AGENDA REQUEST FORM

Return completed form and complete agenda item to the Clerk of the Board
Yakima County Commissioners' Office, Room 232

Prepared by:
Sandra F. Bess, Program Coordinator

Department: YCDOC

Requested Agenda Date: 06/02/2020

Presenting: Ed W. Campbell

Board of County Commissioners Record Assigned
BOCC Agreement
#
120-2020
Yakima County, WA

APPROVED FOR AGENDA:
☐ Consent ☐ Regular
Board of County Commissioners Determined

Document Title:
Jail Services Agreement

Action Requested: *Check Applicable Box*

☐ PASS RESOLUTION ☒ EXECUTE or AMEND **AGREEMENT** CONTRACT or GRANT
☐ ISSUE PROCLAMATION ☐ PASS ORDINANCE ☐ OTHER_____

Describe Fiscal Impact:
This is a small revenue generating agreement, which normally falls under $50,000 annually.

Background Information:
YCDOC has been contracting with the WA State DCFS since 2014. Our goal has been to assist the State in housing youths 18 years or older.

Summary & Recommendation:
Renewal of this agreement is being recommended at this time.

Motion:

Department Head/ Elected Official

Signature

AGREEMENT Attached Is Approved as to Form
Corporate Counsel Initial

Late Agenda Requests Require BOCC Chairman Signature:

BOCC Agreement

120-2020

Yakima County, WA

COUNTY PROGRAM AGREEMENT

Jail Services for Youth 18 years old or Older

DCYF Agreement Number
1963-56314

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
JR Region 1
County Agreement Number

DCYF ADMINISTRATION	DCYF DIVISION	DCYF INDEX NUMBER	DCYF CONTRACT CODE
Department of Children, Youth, and Families	Children, Youth and Families	1073	2000CC-63

DCYF CONTACT NAME AND TITLE	DCYF CONTACT ADDRESS
Del Hontanosas Grants & Contracts Manager	PO Box 45720 Olympia, WA 98504

DCYF CONTACT TELEPHONE	DCYF CONTACT FAX	DCYF CONTACT E-MAIL
(360)902-8087	(360)902-8108	del.hontanosas@dcyf.wa.gov

COUNTY NAME	COUNTY ADDRESS
Yakima County Dept. of Corrections	111 North Front Street Yakima, WA 98901
COUNTY FEDERAL EMPLOYER IDENTIFICATION NUMBER	COUNTY CONTACT NAME Ed Campbell

COUNTY CONTACT TELEPHONE	COUNTY CONTACT FAX	COUNTY CONTACT E-MAIL
(509) 574-1700		ed.campbell@co.yakima.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
07/01/2019	06/30/2021	$20,000.00

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
	Ed W. Campbell, Director	5/27/20

DCYF SIGNATURE	PRINTED NAME AND TITLE	DATE SIGNED

Special Terms and Conditions

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

   a. "DCYF" means the Department of Children, Youth, and Families.

   b. Juvenile Rehabilitation" or "JR" means the Division under the Department of Children, Youth, and Families.

2. **Purpose**. The purpose of this Agreement is for the Yakima County Department of Corrections to provide detention services at the Yakima County Department of Corrections for Juvenile Rehabilitation (JR) youth eighteen (18) years old or older committed to Juvenile Rehabilitation that are accepted for admittance at the direction of JR.

3. **Data Security Requirements – Exhibit A.** The Contractor shall protect, segregate, and dispose of data from DCYF as described in Exhibit A.

4. **Statement of Work-Exhibit A.** The Contractor shall provide the services and staff, and otherwise do all things necessary for or incidental to the performance of work, as set forth in Exhibit B-Statement of Work.

5. **Consideration**. Total consideration payable to Contractor for satisfactory performance of the work under this Agreement is up to a maximum of **$20,000**, including any and all expenses, and shall be based upon Exhibit B-Statement of Work-Jail Services for Youth 18 years old or older.

6. **Background Checks and Sexual Misconduct.**

   a. Background Check/Criminal History - In accordance with Chapters 388-700 WAC (JR-Practices & Procedures), 72.05 RCW (Children & Youth Services), and by the terms of this Agreement, Contractor and each of its employees, subcontractors, and/or volunteers who may or will have regular access to any client/juvenile must be cleared through a JR approved criminal history and background check. In addition, Contractor, each of their employees, subcontractors, and/or volunteers, who may or will have limited access to any client/juvenile, may be required to be cleared through a JR approved criminal history and background check.

