INTERLOCAL AGREEMENT

Understanding Reentry Needs and Challenges for Individuals Exiting JR

DCYF Agreement Number: 2165-25643

This Agreement is by and between the State of Washington Department of Children, Youth & Families (DCYF) and the Contractor identified below, and is issued pursuant to the Interlocal Cooperation Act, chapter 39.34 RCW.

Program Contract Number:

Contractor Contract Number:

CONTRACTOR NAME	CONTRACTOR doing business as (DBA)		
Washington State University			
CONTRACTOR ADDRESS	WASHINGTON UNIFORM BUSINESS IDENTIFIER (UBI)	DCYF INDEX NUMBER	
305 NE Troy Mall Suite 362 Pullman, WA 99164-4820	385-000-328	1477	
CONTRACTOR CONTACT	CONTRACTOR TELEPHONE	CONTRACTOR FAX	CONTRACTOR E-MAIL ADDRESS
Marcus Poppen	(509) 335-6363	(509) 335-5046	marcus.poppen@wsu.edu

DCYF ADMINISTRATION	DCYF DIVISION	DCYF CONTRACT CODE
Department of Children, Youth, and Families	Children, Youth and Families	2000LC-65

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 ADDRESS
(360)870-5727	Click here to enter text.	karena.mcgovern@dcyf.wa.gov

IS THE CONTRACTOR A SUBRECIPIENT FOR PURPOSES OF THIS CONTRACT?	CFDA NUMBER(S)
No	

AGREEMENT START DATE	**AGREEMENT END DATE**	MAXIMUM AGREEMENT AMOUNT
08/23/2021	06/30/2022	$69,253.00

EXHIBITS. The following Exhibits are attached and are incorporated into this Agreement by reference:

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

☐ **No Exhibits.**

The terms and conditions of this Agreement 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 Agreement, between the parties. The parties signing below represent they have read and understand this Agreement, and have the authority to execute this Agreement. This Agreement shall be binding on DCYF only upon signature by DCYF.

CONTRACTOR SIGNATURE	PRINTED NAME AND TITLE	DATE SIGNED
	Samuel Schirer, Contracts Specialist	8/13/2021
DCYF SIGNATURE	PRINTED NAME AND TITLE	DATE SIGNED
Karena McGovern	Karena McGovern Contract Specialist	8/13/2021

Special Terms and Conditions

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

a. "Contract" or "Agreement" means the entire written agreement between DCYF and the Contractor, including any Exhibits, documents, or materials incorporated by reference. The parties may execute this contract in multiple counterparts, each of which is deemed an original and all of which constitute only one agreement. E-mail or Facsimile transmission of a signed copy of this contract shall be the same as delivery of an original.

b. "Contractor" means the individual or entity performing services pursuant to this Contract and includes the Contractor's owners, members, officers, directors, partners, employees, and/or agents, unless otherwise stated in this Contract. For purposes of any permitted Subcontract, "Contractor" includes any Subcontractor and its owners, members, officers, directors, partners, employees, and/or agents.

c. "DCYF Contracts Administrator" means the individual in the DCYF Contracts Department with oversight authority for the Department of Children, Youth & Families statewide agency contracting procedures, or their appropriate designee.

d. "DCYF Contracts Department" means the Department of Children, Youth & Families statewide agency headquarters contracting office, or successor section or office.

e. "Department of Children, Youth & Families" or "DCYF" means the Washington agency devoted exclusively to serve and support Washington state's youth and their families.

f. "Debarment" means an action taken by a Federal agency or official to exclude a person or business entity from participating in transactions involving certain federal funds.

g. "Program Agreement" means an agreement between the Contractor and DCYF containing special terms and conditions, including a statement of work to be performed by the Contractor and payment to be made by DCYF.

h. "RCW" means the Revised Code of Washington. All references in this Contract to RCW chapters or sections shall include any successor, amended, or replacement statute. Pertinent RCW chapters can be accessed at http://apps.leg.wa.gov/rcw/.

i. "Regulation" means any federal, state, or local regulation, rule, or ordinance.

j. "Subcontract" means any separate agreement or contract between the Contractor and an individual or entity ("Subcontractor") to perform all or a portion of the duties and obligations that the Contractor is obligated to perform pursuant to this Contract.

k. "WAC" means the Washington Administrative Code. All references in this Contract to WAC chapters or sections shall include any successor, amended, or replacement regulation. Pertinent WAC chapters or sections can be accessed at http://apps.leg.wa.gov/wac/.

