Washington State DEPARTMENT OF SOCIAL & HEALTH SERVICES

# INDIAN NATION PROGRAM AGREEMENT

## Federal Offset Certification for Tribal Child Support Program

DSHS Agreement Number: 1562-26115

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 a DSHS and Indian Nation Agreement on 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 | 1309 | 3000NC-62 |

| DSHS CONTACT NAME AND TITLE | DSHS CONTACT ADDRESS |
|---|---|
| Saundra Cheek<br>Program Administrator | 712 Pear St SE<br>PO Box 9162<br>Olympia, WA 98507-9162 |

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

| INDIAN NATION NAME | INDIAN NATION ADDRESS |
|---|---|
| Lummi Nation | 2665 Kwina Road<br>Bellingham, WA 98226-9291 |
| INDIAN NATION FEDERAL EMPLOYER IDENTIFICATION NUMBER | INDIAN NATION CONTACT NAME<br>Ralph Jefferson |

| INDIAN NATION CONTACT TELEPHONE | INDIAN NATION CONTACT FAX | INDIAN NATION CONTACT E-MAIL |
|---|---|---|
| (360) 384-7165 | (360) 312-9192 | ralphj@lummi-nsn.gov |

| 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 |
|---|---|---|
| 01/01/2015 | 12/31/2017 | $0.00 |

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 – Indian Nation Security Requirements, Exhibit B – IRS Confidentiality and Security**

☐ **No Exhibits.**

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 |
|---|---|---|
| | Rita Jefferson, Treasurer | 1/19/15 |
| **DSHS SIGNATURE** | **PRINTED NAME AND TITLE** | **DATE SIGNED** |
| | Ann Polanco, DCS Contract Administrator<br>DSHS/ESA/Division of Child Support | 1/30/15 |

**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 the terms of this program agreement, 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 the public.

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

**2. Definitions**

a. "Administrative Review" means the process described in 45 CFR 303.72 whereby a noncustodial parent may contest certification of a debt to the Internal Revenue Service (IRS).

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. "CFR" means the Code of Federal Regulations.

d. "CP" means the Custodial Parent.

e. "Data" means "confidential information" or "confidential data" as defined the DSHS and Indian Nation Agreement on General Terms and Conditions (INGT&C).

f. "DCS" means the Division of Child Support of the Economic Services Administration.

g. "ESA" means the DSHS Economic Services Administration.

h. "FTI" means Federal Tax Information and includes "returns" and "return information" as defined in 26 USC 6103(b) and is confidential in nature regardless of the means by which the FTI is conveyed and where the FTI is recorded.

i. "Indian Nation GT&C" is the DSHS and Indian Nation Agreement on General Terms and Conditions.

j. "IRC" means Internal Revenue Code.

k. "IRS" means Internal Revenue Service.

l. "IRS Publication 1075" is an IRS publication entitled "Tax Information Security Guidelines for Federal, State, and Local Agencies – Safeguards for Protecting Federal Tax Returns and Return Information."

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

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

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

p. "SEMS" means Support Enforcement Management System.

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

r. "Taxpayer" means any individual subject to any internal revenue tax.

s. "Tribe" means the entity requesting 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.

t. "Tribal IV-D Program" or "Tribal Child Support Program" means an Indian Tribe in Washington State that administers a federally-approved child support programs.

u. "USC" means the United States Code.

**3. Purpose**

This Agreement is necessary in order for the DSHS Division of Child Support (DCS) to provide federal offset certification action on cases involving Tribal Child Support programs.

**4. Statement of Work**

a. CASE REQUIREMENTS

The Tribe will ensure the case meets the federal requirements listed in 45 CFR 303.72 (a), before sending DCS a referral for federal offset certification. The requirements are currently as follows:

(1) The debt is based on an established court or administrative order.

(2) The NCP's name and social security number (SSN) are correct.

(3) For a nonassistance case, the Tribe will:

(a) Ensure that the debt is at least $500

(b) Provide a current address for a nonassistance CP.

(4) For a TANF case, the Tribe will ensure that the debt is:

(a) At least $150

(b) Past due for at least thirty (30) days.

