JEFFERSON COUNTY
BOARD OF COUNTY COMMISSIONERS

AGENDA REQUEST

TO: Board of County Commissioners
Mark McCauley, County Administrator
FROM: James Kennedy, Prosecuting Attorney

DATE: 11/04/2024
SUBJECT: DSHS County Program Agreement: County Data Security & Use of State Resources

---

STATEMENT OF ISSUE:
This Program Agreement between the Division of Child Support (DCS) and the Jefferson County Prosecuting Attorney is to update requirements and standards for data security and use of state resources for non-DSHS staff. The Jefferson County Prosecuting Attorney provides Title IV-D Child Support Enforcement services on behalf of DCS and utilizes state resources to do that work.

ANALYSIS:
The Jefferson County Office of the Prosecuting Attorney provides Support Enforcement services on behalf of DCS. To perform this work, the Title IV-D County must have access to Support Enforcement Management System (SEMS), the Automated Client Eligibility System (ACES), and may have access to additional databases. This Program Agreement outlines the requirements and standards for obtaining and maintaining access to these systems by non-DSHS staff. Updates have been made to the process of Incident Response in section 5.b.(4) of the Special Terms and Conditions.

The current County Data Security and Use of State Resources agreement with DSHS/DCS is up for renewal for the term of July 1, 2024 through June 30, 2029.

FISCAL IMPACT:
There are no fiscal impacts associated with this Program Agreement.

RECOMMENDATION:
Jefferson County Prosecuting Attorney requests the Jefferson County Board of County Commissioners approve the contract and initiate a motion to delegate authority to James Kennedy to sign the contract on behalf of the County.

REVIEWED BY:

Mark McCauley, County Administrator

11/1/24
Date

CONTRACT REVIEW FORM

Clear Form

(INSTRUCTIONS ARE ON THE NEXT PAGE)

CONTRACT WITH: Washington State Department of Social & Health Services Contract No: 2463-57761

Contract For: DSHS County Data Security & Use of State Resources Agreement Term: Start 07/01/2024 to End 06/30/2029

COUNTY DEPARTMENT:	Jefferson County Prosecuting Attorney
Contact Person:	Melissa Pleimann
Contact Phone:	(360) 385-9180
Contact email:	mpleimann@co.jefferson.wa.us

AMOUNT: N/A

Revenue: _____

Expenditure: _____

Matching Funds Required: _____

Sources(s) of Matching Funds _____

Fund # _____

Munis Org/Obj _____

PROCESS:

- ☐ **Exempt from Bid Process**
- ☐ **Cooperative Purchase**
- ☐ **Competitive Sealed Bid**
- ☐ **Small Works Roster**
- ☐ **Vendor List Bid**
- ☐ **RFP or RFQ**
- ☑ **Other:** Program Agreement

APPROVAL STEPS:

STEP 1: DEPARTMENT CERTIFIES COMPLIANCE WITH JCC 3.55.080 AND CHAPTER 42.23 RCW.

CERTIFIED: ☐ **N/A:** ☑ _____ November 1, 2024

Signature Date

STEP 2: DEPARTMENT CERTIFIES THE PERSON PROPOSED FOR CONTRACTING WITH THE COUNTY (CONTRACTOR) HAS NOT BEEN DEBARRED BY ANY FEDERAL, STATE, OR LOCAL AGENCY.

CERTIFIED: ☐ **N/A:** ☑ _____ November 1, 2024

Signature Date

STEP 3: RISK MANAGEMENT REVIEW (will be added electronically through Laserfiche):

Electronically approved by Risk Management on 11/1/2024.

STEP 4: PROSECUTING ATTORNEY REVIEW (will be added electronically through Laserfiche):

Electronically approved as to form by PAO on 11/1/2024.
State Contract - Cannot Change

STEP 5: DEPARTMENT MAKES REVISIONS & RESUBMITS TO RISK MANAGEMENT AND PROSECUTING ATTORNEY(IF REQUIRED).

STEP 6: CONTRACTOR SIGNS

STEP 7: SUBMIT TO BOCC FOR APPROVAL

Washington State Department of Social & Health Services
Transforming lives

COUNTY PROGRAM AGREEMENT

County Data Security & Use of State Resources

DSHS Agreement Number
2463-57761

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

Administration or Division Agreement Number

County Agreement Number

DSHS ADMINISTRATION	DSHS DIVISION	DSHS INDEX NUMBER	DSHS CONTRACT CODE
Economic Services Administration	Division of Child Support	1223	3039CS-63

DSHS CONTACT NAME AND TITLE	DSHS CONTACT ADDRESS
Serena Hart Local Government Liaison	P.O. Box 9162 Olympia, WA 98507-9162

DSHS CONTACT TELEPHONE	DSHS CONTACT FAX	DSHS CONTACT E-MAIL
(360)515-6294	(360)664-5342	hartss@dshs.wa.gov

COUNTY NAME	COUNTY ADDRESS
Jefferson County Prosecuting Attorney	PO Box 1220 615 Sheridan St Port Townsend, WA 98368
COUNTY FEDERAL EMPLOYER IDENTIFICATION NUMBER	COUNTY CONTACT NAME James Kennedy

COUNTY CONTACT TELEPHONE	COUNTY CONTACT FAX	COUNTY CONTACT E-MAIL
(360) 385-9180		jkennedy@co.jefferson.wa.us

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

PROGRAM AGREEMENT START DATE	**PROGRAM AGREEMENT END DATE**	MAXIMUM PROGRAM AGREEMENT AMOUNT
07/01/2024	06/30/2029	No Payment

EXHIBITS. When the box below is marked with an X, the following Exhibits are attached and are incorporated into this County Program Agreement by reference:

☒ **Data Security: Exhibit A - Data Security Requirements**
☒ **Exhibits (specify): Exhibit B IRS Contract Language for General Services**
☒ **Exhibits (specify): Exhibit C Access to ACES**

The terms and conditions of this Contract are an integration and representation of the final, entire and exclusive understanding between the parties superseding and merging all previous agreements, writings, and communications, oral or otherwise, regarding the subject matter of this Contract. The parties signing below represent that they have read and understand this Contract, and have the authority to execute this Contract. This Contract shall be binding on DSHS only upon signature by DSHS.

