1. Definitions

a. “Authorization for Purchase (AFP)” means the formal DVR fiscal document that officially identifies and authorizes a DVR Contractor to deliver a specific service.

b. “CRP” or “Community Rehabilitation Program”, means provider which provides vocational rehabilitation service to individuals with disabilities to enable those individuals to maximize their opportunities for employment.

c. “Contractor” means XX County.

d. “County” means the political subdivision of the State of Washington, named above, performing services pursuant to this Program Agreement and includes the County’s officers, employees, and authorized agents.

e. “County Coordinator” means the official developmental disabilities program coordinator or their designee.

f. “Customer” means a person with a disability who has an employment goal that requires long-term extended services provided by an entity other than DVR and is jointly a Customer of DVR and the County Developmental Disabilities and Early Childhood Supports who will be exiting high school.

g. “DVR” means Department of Social and Health Services, Division of Vocational Rehabilitation.

h. “DVR Coordinator(s)” means Vocational Rehabilitation Counselor(s) appointed by DVR, or their designee(s).

i. “Extended Services” means ongoing support services and other appropriate services needed to support youth with a most significant disability in supported employment and that are provided by a State agency, a private nonprofit organization, employer, or any other appropriate resource. Extended services are time limited and temporary in nature.

j. “Individual Plan for Employment (IPE)” means a DVR form that documents important decisions about vocational rehabilitation services for a Customer as defined in WAC 388-891-1115. The decisions documented on the IPE include, but are not limited to:

   (1) The employment outcome the Customer plans to achieve;

   (2) Each major step needed to accomplish the employment outcome;

   (3) The Customers responsibilities in accomplishing each step of the plan;

   (4) DVR’s responsibilities in assisting the Customer to accomplish each step of the plan;

   (5) Vocational Rehabilitation (VR) services needed to complete each step; and

   (6) Terms and conditions the Customer and the DVR Counselor agree are required for continued support from DVR.

k. “Job Foundation” – The Job Foundation and Value Based Payment Project is intended to engage students earlier in targeted employment planning and connection; increase partnerships with school staff to complete student’s Job Foundation report with actionable next steps; and increase the number of students completing transition programs with a job or secondary education connection.

    (1) Job Foundation Report should include all information necessary for VRC to complete the vocational assessment.

    (2) Job Foundation process and comprehensive report may replace the need for a Community Based Assessment, including County S2W CBAs

l. “Job Placement” means locating, securing, and placing a Customer into a paid, integrated, and competitive job that is mutually agreed upon by the DVR Counselor, the Contractor, and the Customer and/or their representative.

m. “Intensive Training Services” means individualized, one-on-one job skills training and support provided at the supported employment job site to enable a Customer to:

    (1) Attain job stabilization in on-the-job performance, with job supports;

    (2) Meet the employer’s expected level of work productivity; and

    (3) Transition to long-term Extended Services when stabilization is achieved.

n. “Job Stabilization” means the DVR Customer, the employer, the DVR Counselor and the Contractor mutually agree that a Customer placed in a Supported Employment position has demonstrated and maintained satisfactory on-the-job performance and has the quantity and type of long-term employment supports available from the extended services provider that are needed to maintain satisfactory on-the-job performance.

o. School to Work Assessment means:

    (1) Verify a Customer’s unique work interests, abilities, and any competitive employment barriers related to communication, mobility, work skills, work tolerance, self-direction (cognition and learning), and interpersonal attitudes, skills, behavior, or self-care, etc.; and

    (2) Identify the nature and extent of support(s) and accommodations needed for the Customer to obtain and maintain competitive employment.

p. “SDOP” or “Service Delivery Outcome Plan” is a written plan jointly developed by the Customer, DVR counselor, and the Contractor for obtaining School to Work services.

2. **Purpose**. The purpose of this agreement is to:

Collaborate with the Contractor to provide employment related services to individuals with developmental disabilities who will be exiting high school.

3. **Statement of Work.** The Contractor shall provide the services and staff, and otherwise

do all things necessary for or incidental to the performance of work, as set forth below:

a. Provide all services, as described in the Statement of Work, of this Contract in a manner and setting(s) that meet the requirements of the Washington State DSHS Administrative Policy 7.02.

b. Arrange and be responsible for all costs associated with communication interpreter services, as needed, to provide disability-related access per the Americans with Disabilities Act (ADA) unless the cost involved would cause an undue hardship (significant difficulty or expense) for the Contractor. Determination of what constitutes an undue hardship will be made on a case-by-case basis, relative to the Contractor's overall resources.