2. Amendment. This Contract may only be modified by a written amendment signed by both parties. Only personnel authorized to bind each of the parties may sign an amendment.

3. Assignment. The Contractor shall not assign this Contract or any Program Agreement to a third party without the prior written consent of DCYF.

4. Billing Limitations.

a. DCYF shall pay the Contractor only for authorized services provided in accordance with this Contract.

b. DCYF shall not pay any claims for payment for services submitted more than twelve (12) months after the calendar month in which the services were performed.

c. The Contractor shall not bill and DCYF shall not pay for services performed under this Contract, if the Contractor has charged or will charge another agency of the state of Washington or any other party for the same services.

5. Compliance with Applicable Law. At all times during the term of this Contract, the Contractor shall comply with all applicable federal, state, and local laws and regulations, including but not limited to, nondiscrimination laws and regulations.

6. Debarment Certification. The Contractor, by signature to this Contract, certifies that the Contractor is not presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded by any Federal department or agency from participating in transactions (Debarred). The Contractor also agrees to include the above requirement in any and all Subcontracts into which it enters. The Contractor shall immediately notify DCYF if, during the term of this Contract, Contractor becomes Debarred. DCYF may immediately terminate this Contract by providing Contractor written notice if Contractor becomes Debarred during the term hereof.

7. Governing Law and Venue. This Contract shall be construed and interpreted in accordance with the laws of the state of Washington and the venue of any action brought hereunder shall be in Superior Court for Thurston County.

8. Independent Contractor. The parties intend that an independent contractor relationship will be created by this Contract. The Contractor and his or her employees or agents performing under this Contract are not employees or agents of the Department. The Contractor, his or her employees, or agents performing under this Contract will not hold himself/herself out as, nor claim to be, an officer or employee of the Department by reason hereof, nor will the Contractor, his or her employees, or agent make any claim of right, privilege or benefit that would accrue to such officer or employee.

9. Inspection. The Contractor shall, at no cost, provide DCYF and the Office of the State Auditor with reasonable access to Contractor's place of business, Contractor's records, and DCYF client records, wherever located. These inspection rights are intended to allow DCYF and the Office of the State Auditor to monitor, audit, and evaluate the Contractor's performance and compliance with applicable laws, regulations, and these Contract terms. These inspection rights shall survive for six (6) years following this Contract's termination or expiration.

10. Maintenance of Records. The Contractor shall maintain records relating to this Contract and the performance of the services described herein. The records include, but are not limited to, accounting procedures and practices, which sufficiently and properly reflect all direct and indirect costs of any nature expended in the performance of this Contract. All records and other material relevant to this Contract shall be retained for six (6) years after expiration or termination of this Contract.

Without agreeing that litigation or claims are legally authorized, if any litigation, claim, or audit is started before the expiration of the six (6) year period, the records shall be retained until all litigation, claims, or audit findings involving the records have been resolved.

11. Order of Precedence. In the event of any inconsistency or conflict between the General Terms and Conditions and the Special Terms and Conditions of this Contract or any Program Agreement, the inconsistency or conflict shall be resolved by giving precedence to these General Terms and

Conditions. Terms or conditions that are more restrictive, specific, or particular than those contained in the General Terms and Conditions shall not be construed as being inconsistent or in conflict.

12. **Severability.** If any term or condition of this Contract is held invalid by any court, the remainder of the Contract remains valid and in full force and effect.

13. **Survivability.** The terms and conditions contained in this Contract or any Program Agreement which, by their sense and context, are intended to survive the expiration or termination of the particular agreement shall survive. Surviving terms include, but are not limited to: Billing Limitations; Disputes; Indemnification and Hold Harmless, Inspection, Maintenance of Records, Notice of Overpayment, Ownership of Material, Termination for Default, Termination Procedure, and Treatment of Property.