COUNTY SIGNATURE(S)	PRINTED NAME(S) AND TITLE(S)	DATE(S) SIGNED
	The Honorable James Kennedy Prosecuting Attorney Jefferson County	
DSHS SIGNATURE	PRINTED NAME AND TITLE	DATE SIGNED
	Serena S.A. Hart Government Liaison DSHS/ESA/ Division of Child Support	

*

Special Terms and Conditions

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

   a. "ACES" means Automated Client Eligibility System, the Community Services Division's electronic management system.

   b. "Agency" means the Division of Child Support.

   c. "Contractor" or "PA" means Prosecuting Attorney is the entity performing services pursuant to this County Agreement and includes the Contractor's officers, directors, trustees, employees and/or agents unless otherwise stated in this Interlocal Agreement. For purposes of this County Agreement, the Contractor shall not be considered an employee or agent of DSHS.

   d. "DCS" means the Division of Child Support.

   e. "DSHS" means the Washington State Department of Social and Health Services.

   f. "IRS" means Internal Revenue Service.

   g. "Personal Information" means information identifiable to any person, including, but not limited to, information that relates to a person's name, health, finances, education, business, use or receipt of governmental services or other activities, addresses, telephone numbers, social security numbers, driver license numbers, other identifying numbers, and any financial identifiers.

   h. "SEMS" means Support Enforcement Management System, the DCS electronic management system for Child Support services.

2. **Purpose**.

   This Agreement between the Division of Child Support (DCS) and the County Prosecuting Attorney identified on page one is to update requirements and standards for data security and use of state resources for non-DSHS staff. The County Prosecuting Attorney provides Title IV-D Child Support Enforcement services on behalf of DCS and utilizes state resources to do that work.

3. **Legal Authority:**

   The Office of the Prosecuting Attorney provides Support Enforcement services under Title IV-D of the Social Security Act, 42 USC Chapter 7, Subchapter IV, Part D, section 651 et. seq; the Interlocal Cooperation Act, RCW 39.34; the Code of Federal Regulations, 45 CFR, Ch.III, Parts 301 through 308; applicable provisions of RCW 26 and RCW 74.20; and through interlocal agreements. For this work, the DSHS Division of Child Support provides and maintains state computers and other equipment used by the Title IV-D county staff.

   To perform this work, the Title IV-D County will have access to Support Enforcement Management System (SEMS), the Automated Client Eligibility System (ACES), and may have access to additional databases. DCS will manage County access through the SGN, IGN, networks, servers, and related equipment.

   Additional requirements for access to ACES are detailed in Exhibit C.

4. **Access to SEMS**

a. County staff shall request access to State Systems through the DCS Government Liaison.

(1) Any County staff that requests access to State Systems must be able to complete and pass a background check with the following requirements.

(a) Meet the background check requirements defined in IRS Publications 1075; and

(b) Receive disclosure awareness training prior to initial access to or use of Federal Tax Information (FTI)

(c) Background checks will be coordinated with DCS.

(2) All staff with access to State Systems shall sign DCS form 09-994 – Confidentiality Statement – Prosecuting Attorney Employee, Exhibit D, prior to access to any system. County shall retain a copy of the signed form and provide it to DCS upon request.

(3) When County staff job duties no longer perform Title IV-D duties or staff are no longer employed with the County, the County shall notify the Government Liaison within three (3) business days to have the staff member's access to SEMS revoked

b. The County shall only use authorized equipment provided by DCS for the performance of any functions under this agreement or for IV-D purposes.

c. Access to SEMS will occur via a supported browser that is patched with the most current updates.

d. The Browser will need to run on a supported agency owned or leased hardware platforms with a supported and patched operating system.

e. The platform will need to be protected with an up to date, Federally accepted, antivirus product.

f. County staff shall take reasonable precautions to secure against unauthorized physical and electronic access to information.

g. The County shall only access State Systems when physically within Washington State.

(1) Access to Systems when physically outside of the Washington State must have prior approval.

(2) State Systems can never be accessed outside of the United States.

h. No subcontractor shall have access to the use of State Resources or Systems without prior written approval.

5. Security Requirements

a. During the duration of this Agreement, the County shall be responsible for compliance with the following security standards:

(1) This Use of State Resources agreement with DCS;

(2) IRS Publication 1075, Exhibit 7 Safeguarding Contract Language (the current version, as of signing, is attached as Exhibit B) and the Background Check Requirements listed below;

(3) DSHS IT Security Manual;

(4) Any applicable DSHS, ESA, and DCS Administrative Policy; and

(a) In particular, DCS AP Section 10: Information Security.

(5) The following statutes:

(a) RCW 42.56.230 Personal Information;

(b) RCW 74.04.060 Records, Confidential – Exception – Penalty;

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

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

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

b. IRS Security Requirements

(1) IRS Right to Audit

(a) The County hereby acknowledges that the IRS shall have the right to inspect the County's facilities and operations as it relates to the County's IV-D activities and use of FTI.

(b) The County hereby acknowledges that IRS inspections may include manual and/ or automated scanning tools to perform compliance and vulnerability assessments of information technology assets that access, store, process, or transmit FTI.

(2) County's Responsibility to Address Corrective Action Plans

(a) The County agrees to work collaboratively with DCS to address any Corrective Action Plans as directed by the IRS to resolve findings of noncompliance as it relates to the County's duties and responsibilities under this Agreement.

(3) DCS Internal Inspection

(a) DCS will conduct an internal inspection every 18 months as required under IRS Publication 1075.

(4) Incident Response

(a) The County acknowledges its obligation to abide by the following incident response and incident reporting requirements:

i. Upon discovery of a possible improper inspection or disclosure of FTI by a DCS or County employee or any other person, the individual making the observation or receiving information must contract the IRS Office of Safeguards.

ii. Document the specifics of the incident known at that time into a Data Incident Report, including, but not limited to:

(A) Name of agency and agency point of contact for resolving data incident with their

contact information;

(B) Date and time of the incident;

(C) Date and time the incident was discovered;

(D) How the incident was discovered;

(E) Description of the incident and the data involved. Include specific data elements if known;

(F) Potential number of FTI records involved. If unknown, provide a range if possible;

(G) Address where the incident occurred; and

(H) Information technology involved (e.g. laptop, server, mainframe).