   If an undue hardship does exist, the DVR supervisor may authorize paying for interpreter services apart from the contracted fee for service; and

c. Provide and be responsible for the cost of providing services through alternative formats, methods, and languages, as needed, for customers who have Limited English Proficiency (LEP) as per the Civil Rights Act of 1964, as amended.

d. Eligibility: DVR Customers, who receive the Contractor's services as specified in this agreement, will be Customers exiting high school who:

   (1) DVR accepts all referrals of students eligible and interested in STW.

   (2) Have a DVR Individual Plan for Employment (IPE) with a DVR approved employment goal that requires Extended Services in order to be achieved.

   (3) Between ages of 20-21.

   (4) Have an Individualized Education Plan (IEP).

e. All subcontractors utilized by the Contractor in delivery of direct services described in this agreement shall hold a current DVR Community Rehabilitation Program (CRP) contract:

   (1) Community Based Assessment;

   (2) CRP Job Placement; and

   (3) CRP Intensive Training Services.

f. Subcontracts

   All subcontracts must incorporate this contract by reference and include all of this contract's requirements. The Contractors will provide copies of signed subcontracts between the Contractor and subcontracted CRPs to DVR:

   (1) Prior to the start date of this agreement;

   (2) Within 30 calendar days from the start date of the subcontract if its execution occurs after the start date of this agreement;

(3) Within 30 calendar days from the start date of the contract for established or pre-approved subcontractors.

(4) Upon request.

g. Service Delivery: The Contractor's delivery of VR services specified in this agreement will begin upon the Contractor's receipt of a DVR Authorization for Purchase (AFP) for each participating DVR Customer.

(1) One AFP shall be issued per Customer for the total fee; and

(2) All DVR AFPs for services shall be issued prior to the agreement end date.

h. The specific detail to be included in the STW Assessment, and the Job Placement, and Intensive Training Services that are provided under this Contract shall be as follows:

(1) Individualized to meet the unique vocational rehabilitation needs of each Customer;

(2) Mutually agreed upon by Customer, Guardian, DVR and the Contractor;

(3) Documented on the DVR SDOP as follows:

(4) Where the Job Foundation Report replaces the STW assessment: on a single DVR School to Work Service Delivery Outcome Plan (SDOP) for both Job Placement and Intensive Training.

(5) Where a Job Foundation Report is not utilized: Two SDOP's will be used. One School to Work SDOP for STW Assessment and one School to Work SDOP that combines Job Placement and Intensive Training Services.

(6) The Contractor may delegate, in writing, authority to the Subcontractor to negotiate and sign School to Work SDOPs on behalf of the Contractor.

(7) The VRC shall provide a copy of the signed SDOP(s) to the Contractor.

i. Services: The Contractor shall provide the following services to help the Customer achieve job stabilization in order to transition to Extended Services. Services shall be provided for DVR Customers who are exiting high school and are eligible and ready to concurrently participate in Contractor and DVR vocational rehabilitation (VR) programs and services:

(1) STW Assessment

(a) Assessment may be conducted when information, in addition to the school district assessment or job foundation report, is needed to determine a vocational goal.

(b) The Contractor shall locate, secure, and place a DVR Customer into a paid employment setting(s), or other realistic work setting(s), in which the Customer performs work for a specified period of time with the direct

provision of needed job supports and training to:

i. Verify a Customer's unique work interests, abilities, and any competitive employment barriers related to communication, mobility, work skills, work tolerance, self-direction (cognition and learning), and interpersonal attitudes, skills, behavior, or self-care, etc. and

ii. Identify the nature and extent of support(s) and accommodations needed for the Customer to obtain and maintain competitive employment.

(2) Job Placement

The Contractor shall provide all services necessary to locate, secure, and place a Customer into a paid, integrated, and competitive job that is mutually agreed upon by the DVR Counselor, the Contractor, and the Customer or their representative specific placement expectations shall be outlined on the DVR SDOP for Job Placement and Intensive Training.

(a) The Contractor shall secure placement based on the customer's employment goal as determined in the SDOP.