14. **Termination Due to Change in Funding.** If the funds DCYF relied upon to establish this Contract or Program Agreement are withdrawn, reduced or limited, or if additional or modified conditions are placed on such funding, DCYF may immediately terminate this Contract by providing written notice to the Contractor. The termination shall be effective on the date specified in the termination notice.

15. **Waiver.** Waiver of any breach or default on any occasion shall not be deemed to be a waiver of any subsequent breach or default. Any waiver shall not be construed to be a modification of the terms and conditions of this Contract. Only the DCYF Contracts Administrator or designee has the authority to waive any term or condition of this Contract on behalf of DCYF.

Additional General Terms and Conditions – Interlocal Agreements:

16. **Disputes**. Both DCYF and the Contractor ("Parties") agree to work in good faith to resolve all conflicts at the lowest level possible. However, if the Parties are not able to promptly and efficiently resolve, through direct informal contact, any dispute concerning the interpretation, application, or implementation of any section of this Agreement, either Party may reduce its description of the dispute in writing, and deliver it to the other Party for consideration. Once received, the assigned managers or designees of each Party will work to informally and amicably resolve the issue within five (5) business days. If managers or designees are unable to come to a mutually acceptable decision within five (5) business days, they may agree to issue an extension to allow for more time.

If the dispute cannot be resolved by the managers or designees, the issue will be referred through each Agency's respective operational protocols, to the Secretary of DCYF ("Secretary") and the Contractor's Agency Head ("Agency Head") or their deputies or designated delegates. Both Parties will be responsible for submitting all relevant documentation, along with a short statement as to how they believe the dispute should be settled, to the Secretary and Agency Head.

Upon receipt of the referral and relevant documentation, the Secretary and Agency Head will confer to consider the potential options of resolution, and to arrive at a decision within fifteen (15) business days. The Secretary and Agency Head may appoint a review team, a facilitator, or both, to assist in the resolution of the dispute. If the Secretary and Agency Head are unable to come to a mutually acceptable decision within fifteen (15) business days, they may agree to issue an extension to allow for more time.

The final decision will be put in writing, and will be signed by both the Secretary and Agency Head. If the Agreement is active at the time of resolution, the Parties will execute an amendment or change order to incorporate the final decision into the Agreement. The decision will be final and binding as to the matter reviewed and the dispute shall be settled in accordance with the terms of the decision.

If the Secretary and Agency Head are unable to come to a mutually acceptable decision, the Parties will request intervention by the Governor, per RCW 43.17.330, in which case the governor shall employ

whatever dispute resolution methods that the governor deems appropriate in resolving the dispute.

Both Parties agree that, the existence of a dispute notwithstanding, the Parties will continue without delay to carry out all respective responsibilities under this Agreement that are not affected by the dispute.

17. Hold Harmless.

a. The Contractor shall be responsible for and shall hold DCYF harmless from all claims, loss, liability, damages, or fines arising out of or relating to the Contractor's, or any Subcontractor's, performance or failure to perform this Agreement, or the acts or omissions of the Contractor or any Subcontractor. DCYF shall be responsible for and shall hold the Contractor harmless from all claims, loss, liability, damages, or fines arising out of or relating to DCYF' performance or failure to perform this Agreement.

b. The Contractor waives its immunity under Title 51 RCW to the extent it is required to indemnify, defend, and hold harmless the State and its agencies, officials, agents, or employees.

c. Notwithstanding the preceding, the parties expressly acknowledge and agree that their respective indemnification obligations are subject to the coverage limits (as to type and amount) of the State of Washington's Self-Insurance Liability Program.

18. Ownership of Material. Material created by the Contractor and paid for by DCYF as a part of this Contract shall be owned by DCYF and shall be "work made for hire" as defined by Title 17 USCA, Section 101. This material includes, but is not limited to: books; computer programs; documents; films; pamphlets; reports; sound reproductions; studies; surveys; tapes; and/or training materials. Material which the Contractor uses to perform the Contract but is not created for or paid for by DCYF is owned by the Contractor and is not "work made for hire"; however, DCYF shall have a perpetual license to use this material for DCYF internal purposes at no charge to DCYF, provided that such license shall be limited to the extent which the Contractor has a right to grant such a license.

