Special Terms and Conditions

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

   a. "Admin/Support Staff" means the costs of fiscal staff, Human Resources staff, contract staff, administrative staff, and others who indirectly support the County program.

   b. "Communication" means all means needed to communicate with students and their families. This may include translators, translating materials, use of a Zoom account, and other means approved by DVR.

   c. "Community Outreach/Information Education" means the work completed to reach out to partners and collaborating entities. This may include outreach to schools, students and their families, CRPs, scheduling events, and sharing information and resources.

   d. "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.

   e. "Contractor" means XX County

   f. "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.

   g. "County Coordinator" means the official developmental disabilities program coordinator or their designee.

   h. "Customer" means a student with an intellectual/developmental disability who will be exiting their final year of their high school transition program, ages 20 to 21.

   i. "Data Collection and Reporting/Database/Tracking" means the tools and/or processes the Contractor has established as a means to track data.

   j. "DDA" means the Developmental Disabilities Administration, within the Department of Social and Health Services.

   k. "DVR" means Division of Vocational Rehabilitation, within the Department of Social and Health Services.

   l. "Indirect Costs" means all costs associated with being an employee of your county, including but not limited to the cost of paper, pens, copier machine needs, cellphones, laptops, etc.

   m. "Office Space/Location" means the cost to rent, lease, or pay for use of that location for county business.

   n. "Resource Fair, Event Planning" means an event held by Contractor as a means to share information and resources with Customers. Event Planning includes all activities and expenses needed for the resource fair to occur.

   o. "Resource/Marketing Development" means the cost associated with creating, producing, and developing resources and marketing materials for the purpose of growing your transition program and recruiting students for School to Work.

   p. "School-to-Work" means a seamless transition for students with intellectual/developmental disabilities from school to adult services through employment and connecting students to the

necessary resources for success.

q. "Staffing" means the amount associated with the direct staff time spent on School to Work efforts. This may include direct salary, benefits package.

r. "Subcontractor" means an individual or outside organization hired by the County to assist with different functions of the School-to-Work program development.

s. "Training and Resources" means the amount associated with bringing workshops, trainings, and resources to the community for the purpose of transition services for students in their last year of transition, ages 20 to 21.

t. "Transportation" means the reimbursement of mileage to travel in your county when carrying out work towards developing the School-to-Work program.

u. "Website" means a website where Contractor's Customers are able to access details and information about transition services and resources.

v. "Workgroup Participation" means the Contractor's participation in meetings to share School-to-Work efforts and progress.

2. **Purpose**. The purpose of this Contract is to provide support and reimbursement to counties to develop and establish a School-to-Work program which will provide employment related services to Customers with intellectual/developmental disabilities who will be exiting their high school transition program, ages 20 to 21.

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:

Create a county-wide School-to-Work program. The Contractor shall establish a person who will lead county School-to-Work transition efforts. This may be an existing staff member, hiring a new staff member, or subcontracting to an entity to provide the work as a staff member.

Contractor shall be reimbursed for costs incurred performing the below objectives. Contractor is not obligated to complete all objectives below other than those that shall allow for the development of a successful School-to-Work program:

a. Staffing

(1) Hire staff to establish relationships with schools, DVR, DDA, CRPs, Customers, parents and others who support Customers in their last year of transition as they move towards employment in the community, OR;

(2) Establish amongst current staff or subcontractor who shall be the County representative to establish relationships with schools, DVR, DDA, CRPs, Customers, parents, and others who support Customers in their last year of transition as they move towards employment in the community.

(3) Invoicing/Billing: Contractor shall submit a monthly invoice of billable hours of staff and/or subcontractor with copy of proof of payment.

b. Training and Resources

(1) The Contractor shall determine the training needs of staff, schools, and community partners regarding transition services and resources in the county and create and execute opportunities

for trainings to fit the needs of the transition community. This may include, but is not limited to, direct training for county staff, program planning, and/or large-scale trainings for the community. Topics of trainings must be approved by DVR.

(2) Workshop development to strengthen knowledge and resources pertaining to transition services, specifically for County staff and community partners such as Educators and CRPs. These may include, but are not limited to, trainings and workshops around resources such as Social Security, employment and job development, housing, and transportation. Topics of workshops must be approved by DVR.