(I) DO NOT include any FTI in the Data Incident Report.

iii. Email the Data Incident Report to the SafeguardReports@IRS.gov mailbox.

(b) The IRS Office of Safeguards should be contacted immediately but no later than 24 hours after identification of a possible issue involving FTI.

(c) The County shall then notify the DCS Director and DCS Government Liaison after the IRS Office of Safeguards has been notified.

(d) The County must coordinate with DCS in any IRS 45-day notifications that relate to the County's use of FTI.

c. Other State Systems

(1) The County may be granted access to other databases to assist in the performance of the IV-D actions for DCS.

(2) County staff shall not access those databases for any other purpose, unless the County has its own data sharing agreement with the data owner.

(3) The County shall be responsible for assuring its own staff abide by the requirements of those additional databases.

6. IRS Mandatory Contract Language.

The Internal Revenue Service requires specific contract language in agreements with all non-DSHS employees with access to IRS information as part of their work for the Department. Attached is Exhibit B, Safeguarding Contract Language. This exhibit represents the present IRS requirements agreed to by the County and includes criminal and civil penalties for improper disclosure, notice to employees of sanctions for improper disclosure, and the IRS right of inspection and audit for compliance. The parties agree to follow the IRS provisions in Exhibit B. The IRS amends the language from time to time, and the most current version of Publication 1075 can be found here: https://www.irs.gov/pub/irs-pdf/p1075.pdf.

7. Use of State Resources.

When granting a non DSHS employee access to department IT equipment or other IT resources, DSHS is required to provide in an agreement that any use of State resources must be limited to specified purposes. The specified purpose for county employees is child support related activities. Counties have policies and procedures for use of county equipment and resources for official business purposes only. DSHS Administrative Policy 18.91 sets forth the requirements for state computers and resources and is an additional program requirement for the County Prosecuting Attorney Title IV-D staff. This policy may be reviewed by County Title IV-D staff, on-line through the DSHS intranet at: DSHS-AP-18-91-Internet-Official-Housekeeping-2024.pdf (wa.gov). The parties agree to follow DSHS Administrative Policy 18.91 as it relates to use of state resources.

8. IT Security Manual.

Non-DSHS employees using state computers and other IT resources are required to abide by the DSHS Security regulations and provisions as set forth in the DSHS IT Security Manual. Many IT functions are the responsibility of DCS as the computers and equipment used by the counties in their Title IV-D child support work are state owned and managed. Further, the servers, network, and applications are provided and managed by the State through DCS. County Prosecuting Attorney Title IV-D child support related employees may review the IT Security Manual through the DSHS intranet at: http://ishare.dshs.wa.lcl/Security/Manuals/Pages/default.aspx . To the extent the provisions apply, the parties agree to follow the applicable provisions of the DSHS IT Security Manual.

9. Data Security Requirements.

DSHS requires proper use and disposition of DSHS data for DSHS and non-DSHS users. Attached as Exhibit A and incorporated herein are data security requirements. As DSHS/DCS provides state computers and equipment for use in the County Prosecuting Attorney's Title IV-D child support related activities, the Parties agree to follow the data security requirements attached to the extent they apply to functions and use by County Title IV-D child support related employees.

Data Disclosure/ breach:

a. The County shall notify the Economic Services Administration (ESA) within one (1) business day of discovery of any unauthorized disclosure or access of ACES, SEMS, Employment Security (ES) information or any other state system. Notification to ESA shall be done by sending an email to databreach@dshs.wa.gov and the DCS Local Government Liaison.

b. If the breach involves possible IRS Data, the County shall follow the instructions above in Section 5.b. IRS Security Requirements.

10. RECORDS MAINTENANCE

The County and DSHS shall each maintain books, records, documents and other evidence which sufficiently and properly reflect all direct and indirect costs expended by either party in the performance of the services described herein. These records shall be subject to inspection, review, or audit by personnel of both parties, other personnel duly authorized by either party, the Office of the State Auditor, and federal officials so authorized by the law. The County shall retain all books, records, documents, and other material relevant to this agreement for six years after expiration, and the Office of the State Auditor, federal auditors, and any persons duly authorized by the parties shall have full access and the right to examine any of these materials during this period.

Records and other documents, in any medium, furnished by one party to this agreement to the other

party, will remain the property of the furnishing party, unless otherwise agreed. The receiving party will not disclose or make available this material to any third parties without first giving notice to the furnishing party and giving them a reasonable opportunity to respond except as required for purposes directly related with the administration of the Title IV-A, IV-D and Title IV-E programs. Each party will utilize reasonable security procedures and protections to assure that records and documents provided by the other party are not erroneously disclosed to third parties.

11. RIGHTS IN DATA

Unless otherwise provided, data which originates from this agreement shall be works for hire" as defined by the U.S. Copyright Act of 1976 and shall be owned by DSHS. Data shall include, but not be limited to, reports, documents, pamphlets, advertisements, books, magazines, surveys, studies, computer programs, films, tapes, and/or sound reproductions. Ownership includes the right to copyright, patent, register, and the ability to transfer these rights.

12. TERMINATION

DSHS may immediately terminate this agreement if it is determined that the provisions of this agreement are not being met.

