identity Provider, our SSO process is able to use the SAML responses generated by Active Directory to authenticate the user and allow them access to the application.		
VH4	The proposed solution provider operates a 24/7/365 Security Operations Center (SOC). Provide detailed answers to each of the following questions in the Vendor Response field, below:	C

#	Vendor-Hosted (SaaS) Only	Response Code
	• How do you determine if there is a data breach in your hosted environment? o Will you or your cloud vendor notify your customers? o If you are using a third party cloud vendor, provide their name and other applicable information. o Have you had a security breach that involved notifying the public or a government agency? • Will you allow the county or a third-party to conduct vulnerability or penetration testing against your servers? o If you are using a third-party to conduct vulnerability or penetration testing, provide their name and other applicable information. • Does your system provide 24/7 threat monitoring? If so, what type of monitoring? • Does the proposed solution offer multifactor authentication? If so, is there additional cost? • Are you listed on FedRAMP? - NO • Are you HIPAA compliant? - YES • Are you CJIS compliant? • If this solution includes credit card processing, do you store credit card information (PCI) on your system?	

Vendor Response: Vendor Response: (1) How do you determine if there is a data breach in your hosted environment? We have extensice security monitoring tools in place to detect data breaches. Tools provide alerts to our staff. (2) Will you or your cloud vendor notify your customers? We notify customers within 24 hours of a suspected or actual breach. (3) If you are using a third party cloud vendor, provide their name and other applicable information. We use a private cloud within Oracle Cloud Infrastructure (OCI), an Infrastructure-as-a-Service provider, to host WorkForce Suite. Each of our processing regions (the United States, Europe, Canada, and Australia) have primary and disaster recovery processing sites. The customer chooses which region to host from, and all customer data stays in the chosen region. Our US primary site (Phoenix, AZ) is a cluster of three data centers, each data center containing three "fault domains" - physically separate hardware, power and networking. WorkForce Suite is load balanced across the nine fault domains across the three data centers and we can lose a fault domain or a data center with minimal or no customer disruption. We use Oracle RAC database clusters running on Oracle's Exadata platform for highly available databases. We replicate in real-time to a standby Oracle RAC database cluster in a different data center in the primary data center cluster, and in near-real-time to the Disaster Recovery data center cluster in Ashburn, Virginia - a another set of three data centers. (4) Have you had a security breach that involved notifying the public or a government agency? No. (5) Will you allow the county or a third-party to conduct vulnerability or penetration testing against your servers? Yes (6) If you are using a third-party to conduct vulnerability or penetration testing, provide their name and other applicable information. Yes. We use Rapid7 Consulting for perform data center network pen testing annually against each of our data centers. We use HackerOne to perform a month-long web application security assessment annually. We can provide executive summaries of the reports to you. (7) Does your system provide 24/7 threat monitoring? Yes. (8) If so, what type of monitoring? Firewalls and/or Network Security Groups demarcate a DMZ which contains Internet facing

<table>
<tr><th>#</th><th>Vendor-Hosted (SaaS) Only</th><th>Response Code</th></tr>
<tr><td colspan="3">services. Logs are maintained around network traffic and blocked traffic, and stored on a separate secure log server. host-based firewalls adding an additional layer of security. The perimeter has DDoS protection, reverse proxy, and web application firewalls. Intrusion detection systems monitor for potential security events. We use a SIEM to consolidate logs and send out alerts. (9) Does the proposed solution offer multifactor authentication? It supports the customer’s existing MFA system – we do not sell MFA. (10) If so, is there additional cost? Our support for your MFA is no additional charge. We will integrate with your Single Sign On system that support MFA using SAML 2.0. (11) Are you listed on FedRAMP? No (12) Are you HIPAA compliant? Yes, although we are not a Covered Entity. (13) Are you CJIS compliant? No – Not Applicable to our product. (14)If this solution includes credit card processing, do you store credit card information (PCI) on your system? Not applicable – we do not store or process credit cards..</td></tr>
<tr><td>VH5</td><td>The proposed solution securely stores all customer data within the United States.
Provide detailed answers to each of the following questions in the Vendor Response field, below:
• Will customer data physically reside in any countries besides the United States?
• In which countries are all copies of backup customer data stored?
• Is customer data encrypted at rest?
o If so, what encryption method and standard is used?
• Can any cloud provider staff view unencrypted customer data?
• Do you conduct background investigations for employees that have access to the data?
• Do you require annual security awareness training for your employees?
• Does the cloud service offer file versioning for documents?
o If so, how many days or revisions are in the version history?
• Do you provide Single-Tenant Data Isolation (data is completely isolated logically and physically from other customer’s data)?
• Does your solution include disaster recovery with geo-redundant document and data storage?
• What are the penalties and costs to remove county data from the cloud vendor?
• What is your data retention policy after the conclusion of a contract? (Such as how is the data removed from the cloud storage?)</td><td>C</td></tr>
<tr><td colspan="3"><i>Vendor Response:</i> Vendor Response: •   Will customer data physically reside in any countries besides the United States? NO • In which countries are all copies of backup customer data stored? Only the US • Is customer data encrypted at rest? Yes. o If so, what encryption method and standard is used? All data at rest is encrypted with AES-256 at the storage layer. Core data stored in Oracle databases is encrypted with Transparent Database Encryption (AES-128). Certain sensitive data (ACT documents included) are encrypted within the database using AES 128-bit encryption. PGP file encryption is an optional feature for files transferred over SFTP. • Can any cloud provider staff view unencrypted customer data? Yes • Do you conduct background investigations for employees that have access to the data? Yes • Do you require annual security awareness training for your employees? Yes – and we</td></tr>
</table>

<table>
<tr><th>#</th><th>Vendor-Hosted (SaaS) Only</th><th>Response Code</th></tr>
<tr><td colspan="3">disable their network access if they don’t take the training and don’t pass the tests. We also do continuous phishing campagns against our users. • Does the cloud service offer file versioning for documents? Not applicable. o If so, how many days or revisions are in the version history? Not applicable • Do you provide Single-Tenant Data Isolation (data is completely isolated logically and physically from other customer’s data)? Core data is stored in dedicated Oracle Pluggable Databases. A pluggable database is essentially a database within a shared database, with its own resources and security. Customers get three environments (Dev, Test, and Prod) and each environment has its own dedicated Oracle Pluggable Database. The data in each Pluggable Database is encrypted using Oracle Transparent Database Encryption (TDE) using AES-128 encryption.Some data may be stored in multi-tenant databases and is segregated using a unique organization identifier. Access to any data in multi-tenant database requires authentication and authorization that includes that identifier. File transfer files are stored on a file transfer server in customer-dedicated folders with unique credentials (RSA key) required to access. There are separate folders for Dev, Test, and Prod file transfers. We provide optional PGP file encryption. With PGP, files are never decrypted on disk – they are only decrypted in memory. • Does your solution include disaster recovery with geo-redundant document and data storage? Yes • What are the penalties and costs to remove county data from the cloud vendor? No penalties or costs. At the end of the contract, we can return your data. We will purge all data from our systems, • What is your data retention policy after the conclusion of a contract? (Such as how is the data removed from the cloud storage?) Data is removed after 30 days after contract termination.</td></tr>
<tr><td>VH6</td><td>The proposed solution allows customers to audit the cloud SOC and their processes and procedures.
• Explain if the cloud vendor is SAS 70 Type II audited and willing to provide a copy of their SOC 2 report?
o ((SAS 70 is a report on audit and controls verification); SOC 2 Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy.)
• Can a customer audit the cloud SOC and their processes and procedures?
• Does your solution log successful and failed authentication attempts?</td><td>C</td></tr>
<tr><td colspan="3"><i>Vendor Response:</i> WorkForce Suite is ISO 27001, ISO 27017, ISO 27018, and ISO 27701 Certified (https://www.schellman.com/certificate-directory?certificateNumber=1736251-7) and we perform annual SOC 1 Type II, SOC 2 Type II, and ISO 27001, ISO 27017, ISO 27018, and ISO 27701 audits. Customer can perform audits. The solution logs successful and failed authentication attempts</td></tr>
</table>

Attachment 2
Milestone Acceptance Form Sample

Payment Milestone	Milestone 1
Milestone Description	Module Kick-off
Payment Amount	$7,268.00

The above project milestone has been achieved. The associated deliverables have been completed, delivered, and approved.

The undersigned has confirmed that the milestone has been completed in accordance with the Statement of Work signed _________________, 2024

Authorization
Snohomish County accepts that AspireHR, LLC has delivered the products and/or services required to satisfy the Acceptance criteria for the above noted Payment Milestone in accordance with the Statement of Work and related contract.

Snohomish County	**AspireHR, LLC**
Name	Name
Title	Title
Signature	Signature
Date	Date

Schedule A Attachment 3: Snohomish County Employee Groups

Leave Type												
Employee Type	**Civil Duty Leave**	**Disability Leave**	**Domestic Violence Leave**	**FMLA Personnel**	**Leave Without Pay**	**Military Family**	**Military Service**	**WA PFML**	**WA Paid Sick**	**Pregnancy, Childbirth, Pregnancy Disability**	**WA Family Cares Act**	**WA Leave for Certain Emergency Personnel**
Personnel Rule	Civil Duty. Any employee who is elected or appointed to a political or legislative position which is compatible with the employee’s county employment may be granted leave without pay to perform his or her civil duty or may utilize accrued vacation leave and compensatory time if approved by the employee’s supervisor. An employee will forfeit his or her right to payment for any recognized holiday if he or she is on leave without pay or on leave that has not been approved on the last regular working day preceding such holiday or on the next regular working day	An employee will forfeit his or her right to payment for any recognized holiday if he or she is on leave without pay or on leave that has not been approved on the last regular working day preceding such holiday or on the next regular working day following such holiday.	An employee will forfeit his or her right to payment for any recognized holiday if he or she is on leave without pay or on leave that has not been approved on the last regular working day preceding such holiday or on the next regular working day following such holiday.	Upon an employee's prior written request, submitted at the same time as an FMLA or Washington Family Care Leave Act request is made, an employee may be granted leave of absence without pay and maintain up to forty (40) hours of total paid leave accrual in any designated combination of sick leave, vacation. An employee will forfeit his or her right to payment for any recognized holiday if he or she is on leave without pay or on leave that has not been approved on the last regular working day preceding such holiday or on the next regular working day following such holiday.	Leave Without Pay. An employee may request leave without pay by submitting a written request to the employing official. Each request for such leave shall be considered in light of the circumstances involved and the needs of the organization. Such leave shall be for a defined period of time, not to exceed six months. Any leave without pay beyond six months duration must have the county executive’s approval for good cause shown. All leaves of absence without pay shall be reported to the human resources department in the manner prescribed by the director and	An employee will forfeit his or her right to payment for any recognized holiday if he or she is on leave without pay or on leave that has not been approved on the last regular working day preceding such holiday or on the next regular working day following such holiday.	An employee will forfeit his or her right to payment for any recognized holiday if he or she is on leave without pay or on leave that has not been approved on the last regular working day preceding such holiday or on the next regular working day following such holiday.	Standard Rules	Standard Rules	An employee will forfeit his or her right to payment for any recognized holiday if he or she is on leave without pay or on leave that has not been approved on the last regular working day preceding such holiday or on the next regular working day following such holiday.	Upon an employee's prior written request, submitted at the same time as an FMLA or Washington Family Care Leave Act request is made, an employee may be granted leave of absence without pay and maintain up to forty (40) hours of total paid leave accrual in any designated combination of sick leave, vacation. An employee will forfeit his or her right to payment for any recognized holiday if he or she is on leave without pay or on leave that has not been approved on the last regular working day preceding such holiday or on the next regular working day following such holiday.	An employee will forfeit his or her right to payment for any recognized holiday if he or she is on leave without pay or on leave that has not been approved on the last regular working day preceding such holiday or on the next regular working day following such holiday.