(5) Spousal support may be certified if child support and spousal support are payable under the same order and the minor child is living with the CP.

b. REFERRAL PROCESS

(1) The Tribal IV-D Program will request federal offset services by sending a referral to the local DCS field office for each NCP case they want certified. The referral will include, but is not limited to:

(a) Child Support Enforcement Transmittal #1 – Initial Request

(b) Relevant court orders

(c) Debt calculation

(2) The Tribe will indicate on the referral that they are requesting Federal Tax Offset Withholding.

c. PAYMENT OF ADMINISTRATIVE COSTS

(1) Every 3 months, the ESA Fiscal Office will send an invoice listing the previous quarter's administrative costs associated with the Tribe's referred cases.

(2) Within 30 days of the date of the invoice, the Tribe will pay for the administrative costs that the federal government charges each State for federal offset. Subject to any future changes, these federal charges are currently as follows:

(a) $14.65 each time federal offset funds are intercepted

(b) $15.00 each time administrative offset funds are intercepted

(3) The Tribe shall make checks payable to "DSHS/DCS", reference the "Tribe Name / DCS Federal Offset Agreement" on the check, and remit payment to:

ESA/OS Fiscal/DCS Accounting Unit
PO Box 45445
Olympia WA 98504-5445

**Exception**: DCS will not bill the Tribe for these costs if DCS, on its own behalf, also certified for federal offset another debt for the same NCP in the same tax year.

d. DISTRIBUTION OF FEDERAL OFFSET FUNDS

(1) DCS will hold potentially suspicious intercept payments until those payments have been verified as belonging to the NCP.

(2) DCS will distribute federal income tax refunds owing to the Tribe within two (2) days of receipt if one of the following is true:

(a) The NCP did not file a joint return.

(b) The NCP filed a joint return, and an injured spouse allocation request was filed with the original income tax return.

(3) If the NCP filed a joint return on a nonassistance case, but no injured spouse claim was filed with the original income tax return:

(a) DCS will distribute up to 50% of the income tax funds owing to the Tribe within 2 days of receipt, and the remaining funds within 120 days of receipt (unless an injured spouse allocation request is filed).

i. If the CP claims that the 120 day delay of the tax refund causes undue hardship, DCS will forward the request to the Tribe. The Tribe decides if and how to grant relief regarding the portion of the funds being held on the Tribe's behalf.

ii. If the Tribe decides to send any funds to the CP before the 120 days pass, the Tribe must notify the DCS Tribal Liaison in writing of the decision. DCS Headquarters will then send the funds to the Tribe for distribution to the CP.

(b) If DCS distributes funds to the Tribe, and an injured spouse allocation request is later filed and DCS must return the intercept to the Treasury, the Tribe agrees to repay the funds. (The majority of injured spouse allocation requests are filed within 120 days of DCS receiving the funds; however the NCP's spouse has 6 years to file an allocation request).

i. DCS will work with the Tribe to establish a payment plan for the repayment of these funds to DCS.

ii. The Tribe will repay DCS within 90 days of being notified DCS returned an intercept to the Treasury.

(c) DCS does not automatically hold in suspense any portion of the IRS offset funds on a state TANF case.

(4) The Tribe agrees to repay DCS if a portion of the funds distributed to the Tribe must be returned due to the wrong individual being certified, debt inaccuracy (this does **not** apply if DCS is responsible for the debt inaccuracy), or the payment received was from a fraudulent tax return.

(a) DCS will work with the Tribe to establish a payment plan for the repayment of these funds to DCS.

(b) The Tribe will repay DCS within 90 days of being notified DCS returned an intercept to the Treasury.

(5) The Tribe agrees to return to DCS any portion of the funds that result in an overpayment due to NCP payments following certification.

**Exception**: If the Tribe verifies with DCS that the NCP does not have any other debts certified for federal offset, then the Tribe can refund the payment directly to the NCP.

e. ADMINISTRATIVE REVIEW ON CASES REFERRED BY A TRIBAL IV-D PROGRAM

If the NCP requests an administrative review because the NCP contests certification of a debt to the Internal Revenue Service (IRS):

(1) DCS will send a copy of the administrative review request to the Tribe.

