Approved: 4/26/2023
Effective: 5/19/2023

SNOHOMISH COUNTY COUNCIL
SNOHOMISH COUNTY, WASHINGTON

ORDINANCE NO. 23-022

APPROVING AGREEMENT WITH WASHINGTON STATE DEPARTMENT OF SOCIAL AND HEALTH SERVICES TO ASSIST RECIPIENTS OF TEMPORARY ASSISTANCE FOR NEEDY FAMILIES THROUGH THE WORKFIRST PROGRAM

WHEREAS, the Snohomish Health District was integrated into Snohomish County effective December 31, 2022, and now operates as the Snohomish County Health Department; and

WHEREAS, prior to its integration into Snohomish County, the Snohomish Health District entered into a program agreement with Washington State Department of Social and Health Services to assist recipients of Temporary Assistance for Needy Families (TANF) to meet their goals and provide well-being for their family through the WorkFirst Program; and

WHEREAS, the Washington State Department of Social and Health Services and the Snohomish County Health Department wish to continue this partnership; and

WHEREAS, the County Council held a public hearing on April 26, 2023, to consider approving the program agreement with Washington State Department of Social and Health Services and to authorize the Snohomish County Executive to enter into such agreement in substantially the form attached as Exhibit A;

NOW, THEREFORE, BE IT ORDAINED:

Section 1. The County Council hereby adopts the foregoing recitals as findings of fact and conclusions as if set forth in full herein.

Section 2. The County Council hereby authorizes the County Executive, or designee, to execute the program agreement between Snohomish County and Washington State Department of Social and Health Services in substantially the form attached hereto as Exhibit A.

PASSED this 26th day of April, 2023.

SNOHOMISH COUNTY COUNCIL
Snohomish County, Washington

Jared Mead
Chairperson

ATTEST:

Deputy Clerk of the Council

(X) APPROVED
( ) EMERGENCY
( ) VETOED

DATE: May 9, 2023

County Executive

ATTEST:

Approved as to form only:

Deputy Prosecuting Attorney

EXHIBIT A

Washington State Department of Social & Health Services	**COUNTY** **PROGRAM AGREEMENT** **WorkFirst** **Children with Special Needs**	DSHS Agreement Number 2363-46789

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	Community Services Division	1065	3003CS-63

DSHS CONTACT NAME AND TITLE	DSHS CONTACT ADDRESS
Anne Cervantes Regional WorkFirst Coordinator	840 N. Broadway Suite 200 Everett, WA 98201

DSHS CONTACT TELEPHONE	DSHS CONTACT FAX	DSHS CONTACT E-MAIL
(206) 402-2560	Click here to enter text.	anne.cervantes@dshs.wa.gov

COUNTY NAME	COUNTY ADDRESS
Snohomish County Snohomish County Health Department	3020 Rucker Ave Suite 203 Everett, WA 98201

COUNTY CONTACT NAME
Katie Curtis

COUNTY CONTACT TELEPHONE	COUNTY CONTACT FAX	COUNTY CONTACT E-MAIL
(425) 339-8711		katie.curtis@co.snohomish.wa.us

IS THE COUNTY A SUBRECIPIENT FOR PURPOSES OF THIS PROGRAM AGREEMENT?No		ASSISTANCE LISTING NUMBERS
PROGRAM AGREEMENT START DATE 01/01/2023	**PROGRAM AGREEMENT END DATE** 06/30/2023	MAXIMUM PROGRAM AGREEMENT AMOUNT $3,575.00

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**
☒ **Exhibit B – Statement of Work:Children with Special Needs Evaluation; and Exhibit C – Monthly Report**
☐ **Other Exhibits (specify):**

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
	Dave Somers, County Executive	May 9, 2023
DSHS SIGNATURE	**PRINTED NAME AND TITLE**	**DATE SIGNED**
	Alice Hildebrant, Contracts Officer	May 9, 2023

COUNCIL USE ONLY
Approved 4/26/2023
ECAF # 2023-0272
MOT/ORD Ordinance 23-022

SPECIAL TERMS AND CONDITIONS

1. Definitions.

The words and phrases listed below, as used in this Contract, shall each have the following definitions:

a. "CSD" means the DSHS, Economic Services Administration (ESA,) Community Services Division (CSD).

b. "Data" means any Personal Information, and/or other information accessed and gained while providing services in association with this Contract.