	following such holiday.				may cause the employee’s seniority and anniversary dates to be adjusted. An employee will forfeit his or her right to payment for any recognized holiday if he or she is on leave without pay or on leave that has not been approved on the last regular working day preceding such holiday or on the next regular working day following such holiday.							
AFSCME Master Agreement	Civil Duty. Any employee who is elected or appointed to a political or legislative position which is compatible with the employee's County employment may be granted leave without pay to perform their civil duty or the employee may utilize accrued vacation leave and/or compensatory time.	Standard Rules	Standard Rules	Upon an employee's prior written request, submitted at the same time as an FMLA or Washington Family Care Leave Act request is made, an employee may be granted leave of absence without pay and maintain up to forty (40) hours of total paid leave accrual in any designated combination of sick leave, vacation forfeiture of Holiday Pay. An employee shall forfeit their right to full payment	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Upon an employee's prior written request, submitted at the same time as an FMLA or Washington Family Care Leave Act request is made, an employee may be granted leave of absence without pay and maintain up to forty (40) hours of total paid leave accrual in any designated combination of sick leave, vacation forfeiture of Holiday Pay. An employee shall forfeit their	Standard Rules

				for any recognized holiday if they are on leave without pay for any portion of the workday on the last regular working day preceding such holiday or on the next regular working day following such holiday. The holiday pay will be prorated to reflect the average paid hours worked or taken as paid leave the day before and day after the holiday.							right to full payment for any recognized holiday if they are on leave without pay for any portion of the workday on the last regular working day preceding such holiday or on the next regular working day following such holiday. The holiday pay will be prorated to reflect the average paid hours worked or taken as paid leave the day before and day after the holiday.	
Assessor Supervisors (AFSCME 1811-S)	An employee shall forfeit their right to full payment for any recognized holiday if they are on leave without pay for any portion of the workday on the last regular working day preceding such holiday or on the next regular working day following such holiday. The holiday pay will be prorated to reflect the average paid hours worked or taken as paid leave the day before and day after the	An employee shall forfeit their right to full payment for any recognized holiday if they are on leave without pay for any portion of the workday on the last regular working day preceding such holiday or on the next regular working day following such holiday. The holiday pay will be prorated to reflect the average paid hours worked or taken as paid leave the day before and day after the holiday.	An employee shall forfeit their right to full payment for any recognized holiday if they are on leave without pay for any portion of the workday on the last regular working day preceding such holiday or on the next regular working day following such holiday. The holiday pay will be prorated to reflect the average paid hours worked or taken as paid leave the day before and day after the	An employee shall forfeit their right to full payment for any recognized holiday if they are on leave without pay for any portion of the workday on the last regular working day preceding such holiday or on the next regular working day following such holiday. The holiday pay will be prorated to reflect the average paid hours worked or taken as paid leave the day before and day after the	An employee shall forfeit their right to full payment for any recognized holiday if they are on leave without pay for any portion of the workday on the last regular working day preceding such holiday or on the next regular working day following such holiday. The holiday pay will be prorated to reflect the average paid hours worked or taken as paid leave the day before and day after the	An employee shall forfeit their right to full payment for any recognized holiday if they are on leave without pay for any portion of the workday on the last regular working day preceding such holiday or on the next regular working day following such holiday. The holiday pay will be prorated to reflect the average paid hours worked or taken as paid leave the day before and day after the	An employee shall forfeit their right to full payment for any recognized holiday if they are on leave without pay for any portion of the workday on the last regular working day preceding such holiday or on the next regular working day following such holiday. The holiday pay will be prorated to reflect the average paid hours worked or taken as paid leave the day before and day after the	An employee shall forfeit their right to full payment for any recognized holiday if they are on leave without pay for any portion of the workday on the last regular working day preceding such holiday or on the next regular working day following such holiday. The holiday pay will be prorated to reflect the average paid hours worked or taken as paid leave the day before and day after the	Standard Rules	An employee shall forfeit their right to full payment for any recognized holiday if they are on leave without pay for any portion of the workday on the last regular working day preceding such holiday or on the next regular working day following such holiday. The holiday pay will be prorated to reflect the average paid hours worked or taken as paid leave the day before and day after the	An employee shall forfeit their right to full payment for any recognized holiday if they are on leave without pay for any portion of the workday on the last regular working day preceding such holiday or on the next regular working day following such holiday. The holiday pay will be prorated to reflect the average paid hours worked or taken as paid leave the day before and day after the	An employee shall forfeit their right to full payment for any recognized holiday if they are on leave without pay for any portion of the workday on the last regular working day preceding such holiday or on the next regular working day following such holiday. The holiday pay will be prorated to reflect the average paid hours worked or taken as paid leave the day before and day after the

	holiday. Employees shall not be eligible for holiday pay when receiving "time loss" payments under the provisions of the Industrial Insurance	Employees shall not be eligible for holiday pay when receiving "time loss" payments under the provisions of the Industrial Insurance	holiday. Employees shall not be eligible for holiday pay when receiving "time loss" payments under the provisions of the Industrial Insurance	holiday. Employees shall not be eligible for holiday pay when receiving "time loss" payments under the provisions of the Industrial Insurance	holiday. Employees shall not be eligible for holiday pay when receiving "time loss" payments under the provisions of the Industrial Insurance	holiday. Employees shall not be eligible for holiday pay when receiving "time loss" payments under the provisions of the Industrial Insurance	holiday. Employees shall not be eligible for holiday pay when receiving "time loss" payments under the provisions of the Industrial Insurance	holiday. Employees shall not be eligible for holiday pay when receiving "time loss" payments under the provisions of the Industrial Insurance		holiday. Employees shall not be eligible for holiday pay when receiving "time loss" payments under the provisions of the Industrial Insurance	holiday. Employees shall not be eligible for holiday pay when receiving "time loss" payments under the provisions of the Industrial Insurance	holiday. Employees shall not be eligible for holiday pay when receiving "time loss" payments under the provisions of the Industrial Insurance
Clerk's Association	An employee will forfeit his or her right to payment for any recognized holiday if he or she is on leave without pay or on leave that has not been approved on the last regular working day preceding such holiday or on the next regular working day following such holiday.	Non-Occupational Disability Leave. Non-occupational disability leave is leave resulting from a medical condition that is not an industrial injury or occupational disease suffered in County employment in accordance with this Article. Employees are required to exhaust accrued sick leave and accrued compensatory time and vacation leave before applying for or being granted a leave without pay. Non-Occupational Disability Leave. Non-occupational disability leave is leave resulting from a medical condition that is not an industrial injury or occupational disease suffered	An employee will forfeit his or her right to payment for any recognized holiday if he or she is on leave without pay or on leave that has not been approved on the last regular working day preceding such holiday or on the next regular working day following such holiday.	Upon an employee's prior written request, submitted at the same time as an FMLA or Washington Family Care Leave Act request is made, an employee may be granted leave of absence without pay and maintain up to forty (40) hours of total paid leave accrual in any designated combination of sick leave, vacation An employee shall forfeit his/her right to full payment for any recognized holiday if he/she is on leave without pay on the last regular working day preceding such holiday or on the next regular working day following such holiday. The holiday pay will be prorated to reflect the average paid	Standard Rules	An employee will forfeit his or her right to payment for any recognized holiday if he or she is on leave without pay or on leave that has not been approved on the last regular working day preceding such holiday or on the next regular working day following such holiday.	An employee will forfeit his or her right to payment for any recognized holiday if he or she is on leave without pay or on leave that has not been approved on the last regular working day preceding such holiday or on the next regular working day following such holiday.	An employee will forfeit his or her right to payment for any recognized holiday if he or she is on leave without pay or on leave that has not been approved on the last regular working day preceding such holiday or on the next regular working day following such holiday.	Standard Rules	Standard Rules	Upon an employee's prior written request, submitted at the same time as an FMLA or Washington Family Care Leave Act request is made, an employee may be granted leave of absence without pay and maintain up to forty (40) hours of total paid leave accrual in any designated combination of sick leave, vacation An employee shall forfeit his/her right to full payment for any recognized holiday if he/she is on leave without pay on the last regular working day preceding such holiday or on the next regular working day following such holiday. The holiday pay will be prorated to reflect the	Standard Rules

		in County employment in accordance with this Article. Employees are required to exhaust accrued sick leave and accrued compensatory time and vacation leave before applying for or being granted a leave without pay.		hours worked or taken as paid leave the day before and day after the holiday							average paid hours worked or taken as paid leave the day before and day after the holiday	
Corrections Guild	Standard Rules	Available vacation slots shall not be impacted by deputies on long-term leave (i.e. FMLA, L&l, military leave, etc.) until the completion of the secondary vacation days selection. Industrial Injury Supplement - Each member of the bargaining unit shall be provided two hundred forty (240) hours of industrial injury leave to be used to supplement the difference between time loss payments made through the County's Workers' Compensation program and the employee's straight-time base hourly wage for qualifying injuries sustained	Available vacation slots shall not be impacted by deputies on long-term leave (i.e. FMLA, L&l, military leave, etc.) until the completion of the secondary vacation days selection.	Available vacation slots shall not be impacted by deputies on long-term leave (i.e. FMLA, L&l, military leave, etc.) until the completion of the secondary vacation days selection.	Available vacation slots shall not be impacted by deputies on long-term leave (i.e. FMLA, L&l, military leave, etc.) until the completion of the secondary vacation days selection.	Available vacation slots shall not be impacted by deputies on long-term leave (i.e. FMLA, L&l, military leave, etc.) until the completion of the secondary vacation days selection.	Available vacation slots shall not be impacted by deputies on long-term leave (i.e. FMLA, L&l, military leave, etc.) until the completion of the secondary vacation days selection.	Available vacation slots shall not be impacted by deputies on long-term leave (i.e. FMLA, L&l, military leave, etc.) until the completion of the secondary vacation days selection.	Standard Rules	Available vacation slots shall not be impacted by deputies on long-term leave (i.e. FMLA, L&l, military leave, etc.) until the completion of the secondary vacation days selection.	Available vacation slots shall not be impacted by deputies on long-term leave (i.e. FMLA, L&l, military leave, etc.) until the completion of the secondary vacation days selection.	Available vacation slots shall not be impacted by deputies on long-term leave (i.e. FMLA, L&l, military leave, etc.) until the completion of the secondary vacation days selection.

		as a direct result of an intentional act of aggression while in the performance of their duties as determined by the Bureau Chief or designee or in defensive tactics training.										
Corrections Sergeants and lieutenants (Teamsters 763)	Standard Rules	Industrial Injury Supplement - Each member of the bargaining unit shall be provided two hundred forty (240) hours of industrial injury leave to be used to supplement the difference between time loss payments made through the County's Workers' Compensation program and the employee's straight-time base hourly wage for qualifying injuries sustained as a direct result of an intentional act of aggression while in the performance of their duties as determined by the Bureau Chief or designee or in defensive tactics training.	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules
Corrections Supervisors (Teamsters 763)	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules

Corrections Support (Teamsters 763)	Standard Rules	Industrial Injury Supplement - Each member of the bargaining unit shall be provided two hundred forty (240) hours of industrial injury leave to be used to supplement the difference between time loss payments made through the County's Workers' Compensation program and the employee's straight-time base hourly wage for qualifying injuries sustained as a direct result of an intentional act of aggression while in the performance of their duties as determined by the Director or designee or in defensive tactics training.	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules
Deputy Sheriff's Association	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Extended Sick Leave - If the period of illness, quarantine or incapacity for which sick leave is granted extends beyond the employee's accrued sick leave, the employee may utilize any other paid leave time available to him and may take leave of absence without pay or	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules

					benefits for a reasonable period of time not to exceed one hundred twenty (120) working days, inclusive of FMLA leave.							
District Court-Economic (AFSCME 1811-CA)	Standard Rules	Standard Rules	Standard Rules	Upon an employee's prior written request, submitted at the same time as an or Washington Family Care Leave Act request is made, an employee may be granted leave of absence without pay and maintain up to forty (40) hours of total paid leave accrual in any designated combination of sick leave, vacation, compensatory time and floating holidays.	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Upon an employee's prior written request, submitted at the same time as an or Washington Family Care Leave Act request is made, an employee may be granted leave of absence without pay and maintain up to forty (40) hours of total paid leave accrual in any designated combination of sick leave, vacation, compensatory time and floating holidays.	Standard Rules
Fleet, Roads and Solid Waste Supervisors (AFSCME 109-S)	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules
Human Services Supervisors (AFSCME 1811-HS)	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules

Juvenile Court Supervisors Association - Economic Agreement	Standard Rules	Standard Rules	Standard Rules	Upon an employee's prior written request, submitted at the same time as an FMLA or Washington Family Care Leave Act request is made, an employee may be granted leave of absence without pay and maintain up to forty (40) hours of total paid leave accrual in any designated combination of sick leave, vacation and floating holidays.	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Upon an employee's prior written request, submitted at the same time as an FMLA or Washington Family Care Leave Act request is made, an employee may be granted leave of absence without pay and maintain up to forty (40) hours of total paid leave accrual in any designated combination of sick leave, vacation and floating holidays.	Standard Rules
Law Enforcement Support (Teamsters 763)	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules
Paine Field Airport Fire Fighters (IAFF 2597)	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules
Professional and Technical Employees Local 17 (allied Health Unit)	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules
Professional and Technical Employees Local 17 (Environmental Health Unit)	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules
Professional and Technical Employees Local 17 (Environmental Health Unit Supervisors)	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules

Prosecutor's Criminal and Family Support Deputies (AFSCME 1811-PA)	Standard Rules	Standard Rules	Standard Rules	Upon an employee's prior written request, submitted at the same time as an FMLA or Washington Family Care Leave Act request is made, an employee may be granted leave of absence without pay and maintain up to forty (40) hours of total paid leave accrual in any designated combination of sick leave, vacation, compensatory time and floating holidays.	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Upon an employee's prior written request, submitted at the same time as an FMLA or Washington Family Care Leave Act request is made, an employee may be granted leave of absence without pay and maintain up to forty (40) hours of total paid leave accrual in any designated combination of sick leave, vacation, compensatory time and floating holidays.	Standard Rules
Sheriff's Office Management Team	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules
Superior Court - Juvenile Economic (AFSCME 1811-JPD)	Standard Rules	Standard Rules	Standard Rules	Upon an employee's prior written request, submitted at the same time as an FMLA or Washington Family Care Leave Act request is made, an employee may be granted leave of absence without pay and maintain up to forty (40) hours of total paid leave accrual in any designated combination of sick leave, vacation, compensatory	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Upon an employee's prior written request, submitted at the same time as an FMLA or Washington Family Care Leave Act request is made, an employee may be granted leave of absence without pay and maintain up to forty (40) hours of total paid leave accrual in any designated combination of sick leave, vacation,	Standard Rules

				time and floating holidays.							compensatory time and floating holidays.	
Superior Court - Supervisors Economic (AFSCME 1811-ES)	Standard Rules	Standard Rules	Standard Rules	Upon an employee's prior written request, submitted at the same time as an FMLA or Washington Family Care Leave Act request is made, an employee may be granted leave of absence without pay and maintain up to forty (40) hours of total paid leave accrual in any designated combination of sick leave, vacation and floating holidays.	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Upon an employee's prior written request, submitted at the same time as an FMLA or Washington Family Care Leave Act request is made, an employee may be granted leave of absence without pay and maintain up to forty (40) hours of total paid leave accrual in any designated combination of sick leave, vacation and floating holidays.	Standard Rules
Washington State Nurses Association (WSNA)	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules	Standard Rules

SCHEDULE B WORKFORCE SOFTWARE INDIRECT SAAS AGREEMENT

This WorkForce Software Indirect SaaS Agreement (the “Agreement”) is entered into as of the Effective Date between WorkForce Software, LLC, with an office at 38705 Seven Mile Road, Suite 300, Livonia, Michigan 48152 (“WFS”) and Snohomish County Government, with an office at 3000 Rockefeller Avenue, Everett, WA 98201(“Customer”).

