



IT SERVICES CONTRACT

Origami Risk Subscription Agreement

DSHS Contract Number:
2523-67989
 Resulting From Competition
 Number: 2523-881
 Competition Exempt
 Sole Source

This Contract is between the state of Washington Department of Social and Health Services (DSHS) and the Contractor identified below, and is governed by chapter 43.19 and 43.105 RCW.

Program Contract Number:

 Contractor Contract Number:

CONTRACTOR NAME Origami Risk LLC		CONTRACTOR doing business as (DBA)	
CONTRACTOR ADDRESS 222 N. La Salle Street Suite 2100 Chicago, IL 60601-1106		WASHINGTON UNIFORM BUSINESS IDENTIFIER (UBI)	DSHS INDEX NUMBER 249726
CONTRACTOR CONTACT Christian Schiavone	CONTRACTOR TELEPHONE Click here to enter text.	CONTRACTOR FAX	CONTRACTOR E-MAIL ADDRESS cschiavone@origamirisk.com
DSHS ADMINISTRATION Office of the Secretary	DSHS DIVISION Enterprise Risk Management Office	DSHS CONTRACT CODE 8900SC-23	
DSHS CONTACT NAME AND TITLE Jamie Gerken Manager, Contracts Coordination		DSHS CONTACT ADDRESS 1115 Washington St SE Olympia, WA 98501	
DSHS CONTACT TELEPHONE (360)584-8781	DSHS CONTACT FAX Click here to enter text.	DSHS CONTACT E-MAIL ADDRESS jamie.gerken@dshs.wa.gov	
IS THE CONTRACTOR A SUBRECIPIENT FOR PURPOSES OF THIS CONTRACT? No		ASSISTANCE LISTING NUMBER(S)	
CONTRACT START DATE 12/28/2025	CONTRACT END DATE 12/27/2028	CONTRACT MAXIMUM AMOUNT \$810,000.00	
EXHIBITS. The following Exhibits are attached and are incorporated into this Contract by reference: <input checked="" type="checkbox"/> Exhibits (specify): Exhibit A – Data Security Requirements Exhibit; Exhibit B Data Licensing Statement; Exhibit C - Statement of Work (SOW); Exhibit D - Service Level Agreement (SLA).			
The terms and conditions of this Contract are an integration and representation of the final, entire and exclusive understanding between the parties superseding and merging all previous agreements, writings, and communications, oral or otherwise, regarding the subject matter of this Contract. The parties signing below represent that they have read and understand this Contract, and have the authority to execute this Contract.			
CONTRACTOR SIGNATURE 		PRINTED NAME AND TITLE Ryan Dardis - CRO	DATE SIGNED 2025-02-19
DSHS SIGNATURE 		PRINTED NAME AND TITLE Caleb Clark, Contracts Consultant	DATE SIGNED 20FEB2026

DSHS General Terms and Conditions

1. **Definitions.** The words and phrases listed below, as used in this Contract, shall each have the following definitions:
- a. “Central Contracts and Legal Services” means the DSHS central headquarters contracting office, or successor section or office.
 - b. “Confidential Information” or “Data” means information that is exempt from disclosure to the public or other unauthorized persons under RCW 42.56 or other federal or state laws. Confidential Information includes, but is not limited to, Personal Information.
 - c. “Contract” or “Agreement” means the entire written agreement between DSHS and the Contractor, including any Exhibits, documents, or materials incorporated by reference. The parties may execute this contract in multiple counterparts, each of which is deemed an original and all of which constitute only one agreement. E-mail or Facsimile transmission of a signed copy of this contract shall be the same as delivery of an original.
 - d. “CCLS Chief” means the manager, or successor, of Central Contracts and Legal Services or successor section or office.
 - e. “Contractor” means the individual or entity performing services pursuant to this Contract and includes the Contractor’s owners, members, officers, directors, partners, employees, and/or agents, unless otherwise stated in this Contract. For purposes of any permitted Subcontract, “Contractor” includes any Subcontractor and its owners, members, officers, directors, partners, employees, and/or agents.
 - f. “Debarment” means an action taken by a Federal agency or official to exclude a person or business entity from participating in transactions involving certain federal funds.
 - g. “DSHS” or the “Department” means the state of Washington Department of Social and Health Services and its employees and authorized agents.
 - h. “Encrypt” means to encode Confidential Information into a format that can only be read by those possessing a “key;” a password, digital certificate or other mechanism available only to authorized users. Encryption must use a key length of at least 256 bits for symmetric keys, or 2048 bits for asymmetric keys. When a symmetric key is used, the Advanced Encryption Standard (AES) must be used if available.
 - i. “Personal Information” means information identifiable to any person, including, but not limited to, information that relates to a person’s name, health, finances, education, business, use or receipt of governmental services or other activities, addresses, telephone numbers, Social Security Numbers, driver license numbers, other identifying numbers, and any financial identifiers.
 - j. “Physically Secure” means that access is restricted through physical means to authorized individuals only.
 - k. “Program Agreement” means an agreement between the Contractor and DSHS containing special terms and conditions, including a statement of work to be performed by the Contractor and payment to be made by DSHS.
 - l. “RCW” means the Revised Code of Washington. All references in this Contract to RCW chapters or sections shall include any successor, amended, or replacement statute. Pertinent RCW chapters can be accessed at <http://apps.leg.wa.gov/rcw/>.

DSHS General Terms and Conditions

- m. "Regulation" means any federal, state, or local regulation, rule, or ordinance.
- n. "Secured Area" means an area to which only authorized representatives of the entity possessing the Confidential Information have access. Secured Areas may include buildings, rooms or locked storage containers (such as a filing cabinet) within a room, as long as access to the Confidential Information is not available to unauthorized personnel.
- o. "Subcontract" means any separate agreement or contract between the Contractor and an individual or entity ("Subcontractor") to perform all or a portion of the duties and obligations that the Contractor is obligated to perform pursuant to this Contract.
- p. "Tracking" means a record keeping system that identifies when the sender begins delivery of Confidential Information to the authorized and intended recipient, and when the sender receives confirmation of delivery from the authorized and intended recipient of Confidential Information.
- q. "Trusted Systems" include only the following methods of physical delivery: (1) hand-delivery by a person authorized to have access to the Confidential Information with written acknowledgement of receipt; (2) United States Postal Service ("USPS") first class mail, or USPS delivery services that include Tracking, such as Certified Mail, Express Mail or Registered Mail; (3) commercial delivery services (e.g. FedEx, UPS, DHL) which offer tracking and receipt confirmation; and (4) the Washington State Campus mail system. For electronic transmission, the Washington State Governmental Network (SGN) is a Trusted System for communications within that Network.
- r. "WAC" means the Washington Administrative Code. All references in this Contract to WAC chapters or sections shall include any successor, amended, or replacement regulation. Pertinent WAC chapters or sections can be accessed at <http://apps.leg.wa.gov/wac/>.

2. Amendment. This Contract may only be modified by a written amendment signed by both parties. Only personnel authorized to bind each of the parties may sign an amendment.

3. Assignment. The Contractor shall not assign this Contract or any Program Agreement to a third party without the prior written consent of DSHS except as permitted under the Special Terms and Conditions.

4. Billing Limitations.

- a. DSHS shall pay the Contractor only for authorized services provided in accordance with this Contract.
- b. DSHS shall not pay any claims for payment for services submitted more than twelve (12) months after the calendar month in which the services were performed.
- c. The Contractor shall not bill and DSHS shall not pay for services performed under this Contract, if the Contractor has charged or will charge another agency of the state of Washington or any other party for the same services.

5. Compliance with Applicable Law and Washington State Requirements.

- a. **Applicable Law.** Throughout the performance of this Agreement, Contractor shall comply with all federal, state, and local laws, regulations, and executive orders to the extent they are applicable to Contractor generally and without consideration of DSHS's particular use of the Service.
- b. **Civil Rights and Nondiscrimination.** Contractor shall comply with all federal and state civil rights

DSHS General Terms and Conditions

and nondiscrimination laws, regulations, and executive orders to the extent they are applicable to this Agreement, including, but not limited to, and as amended, Titles VI and VII of the Civil Rights Act of 1964; Sections 503 and 504 of the Rehabilitation Act of 1973; the Americans with Disabilities Act (ADA); Executive Order 11246; the Health Insurance Portability and Accountability Act of 1996 (HIPAA); the Age Discrimination in Employment Act of 1967, the Age Discrimination Act of 1975, the Vietnam Era Veterans' Readjustment Assistance Act of 1974, and Chapter 49.60 of the Revised Code of Washington, Washington's Law Against Discrimination. These laws, regulations and executive orders are incorporated by reference herein to the extent that they are applicable to Contractor generally and required by law to be so incorporated.

In the event of the Contractor's noncompliance following notice and an opportunity to cure, or refusal to comply with any applicable nondiscrimination laws, regulations, and executive orders, this Agreement may be rescinded, canceled, or terminated in whole or in part.

c. **Nondiscrimination.**

(1) **Nondiscrimination Requirement.** During the term of this Contract, Contractor, including any subcontractor, shall not discriminate on the bases enumerated at RCW 49.60.530(3). In addition, Contractor, including any subcontractor, shall give written notice of this nondiscrimination requirement to any labor organizations with which Contractor, or subcontractor, has a collective bargaining or other agreement.

(2) **Obligation to Cooperate.** Contractor, including any subcontractor, shall cooperate and comply with any Washington state agency investigation regarding any allegation that Contractor, including any subcontractor, has engaged in discrimination prohibited by this Contract pursuant to RCW 49.60.530(3).

d. **Certification Regarding Russian Government Contracts and/or Investments.** The Contractor, by signature to this Contract, certifies that the Contractor is not presently an agency of the Russian government, an entity which is Russian-state owned to any extent, or an entity sanctioned by the United States government in response to Russia's invasion of Ukraine. The Contractor also agrees to include the above certification in any and all Subcontracts into which it enters. The Contractor shall immediately notify DSHS if, during the term of this Contract, Contractor no longer complies with this certification. DSHS may immediately terminate this Contract by providing Contractor written notice if Contractor does not comply with this certification during the term hereof. This is a requirement under Directive of the Governor 22-03.

e. **Reporting Certain Requests from the Federal Government or Law Enforcement Entities.** Contractor shall report to DSHS, within 72 hours, all non-routine requests from a law enforcement authority or federal agency for any of the following to the extent such requests concern DSHS Data : (i) health care information, as defined in RCW 70.02.010, (ii) program eligibility information for individuals, or (iii) information that may identify a health care provider's or facilities delivery of health care services to noncitizens, or delivery of protected health care services as defined in RCW 7.115.010 (gender affirming treatment and reproductive health care services that are lawful in the state of Washington). This is a requirement under Chapter 424, Laws of 2025.

Examples of non-routine requests include surveys, requests for disclosure, subpoenas, and other mechanisms for obtaining data or information. Additionally, search warrants or other requests for disclosure are considered non-routine if they expressly seek data or information about services to noncitizens, gender affirming services, or reproductive health care services.

6. **Confidentiality.**

DSHS General Terms and Conditions

- a. The Contractor shall not use, publish, transfer, sell or otherwise disclose any Confidential Information gained by reason of this Contract for any purpose that is not directly connected with Contractor's performance of the services contemplated hereunder, except:
 - (1) as provided by law; or,
 - (2) in the case of Personal Information, with the prior written consent of the person or personal representative of the person who is the subject of the Personal Information.
- b. The Contractor shall protect and maintain all Confidential Information gained by reason of this Contract against unauthorized use, access, disclosure, modification or loss. This duty requires the Contractor to employ industry standard security measures, which include restricting access to the Confidential Information by:
 - (1) Allowing access only to staff that have an authorized business requirement to view the Confidential Information.
 - (2) Physically Securing any computers, documents, or other media containing the Confidential Information.
 - (3) Ensure the security of Confidential Information transmitted via fax (facsimile) by:
 - (a) Verifying the recipient phone number to prevent accidental transmittal of Confidential Information to unauthorized persons.
 - (b) Communicating with the intended recipient before transmission to ensure that the fax will be received only by an authorized person.
 - (c) Verifying after transmittal that the fax was received by the intended recipient.
 - (4) Send paper documents containing Confidential Information via a Trusted System.
 - (5) Following the requirements of the DSHS Data Security Requirements Exhibit, if attached to this contract.
- c. Upon request by DSHS within 30 (thirty) days of the Contract term, or when no longer needed with the exception of DSHS Data, Confidential Information shall be returned to DSHS or Contractor shall certify in writing that they employed a DSHS approved method to destroy the information. Contractor may obtain information regarding approved destruction methods from the DSHS Contact identified on the cover page of this Contract.
- d. Paper documents with Confidential Information may be recycled through a contracted firm, provided the contract with the recycler specifies that the confidentiality of information will be protected, and the information destroyed through the recycling process. Paper documents containing Confidential Information requiring special handling (e.g. protected health information) must be destroyed on-site through shredding, pulping, or incineration.
- e. Notification of Compromise or Potential Compromise. The compromise or potential compromise of Confidential Information must be reported to the DSHS Contact designated on the contract within seventy-two (72) hours of discovery. Contractor must also take actions to mitigate the risk of loss and comply with any notification or other requirements imposed on Contractor by law.

