

**TANF Operating Agreement  
Between the  
Port Gamble S'Klallam Tribe and the Bremerton Community Services Office  
May 1, 2018 to September 30, 2019**

This summary constitutes a record of the operational agreements reached between the Port Gamble S'Klallam Tribe, the Bremerton Community Service Office and Region 3 Community Service Division, for the on-going operation of the Port Gamble S'Klallam Tribal TANF program.

This agreement is not static, but represents a starting point for the parties involved. Further cooperative agreements or operational modifications are likely as the needs change. As long as modifications are carried out with the knowledge and agreement of the parties involved, it is to be encouraged.

In accordance with the Centennial Accord and DSHS Administrative Policy 7.01, the purpose of this agreement is to further strengthen the government-to-government working relationship between all of the parties; and to assure that all of our mutual clients receive the best possible services at all times during the day-to-day operation of our TANF programs.

**1. General Agreement**

For the purposes of this agreement, when the CSO is referenced it includes the Statewide Customer Service Contact Center (CSCC) unless otherwise specified.

- A. The CSO and CSCC will provide current Tribal Liaison contact name and number. The Tribe will provide a current listing of staff names, functions, and phone numbers.
- B. The CSO will adhere to the provisions in the current CSD Region 3 version of the Administrative Policy 7.01 Plan.
- C. The CSO will continue working to improve access to services by providing alternatives to CSO visits whenever supported by DSHS policy. Alternatives may include, but are not limited to, options such as on-line CSO, Statewide Customer Service Contact Center, ANSWER phone, and telephone interviews.

Initially, the contact persons for this purpose will be:

Port Gamble S'Klallam Tribe	Cheryl Miller, Director
Bremerton CSO:	Gina Lindal, CSO Administrator
Customer Service Contact Center:	Ron Thomas, CSCC Administrator

## 2. TANF Agreement

### A. Target Population:

The TANF population affected by this agreement is defined as any enrolled American Indian residing on the Port Gamble S'Klallam reservation and any Port Gamble S'Klallam Tribal member living off the reservation but within Kitsap County who is a recipient of or applicant for TANF benefits.

1. This definition includes an eligible child(ren) in the home of a non-needy relative, so long as the child(ren) is a tribal member or enrolled American Indian living on the reservation.
2. The Tribe will not handle a TANF case for a family whose only tribal member is on SSI.
3. Only the Tribe can define who is a tribal member or American Indian for eligibility purposes.
4. If there is a question about which state or tribal TANF Program should serve a family, the state or Tribal TANF Program to which the family first presents itself will take their application for TANF and will then promptly contact the other TANF Program(s) to resolve who will serve that family.
5. Whenever a case does not clearly meet the household criteria spelled out in this agreement, the Tribe and CSO will jointly staff the case and make a decision which appears to be in the best interests of the child(ren). This may include cases where the state is continuing TANF cash aid to a parent while his or her child is temporarily removed from the home. In these cases, the state will, upon the PGST Tribal TANF request, provide state TANF (or federal) benefits for a financially eligible caretaker relative and/or child to avoid duplication of state and tribal TANF benefit receipt.
6. If a potential state TANF applicant or household member present themselves as an enrolled American Indian residing on the PGSK reservation, or any PGSK member living off the reservation but within Kitsap County, CSO staff will give the family information about the services provided by the PGSK TANF Program and encourage them to apply with the PGSK TANF Program.

### B. Eligibility

1. Tribal TANF benefit standards and eligibility requirements are based on the specific criteria set forth in the current federal Port Gamble S'Klallam Tribal TANF Plan.
2. Persons who receive Tribal TANF are not eligible to receive DSHS benefits in the form of Additional Requirements for Emergent Needs (AREN), Diversion Cash Assistance (DCA), or WorkFirst Support Services.
3. The CSO will send a notification letter to a client and set a tickle to CSO 251, within 60 days of determination of eligibility for DSHS state TANF, to refer the client to the Tribal TANF program.

C. Training and Technical Assistance

1. Orientation to facilities and TANF services: Each party is willing to arrange orientation to their office and basic services as a way to help train staff to better serve our mutual clients.
2. Region 3 will invite the Tribal TANF office staff to local training or make available written materials that appear relevant for the administration of TANF.
3. The Tribe and CSO will meet as needed to further refine the local TANF process.

**3. Non-TANF Benefit Agreement:**

A. SNAP

Port Gamble S'Klallam Tribe operates SNAP assistance under an eligibility determination (ED) project with the State of Washington Department of Social & Health Services. If anything changes with the demonstration pilot program for SNAP assistance, this Operating Agreement will be modified to reflect those changes. All families receiving TANF through the PGST Tribal TANF program will also receive their SNAP assistance through the PGST ED project.

B. Child Care Subsidy Program

Persons eligible for Tribal TANF benefits may also qualify other programs and services through the CSO, in particular, child care subsidies through the Subsidy Programs (CCSP) program. CCSP applications and benefit maintenance are managed by the CSCC.

Tribal TANF recipients may apply for CCSP either on-line through the Washington Connections website at <https://www.washingtonconnection.org> or by telephone at 1-877-501-2233. No in-person interview is required for CCSP.

C. Medicaid

To the extent tribal members or the Tribe must access public benefits' medical care coverage programs that are managed by the Health Care Authority (HCA), or submit applications or renewals through the Washington Healthplanfinder, the PGST Tribe should contact the HCA or the Washington Health Benefit Exchange directly.