WHEREAS, Customer has entered into an agreement with Aspire HR, LLC, a Reseller, for the purchase of SaaS Services; and

WHEREAS, WFS desires to make available to Customer and Customer desires to accept from WFS, a right to use the SaaS Services upon the terms and conditions set out in this Agreement; and

WHEREAS, Customer understands and acknowledges that Reseller is not an agent of WFS.

NOW THEREFORE, for good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the Parties hereby agree as follows:

1. Definitions

1.1. “Affiliate” means a legal entity separate from and controlled by or under common control with a Party. For purposes of this Agreement, the term “control” shall mean ownership of a beneficial controlling interest.

1.2. “Customer Data” shall mean any content, materials, data, and information provided by the Customer to WFS in the course of using the SaaS Service.

1.3. “Confidential Information” shall mean Customer Data, the SaaS Service, the terms of this Agreement, benchmarks, statistics or information on the capabilities of the SaaS Service, financial information, business plans, technology, marketing or sales plans that are disclosed to a Party, and any other information that is disclosed pursuant to this Agreement and reasonably should have been understood by the receiving Party to be proprietary and confidential to the disclosing Party because of (a) legends or other markings; (b) the circumstances of disclosure; or (c) the nature of the information itself. Notwithstanding the foregoing, “Confidential Information” shall not include any information which (i) is or becomes generally available to the public other than as a result of the improper action of the recipient; (ii) is rightfully known from a source independent of any restrictions imposed by the disclosing Party or becomes rightfully known to the recipient from such a source; (iii) has been independently developed by the recipient, provided such independent development can be substantiated by documentary evidence; or (iv) is generally furnished to others by the disclosing Party without restrictions on the receiving Party's right to disclose.

1.4. “Documentation” shall mean all written or electronic materials provided to Customer for facilitating use of the SaaS Service, as applicable, but does not include advertising or similar promotional materials.

1.5. “Effective Date” is the date of last signature hereto.

1.6. "e-Learning Courseware" shall mean video or online training content and related materials which may be provided to Customer.

1.7. "Force Majeure" shall mean any event outside of the control of a Party, such as, but not limited to, a natural disaster, fire, extended power, electrical, or Network outage, labor dispute, strike, lockout, denial of service or other malicious attack, telecommunications failure or degradation, pandemic, epidemic, public health emergency, governmental order or act (including government-imposed travel restrictions and quarantines), material change in law, war, terrorism, riot, or other act of God which renders the SaaS Service unavailable or affects or prevents performance under this Agreement.

1.8. "Intellectual Property Rights" shall mean all copyrights, trade secrets, patents, and other intellectual property rights or portion thereof.

1.9. "Order Form" means one or more agreements entered into between Customer and Reseller for the sale and purchase of WFS SaaS Services.

1.10. "Network" means the internet, phone network, cell phone network, and other transmission methods by which the SaaS Service is delivered.

1.11. "Party" or "Parties" shall mean WFS or Customer individually or collectively.

1.12. "Production Environment" means an environment provided in the SaaS Service which Customer uses for live processing.

1.13. "Related Systems" shall mean Customer owned or operated computers, web-browsers, operating systems, firewalls, e-mail servers, LDAP servers, portals, Networks, third party software, internet connection, and any other hardware or software that connects to the SaaS Service or affects the SaaS Service, whether or not provided by or configured by WFS.

1.14. "Reseller" means a third party which is authorized to resell the SaaS Services and from which Customer has purchased the SaaS Services.

1.15. "SaaS Service" means the WFS software as a service platform, together with updates and upgrades thereto, including Support Services, to which Customer is provided use and access rights in accordance with this Agreement and the applicable Order Form.

1.16. "Service Level Agreement" or "SLA" means the service levels specified in Exhibit A.

1.17. "Support Services" shall mean the services, as described in Exhibit A, specified in the Support Plan set forth in the applicable Order Form(s), including reasonable technical support via telephone, e-mail, and/or the web, to answer questions or provide assistance in the use of the SaaS Service.

2. Services Delivered

2.1. Subject to the terms and conditions of this Agreement, WFS hereby grants Customer a limited, non-exclusive, non-transferable right to access and use the SaaS Service as specified in the applicable Order Form(s), solely for Customer's internal business purposes. This Agreement governs Customer's use of the SaaS Services. By signing below or otherwise using the SaaS Services, Customer agrees to be bound by the terms of this Agreement. Within the Production Environment, Customer may use only the applications and extensions specified in the Order Form(s), even if other applications and extensions are made available.

2.2. WFS may periodically update ("Update") the SaaS Service, but makes no representations as to the frequency of new releases or the features, enhancements, or corrections that will be provided in the Updates.

2.3. Customer shall limit access to the SaaS Service to its own employees, consultants, and other authorized users (collectively, "Authorized Users") and shall not make the SaaS Service available to third parties or make it available on a service bureau basis. Customer shall ensure that each Authorized User complies with all applicable terms and conditions of this Agreement and Customer is responsible for acts or omissions by Authorized Users in connection with their use of the SaaS Service.

2.4. WFS shall take commercially reasonable measures, consistent with those generally accepted in the industry, to prevent unauthorized parties from gaining (a) physical access to the data centers where the SaaS Service is hosted; and (b) electronic access to the SaaS Service or the Customer Data. WFS shall promptly notify Customer of any unauthorized access to the SaaS Service which WFS detects.

2.5. WFS shall periodically backup the Customer Data ("Backup Services") as specified in Exhibit A. WFS will undertake commercially reasonable steps to begin the restoration of Customer Data from the backup as soon as WFS is notified or becomes aware of the need to restore Customer Data. WFS shall not be responsible if Customer Data is lost or corrupted in between scheduled backups or for a reason caused by the acts or omissions of Customer. Customer Data shall not be used by WFS for any other purpose except to provide the SaaS Services. WFS shall not preserve such Customer Data longer than contracted.

2.6. If a Force Majeure event causes the SaaS Service to become unavailable, WFS shall make commercially reasonable efforts to restore the SaaS Service at an alternate facility as soon as feasible. Until such Force Majeure event shall have passed, the SaaS Service may be provided on a reduced use basis and Customer may be required to make changes to the procedures used to access the SaaS Service. Except for a Party's payment obligations hereunder, neither Party shall incur any liability to the other Party on account of any loss or damage resulting from any delay or failure to perform all or any part of this Agreement, where such delay or failure is caused, in whole or in part, by a Force Majeure event. If a Party asserts a Force Majeure event for failure to perform the Party's obligations, then the asserting Party shall notify the other Party of the event and take commercially reasonable steps to minimize the delay or damages caused by the Force Majeure event.

2.7. WFS shall provide the Support Services specified in the Support Plan selected by Customer, as set forth in the applicable Order Form(s). The Support Plan description attached as Exhibit A provides details of the service levels and items provided under each plan. Terms of the Support Plan supersede the terms in this Agreement.

2.8. WFS may provide Customer and its Authorized Users access to certain Third-Party Services (as defined in Exhibit D) through the SaaS Service. Any usage of such Third-Party Services will be governed by Exhibit D, and Customer will remain responsible for Customer's access and use of the Third-Party Services.

2.9. From time-to-time Customer or its Authorized Users may provide WFS with suggestions, comments, feedback or the like with regard to the SaaS Service (collectively, "Feedback"). Customer hereby grants WFS a perpetual, irrevocable, royalty-free and fully paid-up license to use and exploit all Feedback in connection with WFS's business purposes, including, without limitation, the testing, development, maintenance and improvement of the SaaS Service.

2.10. Notwithstanding anything to the contrary in this Agreement, if there is a Security Emergency then WFS may automatically suspend use of the SaaS Service and will make commercially reasonable efforts to narrowly tailor the suspension as needed to prevent or terminate the

Security Emergency. "Security Emergency" means: (a) use of the SaaS Service that does or could disrupt the SaaS Service, other customers' use of the SaaS Service, or the infrastructure used to provide the SaaS Service; and (b) unauthorized third-party access to the SaaS Service.

3. Customer Responsibilities

3.1. Customer shall be responsible for entering its Customer Data into the SaaS Service, and Customer shall be responsible for the maintenance of the Customer Data supplied by it. Customer hereby represents and warrants to WFS that: (a) the Customer Data is free of all viruses, Trojan horses, and comparable elements which could harm the systems or software used by WFS or its subcontractors to provide the SaaS Service; (b) Customer has collected and shall maintain, during the term of this Agreement, all necessary rights, authority and licenses for the access to and use of the Customer Data; (c) Customer will handle all Customer Data in compliance with all applicable data privacy and protection laws, rules and regulations; and (d) WFS's use of the Customer Data in accordance with this Agreement will not violate any applicable laws or regulations or cause a breach of any agreement or obligations between Customer and any third party.

3.2. Customer has sole responsibility to maintain the integrity, confidentiality and availability of information on Customer equipment.

3.3. Customer has sole responsibility to (a) check the accuracy of information processed using the SaaS Service; (b) run all normal processes and procedures within the SaaS Service, such as end of period processing, imports, exports, and file transfers; and (c) manage and configure its Related Systems and ensure they operate properly. Customer is responsible for any inputs to the SaaS Service, including data and business rules that are set up for Customer, and any incorrect output that results therefrom. When using and applying the information generated by the SaaS Service, Customer is responsible for ensuring that Customer complies with the applicable requirements of federal and state law. Customer agrees that: (i) using the SaaS Service does not release Customer from any professional obligation concerning the preparation and review of reports and documents generated by the SaaS Service; and (ii) Customer does not rely upon WFS or the SaaS Service for any advice or guidance regarding compliance with federal and state laws or the appropriate tax treatment of items reflected on such reports or documents.

3.4. Customer assumes all responsibilities, obligations, and expertise with respect to (a) the selection of the SaaS Service to meet its intended results; and (b) any decision it makes based on the results produced by the SaaS Service. Customer understands and acknowledges that WFS and the Third-Party Content Vendors (as defined in Exhibit D) are not engaged in rendering legal, accounting, tax or other professional advice either as a service or through the SaaS Service and it is not relying on WFS and the Third-Party Content Vendors for any advice or guidance regarding laws and regulations. Customer shall review all calculations and determinations made using the SaaS Service and satisfy itself those results are accurate. If legal, accounting, tax, or other expert assistance is required, the services of a competent professional will be sought by Customer. To the extent permitted by law, Customer shall indemnify and hold WFS harmless from claims and demands of its employees or former employees arising from the use by Customer of the SaaS Service.

3.5. Customer is solely responsible to ensure Related Systems operate properly. The support provisions of this Agreement do not apply to Related Systems or problems in the SaaS Service caused by Related Systems, regardless of who provided, installed, or distributed such. Should WFS identify that the root cause of a problem is caused by Customer modifications to the

SaaS Service or behavior in Related Systems it shall notify Customer and request approval to provide additional assistance (if applicable).

3.6. Customer will not at any time, and will not permit any person (including, without limitation, Authorized Users) to, directly or indirectly: (a) use the SaaS Service in any manner beyond the scope of rights expressly granted in this Agreement; (b) modify or create derivative works of the SaaS Service or Documentation, in whole or in part; (c) reverse engineer, disassemble, decompile, decode or otherwise attempt to derive or gain improper access to any software component of the SaaS Service, in whole or in part; (d) except as expressly allowed herein or within an Order Form, frame, mirror, sell, resell, rent or lease use of the SaaS Service to any other entity, or otherwise allow any entity to use the SaaS Service for any purpose other than for the benefit of Customer in accordance with this Agreement; (e) use the SaaS Service or Documentation in any manner or for any purpose that infringes, misappropriates, or otherwise violates any Intellectual Property Right or other right of any entity, or that violates any applicable law; (f) interfere with, or disrupt the integrity or performance of, the SaaS Service, or any data or content contained therein or transmitted thereby; (g) access or search the SaaS Service (or download any data or content contained therein or transmitted thereby) through the use of any engine, software, tool, agent, device or mechanism (including spiders, robots, crawlers or any other similar data mining tools) other than software or SaaS Service features provided by WFS for use expressly for such purposes; or (h) use the SaaS Service, Documentation or any other WFS Confidential Information for benchmarking or competitive analysis with respect to competitive or related products or services, or to develop, commercialize, license or sell any product, service or technology that could, directly or indirectly, compete with the SaaS Service.

3.7. Customer shall not perform any stress test, load test, or security test on the SaaS Service without first obtaining WFS permission and executing a separate agreement for the services required by WFS to support such tests.

3.8. Customer will, and will require all Authorized Users to, use all reasonable means to secure usernames, passwords, hardware and software used to access the SaaS Service in accordance with customary security protocols. Customer shall change all passwords used to access the SaaS Service at regular intervals. Should Customer learn of an unauthorized third party having obtained knowledge of a password, Customer shall inform WFS thereof without undue delay and promptly change the password. Customer will terminate old users in the SaaS Service.

