JEFFERSON COUNTY
BOARD OF COUNTY COMMISSIONERS

AGENDA REQUEST

TO: **Board of Commissioners**

FROM: **Shannon S. Burns, Juvenile Court Administrator**

DATE: 3/20/2023

RE: **Contract Amendment DCYF**

STATEMENT OF ISSUE: The original contract included reimbursement to the County for quality assurance performed by Jefferson County Juvenile Services staff for statewide implementation of i-ACT, Individual Alternative Choice Training, a promising program for court involved youth. Due to position changes within Juvenile Services, new hire and promotion, the amount of work towards this contract has been reduced. The funds we cannot use can be reallocated on a State level.

ANALYSIS: None

FISCAL IMPACT: The original contract amount of $60,388.00 will be reduced to $48,388.00 ($12,000 reduction)

RECOMMENDATION:

That the Board approve the amended agreement.

REVIEWED BY:

Mark McCauley, County Administrator — Date 3/15/23

CONTRACT AMENDMENT
i-ACT Program Development

DCYF CONTRACT NUMBER:
2163-24537

Amendment No. 01

This Contract Amendment is between the State of Washington Department of Children, Youth & Families (DCYF) and the Contractor identified below.

Program Contract Number
Click here to enter text.
Contractor Contract Number

CONTRACTOR NAME Jefferson County	CONTRACTOR doing business as (DBA)		
CONTRACTOR ADDRESS PO Box 1220 Port Townsend, WA 98368-	WASHINGTON UNIFORM BUSINESS IDENTIFIER (UBI) 161-001-169	DCYF INDEX NUMBER 1223	
CONTRACTOR CONTACT Shannon Burns	CONTRACTOR TELEPHONE (360) 385-9190	CONTRACTOR FAX Click here to enter text.	CONTRACTOR E-MAIL ADDRESS Sburns@co.jefferson.wa.us
DCYF ADMINISTRATION Department of Children, Youth, and Families	DCYF DIVISION Children, Youth and Families	DCYF CONTRACT CODE 2000CC-63	
DCYF CONTACT NAME AND TITLE Karena McGovern Contract Specialist	DCYF CONTACT ADDRESS 1115 Washington St SE Olympia, WA 98504		
DCYF CONTACT TELEPHONE (360)870-5727	DCYF CONTACT FAX Click here to enter text.	DCYF CONTACT E-MAIL ADDRESS karena.mcgovern@dcyf.wa.gov	
IS THE CONTRACTOR A SUBRECIPIENT FOR PURPOSES OF THIS CONTRACT? No	CFDA NUMBERS		
AMENDMENT START DATE 03/20/2023	**CONTRACT END DATE** 06/30/2023		
PRIOR MAXIMUM CONTRACT AMOUNT $60,388.00	AMOUNT OF INCREASE OR DECREASE $-12,000.00	TOTAL MAXIMUM CONTRACT AMOUNT $48,388.00	

REASON FOR AMENDMENT:
CHANGE OR CORRECT MAXIMUM CONTRACT AMOUNT

ATTACHMENTS. When the box below is marked with an X, the following Exhibits are attached and are incorporated into this Contract Amendment by reference:
☐ Additional Exhibits (specify):

This Contract Amendment, including all Exhibits and other documents incorporated by reference, contains all of the terms and conditions agreed upon by the parties as changes to the original Contract. No other understandings or representations, oral or otherwise, regarding the subject matter of this Contract Amendment shall be deemed to exist or bind the parties. All other terms and conditions of the original Contract remain in full force and effect. The parties signing below warrant that they have read and understand this Contract Amendment, and have authority to enter into this Contract Amendment.

CONTRACTOR SIGNATURE	PRINTED NAME AND TITLE	DATE SIGNED
DCYF SIGNATURE	**PRINTED NAME AND TITLE**	**DATE SIGNED**
	Karena McGovern Contracts Specialist	

P. C. Hunsucker March 16, 2023

Philip C. Hunsucker Date
Chief Civil Deputy Prosecuting Attorney

This Contract between the State of Washington Department of Children, Youth & Families (DCYF) and the Contractor is hereby amended as follows:

1. **Purpose.** The purpose of this Amendment is to decrease the contract Consideration by $12,000 for FY23 and revise the Statement of Work to reflect the changes.