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

d. "TANF" means Temporary Assistance for Needy Families.

e. "WorkFirst Program" means Washington State's program to assist recipients of Temporary Assistance for Needy Families (TANF) to meet their goals and provide well-being for their family.

f. "DSHS Contact" means the DSHS Contact listed on page one (1) of this Contract.

g. "Personnel" means the Contractor's employees, or subcontractors employees and or volunteers.

2. Purpose.

The purpose of this Contract is as set forth in attached Exhibit(s).

3. Statement of Work.

The Contractor shall provide the services and staff, and otherwise do all things necessary for or incidental to the performance of work, as set forth in the attached Exhibit(s).

4. Consideration.

Total consideration payable to Contractor for satisfactory performance of the work under this Contract, shall be paid in accordance with the fees set forth in the attached Exhibit(s).

Total consideration payable for the contract period to the Contractor for satisfactory work performance including any and all expenses under this Contract is up to a maximum of $ 3,575.

Unspent funds designated for any State Fiscal Year shall remain unspent and may not be carried forward into the following State Fiscal Year.

5. Billing and Payment.

a. Invoice System. The Contractor shall submit invoices using State Form A-19 Invoice Voucher, or such other form as designated by DSHS. Consideration for services rendered shall be payable upon receipt of properly completed invoices, which shall be submitted to the DSHS Contact. The Contractor shall submit one (1) invoice for each month. Invoices must be received by the DSHS Contact no later than thirty (30) calendar days after the last day of each month. The invoices shall describe and document to DSHS' satisfaction a description of the work performed, activities accomplished, and fees.

b. Payment. Payment shall be considered timely if made by DSHS within thirty (30) days after receipt and acceptance by DSHS of the properly completed invoices. Payment shall be sent to the

address designated by the Contractor on page one (1) of this Contract. DSHS may, at its sole discretion, withhold payment claimed by the Contractor for services rendered if Contractor fails to satisfactorily comply with any term or condition of this Contract.

6. Child Abuse and Health and Safety Concerns.

In the delivery of services under this Contract, the health and safety of children and vulnerable adults shall always be the first concern of the Contractor. The Contractor shall immediately report all instances of suspected child or vulnerable adult abuse to Child Protective Services at 1-866-END HARM.

7. Fraud Reporting.

The Contractor shall report any knowledge of welfare fraud by calling 1-800-562-6906 or online at https://wadshs.libera.com/Sys7CMSPortal-FCMS-WA/fraud/report.aspx.

8. Contractor Information.

The Contractor shall forward to the DSHS Contact (or successor) within ten (10) working days, any information concerning the Contractor's change of circumstances. Changes in the Contractor's circumstances include change of business name, address, telephone number, fax number, e-mail address, business status and names of staff who are current state employees.

9. Contract Suspension.

DSHS may take certain actions in the event the Contractor, or any of its partners, officers, directors, or employees, is investigated by a local, county, state or federal agency, for a matter which DSHS determines may adversely affect the delivery of services provided under this Contract. DSHS may, without prior notice, either suspend the delivery of services or disallow the person(s) involved in the allegation(s) from providing services or having contact with clients pending final resolution of the investigation.

10. Criminal History Background Checks.

a. **The Contractor Must:**

(1) Have current Background checks on file for any employee, subcontractor and/or volunteer, who will provide direct, one-on-one services to DSHS clients under this contract. Require a DSHS executed criminal background check for each employee and volunteer who will provide direct, one-on-one services to DSHS clients under this contract. The Contractor will obtain a DSHS Background Check Authorization form 09-653 provided by the DSHS Contract Contact listed on page one (1) of this contract, or their designee. Email or fax the Background Check Authorization form to the DSHS Contact, or their designee.

