RESOLUTION 2025-_053___

RE: Approval of the Indian Nation Program Agreement Data Share Agreement for the Automated Client Eligibility System (ACES) and Support Enforcement Management System (SEMS) with the State of Washington Department of Social and Health Services effective October 1, 2025 through September 30, 2028

WHEREAS the Upper Skagit Tribal Council is the duly elected governing body of the Upper Skagit Indian Tribe, a federally recognized Indian Tribe recognized pursuant to section sixteen of the Indian Reorganization Act of 1934, 25 U.S.C., Section 476, and

WHEREAS, the Personal Responsibility and Work Opportunities Reconciliation Act (PRWORA) of 1996 authorizes Federally Recognized Indian Tribes to administer Temporary Assistance for Needy Families (Tribal TANF) programs; and

WHEREAS, the Upper Skagit Tribe has operated a Tribal TANF program from 2007 and has approved operating the program through June 30, 2028; and

WHEREAS, the Upper Skagit Tribal Council is responsible for the operation, policy, and procedures of the Upper Skagit Tribal Temporary Assistance for Needy Families (TANF) program; and

WHEREAS, in order to operate the Upper Skagit Tribal T ANF Program, it is necessary to access TANF Program client data from and share TANF Program client data with the State of Washington, Department of Social and Health Services through the use of the Automated Client Eligibility System (ACES) and Support Enforcement Management System (SEMS); and

NOW THEREFORE BE IT RESOLVED, that the Upper Skagit Tribal Council approves the Indian Nation Program Agreement Amendment for the Automated Client Eligibility System (ACES) and Support Enforcement Management System (SEMS) with the State of Washington Department of Social and Health Services for the period of effective October 1, 2025 through September 30, 2028, and

BE IT FURTHER RESOLVED, that the Upper Skagit Tribal Council hereby authorizes the Tribal Council Chair and/or the Tribe's General Manager to sign any and all documents pertaining to the Indian Nation Program Agreement Data Share Agreement on behalf of the Tribe.

CERTIFICATION

As Secretary of the Upper Skagit Indian Tribal Council, I hereby certify that the foregoing resolution was approved at a Special Session of the Upper Skagit Tribal Council held on November 25, 2025, at which time a quorum was present and the resolution was passed by a vote of 6 *FOR*, Ø *AGAINST*, and Ø ABSTENTIONS.

ATTEST:

Jennifer R. Washington
Tribal Council Chairwoman

Marilyn M. Scott
Tribal Council Secretary

Washington State DEPARTMENT OF SOCIAL & HEALTH SERVICES

INDIAN NATION PROGRAM AGREEMENT DATA SHARE AGREEMENT ACES & SEMS WEB

DSHS Agreement Number: 2562-65192

This Program Agreement is by and between the State of Washington Department of Social and Health Services (DSHS) and the Indian Nation identified below, and is issued in conjunction with the DSHS and Indian Nation Agreement Regarding General Terms and Conditions, which is incorporated by reference.

Administration or Division Agreement Number

Indian Nation Agreement Number

DSHS ADMINISTRATION	DSHS DIVISION	DSHS INDEX NUMBER	CCS CONTRACT CODE
Economic Services Administration	Community Services Division	1329	3042NS-62

DSHS CONTACT NAME AND TITLE	DSHS CONTACT ADDRESS
Freda Cogger Tribal Relations Program Administrator	712 Pear Street Olympia, WA 98506

DSHS CONTACT TELEPHONE	DSHS CONTACT FAX	DSHS CONTACT E-MAIL
(360) 522-2155	Click here to enter text	coggefx@dshs.wa.gov

INDIAN NATION NAME	INDIAN NATION ADDRESS
Upper Skagit Tribe	25944 Community Plaza Way Sedro Woolley, WA 98284

INDIAN NATION CONTACT NAME: Doreen Maloney

INDIAN NATION CONTACT TELEPHONE	INDIAN NATION CONTACT FAX	INDIAN NATION CONTACT E-MAIL
(360) 854-7090	(360) 854-7004	doreenM@upperskagit.com

IS THE INDIAN NATION A SUBRECIPIENT FOR PURPOSES OF THIS PROGRAM AGREEMENT?	ASSISTANCE LISTING NUMBERS
No	

PROGRAM AGREEMENT START DATE	PROGRAM AGREEMENT END DATE	MAXIMUM PROGRAM AGREEMENT AMOUNT
10/01/2025	09/30/2028	No Payment

EXHIBITS. When the box below is marked with a check (✓) or an X, the following Exhibits are attached and are incorporated into this Indian Nation Program Agreement by reference:

☒ **Data Security: Exhibit A – Data Security Requirements**

☒ **Exhibits (specify): Exhibit B – Assurances & Certifications form, Exhibit C – Washington State Department of Social & Health Services – Notice of Nondisclosure, Exhibit D – DSHS Form 9-989 (Confidentiality Statement – Tribal Employee)**

By their signatures below, the parties agree to the terms and conditions of this Indian Nation Program Agreement and all documents incorporated by reference. No other understandings or representations, oral or otherwise, regarding the subject matter of this Program Agreement shall be deemed to exist or bind the parties. The parties signing below certify that they are authorized, as representatives of their respective governments, to sign this Program Agreement.

INDIAN NATION SIGNATURE	PRINTED NAME AND TITLE	DATE SIGNED
[signature]	Jennifer R Washington, Chairman	11/25/25
DSHS SIGNATURE (CSD ACES) Michelle Malmoe	PRINTED NAME AND TITLE Michelle Malmoe, Contract Officer DSHS/ESA/Community Services Division	DATE SIGNED 11/26/2025
DSHS SIGNATURE (DCS SEMS) S Weigelt	PRINTED NAME AND TITLE Sarah Weigelt, Key Contracts Admin. DSHS/ESA Division of Child Support	DATE SIGNED 11/26/2025

Government to Government Relations

The Indian Nation named above and the State of Washington are sovereign governments. The Indian Nation and DSHS agree to these Special General Terms and Conditions for the purpose of furthering the government-to-government relationship acknowledged in the Centennial Accord and to achieve their mutual objectives of providing efficient and beneficial services to their people.