Statement of Work-Exhibit B is amended as follows:

2. **Section 3. Consideration** is deleted and replaced as follows:

Total consideration payable to Contractor for satisfactory performance of the work under this Contract is up to a maximum of **$48,388.00** including any and all expenses, and shall be based on the following:

a. The maximum consideration payable for Fiscal Year 2022 is **$30,194.00**. Funds not expended in Fiscal Year 2022 cannot be carried over to the following Fiscal Year.

b. The maximum consideration payable for Fiscal Year 2023 is **$18,194.00**. Funds not expended in Fiscal Year 2023 cannot be carried over to the following Fiscal Year.

b. The Contractor shall be paid **$46.00** per hour for clinical consultation services and payment shall be based upon the JR Juvenile Court Program Administrator receipt and approval of monthly summary report.

c. The Contractor shall only be reimbursed for travel costs pre-approved in writing by the JR Juvenile Court Program Administrator.

All other terms and conditions of this Contract remain in full force and effect.

COUNTY PROGRAM AGREEMENT
i-ACT Program Development

DCYF Agreement Number
2163-24537

This Program Agreement is by and between the State of Washington Department of Children, Youth & Families (DCYF) and the County identified below, and is issued in conjunction with a County and DCYF Agreement On General Terms and Conditions, which is incorporated by reference.

Administration or Division Agreement Number

County Agreement Number

DCYF ADMINISTRATION	DCYF DIVISION	DCYF INDEX NUMBER	DCYF CONTRACT CODE
Department of Children, Youth, and Families	Children, Youth and Families	1223	2000CC-63

DCYF CONTACT NAME AND TITLE	DCYF CONTACT ADDRESS
Karena McGovern Contract Specialist	1115 Washington St SE Olympia, WA 98504

DCYF CONTACT TELEPHONE	DCYF CONTACT FAX	DCYF CONTACT E-MAIL
(360)870-5727	Click here to enter text.	karena.mcgovern@dcyf.wa.gov

COUNTY NAME	COUNTY ADDRESS
Jefferson County	Jefferson County PO Box 1220 Port Townsend, WA 98368
COUNTY FEDERAL EMPLOYER IDENTIFICATION NUMBER	COUNTY CONTACT NAME Barbara Carr

COUNTY CONTACT TELEPHONE	COUNTY CONTACT FAX	COUNTY CONTACT E-MAIL
(360) 385-9190	(360) 385-9191	bcarr@co.jefferson.wa.us

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

PROGRAM AGREEMENT START DATE	PROGRAM AGREEMENT END DATE	MAXIMUM PROGRAM AGREEMENT AMOUNT
07/01/2021	06/30/2023	$60,388.00

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:

☒ **Exhibits (specify): Exhibit A-Data Security Requirements; Exhibit B-Statement of Work**

☐ **No Exhibits.**

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 DCYF only upon signature by DCYF.

COUNTY SIGNATURE(S)	PRINTED NAME(S) AND TITLE(S)	DATE(S) SIGNED
	Kate Dean, Chair BOCC	7/6/21
DCYF SIGNATURE	**PRINTED NAME AND TITLE**	**DATE SIGNED**
	Karena McGovern Contract Specialist	7-23-21

Approved as to Form Only:

June 30, 2021

Philip C. Hunsucker DATE
Chief, Civil Deputy Prosecuting Attorney

DATA SECURITY REQUIREMENTS

ORGANIZATION OF 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 DCYF Confidential Information and who has been authorized to do so.

c. "Business Associate Agreement" means an agreement between DCYF 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. "Confidential Information" 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. "Data" means DCYF's records, files, forms, information and other documents in electronic or hard copy medium. "Data" includes, but is not limited to, Confidential Information, Category 4 Data, Sensitive Personal Information, or Materials.

h. "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.

i. "FedRAMP" means the Federal Risk and Authorization Management Program (see https://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.

j. "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.

k. "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.

l. "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.

m. "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.

n. "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.