   By execution of this Agreement, Contractor affirms that Contractor, each of its employees, subcontractors, and/or volunteers, who may or will have regular access have not been convicted of any of the following:

   (1) Any felony sex offense as defined in 9.94A.030 RCW (Sentencing Reform Act-Definitions) and 9A.44.130 RCW (Sex Offenses);

   (2) Any crime specified in Chapter 9A.44 RCW (Sex Offenses) when the victim was a juvenile in the custody of or under the jurisdiction of JR; or

   (3) Any violent offense as defined in 9.94A.030 RCW (Sentencing Reform Act-Definitions).

   Contractor must require that current employees, volunteers, and contracted service providers who are authorized for regular access to a juvenile(s) report any guilty plea or conviction of any of the above offenses. The report must be made to the person's supervisor within seven (7) days of conviction and any person who have reported a guilty plea or conviction for one or more of these offenses must not have regular access to any offender. Contractor shall also document background checks/criminal history clearances for monitoring purposes.

b. Sexual Misconduct - 13.40.570 RCW (Sexual misconduct by state employees, contractors) states that when the Secretary has reasonable cause to believe that sexual intercourse or sexual contact between the employee of a contractor and an offender has occurred, the Secretary shall require the employee of a contractor to be immediately removed from any employment position which would permit the employee to have any access to any offender.

By execution of this Agreement, contractor affirms that contractor, each of its employees, subcontractors, and/or volunteers are knowledgeable about the requirements of 13.40.570 RCW (Sexual misconduct by state employees, contractors) and of the crimes included in 9A.44 RCW (Sex Offenses).

In addition, the Secretary shall disqualify for employment with a contractor in any position with access to an offender, any person:

(1) Who is found by the department, based on a preponderance of the evidence, to have had sexual intercourse or sexual contact with the offender; or

(2) Convicted of any crime specified in chapter 9A.44 RCW (Sex Offenses) when the victim was an offender

If any actions are taken under 13.40.570 RCW, subsections (3) or (4), the Contractor must demonstrate to the Secretary they have greatly reduced the likelihood that any of its employees, volunteers, or subcontractors could have sexual intercourse or sexual contact with any offender. The Agreement shall not be renewed unless the Secretary determines significant progress has been made.

7. Federal Prison Rape Elimination Act.

In accordance with the Federal Prison Rape Elimination Act (PREA) of 2003, 28 CFR Part 115, http://www.ojp.usdoj.gov/programs/pdfs/prea_final_rule.pdf
Subpart A, the Contractor shall:

a. Adopt and be in compliance with the PREA standards for preventing, detecting and responding to sexual misconduct in adult prisons and jail.

b. Allow the JR reasonable access to the County Jail so it may ensure to its satisfaction that the County is in compliance with the PREA standards.

c. Reference is located at: http://www.ojp.usdoj.gov/programs/pdfs/prea_final_rule.pdf

8. Compliance.

a. The County shall comply with all applicable Federal and State laws, pertinent WACs and RCWs, JR bulletins, and other rules, regulations and publications identified throughout the Statement of Work.

b. In case of conflict or inconsistency between the aforementioned, the higher standard of compliance shall prevail.

c. If the County utilizes subcontractors for the provision of services under this contract, the County must notify JR in writing and maintain sufficient documentation to verify that the subcontractors meet all the requirements under this contract. In no event shall the existence of a subcontract release or reduce the liability of the County for any breach of performance. Subcontractors shall be the agent of the County and agree to hold JR harmless for acts or omissions of the subcontractors.

d. The County shall assist the JR to perform reviews of sites where services are delivered at regular intervals using agreed upon forms and methods.

9. Payment and Billing.

a. The contracted activities shall be paid up to the amount specified for the deliverables identified in the Statement of Work and payment shall be made upon receipt of the deliverable. JR shall not make payment for any deliverable not completed to JR's satisfaction.

d. DCYF shall pay the Contractor upon acceptance by DCYF of a properly completed A-19 Invoice Voucher. The invoice shall describe and document the following:

1) Date and time period of service(s) performed;

2) Name or other client identifier; and

3) Description of work performed

e. Payment shall be considered timely if made by DCYF within 30 days after the receipt of the properly completed invoice.

f. Payment shall be sent to the Contractor's address on page 1 of this Agreement.

g. The County shall submit an A-19 Invoice Voucher to DCYF each month for services provided, detailing client names and jail detention dates/times.

h. The County shall accept this payment as sole and complete remuneration for services provided to offenders under this Agreement. This does not preclude the County from seeking other funding sources.

i. The County shall use these funds to supplement, not supplant, the amount of federal, state, and local funds otherwise expended for the services provided under this agreement.

j. Under no circumstances shall the County bill twice for the same service.

k. Payment shall be considered timely if made by DCYF within 30 days after the receipt of the properly completed invoice.

l. Payment shall be sent to the Contractor's address on page one of this Agreement.

m. DCYF shall not pay the Contractor for authorized services not provided to clients, or for services provided which are not authorized or are not provided in accordance with the "Statement of Work." If DCYF pays the Contractor for services authorized but not provided by the Contractor in accordance with this Agreement's "Statement of Work," the amount paid shall be considered to be an overpayment.

n. If this Agreement is terminated for any reason, DCYF shall pay for only those services authorized and provided through the date of termination.