(2) If there is **only** tribal interest in the certified funds, the Tribe will perform the administrative review process. The Tribe will notify DCS in writing of the administrative review decision which will allow the Tribal Liaison to take any necessary action.

(3) In cases where there is a joint tribal and DCS interest in the certified funds, DCS and the Tribe will work together to provide the administrative review:

(a) DCS will make the final determination on the portion of the debt it certified on its own behalf.

(b) The Tribe makes the final determination on any debt certified on its behalf, and provides DCS with written recommendations instructing DCS if and how to provide relief to the NCP with regard to any debt certified on the tribe's behalf.

**Note**: The NCP may choose to affirmatively request that the order state or order tribe perform the administrative review if the IV-D Tribe did not issue the order. If the tribe who certified the

debt does not have a IV-D program with an established administrative review process, then either DCS or the state or tribe (which issued the order on which certification is based), must perform the review.

f. CASE CLOSURE

DCS will close the case after receiving from the Tribe a Child Support Enforcement Transmittal #2 form, requesting closure.

g. DESCRIPTION OF THE DATA

(1) At the request of the Tribal IV-D program signing this agreement, DCS shall release the following information related to a case certified for federal offset when necessary for processing and distributing federal offset funds:

(a) Confirmation that a payment received was the result of a federal offset.

(b) Whether a joint return was filed.

(c) Whether an injured spouse allocation request has been filed.

(d) The total amount of the intercept if a hardship review is requested.

(e) The spouse's name in the case of a joint filing if a refund is necessary due to an overpayment.

(f) The address of all parties on the return if a refund is necessary due to an overpayment.

(g) All documentation pertaining to the request for an administrative review or a hardship review.

(2) The Tribal IV-D program will provide monthly summary to DCS listing critical debt information for each case certified for federal offset (see h.1.c.).

h. ACCESS TO FEDERAL OFFSET PAYMENTS AND RELATED DATA

(1) METHOD AND FREQUENCY OF ACCESS/TRANSFER

(a) DCS will provide the data listed in g. (1) (see above) by the following methods: hand deliver, mail, secured email, or telephone.

- If mailed, the data (hard copy) will be sent using any of the methods (Trusted Systems) in 1.i. of **Exhibit A**.

(b) DCS will send applicable federal offset funds to the Tribe via electronic funds transfer (EFT).

(c) The Tribal IV-D Program must submit a monthly summary to the Tribal Liaison in the local DCS field office by the 10th of every month. The summary is required to ensure that the debt certified for federal offset is accurate, and must include the following information for each case:

i. NCP's name

ii. CP's name

iii. DCS case number (D#), if known (if not, include NCP social security number)

iv. Balance of the debt as of the last day of the prior month

v. Date and amount of last payment included in the debt balance

(2) PERSONS HAVING ACCESS TO DATA

All SEMS data, child support case-related information, and FTI shall be private and confidential and shall not be disclosed unless otherwise permitted by applicable law. The tribal IV-D program will comply with all safeguarding requirements with respect to federal tax offset in accordance with 45 CFR 309.80, 42 USC 664(26), and the Internal Revenue Code 26 USC 6103, which prohibits the release of IRS information outside of the IV-D program. The Tribe shall ensure that only designated staff have access to information necessary for the processing and distribution of funds received from federal offset.

i. SECURITY OF DATA, CONFIDENTIALITY, AND NONDISCLOSURE

(1) The tribal IV-D program will comply with all safeguarding requirements with respect to federal tax offset in accordance with 45 CFR 309.80, 42 USC 654(26), and the Internal Revenue Code 26 USC, which prohibits the release of IRS information outside of the IV-D program. The Tribe agrees to comply with section 6103 of the IRS Code, and IRS Publication 1075, which includes very specific criteria for maintaining, using, storing, safeguarding, reporting and destroying FTI. This includes, but is not limited to:

(a) FTI includes a taxpayer's identity and the nature, source, or amount of a payment.