3.9. Customer is responsible for monitoring user access to the SaaS Service.

3.10. Customer is responsible for the connection to the SaaS Service, including the internet connection.

3.11. Customer will prevent unauthorized use of the SaaS Service by its Authorized Users and will terminate any unauthorized use of or access to the SaaS Service. The SaaS Service is not intended for users under the age of 13. Customer will ensure that it does not allow any person under 13 to use the SaaS Service. Customer will promptly notify WFS of any unauthorized use of or access to the SaaS Service, provided, however, that WFS shall be under no obligation to take any action in respect of Customer’s failure to prevent unauthorized access to the SaaS Service.

3.12. Customer and its Authorized Users must use the SaaS Service in compliance with the Acceptable Use Policy attached hereto as Exhibit E.

3.13. Customer may specify Authorized Users to have advanced administrative access, which may include the ability to access, disclose, restrict, or remove Customer Data in or from SaaS Service accounts ("Administrators"). Administrators may also have the ability to monitor, restrict, or terminate access to Authorized User accounts. WFS's responsibilities do not extend to the Customer's internal management or administration of the SaaS Service. Customer is responsible for: (a) maintaining the confidentiality of passwords and Administrator accounts; (b) managing access to Administrator accounts; and (c) ensuring that Administrators' use of the SaaS Service complies with the Agreement.

3.14. If an Authorized User (a) violates the Agreement or (b) uses the SaaS Service in a manner that WFS reasonably believes will cause it liability, then WFS may request that Customer suspend service or terminate the applicable Authorized User account. If Customer fails to promptly suspend or terminate the Authorized User account, WFS may do so.

3.15. Customer certifies that it, including its Authorized Users, shall not (a) access from and/or (b) export, transfer, or otherwise send, the WFS product(s) that is the subject of this Agreement to any country subject to comprehensive U.S. sanctions.

4. Term and Termination

4.1. The term of this Agreement starts on the Effective Date continues until terminated in accordance with the terms of this Agreement.

4.2. The provisions of Sections 3, 4.2, 5, 7, 8.4, 8.5, 8.8 and any payment obligations incurred by Customer prior to or upon termination shall survive termination of this Agreement.

4.3. This Agreement may be terminated by either Party upon notice to the other Party, so long as no Order Forms are in effect at the time of termination.

4.4. If either Party commits a material breach of this Agreement, and such breach is not corrected within thirty (30) days after receipt of written notice from the non-breaching Party, this Agreement may be terminated by the non-breaching Party upon written notice. Notwithstanding the foregoing, if the nature of the breach requires longer than thirty (30) days to cure, and WFS is taking commercially reasonable efforts to cure such breach at the end of the initial thirty (30) day cure period, WFS shall have a reasonable time thereafter to continue to effectuate a cure of such breach. Upon Customer's termination in such instance, WFS shall refund the unexpired portion of any fees paid. Where Customer is entitled to receive a refund pursuant to this Section 4.3, WFS will issue the refund to Reseller who will forward such credits to Customer.

4.5. Upon the effective date of termination, Customer's access to the SaaS Service will be terminated. No less than thirty (30) days after the effective date of termination, WFS shall use commercially reasonable efforts to permanently and irrevocably remove, purge, or overwrite all data still remaining on the servers used to host the SaaS Service, including, but not limited to, Customer Data, unless and to the extent applicable laws and regulations require further retention of such data. If the Customer submits a request within thirty (30) days of termination, WFS shall provide a full copy of the Oracle backup for Customer download. WFS shall have no obligation to maintain or provide any Customer Data more than thirty (30) days following the effective date of termination. All indemnifications relating to the unauthorized disclosure of Customer Data shall continue until such Customer Data is returned to Customer or destroyed.

4.6. Customer expressly acknowledges and agrees that WFS is entitled to rely on written information from Reseller in making any determination as to the suspension of the SaaS

Services or termination of the Agreement, and WFS shall have no liability to Customer for any actions thereunder based on WFS's reasonable belief in the accuracy or reliability of such information. Customer acknowledges that in the event payment from Reseller for the SaaS Service more than forty-five (45) days past due, WFS reserves the right to suspend Customer's access to the SaaS Service for so long as such payment remains outstanding.

5. Proprietary Right, Non-Disclosure

5.1. Each Party shall maintain as confidential and shall not disclose, publish, or use for purposes other than to perform its obligations under this Agreement the other Party's Confidential Information, except that a Party may disclose the other Party's Confidential Information to those employees, contractors, legal or financial consultants and auditors of the recipient and its Affiliates who need to know such Confidential Information in connection with the recipient's performance of its rights and obligations under this Agreement and in the normal course of its business and who are bound by confidentiality obligations no less stringent than those contained herein. Each Party shall protect the Confidential Information of the other Party with reasonable care, but in no event less care than it would exercise to protect its own Confidential Information of a like nature, and prevent the unauthorized, negligent, or inadvertent use, disclosure, or publication thereof. Notwithstanding anything else in this Agreement, either Party may disclose Confidential Information in accordance with a judicial or governmental order, or as otherwise required by law, provided that the recipient either: (a) gives the disclosing Party reasonable notice prior to such disclosure to allow the disclosing Party a reasonable opportunity to seek a protective order or equivalent, or (b) obtains written assurance from the applicable judicial or governmental entity that it will afford the Confidential Information the highest level of protection afforded under applicable law or regulation. Notwithstanding the foregoing, neither Party shall disclose any computer source code that contains Confidential Information in accordance with a judicial or other governmental order unless it complies with the requirement set forth in sub-section (a) of this Section 5.1.

5.2. Either Party may disclose the existence of this Agreement and its terms to the extent required by law, the rules of any applicable regulatory authority or the rules of a stock exchange or other trading system on which that Party's securities are listed, quoted, and/or traded.

5.3. Each Party acknowledges and agrees that a breach of the obligations in Section 5 may cause irreparable damage to the disclosing Party and therefore, in addition to all other remedies available at law or in equity, the disclosing Party shall have the right to seek equitable and injunctive relief for such breach. In the event of any litigation to enforce or construe this Section 5, the prevailing Party shall be entitled to recover, in addition to any charges fixed by the court, its costs and expenses of suit, including reasonable attorneys' fees, costs and expenses.

5.4. WFS shall retain all rights, title, and interest, including all Intellectual Property Rights, in the e-Learning Courseware, Third Party Services, Documentation, and the SaaS Service, including, but not limited to, the ideas, methodologies, methods of operation, processes, and look and feel in the SaaS Service. Customer shall not alter, modify, copy, edit, format, translate, or create derivative works of these materials, except as provided herein or when approved in writing by WFS.

5.5. As between WFS and Customer, Customer shall own all title, rights, and interest in Customer Data.

5.6. Both Parties agree to comply with all applicable privacy and data protection statutes, rules, or regulations governing the respective activities of the Parties. Customer hereby consents to the use, processing and/or disclosure of Customer Data only for the purposes described herein and to the extent such use or processing is necessary for WFS to carry out its duties and responsibilities under this Agreement or as required by law.

6. Payments and Credits

6.1. Customer shall pay Reseller (or successors in interest or assignee(s) of Reseller) fees and any applicable taxes for the SaaS Services specified in the applicable Order Form, pursuant to the payment terms between Reseller and Customer. Provision of the SaaS Services is contingent upon payment and the receipt by WFS of such fees. Unless specified otherwise in the Order Form: (i) fees are based on services purchased in the Order Form and overage fees; (ii) payment obligations in each Order Form are non-cancelable and fees paid are non-refundable; and (iii) the quantities ordered under the Order Form cannot be decreased during the term. The Order Form specifies how the Customer may use the SaaS Service and how the usage of the SaaS Service will be measured.

6.2. In the event of termination of the agreement between WFS and Reseller, or if for any other reason Reseller is no longer entitled to receive fees for the SaaS Services hereunder, WFS may, at its option and upon notice to Customer, require continued payment of fees for the SaaS Services hereunder to either another reseller or to WFS. Failure to pay such fees shall be considered a material breach of this Agreement.

6.3. Should WFS fail to satisfy the Uptime Commitment set forth in the SLA, Customer shall have the right to receive from Reseller a credit of the fees as calculated in the SLA. Where Customer is entitled to receive credits under this Section 6.3, WFS will issue credits to Reseller who will forward such credits to Customer. The credits provided to Customer shall be its sole and exclusive remedy for WFS's failure to comply with the Uptime Commitment.

7. Warranties, Indemnifications, and Limitation of Liability

7.1. WFS shall, at its expense, indemnify and defend Customer from and against any third-party claim that the SaaS Service infringes any of such third party's Intellectual Property Right; provided, however, that Customer (a) promptly notifies WFS of any such claim; (b) permits WFS to defend such claim with counsel of its own choice; and (c) gives WFS all information and/or assistance in the defense thereof as WFS may reasonably request. In no event shall Customer settle any such claim without the written consent of WFS. At any time after notice of an indemnifiable claim hereunder, or if WFS believes there is a basis for such a claim, WFS may, at its expense and election either: (i) procure the right for Customer to continue using the infringing items; (ii) replace the infringing items with a functionally equivalent non-infringing product; (iii) modify the infringing items so that they are non-infringing; or (iv) terminate the affected Order Form and refund the unexpired portion of any fees paid. This Section 7.1 will not apply to, and in no event shall WFS, its employees, agents and sub-contractors be liable to the Customer for, any alleged infringement to the extent it arises or results from: (1) a modification of the SaaS Services by anyone other than WFS; (2) the Customer's use of the SaaS Services in a manner contrary to the instructions given to the Customer by WFS; (3) Customer's breach of this Agreement, negligence, willful misconduct or fraud; (4) any Customer Data; (5) combinations of the SaaS Service with software, data or materials not provided by WFS; or (6) the Customer's use of the SaaS Services after notice of the alleged or actual infringement from WFS or any appropriate authority. The provisions of Section 7.1 constitute the entire liability of WFS and sole remedy of Customer with respect to any claims or actions based in whole or in part upon infringement or violation of an Intellectual Property Right of any third party.

7.2. WFS represents and warrants: (a) it has the right to grant the rights specified herein; and (b) the SaaS Service will not contain any viruses or Trojan horses.

7.3. SaaS Services being offered on a free trial basis are being provided 'as-is' without any warranties, indemnities, SLAs, or support. WFS shall have no liability arising out of Customer's use of free trial SaaS Services.

7.4. THE WARRANTIES AND REMEDIES SET FORTH HEREIN ARE EXCLUSIVE AND IN LIEU OF ALL OTHERS, WHETHER ORAL OR WRITTEN, EXPRESSED OR IMPLIED. EXCEPT AS SPECIFICALLY SET FORTH IN THIS SECTION 7, WFS SPECIFICALLY DISCLAIMS ANY AND ALL IMPLIED WARRANTIES TO THE SAAS SERVICES AND ANY OTHER SERVICES, DOCUMENTATION, OR OTHER MATTER WHATSOEVER. IN PARTICULAR, BUT WITHOUT LIMITATION, WFS SPECIFICALLY DISCLAIMS ANY AND ALL IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT OF THIRD-PARTY RIGHTS OR ANY OTHER WARRANTY ARISING FROM A COURSE OF DEALING OR USAGE OF TRADE. NO WFS AGENT, CONTRACTOR OR EMPLOYEE IS AUTHORIZED TO MAKE ANY MODIFICATION TO THIS WARRANTY, UNLESS IN A SIGNED WRITING EXECUTED BY A WFS EMPLOYEE WITH ACTUAL AUTHORIZATION TO BIND WFS. WFS DOES NOT WARRANT THAT THE SAAS SERVICE OR ANY PORTION THEREOF WILL OPERATE UNINTERRUPTED, WILL BE ERROR FREE OR THAT WFS WILL CORRECT ALL NON-MATERIAL ERRORS.

7.5. In no event shall either Party be liable for any loss of profits, loss of use, loss of data, interruption of business or indirect, special, incidental or consequential damages of any kind in connection with or arising out of this Agreement, whether alleged as a breach of contract or tortious conduct. The limitation of liability specified in this paragraph applies regardless of the cause or circumstances giving rise to such losses or damages, including without limitation, whether the other Party has been advised of the possibility of damages, the damages are foreseeable, or the alleged breach or default is a fundamental breach or breach of a fundamental term.

7.6. WFS's liability hereunder shall not, in any event, exceed the fees paid by Customer in the twelve (12) month period preceding which the claim arose. Such fees shall be limited to the particular Order Form to which the default relates. The limitations specified in this Section 7.5 shall not apply to a willful breach of the confidentiality provisions of Section 5, the indemnification provisions of Section 7.1, or to any death, bodily injury, or damage to tangible property caused solely by the negligence or willful misconduct of WFS's staff while on-site at Customer's locations.

8. General Provisions

8.1. Each Party may include the other Party's name or logo in a list of its clients, vendors, or service providers. Each Party may make reference to the other in an initial press release, provided that any use of the other Party's trademark(s) retain proprietary notices and/or are properly attributed to their owner and also provided that any such press release will require the review and prior written consent of both Parties, which shall not be unreasonably withheld, conditioned, or delayed.

8.2. In recognition of the pricing provided under this Agreement, Customer shall (subject to its reasonable right to review and approve): (a) allow WFS to include a brief description of the SaaS Service furnished to Customer in WFS promotional materials; (b) allow WFS to make reference to Customer in case studies, ROI analyses, white papers and related marketing materials; (c) serve as a reference for WFS potential clients; (d) provide interviews to the news media and provide quotes for press releases; (e) organize mutually convenient site visits for WFS potential clients; and (f) make presentations at conferences, upon WFS reasonable request and at WFS's cost.