Nothing in this Agreement shall be construed as a waiver of tribal sovereign immunity.

Indian Nation General Terms and Conditions

1. **Definitions.** The words and phrases listed below, as used herein, shall each have the following definitions:

   a. "Agreement" means this Indian Nation and Department of Social and Health Services Agreement regarding General Terms and Conditions, any Program Agreements between the parties, and any other documents attached to or incorporated therein by reference. Unless plainly inconsistent with context, the term "Agreement" includes and refers to all such agreements collectively.

   b. "CCLS Chief" means the manager, or successor, of Central Contracts and Legal Services or successor section or office.

   c. "Central Contracts and Legal Services" means the DSHS central headquarters contracting office, or successor section or office.

   d. "CFR" means the Code of Federal Regulations. All references in this Agreement to CFR chapters or sections shall include any successor, amended, replacement regulation, or any successor or replacement federal Office of Management and Budget circular or regulation.as of the effective date of such successor, amended, or replacement regulation.

   e. "DSHS" or the "Department" means the state of Washington Department of Social and Health Services and its employees and authorized agents.

   f. "DSHS Representative" means any DSHS employee who has been delegated contract-signing authority by the DSHS Secretary or his/her designee.

   g. "Indian Nation" means the federally recognized Indian Tribe that has executed this Agreement and its designated subdivisions and agencies performing services pursuant to this Agreement and includes the Indian Nation's officers, employees, and/or agents. For purposes of any permitted Subcontract, "Indian Nation" includes any Subcontractor of the Indian Nation and the Subcontractor's owners, members, officers, directors, partners, employees, and/or agents.

   h. "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 numbers.

   i. "Program Agreement" or "Indian Nation and DSHS Program Agreement" means an agreement between the Indian Nation and DSHS which incorporates these General Terms and Conditions and contains special terms and conditions, including a statement of work to be performed by the Indian Nation and payment to be made by DSHS.

j. "RCW" means the Revised Code of Washington. All references in this Agreement to RCW chapters or sections shall include any successor, amended, or replacement statute, as of the effective date of such successor, amended, or replacement statute.

k. "Subcontract" means a separate contract between the Indian Nation and an individual or entity ("Subcontractor") to perform all or a portion of the duties and obligations that the Indian Nation is obligated to perform pursuant to any Program Agreement.

l. "Tribal Law" means the resolutions, law, codes, and/or ordinances enacted by the Indian Nation executing this Agreement, and any of the Indian Nation's tribal court decisions interpreting the same. All references in this Agreement to tribal law shall include any successor, amended, or replacement law, as of the effective date of such successor, amended, or replacement law.

m. "Tribal Authority" means any person or persons the Tribe has authorized through a letter or resolution designating contract signing authority.

n. "WAC" means the Washington Administrative Code. All references in this Agreement 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 Agreement 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 Indian Nation shall not assign this Agreement, or its rights or obligations, without obtaining prior written consent of DSHS. DSHS shall not recognize any assignment without such prior written consent. In the event that consent is given and this Agreement is assigned, all terms and conditions of this Agreement shall be binding upon the Indian Nation's successors and assigns.

4. **Compliance with Applicable Law.** At all times during the term of this Agreement, the parties shall comply with all applicable federal, tribal, and state laws and regulations.

5. **Confidentiality.**

a. The parties shall not use, publish, transfer, sell or otherwise disclose any Confidential Information gained by reason of any Program Agreement for any purpose that is not directly connected with the 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 parties shall protect and maintain all Confidential Information gained by reason of any Program Agreement against unauthorized use, access, disclosure, modification or loss. This duty requires the parties 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.

c. To the extent allowed by law, at the end of the Agreement term, or when no longer needed, the parties shall return Confidential Information or certify in writing the destruction of Confidential Information upon written request by the other party.

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. The Indian Nation must also take actions to mitigate the risk of loss and comply with any notification or other requirements imposed by law or DSHS.

6. **Culturally Relevant Services.** In performing work pursuant to any Program Agreement, the Indian Nation may develop and operate programs and deliver goods, services, and/or benefits in a manner that is culturally relevant and appropriate, and that is particularly suited to and/or particularly located for access by members of the Indian Nation's tribe or other tribes, in accordance with tribal laws and policies.

7. **Debarment Certification.** The Indian Nation, by signature to this Agreement, certifies that it is not presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participating in this Agreement by any Federal department or agency. The Indian Nation also agrees to include the above requirement into any subcontracts entered into in connection with the Indian Nation's duty to provide services under this Agreement.

8. **Disputes.** The Parties agree to work cooperatively to accomplish all of the terms of this Agreement, however, acknowledge that there may be instances in which either the Tribe or the Department has not complied with the conditions of this Agreement or that clarification is necessary to interpret provisions of this Agreement. In such an instance, the Tribe and the Department shall attempt to resolve the matter through discussions. If unsuccessful, the Tribe and the Department agree to refer the matter to non-binding mediation.

Either Party may request that a mediator be selected to assist in resolving any conflict or dispute. The mediator shall be jointly selected and shall be approved by both the Tribe and the Department. The cost of a mediator shall be born equally by the Tribe and the Department with neither Party using funds dedicated for the programs nor services contained in this Agreement

If the mediator cannot resolve the conflict or dispute, then the issue shall be brought before a Disputes Board. The Disputes Board shall consist of three (3) individuals; one (1) selected by the Tribe, one (1) selected by the Department and a third party to be chosen by the first two. The Disputes Board shall review all issues, concerns and conflicts with a goal to determine acceptable solutions for both parties. The decisions of the Disputes Board shall be final and binding on both parties. These dispute resolution procedures shall not modify or reduce the Indian Nation's rights to judicial proceedings.