DSHS General Terms and Conditions

7. **Digital Accessibility.** If this Contract includes the acquisition, procurement, development, modification or enhancement of public-facing digital content or tools; including websites, applications, and media (Covered Technology), the following requirements shall apply:
- All Covered Technology under this Contract must meet Level AA compliances with Web Content Accessibility Guidelines (WCAG) 2.1.
 - Contractor shall validate compliance with this requirement through either a third-party accessibility validation report, a Vendor Product Accessibility Template (VPAT), or compliance review documentation.
 - Should the Covered Technology under this Contract fails to meet the required compliance level, the Contractor shall certify to DSHS in writing that Contractor has created or is in the process of creating a remediation plan addressing all issues identified to the DSHS Contact identified on the cover page of this Contract. Contractor's failure to engage in continual commercially reasonable efforts to remediate all issues identified shall be considered a material breach of this Contract.
8. **Debarment Certification.** The Contractor, by signature to this Contract, certifies that the Contractor is not presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded by any Federal department or agency from participating in transactions (Debarred). The Contractor also agrees to include the above requirement in any and all Subcontracts into which it enters. The Contractor shall immediately notify DSHS if, during the term of this Contract, Contractor becomes Debarred. DSHS may immediately terminate this Contract by providing Contractor written notice if Contractor becomes Debarred during the term hereof.
9. **E-Signature and Records.** An electronic signature or electronic record of this Contract or any other ancillary agreement shall be deemed to have the same legal effect as delivery of an original executed copy of this Contract or such other ancillary agreement for all purposes.
10. **Governing Law and Venue.** This Contract shall be construed and interpreted in accordance with the laws of the state of Washington and the venue of any action brought hereunder shall be in Superior Court for Thurston County.
11. **Independent Contractor.** The parties intend that an independent contractor relationship will be created by this Contract. The Contractor and his or her employees or agents performing under this Contract are not employees or agents of the Department. The Contractor, his or her employees, or agents performing under this Contract will not hold himself/herself out as, nor claim to be, an officer or employee of the Department by reason hereof, nor will the Contractor, his or her employees, or agent make any claim of right, privilege or benefit that would accrue to such officer or employee.
12. **Inspection.** No more than once in any 12 month period, the Contractor shall, at no cost, provide DSHS and the Office of the State Auditor with copies of Contractor's records necessary to confirm the accuracy of Contractor's invoices. These inspection rights shall survive for six (6) years following this Contract's termination or expiration.
13. **Maintenance of Records.** The Contractor shall maintain records relating to this Contract and the performance of the services described herein. The records include, but are not limited to, accounting procedures and practices, which sufficiently and properly reflect all direct and indirect costs of any nature expended in the performance of this Contract. All records and other material relevant to this Contract shall be retained for six (6) years after expiration or termination of this Contract.

Without agreeing that litigation or claims are legally authorized, if any litigation, claim, or audit is started

DSHS General Terms and Conditions

before the expiration of the six (6) year period, the records shall be retained until all litigation, claims, or audit findings involving the records have been resolved.

14. **Order of Precedence.** In the event of any inconsistency or conflict between the General Terms and Conditions and the Special Terms and Conditions of this Contract or any Program Agreement, the inconsistency or conflict shall be resolved by giving precedence to these General Terms and Conditions. Terms or conditions that are more restrictive, specific, or particular than those contained in the General Terms and Conditions shall not be construed as being inconsistent or in conflict.
15. **Severability.** If any term or condition of this Contract is held invalid by any court, the remainder of the Contract remains valid and in full force and effect.
16. **Survivability.** The terms and conditions contained in this Contract or any Program Agreement which, by their sense and context, are intended to survive the expiration or termination of the particular agreement shall survive. Surviving terms include, but are not limited to: Billing Limitations; Confidentiality, Disputes; Indemnification and Hold Harmless, Inspection, Maintenance of Records, Notice of Overpayment, Ownership of Material, Termination for Default, Termination Procedure, and Treatment of Property.
17. **Contract Renegotiation, Suspension, or Termination Due to Change in Funding.**

If the funds DSHS relied upon to establish this Contract or Program Agreement are withdrawn, reduced or limited, or if additional or modified conditions are placed on such funding, after the effective date of this Contract but prior to the normal completion of this Contract or Program Agreement:

- a. The Contract or Program Agreement may be renegotiated under the revised funding conditions.
- b. DSHS's discretion, DSHS may give notice to Contractor to suspend performance when DSHS determines that there is reasonable likelihood that the funding insufficiency may be resolved in a timeframe that would allow Contractor's performance to be resumed prior to the normal completion date of this contract.
- c. During the period of suspension of performance, each party will inform the other of any conditions that may reasonably affect the potential for resumption of performance.
- d. When DSHS determines that the funding insufficiency is resolved, it will give Contractor written notice to resume performance. Upon the receipt of this notice, Contractor will provide written notice to DSHS informing DSHS whether it can resume performance and, if so, the date of resumption. For purposes of this subsection, "written notice" may include email.
- e. If the Contractor's proposed resumption date is not acceptable to DSHS and an acceptable date cannot be negotiated, DSHS may terminate the contract by giving written notice to Contractor. The parties agree that the Contract will be terminated retroactive to the date of the notice of suspension. DSHS shall be liable only for payment in accordance with the terms of this Contract for services rendered prior to the retroactive date of termination.
- f. DSHS may terminate this Contract effective as of the date funds expire by providing written notice to the Contractor. The termination shall be effective on the date specified in the termination notice. DSHS shall be liable only for payment in accordance with the terms of this Contract for services rendered prior to the effective date of termination. No penalty shall accrue to DSHS in the event the termination option in this section is exercised.

DSHS General Terms and Conditions

18. **Waiver.** Waiver of any breach or default on any occasion shall not be deemed to be a waiver of any subsequent breach or default. Any waiver shall not be construed to be a modification of the terms and conditions of this Contract. Only the CCLS Chief or designee has the authority to waive any term or condition of this Contract on behalf of DSHS.

Additional General Terms and Conditions – Information Technology Service Contracts:

19. **Advance Payment.** Intentionally omitted.
20. **Commencement of Work.** No work shall be performed by the Contractor until the Contract is executed by the Contractor and DSHS and received by DSHS.
21. **Construction.** The language in this Contract shall be interpreted as to its fair meaning and not strictly for or against any party. Any rule of construction to the effect that ambiguities are to be resolved against the drafting party shall not apply in interpreting this Contract.
22. **Contractor Certification Regarding Ethics.** The Contractor certifies that the Contractor is now, and shall remain, in compliance with Chapter 42.52 RCW, Ethics in Public Service, throughout the term of this Contract.
23. **Contractor Commitments, Warranties and Representations.** Intentionally omitted.
24. **Disputes.**
- a. In the event a bona fide dispute concerning a question of fact arises between DSHS and the Contractor that cannot be resolved between the parties, either party may initiate the dispute resolution procedure provided herein.
 - b. The initiating party shall reduce its description of the dispute to writing and deliver it to the responding party. The responding party shall respond in writing within three (3) Business Days (which shall mean Monday through Friday, 8:00 a.m. to 5:00 p.m., Pacific Time, except for holidays observed by the state of Washington). The initiating party shall have three (3) Business Days to review the response. If after this review a resolution cannot be reached, both parties shall have three (3) Business Days to negotiate in good faith to resolve the dispute.
 - (1) If the dispute cannot be resolved after three (3) Business Days, a dispute resolution panel may be requested in writing by either party who shall also identify the first panel member. Within three (3) Business Days of receipt of the request, the other party will designate a panel member. Those two panel members will appoint a third individual to the dispute resolution panel within the next three (3) Business Days.
 - (2) The dispute resolution panel will review the written descriptions of the dispute, gather additional information as needed, and render a written decision on the dispute in the shortest practical time.
 - (3) Each party shall bear the cost for its panel member and share equally the cost of the third panel member.
 - c. Unless irreparable harm will result, the parties agree that this dispute process shall precede any action in a judicial or quasi-judicial tribunal.
 - d. Both parties agree to exercise good faith in dispute resolution and to settle disputes prior to using a

DSHS General Terms and Conditions

dispute resolution panel whenever possible.

- e. Except to the extent that disclosure is required by applicable law or court order, all negotiations pursuant to this clause are confidential and shall be treated by the parties as statements made in compromise negotiations for purposes of the rules of evidence.
- f. DSHS and the Contractor agree that, the existence of a dispute notwithstanding, they will continue without delay to carry out all their respective responsibilities under this Contract that are not affected by the dispute.
- g. If the subject of the dispute is the amount due and payable by DSHS for services being provided by the Contractor, the Contractor shall continue providing services pending resolution of the dispute provided DSHS pays the Contractor the amount DSHS, in good faith, believes is due and payable, and may withhold the difference between such amount and the amount the Contractor, in good faith, believes is due and payable.

25. Health and Safety. The Contractor shall perform any and all of its obligations under this Contract in a manner that does not compromise the health or safety of any DSHS client with whom the Contractor has physical contact.

26. Industrial Insurance Coverage. The Contractor shall comply with the provisions of Title 51 RCW, Industrial Insurance. If the Contractor fails to provide industrial insurance coverage or fails to pay premiums or penalties on behalf of its employees, as may be required by law, Agency may collect from the Contractor the full amount payable to the Industrial Insurance accident fund. The Agency may deduct the amount owed by the Contractor to the accident fund from the amount payable to the Contractor by the Agency under this contract, and transmit the deducted amount to the Department of Labor and Industries, (L&I) Division of Insurance Services. This provision does not waive any of L&I's rights to collect from the Contractor.

27. Limitation of Liability.

- a. The following are not considered consequential, incidental, indirect, or special damages as the term is used in the Special Terms and Conditions.
 - (1) Claims for attorney's fees and other litigation costs DSHS becomes entitled to recover as a prevailing party in an action;
 - (2) Claims for physical damage to real or tangible property;
 - (3) Claims arising from reckless or intentional misconduct;
- b. Neither party shall be liable for personal injury to the other party or damage to the other party's tangible property except personal injury or damage to tangible property proximately caused by such party's respective fault or negligence.

28. Notice of Overpayment. If the Contractor receives a Contractor overpayment notice or a letter communicating the existence of an overpayment from DSHS, the Contractor may protest the overpayment determination by requesting an adjudicative proceeding. The Contractor's request for an adjudicative proceeding must:

- a. Be *received* by the Office of Financial Recovery (OFR) at Post Office Box 9501, Olympia, Washington 98507-9501, within twenty-eight (28) calendar days of service of the notice;

DSHS General Terms and Conditions

- b. Be sent by certified mail (return receipt) or other manner that proves OFR received the request;
- c. Include a statement as to why the Contractor thinks the notice is incorrect; and
- d. Include a copy of the overpayment notice.

Timely and complete requests will be scheduled for a formal hearing by the Office of Administrative Hearings. The Contractor may be offered a pre-hearing or alternative dispute resolution conference in an attempt to resolve the overpayment dispute prior to the hearing.

Failure to provide OFR with a written request for a hearing within twenty-eight (28) days of service of a Contractor overpayment notice or other overpayment letter will result in an overpayment debt against the Contractor. DSHS may charge the Contractor interest and any costs associated with the collection of this overpayment. DSHS may collect an overpayment debt through lien, foreclosure, seizure and sale of the Contractor's real or personal property; order to withhold and deliver; or any other collection action available to DSHS to satisfy the overpayment debt.

- 29. Public Records Act.** The Contractor acknowledges that DSHS is subject to the Public Records Act (Chapter 42.56 RCW) and that this Contract is a public record as defined in Chapter 42.56 RCW. Any specific information that is claimed by the Contractor to be Proprietary Information must be clearly identified as such by the Contractor. "Proprietary Information" means information owned by the Contractor to which the Contractor claims a protectable interest under law. Proprietary Information includes, but is not limited to, information protected by copyright, patent, trademark, or trade secret laws. To the extent consistent with Chapter 42.56 RCW, DSHS will maintain the confidentiality of all such information marked Proprietary Information. If a public disclosure request is made to view the Contractor's Proprietary Information, DSHS will notify the Contractor of the request and of the date that such records will be released to the requester unless the Contractor obtains a court order from a court of competent jurisdiction enjoining that disclosure. If the Contractor fails to obtain the court order enjoining disclosure, DSHS will release the requested information on the date specified.
- 30. Publicity.** The Contractor shall not name DSHS as a customer, nor use any information related to this Contract, in any format or media, in any Contractor's advertising or publicity without prior written consent from DSHS.
- 31. Site Security.** While providing services at a DSHS location, the Contractor, its agents, employees, or Subcontractors shall conform in all respects with physical, fire, or other security regulations specific to the DSHS location.
- 32. Subcontracting.** Except as otherwise provided in this Contract, the Contractor shall not Subcontract any of the contracted services without the prior written approval of DSHS. Contractor is responsible to ensure that all terms, conditions, assurances and certifications set forth in this Contract are included in any and all Subcontracts. Any failure of Contractor or its Subcontractors to perform the obligations of this Contract shall not discharge the Contractor from its obligations hereunder or diminish DSHS' rights or remedies available under this Contract.
- 33. Termination for Default.** Either party may terminate this Contract if the other party breaches a material term of this Contract and fails to cure such breach within thirty (30) days after receiving written notice describing the breach in reasonable detail. If the breaching party does not cure the breach within the cure period, termination shall take effect immediately upon written notice from the non-breaching party.
- 34. Termination or Expiration Procedure.** The following terms and conditions apply upon Contract

DSHS General Terms and Conditions

termination or expiration:

- a. The Contractor shall cease to perform, and DSHS shall cease to access, any services required by this Contract as of the effective date of termination or expiration.
- b. Upon written request from DSHS within 30 days of termination or expiration of the Contract, the Contractor shall deliver to the DSHS contact named on page one of this Contract, or to his or her successor, all DSHS property in the Contractor's possession (and with respect to DSHS Data, in accordance with Section 4(b) of the Special Terms and Conditions).
- c. DSHS shall be liable only for payment required under the terms of this Contract for service rendered up to the effective date of termination or expiration.
- d. The rights and remedies provided to DSHS in this Section are in addition to any other rights and remedies provided at law, in equity, and/or under this Contract, including consequential and incidental damages.

