




RECEIVED  
OCT 17 2019  
KITSAP PUBLIC HEALTH DISTRICT

 <p>Washington State Department of Social &amp; Health Services <i>Transforming lives</i></p>	<p><b>INTERLOCAL DATASHARE AGREEMENT</b></p> <p><b>eJAS Access for Home Visiting Services for DSHS-TANF WorkFirst Clients</b></p>	<p>DSHS Agreement Number: 1991-63245</p>	
<p>This Agreement is by and between the State of Washington Department of Social and Health Services (DSHS) and the Contractor identified below, and is issued pursuant to the Interlocal Cooperation Act, chapter 39.34 RCW.</p>		<p>Program Contract Number:  Contractor Contract Number:</p>	
<p>CONTRACTOR NAME Kitsap Public Health District</p>		<p>CONTRACTOR doing business as (DBA)</p>	
<p>CONTRACTOR ADDRESS 345 6th Street Suite 300 Bremerton, WA 98337-1866</p>		<p>WASHINGTON UNIFORM BUSINESS IDENTIFIER (UBI) 601-139-034</p>	<p>DSHS INDEX NUMBER  103543</p>
<p>CONTRACTOR CONTACT Yolanda Fong</p>	<p>CONTRACTOR TELEPHONE Click here to enter text.</p>	<p>CONTRACTOR FAX</p>	<p>CONTRACTOR E-MAIL ADDRESS yolanda.fong@kitsappublichealth.org</p>
<p>DSHS ADMINISTRATION Economic Services Administration</p>	<p>DSHS DIVISION Community Services Division</p>	<p>DSHS CONTRACT CODE 3000DC-91</p>	
<p>DSHS CONTACT NAME AND TITLE  Leslie Harmon WorkFirst Coordinator</p>		<p>DSHS CONTACT ADDRESS  2121 S State Street Tacoma, WA 98405</p>	
<p>DSHS CONTACT TELEPHONE  (253) 476-7030</p>	<p>DSHS CONTACT FAX  (253) 593-2233</p>	<p>DSHS CONTACT E-MAIL ADDRESS  harmonl@dshs.wa.gov</p>	
<p>IS THE CONTRACTOR A SUBRECIPIENT FOR PURPOSES OF THIS CONTRACT?  No</p>		<p>CFDA NUMBER(S)</p>	
<p>AGREEMENT START DATE  10/07/2019</p>	<p>AGREEMENT END DATE  06/30/2021</p>	<p>MAXIMUM AGREEMENT AMOUNT  No Payment</p>	
<p><b>EXHIBITS. The following Exhibits are attached and are incorporated into this Agreement by reference:</b>  <input checked="" type="checkbox"/> Data Security: Exhibit A – Data Security  <input type="checkbox"/> Exhibits (specify):</p>			
<p>The terms and conditions of this Agreement 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 Agreement, between the parties. The parties signing below represent they have read and understand this Agreement, and have the authority to execute this Agreement. This Agreement shall be binding on DSHS only upon signature by DSHS.</p>			
<p>CONTRACTOR SIGNATURE </p>	<p>PRINTED NAME AND TITLE Kerith Grellner, Administrator</p>	<p>DATE SIGNED 10/3/2019</p>	
<p>DSHS SIGNATURE  FOR</p>	<p>PRINTED NAME AND TITLE Charley Barron, CSD Contracts Officer</p>	<p>DATE SIGNED 10/3/19</p>	

## 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.
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.** At all times during the term of this Contract, the Contractor shall comply with all applicable federal, state, and local laws and regulations, including but not limited to, nondiscrimination laws and regulations.
6. **Confidentiality.**
- a. The Contractor shall not use, publish, transfer, sell or otherwise disclose any Confidential

## DSHS General Terms and Conditions

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 reasonable 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) When transporting six (6) or more records containing Confidential Information, outside a Secured Area, do one or more of the following as appropriate:
    - (a) Use a Trusted System.
    - (b) Encrypt the Confidential Information, including:
      - i. Encrypting email and/or email attachments which contain the Confidential Information.
      - ii. Encrypting Confidential Information when it is stored on portable devices or media, including but not limited to laptop computers and flash memory devices.
  - (5) Send paper documents containing Confidential Information via a Trusted System.
  - (6) Following the requirements of the DSHS Data Security Requirements Exhibit, if attached to this contract.
- c. Upon request by DSHS, at the end of the Contract term, or when no longer needed, 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.