Exhibit A – Data Security Requirements

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

   a. "AES" means the Advanced Encryption Standard, a specification of Federal Information Processing Standards Publications for the encryption of electronic data issued by the National Institute of Standards and Technology (http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf).

   b. "Authorized Users(s)" means an individual or individuals with a business need to access DSHS Confidential Information, and who has or have been authorized to do so.

   c. "Business Associate Agreement" means an agreement between DSHS and a contractor who is receiving Data covered under the Privacy and Security Rules of the Health Insurance Portability and Accountability Act of 1996. The agreement establishes permitted and required uses and disclosures of protected health information (PHI) in accordance with HIPAA requirements and provides obligations for business associates to safeguard the information.

   d. "Category 4 Data" is data that is confidential and requires special handling due to statutes or regulations that require especially strict protection of the data and from which especially serious consequences may arise in the event of any compromise of such data. Data classified as Category 4 includes but is not limited to data protected by: the Health Insurance Portability and Accountability Act (HIPAA), Pub. L. 104-191 as amended by the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH), 45 CFR Parts 160 and 164; the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. §1232g; 34 CFR Part 99; Internal Revenue Service Publication 1075 (https://www.irs.gov/pub/irs-pdf/p1075.pdf); Substance Abuse and Mental Health Services Administration regulations on Confidentiality of Alcohol and Drug Abuse Patient Records, 42 CFR Part 2; and/or Criminal Justice Information Services, 28 CFR Part 20.

   e. "Cloud" means data storage on servers hosted by an entity other than the Contractor and on a network outside the control of the Contractor. Physical storage of data in the cloud typically spans multiple servers and often multiple locations. Cloud storage can be divided between consumer grade storage for personal files and enterprise grade for companies and governmental entities. Examples of consumer grade storage would include iTunes, Dropbox, Box.com, and many other entities. Enterprise cloud vendors include Microsoft Azure, Amazon Web Services, and Rackspace.

   f. "Encrypt" means to encode Confidential Information into a format that can only be read by those possessing a "key"; a password, digital certificate or other mechanism available only to authorized users. Encryption must use a key length of at least 256 bits for symmetric keys, or 2048 bits for asymmetric keys. When a symmetric key is used, the Advanced Encryption Standard (AES) must be used if available.

   g. "FedRAMP" means the Federal Risk and Authorization Management Program (see www.fedramp.gov), which is an assessment and authorization process that federal government agencies have been directed to use to ensure security is in place when accessing Cloud computing products and services.

   h. "Hardened Password" means a string of at least eight characters containing at least three of the following four character classes: Uppercase alphabetic, lowercase alphabetic, numeral, and special characters such as an asterisk, ampersand, or exclamation point.

   i. "Mobile Device" means a computing device, typically smaller than a notebook, which runs a mobile operating system, such as iOS, Android, or Windows Phone. Mobile Devices include smart phones, most tablets, and other form factors.

j. "Multi-factor Authentication" means controlling access to computers and other IT resources by requiring two or more pieces of evidence that the user is who they claim to be. These pieces of evidence consist of something the user knows, such as a password or PIN; something the user has such as a key card, smart card, or physical token; and something the user is, a biometric identifier such as a fingerprint, facial scan, or retinal scan. "PIN" means a personal identification number, a series of numbers which act as a password for a device. Since PINs are typically only four to six characters, PINs are usually used in conjunction with another factor of authentication, such as a fingerprint.

k. "Portable Device" means any computing device with a small form factor, designed to be transported from place to place. Portable devices are primarily battery powered devices with base computing resources in the form of a processor, memory, storage, and network access. Examples include, but are not limited to, mobile phones, tablets, and laptops. Mobile Device is a subset of Portable Device.

l. "Portable Media" means any machine readable media that may routinely be stored or moved independently of computing devices. Examples include magnetic tapes, optical discs (CDs or DVDs), flash memory (thumb drive) devices, external hard drives, and internal hard drives that have been removed from a computing device.

m. "Secure Area" means an area to which only authorized representatives of the entity possessing the Confidential Information have access, and access is controlled through use of a key, card key, combination lock, or comparable mechanism. Secure Areas may include buildings, rooms or locked storage containers (such as a filing cabinet or desk drawer) within a room, as long as access to the Confidential Information is not available to unauthorized personnel. In otherwise Secure Areas, such as an office with restricted access, the Data must be secured in such a way as to prevent access by non-authorized staff such as janitorial or facility security staff, when authorized Contractor staff are not present to ensure that non-authorized staff cannot access it.

n. "Trusted Network" means a network operated and maintained by the Contractor, which includes security controls sufficient to protect DSHS Data on that network. Controls would include a firewall between any other networks, access control lists on networking devices such as routers and switches, and other such mechanisms which protect the confidentiality, integrity, and availability of the Data.

o. "Unique User ID" means a string of characters that identifies a specific user and which, in conjunction with a password, passphrase or other mechanism, authenticates a user to an information system.

2. **Authority**. The security requirements described in this document reflect the applicable requirements of Standard 141.10 (https://ocio.wa.gov/policies) of the Office of the Chief Information Officer for the state of Washington, and of the DSHS Information Security Policy and Standards Manual. Reference material related to these requirements can be found here: https://www.dshs.wa.gov/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 Contractor must have the following controls in place:

a. A documented security policy governing the secure use of its computer network and systems, and which defines sanctions that may be applied to Contractor staff for violating that policy.

b. If the Data shared under this agreement is classified as Category 4, the Contractor must be aware of and compliant with the applicable legal or regulatory requirements for that Category 4 Data.

c. If Confidential Information shared under this agreement is classified as Category 4, the Contractor must have a documented risk assessment for the system(s) housing the Category 4 Data.

4. **Authorization, Authentication, and Access.** In order to ensure that access to the Data is limited to authorized staff, the Contractor must:

a. Have documented policies and procedures governing access to systems with the shared Data.

b. Restrict access through administrative, physical, and technical controls to authorized staff.

c. Ensure that user accounts are unique and that any given user account logon ID and password combination is known only to the one employee to whom that account is assigned. For purposes of non-repudiation, it must always be possible to determine which employee performed a given action on a system housing the Data based solely on the logon ID used to perform the action.

d. Ensure that only authorized users are capable of accessing the Data.

e. Ensure that an employee's access to the Data is removed immediately:

(1) Upon suspected compromise of the user credentials.

(2) When their employment, or the contract under which the Data is made available to them, is terminated.

(3) When they no longer need access to the Data to fulfill the requirements of the contract.

f. Have a process to periodically review and verify that only authorized users have access to systems containing DSHS Confidential Information.

g. When accessing the Data from within the Contractor's network (the Data stays within the Contractor's network at all times), enforce password and logon requirements for users within the Contractor's network, including:

(1) A minimum length of 8 characters, and containing at least three of the following character classes: uppercase letters, lowercase letters, numerals, and special characters such as an asterisk, ampersand, or exclamation point.