19. Subrecipients.

a. General. If the Contractor is a subrecipient of federal awards as defined by 2 CFR Part 200 and this Agreement, the Contractor shall:

(1) Maintain records that identify, in its accounts, all federal awards received and expended and the federal programs under which they were received, by Catalog of Federal Domestic Assistance (CFDA) title and number, award number and year, name of the federal agency, and name of the pass-through entity;

(2) Maintain internal controls that provide reasonable assurance that the Contractor is managing federal awards in compliance with laws, regulations, and provisions of contracts or grant agreements that could have a material effect on each of its federal programs;

(3) Prepare appropriate financial statements, including a schedule of expenditures of federal awards;

(4) Incorporate 2 CFR Part 200, Subpart F audit requirements into all agreements between the Contractor and its Subcontractors who are subrecipients;

(5) Comply with the applicable requirements of 2 CFR Part 200, including any future amendments to 2 CFR Part 200, and any successor or replacement Office of Management and Budget (OMB) Circular or regulation; and

(6) Comply with the Omnibus Crime Control and Safe streets Act of 1968, Title VI of the Civil Rights

Act of 1964, Section 504 of the Rehabilitation Act of 1973, Title II of the Americans with Disabilities Act of 1990, Title IX of the Education Amendments of 1972, The Age Discrimination Act of 1975, and The Department of Justice Non-Discrimination Regulations, 28 C.F.R. Part 42, Subparts C.D.E. and G, and 28 C.F.R. Part 35 and 39. (Go to https://ojp.gov/about/offices/ocr.htm for additional information and access to the aforementioned Federal laws and regulations.)

b. Single Audit Act Compliance. If the Contractor is a subrecipient and expends $750,000 or more in federal awards from any and/or all sources in any fiscal year, the Contractor shall procure and pay for a single audit or a program-specific audit for that fiscal year. Upon completion of each audit, the Contractor shall:

(1) Submit to the DCYF contact person the data collection form and reporting package specified in 2 CFR Part 200, Subpart F, reports required by the program-specific audit guide (if applicable), and a copy of any management letters issued by the auditor;

(2) Follow-up and develop corrective action for all audit findings; in accordance with 2 CFR Part 200, Subpart F; prepare a "Summary Schedule of Prior Audit Findings" reporting the status of all audit findings included in the prior audit's schedule of findings and questioned costs.

c. Overpayments. If it is determined by DCYF, or during the course of a required audit, that the Contractor has been paid unallowable costs under this or any Program Agreement, DCYF may require the Contractor to reimburse DCYF in accordance with 2 CFR Part 200.

20. Termination.

a. Default. If for any cause, either party fails to fulfill its obligations under this Agreement in a timely and proper manner, or if either party violates any of the terms and conditions contained in this Agreement, then the aggrieved party will give the other party written notice of such failure or violation. The responsible party will be given fifteen (15) working days to correct the violation or failure. If the failure or violation is not corrected, this Agreement may be terminated immediately by written notice from the aggrieved party to the other party.

b. Convenience. Either party may terminate this Interlocal Agreement for any other reason by providing thirty (30) calendar days' written notice to the other party.

c. Payment for Performance. If this Interlocal Agreement is terminated for any reason, DCYF shall only pay for performance rendered or costs incurred in accordance with the terms of this Agreement and prior to the effective date of termination.

21. Treatment of Client Property. Unless otherwise provided, the Contractor shall ensure that any adult client receiving services from the Contractor has unrestricted access to the client's personal property. The Contractor shall not interfere with any adult client's ownership, possession, or use of the client's property. The Contractor shall provide clients under age eighteen (18) with reasonable access to their personal property that is appropriate to the client's age, development, and needs. Upon termination of the Contract, the Contractor shall immediately release to the client and/or the client's guardian or custodian all of the client's personal property.