(b) Placements less than 10 hours: Job placement goals that are less than 10 hours per week shall be approved in advance by the appropriate Supervisors in consultation with the team. The team may include the Customer, Customer's Family (if applicable), DVR VRC, CRP, and County Staff.

This approved shall be obtained at the time of job placement and intensive training SDOP is developed.

(3) Intensive Training Services

The Contractor shall provide individualized, one-on-one job skills training and support at the supported employment job site that will enable a Customer to:

(a) Achieve job stabilization in on-the-job performance, with job supports;

(b) Meet the employer's expected level of work productivity; and

(c) Transition to long-term Extended Services.

(d) Stabilization is achieved when the DVR Customer, guardian if applicable, DVR Counselor, employer, and the Contractor agree that stabilization has occurred.

i. Intensive training expectations shall be outlined on the DVR SDOP for job placement and intensive training.

ii. If all parties are not able to attend the job placement and intensive training SDOP development in person, use of telephone or video conferences is encouraged in order to complete the process in a timely

manner.

(4) Extended Support Services

(a) DVR shall provide extended services if needed by the student until DDA funds are available.

(b) Extended Services funded by DVR shall be outlined on the DVR Extended Support SDOP.

i. Not to exceed 6 months

ii. Maximum 26 hours per month at the hourly rate of $105.00

iii. Additional Extended Support funding, if required, shall be provided by an entity other than DVR.

j. Monthly Reports

The Contractor or delegate shall submit a monthly progress report for each individual Customer to the designated DVR Vocational Rehabilitation Counselor (VRC).

Reports should be written in language that directly addresses the Customer, and shall continue through Stabilization or through June 30th, whichever is later, or until DVR case closure.

Reports shall document the following information:

(1) Assessment: completion of Assessment as Specified in the Service Deliver Outcome Plan (SDOP). SDOP shall include Assessment findings and summary including, but not limited to, all questions specified in the SDOP

(2) Job Placement – Completion of Job Placement, as specified in the SDOP that contains Job Placement services and the results including, but not limited to:

(a) Name of the employer the Customer was placed at;

(b) Job Title;

(c) Hourly wage;

(d) Number of hours per week; and

(e) Any fringe benefits.

(3) Intensive Training Services – completion of Intensive Training Services as specified in the SDOP that contains Intensive Training Services and the results including, but not limited to:

(a) Date the Customer was considered to be stable in their job performance and

transitioned to the extended Services (Long-Term Support); And

(b) Any Changed in the Customer's job (i.e. number of hours worked, wages, etc.)

(4) Extended Services- completion of Extended Services are specified in the SDOP that contains Extended Services and the results, include but not limited to:

(a) CRP will provide an individualized report regarding the Customer which details all extended `service activities, tools and strategies

(b) Outcome fee paid to CRP upon receipt of an invoice and written report on an SDOR as specified on the SDOP.

(c) Whether a source of Extended Services other than DVR has been identified

k. Annual Meetings: DVR School-to-Work Transition Manager or designee shall work with Counties to plan Annual Meeting to include Counties, CRP services providers, DVR staff and DDA representatives. The gathering of partners on an annual basis will allow discussion of the program process and encourage methods to improve effectiveness of services.

DVR School-to-Work Transition Manager or designee shall be responsible for arranging the time, place, and specific agenda items for these meeting in coordination with DD County partners.

(1) Counties shall invite DVR Regional Administrators or designee and VR Supervisors to attend Local County-initiated service provider meetings that typically occur at least quarterly.

4. Consideration

Total consideration payable to the Contractor for satisfactory performance of the work under this Agreement is dependent upon the number of DVR Customers successfully served, includes any and all expenses, and shall be based on the following:

a. The following consideration section applies during the period of **July 1, 2024 – September 30, 2025**:

(1) Assessment/Job Placement/Intensive Training Services – A one-time payment of $10,500.00 per Customer shall be paid to the Contractor when the individual Customer is considered stable in their on-the-job performance, and working at least 10 hours per week, unless a placement goal of less than 10 hours/week was approved by the DVR Supervisor in consultation with the team.

(2) If a Customer with a placement goal of 10 hours per week or more accepts a placement for less than 10 hours per week, an exception for payment may be granted with approval of the appropriate DVR Supervisor. This approval shall be in consultation with the team including the Customer, Customer's Family

(as applicable), DVR VRC, CRP, and County staff.