8.3. Any notice to be sent relating to this Agreement shall be in writing and mailed to the other Party at the addresses set forth herein addressed to "Legal Department," by certified mail, return receipt requested. For notices from Customer to WFS, a digital copy shall be sent to legal@workforcesoftware.com. This Agreement contains the entire agreement of the Parties with respect to its subject matter, and there are no promises, conditions, representations or warranties except as expressly set forth herein. This Agreement may be modified or amended only by written instrument executed by the Parties. This Agreement has been the subject of arm's length negotiations and shall be construed as though drafted equally by both Parties. No terms, provisions or conditions of any purchase order or other document that Customer may use in connection with this Agreement shall have any effect on the rights, duties or obligations of either Party.

8.4. No term or provision of this Agreement shall be deemed waived, and no breach excused, unless such waiver or consent shall be in writing and signed by the Party claimed to have waived or consented. Any consent by any Party to, or waiver of, a breach by the other Party, whether express or implied, shall not constitute a consent to or waiver of any different or subsequent breach. If a court of competent jurisdiction holds any provision of this Agreement to be illegal, unenforceable, or invalid in whole or in part for any reason, the validity and enforceability of the remaining provisions, or portions of them, will not be affected. The headings and titles provided in this Agreement are for convenience only and shall have no meaning on the terms of this Agreement. Consent is not required for an assignment of this Agreement in connection with a sale or disposition of a majority of all the assets, voting securities or equity interests of WFS, or a reorganization, merger or similar transaction of WFS. For all other assignments, including those related to internal reorganizations of Customer, the prior, written consent of the other Party shall be required, such consent not to unreasonably withheld, conditioned or delayed. This Agreement binds and inures to the benefit of the Parties hereto and their respective successors and permitted assigns. The Parties agree that reliable copies such as scanned or facsimile counterpart signatures are acceptable.

8.5. No action arising out of any claimed breach of this Agreement may be brought by either Party more than one (1) year after the cause of action has accrued. Each Party shall be liable for breaches of its Affiliates and contractors under this Agreement. Any dispute under or in connection with this Agreement or related to any matter which is the subject matter of this Agreement shall be subject to the exclusive jurisdiction of the courts of Wayne County, Michigan, and shall be governed by and interpreted in accordance with Michigan law, without regard to choice of law provisions.

8.6. Customer will comply with all applicable federal laws, regulations and rules that prohibit or restrict the export or re-export of the SaaS Services or any Customer Data outside the United States ("Export Rules"), and will complete all undertakings required by Export Rules, including obtaining any necessary export license or other governmental approval.

8.7. The SaaS Service and Documentation are "commercial computer software" and "commercial computer software documentation," respectively, as such terms are used in FAR 12.212 and other relevant government procurement regulations. Any use, duplication, or disclosure of the SaaS Service or its Documentation by or on behalf of the U.S. government is subject to restrictions as set forth in this Agreement.

8.8. EACH PARTY ACKNOWLEDGES THAT THE WARRANTY DISCLAIMERS, LIABILITY AND REMEDY LIMITATIONS, AND SERVICE LEVELS IN THIS AGREEMENT ARE MATERIAL BARGAINED FOR BASES OF THIS AGREEMENT AND THEY HAVE BEEN TAKEN INTO ACCOUNT AND REFLECTED IN DETERMINING THE CONSIDERATION TO BE GIVEN BY EACH PARTY UNDER THIS AGREEMENT AND IN THE DECISION BY EACH PARTY TO ENTER INTO THIS AGREEMENT.

IN WITNESS WHEREOF, the Parties have executed this Agreement and the Exhibits indicated below as of the Effective Date.

Exhibits

[x] Exhibit A – Service Level and Support Plan
[x] Exhibit B – Data Processing Agreement
[x] Exhibit C – Data Retention Policy
[x] Exhibit D – Third-Party Services
[x] Exhibit E – Acceptable Use Policy

CUSTOMER		**WORKFORCE SOFTWARE, LLC**	
Signature:	______________________	Signature:	______________________
Name:	______________________	Name:	______________________
Title:	______________________	Title:	______________________
Date:	______________________	Date:	______________________

EXHIBIT A – SERVICE LEVEL AND SUPPORT PLAN

Support Overview			
Support Level	**Standard**	**Select**	**Signature**
Support Channels			
• Online Customer Portal	24x7 Access	24x7 Access	24x7 Access
• Email Submission	N/A	Yes	Yes
• Phone Support	24x7x365 Access (Sev 1/2)	24x7x365 Access (Sev 1/2)	24x7x365 Access
• Dedicated Signature Support Line	N/A	N/A	24x7x365 Access
Customer Support Contacts & Certification Requirements			
• Number of Support Contacts	Customer must have a minimum of 2 Certified Contacts, Customer may have 6 total Support Contacts.	Customer must have a minimum of 3 Certified Contacts, Customer may have 10 total Support Contacts.	Customer must have a minimum of 4 Certified Contacts, Customer may have 16 total Support Contacts.
• Certification Classes Included	First Year – 2 Subsequent Years – 1	First Year – 3 Subsequent Years – 1	First Year – 4 Subsequent Years – 2
• Requirements for Certified Contacts	Level 1 Training and Certification	Level 1 Training + Level 2 Training and Certifications	Level 1 Training + Level 2 Training and Certifications
SLA Response Times*			
• SLA Phone Response	90% within 60 minutes	95% within 60 minutes	98% within 60 minutes

• SLA Case Portal and Email Submission Response	85% within 1 Business Day	90% within 1 Business Day	95% within 4 hours
Uptime Commitment**			
• Uptime Commitment	99.0%	99.5%	99.9%
Estimated Resolution Targets – Not Including any Third-Party Services or Hardware			
• Severity Level 1 (“Sev 1”)	80% within 4 hours	85% within 4 hours	90% within 4 hours
• Severity Level 2 (“Sev 2”)	80% 2 Business Days	85% within 1 Business Days	90% within 12 hours
• Severity Level 3 (“Sev 3”)	80% 15 Business Days	85% 10 Business Days	90% 7 Business Days
Technical Account Manager Access (“TAM”)			
Named TAM, available Monday-Friday during Business Hours, excluding Holidays	N/A	Yes	Yes
TAM Support available Monday-Friday (24x5)	N/A	N/A	Yes
TAM Site Visit	N/A	N/A	1 per Year
Support Case Review Meeting Cadence (upon Customer request)	N/A	Monthly	Weekly
Signature Services			
• Solution Health Check	N/A	N/A	One (1) every three (3) years
• VISION User Conference Tickets	N/A	N/A	2 per year
• Compliance Portal Access*** (Available to U.S. Customers Only)	N/A	N/A	Yes
Optional Services			
Dedicated Support Team	N/A	N/A	Optional – pricing available upon request

Customer Help Desk Integration	N/A	N/A	Optional – pricing available upon request
Additional Language Services	N/A	N/A	Optional – pricing available upon request

*Customer must submit the issue via Phone Support for any suspected Severity Level 1 or Severity Level 2 issue for these SLA Response Times to be applicable.

**Not applicable to Hardware (as defined below)

***Compliance Portal Access is a Third-Party Service (as defined in the Agreement) and subject to the Customer having appropriate terms and conditions within the Agreement for Third-Party Services. Additional terms and conditions, which can be accessed via web pages from within the Compliance Portal, shall apply to Customer and remain in full effect throughout the full term of Customer's Signature Support subscription. If Customer is unable to or unwilling to agree to such terms and conditions, this service shall be unavailable to Customer.

Definitions

Capitalized terms used within this Service Level and Support Plan but not defined herein shall be defined in the applicable Agreement and/or Schedule.

1. "Business Hours" means 8:00am-6:00pm in the time zone in which the Customer's headquarters are located, or another location if designated in writing by the Customer.
2. "Business Day" means Monday through Friday in the time zone in which the Customer's headquarters are located, or another location if designated in writing by the Customer, excluding Holidays.
3. "Certified Contact" will be defined as a support contact that has successfully completed Level 1 Certification required for Standard Support: Time and Attendance Troubleshooting and/or Forecasting and Scheduling Troubleshooting, and/or Level 1 & 2 Certification required for Select and Signature Support for all SaaS Services purchased.
4. "Disaster" means an event after which WFS determines the SaaS Service should be failed over to the disaster recovery site.
5. "Downtime" means the Total Minutes in the Month during which the Production Environment is not available, except for Excluded Downtime.
6. "Excluded Downtime" means Total Minutes in the Month during which the Production Environment is not available attributable to:

    (i) Scheduled Maintenance Windows;

(ii) SaaS Service updates;

(iii) Content provided by Third-Party Content Vendors;

(iv) Factors outside of WFS's reasonable control, such as unpredictable and unforeseeable events that could not have been avoided even if reasonable care had been exercised, including, without limitation, a Force Majeure event.

7. "Hardware" shall mean the data collection terminal(s) and any related accessories rented or purchased by Customer from WFS.

8. "Holidays" means public holidays of England and New South Wales, and U.S. federal holidays.

9. "Month" means a calendar month.

10. "Scheduled Maintenance Window" means a window of time during which the SaaS Service may be down for maintenance, which window is (a) 3:00 am Sunday to 4:00 am Sunday U.S. Eastern Time for US and Canada datacenters; (b) 3:00 am Sunday to 4:00 am Sunday Central European Time for European datacenters; (c) 3:00 am Sunday to 4:00 am Sunday Australian Eastern Time for Asia Pacific/Australia datacenters; (d) an extended window of time of which the Customer has been notified at least ten (10) business days in advanced; and (e) a window of time scheduled with the Customer to perform maintenance or updates to the Customer's Production Environment.

11. "Severity Level 1" shall be defined as an issue whereby production application services are down and no workaround is immediately available; all or a substantial portion of the application or critical data is unavailable or at a significant risk of loss or corruption; and business operations have been severely disrupted. Severity Level 1 support requires the Customer to have dedicated resources available to work with WFS on the issue on an ongoing basis while the issue is active. This definition shall be applicable to the SaaS Services and not to the Hardware, which has its own definition of Severity Level 1.

12. "Severity Level 2" shall be defined as an issue whereby major application functionality is severely impaired and a workaround is unavailable; application services are impaired however continue to function without an immediate impact to the critical components of the application; and a major business milestone is at risk. This definition shall be applicable to the SaaS Services and not to the Hardware, which has its own definition of Severity Level 2.

13. "Severity Level 3" shall mean all other issues not categorized as Severity Level 1 or Severity Level 2. A Severity Level 3 issue is an issue that results in a non-critical loss of application services or functionality. A workaround may or may not be available that allows the user to continue to use the non-critical application functionality. Severity Level 3 does not include new enhancements to any WFS SaaS Services. This definition shall be applicable to the SaaS Services and not to the Hardware, which has its own definition of Severity Level 3.

14. "Solution Health Check" is defined as an analysis of the Customer's configuration within the Production Environment where WFS consults with the Customer to understand pain points and other business needs that WFS can solve for. This is initiated by conducting interviews with sample groups from different levels of the Customer's organization and the output is an executive summary of recommendations by WFS. Some of these recommendations include, but are not limited to, additional training, enhancements, and/or configuration changes.

15. "System Availability Percentage" means the average percentage of total time during which the Production Environment is available to Customer, calculated as follows:

$$SystemAvailabilityPercentage = (\left(\frac{TotalMinutesInTheMonth - Downtime}{TotalMinutesInTheMonth}\right) * 100)$$

16. "Technical Account Manager" or "TAM" is a single point of contact responsible for overseeing and coordinating support cases, data trending, product issues, escalations, and questions related to WFS support.

17. "Total Minutes in the Month" are measured 24 hours at 7 days a week during a Month.

18. "WFS" shall mean the applicable WFS contracting entity (as defined within the Agreement with the Customer) and its affiliates.

Service Level Terms and Condition

WFS shall provide the following service levels for the SaaS Service.

Backup Services	WFS is responsible for backup and restoration of data stored in the SaaS Service. WFS shall backup all Customer Data in its entirety every seven (7) days. WFS shall backup all changes to Customer Data every twenty-four (24) hours.
Data Retention	Please refer to the WFS Data Retention Policy
Disaster Recovery Time Objective	Except as otherwise noted herein, failover of Production Environment functionality to the Disaster Recovery site will occur within twelve (12) hours of WFS declaring a Disaster.
Disaster Recovery Point Objective	Maximum data loss of one-and-a-half (1.5) hours of data stored in the Production Environment.

1. If Customer provides written notice to WFS of WFS's failure to satisfy the Uptime Commitment within thirty (30) days of the end of a Month, WFS will credit to Customer 2% of the fees paid for the SaaS Services attributable to the Month in which the failure occurred (the "Monthly Subscription Fees") for each 1% below SLA, not to exceed 100% of Monthly Subscription Fees.

2. The Uptime Commitment does not apply in the first thirty (30) days of use of a Production Environment, during which time WFS may need to tune the environment for Customer based on its actual usage patterns.
3. To ensure WFS can proactively add resources to a Customer's Production Environment so that performance or availability is not impacted, Customer shall notify WFS in writing at least sixty (60) days in advance of any period when it reasonably believes the number of Active Employees or peak usage transaction volume to the SaaS Service may increase by more than 20% over the prior thirty (30) day period and at least ninety (90) days in advance if it expects more than a 50% increase. Failure to provide such notification shall release WFS of the Uptime Commitment and Estimated Resolution Target obligations herein for a period of ninety (90) days from the date such increase occurred.
4. The Uptime Commitment does not apply during a Force Majeure Event and shall be reinstated again only after the SaaS Service has been fully restored at the primary facility.
5. If Customer elects to have any services provided by a third party, WFS shall have no liability for any defect or failure of the SaaS Service caused by such third-party services, and Customer shall not be entitled to any reduction in fees for the SaaS Service. WFS may deny access to the SaaS Service to any third party which WFS determines in its sole discretion poses a security risk or other risk to WFS systems, data or intellectual property.