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. "Agency" means a public or private agency or other organization providing services to DCYF clients.

b. "Compliance Agreement" means a written plan approved by DCYF which identifies deficiencies in Contractor's performance, describes the steps Contractor must take to correct the deficiencies, and sets forth timeframes within which such steps must be taken to return Contactor to compliance with the terms of the Contract.

c. "JR" means Juvenile Rehabilitation which is a Division under the Department of Children, Youth, and Families (DCYF).

d. "Research and Innovation in Special Education (RISE)" means the staff at Washington State University (WSU) that will be tasked with supporting the activities outlined in this contract.

2. Purpose. The purpose of this Contract is to meet the request of DCYF to conduct a program improvement evaluation of their reentry planning processes and practices that will provide information to support agency outcomes for youth and young adults up to age 25 released from youth correctional facilitates. The proposed work will be managed by Dr. Marcus Poppen, with support from Dr. Michael Dunn, WSU RISE. The activities will include planning and coordination with the DCYF JR Reentry Quality Assurance Team; virtual focus groups with reentry participants; and analyses and reporting. More details about the purpose, statement of work, and deliverables are included in Exhibit B.

3. Consideration. Total consideration payable to Contractor for satisfactory performance of the work under this Contract is up to a maximum of $69,253, including any and all expenses, and shall be based on the successful completion of the deliverables outlined in the Statement of Work-Exhibit B.

4. Billing and Payment.

a. Payments shall be made on the following schedule below and after successful completion of all work referenced in Exhibit B. One-quarter (25%) of the total compensation will be billed at the beginning of the work and tied to development and submission of the DCYF IRB application, and the remaining 75% will be billed quarterly throughout the duration of the project.

Payment Schedule	*Invoice Due Date*	*Invoice Amount*
DCYF IRB Application	August 16th, 2021	$17,313
August 1st, 2021-September 30, 2021	October 15th, 2021	$12,985
October 1st, 2021-December 31, 2021	January 15th, 2022	$12,985
January 1st, 2022-March 30th, 2022	April 15th, 2022	$12,985
April 1st, 2022 – June 30tht, 2022	July 15th, 2022	$12,985
Maximum Compensation		*$69,253*

b. Invoice System. The Contractor shall submit an invoice using State Form A-19 Invoice Voucher, or such other form as designated by DCYF. Consideration for services rendered shall be payable upon receipt of a properly completed invoice and deliverables and shall be submitted to the Juvenile Court Program Administrator by the Contractor. The invoice shall describe and document to DCYF's satisfaction a description of the work performed, activities accomplished, the progress of

the project, and fees. The initial invoice at the beginning of the project will provide a summary of what will be accomplished during the duration of the contract (including deliverables) that will be met with the funds.

c. Payment. Payment shall be considered timely if made by DCYF within thirty (30) days after receipt and acceptance by the Lisa McAllister, Office Chief- Reentry and Transition of the properly completed invoice. Payment shall be sent to the address designated by the Contractor on page one (1) of this Contract. DCYF 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.

5. Insurance.

a. DCYF certifies that it is self-insured under the State's self-insurance liability program, as provided by RCW 4.92.130, and shall pay for losses for which it is found liable.

b. The Contractor certifies, by checking the appropriate box below, initialing to the left of the box selected, and signing this Agreement, that:

_____ **X** The Contractor is self-insured or insured through a risk pool and shall pay for losses for which it is found liable; or

_____ ☐ The Contractor maintains the types and amounts of insurance identified below and shall, prior to the execution of this Agreement by DCYF, provide certificates of insurance to that effect to the DCYF contact on page one of this Agreement.

Commercial General Liability Insurance (CGL) – to include coverage for bodily injury, property damage, and contractual liability, with the following minimum limits: Each Occurrence - $1,000,000; General Aggregate - $2,000,000. The policy shall include liability arising out of premises, operations, independent contractors, products-completed operations, personal injury, advertising injury, and liability assumed under an insured contract. The State of Washington, DCYF, its elected and appointed officials, agents, and employees shall be named as additional insureds.

6. Compliance Agreement

In the event that DCYF identifies deficiencies in Contractor's performance under this Contract, DCYF may, at its option, establish a Compliance Agreement. When presented with a Compliance Agreement, Contractor agrees to undertake the actions specified in the plan within the timeframes given to correct the deficiencies. Contractor's failure to do so shall be grounds for termination of this Contract.