7. Disputes. Either the Contractor or JR may initiate a dispute claim for consideration by the other party, as it relates to the terms of this Agreement, or to the services provided by the Contractor under the terms of this Agreement. In accordance with the JR dispute resolution process, attempts to resolve

disputes shall initially be addressed and be resolved at the lowest level possible between the Contractor and JR organization, which initiated the contract. Upon verbal or written request from the Contractor, JR shall provide the Contractor a copy of the JR dispute resolution process within 5 working days of the request.

8. DCYF Program Contact.

The Contractor shall notify the DCYF Program Contact listed below for all notices, billings and correspondence, or any questions or issues related to services under this Agreement:

Chad Kline
Program Manager
Juvenile Rehabilitation-Region 1
Chad.Kline@dcyf.wa.gov
PO Box 11205
Yakima, WA 98909
(509) 225-7919

Shannon Jones
Secretary Senior
Juvenile Rehabilitation-Region 1
Shannon.Jones@dcyf.wa.gov
PO Box 11205
Yakima, WA 98909
(509) 225-4460

EXHIBIT A

DATA SECURITY REQUIREMENTS

ORGANIZATION OF DATA SECURITY REQUIREMENTS

1. Definitions
2. Authority
3. Scope of Protection
4. Compliance with Laws, Rules, Regulations, and Policy
5. Administrative Controls
6. Authorization, Authentication, and Access
7. Protection of Data
8. Method of Transfer
9. System Protection
10. Data Segregation
11. Confidentiality Protection
12. Data Disposition
13. Data shared with Subcontractors
14. Notification of Compromise or Potential Compromise
15. Breach of Data
16. Public Disclosure

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).

Special Terms and Conditions

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

Jail Services for Youth 18 years old or Older

1. **Services Provided.**

   a. The purpose of this Statement of Work is for the Director of the Yakima County Department of Corrections to provide detention services at the Yakima County Department of Corrections, for Juvenile Rehabilitation (JR) youth eighteen (18) years old or older that are accepted for admittance at the direction of the JR.

   b. Detention Services shall include custody, supervision, and routine care for all JR youth eighteen (18) years old or older that are accepted for admittance. Such JR youth shall be housed within the Yakima County Department of Corrections.

   c. The Director of the Yakima County Department of Corrections is primarily responsible for the operation of the Yakima County Department of Corrections.

   d. Any JR youth housed at the Yakima County Department of Corrections under the terms of this agreement shall be subject to all rules and regulations governing other inmates housed in the Yakima County Department of Corrections.

2. **Yakima County Department of Corrections Responsibilities.**

   a. The Director of the Yakima County Department of Corrections has no obligation whatsoever, at any time, to accept JR youth.

   b. Only when the Director of the Yakima County Department of Corrections determines, at their sole discretion, that space exists in the Yakima County Department of Corrections to house JR youth, do they have the obligation to consider accepting JR youth.

   c. Once the Director of the Yakima County Department of Corrections accepts a JR youth, upon a two-day notice, they may request that JR pick up such youth and relocate that youth to another location or facility not under control of the Director of the Yakima County Department of Corrections.

   d. JR youth shall receive such medical, psychiatric and dental treatment as may be necessary to safeguard their health while housed in the Yakima County Department of Corrections, to the extent required by applicable laws and regulations. Yakima County shall provide or arrange for the providing of such medical, psychiatric and dental services. Except for routine minor medical services, JR shall pay Yakima County for any and all costs associated with the delivery of any emergency, major medical and/or outside medical service provided to JR youth.

   e. Should conditions of an unusual nature occur making it impractical or undesirable to continue to house JR youth, the Director of the Yakima County Department of Corrections may suspend or restrict the use of the facility by giving written notice to JR.

f. The Director of the Yakima County Department of Corrections may, without the prior approval of JR, move the youth from the Yakima County Department of Corrections to another suitable location for housing in the event of an emergency such as fire, earthquake, or catastrophe, or conditions presenting imminent danger to the safety of the youth. The Director of the Yakima County Department of Corrections agrees to notify JR as soon as possible of the location at which the JR youth is being held.

g. In the event any JR youth shall escape from the custody of the Yakima County Department of Corrections, the Yakima County shall use all reasonable means to recapture the youth. The escape shall be reported immediately to JR. Any costs incurred by Yakima County in conjunction with recapturing the youth shall be chargeable to and borne by JR.