o. "Physically Secure" means that access is restricted through physical means to authorized individuals only.

p. "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.

q. "Sensitive Personal Information" means personally identifying information including, but not limited to: names, addresses, health information, GPS [Global Positioning System] coordinates, telephone numbers, email addresses, social security numbers, driver's license numbers, or other personally identifying information, and any financial identifiers.

r. "Staff" means the Contractor's directors, officers, employees, and agents who provide goods or services pursuant to this Contract. "Staff" also means Subcontractors' directors, officers, employees, and agents who provide goods or services on behalf of the Contractor. The term "Staff" also means the Subcontractors' directors, officers, employees, and agents who provide goods or services on behalf of the Subcontractor and Contractor.

s. Trusted Network" means a network operated and maintained by the Contractor, which includes security controls sufficient to protect DCYF 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.

t. "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 DCYF Information Security Policy and Standards Manual.

3. **Scope of Protection.** Applies to Confidential Information, Data, Category 4 Data, Sensitive Personal Information, and Materials related to the subject matter of this Contract that is delivered, received, used, shared, acquired, created, developed, revised, modified, or amended by DCYF, the Contractor, or Subcontractors.

4. **Compliance with Laws, Rules, Regulations, and Policies.** For Confidential Information, Data, Category 4 Data, Sensitive Personal Information, and Materials that is delivered, received, used, shared, acquired, created, developed, revised, modified, or amended in connection with this Contract the parties shall comply with the following:

a. All federal and state laws and regulations, as currently enacted or revised, regarding the protection, security, and electronic interchange of Confidential Information, Data, Category 4 Data, Sensitive Personal Information, and Materials; and

b. All federal and state laws and regulations, as currently enacted or revised, regarding the use, disclosure, modification or loss of Confidential Information, Data, Category 4 Data, Sensitive Personal Information, and Materials.

5. **Administrative Controls.** The Contractor must have the following controls in place:

a. A documented security policy governing the secure use of its computer network, mobile devices, portable devices, as well as, any form of paper/hard copy documents, and which defines sanctions that may be applied to Contractor staff for violating that policy.

b. Security awareness training for all staff, presented annually, as follows:

(1). Contractor staff responsibilities under the Contractor's security policy;

(2). Contactor staff responsibilities as outlined under contract Exhibit A; and

(3). Must successfully complete the DCYF Information Security Awareness Training, which can be taken on this web page: https://www.dcyf.wa.gov/sites/default/files/pdf/Security-in-Contracts.pdf

6. **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 that:

(1). Govern access to systems; and

(2). Govern access to paper/hard copy documents and files.

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 staff member to whom that account is assigned. For purposes of non-repudiation, it must always be possible to determine which staff member 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 Data is removed within twenty-four (24) hours:

(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; and

(4). When the staff member has been suspended from performing services under this Contract.

f. Have a process to review and verify, quarterly, that only authorized users have access to systems

containing Confidential Information, Data, Category 4 Data, Sensitive Personal Information, or Materials;

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 eight (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; and

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

h. When accessing Confidential Information, Data, Category 4 Data, Sensitive Personal Information, and Materials 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 that include:

(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 fifteen (15) minutes of inactivity; and

(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 five (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); and

(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 (6) alphanumeric characters;

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

(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 five (5) failed logon attempts.

7. **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.

c. **Optical discs (CDs or DVDs) in local workstation optical disc drives**. Data provided by DCYF 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 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 DCYF 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**.

(1). All paper documents must be protected by storing the records in a Secure Area, with access controlled through use of a key, card key, combination lock, or comparable mechanism, and which is only accessible to authorized personnel.

(2). When being transported outside of a Secure Area, paper documents must be under the physical control of Contractor staff with authorization to access the Data.

(3). Paper documents will not be secured or stored in a motor vehicle any time a staff member is away from the motor vehicle.

(4). Paper documents will be retained in a Secure Area, per the state of Washington records retention requirements.

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

(1). Except where otherwise specified herein, 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; and

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

(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 fifteen (15) minutes; and

(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 quarterly inventories.