9. **E-Signature and Records.** An electronic signature or electronic record of this Agreement or any other ancillary agreement shall be deemed to have the same legal effect as delivery of an original executed copy of this Agreement or such other ancillary agreement for all purposes.

10. **Hiring and Employment Practices.** The Indian Nation may give preference in its hiring and employment practices to members of the Indian Nation, or other Indian Nations, who have met all requirements for that position, including state requirements, and as may be provided by tribal laws and

policies.

11. **Independent Status.** For purposes of this Agreement, the Indian Nation acknowledges that the Indian Nation is not an officer, employee, or agent of DSHS or the State of Washington. The Indian Nation shall not hold out itself, or any of its employees as, nor claim status as, an officer, employee, or agent of DSHS or the State of Washington. The Indian Nation shall not claim for itself or its employees any rights, privileges, or benefits which would accrue to an employee of the State of Washington. The Indian Nation shall indemnify and hold harmless DSHS from all obligations to pay or withhold federal or state taxes or contributions on behalf of the Indian Nation or its employees.

12. **Inspection.** During the term of this Agreement and for one (1) year following termination or expiration of this Agreement, the Indian Nation shall provide reasonable access to the Indian Nation's place of business, relevant Indian Nation records, and client records, to DSHS and to any authorized agent of the state of Washington or the federal government in order to monitor, audit, and evaluate the Indian Nation's performance and compliance with applicable laws, and regulations that pertain solely to this Agreement.

13. **Insurance.** DSHS shall recommend insurance coverage in, and as appropriate to, individual Program Agreements. The Indian Nation may provide DSHS with its Certificate of Insurance or consult with DSHS Central Contracts and Legal Services at 360.664.6055, for guidance on appropriate levels of coverage. Certificates of Insurance may be mailed to: DSHS Central Contracts and Legal Services, PO Box 45811, Olympia, WA, 98504-5811.

14. **Maintenance of Records.** During the term of any Program Agreement and for six (6) years following termination or expiration of the Program Agreement, the parties shall maintain records sufficient to:

    a. Document performance of all acts required by any Program Agreement and applicable statutes, regulations, and rules;

    b. Substantiate the Indian Nation's statement of its organization's structure, tax status, administrative capabilities, and performance; and

    c. Demonstrate accounting procedures, practices, and records, which sufficiently and properly document all invoices, expenditures, and payments.

15. **Notification of Funding.** DSHS shall notify the Indian Nation of any projected or anticipated budget increase or decrease that affects any program or service contained in its Tribal Plan. This includes one-time surplus funding that could be obligated for unmet needs in Indian Nation services and program development.

16. **Operation of General Terms and Conditions.** These General Terms and Conditions are incorporated by reference into and shall govern and apply to each Program Agreement between the Indian Nation and DSHS in effect on or after the effective date of these General Terms and Conditions.

17. **Order of Precedence.** In the event of any inconsistency in these General Terms and Conditions and any Program Agreement the inconsistency shall be resolved by giving precedence to the applicable Program Agreement and its attachments over these General Terms & Conditions.

18. **Ownership of Material.**

    a. All materials of unique cultural significance shall be owned solely by the Indian Nation unless otherwise expressly agreed in the applicable Program Agreement.

    b. Materials created by the Indian Nation which the Indian Nation uses to perform the Program

Agreement (including without limitation books, computer programs, documents, films, pamphlets, reports, sound reproductions, studies, surveys, tapes and/or training materials) shall be owned by the Indian Nation, regardless of whether the materials are paid for in whole or in part by DSHS, except when such materials have been expressly identified within the applicable Program Agreement as belonging to DSHS.

c. If the parties agree within a Program Agreement that certain materials will be owned by DSHS, then the Indian Nation agrees that the materials so identified will either be deemed, to the extent applicable under 17 U.S.C.A. Section 101, "works made for hire," or the Indian Nation will assign to DSHS all rights, title and interest in and to such materials.

19. **Responsibility.** The Indian Nation shall be responsible for the acts or omissions of the Indian Nation and its agents, employees, and officers. DSHS shall be responsible for the acts or omissions of DSHS and its officers, employees, and agents.

20. **Severability.** The provisions of the Agreement are severable. If any provision of the Agreement, including any provision of any document incorporated by reference, is held invalid by any court that invalidity shall not affect the other provisions of the Agreement and the invalid provision shall be considered modified to conform to existing law and regulations.

21. **Survivability.** The terms and conditions contained in this Agreement 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: Confidentiality, Disputes; Inspection, Maintenance of Records, Ownership of Material, Termination for Default, Termination Procedure, and Treatment of DSHS Assets.

22. **Sovereign Immunity.** Nothing whatsoever in this Agreement constitutes or shall be construed as a waiver of the Indian Nation's sovereign immunity.

23. **Subcontracting.** Either party may subcontract services to be provided under Program Agreements. In any event, the Indian Nation shall remain ultimately responsible to DSHS and DSHS shall remain ultimately responsible to the Indian Nation for performance of all duties and obligations within these General Terms and Conditions and in any Program Agreement. Each party shall be responsible for the acts and omissions of its subcontractors.

24. **Subrecipients.** If, as a result of this Agreement, the Indian Nation is a subrecipient of federal awards as defined by 2 CFR Part 200, the Indian Nation shall comply with all applicable requirements of 2 CFR Part 200, including requirements regarding the reimbursement and the overpayment of unallowable costs.

25. **Program Agreement Renegotiation, Suspension, or Termination Due to Change in Funding**

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

a. The Program Agreement may be renegotiated under the revised funding conditions.

b. DSHS may give notice to the Indian Nation to suspend performance when DSHS determines that there is reasonable likelihood that the funding insufficiency may be resolved in a timeframe that would allow the Indian Nation's performance to be resumed prior to the normal completion date of any Program Agreement.