(2) Require if the employee has lived outside of the State of Washington at any time during the past three (3) years, an FBI background check to be completed which requires that the employee be fingerprinted.

(3) Verify that for personnel who have a criminal record that the crime is not "disqualifying" as described on the DSHS Secretary's List of Crimes & Negative Actions. DSHS will provide the Contractor with the DSHS Secretary's List of Crimes & Negative Actions. Personnel with a disqualifying crime are prohibited from providing direct, one-on-one services to DSHS clients under this contract. The Contractor can review what crimes are "disqualifying" as listed in the

following link to the DSHS Secretary's List of Crimes & Negative Actions.

(4) Provide the DSHS contract contact listed on page one (1) of this contract, or their designee, with a list of employees, subcontractors and/or volunteers who will be providing direct, one-on-one services to DSHS clients and have successfully passed a Criminal Background check. Send an updated list to the DSHS contract contact, or their designee, when there are changes in personnel providing direct, one-on-one client services under this contract.

b. The DSHS Contract Contact, or their designee, will receive the background check results and will determine if the applicant "passed" the background check. DSHS will notify the Contractor if Contractor staff or volunteers:

(1) Have a record of disqualifying crime(s). The Contractor shall not hire or retain, directly or by contract, any individual having direct contact with vulnerable adults to work under this contract if the individual has a record of disqualifying crime(s).

(2) In the case of an employee or volunteer having a record of a past crime that is not a disqualifying crime, the Contractor will need to consider character, competence, and suitability of this individual. The Contractor would then weigh the risks before allowing them to have unsupervised access to DSHS clients.

c. Copy of Criminal Background Check result is not provided to the Contractor. Criminal Background Check results are kept confidential between DSHS and the Contractor's staff or volunteers.

d. Background check results will remain in effect for the period of performance of the contract.

e. The Contractor shall conditionally employ an individual without allowing said individual to have direct one-on-one contact with vulnerable adults pending completion of a Criminal Background Check.

f. Provide background check information to DSHS upon request and/or during contract monitoring activities.

11. Notice of Nondisclosure.

The Contractor shall:

a. Ensure each employee, volunteer, etc. who will have access to client confidential information signs an "ESA Nondisclosure of Confidential Information Agreement – Non-Employee" (hereafter, referenced as "Nondisclosure form") provided by DSHS when a new contract is issued and signed annually thereafter.

b. Remind employees, volunteers, etc. annually of DSHS nondisclosure requirements.

c. Retain copies of all signed nondisclosure forms on file for monitoring purposes and must be made available for DSHS review upon request.

d. DSHS will only grant access to client confidential data as required to provide services under this contract.

e. Take precautions to secure against unauthorized physical and electronic access to client data in a manner to prevent unauthorized access persons, including the public, from retrieving data by means of computer, remote terminal, or other means.

f. Take note that violations of the nondisclosure provisions of this contract 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. Sanctions also may apply under other state and federal law, including civil and criminal penalties for violations of the HIPAA Privacy and Security rules.

12. Data Sharing - Access to eJAS.

a. Data Access:

The Contractor shall limit access to DSHS data to authorized personnel whose duties specifically require access to such data in the performance of their assigned duties.

b. Description of Data:

(1) Data Elements:

Client's personal data including but not limited to:

(a) Name.

(b) Date of birth.

(c) Social security number.

(d) Address.

(e) Household composition.

(f) Employer and wage information.

(g) Component history, not including confidential components such as family violence, chemical dependency, mental health, and HIV/AIDS.

(h) Individual Responsibility Plans (IRP's).

(i) eJAS notes, not including notes pertaining to confidential information pertaining to family violence, chemical dependency, mental health, and HIV/AIDS.

c. Frequency and time frame(s) for data disclosure or exchange:

Contractor will have daily access to eJAS for the duration of the Contract.

d. Access to eJAS.

(1) The eJAS access level for the personnel will be as authorized by DSHS.