## DSHS General Terms and Conditions

- 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 one (1) business day of discovery. Contractor must also take actions to mitigate the risk of loss and comply with any notification or other requirements imposed by law or DSHS.

- 7. **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.
- 8. **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.
- 9. **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.
- 10. **Inspection.** The Contractor shall, at no cost, provide DSHS and the Office of the State Auditor with reasonable access to Contractor's place of business, Contractor's records, and DSHS client records, wherever located. These inspection rights are intended to allow DSHS and the Office of the State Auditor to monitor, audit, and evaluate the Contractor's performance and compliance with applicable laws, regulations, and these Contract terms. These inspection rights shall survive for six (6) years following this Contract's termination or expiration.
- 11. **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 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.

- 12. **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.

## DSHS General Terms and Conditions

**13. 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.

**14. 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.

**15. 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. At DSHS's discretion, the Contract or Program Agreement may be renegotiated under the revised funding conditions.
- b. At 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.
  - (1) 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.
  - (2) 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.
  - (3) 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.
- c. DSHS may immediately terminate this Contract 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.

**16. 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 – Interlocal Agreements:

**17. Disputes.** Both DSHS and the Contractor ("Parties") agree to work in good faith to resolve all conflicts

## DSHS General Terms and Conditions

at the lowest level possible. However, if the Parties are not able to promptly and efficiently resolve, through direct informal contact, any dispute concerning the interpretation, application, or implementation of any section of this Agreement, either Party may reduce its description of the dispute in writing, and deliver it to the other Party for consideration. Once received, the assigned managers or designees of each Party will work to informally and amicably resolve the issue within five (5) business days. If managers or designees are unable to come to a mutually acceptable decision within five (5) business days, they may agree to issue an extension to allow for more time.

If the dispute cannot be resolved by the managers or designees, the issue will be referred through each Agency's respective operational protocols, to the Secretary of DSHS ("Secretary") and the Contractor's Agency Head ("Agency Head") or their deputies or designated delegates. Both Parties will be responsible for submitting all relevant documentation, along with a short statement as to how they believe the dispute should be settled, to the Secretary and Agency Head.

Upon receipt of the referral and relevant documentation, the Secretary and Agency Head will confer to consider the potential options of resolution, and to arrive at a decision within fifteen (15) business days. The Secretary and Agency Head may appoint a review team, a facilitator, or both, to assist in the resolution of the dispute. If the Secretary and Agency Head are unable to come to a mutually acceptable decision within fifteen (15) business days, they may agree to issue an extension to allow for more time.

The final decision will be put in writing, and will be signed by both the Secretary and Agency Head. If the Agreement is active at the time of resolution, the Parties will execute an amendment or change order to incorporate the final decision into the Agreement. The decision will be final and binding as to the matter reviewed and the dispute shall be settled in accordance with the terms of the decision.

If the Secretary and Agency Head are unable to come to a mutually acceptable decision, the Parties will request intervention by the Governor, per RCW 43.17.330, in which case the governor shall employ whatever dispute resolution methods that the governor deems appropriate in resolving the dispute.

Both Parties agree that, the existence of a dispute notwithstanding, the Parties will continue without delay to carry out all respective responsibilities under this Agreement that are not affected by the dispute.

### **18. Hold Harmless.**

- a. The Contractor shall be responsible for and shall hold DSHS harmless from all claims, loss, liability, damages, or fines arising out of or relating to the Contractor's, or any Subcontractor's, performance or failure to perform this Agreement, or the acts or omissions of the Contractor or any Subcontractor. DSHS shall be responsible for and shall hold the Contractor harmless from all claims, loss, liability, damages, or fines arising out of or relating to DSHS' performance or failure to perform this Agreement.
- b. The Contractor waives its immunity under Title 51 RCW to the extent it is required to indemnify, defend, and hold harmless the State and its agencies, officials, agents, or employees.