35. Treatment of Property. All tangible property purchased or furnished by DSHS for use by the Contractor during this Contract term shall remain with DSHS. Title to all tangible property purchased or furnished by the Contractor for which the Contractor is entitled to reimbursement by DSHS under this Contract shall pass to and vest in DSHS. The Contractor shall protect, maintain, and insure all DSHS tangible property in its possession against loss or damage and shall return DSHS tangible property to DSHS upon Contract termination or expiration.

36. Taxes

- a. Where required by statute or regulation, Contractor shall pay for and maintain in current status all taxes that are necessary for Contract performance. DSHS will pay sales or use taxes, if any, imposed on the services and materials acquired hereunder. Contractor must pay all other taxes including without limitation Washington Business and Occupation Tax, other taxes based on Contractor's income or gross receipts, or personal property taxes levied or assessed on Contractor's personal property. DSHS, as an agency of Washington State government, is exempt from property tax.
- b. Contractor shall complete registration with the Washington State Department of Revenue and be responsible for payment of all taxes due on payments made under this Contract in accordance with the requirements of [Title 82 RCW](#) and [Title 458 WAC](#). Out-of-state Contractors must contact the Department of Revenue to determine whether they meet criteria to register and establish an account with the Department of Revenue. Refer to WAC 458-20-101 (Tax registration and tax reporting) and call the Department of Revenue at 800-647-7706 for additional information. When out-of-state Contractors are not required to collect and remit sales tax, DSHS shall be responsible for paying use tax, if applicable, directly to the Department of Revenue.
- c. All payments accrued on account of payroll taxes, unemployment contributions, any other taxes, insurance, or other expenses for Contractor or Contractor's staff shall be Contractor's sole responsibility.

37. Preventing Disruption of Adult Care, Mental Health, Addiction, Disability Support, or Youth Services Due to Labor Management Disputes and Employee Unrest.

Washington law requires that all services, direct or ancillary, for adult care, mental health, addiction, disability support, and youth services, be warranted by the Contractor providing those services against

DSHS General Terms and Conditions

disruption. Contractor and DSHS agree that disruptions to these services such as strikes, walk-offs, sick-ins, slowdowns, or any other such action designed to pressure Contractor's management to meet labor, workforce, or subcontractor demands ("Economic or Industrial Action") are covered under this warranty.

If this Contract is expanded at any time to include adult care, mental health, addiction, disability support, or youth services, Contractor agrees to execute and maintain one or more of the following mandatory contractual commitments through the life of the Contract, to the extent required by law:

- a. An agreement between the Contractor and any exclusive representative labor organization representing the employees performing the contracted services. This agreement must contain a provision prohibiting Economic or Industrial Action on the part of all parties. This agreement must also include a process for the resolution of disputes between them; or
- b. An agreement between the Contractor and any labor organization seeking to represent the employees performing the contracted services. This agreement must contain a provision prohibiting the parties from causing, promoting, or encouraging Economic or Industrial Action, or other disruptive activity. This agreement must also include a process for resolution of disputes between parties.

Contractor must notify DSHS if it is unable to form a compliant agreement with a labor organization within 30 days of executing such expansion as contemplated above to this Contract.

If services under this Contract are interrupted due to Contractor's failure to maintain one or more of the required contractual commitments listed above, DSHS may immediately terminate, suspend, or revoke this Contract for default.

38. Mandatory Individual Arbitration and Class or Collective Action Waiver as a Condition of Employment.

- a. "Mandatory Individual Arbitration Clause" or "Class or Collective Action Waiver" means an arbitration clause or waiver in an employment contract which precludes Contractor's employees from resolving employment disputes with their employer through class or collective proceedings in federal court. Instead, employees must bring individualized arbitration proceedings against their employer to resolve any employment disputes.
- b. The Contractor, by signature to this Contract, certifies that the Contractor does not require Contractor's employees to agree to, as a condition of employment, a Mandatory Individual Arbitration Clause or Class or Collective Action Waiver.
- c. Contractor must notify DSHS within ten (10) business days if, during the term of this Contract, Contractor requires Contractor's employees to agree to, as a condition of employment, a Mandatory Individual Arbitration Clause or Class or Collective Action Waiver.
- d. If Contractor, during the term of this contract, requires Contractor's employees to agree to, as a condition of employment, a Mandatory Individual Arbitration Clause or Class or Collective Action Waiver, Contractor shall notify DSHS within 30 days of such change.

HIPAA Compliance

Preamble: This section of the Contract is the Business Associate Agreement as required by HIPAA.

DSHS General Terms and Conditions

39. Definitions

- a. "Business Associate," as used in this Contract, means the "Contractor" and generally has the same meaning as the term "business associate" at 45 CFR 160.103. Any reference to Business Associate in this Contract includes Business Associate's employees, agents, officers, Subcontractors, third party contractors, volunteers, or directors.
- b. "Business Associate Agreement" means this HIPAA Compliance section of the Contract and includes the Business Associate provisions required by the U.S. Department of Health and Human Services, Office for Civil Rights.
- c. "Breach" means the acquisition, access, use, or disclosure of Protected Health Information in a manner not permitted under the HIPAA Privacy Rule which compromises the security or privacy of the Protected Health Information, with the exclusions and exceptions listed in 45 CFR 164.402.
- d. "Covered Entity" means DSHS, a Covered Entity as defined at 45 CFR 160.103, in its conduct of covered functions by its health care components.
- e. "Designated Record Set" means a group of records maintained by or for a Covered Entity, that is: the medical and billing records about Individuals maintained by or for a covered health care provider; the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or Used in whole or part by or for the Covered Entity to make decisions about Individuals.
- f. "Electronic Protected Health Information (EPHI)" means Protected Health Information that is transmitted by electronic media or maintained in any medium described in the definition of electronic media at 45 CFR 160.103.
- g. "HIPAA" means the Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191, as modified by the American Recovery and Reinvestment Act of 2009 ("ARRA"), Sec. 13400 – 13424, H.R. 1 (2009) (HITECH Act).
- h. "HIPAA Rules" means the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Parts 160 and Part 164.
- i. "Individual(s)" means the person(s) who is the subject of PHI and includes a person who qualifies as a personal representative in accordance with 45 CFR 164.502(g).
- j. "Minimum Necessary" means the least amount of PHI necessary to accomplish the purpose for which the PHI is needed.
- k. "Protected Health Information (PHI)" means individually identifiable health information created, received, maintained or transmitted by Business Associate on behalf of a health care component of the Covered Entity that relates to the provision of health care to an Individual; the past, present, or future physical or mental health or condition of an Individual; or the past, present, or future payment for provision of health care to an Individual. 45 CFR 160.103. PHI includes demographic information that identifies the Individual or about which there is reasonable basis to believe can be used to identify the Individual. 45 CFR 160.103. PHI is information transmitted or held in any form or medium and includes EPHI. 45 CFR 160.103. PHI does not include education records covered by the Family Educational Rights and Privacy Act, as amended, 20 USCA 1232g(a)(4)(B)(iv) or employment records held by a Covered Entity in its role as employer. Protected Health Information or PHI as used herein is limited to that information contained within DSHS Data.

DSHS General Terms and Conditions

- l. "Security Incident" means the successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations in an information system.
- m. "Subcontractor" as used in this HIPAA Compliance section of the Contract (in addition to its definition in the General Terms and Conditions) means a Business Associate that creates, receives, maintains, or transmits Protected Health Information on behalf of another Business Associate.
- n. "Use" includes the sharing, employment, application, utilization, examination, or analysis, of PHI within an entity that maintains such information.

- 40. Compliance.** Business Associate shall perform all Contract duties, activities and tasks in compliance with HIPAA, the HIPAA Rules, and all attendant regulations as promulgated by the U.S. Department of Health and Human Services, Office of Civil Rights.
- 41. Use and Disclosure of PHI.** Business Associate is limited to the following permitted and required uses or disclosures of PHI:
- a. **Duty to Protect PHI.** Business Associate shall protect PHI from, and shall use appropriate safeguards, and comply with Subpart C of 45 CFR Part 164 (Security Standards for the Protection of Electronic Protected Health Information) with respect to EPHI, to prevent the unauthorized Use or disclosure of PHI other than as provided for in this Contract or as required by law, for as long as the PHI is within its possession and control, even after the termination or expiration of this Contract.
 - b. **Minimum Necessary Standard.** Business Associate shall apply the HIPAA Minimum Necessary standard to any Use or disclosure of PHI necessary to achieve the purposes of this Contract. See 45 CFR 164.514 (d)(2) through (d)(5).
 - c. **Disclosure as Part of the Provision of Services.** Business Associate shall only Use or disclose PHI as necessary to perform the services specified in this Contract or as required by law, and shall not Use or disclose such PHI in any manner that would violate Subpart E of 45 CFR Part 164 (Privacy of Individually Identifiable Health Information) if done by Covered Entity, except for the specific uses and disclosures set forth below.
 - d. **Use for Proper Management and Administration.** Business Associate may Use PHI for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.
 - e. **Disclosure for Proper Management and Administration.** Business Associate may disclose PHI for the proper management and administration of Business Associate or to carry out the legal responsibilities of the Business Associate, provided the disclosures are required by law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that the information will remain confidential and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been Breached.
 - f. **Impermissible Use or Disclosure of PHI.** Business Associate shall report to DSHS in writing all Uses or disclosures of PHI not provided for by this Contract within seven (7) business days of becoming aware of the unauthorized Use or disclosure of PHI, three (3) business days for Breaches of unsecured PHI, as required at 45 CFR 164.410 (Notification by a Business Associate), as well as any Security Incident of which it becomes aware. Upon request by DSHS, Business Associate shall mitigate, to the extent practicable, any harmful effect resulting from the impermissible Use or

DSHS General Terms and Conditions

disclosure.

- g. Failure to Cure. If DSHS learns of a pattern or practice of the Business Associate that constitutes a violation of the Business Associate's obligations under the terms of this Contract and reasonable steps by DSHS do not end the violation, DSHS shall terminate this Contract, if feasible. In addition, If Business Associate learns of a pattern or practice of its Subcontractors that constitutes a violation of the Business Associate's obligations under the terms of their contract and reasonable steps by the Business Associate do not end the violation, Business Associate shall terminate the Subcontract, if feasible.
- h. Termination for Cause. Business Associate authorizes termination of this Contract by DSHS, if DSHS notifies Business Associate in writing containing sufficient details that Business Associate has violated a material term of this Business Associate Agreement and Business Associate fails to cure such violation within ten (10) days. DSHS may, at its sole option, offer Business Associate additional time to cure such violation of this Business Associate Agreement before exercising a termination for cause.
- i. Consent to Audit. Business Associate shall give reasonable access to PHI, its internal practices, records, books, documents, electronic data and/or all other business information received from, or created or received by Business Associate on behalf of DSHS, to the Secretary of DHHS for use in determining compliance with HIPAA privacy requirements.
- j. Obligations of Business Associate Upon Expiration or Termination. Upon expiration or termination of this Contract for any reason, with respect to PHI received from DSHS, or created, maintained, or received by Business Associate, or any Subcontractors, on behalf of DSHS, Business Associate shall:
 - (1) Retain only that PHI which is necessary for Business Associate to continue its proper management and administration or to carry out its legal responsibilities;
 - (2) In accordance with Section 4(b) of the Special Terms and Conditions, return to DSHS or destroy the remaining PHI that the Business Associate or any Subcontractors still maintain in any form;
 - (3) Continue to use industry standard safeguards and comply with Subpart C of 45 CFR Part 164 (Security Standards for the Protection of Electronic Protected Health Information) with respect to Electronic Protected Health Information to prevent Use or disclosure of the PHI, other than as provided for in this Section, for as long as Business Associate or any Subcontractors retain the PHI;
 - (4) Not Use or disclose the PHI retained by Business Associate or any Subcontractors other than for the purposes for which such PHI was retained and subject to the same conditions set out in the "Use and Disclosure of PHI" section of this Contract which applied prior to termination; and
 - (5) Return to DSHS or destroy the PHI retained by Business Associate, or any Subcontractors, when it is no longer needed by Business Associate for its proper management and administration or to carry out its legal responsibilities.
- k. Survival. The obligations of the Business Associate under this section shall survive the termination or expiration of this Contract.

42. Individual Rights.

DSHS General Terms and Conditions

a. Accounting of Disclosures.

- (1) Business Associate shall document all disclosures, except those disclosures that are exempt under 45 CFR 164.528, of PHI and information related to such disclosures.
- (2) Within fifteen (15) business days of a request from DSHS, Business Associate shall make available to DSHS the information in Business Associate's possession that is necessary for DSHS to respond in a timely manner to a request for an accounting of disclosures of PHI by the Business Associate. See 45 CFR 164.504(e)(2)(ii)(G) and 164.528(b)(1).
- (3) In response to a request made directly to the Business Associate by an Individual, Business Associate shall notify DSHS, in a timely manner and in accordance with HIPAA and the HIPAA Rules (and in no event more than fifteen (15) days), to requests by Individuals for an accounting of disclosures of PHI.
- (4) Business Associate record keeping procedures shall be sufficient to respond to a request for an accounting under this section for the six (6) years prior to the date on which the accounting was requested.

b. Access

- (1) Business Associate shall make available to DSHS PHI that it holds that is part of a Designated Record Set when requested by DSHS or the Individual as necessary to satisfy DSHS's obligations under 45 CFR 164.524 (Access of Individuals to Protected Health Information).
- (2) When the request is made by the Individual to the Business Associate, the Business Associate shall provide the records to DSHS within ten (10) business days.

c. Amendment.