Support Plan Terms and Conditions

General Terms

1. SLA Response Times shall be measured from the time Customer contacts Support via one of the methods described above until a return response from WFS is provided. All communication shall be in English.
2. WFS Support will make analysts available during the Business Hours observed in Customer's time zone (where Customer's headquarters are located), excluding Holidays.
3. WFS and its support staff observe Holidays. No live support is offered to Customer on Holidays, except for Severity Level 1 and Severity Level 2 issues.
4. The response and/or resolution commitments herein shall not apply to any Severity Level 3 issues which require a patch or new functionality, including without limitation (a) product related enhancement requests, or (b) defect issues which do not materially affect the SaaS Service, or (c) any other issues relating to Severity Level 3 which require a patch or new functionality.
5. WFS may modify the service levels, fees, and offerings of any Support Plan, but such changes shall not apply to the Support Plan for the current Service Term.

Training and Certifications

1. Customers shall be entitled to the number of Support Contacts, including Certified Contacts, as displayed above according to the level of Support selected by the Customer.

2. Any Level 1 Training provided for Certified Contacts as stated above must be completed within one hundred and eighty days (180) from the original Agreement Effective Date. Any Level 2 Training provided for Certified Contacts as stated above must be completed within sixty (60) days from the Customer's "Go Live" date. Customer must retain the number of Certified Contacts as listed above for the Support level selected by Customer. If any of the Certified Contacts are replaced by the Customer, the newly named contact(s) shall complete the appropriate WFS Certification Process within sixty (60) days of being selected.

3. Only a Certified Contact may request and approve any alterations of the Customer's Production Environment. Customer's uncertified Support Contacts will have access to WFS Support staff to report only Severity Level 1 or Severity Level 2 issues.

4. Notwithstanding anything else herein, in the event that Customer does not have the number of Certified Contacts as required above, the SLA Response Times and Estimate Resolution Targets shall not apply; however, if Customer loses a Certified Contact but still has a Certified Contact, it shall have a cure period of ninety (90) days to obtain the required amount of Certified Contacts listed above before the SLA Response Times and Estimated Resolution Targets are not applicable.

Professional Services (where applicable)

1. New enhancements, including, but not limited to paycode, pay rules, accrual banks, holiday policies, etc., will be routed to WFS's Service Request Department or Application Managed Services (when contracted) for completion.
2. All professional services will be directly invoiced to Customer as billable technical support at the applicable hourly rate after services have been rendered.
3. All enhancement requests estimated over sixteen (16) hours will require the generation of a Statement of Work defining the project scope and will be assigned a WFS project manager.

Hardware (where applicable)

1. Severity Level Definitions for Hardware

    a. **Severity Level 1:** A critical problem that renders one or more key functions of the Hardware unusable, no reasonable work around exists, and for which immediate resolution is required to meet processing deadlines.

    b. **Severity Level 2:** Any other critical problem that renders one or more key functions of the Hardware unusable.

   c. **Severity Level 3:** Any other problem with the Hardware that is not categorized as Severity Level 1 or Severity Level 2.

2. If the Hardware is rented by the Customer from WFS, the term of this Hardware Support Plan shall match the term of the rental. If the Hardware is purchased by the Customer, the term of the Hardware Support Plan shall be listed in the applicable ordering document, subject to any renewal terms (the "Support Period").

3. Customer may select either Standard or Premium Support for Hardware. Both options cover the cost of parts, labor, and shipping to Customer's facility for any covered repairs of defects in manufacturer's workmanship of the Hardware. Customer is responsible for shipping charges to WFS. To make a support claim, Customer shall first contact WFS and speak to the WFS Support department. After diagnosis and upon authorization, Customer will be provided shipping instructions to return the unit to WFS for repair.
   a. Under Standard Support, WFS will repair the Hardware, or if in its opinion such repair cannot be made, it will provide replacement Hardware. Repairs are generally completed within 4-6 weeks. WFS makes no delivery guarantees, including without limitation for delays caused by international shipping or customs. WFS will return units to the Customer at no charge via ground shipping. Alternate shipping methods may be selected by the Customer at an additional charge.
   b. Under Premium Support, WFS will ship replacement Hardware overnight at no cost to Customer the same Business Day (or the next Business Day for calls after 3 pm Eastern Time). WFS makes no delivery guarantees, including without limitation for delays caused by international shipping or customs. Customer shall ship the faulty Hardware to WFS concurrently via ground shipping. If the faulty Hardware is not received by WFS within ten (10) business days, Customer will be invoiced for the Hardware shipped.

4. The Hardware Support Plans only cover repairs or replacement units of the same type and model. If parts or replacement units are not available, next generation Hardware will be provided.

5. Customer shall be responsible for all set up and maintenance of the Hardware on Customer's site. WFS does not provide installation assistance.

6. Notwithstanding anything to the contrary contained herein, in no event shall any Support Plan for Hardware extend or be effective beyond six (6) years from the date that the Hardware was initially purchased or rented except upon mutual agreement of the parties.

7. Support Plans renew automatically for additional one (1) year periods (but for no more than six (6) years total) upon the end of the Support Period and each subsequent renewal unless Customer notifies WFS of its decision to cancel the Support Plan at least fifteen (15) days prior to the end of the then-current Support Period. To avoid a disruption in the Support services, Customer should pay any fees due for the Support at least fifteen (15) days prior to the beginning of each new Support Period.

8. Normal wear and tear and intentional damage to Hardware is not covered by the Support Plan and fees will be chargeable to Customer at WFS's standard charges for parts and labor in the event that any defect in the Hardware is due to normal wear and tear or intentional damage and Customer requests, and WFS elects to repair, any such normal wear and tear or intentional damage. WFS makes no representations on the availability of parts or replacement units. WFS reserves the right to deliver new Hardware, repaired Hardware, or refurbished Hardware at its option for any covered repair. WFS's obligation shall be subject to its determination that the Hardware has not been modified, serviced,

or repaired by any other party and that the Hardware was installed and operated within the Hardware specifications for its intended use. Any misuse, negligence, accident, abuse, or alteration of a serial number will void the support obligations. This Support Plan extends solely to the original purchaser of the Hardware and all claims must be made by the Customer.

EXHIBIT B – DATA PROCESSING AGREEMENT

BETWEEN:

The entity listed as the Customer in the Workforce Software Indirect SaaS Agreement (the "**Agreement**"), hereinafter to be referred to as the "**Data Controller,**"

AND

WorkForce Software, LLC, a limited liability company under the laws of the State of Delaware in the United States, having its registered office in Wilmington, Delaware at 2711 Centerville Road, Suite 400 and principal place of business in Livonia, Michigan at 38705 Seven Mile Road, Suite 300 (hereinafter to be referred to as: the "**Data Processor**" or "**WFS**").

The Data Processor and the applicable Data Controller are referred to herein individually as a "**Party**" and collectively as the "**Parties**."

THE PARTIES HEREBY AGREE AS FOLLOWS:

This Data Processing Agreement forms part of and is hereby incorporated into the Agreement by reference. Any capitalized terms not otherwise defined in this Data Processing Agreement shall have the meaning given to them in the Agreement. Except as modified below, the terms of the Agreement shall remain in full force and effect.

1. **Subject matter of this Data Processing Agreement**

1.1. This Data Processing Agreement applies to the Processing of Personal Data with respect to the Parties' rights and obligations regarding data processing under the current Agreement by and between WFS and the Data Controller ("**Services**").

1.2. The term "Data Protection Law" shall mean applicable data protection and privacy legislation, regulations and guidance as amended, adopted, or superseded from time to time, including but not limited to: the UK Data Protection Act 2018 (or all applicable legislation enacted in the United Kingdom in respect of the protection of personal data), Regulation (EU) 2016/679 (the "**General Data Protection Regulation**" or "**GDPR**"), the Privacy and Electronic Communications (EC Directive) Regulations 2003, the California Consumer Privacy Act ("**CCPA**"), New Zealand's Privacy Act 2020, Australia's Privacy Act 1988 (Cth), and Singapore's Personal Data Protection Act 2012.

1.3. Any capitalized terms not otherwise defined in this Data Processing Agreement shall have the meaning given to them in the Agreement. Except as modified below, the terms of the Agreement shall remain in full force and effect. Other terms used in this Data Processing Agreement shall have meanings ascribed to them in GDPR, but shall apply irrespective of whether or not GDPR is applicable. This includes, but is not limited to, "Processing", "Personal Data", "Data Subject", and "Personal Data Breach."

1.4. Insofar as the Data Processor will be processing Personal Data subject to Data Protection Law on behalf of the Data Controller in the course of the performance of the Agreement with the Data Controller, the terms of this Data Processing Agreement shall apply.

1.5. In the event of a conflict between any provisions of the Agreement and the provisions of this Data Processing Agreement, the provisions of this Data Processing Agreement shall prevail.

1.6. An overview of the categories of Personal Data, the categories of Data Subjects, and the nature and purposes for which the Personal Data are being processed is provided in **Appendices D and E**.

2. The Data Controller and the Data Processor

2.1. The Parties shall at all times comply with their respective obligations under the Data Protection Laws and this Data Processing Agreement in connection with the Processing of Personal Data.

2.2. The Data Controller will determine the scope, purposes, and manner by which the Personal Data may be accessed or Processed by the Data Processor.

2.3. The Data Processor will only Process the Personal Data to the extent that this is required for the provision of the Services or as otherwise needed to perform its obligations under the terms of the Agreement and this Data Processing Agreement, and otherwise in accordance with the documented instructions of the Data Controller. The Data Processor shall not sell or share Personal Data, or otherwise retain, use, or disclose the Personal Data for any purpose other than for the business purposes specified in Agreement, which shall include any documented instructions from the Data Controller. The Data Processor shall immediately notify the Data Controller if, in its opinion, any instruction infringes Data Protection Law, unless legally prohibited from doing so.

2.4. The Data Controller warrants and undertakes that it has all necessary rights and legally required consents to provide the Personal Data to the Data Processor for the Processing to be performed in relation to the Services and otherwise in connection with the Agreement, and the Data Controller further warrants and undertakes that all Personal Data Processed by either Party under or in connection with this Data Processing Agreement has been obtained fairly and lawfully and, in all respects in compliance with Data Protection Law.

2.5. To the extent that the Data Controller is part of a group of companies, it confirms it has the authority to bind all entities in the group of companies to this Data Processing Agreement.

2.6. Where permitted by Data Protection Law, Data Processor may Process Personal Data: (i) for its internal uses to build or improve the quality of its services; (ii) to detect security Incidents; and (iii) to protect against fraudulent or illegal activity.

2.7. Data Processor may: (i) compile aggregated and/or de-identified information in connection with providing the Services, provided that such information cannot reasonably be used to identify Data Controller or any data subject to whom Personal Data relates ("**Aggregated and/or De-Identified Data**"); and (ii) use Aggregated and/or De-Identified Data for its lawful business purposes.

3. Confidentiality

3.1. Without prejudice to any existing contractual arrangements between the Parties, the Data Processor shall treat all Personal Data as confidential, and shall inform all its employees, staff, agents and/or approved sub-processors engaged in processing the Personal Data of the confidential nature of the Personal Data. The Data Processor shall ensure that all such persons or parties have signed an appropriate confidentiality agreement, are otherwise bound to a duty of confidentiality, or are under an appropriate statutory obligation of confidentiality.

4. Security

4.1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Data Controller and Data Processor shall implement appropriate technical and organizational measures designed to ensure a level of security of the Processing of Personal Data appropriate to the risk. These measures shall include, at a minimum, the security measures described in **Appendix A**.

5. Improvements to security

5.1. The Parties acknowledge that security requirements are constantly changing, and that effective security requires frequent evaluation and regular improvements of outdated security measures. The Data Processor will therefore evaluate the measures as implemented in accordance with Article 4 on an on-going basis in order to maintain compliance with the requirements set out in Article 4. The Parties will negotiate in good faith the cost, if any, to implement material changes required by specific updated security requirements set forth in Data Protection Law or by data protection authorities of competent jurisdiction.

5.2. Where an amendment to this Data Processing Agreement is required following or as part of an update to security measures, as per Section 5.1 above, or in light of changes to Data Protection Law, from time to time, the Parties shall negotiate as needed an amendment to this Data Processing Agreement in good faith.

6. Audit rights

6.1. Upon the Data Controller's reasonable request, the Data Processor shall provide for review, all relevant and necessary material, documentation, and information as required in order to demonstrate the Data Processor's compliance with the Data Protection Law and this Data Processing Agreement.

6.2. In the event that Data Controller reasonably believes that the information referred to in Article 6.1 indicate any material non-compliance by the Data Processor under the Data Protection Law and/or this Data Processing Agreement, then the Data Controller may give the Data Processor not less than thirty (30) days' prior written notice of its intention to undertake an audit, which may include inspections of the Data Processor's premises, provided that:

6.2.1. if a third party is to conduct the audit, the third party must not be a competitor of the Data Processor, and the third party must execute a written confidentiality agreement acceptable to the Data Processor or otherwise be bound by a statutory or legal confidentiality obligation;

6.2.2. such audit shall be limited to once per calendar year, unless the audit reveals material non-compliance with this Data Processing Agreement;

6.2.3. the audit must be conducted during regular business hours at the applicable facility, in a manner which does not unreasonably interfere with the Data Processor's business activities; and

6.2.4. unless the Data Processor expressly agrees otherwise, the audit shall not exceed three (3) business days in duration.