### **19. Ownership of Material.** Material created by the Contractor and paid for by DSHS as a part of this Contract shall be owned by DSHS and shall be "work made for hire" as defined by Title 17 USCA, Section 101. This material includes, but is not limited to: books; computer programs; documents; films; pamphlets; reports; sound reproductions; studies; surveys; tapes; and/or training materials. Material which the Contractor uses to perform the Contract but is not created for or paid for by DSHS is owned by the Contractor and is not "work made for hire"; however, DSHS shall have a perpetual license to use

## DSHS General Terms and Conditions

this material for DSHS internal purposes at no charge to DSHS, provided that such license shall be limited to the extent which the Contractor has a right to grant such a license.

### 20. Subrecipients.

- a. General. If the Contractor is a subrecipient of federal awards as defined by 2 CFR Part 200 and this Agreement, the Contractor shall:
  - (1) Maintain records that identify, in its accounts, all federal awards received and expended and the federal programs under which they were received, by Catalog of Federal Domestic Assistance (CFDA) title and number, award number and year, name of the federal agency, and name of the pass-through entity;
  - (2) Maintain internal controls that provide reasonable assurance that the Contractor is managing federal awards in compliance with laws, regulations, and provisions of contracts or grant agreements that could have a material effect on each of its federal programs;
  - (3) Prepare appropriate financial statements, including a schedule of expenditures of federal awards;
  - (4) Incorporate 2 CFR Part 200, Subpart F audit requirements into all agreements between the Contractor and its Subcontractors who are subrecipients;
  - (5) Comply with the applicable requirements of 2 CFR Part 200, including any future amendments to 2 CFR Part 200, and any successor or replacement Office of Management and Budget (OMB) Circular or regulation; and
  - (6) Comply with the Omnibus Crime Control and Safe streets Act of 1968, Title VI of the Civil Rights Act of 1964, Section 504 of the Rehabilitation Act of 1973, Title II of the Americans with Disabilities Act of 1990, Title IX of the Education Amendments of 1972, The Age Discrimination Act of 1975, and The Department of Justice Non-Discrimination Regulations, 28 C.F.R. Part 42, Subparts C.D.E. and G, and 28 C.F.R. Part 35 and 39. (Go to <https://ojp.gov/about/offices/ocr.htm> for additional information and access to the aforementioned Federal laws and regulations.)
- b. Single Audit Act Compliance. If the Contractor is a subrecipient and expends \$750,000 or more in federal awards from any and/or all sources in any fiscal year, the Contractor shall procure and pay for a single audit or a program-specific audit for that fiscal year. Upon completion of each audit, the Contractor shall:
  - (1) Submit to the DSHS contact person the data collection form and reporting package specified in 2 CFR Part 200, Subpart F, reports required by the program-specific audit guide (if applicable), and a copy of any management letters issued by the auditor;
  - (2) Follow-up and develop corrective action for all audit findings; in accordance with 2 CFR Part 200, Subpart F; prepare a "Summary Schedule of Prior Audit Findings" reporting the status of all audit findings included in the prior audit's schedule of findings and questioned costs.
- c. Overpayments. If it is determined by DSHS, or during the course of a required audit, that the Contractor has been paid unallowable costs under this or any Program Agreement, DSHS may require the Contractor to reimburse DSHS in accordance with 2 CFR Part 200.



## DSHS General Terms and Conditions

### 21. Termination.

- a. Default. If for any cause, either party fails to fulfill its obligations under this Agreement in a timely and proper manner, or if either party violates any of the terms and conditions contained in this Agreement, then the aggrieved party will give the other party written notice of such failure or violation. The responsible party will be given 15 working days to correct the violation or failure. If the failure or violation is not corrected, this Agreement may be terminated immediately by written notice from the aggrieved party to the other party.
- b. Convenience. Either party may terminate this Interlocal Agreement for any other reason by providing 30 calendar days' written notice to the other party.
- c. Payment for Performance. If this Interlocal Agreement is terminated for any reason, DSHS shall only pay for performance rendered or costs incurred in accordance with the terms of this Agreement and prior to the effective date of termination.

### 22. Treatment of Client Property. Unless otherwise provided, the Contractor shall ensure that any adult client receiving services from the Contractor has unrestricted access to the client's personal property. The Contractor shall not interfere with any adult client's ownership, possession, or use of the client's property. The Contractor shall provide clients under age eighteen (18) with reasonable access to their personal property that is appropriate to the client's age, development, and needs. Upon termination of the Contract, the Contractor shall immediately release to the client and/or the client's guardian or custodian all of the client's personal property.