- (1) If DSHS amends, in whole or in part, a record or PHI contained in an Individual's Designated Record Set and DSHS has previously provided the PHI or record that is the subject of the amendment to Business Associate, then DSHS will inform Business Associate of the amendment pursuant to 45 CFR 164.526(c)(3) (Amendment of Protected Health Information).
- (2) Business Associate shall make any amendments to PHI in a Designated Record Set as directed by DSHS or as necessary to satisfy DSHS's obligations under 45 CFR 164.526 (Amendment of Protected Health Information).

43. Subcontracts and other Third Party Agreements. In accordance with 45 CFR 164.502(e)(1)(ii), 164.504(e)(1)(i), and 164.308(b)(2), Business Associate shall ensure that any agents, Subcontractors, independent contractors or other third parties that create, receive, maintain, or transmit PHI on Business Associate's behalf, enter into a written contract that contains the same terms, restrictions, requirements, and conditions as the HIPAA compliance provisions in this Contract with respect to such PHI. The same provisions must also be included in any contracts by a Business Associate's Subcontractor with its own business associates as required by 45 CFR 164.314(a)(2)(b) and 164.504(e)(5) .

44. Obligations. To the extent the Business Associate is to carry out one or more of DSHS's obligation(s) under Subpart E of 45 CFR Part 164 (Privacy of Individually Identifiable Health Information), Business Associate shall comply with all requirements that would apply to DSHS in the performance of such obligation(s).

DSHS General Terms and Conditions

- 45. Liability.** Within fifteen (15) business days, Business Associate must notify DSHS of any complaint, enforcement or compliance action initiated by the Office for Civil Rights based on an allegation of violation of the HIPAA Rules and must inform DSHS of the outcome of that action. Business Associate bears all responsibility for any penalties, fines or sanctions imposed against the Business Associate for violations of the HIPAA Rules and for any imposed against its Subcontractors or agents for which it is found liable.
- 46. Breach Notification.**
- a. Within a minimum of fifteen (15) Business Days, Business Associate agrees to notify the Covered Entity of any use or disclosure of PHI not provided for by this Business Associate Agreement of which it becomes aware, including a breach of unsecured PHI of which it becomes aware as required under 45 C.F.R. § 164.410, and any security incident involving PHI (as defined in 45 CFR § 164.304) of which it becomes aware. Business Associate shall cooperate with the Covered Entity as reasonably requested by the Covered Entity in investigating any non-permitted use or disclosure..
 - b. Business Associate will notify DSHS within three (3) business day by telephone and in writing of any acquisition, access, Use or disclosure of PHI not allowed by the provisions of this Contract or not authorized by HIPAA Rules or required by law of which it becomes aware which materially compromises the security or privacy of the Protected Health Information as defined in 45 CFR 164.402 (Definitions).
 - c. Business Associate will notify the DSHS Contact shown on the cover page of this Contract within three (3) business day by telephone or e-mail of any Breach of security resulting in the unpermitted acquisition, access, or disclosure of PHI. Business Associate will follow telephone or e-mail notification with a faxed or other written explanation of the Breach, to include the following: date and time of the Breach, date Breach was discovered, location and nature of the PHI, type of Breach, origination and destination of PHI, reasonably detailed description of the Breach, anticipated mitigation steps, and the name, address, telephone number, fax number, and e-mail of the individual who is responsible as the primary point of contact. Business Associate will address communications to the DSHS Contact. Business Associate will coordinate and cooperate with DSHS to provide information reasonably requested by DSHS, including advance copies of any notifications Business Associate is required to send by law for DSHS review before disseminating and verification of the dates notifications were sent.
- 47. Miscellaneous Provisions.**
- a. Regulatory References. A reference in this Contract to a section in the HIPAA Rules means the section as in effect or amended.
 - b. Interpretation. Any ambiguity in this Contract shall be interpreted to permit compliance with the HIPAA Rules.

Special Terms and Conditions

1. **Definitions.** The words and phrases listed below, as used in this Contract, shall each have the following definitions:
 - a. "Affiliate" means, with respect to a party, its parent company and subsidiaries and/or controlled corporations or entities which are directly or indirectly controlled by, or under common control with, such party.
 - b. "Customizations" means specifically modified reports, dashboard panels, or other configurations, features or modules of the Service customized for DSHS.
 - c. "Documentation" means all user guides, videos, embedded help text, and other reference materials generally furnished with respect to the Service, whether in printed or electronic format.
 - d. "DSHS Data" means the data provided or inputted by or on behalf of DSHS or any User or Affiliate of DSHS for use with the Service.
 - e. "DSHS Party" means DSHS and each of its Affiliates and Users.
 - f. "Fees" means the fees payable pursuant to this Contract as set forth in any Statement of Work.
 - g. "Intellectual Property Rights" means worldwide intellectual and proprietary property owned or properly licensed by a party and all intellectual or proprietary property rights subsumed therein, including copyright, patent, trademark (including goodwill), trade dress, trade secret and know-how rights.
 - h. "Professional Services" means professional services provided by Contractor to DSHS as set forth in any Statement of Work.
 - i. "Service" means Contractor's software-as-a-service identified in the Statement of Work and accessible by DSHS via <https://live.ContractorRisk.com> or another designated web site or IP address or mobile application, rendered to DSHS by Contractor.
 - j. "Statement of Work" means any statement of work entered into and mutually approved in writing by the parties pursuant to this Contract from time to time. The initial Statement of Work is attached hereto as Exhibit C.
 - k. "**Usage Data**" means all usage and operations data that results from or is generated in connection with Client's use of the Service as well as data derived therefrom. For clarity, DSHS Data does not include Usage Data.
 - l. "User" means any employee, contractor, agent, customer, investor, consultant or service provider of DSHS or any of DSHS's Affiliates who uses or accesses the Service or any other person or entity that is provided user credentials to the Service by or on behalf of DSHS or any of DSHS's Affiliates.
 - m. "Work Product" means Customizations and any software, programming, tools, documentation, and materials that are used, created, developed, or delivered by Contractor to DSHS in connection with Customizations, and all Intellectual Property Rights subsumed therein.
2. **Purpose.** The purpose of this Contract is to set forth the terms and conditions between DSHS and the Contractor under which DSHS purchases, licensing, subscription and hosting services, and professional service hours for the Contractor Risk software solution from the Contractor.
3. **Service.**

Special Terms and Conditions

- a. Service. Subject to the terms and conditions of this Contract, during the term of this Contract, the Contractor hereby grants DSHS a non-exclusive right to permit its Users to access the Service via the Internet. DSHS, its Affiliates and Users may use the Service solely for internal business of DSHS, its Affiliates and Users. Users shall use the Service in accordance with this Contract and the applicable Statement of Work and Documentation.
- b. Storage. DSHS may store DSHS Data through the Service up to the amount set forth in the applicable Statement of Work. If the amount of storage used exceeds this limit, DSHS will be charged, on a monthly basis, the excess storage fees pursuant to the Statement of Work.
- c. Service Level Agreement. Contractor's Service Level Agreement with respect to the Service is set forth as Exhibit D (the "**Service Level Agreement**"). Any Excluded Event (as defined in such Service Level Agreement) and any unavailability of the Service that does not constitute a failure of the Availability Requirement set forth in such Service Level Agreement shall not constitute a breach of this Contract.
- d. Restrictions. Nothing in this Contract shall be construed as a grant to DSHS of any right to, and DSHS shall not, and shall not permit any User or any other third party to:
 - (1) Reproduce, license, sublicense, sell, resell, transfer, assign, distribute or otherwise commercially exploit or make available to any third party the Service or any portion thereof;
 - (2) Distribute, disclose or allow use of any of the Service, or any portion thereof, in any format, through any timesharing service, service bureau, network or by any other means, to or by any third party;
 - (3) Decompile, disassemble, or otherwise reverse engineer or attempt to reconstruct or discover any source code or underlying ideas or algorithms of the Service in any manner;
 - (4) Create derivative works from, modify or alter any of the Service in any manner whatsoever;
 - (5) Use or access the Service in a manner that would reasonably be expected to damage, disable, overburden, or impair any Contractor servers or the networks connected to any Contractor server (and if any access or use of the Service does damage, disable, overburden, or impair any Contractor servers or the networks connected to any Contractor server, then DSHS shall promptly discontinue such access or use upon written notice of such by Contractor);
 - (6) Take any action that would reasonably be expected to interfere with any third party's use and enjoyment of the Service (and if any DSHS action does interfere with any third party's use and enjoyment of the Service, then DSHS shall promptly discontinue such action upon written notice of such by Contractor);
 - (7) Attempt to gain unauthorized access to the Service, accounts, computer systems, or networks connected to any Contractor server;
 - (8) Use any robot, spider or other automatic device or manual process to monitor or copy portions of the Service;
 - (9) Use the Service in a manner intended to abuse or violate the privacy or property rights of others;
 - (10) Perform any vulnerability scanning or penetration testing on the Service or Contractor's systems or networks without Contractor's explicit prior written consent for each such scan or

Special Terms and Conditions

test; or (xi) access the Service in order to (A) build a competitive product or service, or (B) build a product using similar unique and confidential ideas, features, functions or graphics of the Service.

- e. Users. DSHS may permit the number of authorized Users as set forth in the Statement of Work to use the Service. Each authorized User shall access and use the Service in accordance with the terms of this Contract and the applicable Statement of Work and Documentation, and, when applicable, through a unique and reasonably secure username and password as further described in the applicable Statement of Work or Documentation. The Service allows DSHS to grant different levels of access to DSHS Data, to different Users, as described in more detail in the Statement of Work. It is DSHS's responsibility to designate the applicable access to be granted to each User. DSHS shall cause all Users to comply with all obligations of DSHS hereunder, to the extent applicable to Users. Except for DSHS's and its Affiliates' system administrators where reasonably necessary for administrative or security purposes, no User may use the username/user identification or password of any other User. DSHS's failure to cause a User to comply with the terms of this Contract or any uncured User noncompliance shall constitute a material breach of this Contract by DSHS.
- f. Third Party Access. DSHS shall also have the right for DSHS and its Affiliates to permit third party Users to access or use the Service in accordance with the terms and conditions of this Contract and the applicable Statement of Work, provided that each such third party User has agreed in writing to Contractor's Third Party User Contract ("**Third Party Terms**") prior to or upon such User's initial login to the Service. Such Third Party Terms are available from Contractor upon request. DSHS may meet this requirement with respect to any third party User by requiring such third party User to accept the Third Party Terms as part of a click-through that can be enabled to appear upon such third party User's initial login to the Service. Any rights granted hereunder or under the Third Party Terms with respect to the Service to third party Users shall expire or terminate immediately upon the termination of this Contract in accordance with its terms. DSHS shall be fully responsible for (i) ensuring the compliance of each DSHS Party with the terms and conditions of this Contract, the applicable Statement of Work and Documentation, and the applicable Third Party User Contract, and (ii) all violations of the terms or conditions of this Contract, the applicable Statement of Work and Documentation, and the applicable Third Party Terms by each DSHS Party.
- g. Professional Services. During the term of this Contract, Contractor will make available to DSHS certain Professional Services to the extent set forth in the Statement of Work. DSHS may also contract for expanded services for additional days and hours in accordance with the rates set forth in the Statement of Work, or if no such rates are specified, Contractor's then-current policies and prices. Notwithstanding the foregoing, Contractor will not be obligated to provide any support required as a result of, or with respect to:
 - (1) DSHS's operating systems, networks, hardware, or other related equipment of DSHS, or;
 - (2) DSHS's or any of its Users' use of the Service other than in accordance with the applicable Statement of Work and Documentation and as permitted under this Contract.
- h. DSHS Obligations. DSHS shall:
 - (1) Provide Contractor with reasonable access to DSHS's premises to the extent necessary to enable Contractor to perform its obligations hereunder;
 - (2) Provide adequate resources to participate in or facilitate the performance of the Service; (iii) timely participate in meetings relating to the Service;

Special Terms and Conditions

- (3) Assign personnel with relevant training and experience to work in consultation with Contractor;
 - (4) Meet the requirements to use the Service as set forth at <http://www.origamirisk.com/product-requirements>;
 - (5) Safeguard the usernames, passwords and other security data, methods and devices furnished to DSHS in connection with the Service and prevent unauthorized access to or use of the Service and promptly notify Contractor if it becomes aware of any such unauthorized access or that the security of its usernames or passwords has been compromised;
 - (6) Be responsible for DSHS networks, equipment and system security required or appropriate in connection with the Service;
 - (7) Have sole responsibility for the accuracy, quality, legality, reliability and appropriateness of all DSHS Data;
 - (8) Transmit DSHS Data only in an encrypted format as set forth in the Service Level Agreement or as otherwise mutually agreed by the parties;
 - (9) Obtain all consents and authorizations from any third parties that DSHS requires in order for Contractor to provide the Service and perform the Professional Services (and Contractor shall not be required to enter into Contracts with any such third parties), and;
 - (10) Take such other actions as are required of DSHS pursuant to this Contract, including any Statement of Work.
- i. DSHS Warranty. The parties acknowledge and agree that during the term of this Contract a DSHS Party or other third parties may disclose certain DSHS Data, including personally identifiable data regarding employees or other individuals, to Contractor for the benefit of a DSHS Party. With respect to any DSHS Data so disclosed by, or on behalf of, a DSHS Party to Contractor, DSHS represents and warrants to Contractor that:
- (1) Each such DSHS Party, and such other third parties operating on DSHS's behalf are authorized to collect, use and disclose the DSHS Data to Contractor for use and storage pursuant to this Contract;
 - (2) Such disclosure, use or storage does not and shall not violate applicable law or, if applicable, such DSHS Party's Contracts with or privacy notices to individuals with respect to whom the DSHS Data relates; and;
 - (3) DSHS shall not request Contractor to use, store, disclose or otherwise process DSHS Data in any manner that would not be permissible under applicable law or, if applicable, such DSHS Party's Contracts with or privacy notices to individuals with respect to whom the DSHS Data relates, if done by DSHS.
- j. Non-Contractor Events. DSHS acknowledges and agrees that the Contractor shall not be responsible or liable for any delay or failure in its performance of any duties or obligations pursuant to this Contract, including any Statement of Work, to the extent such delays or failures result or arise from any (1) act or omission of any DSHS Party, including any delays in their performance or cooperation with respect to the obligations or warranties set forth in this Contract or any Statement of Work; (2) failure of any DSHS Party's equipment or software (other than the Service); or (3) Force Majeure Event.