6.3. Upon completion of the audit pursuant to Article 6.2, the Data Processor will provide the Data Controller with a copy of the audit report, which is subject to the confidentiality terms of the Agreement. The Data Controller may use the audit reports only for the purposes of meeting the Data

Controller's legal obligations pursuant to Data Protection Law and/or confirming compliance with the requirements of this Data Processing Agreement.

6.4. Each party will bear its own costs in relation to the provision of information or an audit conducted pursuant to this Article.

7. [Intentionally Omitted]

8. Personal Data Breach notification and assistance

8.1. When the Data Processor becomes aware of a Personal Data Breach, it shall promptly notify the Data Controller within 24 hours about the same, and shall reasonably cooperate with the Data Controller in order to enable the Data Controller to take suitable further steps in respect of the Personal Data Breach as required by Data Protection Law.

8.2. Any notifications made to the Data Controller pursuant to this Article 8 shall be addressed to the employee of the Data Controller whose contact details are provided in the Agreement.

9. Contracting with Sub-Processors

9.1. Except as permitted by Article 9.2 of this Data Processing Agreement, the Data Processor shall not subcontract its Processing of the Personal Data without the prior written authorisation of the Data Controller.

9.2. The Data Controller hereby authorises the Data Processor to engage the sub-processors listed in https://workforcesoftware.force.com/customers/s/article/Third-parties-sub-processors-who-store-or-process-customer-data, as updated from time to time, to provide the Services. The Data Processor shall inform the Data Controller of any addition or replacement of such sub-processors giving the Data Controller an opportunity to object to such changes. If the Data Controller sends the Data Processor a written objection notice in a timely manner (but in any event within 30 days of being notified), setting forth a reasonable basis for objection, the Parties will make a good-faith effort to resolve Data Controller's objection. In the absence of a resolution, the Data Processor will, subject to Article 9.3 below, make commercially reasonable efforts to provide Data Controller with the same level of service described in the Agreement, without using the proposed sub-processor to process Data Controller's Personal Data. If the Data Processor's efforts are not successful within a reasonable time, each party may terminate the portion of the service which cannot be provided without the sub-processor, and the Data Controller will be entitled to a pro-rated refund of the applicable service fees.

9.3. The Data Controller understands and acknowledges that the Data Processor has agreed upon certain prices and fees with the Data Controller based on the assumption that it would be able to utilize the sub-processors proposed at https://workforcesoftware.force.com/customers/s/article/Third-parties-sub-processors-who-store-or-process-customer-data, as updated from time to time. In the event Data Controller objects to Data Processor utilizing one or more of those sub-processors in accordance with Article 9.2, Data Processor reserves the right to increase any prices or fees previously agreed upon between the Parties.

9.4. Notwithstanding any authorisation by the Data Controller within the meaning of the preceding Article, the Data Processor shall remain fully liable vis-à-vis the Data Controller for the performance of any such sub-processor that fails to fulfill its data protection related obligations.

9.5. The Data Processor shall ensure that each sub-processor is bound by data protection obligations substantively equivalent to those imposed on the Data Processor as applicable under this Data Processing Agreement.

10. Returning or destruction of Personal Data

10.1. Upon termination of this Data Processing Agreement, upon the Data Controller's written request the Data Processor shall, at the discretion of the Data Controller, either delete, destroy, or return all Personal Data to the Data Controller and destroy or return any existing copies.

11. Assistance to Data Controller

11.1. The Data Processor shall provide reasonable assistance to and comply with all reasonable instructions from Data Controller related to requests from individuals for exercising their data subject rights under the Data Protection Laws, as well as with requests, notices and other communications with an Information Commissioner or other relevant supervisory authority or regulator.

11.2. Taking into account the nature of processing and the information available to the Data Processor, the Data Processor shall provide commercially reasonable assistance to the Data Controller in ensuring compliance with its data security related obligations, as well as other Data Controller obligations under Data Protection Law that are relevant to this Data Processing Agreement, including notifications to a supervisory authority, other regulator, or to Data Subjects, the process of undertaking a Data Protection Impact Assessment, and with prior consultations with supervisory authorities.

12. Duration and termination

12.1. Unless expressly agreed otherwise, this Data Processing Agreement shall come into effect on the date on which the Agreement becomes effective.

12.2. Termination of this Data Processing Agreement shall not discharge the Data Processor from its confidentiality obligations pursuant to Article 3.

12.3. The Data Processor shall process Personal Data until the date of expiration or termination of the Agreement and whereupon this Data Processing Agreement shall automatically terminate without further action on the part of the Parties.

13. Liability

13.1. Each Party's total aggregate liability to the other arising out of or in connection with any breaches of applicable Data Protection Law and/or this Data Processing Agreement shall be subject to the exclusions and limitations of liability set out in the Agreement.

14. Miscellaneous

14.1. This Data Processing Agreement and the Agreement represent the entire agreement of the Parties with respect to the subject matter hereof, and supersedes all prior discussions, writings, communications, emails and/or agreements between the Parties and are intended to be the final expression of their agreement. Each Party acknowledges that, in entering into the Data Processing Agreement and the documents referred to in it, it does not rely on any statement, representation, assurance or warranty ("**Representation"**) of any person (whether a Party to this Data Processing Agreement or not) other than as expressly set out in the Data Processing Agreement or those documents. Each Party agrees that the only rights and remedies available to it arising out of or in connection with a Representation shall be for breach of contract. Nothing in this Article shall limit or exclude any liability for fraud or fraudulent misrepresentation.

14.2. All notices and other communications under this Data Processing Agreement shall be addressed to the Parties made by hand, courier, or first class pre-paid mail (either recorded delivery or registered) and will be deemed to have been communicated upon the date of actual delivery, provided that the Parties may agree to serve notices by ordinary first class pre-paid mail, fax and/or email. The addresses for service shall be as first stated in this Data Processing Agreement, or such other address that each Party may notify to the other in writing for such purpose.

14.3. The rights of any third party under this Agreement, whether pursuant to The Contracts (Rights of Third Parties) Act 1999 or otherwise, are hereby excluded.

14.4. An amendment or change to the terms of this Data Processing Agreement, will be effective when it is documented and agreed in writing by the Parties, and signed by and for and behalf of each of the Parties by their respective authorised signatories.

14.5. No failure or delay by either Party to exercise any right, power or remedy shall operate as a waiver of that right, power or remedy nor shall any partial exercise preclude any further exercise of the same, or of any other right, power or remedy.

14.6. This Data Processing Agreement is governed by the law of the jurisdiction as specified in the Agreement, and each party agrees to submit to the exclusive jurisdiction of the courts in that jurisdiction.

15. Notices

Contact information of the Privacy Officer and Data Protection Officer of the Data Processor:

First point of contact - Data Privacy Officer (for all WFS entities worldwide)

Privacy Officer
WorkForce Software, LLC
38705 Seven Mile Road, Suite 300
Livonia, MI 48152
United States of America
+1-877-493-6723
privacy@workforcesoftware.com

Second point of contact - Data Protection Officer (for all WFS entities worldwide)

GRCI Law
Unit 3 Clive Court
Bartholomews Walk
Cambridgeshire Business Park
Ely
Cambridgeshire
CB7 4EA UK
dpoaas@grcilaw.com
+44 (0) 333 800 7000

Appendix A: TECHNICAL AND ORGANISATIONAL MEASURES

This Appendix is hereby incorporated by reference into this Data Processing Agreement.

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Measures of pseudonymisation and encryption of personal data

The Data Importer shall take steps to employ encryption on personal devices that store or access Personal Data and leverage provided pseudonymisation and encryption capabilities in WorkForce Suite and related software and systems to protect Personal Data.

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

The Data Importer shall take steps to secure endpoints used to access Personal Data with unique user IDs, strong passwords, hard drive encryption, anti-virus/anti-malware, automatic operating system updates, and routine software updates. Access to data shall be performed only over encrypted connections.

The Data Importer shall not bypass or interfere with any confidentiality, integrity, availability, and resilience capabilities in WorkForce Suite and related software and systems.

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

WorkForce Suite and related software and systems provide availability and access features; the Data Importer shall not bypass such functionality, and will leverage such functionality as appropriate;

Processes for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing

The Data Exporter shall periodically assess the effectiveness of technical and organisational measures of the Data Importer. The Data Importer shall periodically assess its compliance with the requirements in this Appendix.

Measures for user identification and authorization

Where appropriate, the Data Importer shall use unique user IDs for Data Importer processing equipment (e.g., PCs, mobile devices) and strong, high entropy passwords. Data Importer shall leverage provided identification and authorization capabilities in WorkForce Suite and related software and systems to the extent applicable to protect Personal Data.

Measures for the protection of data during transmission

The Data Importer shall take steps to ensure that Personal Data is only accessed or transferred over an encrypted connection.

Measures for the protection of data during storage

Data Importer will take steps to ensure all storage devices, hard drives, storage area networks, and mobile devices that are used to process Personal Data have at least AES-256 encryption.

Measures for ensuring physical security of locations at which personal data are processed

Data Importer shall take steps to ensure personal data is only accessed from locations where there is appropriate technical and administrative controls to protect against unauthorized disclosure.

Measures for ensuring events logging

Data Importer shall take steps to enable event logging on all personal devices used to process Personal Data.

Measures for ensuring system configuration, including default configuration

Personal devices (laptops, PCs, mobile devices, etc.) used by Data Importer to process Personal Data shall be run only vendor-supported operating systems that are routinely patched.

Measures for internal IT and IT security governance and management

The Data Importer is solely responsible for security governance and management of systems, software, and processes under its control.

Measures for certification/assurance of processes and products

The Data Importer will provide reasonable evidence of compliance with applicable data protection and privacy legislation, and of compliance with required technical and organisational measures upon request of the Data Exporter.

Measures for ensuring data minimization

The Data Importer, when appropriate, will work with the Data Exporter to determine what data is necessary for its processing to meet customer processing requirements.

Measures for ensuring data quality

The Data Importer, when appropriate, will work with the Data Exporter to determine appropriate data quality measures, which may include data input validation and business rules testing.

Measures for ensuring limited data retention

The Data Importer, when appropriate, will work with the Data Exporter to determine appropriate data retention options.

Measures for ensuring accountability

The Data Importer shall provide its staff responsible for processing Personal Data with unique IDs used to access its devices and applications to ensure accountability through access and change records in logs.

Measures for allowing data portability and ensuring erasure

The Data Importer will advise the Data Exporter on options for data portability (e.g., report options) and take steps to erase any temporary files under its control after the are no longer required.

EXHIBIT C – WORKFORCE DATA RETENTION POLICY

WFS will retain only three (3) years of Customer Data in the SaaS environment. Customers will be notified ninety (90) days prior to the data purge operation. If the Customer does not confirm acceptance of the data purge prior to the end of the ninety (90) days, WFS shall not purge the data and shall instead charge the Customer data storage fees according to this policy but on a monthly basis, to be invoiced monthly in arrears. Customer shall be required to give thirty (30) days' written notice prior to terminating the data storage service herein. Options for Customers who desire to retain their historical data are listed below:

1. Customers may request from WFS a free annual copy of their data, provided as an Oracle backup. Additional backups can be provided for a fee. WFS can also provide the data in a mutually agreed upon format other than Oracle backup for a fee. The Customer may download the copy via SFTP.

2. Customers may elect to have WFS retain their data online in the SaaS environment for an additional fee.

EXHIBIT D – THIRD PARTY SERVICES

1. Definitions

1.1. “Regulatory Content and Data” means legal or regulatory content, reference materials, or data supplied by Third Party Content Vendors as a function of select optional Third-Party Services.

1.2. “Third Party Content Vendors” means CCH Incorporated, its licensors and Affiliates, and any other firm which provides regulatory content, data or legal reference materials in the SaaS Service.

1.3. “Third Party Services” means term-based ancillary services provided by third parties which may involve internet or phone delivery including, but not limited to, the Regulatory Update Service, Compliance Portal, IVR, Text Messaging and Mobile Services and which, if ordered by Customer, will be included on an applicable Order Form. Third Party Services shall be governed by this Exhibit D. Terms of this Exhibit D supersede the terms in the Agreement with regards to any Third-Party Services.

2. Terms and Conditions

2.1. WFS shall provide access to the Third-Party Services specified in the Order Forms for the term specified and for the fees indicated. Third Party Services are non-cancelable and non-refundable for the term specified. Customer may be required to use a compatible version of the SaaS Service to access the Third-Party Services. Such use of the Third-Party Services shall be restricted to Customer’s Authorized Users. Customer shall take necessary steps to prevent unauthorized use of the Third-Party Services by third parties using its passwords and shall be liable for any such unauthorized use.

2.2. Third Party Services, including the Leave Regulation Update Service, may involve services and materials provided by third parties (“Third Party Providers”) including legal and related content (the “Regulatory Content”). The Regulatory Content may be provided by the Third-Party Providers and/or by WFS. Access to the Regulatory Content and Third-Party Services may involve additional terms and conditions, which can be accessed via the web pages of the Third-Party Providers. WFS will make commercially reasonable efforts to communicate any policies, requirements, or guidelines of those third parties to Customer. Customer agrees to be bound to such additional terms and conditions. ANY ACTUAL OR ALLEDGED VIOLATION OF A THIRD-PARTY POLICY, REQUIREMENT, OR GUIDELINE BY CUSTOMER MAY RESULT IN A TERMINATION OF SERVICE AND IS CUSTOMER’S RESPONSIBILITY.