7. Auditing and Monitoring

a. If the Contractor is required to have an audit or if an audit is performed, the Contractor shall forward a copy of the audit report to the DCYF Contact listed on page 1 of this Contract.

b. The Contractor shall be financially responsible for any overpayments by DCYF to the Contractor. The Contractor shall be financially responsible for any audit disallowances resulting from a federal or state audit which resulted from an action, omission or failure to act on the part of the Contractor.

8. Administrative Records

The Contractor shall retain fiscal records that shall substantiate costs charged to DCYF under this Contract.

Special Terms and Conditions

9. Ownership of Material

DCYF must appropriately credit or cite the materials that are created by the Contractor (names, institution, date, etc.). The Contractor retains the rights to use and distribute all materials (documents, artifacts, reports, studies, training materials) created as a part of the Contract. The contractor may disseminate findings from these activities (e.g., peer-reviewed manuscripts, conference presentations, briefs, invited talks, etc.) following guidelines established by WSU Institutional Review Board standards and conduct for research.

EXHIBIT A

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 information that may be exempt from disclosure to the public or other unauthorized persons under either chapter 42.56 RCW or other state or federal laws. Confidential Information includes, but is not limited to, Personal Information, agency source code or object code, and agency security data.

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.

a. 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

Understanding the Reentry Needs and Challenges for Individuals Exiting Juvenile Rehabilitation in Washington

ORGANIZATION OF STATEMENT OF WORK

The Contractor shall ensure that services provided under this Contract at all times meet the specifications described in this Statement of Work Exhibit B.

1. Intent of Services

The intent of the services is to provide a collaborative research effort to understand the reentry needs and challenges for individuals exiting Juvenile Rehabilitation in Washington State. The overall objective of the work is to explore the current reentry planning processes and practices to better understand the needs and challenges youth and young adults up to age 25 released face when leaving juvenile rehabilitation facilities and transitioning back to their communities. Specifically, we seek to gain more understanding about the ways that JR reentry practices align with best practices in reentry programs and match the current needs of youth and families. A better understanding of the current challenges or barriers, and what DCYF-JR can and should focus on to ensure successful reentry, will contribute to practice improvement and better long term outcomes for youth, young people, and their families.

The evaluation will use qualitative inquiry methods (focus groups; interviews) with three key participant groups: (1) youth; (2) families; and (3) community members. Further, audiences for analytic products include the aforementioned participants, as well as superintendents, regional administrators, directors, and secretaries.

The contractor will ensure objectivity, methodological rigor, procedural integrity and content expertise.

2. Contractor Responsibilities

Work with DCYF Office of Innovation, Alignment and Accountability (OIAA) and JR Reentry Quality Assurance Team for a qualitative analysis of JR Reentry programs to include: Background, Purpose, Guiding Questions, Audience, Participant Groups, and Methods.

a. Work with DCYF OIAA on the submission to DCYF for Institutional Review Board (IRB) review. If necessary work with OIAA to take appropriate steps regarding Washington State IRB, if necessary.

b. Development of Reentry Focus Group Criteria and Protocol

   (1) Assisting in identifying criteria to select participants for focus groups, ensuring the selection criteria encourages equitable access to participation and generalizability of results.

   (2) Development of a fully developed interview protocol for each Participant group that participates in a focus group.

c. Conduct focus groups with three key participant groups: (1) youth; (2) families; and (3) community members.

   (1) Schedule and convene "virtual" focus groups and interviews with identified participant groups using finalized protocols.

   (2) Includes 10-12 focus groups, and more if necessary.

   (3) All focus groups or interviews will last between 60-90 minutes and follow a semi-structured approach, using a unique protocol for each Participant group.

   (4) The participant groups will be broken out amongst: youth, family, community members.

   (5) There will be 3-4 focus groups for each participant group, each including 4-7 participants.