Special Terms and Conditions

- k. Mobile Service. The Service may include certain services that are available via an application downloaded and installed on a mobile device. To the extent DSHS chooses to use such application, DSHS acknowledges and agrees that DSHS Data may be stored locally on a mobile device as part of such service and that the physical security of any mobile device used to access such services is DSHS's responsibility. If DSHS or any User elects to store data on a mobile device, Contractor shall not be responsible for any loss of DSHS Data or any other data on such device.

4. Intellectual Property Rights.

- a. Contractor Intellectual Property Rights. As between Contractor and DSHS, Contractor owns all right, title and interest, including all related Intellectual Property Rights in and to, or related to the Service and Work Product, including all software programs contained therein. To the extent that any such Intellectual Property Rights do not otherwise vest in Contractor or its licensors, DSHS hereby agrees to promptly assign such Intellectual Property Rights to Contractor or its licensors, and to do all other acts reasonably necessary to perfect Contractor's or its licensors' ownership thereof, without additional consideration of any kind. The Contractor name, the Contractor logos, and the product names associated with the Service are trademarks of Contractor or third parties, and no right or license is granted with respect to their use. The Service may contain intellectual property belonging to third parties. All such intellectual property is and shall remain the property of its respective owners. Except for the limited rights expressly granted herein, all right, title and interest in and to the Service and Work Product are reserved by Contractor, and, except as expressly granted herein, nothing contained in this Contract shall be construed as conferring any right, title, interest or license with respect to the Service or Work Product upon DSHS, by implication, estoppel or otherwise. In addition, DSHS agrees and acknowledges that Contractor shall have an unlimited right to incorporate into any updates, upgrades, or modifications to the Service all suggestions, ideas, enhancement requests, feedback, recommendations or other information provided by DSHS or any User relating to the Service. Such Service, as updated, upgraded, or modified, shall be owned by Contractor as provided in this Section. DSHS expressly acknowledges and agrees that the Work Product shall not constitute work made-for-hire under the United States Copyright Act, and that Contractor shall have the exclusive right to protect the Work Product by patent, copyright, or any other means. Work Product shall be made available to DSHS as part of the Service to the extent set forth in the Statement of Work, and DSHS shall have no other right to use any Work Product. Notwithstanding anything to the contrary in this Agreement, all rights in and to the Usage Data including all Intellectual Property Rights therein are and shall remain the exclusive property of Origami. Subject to Origami's confidentiality obligations set forth in this Agreement, Client agrees that Origami shall have the right to collect and use data or information resulting from a Client Party's use of the Service so long as such data and information is de-identified and aggregated so that it cannot identify, be traced back to or otherwise be associated in any manner with Client or any particular individual.
- b. DSHS Data. DSHS Data shall be Confidential Information of DSHS under this Contract. As between Contractor and DSHS, DSHS shall own all right, title and interest in and to the DSHS Data, which shall never be deemed to be the Service or Work Product, even if delivered or incorporated therewith. Contractor shall have no responsibility, whatsoever, for the accuracy, quality, legality, reliability, appropriateness, and intellectual property ownership of DSHS Data, and Contractor shall not review, monitor or check the DSHS Data except as necessary to provide the Service to DSHS. Contractor shall not be responsible or liable for the deletion, destruction, damage or loss of any DSHS Data through no fault of Contractor or its providers without limiting Contractor's liability to maintain backup data as set forth in the Service Level Agreement. Upon DSHS's written request within 30 days following the termination of this Contract, Contractor will at its expense provide electronic files to DSHS in delimited text format containing DSHS's DSHS Data.
- c. Notices of Infringement. In the event DSHS discovers or is notified of an actual or suspected

Special Terms and Conditions

infringement of the rights of the Contractor or its licensors in or to the Service or any unauthorized access to or use of the Service (each, an “**Infringement**”) related to DSHS’s use of the Service, DSHS shall promptly notify Contractor of such known or suspected Infringement and terminate such Infringement to the extent within DSHS’s control. DSHS agrees to reasonably cooperate with and assist Contractor (at Contractor’s sole expense) in protecting, enforcing and defending Contractor’s rights in and to the Service.

5. Financial Terms.

- a. Fees. DSHS shall pay to Contractor the Fees set forth in any Statement of Work or as otherwise agreed in writing by the parties.
- b. Expenses. Subject to Washington State limitations on travel reimbursement, DSHS shall reimburse Contractor for all pre-authorized in writing, reasonable, documented out of pocket travel, lodging, meal and other expenses reasonably incurred by Contractor in the course of performing the Service.
- c. Payments. All Fees under this Contract shall be payable by DSHS in accordance with the applicable Statement of Work or as otherwise agreed by the parties. Fees shall be due within 30 days of invoice date. Payments remitted after 30 days shall bear interest at the maximum rate allowed by Washington State law. Except as provided in Sections 7(b) and 9(a), all Fees paid hereunder are non-refundable. Without limiting Contractor’s other rights and remedies, if DSHS does not pay a correct overdue invoice within 15 days after receiving notice from Contractor of nonpayment unless DSHS has notified Contractor of a good faith dispute prior to such time, then Contractor may suspend DSHS’s access to the Service and the Professional Services until Contractor receives such payment, and Fees shall continue to accrue during any such period; provided that this shall not be deemed to limit DSHS’s right to the return of its DSHS Data pursuant to Section 3(b) of this Contract.

6. Confidentiality.

- a. Confidential Information. Each party acknowledges and agrees that during the term of this Contract it may be furnished with or otherwise have access to Confidential Information of the other party. The party that has received Confidential Information (the “**Receiving Party**”), in fulfilling its obligations under this Section, shall exercise the same degree of care and protection with respect to the Confidential Information of the party that has disclosed Confidential Information to the Receiving Party (the “**Disclosing Party**”) that it exercises with respect to its own Confidential Information, but in no event shall the Receiving Party exercise less than a reasonable standard of care. The Receiving Party shall only use, access and disclose Confidential Information as necessary to fulfill its obligations under this Contract, including any Statement of Work, or in exercise of its rights expressly granted hereunder. Receiving Party shall not directly or indirectly disclose, sell, copy, distribute, republish, create derivative works from, demonstrate or allow any third party to have access to any of Disclosing Party’s Confidential Information; provided that the Receiving Party may disclose the Disclosing Party’s Confidential Information to its directors, officers, employees, subcontractors, agents, Affiliates or other representatives (collectively, the “**Representatives**”) who have a need to know and who are bound by confidentiality obligations with respect to such Confidential Information that are substantially similar to those set forth in this Section. The Receiving Party shall be responsible and liable for any breach of this Section by any of its Representatives. This Contract (including all Statements of Work and pricing thereunder) and all Intellectual Property Rights with respect to the Service and Work Product shall be deemed to be Confidential Information of Contractor under this Contract.
- b. Exclusions. The following information shall not be considered Confidential Information subject to this Section:
 - (1) Information that is publicly available or later becomes available other than through a breach of

Special Terms and Conditions

this Contract;

(2) Information that is known to the Receiving Party or its Representatives prior to such disclosure or is independently developed by the Receiving Party or its Representatives subsequent to such disclosure, or;

(3) Information that is subsequently lawfully obtained by the Receiving Party or its Representatives from a third party without obligations of confidentiality. If the Receiving Party is required by law, including but not limited to the Washington State Public Records Act (Chapter 42.56 Revised Code of Washington), to disclose any portion of the Disclosing Party's Confidential Information, Receiving Party shall give prior timely notice of such disclosure to Disclosing Party to permit Disclosing Party to seek a protective or similar order, and, absent the entry of such an order, Receiving Party shall disclose only such Confidential Information as is necessary be disclosed in response to such subpoena, court order or other similar document.

c. Return of Confidential Information. Upon termination or expiration of this Contract, the Receiving Party will promptly return or destroy any Confidential Information in the possession or control of the Receiving Party. Contractor's obligation to return and destroy DSHS Data is set forth in the Contract's Section 4(b).

7. Data Security.

a. Audit Report. Upon DSHS's written request to Contractor during the term of this Contract (no more than once in any 12-month period), Contractor shall provide a copy of its Service Organization Control (SOC) 2 audit report (or an equivalent audit report or pursuant to a successor standard) ("**SOC 2 Report**") to DSHS, and such report shall contain an unqualified opinion. Such audit report shall be deemed Confidential Information under the terms of this Contract.

b. Safeguards. Contractor shall maintain commercially reasonable administrative, technical and physical safeguards designed to protect the security and privacy of DSHS Data. Such safeguards are described in Contractor's most recently completed SOC 2 Report. In no event during the term of this Contract will Contractor materially diminish the protections provided by the controls set forth in such SOC 2 Report. Such safeguards shall comply with data privacy laws that are applicable to Contractor in its performance of this Contract, including, without limitation, any applicable data privacy laws addressing personally identifiable information that may be contained in the DSHS Data. Contractor shall also maintain an internal information security management program that addresses data security and the security controls employed by Contractor in compliance with this Contract. Contractor shall encrypt DSHS Data as set forth in the Service Level Agreement.

c. Notification. Contractor shall inform DSHS promptly and without undue delay in the event that it learns of any breach of Contractor's systems resulting in unauthorized disclosure of, or access to, any DSHS Data. Any such notice will provide a description about the DSHS Data that was accessed to the extent available at the time of the notice. Contractor will provide regular updates to DSHS as additional details about the nature of the affected DSHS Data become available. Contractor agrees to mitigate, to the extent practicable, any harmful effects from such breach that are or become known to Contractor.

8. Limited Warranty.

a. Service Warranty. Contractor warrants that the Service will perform in all material respects in accordance with the Documentation when used in accordance with the terms of this Contract on the hardware and with the third-party software specified by Contractor from time to time. DSHS's sole remedy for any breach by Contractor of the warranty provided in this Section shall be replacement

Special Terms and Conditions

of the nonconforming Service, at Contractor's sole expense, as described herein. Contractor shall deliver to DSHS replacement Service, a work-around and/or an error/bug fix as may be necessary to correct the nonconformity. In the event that DSHS gives Contractor notice of an apparent nonconformity that Contractor reasonably determines is not due to any fault or failure of the Service to conform to the warranty provided herein, all time spent by Contractor resulting in such determination, including time spent attempting to correct the problem, shall be charged against DSHS's DSHS service hours, or, if DSHS service hours have been exhausted, charged to DSHS at Contractor's then current hourly rate for such services.

- b. Professional Services Warranty. Contractor represents and warrants that the Professional Services shall be performed in a professional and commercially reasonable manner consistent with the standard of care exercised by Contractor in performing similar services for other Customers. DSHS's sole remedy for breach of this warranty shall be re-performance of the nonconforming Professional Services, provided that Contractor must have received written notice of the nonconformity from DSHS no later than 30 days after the original performance of the applicable Professional Services by Contractor.
- c. Disclaimers.
 - (1) EXCEPT AS OTHERWISE EXPRESSLY STATED IN THIS CONTRACT, CONTRACTOR MAKES NO WARRANTY OR REPRESENTATION WHATSOEVER, EITHER EXPRESS, IMPLIED OR STATUTORY, WITH RESPECT TO THE SERVICE, WORK PRODUCT, PROFESSIONAL SERVICES, OR ANY OTHER SERVICES PROVIDED HEREUNDER OR THE USE THEREOF BY DSHS AND ITS USERS, INCLUDING QUALITY, PERFORMANCE, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, AND CONTRACTOR HEREBY DISCLAIMS THE SAME. EXCEPT AS OTHERWISE SET FORTH IN THIS CONTRACT, CONTRACTOR AND ITS LICENSORS DO NOT REPRESENT OR WARRANT THAT: (a) THE USE OF THE SERVICE WILL BE UNINTERRUPTED OR ERROR-FREE; OR (b) THE SERVICE WILL MEET DSHS'S REQUIREMENTS OR EXPECTATIONS; OR (c) ALL ERRORS OR DEFECTS IN THE SERVICE WILL BE CORRECTED.
 - (2) DSHS ACKNOWLEDGES AND AGREES THAT THE SERVICE IS A TOOL TO BE USED BY DSHS IN THE COURSE OF EXERCISING ITS PROFESSIONAL JUDGMENT. THE SERVICE MAY BE SUBJECT TO LIMITATIONS, DELAYS, AND OTHER PROBLEMS INHERENT IN THE USE OF THE INTERNET AND ELECTRONIC COMMUNICATIONS. CONTRACTOR IS NOT RESPONSIBLE FOR ANY DELAYS, DELIVERY FAILURES, OR OTHER DAMAGE RESULTING FROM SUCH PROBLEMS OUTSIDE OF ITS REASONABLE CONTROL. NO CONTRACTOR AGENT OR EMPLOYEE IS AUTHORIZED TO MAKE ANY EXPANSION, MODIFICATION OR ADDITION TO THIS LIMITATION AND EXCLUSION OF WARRANTIES IN THIS CONTRACT.
 - (3) Contractor shall not be responsible for: (A) any non-conformities of the Service with Documentation, omissions, delays, inaccuracies or any other failure caused by a DSHS Party's computer systems, hardware or software (other than the Service), including by interfaces with such third party software, or any inaccuracies that such systems may cause within the Service; or (B) any data that Contractor receives from a DSHS Party or third party sources and including the data's accuracy or completeness, or DSHS's claim handling or other decisions. Contractor disclaims any liability for interception of any such data or communications, including of encrypted data. DSHS agrees that Contractor shall have no responsibility or liability for any damages arising in connection with access to or use of the Service by any DSHS Party to the extent such access or use is not authorized by this Contract.

