Washington State DEPARTMENT OF SOCIAL & HEALTH SERVICES

INDIAN NATION PROGRAM AGREEMENT DATA SHARE AGREEMENT ACES & SEMS WEB

DSHS Agreement Number: 0962-60682

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 an Indian Nation and DSHS 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	Division of Child Support	1315	3042NS-62

DSHS CONTACT NAME AND TITLE	DSHS CONTACT ADDRESS
Saundra Cheek Program Administrator	712 Pear St SE PO Box 9162 Olympia, WA 98207-9162

DSHS CONTACT TELEPHONE	DSHS CONTACT FAX	DSHS CONTACT E-MAIL
(360) 664-5025 Ext:	(360) 586-3274	scheek@dshs.wa.gov

INDIAN NATION NAME	INDIAN NATION ADDRESS
Puyallup Tribe of Indians	3009 E Portland Ave Tacoma, WA 98404-

INDIAN NATION FEDERAL EMPLOYER IDENTIFICATION NUMBER	INDIAN NATION CONTACT NAME
910955402	Kimberly Reynon-Spisak

INDIAN NATION CONTACT TELEPHONE	INDIAN NATION CONTACT FAX	INDIAN NATION CONTACT E-MAIL
(253) 680-5740 Ext:	(253) 896-1081	Kimberly.Reynon-Spisak@puyalluptribe.com

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

PROGRAM AGREEMENT START DATE	PROGRAM AGREEMENT END DATE	MAXIMUM PROGRAM AGREEMENT AMOUNT
6/1/2009	5/31/2012	No Payment

EXHIBITS. When the box below is marked with a check (4) or an X, the following Exhibits are attached and are incorporated into this Indian Nation Program Agreement by reference:

☒ Exhibits (specify): Exhibit A, Data Security Requirements

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		DATE SIGNED
Herman Dillon, Sr.	Herman Dillon, Sr., Chairman Puyallup Tribal Council	6/5/09
DSHS SIGNATURE	Kathleen Jenkins, Program Administrator DSHS/ESA/Division of Child Support.	DATE SIGNED 6/11/2009

1. Government to Government Relations

a. 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.

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

2. Definitions

a. "ACES" means Automated Client Eligibility System.

b. "Agreement" means this Indian Nation Data Share Agreement, including all documents attached or incorporated by reference.

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

d. "DSHS" means the Department of Social and Health Services of the State of Washington and its administrations, divisions, programs, employees, and authorized agents.

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

f. "Personal Information" means information identifiable to any person. This includes but is 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.

g. "RCW" means the Revised Code of Washington. All references in this Agreement or any Program Agreement to RCW chapters or sections shall include any successor, amended, or replacement statute.

h. "SEMS" means Support Enforcement Management System.

i. "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.

j. "SGN" means Statewide Governmental Network.

k. "Tribe" 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.

3. Statement of Work

a. Programs Receiving and Providing Data

(1) The Puyallup Tribe of Indians herein referred to as the "Tribe", is the data recipient; contact information is listed on page number one under Indian Nation Name.

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

b. Purpose

(1) To assist the Tribe in administering their Tribal Child Support 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 the Data

(1) SEMS Data

(a) Designated employees or contracted staff of the Tribe shall have limited read–only web based secured access to SEMS cases where the Tribe is coded on the SEMS case. DSHS will provide the Tribe's employees or contracted staff with electronic inquiry only access to Child Support information for verification of child support cases, family relationships, and financial history.

(2) ACES Data

(a) Designated employees or contracted staff of the Tribe shall have limited read–only web based secured access to ACES.

(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, which is accessed through SEMS.

d. Access to Data

(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) The Tribe will submit the IP numbers of the workstations that will need to access ACES and SEMS.

(3) <u>ACES/SEMS</u> - Method of Access / Transfer / Fob Replacement Cost

(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 employees or contracted staff through a Virtual Private Network (VPN) connection provided by the Department of Information Systems (DIS), which uses fobs as a secondary factor of authentication, in addition to user identification and password.

(b) DSHS will provide a maximum of two (2) dual ACES-SEMS fobs to the Tribal Child Support program free of charge. Each of the two (2) fobs will provide access to both ACES & SEMS.

i. Fobs lost or damaged by the Tribe may be replaced by DSHS. DSHS will charge the

Tribe $75.00 to replace a lost or damaged fob.

(c) The Tribe shall ensure that wage and UC information from the ESD is accessed only through SEMS (not through ACES).

e. Persons Having Access to Data

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

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

(a) Route ACES access requests through the ESA Information Technology Division Central Support Help Desk.

(b) Route SEMS access requests through the DCS Program Manager.

(c) Notify the ESA Information Technology Division Central Support Help Desk immediately when employees or contracted staff that have access to ACES terminate, transfer, or change duties.

(d) Notify the DCS Program Manager immediately when employees or contracted staff that have access to SEMS terminate employment, transfer, or change duties.

(e) Perform the following actions upon an employee or contracted staff member (with SEMS or ACES access) terminating employment, transferring, or changing duties:

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

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

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

(3) Supervisors and/or managers must promptly report to the security monitor duty changes or other personnel changes for which removal or reduction of computer system privileges is appropriate.

f. Frequency of the Data Exchange

The exchange of data is accomplished through on-line transactions that may occur whenever ACES and SEMS are available.

g. Security of Data

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

(2) The Tribe shall take reasonable precautions to secure against unauthorized physical and electronic access to data.

(3) To limit potential security breaches, if a fob is inactive for more than ninety (90) days, DSHS

may deactivate it.

(a) If a fob is deactivated, the Tribe agrees to return it to DSHS within 20 days of deactivation.

(4) 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.

(5) 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.