(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 the Indian Nation written notice to resume performance. Upon the receipt of this notice, the Indian Nation will provide written notice to DSHS informing DSHS whether it can resume performance and, if so, the date of resumption. For purposes of this subsubsection, "written notice" may include email.

(3) If the Indian Nation's proposed resumption date is not acceptable to DSHS and an acceptable date cannot be negotiated, DSHS may terminate any Program Agreement by giving written notice to the Indian Nation. The parties agree that the affected Program Agreement 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 the respective Program Agreement for services rendered prior to the retroactive date of termination.

c. DSHS may immediately terminate any Program Agreement by providing written notice to the Indian Nation. 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 any affected Program Agreement 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.

d. If funds are available, DSHS shall pay the Indian Nation for its reasonable costs that directly relate to termination of the Program Agreement. The parties may identify such costs in any Program Agreement. Such costs may include, but are not limited to, close-out costs, unemployment costs, severance pay, retirement benefits, reasonable profits, and termination costs associated with any subcontract.

26. Termination for Convenience. Except for agreements regarding personal services, either party may terminate any Program Agreement by giving the other party at least thirty (30) calendar days' written notice. The Indian Nation shall address such notice to: Central Contracts & Legal Service, PO Box 45811, Olympia, Washington 98504-5811. DSHS shall direct such notice to the Indian Nation Contact named in the first page of the applicable Program Agreement. If either party terminates any Program Agreement for convenience, the terminating party may pay an amount agreed to by the parties for actual costs incurred by the non-terminating party in performance of or in reliance on the Program Agreement.

27. Termination for Default.

a. The CCLS Chief may terminate any Agreement for default, in whole or in part, by written notice to the Indian Nation if DSHS has a reasonable basis to believe that the Indian Nation has:

(1) Failed to meet or maintain any requirement for contracting with DSHS, as specified in any Program Agreement or Tribal Plan;

(2) Failed to perform under any provision of the applicable Agreement;

(3) Negligently failed to ensure the health or safety of any client for whom services are being provided under any Program Agreement;

(4) Violated any applicable law, regulation, rule, or ordinance related to any Program Agreement; or

(5) Otherwise breached any provision or condition of the Agreement.

b. The CCLS Chief shall give the Indian Nation at least ten (10) business days' notice of DSHS' intent to terminate an Agreement, along with a summary of the facts supporting such termination. The Indian Nation shall have at least ten (10) business days in which to cure the default provided that if it

will reasonably take longer than ten (10) business days to cure the default, the cure period shall be a reasonable period agreed by the parties. In the event of a continuing pattern of default, the CCLS Chief will not be required to provide a cure period. The CCLS Chief is not required to offer a cure period if a client's health or safety is at risk, except this provision does not apply if the alleged default is an activity related to tribal law, custom, or practice.

c. The Indian Nation may terminate any Agreement for default, in whole or in part, by written notice to DSHS, if the Indian Nation has a reasonable basis to believe that DSHS has:

(1) Failed to meet or maintain any requirement for contracting with the Indian Nation;

(2) Failed to perform under any provision of the applicable Agreement;

(3) Violated any law, regulation, rule, or ordinance applicable to work performed under the Agreement; or

(4) Otherwise breached any provision or condition of the Agreement.

d. Before the Indian Nation may terminate an Agreement for default, the Indian Nation shall provide DSHS at least ten (10) business days written notice of the Indian Nation's intent to terminate the Agreement, along with a summary of the facts supporting such termination. DSHS shall have at least ten (10) business days in which to cure the default provided that if it will reasonably take longer than ten (10) business days to cure the default, the cure period shall be a reasonable period agreed by the parties. In the event of a continuing pattern of default by DSHS, the Indian Nation will not be required to provide a cure period.

28. **Termination Procedure.** The following provisions shall survive and be binding on the parties in the event any Agreement is terminated:

a. The Indian Nation shall cease to perform any services required by the Agreement as of the effective date of termination and shall comply with all reasonable instructions contained in the notice of termination.

b. If requested by DSHS within ten (10) days of termination, the Indian Nation shall, within a period not to exceed thirty (30) business days, deliver to DSHS all DSHS assets (property) in its possession. If the Indian Nation does not return DSHS property within thirty (30) business days of the Agreement termination, the Indian Nation shall be charged with all reasonable costs of recovery, including transportation and attorney's fees. The Indian Nation shall protect and preserve any property of DSHS that is in the possession of the Indian Nation pending return to DSHS.

c. DSHS shall be liable for and shall pay for those services authorized and provided through the date of termination. DSHS may pay an amount agreed to by the parties for partially completed work and services, if work products are useful to or usable by DSHS.

d. If the CCLS Chief terminates any Agreement for default, DSHS may withhold a sum from the final payment to the Indian Nation that is reasonable and necessary to protect DSHS against reasonably anticipated loss or liability. DSHS shall provide the Indian Nation with written notice of the amount withheld and the nature of the reasonably anticipated loss or liability. If it is later determined that the Indian Nation was not in default, DSHS shall pay the amount withheld to the Indian Nation within ten (10) business days of determining that the Indian Nation was not in default.

29. **Treatment of DSHS Assets.** Except as otherwise provided in any Program Agreement, title to all assets (property) purchased or furnished by DSHS for use by the Indian Nation during the Program Agreement term shall remain with DSHS. During the term of any Program Agreement, the Indian

Nation shall protect, maintain, and insure all DSHS property in the Indian Nation's possession against loss or damage.

30. **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 the Agreement. Only the CCLS Chief or designee has the authority to waive any term or condition of this Agreement on behalf of DSHS. Only the Tribe's official designee has the authority to waive any term or condition of this Agreement on behalf of the Indian Nation.