(2) That a password does not contain a user's name, logon ID, or any form of their full name.

(3) That a password does not consist of a single dictionary word. A password may be formed as a passphrase which consists of multiple dictionary words.

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

h. When accessing Confidential Information from an external location (the Data will traverse the Internet or otherwise travel outside the Contractor's network), mitigate risk and enforce password and logon requirements for users by employing measures including:

(1) Ensuring mitigations applied to the system don't allow end-user modification.

(2) Not allowing the use of dial-up connections.

(3) Using industry standard protocols and solutions for remote access. Examples would include RADIUS and Citrix.

(4) Encrypting all remote access traffic from the external workstation to Trusted Network or to a component within the Trusted Network. The traffic must be encrypted at all times while traversing any network, including the Internet, which is not a Trusted Network.

(5) Ensuring that the remote access system prompts for re-authentication or performs automated session termination after no more than 30 minutes of inactivity.

(6) Ensuring use of Multi-factor Authentication to connect from the external end point to the internal end point.

i. Passwords or PIN codes may meet a lesser standard if used in conjunction with another authentication mechanism, such as a biometric (fingerprint, face recognition, iris scan) or token (software, hardware, smart card, etc.) in that case:

(1) The PIN or password must be at least 5 letters or numbers when used in conjunction with at least one other authentication factor

(2) Must not be comprised of all the same letter or number (11111, 22222, aaaaa, would not be acceptable)

(3) Must not contain a "run" of three or more consecutive numbers (12398, 98743 would not be acceptable)

j. If the contract specifically allows for the storage of Confidential Information on a Mobile Device, passcodes used on the device must:

(1) Be a minimum of six alphanumeric characters.

(2) Contain at least three unique character classes (upper case, lower case, letter, number).

(3) Not contain more than a three consecutive character run. Passcodes consisting of 12345, or abcd12 would not be acceptable.

k. Render the device unusable after a maximum of 10 failed logon attempts.

5. Protection of Data. The Contractor agrees to store Data on one or more of the following media and protect the Data as described:

a. **Hard disk drives**. For Data stored on local workstation hard disks, access to the Data will be restricted to Authorized User(s) by requiring logon to the local workstation using a Unique User ID and Hardened Password or other authentication mechanisms which provide equal or greater security, such as biometrics or smart cards.

b. **Network server disks**. For Data stored on hard disks mounted on network servers and made available through shared folders, access to the Data will be restricted to Authorized Users through the use of access control lists which will grant access only after the Authorized User has authenticated to the network using a Unique User ID and Hardened Password or other authentication mechanisms which provide equal or greater security, such as biometrics or smart cards. Data on disks mounted to such servers must be located in an area which is accessible only to authorized personnel, with access controlled through use of a key, card key, combination lock, or comparable mechanism.

For DSHS Confidential Information stored on these disks, deleting unneeded Data is sufficient as long as the disks remain in a Secure Area and otherwise meet the requirements listed in the above

paragraph. Destruction of the Data, as outlined below in Section 8 Data Disposition, may be deferred until the disks are retired, replaced, or otherwise taken out of the Secure Area.

c. **Optical discs (CDs or DVDs) in local workstation optical disc drives**. Data provided by DSHS on optical discs which will be used in local workstation optical disc drives and which will not be transported out of a Secure Area. When not in use for the contracted purpose, such discs must be Stored in a Secure Area. Workstations which access DSHS Data on optical discs must be located in an area which is accessible only to authorized personnel, with access controlled through use of a key, card key, combination lock, or comparable mechanism.

d. **Optical discs (CDs or DVDs) in drives or jukeboxes attached to servers**. Data provided by DSHS on optical discs which will be attached to network servers and which will not be transported out of a Secure Area. Access to Data on these discs will be restricted to Authorized Users through the use of access control lists which will grant access only after the Authorized User has authenticated to the network using a Unique User ID and Hardened Password or other authentication mechanisms which provide equal or greater security, such as biometrics or smart cards. Data on discs attached to such servers must be located in an area which is accessible only to authorized personnel, with access controlled through use of a key, card key, combination lock, or comparable mechanism.

e. **Paper documents**. Any paper records must be protected by storing the records in a Secure Area which is only accessible to authorized personnel. When not in use, such records must be stored in a Secure Area.

f. **Remote Access**. Access to and use of the Data over the State Governmental Network (SGN) or Secure Access Washington (SAW) will be controlled by DSHS staff who will issue authentication credentials (e.g. a Unique User ID and Hardened Password) to Authorized Users on Contractor's staff. Contractor will notify DSHS staff immediately whenever an Authorized User in possession of such credentials is terminated or otherwise leaves the employ of the Contractor, and whenever an Authorized User's duties change such that the Authorized User no longer requires access to perform work for this Contract.

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

(1) Except where otherwise specified herein, DSHS Data shall not be stored by the Contractor on portable devices or media unless specifically authorized within the terms and conditions of the Contract. If so authorized, the Data shall be given the following protections:

(a) Encrypt the Data.

(b) Control access to devices with a Unique User ID and Hardened Password or stronger authentication method such as a physical token or biometrics.

(c) Manually lock devices whenever they are left unattended and set devices to lock automatically after a period of inactivity, if this feature is available. Maximum period of inactivity is 20 minutes.

(d) Apply administrative and physical security controls to Portable Devices and Portable Media by:

i. Keeping them in a Secure Area when not in use,

ii. Using check-in/check-out procedures when they are shared, and

iii. Taking frequent inventories.

(2) When being transported outside of a Secure Area, Portable Devices and Portable Media with DSHS Confidential Information must be under the physical control of Contractor staff with authorization to access the Data, even if the Data is encrypted.

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

(1) DSHS Confidential Information may be stored on Portable Media as part of a Contractor's existing, documented backup process for business continuity or disaster recovery purposes. Such storage is authorized until such time as that media would be reused during the course of normal backup operations. If backup media is retired while DSHS Confidential Information still exists upon it, such media will be destroyed at that time in accordance with the disposition requirements below in Section 8 *Data Disposition*.