**4. Data Sharing & Communication Agreement**

- A. Per the terms of "Exhibit A- Indian Nation Data Security Requirements", CSO and the Port Gamble S'Klallam TANF Program staff may exchange information necessary to provide and coordinate services, and avoid the duplication of services.
- B. These agreements will routinely be used to share information.



## Exhibit A – Indian Nation Data Security Requirements

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

- a. "Authorized User(s)" means an Individual or individuals with an authorized business requirement to access DSHS Confidential Information.
- b. "Confidential Information" or "Data" means information that is exempt from disclosure to the public or other unauthorized persons under RCW 42.56 or other federal, state, or Tribal laws. Confidential Information includes, but is not limited to, Personal Information.
- c. "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 128 bits.
- d. "Hardened Password" means a string of at least eight characters containing at least one alphabetic character, at least one number and at least one special character such as an asterisk, ampersand or exclamation point.
- e. "Physically Secure" means that access is restricted through physical means to authorized individuals only.
- f. "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. Pertinent RCW chapters can be accessed at <http://apps.leg.wa.gov/rcw/>.
- g. "Secured Area" means an area to which only authorized representatives of the entity possessing the Confidential Information have access. Secured Areas may include buildings, rooms or locked storage containers (such as a filing cabinet) within a room, as long as access to the Confidential Information is not available to unauthorized personnel.
- h. "Tracking" means a record keeping system that identifies when the sender begins delivery of Confidential Information to the authorized and intended recipient, and when the sender receives confirmation of delivery from the authorized and intended recipient of Confidential Information.
- i. "Trusted System(s)" include only the following methods of physical delivery: (1) hand-delivery by a person authorized to have access to the Confidential Information with written acknowledgement of receipt; (2) United States Postal Service ("USPS") first class mail, or USPS delivery services that include Tracking, such as Certified Mail, Express Mail or Registered Mail; (3) commercial delivery services (e.g. FedEx, UPS, DHL) which offer Tracking and receipt confirmation; and (4) the Washington State Campus mail system. For electronic transmission, the Washington State Governmental Network (SGN) is a Trusted System for communications within that Network.
- j. "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. Confidentiality.**

- a. The Indian Nation shall not use, publish, transfer, sell or otherwise disclose any Confidential Information gained by reason of this Agreement for any purpose that is not directly connected with Indian Nation's performance of the services contemplated hereunder, except:

- (1) as provided by law; or,
  - (2) in the case of Personal Information, with the prior written consent of the person or personal representative of the person who is the subject of the Personal Information.
- b. The Indian Nation shall protect and maintain all Confidential Information gained by reason of this Agreement against unauthorized use, access, disclosure, modification or loss. This duty requires the Indian Nation 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 Data.
  - (2) Physically Securing any computers, documents, or other media containing the Data.
  - (3) Sending paper documents containing DSHS Data via a Trusted System.
3. **Data Transport.** When transporting DSHS Confidential Information electronically, including via email, the Data will be protected by:
- a. Transporting the Data within the (State Governmental Network) SGN or Indian Nation's internal network, or;
  - b. Encrypting any Data that will be in transit outside the SGN or Indian Nation's internal network. This includes transit over the public Internet.
4. **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.** 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.** 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 Secured Area and otherwise meet the requirements listed in the above paragraph. Destruction of the Data as outlined in Section 4. Data Disposition may be deferred until the disks are retired, replaced, or otherwise taken out of the Secured 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 Secured Area. When not in use for the agreed 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 Secured 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 Secured 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. **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 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 with a key length of at least 128 bits
    - (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.

Physically Secure 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 Secured Area, portable devices and media with DSHS Confidential Information must be under the physical control of Indian Nation staff with authorization to access the Data.
  - (3) Portable devices include, but are not limited to; smart phones, tablets, flash memory devices (e.g. USB flash drives, personal media players), portable hard disks, and laptop/notebook/netbook computers if those computers may be transported outside of a Secured Area.

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

**h. Data stored for backup purposes.**

- (1) DSHS data 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 in Section 6.
- (2) DSHS Data may be stored on non-portable media (e.g. Storage Area Network drives, virtual media, etc.) as part of a 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 in Section 6. Data Disposition.

**5. 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.
  - b. DSHS Data will be kept on media (e.g. hard disk, optical disc, tape, etc.) which will contain no non-DSHS Data. And/or,
  - c. DSHS Data will be stored in a logical container on electronic media, such as a partition or folder dedicated to DSHS Data. And/or,
  - d. DSHS Data will be stored in a database which will contain no non-DSHS data. And/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.
  - 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.
- 6. Data Disposition.** When the agreed work has been completed or when no longer needed, except as noted in 4.b above, Data shall be returned to DSHS or destroyed. Media on which Data may be stored and associated acceptable methods of destruction are as follows:

<b>Data stored on:</b>	<b>Will be destroyed by:</b>
Server or workstation hard disks, or	Using a "wipe" utility which will overwrite the Data at least three (3) times using either random or single

Removable media (e.g. floppies, USB flash drives, portable hard disks) excluding optical discs	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

7. **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](mailto:dshsprivacyofficer@dshs.wa.gov). 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.
8. **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 subcontractor must be submitted to the DSHS Contact specified for this contract for review and approval.