Special Terms and Conditions

1. Definitions Specific to Special Terms. The words and phrases listed below, as used in this Contract, shall have the following definitions.

   a. "ACES" means Automated Client Eligibility System.

   b. "Centennial Accord" means the agreement entered into between federally recognized tribes in Washington State and the State of Washington on August 4, 1989.

   c. "ESD" means the Employment Security Department of Washington State.

   d. ""Federal" means the United States of America.

   e. "NCP" means the Non-Custodial Parent.

   f. "Non-assistance" means a person who is not receiving public assistance.

   g. "Order State" means the state that issued the child support order.

   h. "Order Tribe" means the tribe that issued the child support order.

   i. "SEMS" means Support Enforcement Management System.

   j. "SGN" means Statewide Governmental Network.

   k. "SST" means Software Security Token, a type of two-factor authentication security software that is used to verify the identity of the user accessing database information, as defined in this agreement. The SST represents software placed on the user's computer.

   l. "State" means the state of Washington.

   m. "TANF" means Temporary Assistance to Needy Families.

   n. "Tribe" or "Tribal" means the entity performing services pursuant to this Indian Nation Program Agreement. This includes the Tribe's officers, directors, trustees, employees and/or agents unless otherwise stated in this Indian Nation Program Agreement. For purposes of this Indian Nation Program Agreement, the Tribe is not considered an employee or agent of DSHS.

2. Statement of Work

   a. Programs Receiving and Providing Data

      (1) The Indian Nation named on page one of this Data Share Agreement, herein referred to as the "Tribe", is the data recipient; contact information is listed on page one (1) under Indian Nation name.

      (2) DSHS is the data provider; contact information is listed on page one (1) under DSHS Administration.

b. Purpose

(1) The purpose of this agreement is to provide access to data for the limited purpose of assisting the Tribe in administering their Tribal Title IV-A TANF Program, DSHS shall provide the Tribe with access to:

(a) Automated Client Eligibility System (ACES)

(b) Support Enforcement Management System (SEMS)

(c) Employment Security Department (ESD) earnings and benefit information.

c. Description of Data

(1) ACES Data

(a) Designated employees or contracted staff of the Tribe shall have limited read–only web based secured access to ACES. DSHS will provide the Tribe's staff with electronic inquiry only access to ACES to determine eligibility and administer their Tribal Title IV-A TANF Program as authorized under RCW 74.04.050 (Department to Administer Public Assistance Programs), RCW 74.08A.040 (Indian Tribes Program Access) and 45 CFR 286 (Tribal TANF Provisions).

(2) SEMS Data

(a) Designated employees or contracted staff of the Tribe shall have limited read–only web based secured access to SEMS Intergovernmental cases where the Tribe is identified on the SEMS case. DSHS will provide the Tribe's staff with electronic inquiry only access to Child Support information for verification of child support cases, family relationships, and financial history as authorized under RCW 26.23.120. The IV-D data in SEMS that DCS may provide to a Tribal IV-A program is limited to the purposes provided for in 45 CFR 307.13.

Data shall not include any Federal Tax Information.

(3) Confidential Benefit and Wage Employment Data

(a) Designated employees or contracted staff of the Tribe shall have limited read-only web based secured access to confidential benefit and wage employment data collected through the Unemployment Compensation (UC) program.

(4) Data Classification - The State classifies data into categories based on the sensitivity of the data pursuant to the Security policy and standards promulgated by the Office of the state of Washington Chief Information Officer (OCIO) and included in OCIO Standard No. 141.10.

(a) The Data that is the subject of this DSA is classified as Category 3 – Confidential Information. Confidential information is information that is specifically protected from release or disclosure by law. It may include but is not limited to;

i. Personal Information about individuals, regardless of how that information is obtained;

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

d. Data Access or Transfer

(1) Unique user identification numbers and passwords obtained from DSHS are required in order for the authorized tribal staff to log on to ACES and SEMS.

(2) ACES/SEMS - Method of Access / Transfer

(a) Connection to ACES and SEMS will occur in one of the following two ways, either:

i. Through a workstation attached to the intergovernmental network (IGN), or

ii. DSHS will grant data access to ACES and SEMS for designated staff through a Virtual Private Network (VPN) connection provided by Washington Technology Solutions (WaTech), which uses software security tokens (SST) as a secondary factor of authentication, in addition to user identification and password.

(A) The Tribe will use SST's:

1. DSHS will provide a maximum of two (2) dual ACES-SEMS SST's to the Tribal TANF program free of charge. Each of the two (2) SST's will provide access to both ACES & SEMS.

2. Each of the SST's provided must be assigned to only one (1) individual, and access and use of the SST's shall not be shared between program employees or contracted staff.

(B) The Tribe may request additional dual ACES-SEMS SST's. In consideration for each additional SST, beyond the two (2) provided at no charge for each program, the Tribe will pay the per month charge DSHS incurs directly from Washington Technology Solutions (WaTech). As of the date of this Agreement, the charge is $9.00 per month per SST.

1. DSHS reserves the right to approve or deny a request made by the Tribe for additional dual ACES-SEMS SST.

(C) Payment and billing conditions for each additional SST:

1. The Tribe will prepay the annual cost of each additional SST, based on the state fiscal year (July 1st to June 30th), with payment due on July 1st each year.

a. DSHS/ESA Accounting Unit will bill the Tribe annually. The bill will describe the time period and charges assessed.

2. If an SST is issued mid-year, the cost will be prorated on a monthly basis and the Tribe shall pay the prorated annual lump sum payment within thirty (30) days after receipt of the SST.

a. DSHS/ESA Accounting Unit will bill the Tribe. The bill will describe the time period and charges assessed.

3. The Tribe shall provide payment for any additional SST provided to their Child Support or TANF program as follows:

a. Additional SST(s) provided to the TANF Program: The Tribe shall make

checks payable to "ESA DFFR" (Division of Finance and Financial Recovery) and reference "Upper Skagit Tribe Additional SST for TANF Program." The Tribe will send payments to: ESA DFFR Accounting Unit, P.O. Box 45445, Olympia, WA 98504-5445.