## Special Terms and Conditions

1. **Definitions Specific to Special Terms.** The words and phrases listed below, as used in this Contract, shall each have the following definitions:
  - a. "CSD" means the DSHS, Economic Services Administration (ESA), Community Services Division
  - b. "Contractor" means your organization that is entering into this agreement with DSHS. The Contractor will provide home visiting services to TANF/WorkFirst clients in order to do case management and will report client information to DSHS case managers electronically.
  - c. "Data" means any personal information, and/or other information accessed and gained while providing services carrying out this contract.
  - d. "Data Provider," as used in the Special Terms and Conditions of this Agreement, means the entity that is disclosing their Data for use by the Data Recipient for completion of this Agreement.
  - e. "Data Recipient," as used in the Special Terms and Conditions of this Agreement, means the entity that is receiving the Data from the Data Provider for purposes of completion of this Agreement.
  - f. "DSHS Contact" means the person whose name appears in the DSHS Contact box on page 1 of this contract.
  - g. "DSHS Client ID Number" is a number assigned to each client by DSHS. DSHS Client ID Number is the primary means of identification of the client. It could be found in the upper right corner of all DSHS correspondence to the client. On the DSHS letter it is called "Client ID #".
  - h. "e-JAS" means the web-based electronic JOBS Automated System for data collection.
  - i. "e-JAS component" means a WorkFirst activity scheduled for participant by the case manager in e-JAS.
  - j. "Home Visitation" means providing home visiting services in the permanent or temporary residence, or in other familiar surroundings, of the family receiving such services. See RCW 43.215.146.
  - k. "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.
  - l. "Portable Device" includes but is not limited to: smart phones, tablets, flash memory devices (e.g. USB flash drives personal media players), portable hard disks, and laptop/notebook/netbook computers if those computers may be transported outside of a Secured Area.
  - m. "Portable Media" includes, but is not limited to: Optical media (e.g. CDs, DVDs), magnetic media (e.g. floppy disks, tape, removable or external hard disk drives), or flash media (e.g. Compact Flash, SD, MMC).
  - n. "TANF" means Temporary Assistance to Needy Families. TANF provides temporary cash for families in need. Families on TANF assistance must participate in the WorkFirst Program.
  - o. "WorkFirst" means Washington State's welfare reform program created to assist financially struggling families on TANF assistance to find and keep jobs.

## Special Terms and Conditions

### 2. Purpose

The purpose of this agreement is to:

- a. Provide the terms and conditions by which DSHS will allow the Contractor limited access to the web-based JOBS Automated System (eJAS), hereinafter called eJAS. Guidelines for the access, use, transmission, and disclosure of the Data are provided to ensure the confidentiality of the Data is protection in accordance with law.
- b. Outline services to be provided by both agencies.
- c. Ensure that each agency cooperatively maintains communication and shares leadership responsibilities to ensure that available resources are utilized in an effective manner.
- d. Ensure cooperative arrangements between Kitsap Public Health District (KPHD) and the Bremerton CSO to provide services to pregnant families.
- e. This agreement applies to families who are receiving Temporary Assistance to Needy Families (TANF) and are identified as eligible to receive home visiting services.
- f. Each agency shall designate a representative who will be responsible for developing communication policies, the day-to-day operations of this program and resolution of issues pertaining to this agreement.

### 3. Contract Management

Contract Managers who will be responsible for day-to-day activities under this Agreement are as follows:

- a. For KPHD, the representative will be the Community Health Director, Yolanda Fong, [Yolanda.fong@kitsappublichealth.org](mailto:Yolanda.fong@kitsappublichealth.org), at 345 6<sup>th</sup> Street, Suite 300, Bremerton, WA 98337.
- b. For the Bremerton CSO the representative will be WorkFirst Social Services Supervisor, Christina Dobson, [dobsoci@dshs.wa.gov](mailto:dobsoci@dshs.wa.gov), 4710 Auto Center Blvd., Bremerton, WA 98312-3300.

### 4. Statement of Work

#### a. The CSO agrees to:

- (1) Collaborate with KPHD who will provide or refer to community partners to provide home visiting services to eligible pregnant families.
- (2) Make referrals of eligible pregnant families in need of home visiting services through KPHD.
- (3) Provide access and assistance to authorized KPHD staff, contractors and consultants in the observation and evaluation of services through KPHD.
- (4) Sign a mutual consent to exchange information with each family receiving Home Visiting Services.
- (5) Provide referrals and monitoring.