(b) Making sure any notes and all FTI are shredded appropriately and timely (5/16 "on the bias or cross cut shredded).

(c) Not sending FTI in the text of E-mail. Messages containing FTI must be attached and encrypted.

(d) Confirming a NCP's address from IRS information via a second source.

(e) Activating a screensaver password on the local workstation computer at all times.

(f) Securing IRS information at all times using two barriers under normal security: secured perimeter/locked container, locked perimeter/secured interior, or locked perimeter/ security container. During duty hours, deny access to areas containing FTI by restricted areas, security rooms, or locked rooms. During non-duty hours, FTI in any form (hard copy, printout, photocopy, notes, backups, etc.) must be protected through a combination of methods: secured or locked perimeter; secured area; or containerization (locked containers, security containers, safes or vaults). FTI must be containerized in areas where other than authorized employees may have access after-hours.

i. Securing keys to IRS cabinet and account for all keys on a master key log.

ii. Maintaining logs that track receipt, use and destruction of IRS reports.

iii. Maintaining up-to-date access list to restrict access to FTI.

iv. Testing IRS locking cabinet periodically to ensure security.

v. Ensuring adequate back-up coverage exists to maintain consistent security.

vi. Preferably not co-mingling data with FTI. If FTI is co-mingled with other data, all co-mingled data will be protected as FTI.

(2) The Tribe agrees to protect all confidential information and confidential data according to applicable laws including the following:

(a) RCW 26.23.120,

(b) 26 USC 6103,

(c) 42 USC 654 (26),

(d) 45 CFR 309.80,

(e) 45 CFR 307.13,

(f) RCW 42.56.230,

(g) RCW 74.04.060, and

(h) WAC 388-14A-2105 through WAC 388-14-A-2160.

(3) All Tribal staff with access to income tax information and payments must:

(a) Be briefed on security procedures and instructions for protecting federal tax information.

(b) Yearly review the IRS Confidentiality and Security training points **(See Exhibit B)** and this agreement; then

(c) Sign a DSHS Confidentiality Statement Tribal Employee form.

(4) In addition to following all the data security requirements in **Exhibit A**, the Tribe shall take all precautions to secure against unauthorized physical and electronic access to data. This includes:

(a) Storing confidential information and confidential data centrally on secure servers. Servers and back-up media must be kept in locked rooms, with access limited to authorized persons.

(b) Restricting access to confidential information and confidential data viewed locally on workstation computers, via network shares to authorized users through the use of access control lists (ACLs) and authentication with a unique user ID and complex password and/or other secure authentication mechanism. Passwords will be changed at least every 90 days.

(c) Not remotely accessing any confidential information or confidential data through any means, including the use of external networks (e.g. the internet).

(d) Printed working documents will be secured when work stations are unattended.

(e) Access to work areas will limited to authorized staff only.

(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) The Tribe shall notify the DSHS Contact listed on page one of this agreement within one (1) business day, upon discovery of any compromise or potential compromise of confidential or sensitive data shared by DSHS with the Tribe.

(7) The Tribe shall report improper inspections or disclosures of FTI as outlined in **Exhibit B** and Publication 1075, Section 10.

(8) The Tribe will promptly destroy the data when the work is completed and/or the need for retention of the records is no longer required as stated in **Exhibit A** –Indian Nation Data Security Requirements.

(9) The Tribe shall remove data received under this Agreement from computer equipment after it's been used for its stated purpose as stated in **Exhibit A**.

(10) In the case of hardware failure, the Tribe must protect data by either removing the hard drive before shipping equipment for repair, or a tribal child support employee will be present while equipment is repaired on site.

(11) Data provided by DSHS remains DSHS property. The Tribe will dispose of all copies of any data sets in its possession within 30 days of the date of termination, and certify such destruction to DSHS. DSHS shall be responsible for destroying the returned documents to ensure confidentiality is maintained.

(12) Data provided by the Tribe will be stored and handled by DSHS, but will remain tribal property.