4. The Tribe will submit payments within thirty (30) days of the due dates referenced above.

   a. If payments are not received within the thirty (30) days of the due dates DSHS may deactivate the additional SST.

5. If the Tribe requests DSHS to deactivate an additional SST provided under this Agreement, DSHS will send applicable pro-rated refunds to the Tribe within thirty (30) days of DSHS receiving notification of the requested deactivation of the SST.

6. If a change in the associated cost DSHS/ESA incurs from WaTech per SST per month creates an underpayment or overpayment by the Tribe, DSHS/ESA will reconcile the twelve month charge and payments as follows:

   a. If the monthly payment is increased, DSHS/ESA will add the balance to the following year's 12 month charge.

   b. If the monthly charges decrease, DSHS/ESA will credit the balance toward the following year's 12 month charge.

e. Limitations on Use of Data

(1) The Tribe shall ensure that Tribal TANF employees or contracted staff persons have access to ACES and SEMS records only when necessary to fulfill the TANF requirements of their program.

(2) ACES – SEMS Security Monitoring

(a) The Tribe shall assign a person as a security monitor as a point of contact for ACES and SEMS.

(b) The security monitor will:

i. Route ACES or SEMS access requests through the DSHS Agreement Monitor, listed on page one (1), or by emailing the Tribal Access inbox at TribalAccessRQ@dshs.wa.gov.

ii. Assist in DSHS' efforts to monitor the security provisions of the DSA, by annually reviewing, completing and submitting the Assurances and Certifications form (see **Exhibit B**) to DSHS annually on:

(A) September 30

iii. Notify the DSHS Agreement Monitor, listed on page one (1), or by emailing the Tribal Access inbox at TribalAccessRQ@dshs.wa.gov immediately when employees or contracted staff that have access to ACES or SEMS terminate employment, transfer, or change duties.

iv. Perform the following actions upon an employee or contracted staff member (with SEMS

or ACES access) terminating employment, transferring, or changing duties:

(A) Promptly revoke access that is no longer needed or appropriate. Disable (revoke) all user IDs within five business days of the termination.

(B) Notify the employee or contracted staff member of his or her duty to keep information confidential.

(C) Disable (revoke) all access and user IDs immediately when an employee or contracted staff member is terminated for cause.

(D) Provide an updated **Exhibit B** (Assurances and Certifications) to the DSHS contact each time the users with SSTs change.

(c) Supervisors and/or managers must promptly report to the DSHS Agreement Monitor, listed on page one (1), or by emailing the Tribal Access inbox at TribalAccessRQ@dshs.wa.gov, duty changes or other personnel changes for which removal or reduction of computer system privileges is appropriate.

f. Frequency of Exchange

The exchange of data is accomplished through on-line transactions that may occur whenever the application is available.

3. Data Security

a. The Tribe shall secure the data provided in accordance with the requirements of **Exhibit A – Data Security Requirements.**

b. The Tribe shall exercise due care to protect data from unauthorized physical and electronic access. Due care includes establishing and maintaining security policies, standards, and procedures which detail:

(1) Access security, identification, and authentication;

(2) Network and workstation security;

(3) Premise security; and

(4) Sanctions for unauthorized use or disclosure of data.

c. To limit potential security breaches, DSHS may deactivate an SST if it is inactive for more than ninety (90) days.

d. DSHS provided data stored by the Tribe may not be accessed remotely — no use of external networks (e.g. the Internet) is allowed under this agreement.

e. The Tribe shall track the location of any copies or backups of data provided by DSHS. The method of tracking shall be sufficient to provide the ability to audit the protections afforded the copied data sets.

f. In the case of hardware failure, the Tribe must protect data by removing the hard drive before shipping equipment for repair.

4. Confidentiality and Nondisclosure

a. The Tribe shall protect information that is exempt from disclosure to the public or unauthorized persons under RCW 42.56 or other State, Federal or Tribal laws including the following, incorporated by reference:

(1) SEMS IV-D Data:

(a) RCW 42.56.230 Personal Information

(b) RCW 26.23.120 Information & Records – Confidentiality – Disclosure – Adjudicative Proceeding – Rules – Penalties

(c) 45 CFR 307.13 Security & Confidentiality for Computerized Support Enforcement Systems in Operation After October 1, 1997

(d) 20 CFR 603 Federal-State Unemployment Compensation (UC) Program, Confidentiality & Disclosure of State UC Information

(e) 42 USC 654(26) Safeguarding Confidential Information

(2) ACES Data:

(a) RCW 74.04.060 Records, Confidential – Exception – Penalty

(b) RCW 42.56.230 Personal Information

(c) 20 CFR 603 Federal-State Unemployment Compensation (UC) Program, Confidentiality & Disclosure of State UC Information

b. For Child Support Information contained in SEMS or the Title IV-D program, all information is private and confidential and shall be exempt from disclosure under RCW 42.56 or other Federal, State, or Tribal laws.

c. The Tribe shall have adequate policies and procedures in place to ensure compliance with confidentiality requirements.

d. The Tribe, its employees and contracted staff may use confidential Information or data gained by reason of this Agreement only for the purposes of this Agreement.

e. The Tribe shall not disclose nor transfer any information as described in this Program Agreement to any party in whole or in part, or to any individual or agency unless the information is exempt from disclosure under applicable State, Federal or Tribal laws.

f. All confidential information DSHS receives from the Tribe under this Agreement will be kept confidential by DSHS employees as required by State, Federal or Tribal laws.

g. Notice of Nondisclosure

(1) ACES: The Tribe must ensure each employee or contracted staff person with access to DSHS and/or ESD records or information, whether direct or indirect, annually reviews and signs the Washington State Department of Social and Health Services, Notice of Nondisclosure (Exhibit C Nondisclosure form) prior to DSHS granting access.

The Tribe shall retain a signed copy of the Nondisclosure form (**Exhibit C**) on file for monitoring purposes and made available for DSHS review upon request.