(3) Invoicing/Billing: Contractor shall submit a monthly invoice of the cost of community trainings and workshops for students in transition and transition-based community partners with proof of payment.

c. Transportation

(1) The Contractor shall track transportation of staff mileage associated with Customers in School-to-Work through travel logs.

(2) Invoicing/Billing: Contractor shall submit a monthly invoice that includes a travel log capturing mileage needed for the development of the School-to-Work program, paid at the rate identified in SAAM 10.90.20 at the time of billing.

d. Communication

(1) The Contractor shall increase communication and accessibility to County programs and information. This may include, but is not limited to;

(a) Translation of transition documents into various languages.

(b) Hiring interpreters.

(c) Setting up appropriate communication methods to fit the needs of Customers (i.e., in-person, over-the-phone, and/or video remote interpreter services).

(2) The Contractor shall establish the communication needs of the county to determine how best to create modes of communication that best fit the needs of Customers in transition and submit the plan of communication for DVR approval.

(3) Invoicing/Billing: Contractor shall submit a monthly invoice of cost for translating materials, providing interpreters, and/or communication methods with proof of payment.

e. Workgroup and School-to-Work Participation

(1) By agreeing to develop a School-to-Work program, it is expected that the Contractor shall attend and participate in local, regional and statewide workgroups and meetings as a means to ensure the progress and success of the School-to-Work program.

(2) Invoicing/Billing: Contractor shall bill for this item under section 3.a.(3) Staffing.

f. Office Space/Location

(1) Office space that is needed to house staff and resources associated with the School-to-Work program (i.e., staff offices, training centers).

(2) Invoicing/Billing: Contractor shall submit a monthly invoice of:

(a) The difference resulting from an increase in the cost of office space due to an increase in staffing for the School-to-Work program; OR

(b) The percentage of staff time designated to the School-to-Work program as it relates to total staff occupying existing office space. An example has been included below for reference:

i. Current office space costs $1,000 a month for two staff. One staff member now spends 50% of their time on School-to-Work. Contractor may bill for reimbursement of $250 ($1000/2 = $500 *.50 = $250)

g. Indirect Costs

(1) Indirect Costs may include, but are not limited to; the cost of copiers, paper, pens, supplies, cellphones, internet access, and/or computers needed in order to perform the services outlined in this contract.

(2) Admin/Support Staff shall be encompassed into Indirect Costs. Admin/Support staff may include, but is not limited to;

(a) Fiscal

(b) Human Resources

(c) Information Technology (IT)

(d) Clerical Support

(3) Invoicing/Billing: Contractor shall submit a monthly invoice that includes a line item for Indirect Costs, expressed as percentage rate that shall not exceed X%, and will not exceed actual costs of all billable items for the month. An example has been provided below for reference:

(a)

3,500	staffing
600	Training and resources
80	transportation
750	for office space
4,930	Sub total for deliverables
10%	Indirect cost
493	total indirect costs
5,423	Total Reimbursement

h. Resource and Marketing Development

(1) Contractor shall create and develop marketing resources to share information to Customers, as well as families, schools, and community partners. Contractor must collaborate with DVR to establish effective School-to-Work marketing messages.

(2) Invoicing/Billing: Contractor shall submit a monthly invoice of the cost of producing community resources and marketing materials for Customers in transition and transition-based community partners with proof of payment.

Special Terms and Conditions

i. Website

(1) Website development and/or updating to include School-to-Work information for Customers to access. This content must be accessible to all Customers, including, but not limited to, language translation, and JAWS-compatible.

(2) Contractor must submit a plan for website development to DVR for approval prior to executing any changes to an existing website or completing work towards the creation of a new website.

(3) Invoicing/Billing: Contractor shall bill for this item under Section 3.a.(3) Staff and/or Section 3.g.(3) Indirect Costs. The Contractor may also bill for the initial set-up cost for translation and/or accessibility program software by providing receipts. Monthly upkeep of translation and/or accessibility software shall be billed under Section.3.g.(3) Indirect Costs.

j. Transition Resource Fair/Event Planning

(1) If the Contractor already has an annual Transition Resource Fair – costs associated with creating a Transition Resource Fair may be reimbursed with DVR approval. This may include, but is not limited to;

(a) Venue rental.

(b) Marketing of the event.