9. Indemnification by the Contractor.

Special Terms and Conditions

- a. Indemnification. The Contractor agrees to indemnify, defend, settle, or pay any third party claim or action against a DSHS Party for infringement of any U.S. patent or copyright arising from DSHS's use of the Service in accordance with this Agreement. If the Service or any part of the Service is held to infringe and the use thereof is enjoined or restrained or, if as a result of a settlement or compromise, such use is materially adversely restricted, Contractor shall, at its own expense and as DSHS's sole remedy therefor (other than the indemnification obligation set forth above), either: (i) procure for DSHS the right to continue to use the Service; or (ii) modify the Service to make it non-infringing, provided that such modification does not materially adversely affect DSHS's authorized use of the Service; or (iii) replace the Service with a functionally equivalent non-infringing program at no additional charge to DSHS; or (iv) if none of the foregoing alternatives is reasonably available to Contractor, terminate this Agreement and refund to DSHS any prepaid but unearned Fees paid to Contractor in advance by DSHS prior to the effective date of the termination.
- b. Exclusions. Contractor's indemnification obligations under Section 10(a) shall not apply to the extent the claim is based on:
 - (1) Modifications to the Service or any component thereof made by anyone other than Contractor or on behalf of Contractor;
 - (2) Use of any Service in combination with a product not supplied by Contractor; or,
 - (3) Use of any Service other than in accordance with this Agreement and the Documentation.
- c. Conduct. Contractor shall have the sole right to conduct the defense of any such infringement claim or action and all negotiations for its settlement or compromise, and to settle or compromise any such claim. DSHS agrees to cooperate and ensure that each DSHS Party cooperates with Contractor in doing so. DSHS agrees to give Contractor prompt written notice, in no case longer than within seven days of receipt or discovery, of any threat, warning, or notice of any such claim or action, with copies of any and all documents each DSHS Party may receive relating thereto.

10. Limitation of Liability.

- a. Disclaimer of Damages. IN NO EVENT WILL EITHER PARTY BE LIABLE FOR ANY INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING UNDER OR IN CONNECTION WITH THIS AGREEMENT, THE SERVICE OR THE PROFESSIONAL SERVICES, WHETHER BASED IN CONTRACT, TORT, INTENDED CONDUCT OR OTHERWISE, INCLUDING WITHOUT LIMITATION, DAMAGES RELATING TO THE LOSS OF PROFITS, INCOME, GOODWILL OR REVENUE, COSTS INCURRED AS A RESULT OF DECISIONS MADE IN RELIANCE ON THE SERVICE, LOSS OF USE OF THE SERVICE OR ANY OTHER SOFTWARE OR OTHER PROPERTY, LOSS OF DATA, THE COSTS OF RECOVERING OR RECONSTRUCTING SUCH DATA OR THE COST OF SUBSTITUTE SOFTWARE, SERVICES OR DATA, OR FOR CLAIMS BY THIRD PARTIES, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

11. Limitation of Liability. EXCEPT FOR DSHS'S PAYMENT OBLIGATIONS, UNDER NO CIRCUMSTANCES SHALL EITHER PARTY'S AGGREGATE MAXIMUM LIABILITY ARISING UNDER OR IN CONNECTION WITH THIS AGREEMENT, THE SERVICE OR THE PROFESSIONAL SERVICES EXCEED THE PAYMENTS ACTUALLY MADE TO CONTRACTOR HEREUNDER DURING THE 12 MONTHS PRECEDING THE DATE ON WHICH ANY CLAIM IS MADE AGAINST CONTRACTOR.

Special Terms and Conditions

12. Export Control.

- a. Export. DSHS shall not export the Service or any Work Product in violation of applicable United States laws and regulations. DSHS also agrees that it will not knowingly export, directly or indirectly, the Service or any Work Product:
 - (1) That it knows will directly assist in the design, development, production, stockpiling or use of missiles, nuclear weapons or chemical/biological weapons;
 - (2) To any entity on the Department of Commerce Entity List or any person or entity on the Department of Commerce Denied Persons List, each currently available at <http://www.bis.doc.gov>; or,
 - (3) To any country subject to sanctions administered by the Department of the Treasury's Office of Foreign Assets Control or to any person or entity on the lists of prohibited entities and persons maintained by such office, currently available at <http://www.ustreas.gov/ofac>.
- b. Disclaimer. Contractor makes no representation that the Service is appropriate or available for use in other locations. If DSHS uses the Service from outside the United States of America, Canada, the United Kingdom and/or the European Union, DSHS is solely responsible for compliance with all applicable laws, including export and import regulations of other countries. Any diversion of the Service contrary to applicable law is prohibited.

13. General.

- a. Notices. Any notice, request, demand or other communication (each, a "**Notice**") given pursuant to this Contract must be in writing and delivered to the other party by either personal delivery, Certified Mail (return receipt requested and postage prepaid), nationally recognized overnight courier (with all fees prepaid) or e-mail at the address of such party listed on the signature page to this Contract. A party may change its address by giving Notice pursuant to this Section.
- b. Assignment. Neither party shall have the right to assign, transfer, or sublicense any obligations or benefit under this Contract without the prior written consent of the other party; provided, however, that no written consent shall be required to assign or transfer this Contract to any parent or wholly owned subsidiary of a party, and further provided that Contractor may assign or transfer this Contract without DSHS's prior written consent to a successor by way of a merger, acquisition, sale, transfer or other disposition of all or substantially all of its assets. Except as otherwise provided herein, this Contract shall be binding on and inure to the benefit of the respective successors and permitted assigns of the parties.
- c. Third Party Beneficiaries. This Contract does not and is not intended to confer any rights or remedies upon any party other than the parties to this Contract.
- d. Publicity. Without prior written approval of the other party or as otherwise set forth in a SOW, neither party shall, directly or indirectly, make any public announcement related to this Contract or the Service. Notwithstanding the foregoing, Contractor may disclose the fact that DSHS has procured a license for the Service; provided that Contractor will not state or imply that DSHS endorses or recommends the Service without the written permission of DSHS.
- e. Entire Contract; Amendments. This Contract (including all exhibits, appendices, schedules and attachments hereto) constitutes the final Contract between the parties. All prior and contemporaneous oral and written communications, negotiations and Contracts between the parties on the matters contained in this Contract, including, without limitation, any nondisclosure or confidentiality Contracts entered into between the parties prior to the date of this Contract, are expressly merged into and superseded by this Contract. No terms or conditions contained in any

Special Terms and Conditions

purchase order shall amend this Contract or shall otherwise constitute an Contract between the parties. The parties may amend this Contract only by a written Contract of the parties that identifies itself as an amendment to this Contract.

- f. Waivers. The parties may waive any provision in this Contract only by a writing executed by the party against whom the waiver is sought to be enforced. No failure or delay in exercising any right or remedy, or in requiring the satisfaction of any condition, under this Contract, and no act, omission or course of dealing between the parties, operates as a waiver or estoppel of any right, remedy or condition. A waiver once given is not to be construed as a waiver on any future occasion or against any other person.
- g. Severability. In the event that any provision of this Contract shall be determined to be illegal or unenforceable, such provision shall be limited or eliminated to the minimum extent necessary so that this Contract shall otherwise remain in full force and effect and enforceable.
- h. Governing Law. The laws of the State of Washington (without giving effect to its conflicts of law principles) govern all matters arising out of or relating to this Contract and the transactions it contemplates, including, without limitation, its interpretation, construction, performance and enforcement.
- i. Force Majeure. Neither party shall have any liability for any failure or delay in performance of its obligations under this Contract (except for payment) because of circumstances beyond its reasonable control, including without limitation, acts of God, fires, floods, earthquakes, wars, civil disturbances, terrorism, sabotage, accidents, unusually severe weather, labor disputes, governmental actions, power failures, viruses that are not preventable through generally available retail products, inability to obtain labor, material or equipment, catastrophic hardware failures, usage spikes, attacks on servers, or any inability to transmit or receive information over the Internet (each, a “**Force Majeure Event**”), nor shall any such failure or delay give any party the right to terminate this Contract.
- j. Counterparts. This Contract and each Statement of Work may be executed in counterparts, each of which will be deemed an original but all of which together shall constitute one and the same Contract. Delivery of an executed counterpart of a signature page to this Contract or any Statement of Work by PDF or other electronic means shall be as effective as delivery of a manually executed counterpart of this Contract or such Statement of Work.

Exhibits

Exhibit A – Data Security Requirements

1. **Definitions.** The words and phrases listed below, as used in this Exhibit, shall each have the following definitions:
 - a. “AES” means the Advanced Encryption Standard, a specification of Federal Information Processing Standards Publications for the encryption of electronic data issued by the National Institute of Standards and Technology (<https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197-upd1.pdf>).
 - b. “Authorized Users(s)” means an individual or individuals with a business need to access DSHS Confidential Information, and who has or have been authorized to do so.
 - c. “Business Associate Agreement” means an agreement between DSHS and a contractor who is receiving Data covered under the Privacy and Security Rules of the Health Insurance Portability and Accountability Act of 1996. The agreement establishes permitted and required uses and disclosures of protected health information (PHI) in accordance with HIPAA requirements and provides obligations for business associates to safeguard the information.
 - d. “Category 4 Data” is data that is confidential and requires special handling due to statutes or regulations that require especially strict protection of the data and from which especially serious consequences may arise in the event of any compromise of such data. Data classified as Category 4 includes but is not limited to data protected by: the Health Insurance Portability and Accountability Act (HIPAA), Pub. L. 104-191 as amended by the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH), 45 CFR Parts 160 and 164; the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. §1232g; 34 CFR Part 99; Internal Revenue Service Publication 1075 (<https://www.irs.gov/pub/irs-pdf/p1075.pdf>); Substance Abuse and Mental Health Services Administration regulations on Confidentiality of Alcohol and Drug Abuse Patient Records, 42 CFR Part 2; and/or Criminal Justice Information Services, 28 CFR Part 20.
 - e. “Cloud” means data storage on servers hosted by an entity other than the Contractor and on a network outside the control of the Contractor. Physical storage of data in the cloud typically spans multiple servers and often multiple locations. Cloud storage can be divided between consumer grade storage for personal files and enterprise grade for companies and governmental entities. Examples of consumer grade storage would include iTunes, Dropbox, Box.com, and many other entities. Enterprise cloud vendors include Microsoft Azure, Amazon Web Services, and Rackspace.
 - f. “Encrypt” means to encode Confidential Information into a format that can only be read by those possessing a “key”; a password, digital certificate or other mechanism available only to authorized users. Encryption must use a key length of at least 256 bits for symmetric keys, or 2048 bits for asymmetric keys. When a symmetric key is used, the Advanced Encryption Standard (AES) must be used if available.
 - g. “FedRAMP” means the Federal Risk and Authorization Management Program (see www.fedramp.gov), which is an assessment and authorization process that federal government agencies have been directed to use to ensure security is in place when accessing Cloud computing products and services.
 - h. “Hardened Password” means a string of at least eight characters containing at least three of the following four character classes: Uppercase alphabetic, lowercase alphabetic, numeral, and special characters such as an asterisk, ampersand, or exclamation point.

Exhibits

- i. “Mobile Device” means a computing device, typically smaller than a notebook, which runs a mobile operating system, such as iOS, Android, or Windows Phone. Mobile Devices include smart phones, most tablets, and other form factors.
- j. “Multi-factor Authentication” means controlling access to computers and other IT resources by requiring two or more pieces of evidence that the user is who they claim to be. These pieces of evidence consist of something the user knows, such as a password or PIN; something the user has such as a key card, smart card, or physical token; and something the user is, a biometric identifier such as a fingerprint, facial scan, or retinal scan. “PIN” means a personal identification number, a series of numbers which act as a password for a device. Since PINs are typically only four to six characters, PINs are usually used in conjunction with another factor of authentication, such as a fingerprint.
- k. “Portable Device” means any computing device with a small form factor, designed to be transported from place to place. Portable devices are primarily battery powered devices with base computing resources in the form of a processor, memory, storage, and network access. Examples include, but are not limited to, mobile phones, tablets, and laptops. Mobile Device is a subset of Portable Device.
- l. “Portable Media” means any machine readable media that may routinely be stored or moved independently of computing devices. Examples include magnetic tapes, optical discs (CDs or DVDs), flash memory (thumb drive) devices, external hard drives, and internal hard drives that have been removed from a computing device.
- m. “Secure Area” means an area to which only authorized representatives of the entity possessing the Confidential Information have access, and access is controlled through use of a key, card key, combination lock, or comparable mechanism. Secure Areas may include buildings, rooms or locked storage containers (such as a filing cabinet or desk drawer) within a room, as long as access to the Confidential Information is not available to unauthorized personnel. In otherwise Secure Areas, such as an office with restricted access, the Data must be secured in such a way as to prevent access by non-authorized staff such as janitorial or facility security staff, when authorized Contractor staff are not present to ensure that non-authorized staff cannot access it.
- n. “Trusted Network” means a network operated and maintained by the Contractor, which includes security controls sufficient to protect DSHS Data on that network. Controls would include a firewall between any other networks, access control lists on networking devices such as routers and switches, and other such mechanisms which protect the confidentiality, integrity, and availability of the Data.
- o. “Unique User ID” means a string of characters that identifies a specific user and which, in conjunction with a password, passphrase or other mechanism, authenticates a user to an information system.