## Special Terms and Conditions

**b. KPHD agrees to:**

- (1) Assist the Bremerton CSO in moving WorkFirst families toward self-sufficiency goals.
- (2) Enroll families eligible for KPHD services or refer to community partners.
- (3) Provide presentations to Bremerton CSO staff about KPHD home visiting services.
- (4) Utilize the Department's eJAS system.

**5. Data Sharing**

Federal and state laws and regulations protect the information disclosed. The Contractor and/or Contractor's staff may not disclose, transfer, or sell any information to any other agency or person without specific written consent of DSHS or as allowed by law. Unauthorized disclosure of information is a gross misdemeanor, punishable by law. The Contractor is subject to the same standards and laws of confidentiality as is DSHS.

**a. Data Provisions:**

The Contractor or Contractor's staff may not release any information to any other agency or person without specific written consent except as provided by law. Unauthorized disclosure of information is a gross misdemeanor, punishable by law. The Contractor is subject to the same standards and laws of confidentiality as is DSHS.

**b. Data Access:**

In order to enter specific client data and review existing caseload information as described above, Agreement data shall be accessed through:

- (1) Personal computers attached to a Local Area Network (LAN) or the State Governmental Network (SGN) using a unique sign in login ID and a complex password, (changed every 90 days), or
- (2) Internet access secured through the Fortress server using a unique sign in login ID and a complex password, (changed every 90 days).
- (3) The Contractor shall limit access to the client data to authorized staff only whose duties specifically require access to such data in the performance of their assigned duties. Prior to making client data available, the Contractor shall notify all staff with access to data of the authorized use and disclosure requirements identified in section 9 – Confidentiality and Nondisclosure.
- (4) DSHS reserves the right to revoke, at any time, an individual's authorization to access information. DSHS shall send a written Notice Termination of Access, effective no later than date of receipt, to the effected individual. Such notice shall be made by certified mail.

## Special Terms and Conditions

**c. Description of data:**

DSHS shall give the Contractor Read Only Access unless otherwise specified to the following WorkFirst data elements in the eJAS program:

- (1) Caseload Client Search/List
- (2) Demographics
- (3) Component History
- (4) Components
  - (a) BE, Basic Education
  - (b) CC, Caring for a Child of a WorkFirst participant
  - (c) CE, Comprehensive Evaluation
  - (d) General Questions Section
    - i. College Evaluation Section
    - ii. ESD Employment Plan Section
    - iii. DSHS Final Decision
  - (e) CJ, Community Jobs, Write
  - (f) ES, ESL
  - (g) FT, Full-time Employment, Write
  - (h) GE, General Education
  - (i) HS, High School
  - (j) HW, High Wage or High Demand
  - (k) IT, Intensive In-home Services
  - (l) JS, Job Search
  - (m) JT, Job Skills Training,
  - (n) JP, Job Preparation when available
  - (o) LP, LEP Pathway
  - (p) OT, On the Job Training
  - (q) PE, Pre-employment Training

## Special Terms and Conditions

- (r) PI, Pregnancy to Employment
- (s) PP, Protective Payee
- (t) PR, Processing Referral Back
- (u) PS, Post-employment, Write
- (v) PT, Part-time Employment, Write
- (w) PU, PRUCOL Activities
- (x) RA, Referred to Community Colleges
- (y) RB, Referred Back,
- (z) RI, Job Search Preparation
- (aa) RO, Other Referral
- (bb) RS, Retention Services, Write
- (cc) RT, Referral to Tribal Services
- (dd) RZ, Referral to Community Colleges, PE/HW
- (ee) SA, Sanction
- (ff) TP, Teen Parent Barrier Removal
- (gg) VE, Vocational Education
- (hh) VU, Vocational Unapproved
- (ii) WC, Community Works
- (jj) WE, Work Experience, Write
- (kk) XB, Applying for SSI or other benefits
- (ll) XC, No child care available
- (mm) XD, In a Division of Vocational Rehabilitation plan
- (nn) XH, Homeless
- (oo) XJ, Learning Disability Services
- (pp) XM, Medical Treatment
- (qq) XP, Parenting Skills
- (rr) ZA, 55 or older caretaker relative