(2) SEMS: The Tribe must ensure that each employee or contracted staff person with SEMS access (including, but not limited to ESD information), annually reviews and signs the Federal and State data access requirements listed in the SEMS, Confidentiality Statement – Tribal Employee (DSHS 9-989) (**Exhibit D**), prior to DSHS granting access.

The Tribe shall retain a signed copy of the DSHS 9-989 form (**Exhibit D**) on file for monitoring purposes and made available for DSHS review upon request.

h. Notification of unauthorized disclosure:

The Tribe shall notify the Economic Services Administration (ESA) within one (1) business day of discovery of any unauthorized disclosure of ACES, SEMS or ESD information. Notification to ESA shall be done by sending an email to databreach@dshs.wa.gov and the DSHS Agreement Monitor listed on page one (1).

31. Disputes

Disputes shall be resolved in accordance with the current DSHS and Indian Nation Agreement on General Terms and Conditions between the Tribe and DSHS.

32. Termination

Termination of this Agreement shall be in accordance with the current DSHS and Indian Nation Agreement on General Terms and Conditions between the Tribe and DSHS.

APPROVED AS TO FORM BY THE OFFICE OF THE ATTORNEY GENERAL

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 Indian Nation and on a network outside the control of the Indian Nation. 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.

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 Indian Nation staff are not present to ensure that non-authorized staff cannot access it.

n. "Trusted Network" means a network operated and maintained by the Indian Nation, 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 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.

3. **Administrative Controls.** The Indian Nation 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 Indian Nation staff for violating that policy.

   b. If the Data shared under this agreement is classified as Category 4, the Indian Nation 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 Indian Nation 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 Indian Nation 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 agreement 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 agreement.

   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 Indian Nation's network (the Data stays within the Indian Nation's network at all times), enforce password and logon requirements for users within the Indian Nation'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 Indian Nation'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 agreement 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 Indian Nation 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 Indian Nation's staff. Indian Nation will notify DSHS staff immediately whenever an Authorized User in possession of such credentials is terminated or otherwise leaves the employ of the Indian Nation, and whenever an Authorized User's duties change such that the Authorized User no longer requires access to perform work for this Agreement.

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

   (1) Except where otherwise specified herein, DSHS Data shall not be stored by the Indian Nation on portable devices or media unless specifically authorized within the terms and conditions of the Agreement. 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 Indian Nation 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 an Indian Nation'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 an Indian Nation'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 Indian Nation 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) Indian Nation has written procedures in place governing use of the Cloud storage and Indian Nation attests in writing that all such procedures will be uniformly followed.

(b) The Data will be Encrypted while within the Indian Nation 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 Indian Nation will possess a decryption key for the Data, and the decryption key will be possessed only by the Indian Nation and/or DSHS.

(f) The Data will not be downloaded to non-authorized systems, meaning systems that are not on either the DSHS or Indian Nation 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 Indian Nation'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 Indian Nation 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 Indian Nation, 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:

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 compromise or potential compromise of DSHS shared Data must be reported to the DSHS Contact designated in the Agreement within one (1) business day of discovery. If no DSHS Contact is designated in the Agreement, then the notification must be reported to the DSHS Privacy Officer at dshsprivacyofficer@dshs.wa.gov. Indian Nation 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 Agreement is to be shared with a subcontractor, the Contract with the subcontractor must include all of the data security provisions within this Agreement and within any amendments, attachments, or exhibits within this Agreement. If the Indian Nation cannot protect the Data as articulated within this Agreement, then the contract with the sub-Contractor must be submitted to the DSHS Contact specified for this Agreement for review and approval.

Exhibit B

Exhibit B - ASSURANCES & CERTIFICATIONS
Upper Skagit Tribe &
State of Washington, Department of Social & Health Services
Indian Nation Program Agreement: 2562-65192 Data Share Agreement - ACES & SEMS Web

1. All Child Support and TANF program employees or contracted staff members comply with the data security provisions of the Data Share Agreement (DSA).
2. Our Tribe has policies in place to ensure confidentiality of ACES and SEMS (including, but not limited to Employment Security Department) data.
3. SEMS Access: All Child Support & TANF program employees or contracted staff members with access to SEMS (including, but not limited to ESD) records and information, whether direct or indirect, have annually signed the DSHS Form 9-989 (Confidentiality Statement – Tribal Employee) (Exhibit D), with a copy kept on file by the Tribe. Staff with direct access must also annually electronically acknowledge this agreement.
4. ACES Access: All Child Support & TANF program employees or contracted staff members with access to DSHS and/or ESD records & information, whether direct or indirect, have annually reviewed and signed the Washington State Department of Social and Health Services, Notice of Nondisclosure form (Exhibit C) with a copy kept on file by the Tribe.
5. Software Security Tokens (SST): Each of the SSTs provided by DSHS to the Tribe are assigned to only one (1) individual and access and use of the SSTs are not shared between program employees or contracted staff.

TANF Program

- Please identify the two (2) individuals with direct access to the ACES, SEMS & ESD databases through use of the two (2) Software Security Tokens provided by DSHS to the TANF program.

Child Support Program

- Please identify the individuals with direct access to the ACES, SEMS & ESD databases through use of the Software Security Tokens provided by DSHS to the Child Support program. Two tokens are provided at no cost to the Tribes; additional tokens are invoiced annually each State Fiscal Year.

TANF PROGRAM

By checking this box, I agree as the Tribe's Security Monitor for the TANF Program, that the Tribe is in compliance with the certification contained herein.*

Marlene Sayers 11/25/25

Security Monitor **Date**

***The Security Monitor for the TANF & Child Support programs may be the same person**

Exhibit C
WASHINGTON STATE DEPARTMENT OF SOCIAL AND HEALTH SERVICES NOTICE OF NONDISCLOSURE

As an employee of the **Upper Skagit Tribe**, Tribal TANF or Child Support Program, which is doing business with the Washington State Department of Social and Health Services (DSHS) under Agreement No. **# 2562-65192**, you may be given access to DSHS and Employment Security Department records and information that are deemed private and confidential by statute.