For the avoidance of doubt, the terms “data”, “Data” and “Category 4 Data” as defined or used herein is limited to DSHS Data (as defined in the Special Terms and Conditions).

2. **Authority.** The security requirements described in this document reflect the applicable requirements of policies and standards of the Washington Technology Services Agency (https://watech.wa.gov/policies?combine=&field_categories_target_id=80&field_type_target_id=All), and of the DSHS Information Security Policy and Standards Manual. Reference material related to these requirements can be found here: <https://www.dshs.wa.gov/ffa/keeping-dshs-client-information-private-and-secure>, which is a site developed by the DSHS Information Security Office and hosted by DSHS Central Contracts and Legal Services. For the avoidance of doubt, the information at the

Exhibits

foregoing links do not impose any rights and obligations on the Contractor and Contractor and DSHS agree that the rights and obligations between the parties are as set forth in this exhibit and the IT Services Contract to which this exhibit is attached.

3. **Administrative Controls.** The Contractor must have the following controls in place:
 - a. A documented security policy governing the secure use of its computer network and systems, and which defines sanctions that may be applied to Contractor staff for violating that policy.
 - b. If the Data shared under this agreement is classified as Category 4, the Contractor must be aware of and compliant with the applicable legal or regulatory requirements for that Category 4 Data.
 - c. If Confidential Information shared under this agreement is classified as Category 4, the Contractor must have a documented risk assessment for the system(s) housing the Category 4 Data.
4. **Authorization, Authentication, and Access.** In order to ensure that access to the Data is limited to authorized staff, the Contractor must:
 - a. Have documented policies and procedures governing access to systems with the shared Data.
 - b. Restrict access through administrative, physical, and technical controls to authorized staff.
 - c. Ensure that user accounts are unique and that any given user account logon ID and password combination is known only to the one employee to whom that account is assigned. For purposes of non-repudiation, it must always be possible to determine which employee performed a given action on a system housing the Data based solely on the logon ID used to perform the action.
 - d. Ensure that only authorized users are capable of accessing the Data.
 - e. Ensure that an employee's access to the Data is removed as soon as practicable, but no later than two (2) business days:
 - (1) Upon suspected compromise of the user credentials.
 - (2) When their employment, or the contract under which the Data is made available to them, is terminated.
 - (3) When they no longer need access to the Data to fulfill the requirements of the contract.
 - f. Have a process to periodically review and verify that only authorized users have access to systems containing DSHS Confidential Information.
 - g. When accessing the Data from within the Contractor's network (the Data stays within the Contractor's network at all times), enforce password and logon requirements for users within the Contractor's network, including:
 - (1) A minimum length of 8 characters, and containing at least three of the following character classes: uppercase letters, lowercase letters, numerals, and special characters such as an asterisk, ampersand, or exclamation point.
 - (2) That a password does not contain a user's name, logon ID, or any form of their full name.

Exhibits

(3) That a password does not consist of a single dictionary word. A password may be formed as a passphrase which consists of multiple dictionary words.

h. When accessing Confidential Information from an external location (the Data will traverse the Internet or otherwise travel outside the Contractor's network), mitigate risk and enforce password and logon requirements for users by employing measures including:

(1) Ensuring mitigations applied to the system don't allow end-user modification.

(2) [reserved]

(3) Using industry standard protocols and solutions for remote access. Examples would include RADIUS and Citrix.

(4) Encrypting all remote access traffic from the external workstation to Trusted Network or to a component within the Trusted Network. The traffic must be encrypted at all times while traversing any network, including the Internet, which is not a Trusted Network.

(5) Ensuring that the remote access system prompts for re-authentication or performs automated session termination after no more than 30 minutes of inactivity.

(6) Ensuring use of Multi-factor Authentication to connect from the external end point to the internal end point.

i. Passwords or PIN codes may meet a lesser standard if used in conjunction with another authentication mechanism, such as a biometric (fingerprint, face recognition, iris scan) or token (software, hardware, smart card, etc.) in that case:

(1) The PIN or password must be at least 5 letters or numbers when used in conjunction with at least one other authentication factor

(2) Must not be comprised of all the same letter or number (11111, 22222, aaaaa, would not be acceptable)

(3) Must not contain a "run" of three or more consecutive numbers (12398, 98743 would not be acceptable)

j. If the contract specifically allows for the storage of Confidential Information on a Mobile Device, passcodes used on the device must:

(1) Be a minimum of six alphanumeric characters.

(2) Contain at least three unique character classes (upper case, lower case, letter, number).

(3) Not contain more than a three consecutive character run. Passcodes consisting of 12345, or abcd12 would not be acceptable.

5. Protection of Data. The Contractor agrees to store Data on one or more of the following media and protect the Data as described:

a. **Hard disk drives.** Origami agrees that it will not store Data in this manner. In the event this should change, the following terms apply. For Data stored on local workstation hard disks, access to the Data will be restricted to Authorized User(s) by requiring logon to the local workstation using a

Exhibits

Unique User ID and Hardened Password or other authentication mechanisms which provide equal or greater security, such as biometrics or smart cards.

- b. **Network server disks.** Origami agrees that it will not store Data in this manner. In the event this should change, the following terms apply. For Data stored on hard disks mounted on network servers and made available through shared folders, access to the Data will be restricted to Authorized Users through the use of access control lists which will grant access only after the Authorized User has authenticated to the network using a Unique User ID and Hardened Password or other authentication mechanisms which provide equal or greater security, such as biometrics or smart cards. Data on disks mounted to such servers must be located in an area which is accessible only to authorized personnel, with access controlled through use of a key, card key, combination lock, or comparable mechanism.

For DSHS Confidential Information stored on these disks, deleting unneeded Data is sufficient as long as the disks remain in a Secure Area and otherwise meet the requirements listed in the above paragraph. Destruction of the Data, as outlined below in Section 8 Data Disposition, may be deferred until the disks are retired, replaced, or otherwise taken out of the Secure Area.

- c. **Optical discs (CDs or DVDs) in local workstation optical disc drives.** Origami agrees that it will not store Data, nor will it accept Data stored, in this manner. In the event this should change, the following terms apply. Data provided by DSHS on optical discs which will be used in local workstation optical disc drives and which will not be transported out of a Secure Area. When not in use for the contracted purpose, such discs must be Stored in a Secure Area. Workstations which access DSHS Data on optical discs must be located in an area which is accessible only to authorized personnel, with access controlled through use of a key, card key, combination lock, or comparable mechanism.
- d. **Optical discs (CDs or DVDs) in drives or jukeboxes attached to servers.** Origami agrees that it will not store Data, nor will accept Data stored, in this manner. In the event this should change, the following terms apply. Data provided by DSHS on optical discs which will be attached to network servers and which will not be transported out of a Secure Area. Access to Data on these discs will be restricted to Authorized Users through the use of access control lists which will grant access only after the Authorized User has authenticated to the network using a Unique User ID and Hardened Password or other authentication mechanisms which provide equal or greater security, such as biometrics or smart cards. Data on discs attached to such servers must be located in an area which is accessible only to authorized personnel, with access controlled through use of a key, card key, combination lock, or comparable mechanism.
- e. **Paper documents.** Origami agrees that it will not store Data, nor will accept Data stored, in this manner. In the event this should change, the following terms apply. Any paper records must be protected by storing the records in a Secure Area which is only accessible to authorized personnel. When not in use, such records must be stored in a Secure Area.
- f. **Remote Access.** Origami agrees that it will not access Data in this manner. In the event this should change, the following terms apply. Access to and use of the Data over the State Governmental Network (SGN) or Secure Access Washington (SAW) will be controlled by DSHS staff who will issue authentication credentials (e.g. a Unique User ID and Hardened Password) to Authorized Users on Contractor's staff. Contractor will notify DSHS staff immediately whenever an Authorized User in possession of such credentials is terminated or otherwise leaves the employ of the Contractor, and whenever an Authorized User's duties change such that the Authorized User no longer requires access to perform work for this Contract.

Exhibits

- g. **Data storage on portable devices or media.** Origami agrees that it will not store Data, nor will accept Data stored, in this manner. In the event this should change, the following terms apply.
- (1) Except where otherwise specified herein, DSHS Data shall not be stored by the Contractor on portable devices or media unless specifically authorized within the terms and conditions of the Contract. If so authorized, the Data shall be given the following protections:
 - (a) Encrypt the Data.
 - (b) Control access to devices with a Unique User ID and Hardened Password or stronger authentication method such as a physical token or biometrics.
 - (c) Manually lock devices whenever they are left unattended and set devices to lock automatically after a period of inactivity, if this feature is available. Maximum period of inactivity is 20 minutes.
 - (d) Apply administrative and physical security controls to Portable Devices and Portable Media by:
 - i. Keeping them in a Secure Area when not in use,
 - ii. Using check-in/check-out procedures when they are shared, and
 - iii. Taking frequent inventories.
 - (2) When being transported outside of a Secure Area, Portable Devices and Portable Media with DSHS Confidential Information must be under the physical control of Contractor staff with authorization to access the Data, even if the Data is encrypted.
- h. **Data stored for backup purposes.**
- (1) Origami agrees that it will not store Data, nor will accept Data stored, in this manner. In the event this should change, the following terms apply. DSHS Confidential Information may be stored on Portable Media as part of a Contractor's existing, documented backup process for business continuity or disaster recovery purposes. Such storage is authorized until such time as that media would be reused during the course of normal backup operations. If backup media is retired while DSHS Confidential Information still exists upon it, such media will be destroyed at that time in accordance with the disposition requirements below in Section 8 *Data Disposition*.
 - (2) Data may be stored on non-portable media (e.g. Storage Area Network drives, virtual media, etc.) as part of a Contractor's existing, documented backup process for business continuity or disaster recovery purposes. If so, such media will be protected as otherwise described in this exhibit. If this media is retired while DSHS Confidential Information still exists upon it, the data will be destroyed at that time in accordance with the disposition requirements below in Section 8 *Data Disposition*.
- i. **Cloud storage.** DSHS Confidential Information requires protections equal to or greater than those specified elsewhere within this exhibit. Cloud storage of Data is problematic as neither DSHS nor the Contractor has control of the environment in which the Data is stored. For this reason:
- (1) Origami agrees that it will not store Data in this manner. In the event this should change, the following terms apply. DSHS Data will not be stored in any consumer grade Cloud solution, unless all of the following conditions are met:

Exhibits

- (a) Contractor has written procedures in place governing use of the Cloud storage and Contractor attests in writing that all such procedures will be uniformly followed.
 - (b) The Data will be Encrypted while within the Contractor network.
 - (c) The Data will remain Encrypted during transmission to the Cloud.
 - (d) The Data will remain Encrypted at all times while residing within the Cloud storage solution.
 - (e) The Contractor will possess a decryption key for the Data, and the decryption key will be possessed only by the Contractor and/or DSHS.
 - (f) The Data will not be downloaded to non-authorized systems, meaning systems that are not on either the DSHS or Contractor networks.
 - (g) The Data will not be decrypted until downloaded onto a computer within the control of an Authorized User and within either the DSHS or Contractor's network.
- (2) Data will not be stored on an Enterprise Cloud storage solution unless either:
- (a) The Cloud storage provider is treated as any other Sub-Contractor, and agrees in writing to all of the requirements within this exhibit; or,
 - (b) The Cloud storage solution used is FedRAMP certified.
- (3) If the Data includes protected health information covered by the Health Insurance Portability and Accountability Act (HIPAA), the Cloud provider must sign a Business Associate Agreement prior to Data being stored in their Cloud solution.

6. System Protection. To prevent compromise of systems which contain DSHS Data or through which that Data passes:

- a. Systems containing DSHS Data must have all security patches or hotfixes applied according to Contractor's risk assessment.
- b. The Contractor will have a method of ensuring that the requisite patches and hotfixes have been applied within the required timeframes.
- c. Systems containing DSHS Data shall have an Anti-Malware application, if available, installed.
- d. Anti-Malware software shall be kept up to date. The product, its anti-virus engine, and any malware database the system uses, will be no more than one update behind current.

7. Data Segregation.

- a. DSHS Data must be segregated or otherwise distinguishable from non-DSHS data. This is to ensure that when no longer needed by the Contractor, all DSHS Data can be identified for return or destruction. It also aids in determining whether DSHS Data has or may have been compromised in the event of a security breach. As such, one or more of the following methods will be used for data segregation.
 - (1) DSHS Data will be kept on media (e.g. hard disk, optical disc, tape, etc.) which will contain no non-DSHS Data. And/or,

Exhibits

- (2) DSHS Data will be stored in a logical container on electronic media, such as a partition or folder dedicated to DSHS Data. And/or,
- (3) DSHS Data will be stored in a database which will contain no non-DSHS data. And/or,
- (4) DSHS Data will be stored within a database and will be distinguishable from non-DSHS data by the value of a specific field or fields within database records.
- (5) When stored as physical paper documents, DSHS Data will be physically segregated from non-DSHS data in a drawer, folder, or other container.

b. When it is not feasible or practical to segregate DSHS Data from non-DSHS data, then both the DSHS Data and the non-DSHS data with which it is commingled must be protected as described in this exhibit.