(3) The Contractor shall submit the required monthly report and a separate original invoice of $10,500.00 to the assigned DVR Vocational Rehabilitation Counselor for each Customer who is successfully served by this Agreement.

(4) The service is determined successful when the Customer is considered to be stable in their job performance and transitioned to Extended Services (Long-Term Support). The funder of Extended Services may be a combination of sources such as time-limited County-funded support or DDA waiver funded services.

(5) DVR has received all required reports;

(6) Partial payments shall not be made for any service provided through this agreement.

5. Billing and Payment

a. Invoice System. The Contractor shall submit the required monthly report and a separate original invoice of $10,500.00 to the assigned DVR Vocational Rehabilitation Counselor for each Customer who is successfully served by this Agreement. The service is determined successful when the Customer is considered to be stable in their job performance and transitioned to Extended Services (Long-Term Support).

(1) Payment shall be considered timely if made by DSHS within thirty (30) days after receipt and acceptance by the designated DVR VR Counselor of the properly completed invoice. Payment shall be sent to the address designated by the Contractor on page one (1) of this Agreement.

b. DSHS may at its sole discretion, withhold payment claimed by the Contractor for services rendered if the Contractor fails to satisfactory comply with any term or condition of this Agreement.

c. No later than September 30, 2025, the Contractor shall submit a single spreadsheet listing all milestone payments allowable under Special Terms and Conditions Section 4(a)(5):

(1) The Contractor shall send the spreadsheet directly to:

Melinda Bocci
School-to-Work Transition Manager
Melinda.Boccia@dshs.wa.gov

(2) The Spreadsheet shall list the following information:

(a) Name of Customer;

(b) Whether the Job Placement milestone was achieved.

(3) For each milestone payment listed on the spreadsheet, the Contractor shall attach the following additional documentation.

(a) For Job Placement milestone payments, a written Job Placement outcome report indicating:

i. Customer's placement into a paid integrated job as mutually agreed to by the VRC.

ii. Customer's completion of first full day of paid employment as defined by the employer;

iii. Name, contact name, and address of employer;

iv. Date of customer's first day of employment;

v. Type of job the customer was performing;

vi. Number of hours per week the customer was schedule to work;

vii. Customer's hourly wage and any fringe benefits; and

viii. A brief description of the reason job stabilization was not achieved.

6. Insurance - Self-Insured

a. DSHS 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:

(1) ☐ The Contractor is self-insured or insured through a risk pool and shall pay for losses for which it is found liable; or

(2) ☐ The Contractor maintains the types and amounts of insurance identified below and shall, prior to the execution of this Agreement by DSHS, provide certificates of insurance to that effect to the DSHS 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, DSHS, its elected and appointed officials, agents, and employees shall be named as additional insureds.

7. Investigations of Contractor or Related Personnel

a. DSHS may, without prior notice, suspend the Contractor's performance of the

Contract if the Contractor, or any partner, officer or director of the Contractor, or a subcontractor, or any employee or volunteer of the Contractor or a subcontractor, is investigated by DSHS or a local, county, state or federal agency regarding any matter that, if ultimately established, could either:

(1) Result in a conviction for violating a local, state or federal law.

(2) In the sole judgment of DSHS, adversely affect the delivery of services under this Contract or the health, safety or welfare of DSHS Customers.

b. DSHS may also take other lesser action, including, but not limited to, disallowing a staff member, employee, or other individual associated with the Contractor or a subcontractor, from providing services, or from having contact with DSHS Customers, until the investigation is concluded and a final determination made by the investigating agency.

8. Removal of Individuals from Performing Services

a. In the event that any of the Contractor's employees, subcontractors, or volunteers who provide services under this Contract do not meet qualifications required by this Contract or do not perform the services as required in this Contract, DSHS may require that Contractor remove such individual from providing services to DSHS Customers under this Contract.

b. DSHS shall notify the Contractor of this decision verbally and in writing and the Contractor shall, within 24 hours, remove that individual from providing direct services to DSHS Customers. Failure to do so may result in a Corrective Action Plan.

9. Compliance with Corrective Action Plan

In the event that DSHS identifies deficiencies in Contractor's performance under this Contract, DSHS may establish a Corrective Action Plan When presented with a Corrective Action Plan, 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.