(2) The Contractor shall access eJAS through on-line personal computers attached to a Local Area Network (LAN) or dial-up connection on a secured Internet connection. All transactions shall be secured through the Washington State Fortress server.

(3) The Contractor shall provide the DSHS Contact a list of personnel that will have access to DSHS client data and or will have access to eJAS.

(a) The Contractor shall provide this information within one month after the Contract start date.

(b) If there are any changes to this list, within ten (10) business days, the Contractor shall provide the DSHS Contact an updated list.

(4) The Contractor shall contact the DSHS Contact whenever they need to increase the number of their staff that are granted access to eJAS.

(5) The Contractor shall notify the DSHS Contact when any personnel with access to DSHS client data is terminated from employment or when their duties no longer require access to DSHS client data.

(6) The Contractor shall provide staff with appropriate privacy and confidentiality training and ensure staff, contractors, and subcontractors read and sign **ESA Nondisclosure of Confidential Information Agreement – Non Employee** form, prior to initial access and annually thereafter. The DSHS Contact, or their designee, will provide the Contractor with the form.

(a) The Contractor shall retain the original signed copies of the forms for their records.

(b) Upon DSHS request, the Contractor shall provide DSHS with copies of the signed forms.

(7) DSHS reserves the right to revoke, at any time, an individual's authorization to access information. DSHS shall send a written Notice Termination of Access, effective no later than date of receipt, to the affected individual. Such notice shall be made by certified mail.

(8) The Contractor or their personnel may not release any DSHS data to any other agency or person without the specific written consent of the client.

(9) Unauthorized disclosure of data is a gross misdemeanor, punishable by law.

(10) The Contractor is subject to the same standards and laws of confidentiality as is DSHS.

13. Data Confidentiality.

All data within eJAS belongs to DSHS. The contractor shall not use, publish, transfer, sell or otherwise disclose any Confidential Information gained for any purpose that is not directly connected with the purpose of this Contract set out in the Special Terms and Conditions except with the prior written consent of DSHS.

14. Data Breach.

Specific to this Agreement if any employee becomes aware of compromise or potential compromise of Confidential Information, the employee must immediately contact the ESA Privacy Officer and Security Contact (DSHS: dshsprivacyofficer@dshs.wa.gov and ESA: esadsa@dshs.wa.gov) within one (1) business day of discovery. The notifying party must also take actions to mitigate the risk of loss and comply with any notification or other requirements imposed by law.

15. Re-disclosure of Data.

The data to be shared under this Contract is confidential and is subject to state and federal confidentiality requirements and all confidentiality and data use terms and conditions provided in the Contract.

SPECIAL TERMS AND CONDITIONS

16. Consent.

a. The Contractor must obtain and retain a **valid written consent form signed in advance by the client** that allows DSHS to share information with the Contractor. The form must meet the DSHS authorization standards, or get DSHS approval on Contractors consent language. The contractor can request the **DSHS consent form 14-012(x)** from the DSHS contact.

b. The Contractor must retain copies of the signed application and consent form(s) on file in either an electronic format, hardcopy format, or both for monitoring purposes. Contractor must make these forms available to DSHS Contact upon request.

c. The Contractor agrees not to access any other clients' data in eJAS who hasn't applied for Contractor's services or who have not signed a consent.

17. Contract Monitoring.

The Contractor's records related to this Contract will be reviewed for compliance with terms and conditions. DSHS reserves all other rights of inspection as provided in the General Terms and Conditions of the Contract.

18. Subcontracting.

The Contractor is prohibited from subcontracting services under this contract.

19. Interpretation and Translation Services.

The Contractor shall provide interpreter and translation services as necessary to perform the obligations of this Contract, and DSHS shall not reimburse the Contractor for the use of interpreter or translation services, except if specifically stated in an Exhibit of this Contract.

20. Participant Referrals.

DSHS, at its sole discretion, shall refer participants to the Contractor on an as-needed basis, and does not guarantee any participants shall be referred to the Contractor during the period of performance of this Contract. DSHS reserves the right to withdraw any participant(s) referred to the Contractor.