(c) Hiring support staff to put on the event.

(2) If the Contractor does not have an annual Transition Resource Fair – it is expected that the Contractor shall work to establish an annual Transition Resource Fair with a focus on employment, assisting students in their final year of transition to know and understand options beyond their school years. This may include creating a series of Parent Nights, as approved by DVR, in place of an annual Transition Resource Fair, or collaborating with other community partners to establish a Transition Resource Fair.

(3) Invoicing/Billing:

(a) Renting Space: Contractor shall submit an invoice of the cost of renting space for Transition Resource Fairs or county sponsored events for Customers transition-based community partners with proof of payment.

(b) Marketing: Contractor shall submit an invoice of the cost of marketing materials, including printing, envelopes, and postage.

(c) Event Planning Agency/Person: Contractor shall submit an invoice of the cost of hiring a company or person to plan the annual Transition Resource Fair.

(d) Community Partners Collaborating: Contractor shall submit an invoice of the cost of their portion of the total bill to have a local Transition Resource Fair.

k. Community Outreach/Information and Education

(1) Efforts to connect with communities and schools across the county are expected to start and grow the School-to-Work program. It is expected that these efforts shall be the primary focus and/or part of the established or new staff.

(2) Invoicing/Billing: Contractor shall submit billable hours for staff following guidelines in Section

3.a.(3) Staff and billable mileage following guidelines in Section 3.c.(2) Transportation.

l. Data Collection and Reporting

(1) The Contractor shall work with DVR to determine the information and data gathered to show the progress being made with School-to-Work efforts, including but not limited to; sharing data regarding Customers' progress in the School-to-Work program, Customers' progress towards employment, and reasons why potential Customers choose not to participate in the School-to-Work program.

(2) Invoicing/Billing: Contractor shall submit billable hours for staff time following guidelines in Section 3.a.(3) Staff.

4. Consideration. Total consideration payable to Contractor for satisfactory performance of the work under this Contract is up to a maximum of $_____, including any and all expenses, and shall be based on the information in Exhibit B – Estimated Bi-Annual Budget.

a. The Program Development Objective amounts are estimates, and in no way capped by each objective, as long as the total contract consideration amount is not surpassed. Amendments to the consideration for this Contract are acceptable through mutual agreement of both parties.

b. All expenses toward a Program Development Objective that are $10,000 or more not related to staffing must be approved by the School-to-Work/Transition Program Manager prior to being purchased.

5. Deliverables.

The Contractor shall submit reports, documents, receipts, and/or summaries monthly to the School-to-Work/Transition Program Manager for review. The School-to-Work/Transition Program Manager shall verify the submittals are accurate and correct as specified in Section 3, Statement of Work. If any discrepancies arise upon reviewing Program Development submittals, DVR may, at its sole discretion, withhold payment until the discrepancies are addressed by the Contractor and approved by School-to-Work/Transition Program Manager.

6. Subcontracting.

The Contractor is allowed to subcontract the work performed under this agreement with written approval from the School-to-Work/Transition Program Manager. The School-to-Work/Transition Program Manager shall review and make a final determination regarding the subcontract and the subcontractor.

7. Monitoring.

The Contractor shall meet with the School-to-Work/Transition Program Manager semi-annually, on dates mutually agreed upon by both parties, to discuss the performance of this Contract. Topics of discussion include, but are not limited to; unresolved issues, potential amendments, and/or any assistance that is needed.

8. Billing and Payment.

a. Invoice System. The Contractor shall submit invoices using State Form A-19 Invoice Voucher, or such other form as designated by DSHS. Consideration for services rendered shall be payable upon receipt of properly completed invoices which shall be submitted to School-to-Work/Transition Program Manager by the Contractor by the 25th of each month. The invoices shall describe and document to DSHS' satisfaction a description of the work performed, activities accomplished, the

progress of the project, and fees.

b. Payment. Payment shall be considered timely if made by DSHS within thirty (30) days after receipt and acceptance by School-to-Work/Transition Program Manager of the properly completed invoices. Payment shall be sent to the address designated by the Contractor on page one (1) of this Contract. DSHS may, at its sole discretion, withhold payment claimed by the Contractor for services rendered if Contractor fails to satisfactorily comply with any term or condition of this Contract.

9. Insurance.

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.

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.