2.3. Customer acknowledges that the Third-Party Services may be subject to limitations, delays, and other problems which are beyond the control of WFS and that WFS shall have no liability for any delays, failures, or unavailability resulting from such problem. Notwithstanding anything else in this Agreement, in the event that a Third Party Service fails or is not available, WFS’s sole and exclusive liability in any way related to such unavailability of the Third Party Service will be to return the fees paid for the Third Party Service for the period of time the Third Party Service was unavailable. This Section survives the termination of the Agreement.

2.4. Notwithstanding anything else in the Agreement, including, but not limited to, claims for breach of confidentiality and data security, or Intellectual Property Right infringement, (a) WFS and Third Party Providers shall have no liability whatsoever for the Regulatory Content and Third Party Services and does not provide any warranties; (b) WFS assumes no responsibility regarding Customer Data used in any text messages as part of a Third Party

Service and Customer understands that such data will not be encrypted, and agrees to not send Social Security numbers, national identification numbers, payroll information, or other data considered sensitive in nature via text messages; (c) the Regulatory Content and Third Party Services are the copyrighted materials of WFS, the Third Party Providers or its licensors and they exclusively reserve all rights and interests in such; (d) THE THIRD PARTY PROVIDERS SHALL HAVE NO LIABILITY TO THE CUSTOMER; (e) THE REGULATORY CONTENT AND THIRD PARTY SERVICES ARE PROVIDED ON AN "AS, IS" BASIS AND WITHOUT ANY WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED; and (f) THE THIRD PARTY PROVIDER AND WFS DISCLAIM ALL WARRANTIES WITH RESPECT TO THE REGULATORY CONTENT AND THIRD PARTY SERVICES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, UNINTERRUPTED USE, TITLE, QUIET ENJOYMENT AND INFORMATION COMPLETENESS, CURRENCY OR ACCURACY. TO THE EXTENT SUCH DISCLAIMER CONFLICTS WITH APPLICABLE LAW, THE SCOPE AND DURATION OF ANY APPLICABLE WARRANTY WILL BE THE MINIMUM PERMITTED UNDER SUCH LAW. This Section survives the termination of the Agreement.

2.5. Access to the Compliance Portal (if ordered by Customer) may involve additional terms and conditions, which can be accessed via web pages from within the Compliance Portal. If Customer does not agree with such additional terms and conditions, it may terminate the order for the Compliance Portal within thirty (30) days of delivery of the Compliance Portal and WFS shall return all fees related to the Compliance Portal.

2.6. Customer will not, and will not permit any person (including, without limitation, Authorized Users) to, at any time, directly or indirectly: (a) use the Third Party Service in any manner beyond the scope of rights expressly granted in this Agreement; (b) modify or create derivative works of the Third Party Service or Documentation, in whole or in part; (c) reverse engineer, disassemble, decompile, decode or otherwise attempt to derive or gain improper access to any software component of the Third Party Service, in whole or in part; (d) except as expressly allowed herein or within an Order Form, frame, mirror, sell, resell, rent or lease use of the Third Party Service to any other entity, or otherwise allow any entity to use the Third Party Service for any purpose other than for the benefit of Customer in accordance with this Agreement; (e) use the Third Party Service or Documentation in any manner or for any purpose that infringes, misappropriates, or otherwise violates any intellectual property right or other right of any entity, or that violates any applicable law; (f) interfere with, or disrupt the integrity or performance of, the Third Party Service, or any data or content contained therein or transmitted thereby; (g) access or search the Third Party Service (or download any data or content contained therein or transmitted thereby) through the use of any engine, software, tool, agent, device or mechanism (including spiders, robots, crawlers or any other similar data mining tools) other than software or Third Party Service features provided by WFS or the Third Party Provider for use expressly for such purposes; or (h) use the Third Party Service, Documentation or any other WFS or Third Party Provider Confidential Information for benchmarking or competitive analysis with respect to competitive or related products or services, or to develop, commercialize, license or sell any product, service or technology that could, directly or indirectly, compete with the Third Party Service.

3. Additional Terms and Conditions – Text Messaging Services

3.1. WFS is not responsible for any fees incurred as a result of text messages received by Customer employees regardless of whether or not such employees authorize the use of the Text Messaging Service. WFS shall not be responsible for the content of any text messages sent to

Customer employees. Customer shall indemnify and hold harmless WFS against all employee claims resulting from Customer's use of the Text Messaging Service.

3.2. Customer shall not attempt to use the Text Messaging Services to access or allow access to emergency services. WFS and the Third-Party Provider disclaim all liability arising from such use. Neither WFS nor its Third-Party Provider and representatives will be liable under any legal or equitable theory for any claim, damage, or loss arising from or relating to the inability to use the Text Messaging Services to contact emergency services. Customer shall ensure that the Text Messaging Services provided hereunder are used in accordance with all applicable laws, regulations and third-party rights, as well as the terms of this Agreement, including the Third-Party Provider's Acceptable Use Policy, which is hereby incorporated into this Agreement, and any data protection statute, regulation, order or similar laws.

3.3. WFS and/or Third-Party Providers exclusively own and reserve all right, title and interest in and to the Text Messaging Services and related materials provided by WFS or Third-Party Provider. All terms and conditions contained within the Agreement related to ownership and confidentiality shall extend equally to the property and information of Third-Party Providers.

4. EXCEPT FOR LIABILITY ARISING FROM VIOLATIONS OF SECTION 3.1, 3.2, OR 3.3 OF THIS EXHIBIT, UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY, WHETHER IN TORT, CONTRACT, OR OTHERWISE, WILL WFS, CUSTOMER OR THIRD PARTY PROVIDERS BE LIABLE TO THE OTHER FOR ANY INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL OR PUNITIVE DAMAGES OF ANY CHARACTER, INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF GOODWILL, LOST PROFITS, LOST SALES OR BUSINESS, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, LOST DATA, EVEN IF SUCH PARTY HAS BEEN ADVISED, KNEW OR SHOULD HAVE KNOWN OF THE POSSIBILITY OF SUCH DAMAGES, IN CONNECTION WITH OR ARISING OUT OF THIS EXHIBIT OR THE THIRD PARTY SERVICES.

5. EXCEPT FOR LIABILITY ARISING OUT OF SECTION 3.3 OF THIS EXHIBIT, UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY, WHETHER IN TORT, CONTRACT, OR OTHERWISE, WILL WFS OR THIRD PARTY PROVIDER BE LIABLE TO CUSTOMER FOR ANY DIRECT DAMAGES, COSTS, OR LIABILITIES IN EXCESS OF THE AMOUNTS PAID BY CUSTOMER FOR THE THIRD PARTY SERVICES DURING THE TWELVE MONTHS PRECEDING THE INCIDENT OR CLAIM.

6. THE PROVISIONS OF THIS EXHIBIT ALLOCATE THE RISKS UNDER THIS AGREEMENT BETWEEN THE PARTIES AND THE PARTIES HAVE RELIED ON THE LIMITATIONS SET FORTH HEREIN IN DETERMINING WHETHER TO ENTER INTO THIS AGREEMENT.

EXHIBIT E – ACCEPTABLE USE POLICY

This Acceptable Use Policy describes policies regarding the acceptable use of the SaaS Service.

Authorized Users shall not:

- use another user's account without permission;
- send unsolicited communications, promotions or advertisements, or spam;
- publish or link to malicious content intended to damage or disrupt another user's browser or computer or to compromise a user's privacy;
- access, tamper with, or use non-public areas of the SaaS Service, WFS's computer systems, or the technical delivery systems of WFS's providers;
- probe, scan, or test the vulnerability of any system or network or breach or circumvent any security or authentication measures;
- access or search the SaaS Services by any means other than publicly supported interfaces;
- use the SaaS Service to send altered, deceptive or false source-identifying information;
- interfere with, or disrupt, the access of any user, host or network, including, without limitation, sending a virus, overloading, flooding, spamming, mail-bombing the SaaS Service, or by scripting the creation of content in such a manner as to interfere with or create an undue burden on the SaaS Service. International users shall comply with all local laws regarding online conduct and acceptable content.

Authorized Users shall not post content that:

- may create a risk of harm, loss, physical or mental injury, emotional distress, death, disability, disfigurement, or physical or mental illness to the Authorized User, to any other person, or to any animal;
- may create a risk of any other loss or damage to any person or property;
- seeks to harm or exploit children by exposing them to inappropriate content, asking for personally identifiable details or otherwise;
- may constitute or contribute to a crime or tort;
- contains any information or content that WFS deems to be unlawful, harmful, abusive, racially or ethnically offensive, defamatory, infringing, invasive of personal privacy or publicity rights, harassing, humiliating to other people (publicly or otherwise), libelous, threatening, profane, or otherwise objectionable;
- contains any information or content that is illegal (including, without limitation, the disclosure of insider information under securities law or of another party's trade secrets);
- contains pornographic content or content that depicts violence or illegal activity;
- contains any information or content that you do not have a right to make available under any law or under contractual or fiduciary relationships;
- contains any information or content that you know is not correct and current.
- violates rights of any kind, including without limitation any intellectual property rights or rights of privacy.

PARTNER ORDER FORM - SAAS

This Order Form – SaaS (“Order Form”) shall be governed by the Master Professional Services Agreement dated _______________ 2024 (the “Agreement”) between Snohomish County Government (“County”) and Aspire HR, LLC. (“AspireHR”), the terms of which are incorporated herein by reference, where AspireHR is reselling the SaaS services as outlined below from Workforce Software (“WFS”) to the County. Additionally, this Order Form further incorporates specific terms related to the WFS SaaS service that the County explicitly agrees to be bound by as part of this Order Form. Partner shall be authorized to resell the SaaS Services set forth herein to the Customer set forth below:

Customer:	Snohomish County, WA	Order Form Effective Date:	August 14, 2023
Customer Address:	3000 Rockefeller Avenue Everett, WA 98201 United States	Commencement Date:	Upon contract execution
		Service Term:	5 years from Commencement Date followed by optional 5-year terms upon written notice from the County for the life of use

Suite Component	Service/Item Ordered	Description	Quantity	List Unit Price	Customer Discounted Unit Price	Extended Amount	Payment Terms
	WFS SaaS Products						
Time & Absence	1. WFS Absence	Absence Management - Time Off Requests, Accruals, Leave Cases	3,000	$20.00 PEPY	$10.00 PEPY	$30,000.00	Minimum Amount Due: $55,800.00/yr. fixed for years 1-5 total $279,000.00 5% annual increase each subsequent 5-year term

							Payments are due annually in advance, with the first payment invoiced on the Commencement Date. Customer shall be charged Overage Fees for any excess usage over the committed quantities herein, which shall be invoiced monthly in arrears.
Time & Absence	2. WFS Absence Compliance NA Rules Pak	Absence Compliance Rules for North America (US + Canada)	3,000	$14.00 PEPY	$8.60 PEPY	$25,800.00	
	Environment / Setup / Miscellaneous Fees						
Time & Absence	3. Support Plan	Standard Software Support	1	Included	Included	Included	
	AMOUNT DUE – FIRST YEAR					$55,800.00	
	TOTAL AMOUNT DUE YEARS 1-5				**Currency:** USD	**$279,000.00**	**Plus Overage Fees, if any**

Definitions

PM = Per Month | PEPY = Per Employee Per Year | PIPY = Per Item Per Year | PNUPY = Per Named User Per Year | PMIN = Per Minute
PSEC = Per Second | PSPY = Per Store Per Year

Terms and Conditions

The following Terms and Conditions shall apply to the SaaS Services ordered on this Order Form.

1. Usage of the applications and extensions herein shall be measured by Active Employee unless specified otherwise. “Active Employee” or “Employee” means an employee, leased employee, contractor, or sub-contractor, or equipment that has employee records with an

active status within the SaaS Service. All employees terminated within the Customer HRIS system shall retain an active status within the SaaS Service for a period of thirty (30) days. Such post-termination active status within the SaaS Service shall be for a period sufficient to account for the final, post-termination processing of employee data.

2. “Named User” is an individual authorized by Customer to use the particular application or service regardless of whether the individual is actively using the program or service at any given time.
3. The Report Authoring Seat and associated ability to view reports may only be used if the reports created or viewed contain data generated by the SaaS Service.
4. Although WFS may provide access to Customer to modules other than those subscribed to above, Customer may use only the modules of the SaaS Service specified in this Order Form.
5. One (1) Production Environment, one (1) Test Environment, and one (1) Development Environment shall be provided in addition to any other environments specified in this Order Form. Notwithstanding the foregoing, only one (1) Production Environment shall be provided for the Employee Experience Suite Components.
6. Except for the Employee Experience Suite Components, Customer shall be entitled to one (1) Environmental Refresh per year at no additional charge. An Environmental Refresh shall be the duplication of data between any of the aforementioned environments.
7. Customer data will be hosted within the following region: United States
8. This Order Form shall automatically renew at the end of the Service Term for an additional five (5) year period (the “Renewal Term") unless County provides notice to AspireHR of its intent not to renew the Order Form at least sixty (60) days prior to the end of the Service Term. The per-unit pricing during the Renewal Term shall be increased by five percent (5%) over the prices set forth herein.

All capitalized terms used in this Order Form have the meanings set forth herein or as specified in the Agreement. Execution of this Order Form represents the acceptance by County and Aspire of all terms set forth herein. Except as expressly set forth or modified herein, all terms of the Agreement shall remain in full force and effect. In the event of any conflict between the terms of this Order Form and of the Agreement, the terms of this Order Form shall control.

<u>Snohomish County</u>

Date: ______________________________

Signature: ______________________________

Printed Name: ______________________________

Title: ______________________________

<u>Aspire HR, LLC</u>

Date: ______________________________

Signature: ______________________________

Printed Name: ______________________________

Title: ______________________________