(2). When being transported outside of a Secure Area, Portable Devices and Portable Media with Data must be under the physical control of Contractor staff with authorization to access the Data, even if the Data is encrypted. Portable Devices and Portable Media will not be secured or stored within motor vehicles at any time the staff member is away from the motor vehicle.

g. **Data stored for backup purposes**.

(1) DCYF 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 DCYF Confidential Information still exists upon it, refer to Section 12 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 DCYF Confidential Information still exists upon it, refer to Section 12 Data Disposition.

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

(1). 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 DCYF;

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

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

(h). Access to the cloud storage requires Multi Factor Authentication or Two Step Authentication.

(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.

8. Method of Transfer.

a. All Data transfers to or from the Contractor shall only be made by using the secure data.wa.gov portal provided by the state of Washington with login and hardened password security.

b. The Contractor shall use an encrypted email account for electronic submissions which contain Confidential, and Personal Information, as defined in the General Terms and Conditions. Information regarding encrypted email accounts can be obtained at DCYF's website, located at: https://www.dcyf.wa.gov/services/child-welfare-providers/encrypted-email.

9. System Protection. To prevent compromise of systems which contain DCYF Data or through which that Data passes:

a. Systems containing Data must have all security patches or hotfixes applied within three (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 Data shall have an Anti-Malware application, if available, installed; and

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.

10. Data Segregation.

a. Data must be segregated or otherwise distinguishable from non-DCYF data. This is to ensure that when no longer needed by the Contractor, all Data can be identified for return or destruction. It also aids in determining whether 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). Data will be kept on media (e.g. hard disk, optical disc, tape, etc.) which will contain no non-DCYF Data; and/or;

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

(3). Data will be stored in a database which will contain no non-DCYF data; and/or;

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

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

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

11. Confidentiality Protection. To safeguard confidentiality, and ensure that access to all Data is limited to authorized staff, the Contractor must:

a. Ensure that the Contractor's Staff, Subcontractors, and the Subcontractors' Staff use Data solely for the purposes of accomplishing the services set forth in this Contract;

b. Ensure that no Data is released, disclosed, published, modified, transferred, sold, or otherwise made known to unauthorized persons without the prior written consent of the individual named or as otherwise authorized by law;

c. The Contractor shall not use, publish, transfer, sell or otherwise disclose any Confidential Information of a minor except as provided by law or with the prior written consent of the minor's parent, legal representative or guardian. If a child is a dependent of Washington State, then prior written consent must be obtained from DCYF; and

d. Require that the Contractor's Staff and Subcontractors' Staff having access to Data sign a Statement of Confidentiality and Non-Disclosure Agreement (DCYF Form 03-374B), which can be found at this webpage: https://www.dcyf.wa.gov/forms. Data shall not be released to the Contractor's Staff person(s) or Subcontractors' Staff person(s) until the following conditions have been met:

(1). DCYF approves the Contractor's Staff person(s) or Subcontractors' Staff person(s), to work on this Contract; and

(2). If requested by DCYF, Contractor must submit the signed original Statement of Confidentiality and Non-Disclosure Agreement, signed by the Staff person(s) or Subcontractors' Staff person(s).

12. **Data Disposition**. Contractor is responsible to ensure that all Data, including paper and electronic records, is retained pursuant to Washington State retention standards. Prior to the destruction of any Data, the DCYF Contact specified for this contract, must be notified in writing and permission given in writing to destroy any such Data. When the contracted work has been completed or when the Data is no longer needed, Data shall be retained pursuant to the retention standards required by chapter 40.14 RCW, or returned to DCYF.

c. Once written permission to destroy Data has been granted by DCYF to the Contractor, the following acceptable methods of destruction must be used:

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

b. If any Data is required to be destroyed pursuant to this Section, within fifteen (15) calendar days after completion of such destruction the Contractor shall complete and deliver to DCYF a signed Certification of Data Disposition, which can be found at this webpage: https://www.dcyf.wa.gov/forms.

13. **Data shared with Subcontractors**. If 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 subcontractor must be submitted to the DCYF Contact specified for this contract for review and approval.