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

(7) The Tribe shall protect information according to State, Federal and Tribal laws including the following, incorporated by reference:

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

(b) RCW 42.56.230 Personal Information

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

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

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

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

h. Confidentiality and Nondisclosure

(1) The information to be shared under this Agreement is confidential in nature and is subject to State, Federal and Tribal confidentiality requirements. The Tribe shall maintain the confidentiality of client information in accordance with State, Federal, and Tribal laws.

(2) Notification of unauthorized disclosure

(a) The Tribe shall notify the Economic Services Administration (ESA) within one (1) business day if the Tribe discovers any unauthorized disclosure of ACES or SEMS information. Notification to ESA shall be done by sending an email to databreach@dshs.wa.gov.

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

(4) 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.

(5) The Tribe shall not disclose nor transfer any information as described in this agreement to any party in whole or in part, or to any individual or agency not specifically authorized by this agreement except as provided by law.

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

(7) Notice of Nondisclosure

(a) ACES: The Tribe must ensure each employee or contracted staff person with ACES access signs the following nondisclosure forms provided by DSHS prior to DSHS granting access:

i. Washington State Department of Social and Health Services Notice of Nondisclosure: The Tribe shall retain a signed copy of the form on file for monitoring purposes.

(b) SEMS: The Tribe must ensure that each employee or contracted staff person with SEMS access accepts the Federal and State data access requirements listed in the SEMS, Confidentiality Statement – Tribal Employee, prior to DSHS granting access.

(8) After being granted access each employee or contracted staff person will be required to annually review and accept the SEMS Confidentiality Statement – Tribal Employee.

4. 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.

5. 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

6. **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.** Data stored on local workstation hard disks. Access to the data will be restricted to authorized users by requiring logon to the local workstation using a unique user ID and complex password or other authentication mechanisms which provide equal or greater security, such as biometrics or smart cards.

   b. **Network server disks.** 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 complex 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.

   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 locked in a drawer, cabinet or other container to which only authorized users have the key, combination or mechanism required to access the contents of the container. 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 complex 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 locked container, such as a file cabinet, locking drawer, or safe, to which only authorized persons have access.

   f. **Access via remote terminal/workstation over the State Governmental Network (SGN).** Data accessed and used interactively over the SGN. Access to the data will be controlled by DSHS staff who will issue authentication credentials (e.g. a unique user ID and complex password) to authorized contractor staff. Contractor will notify DSHS staff immediately whenever an authorized person in possession of such credentials is terminated or otherwise leaves the employ of the contractor, and whenever a user's duties change such that the user no longer requires access to perform work for this contract.

   g. **Access via remote terminal/workstation over the Internet through Secure Access Washington.** Data accessed and used interactively over the SGN. Access to the data will be controlled by DSHS staff who will issue authentication credentials (e.g. a unique user ID and complex password) to authorized contractor staff. Contractor will notify DSHS staff immediately

whenever an authorized person in possession of such credentials is terminated or otherwise leaves the employ of the contractor and whenever a user's duties change such that the user no longer requires access to perform work for this contract.

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

(1) DSHS data shall not be stored by the Contractor on portable devices or media unless specifically authorized within the Special Terms and Conditions of the contract. If so authorized, the data shall be given the following protections:

(a) Encrypt the data with a key length of at least 128 bits

(b) Control access to devices with a unique user ID and 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.

Physically protect the portable device(s) and/or media by

(d) Keeping them in locked storage when not in use

(e) Using check-in/check-out procedures when they are shared, and

(f) Taking frequent inventories

(2) When being transported outside of a secure area, portable devices and media with confidential DSHS data must be under the physical control of contractor staff with authorization to access the data.

(3) Portable devices include, but are not limited to; handhelds/PDAs, Ultramobile PCs, flash memory devices (e.g. USB flash drives, personal media players), portable hard disks, and laptop/notebook computers if those computers may be transported outside of a secure area.

(4) Portable media includes, but is not limited to; optical media (e.g. CDs, DVDs), magnetic media (e.g. floppy disks, tape, Zip or Jaz disks), or flash media (e.g. CompactFlash, SD, MMC).

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.

b. DSHS data will be kept on media (e.g. hard disk, optical disc, tape, etc.) which will contain no non-DSHS data. Or,

c. DSHS data will be stored in a logical container on electronic media, such as a partition or folder dedicated to DSHS data. Or,

d. DSHS data will be stored in a database which will contain no non-DSHS data. Or,

e. 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. Or,

f. When stored as physical paper documents, DSHS data will be physically segregated from non-DSHS data in a drawer, folder, or other container.

g. 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 no longer needed, whichever is earlier, data shall be returned to DSHS or destroyed in accordance with DSHS IT Security Policy. 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	Using a "wipe" utility which will overwrite the data at least three (3) times using either random or single character data Degaussing sufficiently to ensure that the data cannot be reconstructed, or Physically destroying the disk
Paper documents with sensitive or confidential data	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 course abrasive
Magnetic tape	Degaussing, incinerating or crosscut shredding
Removable media (e.g. floppies, USB flash drives, portable hard disks, Zip or similar disks)	Using a "wipe" utility which will overwrite the data at least three (3) times using either random or single character data Physically destroying the disk Degaussing magnetic media sufficiently to ensure that the data cannot be reconstructed, or

9. **Notification of Compromise or Potential Compromise**. The compromise or potential compromise of DSHS shared data must be reported to the DSHS Contact designated on the contract within one (1) business day of discovery.

10. **Data shared with Sub-contractors.** If DSHS data provided under this contract is to be shared with a sub-contractor, the contract with the sub-contractor 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 sub-contractor must be submitted to the DSHS Contact specified for this contract for review and approval.