(2) Data may be stored on non-portable media (e.g. Storage Area Network drives, virtual media, etc.) as part of a Contractor's existing, documented backup process for business continuity or disaster recovery purposes. If so, such media will be protected as otherwise described in this exhibit. If this media is retired while DSHS Confidential Information still exists upon it, the data will be destroyed at that time in accordance with the disposition requirements below in Section 8 *Data Disposition*.

i. **Cloud storage**. DSHS Confidential Information requires protections equal to or greater than those specified elsewhere within this exhibit. Cloud storage of Data is problematic as neither DSHS nor the Contractor has control of the environment in which the Data is stored. For this reason:

(1) DSHS Data will not be stored in any consumer grade Cloud solution, unless all of the following conditions are met:

(a) Contractor has written procedures in place governing use of the Cloud storage and Contractor attests in writing that all such procedures will be uniformly followed.

(b) The Data will be Encrypted while within the Contractor network.

(c) The Data will remain Encrypted during transmission to the Cloud.

(d) The Data will remain Encrypted at all times while residing within the Cloud storage solution.

(e) The Contractor will possess a decryption key for the Data, and the decryption key will be possessed only by the Contractor and/or DSHS.

(f) The Data will not be downloaded to non-authorized systems, meaning systems that are not on either the DSHS or Contractor networks.

(g) The Data will not be decrypted until downloaded onto a computer within the control of an Authorized User and within either the DSHS or Contractor's network.

(2) Data will not be stored on an Enterprise Cloud storage solution unless either:

(a) The Cloud storage provider is treated as any other Sub-Contractor, and agrees in writing to all of the requirements within this exhibit; or,

(b) The Cloud storage solution used is FedRAMP certified.

(3) If the Data includes protected health information covered by the Health Insurance Portability and Accountability Act (HIPAA), the Cloud provider must sign a Business Associate Agreement prior to Data being stored in their Cloud solution.

6. **System Protection**. To prevent compromise of systems which contain DSHS Data or through which that Data passes:

   a. Systems containing DSHS Data must have all security patches or hotfixes applied within 3 months of being made available.

   b. The Contractor will have a method of ensuring that the requisite patches and hotfixes have been applied within the required timeframes.

   c. Systems containing DSHS Data shall have an Anti-Malware application, if available, installed.

   d. Anti-Malware software shall be kept up to date. The product, its anti-virus engine, and any malware database the system uses, will be no more than one update behind current.

7. **Data Segregation**.

   a. DSHS Data must be segregated or otherwise distinguishable from non-DSHS data. This is to ensure that when no longer needed by the Contractor, all DSHS Data can be identified for return or destruction. It also aids in determining whether DSHS Data has or may have been compromised in the event of a security breach. As such, one or more of the following methods will be used for data segregation.

      (1) DSHS Data will be kept on media (e.g. hard disk, optical disc, tape, etc.) which will contain no non-DSHS Data. And/or,

      (2) DSHS Data will be stored in a logical container on electronic media, such as a partition or folder dedicated to DSHS Data. And/or,

      (3) DSHS Data will be stored in a database which will contain no non-DSHS data. And/or,

      (4) DSHS Data will be stored within a database and will be distinguishable from non-DSHS data by the value of a specific field or fields within database records.

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

   b. When it is not feasible or practical to segregate DSHS Data from non-DSHS data, then both the DSHS Data and the non-DSHS data with which it is commingled must be protected as described in this exhibit.

8. **Data Disposition**. When the contracted work has been completed or when the Data is no longer needed, except as noted above in Section 5.b, Data shall be returned to DSHS or destroyed. Media on which Data may be stored and associated acceptable methods of destruction are as follows:

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 Contract within one (1) business day of discovery. If no DSHS Contact is designated in the Contract, then the notification must be reported to the DSHS Privacy Officer at dshsprivacyofficer@dshs.wa.gov. Contractor must also take actions to mitigate the risk of loss and comply with any notification or other requirements imposed by law or DSHS.

10. **Data shared with Subcontractors**. If DSHS Data provided under this Contract is to be shared with a subcontractor, the Contract with the subcontractor must include all of the data security provisions within this Contract and within any amendments, attachments, or exhibits within this Contract. If the Contractor cannot protect the Data as articulated within this Contract, then the contract with the sub-Contractor must be submitted to the DSHS Contact specified for this contract for review and approval.

Exhibit B – IRS Publication 1075

Exhibit 7 Safeguarding Contract Language

I.PERFORMANCE

In performance of this contract, the Contractor agrees to comply with and assume responsibility for compliance by officers or employees with the following requirements:

(1) All work will be performed under the supervision of the contractor.

(2) The contractor and contractor's officers or employees to be authorized access to FTI must meet background check requirements defined in IRS Publication 1075. The contractor will maintain a list of officers or employees authorized access to FTI. Such list will be provided to the agency and, upon request, to the IRS.

(3) FTI in hardcopy or electronic format shall be used only for the purpose of carrying out the provisions of this contract. FTI in any format shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Inspection or disclosure of FTI to anyone other than the contractor or the contractor's officers or employees authorized is prohibited.

(4) FTI will be accounted for upon receipt and properly stored before, during, and after processing. In addition, any related output and products require the same level of protection as required for the source material.

(5) The contractor will certify that FTI processed during the performance of this contract will be completely purged from all physical and electronic data storage with no output to be retained by the contractor at the time the work is completed. If immediate purging of physical and electronic data storage is not possible, the contractor will certify that any FTI in physical or electronic storage will remain safeguarded to prevent unauthorized disclosures.

(6) Any spoilage or any intermediate hard copy printout that may result during the processing of FTI will be given to the agency. When this is not possible, the contractor will be responsible for the destruction of the spoilage or any intermediate hard copy printouts and will provide the agency with a statement containing the date of destruction, description of material destroyed, and the destruction method.