A. CONFIDENTIALITY OF INDIVIDUALLY IDENTIFIABLE DATA

1. Individually identifiable data is confidential and is protected by various state and federal laws (e.g. RCW 42.17, 70.02 and 74.04.060).
2. Confidential data includes all personal information (e.g., name, birth date, social security number) which may, in any manner, identify the individual.

B. USE OF CONFIDENTIAL DATA

1. Confidential data may be used only for purposes directly related to the operation of the contractor's program(s).
2. Any personal use of confidential data is strictly prohibited.
3. Access to data must be limited to those staff whose duties specifically require access to such data in the performance of their assigned duties.

C. DISCLOSURE OF CONFIDENTIAL DATA

1. Confidential data may be provided to the individual or their representative with a signed release of information.
2. Confidential data may be disclosed to other individuals or agencies only for purposes directly related to the administration of the contractor's program(s) pursuant to data sharing agreements.
3. Any disclosure of confidential data contrary to 1 and 2 above is unauthorized.

D. EMPLOYMENT SECURITY DEPARTMENT EARNINGS AND BENEFIT INFORMATION

1. As a non Employment Security Department (ESD) employee, I may be given access to records or information that is deemed private and confidential by statute. I may not make any unauthorized disclosure of private or confidential information about employers, clients/claimants or employees to any person or entity. Confidential information includes but is not limited to employee's wages or hours, unemployment insurance benefit records, and the North American Industry Classification System (NAICS) codes of individual employers. I may not disclose my password to other employees or allow others to access the ESD Mainframe System through my password and user identification. The unauthorized disclosure or abuse of information deemed private and confidential may subject me to a civil penalty of Five Thousand dollars ($5,000) and other applicable sanctions under federal and state law (RCW 50.13).

I have read and understand the above Notice of Nondisclosure.

Caniece Perez Printed Name	Case Worker Position
CPerez Signature Date	360-854-7030 canieceep@upperskagit.com Telephone Number/e-mail address

The above individual has been informed of the limitations, use or publishing of confidential data.

DOREEN K KAHNEY Supervisor's/Authorizing Staff's Printed Name	ESIT General Mgr Position
Doreen K Kahney 11/15/22 Supervisor's/Authorizing Staff's Signature Date	(360) 854-7090 doreenk@upperskagit.com Telephone Number/e-mail address

(TRIBAL TANF & CHILD SUPPORT PROGRAMS TO KEEP A COPY ON FILE)

Washington State Department of Social & Health Services
DCS Division of Child Support

Exhibit D
STATE OF WASHINGTON DEPARTMENT OF
SOCIAL AND HEALTH SERVICES DIVISION OF
CHILD SUPPORT (DCS)

Confidentiality Statement - Tribal Employee

I, _____, understand and agree that:

1. I may come into contact with confidential information from the Department of Social and Health Services (DSHS) administrations and from other departments. Confidential information may be electronic or paper and includes, but is not limited to: names, addresses, social security numbers, employee's wages or hours, unemployment benefit records, employer information, or any other information identifying individuals.
2. As a part of my job, I have access to confidential information to assist me in carrying out my duties. I may not use confidential information acquired through the Division of Child Support (DCS) for any purposes except for child support purposes and those directly associated with the scope of my employment. I may not use the Support Enforcement Management System (SEMS) or DCS access to other databases and information sources to access confidential information on: (a) myself, my friends, my relatives, or my co-workers; (b) for personnel purposes (e.g., hiring of staff), or (c) any other person unless the purpose is directly associated with child support or within the scope of my employment.
3. I will discuss confidential and personal DCS information only when necessary for a child support specific purpose.
4. I have reviewed and understand the terms of the DSHS Indian Nation Program Agreement(s) and agree to abide by it / them.
5. I understand that the Internal Revenue Service (IRS) requires that anyone who has access to income tax information and payments must be briefed on security procedures and instructions for protecting federal tax information. I understand that IRS returns and return information shall be confidential. If I have access to IRS information or payments, I will annually review the IRS Confidentiality and Security Exhibit in the DSHS Indian Nation Program Agreement. I am aware of the federal civil and criminal penalties associated with unauthorized disclosure or unauthorized inspection of federal tax information, found in IRC 7431, 7213, and7213A.
6. As a non Employment Security Department (ESD) employee, I may be given access to records or information that is deemed private and confidential by statute. I may not make any unauthorized disclosure of private or confidential information about employers, clients / claimants or employees to any person or entity. Confidential information includes but is not limited to employee's wages or hours, unemployment insurance benefit records, and the North American Industry Classification System (NAICS) codes of individual employers. I may not disclose my password to other employees or allow others to access the ESD Mainframe System through my password and user identification. The unauthorized disclosure or abuse of information deemed private and confidential may subject me to a civil penalty of Five Thousand dollars ($5,000) and other applicable sanctions under federal and state law (RCW 50.13).
7. After I leave my current position, DCS information obtained during my employment will remain confidential.
8. DCS records contain information from other government agencies. Wrongful disclosure of that information may lead to civil and criminal penalties.
9. My breach of any provision of this agreement may subject me to disciplinary action or penalties as defined by Tribal Codes, other applicable law, and policies or other instruction.

I agree to the terms of this confidentiality agreement, and I must annually review and sign this statement I understand that I will be given a copy of this form and a copy will be kept on file.

PRINT EMPLOYEE'S NAME	EMPLOYEE'S SIGNATURE	DATE
Caniece Perez	Cperez	11.25.25
PRINT SUPERVISOR'S NAME	SUPERVISOR'S SIGNATURE	DATE
DOREEN M MALONEY	Doreen M. Maloney	11-25-25