14. **Notification of Compromise or Potential Compromise**. The compromise or potential compromise of DCYF shared Data must be reported to the DCYF Contact designated in the Contract within one (1) business day of discovery. If no DCYF Contact is designated in the Contract, then the notification must be reported to the DCYF Privacy Officer at: dcyfprivacyofficer@dcyf.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 DCYF.

15. **Breach of Data.** In the event of a breach by the Contractor of this Exhibit and in addition to all other

rights and remedies available to DCYF, DCYF may elect to do any of the following:

a. Terminate the Contract;

b. Require that the Contractor return all Data to DCYF that was previously provided to the Contractor by DCYF; or

c. Suspend the Contractor's access to accounts and other information.

16. Public Disclosure.

a. If a third party requestor seeks information of the Contractor for DCYF Data, a copy of the notice/request shall be emailed to DCYF by way of the DCYF Contracts and Procurement Office email at dcyf.contractdatabreach@dcyf.wa.gov within three calendar (3) days of third party request.

b. DCYF Contracts and Procurement Office will respond to the Contractor on how to proceed with the request within five (5) calendar days of receiving such notification.

Exhibit B

STATEMENT OF WORK

Individual – Alternative Choice Training (i-ACT)
Training and Consultation for County Juvenile Courts

1. Service Delivery

The Contractor shall provide to statewide i-ACT Trainers, by telephone or in-person, clinical consultation services. Services shall include, but are not limited to:

a. Providing clinical consultation to i-ACT Trainers throughout the state;

b. Participating in and providing i-ACT Trainer training;

c. Monitoring by direct observation or video recordings of i-ACT sessions for adherence and compliance to i-ACT program standards;

d. Reporting monitoring results to the JR Juvenile Court Program Administrator and to the statewide WSART Quality Assurance Specialist on a monthly basis;

e. Providing assistance with individual i-ACT Trainers improvement plans; and

f. Participating in implementation and ongoing program development meetings.

2. Deliverables

a. Monthly Reporting

The Contractor shall provide monthly activity and monitoring summary reports to the JR Juvenile Court Program Administrator.

b. Quarterly / Annual Reporting

The Contractor on a quarterly basis shall provide the JR Juvenile Court Program Administrator and the Statewide WSART Quality Assurance Specialist (QAS) a report that summarizes the following information for all i-ACT Trainers served that quarter:

(1) Number of i-ACT Trainers served;

(2) Number of i-ACT Trainers placed on Informal Improvement Plans;

(3) Number of i-ACT Trainers who successfully completed their Informal Improvement Plans;

(4) Number of i-ACT Trainers who did not complete or unsuccessfully completed their Informal Improvement Plans and were referred to the WSART QAS for further action.

(5) A final annual summary will be provided, summarizing items 1 – 4 above.

c. Outcome Reporting

The Contractor shall report to the JR Juvenile Court Program Administrator at the completion of services to i-ACT Trainers the following information:

(1) The frequency of participation of each Juvenile Court's i-ACT Trainers participation in telephone consultation;

(2) Any changes in the Juvenile Courts' i-ACT program.

3. Consideration

Total consideration payable to Contractor for satisfactory performance of the work under this Contract is up to a maximum of **$60,388.00** including any and all expenses, and shall be based on the following:

a. The maximum consideration payable for Fiscal Year 2022 is **$30,194.00**. Funds not expended in Fiscal Year 2022 cannot be carried over to the following Fiscal Year.

b. The maximum consideration payable for Fiscal Year 2023 is **$30,194.00**. Funds not expended in Fiscal Year 2023 cannot be carried over to the following Fiscal Year.

c. The Contractor shall be paid **$46.00** per hour for clinical consultation services and payment shall be based upon the JR Juvenile Court Program Administrator receipt and approval of monthly summary report.

d. The Contractor shall only be reimbursed for travel costs pre-approved in writing by the JR Juvenile Court Program Administrator.

4. DCYF/JR Program Contact

The Contractor shall notify the DCYF Program Contact listed below for any questions or issues related to services under this contract:

Cory Redman
Juvenile Court Programs Administrator
Juvenile Rehabilitation - HQ
360.480.1194
cory.redman@dcyf.wa.gov