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	Using a “wipe” utility which will overwrite the Data at least three (3) times using either random or single character data, or

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

Statement of Work
Children with Special Needs Evaluation

1. Definitions.

a. "Case staffing" means a meeting, facilitated by the WorkFirst Social Worker or Case Manager, which may include but is not limited to; the parent(s), Public Health Nurse, representatives of Developmental Disabilities, Children's Administration, child care provider, or others invited by the parent or DSHS staff.

b. "Children with Special Needs" for purposes of this contract means, children age 0-18 (up through age 21 if enrolled in Special Education or the Division of Developmental Disabilities) having a medical, developmental, mental health, or behavioral issue that requires specialized care.

c. "DSHS Staff" means the WorkFirst Social Worker, WorkFirst Case Manager, WorkFirst Supervisor, or other Community Services Division staff acting on behalf of the WorkFirst staff authorizing the evaluation or re-evaluation.

d. "Follow-Up Evaluation" means all subsequent evaluations occurring within one (1) calendar year of the date of the initial evaluation regardless of program or fiscal year.

2. Purpose.

The purpose of this contract is for the Contractor to assist DSHS staff in determining a parent's ability to participate in the WorkFirst program through an evaluation of a child's special needs.

3. Contractor Obligations.

The Contractor shall:

a. Contact the parent within five (5) working days of receipt of a DSHS referral to arrange an appointment with the parent.

b. Contact DSHS staff within one (1) business day if the parent misses the prearranged appointment or refuses the evaluation.

c. Assess the impact of a child's special needs using the Special Needs Evaluation and Engagement Recommendations form (DSHS 10-255). (Forms are available through the DSHS contact).

d. Complete evaluation within ten (10) business days of contacting the parent. If the evaluation cannot be completed within ten (10) business days the Public Health Nurse will contact DSHS staff. DSHS staff will either approve an extension past ten (10) business days, (not to exceed thirty (30) business days) or request that the parent be referred back.

e. Return the evaluation form (DSHS 10-255) within ten (10) business days of completing the evaluation.

f. Attend DSHS case staffing meetings as requested.

g. Provide a one-time consultation with the parent and child care provider to determine if child care is appropriate.

h. Refer parents to community resources, such as Childcare Resource and Referral, HeadStart, and other resources.

i. Conduct follow-up evaluations and return the evaluation form (DSHS 10-255) when requested and approved by DSHS staff.

4. Reporting Requirements.

The Contractor shall:

a. Return the completed evaluation form (DSHS 10-255) the DSHS staff making the referral within (10) business days of date of the evaluation;

b. Submit a completed Monthly Report (Exhibit C) or attach a copy of the completed evaluations with each billing invoice.

When approved by DSHS staff, the contractor may also choose to use the eJAS system to provide additional documentation. EJAS documentation cannot be substituted for the DSHS 10-255.

5. eJAS Reporting.

The Contractor shall:

a. Use the Contractor Caseload screen:

b. Accept or reject each referral within three (3) business days of receipt.

c. Enter the evaluation start and end dates on or within ten (10) business days following the evaluation end date.

d. Notify DSHS staff within one (1) business day when the client has not been present for the pre-arranged evaluation appointment.

e. Document findings within ten (10) business days of completing an evaluation or appraisal

6. Compensation.

DSHS shall compensate the Contractor for the following:

a. Payment Point #1:

$ 325 for each child for whom an evaluation was completed and returned to DSHS staff.

b. Payment Point #2:

$ 225 for each child whom a DSHS authorized, follow-up evaluation was completed and returned to DSHS staff.

Note: Payment points include consultation with DSHS staff, the parent, and/or child care provider when requested and DSHS staff.

Exhibit C

Monthly Report

Contractor ID: _____

Service Month: _____

eJAS or Client ID	Comments

APPROVED: _____

DIRECTIONS: At minimum the eJAS or Client ID must be listed for each client who received services in the service month. Comments such as a summary of services received may be entered.