8. Data Disposition. When the contracted work has been completed or when the Data is no longer needed, except as noted above in Section 5.b, Data shall be returned to DSHS or destroyed. Media on which Data may be stored and associated acceptable methods of destruction are as follows:

Data stored on:	Will be destroyed by:
Server or workstation hard disks, or Removable media (e.g. floppies, USB flash drives, portable hard disks) excluding optical discs	Using a “wipe” utility which will overwrite the Data at least three (3) times using either random or single character data, or Degaussing sufficiently to ensure that the Data cannot be reconstructed, or Physically destroying the disk
Paper documents with sensitive or Confidential Information	Recycling through a contracted firm, provided the contract with the recycler assures that the confidentiality of Data will be protected.
Paper documents containing Confidential Information requiring special handling (e.g. protected health information)	On-site shredding, pulping, or incineration
Optical discs (e.g. CDs or DVDs)	Incineration, shredding, or completely defacing the readable surface with a coarse abrasive
Magnetic tape	Degaussing, incinerating or crosscut shredding

9. Notification of Compromise or Potential Compromise. The actual compromise of DSHS shared Data must be reported to the DSHS Contact designated in the Contract within seventy-two (72) hours of discovery. If no DSHS Contact is designated in the Contract, then the notification must be reported to the DSHS Privacy Officer at dshsprivacyofficer@dshs.wa.gov. Contractor must also take actions to mitigate the risk of loss and comply with any notification or other requirements imposed by law.

10. Data shared with Subcontractors. If DSHS Data provided under this Contract is to be shared with a subcontractor, the Contract with the subcontractor must include all of the data security provisions within this Contract and within any amendments, attachments, or exhibits within this Contract. If the

Exhibits

Contractor cannot protect the Data as articulated within this Contract, then the contract with the sub-Contractor must be submitted to the DSHS Contact specified for this contract for review and approval.

Exhibits

Exhibit B: Data Licensing Statement

1. Justification and Authority for Data Sharing:

DSHS currently uses the Origami Risk Platform across several offices for varying purposes. The Confidential Information to be shared under this DSA is shared for the purpose of administering, configuring, and providing technical support for DSHS’s use of the Origami Risk Platform.

2. Purpose / Use / Description of Data:

- a. The purpose of this DSA is to provide terms and conditions under which DSHS will allow the restricted use of its Data to the Data Recipient, and under which the Data Recipient may receive and use the Data. This DSA ensures that Data is provided, protected, and used only for purposes authorized by state and federal law governing such Data use.
- b. DSHS has two automatic feeds of data into the Origami Risk Platform. They supply information on employees that allow DSHS to assign and automate notifications, tasks, another other business process flows (workflows). DSHS sends the data to Origami who then pulls it into the system for DSHS use on a weekly basis.

Data	Use of data
HRMS feed	Provides HRMS employee data to the DSHS instance of the Origami Risk Platform, including name, position, title, job site, dob, home address, etc.
AD feed	Provides active directory data to the DSHS instance of the Origami Risk Platform, including name, email address, supervisor, etc.

- c. **Permissible Use:** Data Recipient may only use the Data for the purposes of administering, configuring, and providing technical support directly related to DSHS’s use of the Origami Risk platform.

d. Description of Data:

Use:	Confidential data included but not limited to:
Major Incident Reporting (AP 9.01)	May include names of clients/patients or medical information.
Enterprise Risk Register	Does not contain confidential data
Tort Claim and Litigation Management	May contain patient names and other PII, medical information, Attorney-Client Privileged information, Attorney-Client Work Product, social security numbers,

Exhibits

	personal employee information (home address, phone, dob, etc.)
Workers Compensation/Industrial Insurance	Contains confidential Labor & Industries workers' compensation file information, medical information, reasonable accommodation data, social security numbers, personal employee information (home address, phone, dob, etc.)
EEOC and HRC claims	May contain patient names and other PII, medical information, Attorney-Client Privileged information, Attorney-Client Work Product, social security numbers, personal employee information (home address, phone, dob, etc.)
Ethics and Whistleblower complaints	May contain patient names and other PII, medical information, Attorney-Client Privileged information, Attorney-Client Work Product, social security numbers, personal employee information (home address, phone, dob, etc.), whistleblower data
HR Investigations (beginning 2026)	May contain patient names and other PII, medical information, Attorney-Client Privileged information, Attorney-Client Work Product, social security numbers, personal employee information (home address, phone, dob, etc.), whistleblower data, criminal conviction and/or non-conviction data
HRMS feed (provides HRMS employee data to the DSHS instance of the Origami Risk Platform)	Confidential employee information such as DOB, home address, phone, social security number, work history, and salary.
AD feed (provides active directory data to the DSHS instance of the Origami Risk Platform)	Not likely to include any confidential information.

Exhibits

**Exhibit C – Statement of Work
Origami Risk Order Form #20251228**

CONTACT INFORMATION	
Client: State of Washington, Department of Social & Health Services Address: Washington State Department of Social and Health Services 1115 Washington Street PO BOX 45020 Olympia, WA 98501-5891	Bill To Contact: Jamie Gerkin Bill To Email: jamie.gerken@dshs.wa.gov Is purchase order (PO) required? <input type="checkbox"/> Upon entering into this Order Form, please send any Pos, vendor registration links or tax exemption certificates to finance@origamirisk.com

SUBSCRIPTION DETAILS
Subscription Term: 36 Months Effective Date: 2025-12-28

RECURRING SUBSCRIPTIONS – LICENSES	
Subscription	Quantity / Functionality Purchased
RMIS	Functionality Selected
Full User(s)	31 User(s)
Light User(s)	182 User(s)
SMS Messaging	1 blocks of 10,000 SMS Messages
Enterprise-Wide Record Entry	Up to 5000 records added per year
Reviewer User License(s)	250 Special License(s)*
Origami API Access	Up to 5,000 call(s) per day
GRC – Enterprise License – Enterprise Risk Management (ERM)	Up to 999 User(s)
ERM User License(s)	24 Special License(s)**
Annual Total: \$287,029.00	

RECURRING SUBSCRIPTIONS – HOSTING	
Subscription	Quantity / Functionality Purchased
Hosting, Network & Storage	Up to 15 GBs of Database Size
Free Non-Searchable File Attachment Storage	Includes 100 GBs of Non-Searchable file storage
Additional Non-Searchable File Attachment Storage	100 Additional GBs of Non-Searchable File Attachment Storage
Additional Tenant	1 Additional Production Tenant(s) Selected
Annual Total: \$44,275.00	

RECURRING SUBSCRIPTIONS – DATA PROCESSING	
Subscription	Quantity / Functionality Purchased
HR Employee Demographic Import	HRMS Employee Update Feed
HR Employee Demographic Import	HR Active Directory New Employee Import
Annual Total: \$11,500.00	

RECURRING SUBSCRIPTIONS – Client Support	
Subscription	Quantity / Functionality Purchased

Exhibits

Client Support Tier 3	Selected Client Support tier includes support resourcing based on up to 10 hours of Client Support services per month beginning on the Effective Date.
Annual Total: \$27,500.00	
Annual Fees (before discount): \$370,304.00	
Discount (applied to \$370,304.00): (\$104,113.75)	
Total Annual Fees: \$266,190.25	

BILLING DETAILS AND ADDITIONAL TERMS

This Order Form is effective as of the Effective Date (as identified above) for the purchase of the subscription services listed above from Origami Risk LLC (“Origami”). This Order Form is subject to all the terms and conditions of the Contract between DSHS and Origami, designated by DSHS as Contract #2623-67989 (the “Contract”). To the extent the Contract does not contemplate order forms, this Order Form will be deemed a Statement of Work for purposes of the Contract. This Order Form will be deemed a part of the Contract. Origami and DSHS agree that the term of the Contract shall be extended through the duration of the term of this Order form.

Fees for the first year of recurring subscription fees and all one-time fees under this Order Form will be invoiced and due upon execution of this Order Form. Fees for ongoing contract years are due annually upfront on each anniversary date thereafter. All fees are subject to applicable sales tax, which will appear separately on each invoice. All travel costs and expenses will be pre-approved by Client in writing and billed to Client as incurred.

Service descriptions and service-specific terms and conditions are set forth at origamirisk.com/serviceterms, which are hereby incorporated by reference in the form available at such link as of the Effective Date. Additional professional services may be set forth in other Statements of Work as agreed between the parties.

*** Reviewer User License(s)** – These licenses have access to all the features and capabilities of the Service under the base functionality selected above, including those features utilized reviewing/investigating claims, incidents, and complaints. User’s functional permissions are handled through system security. These licenses have access to Extended Functionality features.

**** ERM License(s)** – These licenses have access to all the features and capabilities of the Service under the base functionality selected above, including those features utilized in the administration of Client’s Enterprise Risk Management program. User’s functional permissions are handled through system security. These licenses have access to Extended Functionality features.

ORDER FORM APPROVAL

The undersigned agree to this Order Form.

ORIGAMI RISK LLC

STATE OF WASHINGTON, DEPARTMENT OF SOCIAL & HEALTH SERVICES

By: _____

By: _____

Name: Ryan Dardis
(Print Name)

Name: _____
(Print Name)

Title: Chief Revenue Officer

Title: _____

Date:

Date: _____

Exhibits

Exhibit D - Service Level Agreement (SLA)

1. System Availability

Origami Risk will be available 99.5% of the time, excluding unavailability as a result of any Excluded Event (the "Availability Requirement"). This includes holidays, weekends, and non-business hours. It does not include planned downtime. In normal circumstances, Origami Risk will schedule downtime between 8:00 PM CT and 7:00 AM CT. Origami Risk will post system availability statistics quarterly.

"Excluded Event" means (i) scheduled maintenance windows of which Client is notified at least 24 hours in advance and which occur outside of normal business hours; (ii) scheduled repairs of not more than two hours duration in any one week period of which Client is notified at least four hours in advance and which occur outside of normal business hours; (iii) critical repairs including security updates where advance notice cannot be reasonably provided; (iv) interruptions caused by transmission errors, Internet service providers, vandalism, user error or other factors beyond Origami's or its direct service providers' reasonable control; or (v) interruptions caused by any act or omission of Client (including any employee, contractor, agent, customer, investor, consultant or third party user of Client or any of Client's affiliates who uses or accesses the service), including any failure or delay in the performance of its obligations or failure of Client's equipment or non-Origami software. The Availability Requirement applies only to Origami's production environment and not to Origami's staging environment.

2. Service Credits:

In the event there is a material failure of Origami's service to meet the Availability Requirement (a "Service Level Failure") in any calendar month, then Client shall have the following sole and exclusive remedy: Origami will provide Client with a service credit on the next annual invoice equal to the pro-rated charges for one (1) full day of the affected services (i.e., 1/30 of the monthly fee, assuming a thirty (30) day month) for each day during which there was a Service Level Failure in such calendar month (a "Service Credit"). For clarity, such Service Credit shall not include credit for hosting fees, data processing fees, professional services fees or any other prepaid bundled fees other than licensing fees.

If Client believes that it is entitled to receive Service Credits, Client shall notify Origami in writing within seven business days after the applicable calendar month with a description of the Service Level Failure and the date and time of such Service Level Failure. If Client does not notify Origami within such timeframe, then Client shall be deemed to have waived all claims with respect to such Service Level Failure (but not to any future Service Level Failure). Origami will make all determinations regarding Service Credits in its reasonable discretion.

For any given month, Client shall in no event be entitled to receive a Service Credit that exceeds 100% of its monthly license fees for such month. Client agrees that Service Credits are the sole and exclusive remedy for any Service Level Failure.

3. BACKUP AND RECOVERY

Origami currently backs up transactions every 15 minutes via incremental backups. A differential database backup is performed nightly and a full backup is performed weekly. Backups are stored off site via Amazon S3, which has multiple redundancy and 99.99999999% durability and 99.99% availability of objects over a given year. Periodic database restore tests are performed to validate that backups are valid. Origami retains weekly backups for a minimum of six months.

Exhibits

4. NOTICES

Two email subscription options are available to each Origami Risk user. These determine the type of communication that they will receive from Origami Risk.

- a. Emergency: Receive emails concerning outages and other system problems
- b. Maintenance: Receive emails concerning scheduled maintenance on the system.

In addition, any Origami Risk user can visit <http://status.origamirisk.com/> to view the current system status.

5. SERVICE REQUESTS

Origami Risk will respond to service-related incidents or issues within the following time frames:

Urgent Requests

An urgent request for service concerns a new development that significantly affects a major business task with no workaround. Client will request urgent support by sending an email to support@origamirisk.com with the word "Urgent" in the subject line. An urgent request made between 7:00 AM CT and 8:00 PM CT will typically be responded to immediately, and Client may also call any member of the Origami Risk support team directly. If Client does not receive a prompt response, Client may escalate by contacting any Origami Risk service or support employee or manager via contact information provided to Client. The target resolution time for an urgent issue is as soon as possible.

Normal Requests

A normal request for service is any service request that is not urgent. A normal service request will typically be responded to within one business day. Client will request support by sending an email to support@origamirisk.com. Client may also call or email any member of the Origami Risk support team directly.

6. SECURITY

Any access to Origami Risk requires a unique user id and password. Passwords must adhere to standard password security rules including minimum length and complexity. Origami Risk uses a role-based security model. Client is responsible for assigning and maintaining role, location, and coverage security for users. Client's system administrators can use the tools in Origami Risk to review and change security rights, edit the user profile, and reset the password. User passwords are encrypted in the Origami database using a SHA-256 hash algorithm.

System locks out user after five login attempts with an incorrect password. An administrative user must then reset the user's password and unlock the user account.

Origami Risk uses TLS v1.2 or higher for all communications over https. Origami databases are fully encrypted using 256-bit AES encryption.

Claim, Transaction, and Notes data sent to the Origami Risk SFTP site must be encrypted using at least 128 bits. Origami uses Open PGP for file encryption and can provide an encryption key to be used by the client. Origami Risk will keep the files on a secured files system in encrypted format except during the import process. When the import process is completed, unencrypted files are removed from the system.