(7) All computer systems receiving, processing, storing, or transmitting FTI must meet the requirements in IRS Publication 1075. To meet functional and assurance requirements, the security features of the environment must provide for the managerial, operational, and technical controls. All security features must be available and activated to protect against unauthorized use of and access to FTI.

(8) No work involving FTI furnished under this contract will be subcontracted without the prior written approval of the IRS.

(9) Contractor will ensure that the terms of FTI safeguards described herein are included, without modification, in any approved subcontract for work involving FTI.

(10) To the extent the terms, provisions, duties, requirements, and obligations of this contract apply to performing services with FTI, the contractor shall assume toward the subcontractor all obligations, duties and responsibilities that the agency under this contract assumes toward the contractor, and the subcontractor shall assume toward the contractor all the same obligations, duties and responsibilities which the contractor assumes toward the agency under this contract.

(11) In addition to the subcontractor's obligations and duties under an approved subcontract, the terms and conditions of this contract apply to the subcontractor, and the subcontractor is bound and obligated to the contractor hereunder by the same terms and conditions by which the contractor is bound and obligated to the agency under this contract.

(12) For purposes of this contract, the term "contractor" includes any officer or employee of the contractor with access to or who uses FTI, and the term "subcontractor" includes any officer or employee of the subcontractor with access to or who uses FTI.

(13) The agency will have the right to void the contract if the contractor fails to meet the terms of FTI safeguards described herein.

II. CRIMINAL/CIVIL SANCTIONS

(1) Each officer or employee of a contractor to whom FTI is or may be disclosed shall be notified in writing that FTI disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any FTI for a purpose not authorized herein constitutes a felony punishable upon conviction by a fine of as much as $5,000 or imprisonment for as long as 5 years, or both, together with the costs of prosecution.

(2) Each officer or employee of a contractor to whom FTI is or may be accessible shall be notified in writing that FTI accessible to such officer or employee may be accessed only for a purpose and to the extent authorized herein, and that access/inspection of FTI without an official need-to-know for a purpose not authorized herein constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as $1,000 or imprisonment for as long as 1 year, or both, together with the costs of prosecution.

(3) Each officer or employee of a contractor to whom FTI is or may be disclosed shall be notified in writing that any such unauthorized access, inspection or disclosure of FTI may also result in an award of civil damages against the officer or employee in an amount equal to the sum of the greater of $1,000 for each unauthorized access, inspection, or disclosure, or the sum of actual damages sustained as a result of such unauthorized access, inspection, or disclosure, plus in the case of a willful unauthorized access, inspection, or disclosure or an unauthorized access/inspection or disclosure which is the result of gross negligence, punitive damages, plus the cost of the action. These penalties are prescribed by IRC sections 7213, 7213A and 7431 and set forth at 26 CFR 301.6103(n)-1.

(4) Additionally, it is incumbent upon the contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to contractors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.

(5) Granting a contractor access to FTI must be preceded by certifying that each officer or employee understands the agency's security policy and procedures for safeguarding FTI. A contractor and each officer or employee must maintain their authorization to access FTI through annual recertification of their understanding of the agency's security policy and procedures for safeguarding FTI. The initial certification and recertifications must be documented and placed in the agency's files for review. As part of the certification and at least annually afterwards, a contractor and each officer or employee must be advised of the provisions of IRC sections 7213, 7213A, and

7431 (see Exhibit 4, *Sanctions for Unauthorized Disclosure*, and Exhibit 5, *Civil Damages for Unauthorized Disclosure*). The training on the agency's security policy and procedures provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches. (See Section 10) For the initial certification and the annual recertifications, the contractor and each officer or employee must sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

III. **INSPECTION**

The IRS and the Agency, with 24 hour notice, shall have the right to send its inspectors into the offices and plants of the contractor to inspect facilities and operations performing any work with FTI under this contract for compliance with requirements defined in IRS Publication 1075. The IRS' right of inspection shall include the use of manual and/or automated scanning tools to perform compliance and vulnerability assessments of information technology (IT) assets that access, store, process or transmit FTI. Based on the inspection, corrective actions may be required in cases where the contractor is found to be noncompliant with FTI safeguard requirements.

Exhibit C Access to ACES

1. INTRODUCTION

DSHS is the single state agency responsible for the administration of cash, food stamp, and medical assistance programs. As a condition of eligibility for Temporary Assistance to Needy Families (TANF) cash and TANF related medical only, custodial parent must refer responsible parents to the Division of Child Support (DCS) for collection of child support, paternity establishment, require obligated parents to provide health insurance coverage, and establish support orders. DCS also establishes paternity, creates support orders, and collects child support for federal and state funded foster care. DCS is the organizational unit responsible for administration, supervision and monitoring of Washington State's Child Support Enforcement program and the State Plan under Title IV-D of the Social Security Act.

The Prosecuting Attorney is empowered by state law to pursue judicial actions for determinations of parentage, establish, modify, and enforce support obligations.

2. DESCRIPTION OF DATA

Case information is maintained primarily in an electronic file. Access will enable the Prosecuting Attorneys to efficiently and effectively pursue actions related to Child Support Enforcement. Prosecuting Attorneys must use this confidential information strictly for purposes directly related to the administration of this agreement.

3. ACCESS TO DATA

a. METHOD OF ACESS/TRANSFER

(1) All Counties have access via TCP/IP connections on either the Washington State Government Network (SGN) or the Inter-Governmental Network (IGN) that meet both parties' security requirements and are equipped with Windows 7 or Windows 10 and IP numbers and they may access ACES-Online via a web browser interface.

(2) Data under this agreement shall be accessed through the on-line workstations attached to the IGN or SGN through the local area network (LAN). A dial-up or broadband connection utilizing VPN (Virtual Private Network) may be used on a limited basis in order to enter specific client data and review existing caseload information as described above. Access through the Internet will be secured through the state fortress server.

(3) Access to data shall be limited to authorized staff whose duties require access to such data in the performance of their assigned duties. The PA shall immediately inform DSHS ACES/IT Help Desk security at (360) 664-4560, when staff are terminated from employment, or no longer need access to either the ACES mainframe or ACES Online.