(13) In accordance with 26 USC 6103, 42 USC 654 (26), 45 CFR 309.80, RCW 26.23.120, RCW 74.04.060, and WAC 388-14A-2105 through WAC 388-14A-2160, any information concerning individuals who owe a support obligation or for whom support enforcement services are being provided is private and confidential and shall be exempt from disclosure under RCW 42.56 or other Federal, State, or Tribal laws.

(14) The Tribe shall not disclose, transfer, or sell 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 or further defined in both Exhibits A and B.

j. MONITORING

(1) To ensure FTI safeguarding measures are maintained, the Tribe will assign a security monitor, who will:

(a) Perform internal inspections to monitor compliance with the requirements of this agreement.

(b) Ensure staff annually review and sign DSHS Confidentiality Statement Tribal Employee form and review this agreement, including the attached **Exhibits**.

(c) Complete an annual IRS Safeguards Program Internal Inspections Report-Field Office and submit it to the DSHS Contact listed on page 1 of this contract. Each year the Tribe will

provide the report 15 days prior to the SSR Due Date for Washington State as specified in IRS Publication 1075.

(2) DCS may test compliance with the terms of this Agreement by reviewing the IRS Safeguards Program Internal Inspections Report – Field Office and through contact with the Tribe to monitor compliance.

k. LEGAL REFERENCES IN THIS CONTRACT

All references in the contract to IRC, USC, CFR, RCW, or WAC chapters or sections shall include any successor, amended, or replacement code, regulation or statute.

**5. Dispute Resolution**

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

**6. Amendments or Termination**

a. AMENDMENTS

(1) This contract may be altered or amended by written agreement signed by both parties.

(2) Each party reserves the right to renegotiate fundamental terms that are in conflict with new or changes in policy.

b. TERMINATION

(1) Parties will abide by the Termination procedures identified in the Indian Nation GT&C (pages 5-7).

(2) In addition, the DCS Director may terminate the agreement if an external entity (i.e. Internal Revenue Service, federal Office of Child Support Enforcement) determines that a breach has occurred by DSHS or by the Tribe.

**APPROVED AS TO FORM BY THE OFFICE OF THE ATTORNEY GENERAL**

## 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:

| Data stored on: | Will be destroyed by: |
|---|---|
| Server or workstation hard disks, or<br><br>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<br><br>Degaussing sufficiently to ensure that the Data cannot be reconstructed, or<br><br>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. 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.

# EXHIBIT B

## IRS CONFIDENTIALITY AND SECURITY

**Employee Awareness Training Points from**
**Internal Revenue Code (IRC) Sections**

**TAX RETURN INFORMATION:**

- *IRS provides certain return information to federal, state and local child support agencies.*

**GENERAL RULE – 6103(a):**

- *Returns and return information shall be confidential, and except as authorized – no employee of the U.S., no employee of any State, any local child support enforcement agency…shall disclose any return information obtained by him in any manner in connection with his service as an employee…*

**DISCLOSURE:**

- *The making known of any return or return information in any manner to anyone.*

**IRC §7213 UNAUTHORIZED DISCLOSURE:**

- *Willful disclosure of return/return information*
- *Felony*
- *Fine not to exceed $5,000 or*
- *Imprisonment, not to exceed five (5) years, or both*
- *Cost of prosecution, and*
- *Dismissal*

**IRC §7213A UNAUTHORIZED INSPECTION:**

- *Fine not exceeding $1,000, or*
- *Imprisonment not to exceed 1 year, or both, with*
- *Cost of prosecution*

**IRC §7431 CIVIL DAMAGES FOR UNAUTHORIZED DISCLOSURE OF RETURN/RETURN INFORMATION:**

- *The greater of: $1,000 for each act of unauthorized inspection or disclosure; or*
- *Actual damages plus*
- *Punitive damages plus*
- *The cost of the action.*

**SAFEGUARDS:**

- *IRC §6103(p) (4): as a condition of receiving return/return information must comply with specific criteria for maintaining, using, storing, reporting and destroying return/return information.*

**IRC §6103(a)**

- *Returns and return information shall be confidential…no employee…shall disclose any return information obtained by him in any manner**