   (6) Careful consideration will be taken to the environment for the students, staff and families who participate in the focus groups.

d. Transcribe, code, and thematically analyze all focus group and interview data; using a multi-cycle coding approach, integration with field notes, and member checking. Themes will be identified within and across Participant groups.

e. Provide a summary reporting findings, including a set of recommendations to DCYF OIAA and JR Reentry QA Team (See Report section for a more complete description of the reports).

f. Participate in monthly meetings (or more) with DCYF OIAA and the JR Reentry Quality Assurance Team to discuss project management and planning.

3. Deliverables and Deliverable Timelines

a. DCYF IRB Application (August 16, 2021)

b. Develop Finalized Analysis Plan (August and September 2021)

c. Washington State IRB Application (August and September 2021)

d. Participant Recruitment and Focus Groups (August through December, 2021)

e. Data analyses (January through May, 2022)

f. Final Written Report and Redacted Focus Group Transcripts (by May 31st, 2022)

g. Final Oral Report (by July 31st, 2022)

4. DCYF Responsibilities

a. Schedule monthly meetings (or more) with the Contractor to discuss project management and planning. Including Project Background, Purpose, Guiding Questions, Audience, Participant Groups, and Methods.

b. OIAA to provide support and consultation for a collaborative research effort and submission of DCYF IRB review. If necessary, work with Contractor on the Washington State IRB process.

c. DCYF Juvenile Rehabilitation will assist in the coordination and scheduling of focus groups during the months of August – December 2021,

d. The DCYF Office of Innovation and Accountability will provide data as necessary in the development of the report.

5. Culturally Relevant Services

The Contractor shall provide appropriate, accessible, and culturally relevant services to clients and their families. Service delivery shall be culturally competent and responsive to each client's cultural beliefs and values, ethnic norms, language needs, and individual differences. Contractors are encouraged to employ a diverse workforce that reflects the diversity of their clientele and the community.

6. Reports

The contractor shall provide the following:

a. Quarterly reports summarize progress towards proposed activities and deliverables.

b. Final written report on JR reentry planning processes, including:

(1) A brief summary of the alignment of these practices with best practices in reentry programs,

(2) An assessment of the extent to which the current practices are meeting the needs of youth and families, and a set of recommendations

c. Final written report will include a copy of the qualitative code books used for first and second cycle coding.

d. Final oral report and PowerPoint Presentation to be shared with DCYF audiences. Additional Executive summary(s) targeted at specific audience(s), if requested.

e. Redacted focus group transcripts will be provided to DCYF if done in a way that ensures confidentiality of participants.

7. Consideration

The total maximum consideration payable to the Contractor for satisfactory performance of the work under this contract shall be up to **$69,253** for SFY22 including any and all expenses.

All State funds must be expended within each State Fiscal Year and any unspent funds in SFY22 may not be carried forward to SFY23. No funds may be spent after June 30, 2022 unless pursuant to Section 6 of the Statement of Work.

8. Billing and Payments

a. DCYF IRB Application ($17,313) – Due August 16,2021

b. Quarter 1 Aug. 1, 2021 to Sept. 30, 2021 ($12,985) – Due Oct. 15th, 2021

c. Quarter 2 Oct. 1, 2021 to Dec. 30, 2021 ($12,985) – Due Jan. 15th, 2022

d. Quarter 3 Jan. 1, 2022 to Mar. 30, 2022 ($12,985) – Due April 15th, 2022

e. Final Report Initial Draft Due June 30, 2022 with final report submitted by July 31, 2022. Invoice due July 15, 2022 ($12,985).

9. DCYF/JR Program Contact

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

Lisa McAllister
Office Chief, Reentry and Transition
Juvenile Rehabilitation – HQ
360.902.8463
lisa.mcallister@dcyf.wa.gov

10. WSU RISE Program Contacts

WSU RISE Contacts are listed below:

Marcus Poppen, Ph.D.
Principal Investigator (PI)
Assistant Professor,
Special Education
Washington State University
Marcus.poppen@wsu.edu
509-335-6363

Michael Dunn, Ph.D.
Co-PI
Associate Professor,
Special Education
Washington State University
dunnmi@wsu.edu

Beverly Rhoades
Director of Administrative Services
College of Education
Washington State University
bevr@wsu.edu
509-335-7912