## Special Terms and Conditions

- (ss) ZB, Caring for an adult with disabilities
- (tt) ZC, Caring for a Child with Special Needs
- (uu) ZD, Adult with severe and chronic disabilities or applying for SSI
- (5) Individual Responsibility Plans
- (6) Employment History
- (7) Notes as follows:
  - (a) Non-Special Records: Read for monitoring purposes as approved by DSHS
  - (b) Assessment: Read for monitoring purposes as approved by DSHS
  - (c) Case Staffing: Read for monitoring purposes as approved by DSHS
  - (d) Whole Family Services: Read for monitoring as approved by DSHS
- (8) DSHS Funding/Payment History
- (9) Message Center/e-Message: Write
- (10) Follow-up Messages: Write
- (11) Non-Special Records WorkFirst Reports/Ad hoc Reports: Write
- (12) Frequently Asked Questions (FAQ)
- (13) Success Plan
- (14) Subcategory Funding Information: All except for Counseling (64), Medical Exams (37), and Testing Diagnostic (34)
- (15) Education and Training Worksheet
- (16) Any common data elements developed jointly needed to perform the duties of the WorkFirst Program.

### d. 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 one (1) business day of discovery. Contractor must also take actions to mitigate the risk of loss and comply with any notification or other requirements imposed by law or DSHS.

## 6. EJAS Reporting Requirements

The Contractor shall provide the services and staff, and otherwise do all things necessary for or incidental to eJAS reporting, as set forth below:

## Special Terms and Conditions

- a. Complete training on use of eJAS, to be provided by DSHS staff, prior to use of the system and follow all system rules.
- b. Use the Contractor Caseload screen to:
  - (1) Accept or reject each referral within 3 business days of receipt

### 7. Contractor Staff Who Have Access to Data

- a. The Contractor shall limit client information to staff whose duties specifically require access to such data in the performance of their assigned duties.
- b. The Contractor shall ensure that all staff/vendors/sub-contractors with access to client information sign the ESA Nondisclosure of Confidential Information Agreement form provided by the Contact person whose name appears in the DSHS Contact box on page 1 of this contract.
- c. The Contractor shall retain the original signed Nondisclosure of Confidential Information Agreement forms signed by staff/vendors/sub-contractors on their premises and send a scanned copy of the signed forms to the Contact person whose name appears in the DSHS Contact box on page 1 of this contract.
- d. The Contractor shall train all staff with access to client information on client data use and disclosure requirements prior to making that information available.
- e. The Contractor shall keep a record of staff training to be available for inspection upon request of the DSHS Contact person whose name appears in the DSHS Contact box on page 1 of this contract.
- f. To request access for new staff, the Contractor shall notify the DSHS contact person listed on page one, and provide the contact with a PDF copy of original Nondisclosure of Confidential Information Agreement completed and signed by that new staff. The Contractor must immediately notify the DSHS contact person listed on page one when any staff with access to the website is terminated from employment with the Contractor.

### 8. Limitations on Use of Data

The Contractor may use personal data and other data gained by reason of this agreement only for the purpose of this agreement. If the Data and analyses generated by Data Recipient contain personal information about DSHS clients, then any and all reports utilizing these Data shall be subject to review and approval by the Data Provider prior to publication in any medium or presentation in any forum.

### 9. Security of Data

- a. The Contractor shall ensure each employee signs a Notice of Nondisclosure form provided by DSHS to acknowledge the data access requirements prior to DSHS granting Access. DSHS will give access only to data necessary to the performance of this agreement. The Contractor shall provide, for each employee, the PDF copy of signed Notice of Nondisclosure to the DSHS contact person listed on page one and retain the signed originals of Notice of Nondisclosure forms on file for monitoring purposes. The Contractor must remind employees of the nondisclosure requirements and make available to DSHS upon request evidence that they have reminded all employees with access to data of the limitations, use or publishing of data.