  **This does not apply to tax information received directly from the noncustodial parent, custodial parent or their representative.*

## Staff Procedures

**YOU MAY DISCLOSE IRS PAYMENT TYPE AND AMOUNT TO:**

- *Noncustodial parent taxpayer*
- *Other IV-D Agencies (Child Support)*
- *IV-D Contractors: Prosecutors and Attorneys General*

**STAFF WITH ACCESS MUST:**

- *Only access IRS information when necessary to perform their duties.*
- *Shred any note jotted down from IRS report information.*
  - *This includes addresses without taxpayer identifying information. Even without the taxpayer's identity the information retains its IRS nature and all the same safeguards necessary for protecting IRS reports must be followed.*
- *Be aware that "B9" payment type on the Case Financial screen is considered IRS information.*
- *Confirm NCP address from IRS report via a second source (i.e., US Postal Service, employer, etc.) before adding it to the NCP address screen.*
- *Activate the screensaver password on personal computer at all times (be sure to reactivate after service performed on the computer).*

**IRS CUSTODIAN MUST:**

- *Secure IRS reports at all time.*
- *Secure keys to IRS cabinet and account for all keys on a Master Key Log.*
- *Maintain logs that track receipt, use and destruction of IRS reports within their office.*
- *Maintain up-to-date Access List to restrict IRS report access to only those staff meeting annual training requirement.*
- *Make sure any notes and all IRS reports are shredded appropriately and timely (5/16" on the bias or cross cut shredded).*
- *Test IRS locking cabinet lock periodically to ensure security.*
- *Ensure that adequate back up coverage exists to maintain consistent security when primary IRS Custodian is gone*

**ANY PERSON (FEDERAL EMPLOYEE, STATE EMPLOYEE, OR ANY OTHER INDIVIDUAL) THAT DISCOVERS A POSSIBLE IMPROPER INSPECTION OR DISCLOSURE OF FTI MUST:**

- *Contact the office of the appropriate special agent-in-charge, Treasury Inspector General for Tax Administration (TIGTA) immediately, but no later than 24 hours after identification of a possible issue involving FTI.* ***Call the local TIGTA Field Division Office first.***
  - *Denver office serves Alaska, Arizona, Colorado, Idaho, Montana, Nevada, New Mexico, Oregon, Utah, Washington, and Wyoming.*
  - *Telephone for Denver Field Division Office is 303-291-6102*
  - *If unable to contact the local TIGTA Field Division, contact the National Office;*
    - ***Hotline Number:*** *800-589-3718*
    - ***Online:*** *http://www.treasury.gov/tigta/*
    - ***Mailing Address:*** *Treasury Inspector General for Tax Administration*
      *Ben Franklin Station*
      *P.O. Box 589*
      *Washington, DC 20044-0589*
  - *In conjunction with contacting the TIGTA, the Office of Safeguards must be notified (see Section 10.2 Publication 1075 and next page).*

## OFFICE OF SAFEGUARDS NOTIFICATION PROCESS:

*Concurrent to notifying TIGTA, the agency must notify the Office of Safeguards. To notify the Office of Safeguards, the agency must document the specifics of the incident known at that time into a data incident report, including but not limited to:*

- *Name of agency and agency Point of Contact for resolving data incident with contact information*
- *Date and time of the incident*
- *Date and time the incident was discovered*
- *How the incident was discovered*
- *Description of the incident ant the data involved, including specific data elements, if known*
- *Potential number of FTI records involved, if unknown, provide a range if possible*
- *Address where the incident occurred*
- *Information Technology involved (e.g. laptop, server, mainframe)*
- *Do not include any FTI in the data incident report*
- *Email the Data Incident Report to the SafeguardReports@IRS.gov mailbox. Reports must be sent electronically and encrypted via IRS-approved encryption techniques. Use the term 'Data Incident Report' in the subject line of the email.*

***Even if all information is not available, immediate notification is the most important factor, not the completeness of the data incident report. Additional information must be provided to the Office of Safeguards as soon as it is available.***