10. Order of Precedence in DVR Process

In the event of any inconsistency or conflict between the Terms and Conditions of this Contract and the DVR Service Delivery Outcome Plan (SDOP) and the Authorization for Purchase (AFP), the inconsistency or conflict shall be resolved by giving precedence this contract in its entirety. Terms or conditions that are more restrictive, specific, or particular than those contained in this contract shall not be construed as being inconsistent or in conflict.

11. Disputes

When a dispute arises over an issue concerning the terms of this Contract, the following process is used to address the dispute:

a. The Contractor and DVR shall attempt to resolve the dispute through informal means between the Contractor and the assigned Vocational Rehabilitation Counselor (VRC). For those contracts where a VRC is not assigned, the Contractor shall attempt to resolve the dispute with the contact person identified on the first page of the contract.

b. If the Contractor is not satisfied with the outcome of the resolution with the VRC or DSHS contact person, the Contractor may submit a request for review of the disputed issue, in writing, for review within thirty (30) business days of the outcome to:

   DVR Director
   DSHS/DVR
   PO Box 45340
   Olympia WA 98504-5340

c. The Director may appoint a designee to review the disputed issue.

d. A request for dispute resolution shall include:

   (1) Name of the requester.

   (2) Contractor's name, full address, phone number, and email.

   (3) Contract number.

   (4) Description of the issue in dispute.

   (5) A statement describing the requester's position on the issue in dispute, including any documentation that supports this position.

   (6) Steps already taken to resolve the dispute.

e. The reviewer may request additional supporting documentation from either party to assist in reaching a fair resolution.

f. The Director shall issue a written decision to the Contractor within thirty (30) business days of receipt of all information relevant to the issue.

g. The dispute resolution process described above is the sole administrative remedy available under this Contract.

Exhibit A – Data Security Requirements

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2. **Authority**. The security requirements described in this document reflect the applicable requirements of Standard 141.10 (https://ocio.wa.gov/policies) of the Office of the Chief Information Officer for the state of Washington, and of the DSHS Information Security Policy and Standards Manual. Reference material related to these requirements can be found here: https://www.dshs.wa.gov/ffa/keeping-dshs-client-information-private-and-secure, which is a site developed by the DSHS Information Security Office and hosted by DSHS Central Contracts and Legal Services.

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

a. A documented security policy governing the secure use of its computer network and systems, and

which defines sanctions that may be applied to Contractor staff for violating that policy.

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

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

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

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

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

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

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

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

(1) Upon suspected compromise of the user credentials.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(1) Be a minimum of six alphanumeric characters.

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

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

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

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

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

b. **Network server disks**. For Data stored on hard disks mounted on network servers and made available through shared folders, access to the Data will be restricted to Authorized Users through the use of access control lists which will grant access only after the Authorized User has authenticated to the network using a Unique User ID and Hardened Password or other

authentication mechanisms which provide equal or greater security, such as biometrics or smart cards. Data on disks mounted to such servers must be located in an area which is accessible only to authorized personnel, with access controlled through use of a key, card key, combination lock, or comparable mechanism.

For DSHS Confidential Information stored on these disks, deleting unneeded Data is sufficient as long as the disks remain in a Secure Area and otherwise meet the requirements listed in the above paragraph. Destruction of the Data, as outlined below in Section 8 Data Disposition, may be deferred until the disks are retired, replaced, or otherwise taken out of the Secure Area.

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

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

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

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

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

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

(a) Encrypt the Data.

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

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

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

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

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

iii. Taking frequent inventories.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

7. Data Segregation.

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

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

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

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

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

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

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

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

Data stored on:	Will be destroyed by:
Server or workstation hard disks, or Removable media (e.g. floppies, USB flash drives, portable hard disks) excluding optical discs	Using a "wipe" utility which will overwrite the Data at least three (3) times using either random or single character data, or Degaussing sufficiently to ensure that the Data cannot be reconstructed, or Physically destroying the disk
Paper documents with sensitive or Confidential Information	Recycling through a contracted firm, provided the contract with the recycler assures that the confidentiality of Data will be protected.
Paper documents containing Confidential Information requiring special handling (e.g. protected health information)	On-site shredding, pulping, or incineration
Optical discs (e.g. CDs or DVDs)	Incineration, shredding, or completely defacing the readable surface with a coarse abrasive
Magnetic tape	Degaussing, incinerating or crosscut shredding

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

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