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

(5) DSHS reserves the right to revoke, at any time, an individual's authorization to access data. User IDs and passwords shall not be shared by staff.

(6) DSHS will provide technical training (through DCS) to County Prosecuting Attorneys and other county personnel who will access ACES.

(7) DSHS will provide the Prosecuting Attorney limited access to the ACES mainframe and ACES On-line. The Prosecuting Attorney agrees to abide by DSHS guidelines for the access, use, transmission, and disclosure of Data.

b. PERSONS HAVING ACCESS TO DATA

(1) The County shall ensure that only Prosecuting Attorneys have access to ACES records. The Contractor shall assign a security monitor as a point of contact for ACES. The security monitor will route access requests through the ESA Operations Support Division Central Support Help Desk.

(2) The County security monitor must notify the ESA Central Support Help Desk immediately when Contractor staff that have access to ACES are terminated from employment.

(3) All client records are confidential and shall only be used for the purposes of this agreement.

c. FREQUENCY OF DATA EXCHANGE

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

4. ADDITIONAL SECURITY OF DATA REQUIREMENTS

In addition to the data security requirements in Exhibit A, the County shall:

a. Provide security measures required by DSHS (and all applicable laws) needed to keep the information confidential and limit access only to authorized information..

b. Take reasonable precautions to secure against unauthorized physical and electronic access to data, which shall be protected in a manner that prevents unauthorized persons, including the general public, from retrieving Data by means of computer, remote terminal, or other means. The Counties agrees not to copy or retain information provided via ACES regardless of format.

c. Notify the ESA Operations Support Division Central Support Help Desk within one (1) business day if unauthorized disclosure is discovered by the Contractor.

d. Remove date received under this Agreement from computer equipment after its been used for its stated purposes by using a "WIPE" utility for purging the Data from electronic storage media, degaussing the media, or physically destroying the media in such a way that Data cannot be recovered. Media includes, but is not limited to, the following:

(1) Hard drives (workstation and network) – Zero-fill or Wipe utility to destroy data in file space Floppy disks

(2) Floppy disks – Physical destruction of the media

(3) Magnetic tapes (reels or cartridges) – Degaussing or cross-cut shredding of the tape

(4) CDs/DVDs – Scour readable (label) side with a coarse abrasive or shred

(5) Zip/JAZZ disks and other removable magnetic media (other than floppy disks) – Media and associated acceptable data destruction methods are: Zero-fill or Wipe utility

(6) Flash memory and memory cards (Compact Flash, Secure Digital, Memory Stick, etc.) – Zero fill or Wipe utility

e. Disks and/or documents generated in printed form from the electronic file shall be properly returned, destroyed or shredded when no longer needed so unauthorized individuals cannot access client information. Data destroyed shall include all copies of any data sets in possession after the data

has been used for the purpose specified herein or 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.

f. Ensure any data placed on portable devices must be protected by:

(1) Encrypting the data,

(2) Controlling access to the device with a password or stronger authentication devices such as tokens or biometrics,

(3) Manually locking the devices whenever it is left unattended and setting the device to lock automatically after a period of inactivity, if this feature is available. Maximum period of inactivity is 20 minutes, and;

(4) Physically protect the portable devices(s) by keeping them in locked storage when not in use.

(5) When not in use, hard copies of the data shall be stored in a locked cabinet or other secure location to which only authorized users have access.

g. The Contractor shall protect information according to state and federal laws including the following, incorporated by reference:

(1) RCW 74.04 General Provisions - Administration

(2) RCW 42.56 Public Records

5. CONFIDENTIALITY AND NONDISCLOSURE

a. The information to be shared under this Agreement is confidential in nature and is subject to state and federal confidentiality requirements. The County shall maintain the confidentiality of client information in accordance with state and federal laws.

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

c. The County, its employees and contracted staff may use confidential Information or data gained by reason of this Agreement only for the purpose of this Agreement.

d. The County must be willing to obtain written consent in advance, as appropriate, on forms that meet DSHS standards, before accessing client information housed in ACES, if required.

e. The County shall not disclose, in whole or in part, the data described in this agreement to any individual or agency not specifically authorized by federal or state law, rule or regulation. Client data is confidential and is protected by various state and federal laws. RCW 74.04.060 currently requires that information about public assistance applicants and recipients shall not be disclosed except for purposes directly connected with the administration of programs under Title 74 of the Revised Code of Washington. Other pertinent laws currently include 42 U.S.C. 602(a)(1)(A)(iv); 45 CFR 205.50 and RCW 42.56.10.

f. Violations of the non-disclosure provisions of this agreement may result in criminal or civil penalties. Violation is a gross misdemeanor under RCW 74.04.060, punishable by imprisonment of not more than one year and/or a fine not to exceed five thousand dollars.

g. The County must provide a signed Notice of Nondisclosure form from all employees with access to

the data to remind them of the limitations, use or publishing of data. The Contractor shall retain a copy of the Notice of Nondisclosure form on file for monitoring purposes and forward the ***original*** to the Government Liaison located in the Division of Child Support.

h. The County shall ensure all employees electronically read, acknowledge, and accept data access and nondisclosure restrictions annually in order to continue access and use of SEMS and related databases.

i. During the term of this Agreement the County shall give DSHS reasonable access to the Contractor's records in order to monitor, audit, and evaluate the Contractor's performance and compliance with applicable laws, regulations, and this Agreement.

j. Protect data from access by the general public. In addition, reasonable precautions shall be taken to secure the data from other individuals who are not authorized access to the data.

k. Ensure client information will be used only for purposes directly related to the prosecution of Child Support Enforcement cases. Any personal use of client information is strictly prohibited.

l. The County shall not use or disclose Personal Information in any manner that would constitute a violation of federal law, the Health Information Portability and Accountability Act of 1996 (HIPAA) or any regulations enacted or revised pursuant to the HIPAA provisions and applicable provisions of Washington State law. The County agrees to comply with all federal and state laws and regulations, as currently enacted or revised, regarding data security and electronic data interchange.

m. The County shall ensure these guidelines are included in any subcontract they may enter into. the Contractor shall be responsible for the acts and omissions of any of its subcontractors.