## Special Terms and Conditions

- b. Violations of the Nondisclosure provisions of this agreement may result in criminal or civil penalties. Violation is a gross misdemeanor under RCW 74.04.060 Records, confidential – Exceptions - Penalty, punishable by imprisonment of not more than one year and/or a fine not to exceed five thousand dollars.
- c. If the Contractor chooses to retain hard copies of clients' information obtained under this Agreement, the Contractor shall maintain all hard copies of information in a locked filing cabinet when not in use and only authorized users shall have the key.
- d. When the Contractor is required to retain any information, document, application or consent identified in this agreement, the Contractor may maintain such information, document, application or consent in either electronic format, hardcopy format, or both. The storage of clients' personal information on personal or company issued portable devices/media for the provision of services under this contract is prohibited.
- e. The information provided under this agreement will remain the property of DSHS and will be promptly destroyed by the Contractor, or returned to the DSHS, when the work for which the information was required, as fully described herein, is completed.
- f. The Contractor is responsible for the cost of mitigating any loss of DSHS data that results from a confidentiality breach caused by the Contractor.

### 10. Confidentiality and Nondisclosure

- a. The data to be shared under this agreement is confidential in nature and is subject to state and federal confidentiality requirement that bind the Contractor, and its employees to protect the confidentiality of the personal information contained in ESA data. The Contractor shall protect information according to federal and state laws including the following incorporated by reference.

Chapter 74.04 RCW General Provision- Administration

Chapter 42.56 RCW Public Records Act

- b. The Contractor shall have adequate policies and procedures in place to ensure compliance with confidentiality requirements, including restrictions on re-disclosure.
- c. The Contractor shall not disclose, transfer, or sell any data as described in this agreement to any party in whole or in part, except as provided by law, or to any individual or agency not specifically authorized by federal or state law, rule or regulation.
- d. The Contractor's staff shall not re-disclose the data unless specifically authorized in this agreement or as allowed by law.
- e. The Contractor must obtain a signed Notice of Nondisclosure; DSHS form 03-374D, from all employees with access to the data to remind them of the limitations, use or publishing of data. The Contractor shall retain a copy on file for monitoring purposes on their premises.

## Special Terms and Conditions

### 11. Criminal History Background Checks

#### a. The Contractor Must:

Require a DSHS executed criminal background check for each employee and volunteer who will provide direct, one-on-one services to DSHS clients under this contract.

#### b. The Contractor must:

- (1) Immediately obtain a Nondisclosure statement DSHS form 03-374D and Background authorization DSHS form 09-653. Section 2 on the Background authorization form must be completed and signed by the new employee or volunteer. Email or fax to the DSHS Contract Contact listed on page one of this contract completed 03-374D and 09-653 forms, to request a background inquiry from the Background Check Central Unit (BCCU.)
- (2) Require if the employee has lived outside the State of Washington at any time during the past three years, an FBI background check must be completed which requires that the employee be fingerprinted.
- (3) Provide the DSHS contract contact listed on page one (1) of this contract with a list of employees, subcontractors and/or volunteers who will be providing direct, one-on-one services to DSHS clients. Send an updated list to the DSHS contract contact when there are changes in personnel providing direct, one-on-one client services under this contract.
- (4) Verify that for personnel who have a criminal record that the crime is not "disqualifying" as described on the DSHS Secretary's List of Crimes & Negative Actions. Personnel with a disqualifying crime are prohibited from providing direct, one-on-one services to DSHS clients under this contract. The Contractor can review what crimes are "disqualifying" as listed in the following link to the DSHS Secretary's List of Crimes & Negative Actions:

<https://www.dshs.wa.gov/sesa/background-check-central-unit/disqualifying-list-crimes-and-negative-actions>

#### c. DSHS Contract Contact listed on page one of this contract will receive the background check results and will determine if the applicant "passed" the background check. DSHS will notify the Contractor if Contractor staff or volunteers:

- (1) Have a record of disqualifying crime(s). The Contractor shall not hire or retain, directly or by contract, any individual having direct contact with vulnerable adults to work under this contract if the individual has a record of disqualifying crime(s).
- (2) In the case of an employee or volunteer having a record of a past crime that is not a disqualifying crime, the Contractor will need to consider character, competence and suitability of this individual. The contractor would then weigh the risks before allowing them to have unsupervised access to DSHS clients.

#### d. Copy of Criminal Background Check result is not provided to the Contractor. Criminal Background Check results are kept confidential between DSHS and the Contractor's staff or volunteers.