3. JR Responsibilities.

a. JR shall at all times, except as may be provided to the contrary herein, be responsible for the delivery and retaking of JR youth.

b. JR shall be responsible for transporting youth from the Yakima County Department of Corrections to the following:

(1) Court,
(2) Medical appointments, and
(3) Hospital stays.

c. In an emergency, Yakima County Department of Corrections staff may provide transport duties but will be relieved as soon as possible by JR staff.

d. JR shall have access, at all reasonable times, to the Yakima County Department of Corrections for the purpose of inspecting the facilities and visiting any of its youth confined therein under the terms of this Agreement.

4. Compliance.

a. The County shall comply with all applicable Federal and State laws, pertinent WACs and RCWs, JR bulletins, and other rules, regulations and publications identified throughout the Statement of Work.

b. In case of conflict or inconsistency between the aforementioned, the higher standard of compliance shall prevail.

c. If the County utilizes subcontractors for the provision of services under this Agreement, the County must notify JR in writing and maintain sufficient documentation to verify that the subcontractors meet all the requirements under this Agreement. In no event shall the existence of a subcontract release or reduce the liability of the County for any breach of performance. Subcontractors shall be the agent of the County and agree to hold JR harmless for acts or omissions of the subcontractors.

d. The County shall assist the JR to perform reviews of sites where services are delivered at regular intervals using agreed upon forms and methods.

Special Terms and Conditions

5. Billing.

a. The contracted activities shall be paid up to the amount specified for the deliverables identified in the Statement of Work and payment shall be made upon receipt of the deliverable. JR shall not make payment for any deliverable not completed to JR's satisfaction.

b. The County shall be paid based on the Monthly Average Daily Population (MADP) sliding scale (listed below) through termination of this Agreement. A billable day will be those days that the youth spends the night in the detention facility. The County shall provide JR with notice of any rate changes.

Monthly Average Daily Population		Daily Rate Per Inmate
151	above	$51.20
126	150	$52.20
101	125	$53.20
76	100	$54.20
51	75	$55.20
26	50	$56.20
0	25	$57.20

c. The County shall submit an A-19 Invoice Voucher to the DCYF/JR contact each month for services provided, detailing client names and jail detention dates/times.

d. The County shall accept this payment as sole and complete remuneration for services provided to offenders under this Agreement. This does not preclude the County from seeking other funding sources.

e. The County shall use these funds to supplement, not supplant, the amount of federal, state, and local funds otherwise expended for the services provided under this agreement.

f. Under no circumstances shall the County bill twice for the same service.

g. Payment shall be considered timely if made by DCYF within 30 days after the receipt of the properly completed invoice.

h. Payment shall be sent to the Contractor's address on page one of this Agreement.

i. DCYF shall not pay the Contractor for authorized services not provided to clients, or for services provided which are not authorized or are not provided in accordance with the "Statement of Work." If DCYF pays the Contractor for services authorized but not provided by the Contractor in accordance with this Agreement's "Statement of Work," the amount paid shall be considered to be an overpayment.

j. If this Agreement is terminated for any reason, DCYF shall pay for only those services authorized and provided through the date of termination.

Special Terms and Conditions

6. Mailing Addresses.

All notices and correspondence among the parties to this agreement shall be sent to the following addressees at the following addresses:

Director:	Ed Campbell Yakima County Dept. of Corrections 111 N Front Street Yakima, WA 98901
Region 1 Administrator:	Lori Kesl Rehabilitation Administration 1626 West Boone Avenue Spokane, WA 99201

Additionally, the individuals listed hereinabove are each respectively designated to act as each party's representative for administering their respective obligations under the terms of this Agreement.

BOARD OF YAKIMA COUNTY COMMISSIONERS AGREEMENT

Agreement Number

Jail Services Agreement

WA State Dept. of Children, Youth & Families (DCYF)

BOARD OF COUNTY COMMISSIONERS

_____
Norm Childress, Chairman

_____
Ron Anderson, Commissioner

_____
Vicki Baker, Commissioner

DATED

Attest:

_____
_____ Melissa Paul, *Clerk of the Board*
_____ Linda Kay O'Hara, *Deputy Clerk*

Approved as to Form:

Stefanie Weigand
Stefanie Weigand, Deputy Prosecuting Attorney

BOCC Agreement

120-2020

Yakima County, WA