#### e. Background Check results will remain in effect for the period of performance of the contract.

## Special Terms and Conditions

### 12. Hold Harmless

DSHS and the Contractor agree that each party will hold each other harmless of the acts or omissions of the other.

### 13. Payment

- a. DSHS will provide the information under this agreement at no charge to the Contractor. Each party shall be responsible for any expenses incurred in providing or receiving Data. In exchange for the receipt of data, the Contractor agrees to abide by the terms and conditions in this agreement.
- b. The Contractor will incur the responsibility of any costs in order to access client data. This includes any costs for hardware/software upgrades, and costs to improve any systems or processors that will enable the Contractor to access the data.
- c. There is no funding exchange in this agreement therefore financial audit requirements are not applicable.

### 14. Child Abuse and Health and Safety Concerns

In the delivery of services under this Contract, children's health and safety shall always be the first concern of the Contractor. The Contractor shall immediately report all instances of suspected child abuse to Child Protective Services at **1-866-END HARM**.

### 15. Insurance

- a. DSHS certifies that it is self-insured under the State's self-insurance liability program, as provided by RCW 4.92.130, and shall pay for losses for which it is found liable.
- b. The Contractor certifies that it is self-insured or insured through a risk pool and shall pay for losses for which it is found liable.

### 16. Contractor Information

The Contractor shall forward to the DSHS Contact person named on page 1 of this Contract (or successor) within ten (10) working days, any information concerning the Contractor's change of circumstances.

### 17. Change of Contractor Information

DSHS shall consider the Contractor business name, address, telephone number, fax number, and e-mail address to be as shown on the first page of this Contract. Changes in the Contractor's circumstances include change of business name, address, telephone number, fax number, e-mail address, business status, and names of staff that are current employees.

If the Contractor's address, telephone number, fax number, or e-mail address change, the Contractor shall provide **written notice** of the change(s) to the DSHS Contact as shown on the first page of this Contract **within ten (10) working days of the date of the change(s)**.

## Special Terms and Conditions

### 18. Contract Monitoring

DSHS may conduct on-site visits. The Contractor's records related to this agreement will be reviewed for compliance with the terms and conditions of this Contract. DSHS reserves all other rights of inspection as provided in the General Terms and Conditions of this Contract.

### 19. Contract Suspension

DSHS may take certain actions in the event the Contractor, or any of its partners, officers, directors, or employees, is investigated by a local, county, state or federal agency, for a matter which DSHS determines may adversely affect the delivery of services provided under this contract. DSHS may, without prior notice, either suspend the delivery of services or disallow the person(s) involved in the allegation(s) from providing services or having contact with clients pending final resolution of the investigation.

### 20. Dispute Resolution

Either party may submit a request for resolution of a Contract dispute (rates set by law, regulation or DSHS policy are not disputable). The requesting party shall submit a written statement identifying the issue(s) in dispute and the relative positions of the parties. A request for a dispute resolution must include the Contractor's name, address, and Contract number, and be mailed to the address listed below within 30 calendar days after the party could reasonably be expected to have knowledge of the issue in dispute.

DSHS/Community Services Division  
Attention: Contracts Unit  
PO Box 45470  
Olympia, WA 98504-5470

## 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 (<http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.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](http://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.

- 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.

2. **Authority.** The security requirements described in this document reflect the applicable requirements of Standard 141.10 (<https://ocio.wa.gov/policies>) of the Office of the Chief Information Officer for the state of Washington, 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/sesa/central-contract-services/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.

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 immediately:
  - (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.
  - (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.
  - (4) That passwords are significantly different from the previous four passwords. Passwords that increment by simply adding a number are not considered significantly different.

- 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) Not allowing the use of dial-up connections.
  - (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.
- k. Render the device unusable after a maximum of 10 failed logon attempts.

**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.** 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 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.** 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.** 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.** 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.** 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.** 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.
- g. **Data storage on portable devices or media.**

(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) 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) DSHS Data will not be stored in any consumer grade Cloud solution, unless all of the following conditions are met:
    - (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 within 3 months of being made available.
- 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,
  - (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:

<b>Data stored on:</b>	<b>Will be destroyed by:</b>
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 compromise or potential compromise of DSHS shared Data must be reported to the DSHS Contact designated in the Contract within one (1) business day 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](mailto: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 or DSHS.

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