Whatcom County
Developmental Disabilities
Child Development Services

Program Implementation Guide

2019-21

Effective 7.1.19

2017-19 Child Development Services Program Implementation Guide

Contents

1.0 PURPOSE

The Whatcom County Health Department, Developmental Disabilities Program currently contracts with providers within the State of Washington to provide Child Development Services through funding from the Washington State Department of Social and Health Services, Developmental Disabilities Administration (DSHS/DDA).

The purpose of this Program Implementation Guide is to provide an overview of County service requirements, policies, and procedures related to the implementation of County-funded Child Development Services.

The requirements outlined in this guide, as well as those contained in the attached contract, will provide the basis for contract compliance reviews. All references to DSHS/DDA policy may be found online at https://www.dshs.wa.gov/dda/policies-and-rules/policy-manual.

1.1 Modification

This guide provides a summary of State policy and County procedures and references applicable state and federal laws. The Implementation Guide may be amended or updated with prior notification by the County and agreement from County-contracted providers. A contract amendment is not required.

2.0 DEFINITIONS OF TERMS

Authorized User(s):	An individual or individuals with an authorized business requirement to access DSHS Confidential Information.
CDS:	Child Development Services
CMIS:	Case Management Information System
Client:	An infant or child with a developmental disability, authorized for service by the Washington State Department of Social and Health Services, Developmental Disabilities Administration
Confidential:	Information that is exempt from disclosure to the public or other information unauthorized persons under Chapter 42.56 RCW or other federal of state laws. Confidential information includes, but is not limited to personal information.
Contractor:	A vendor (i.e. a for-profit or non-profit agency) that delivers specified services under contract with the Whatcom County Health Department, Developmental Disabilities Program
CSA:	County Service Authorization
DDA:	Developmental Disabilities Administration
DSHS:	Washington State Department of Social and Health Services

EIS:	Early Intervention Services
Encrypt:	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 128 bits.
FRC:	Family Resources Coordinator
IFSP:	Individual Family Service Plan
ESIT:	Early Services for Infants and Toddlers
Personal Information:	Information identifiable to the person, including but not limited to information that relates to a person's name, health, finances, education, business, use or receipt of governmental services, address, telephone number, social security number, driver's license number, financial identifiers or other identifying numbers.
RCW:	Revised Code of Washington
WAC:	Washington Administrative Code

3.0 APPLICABLE POLICIES, LAWS, AND REGULATIONS

The Contractor will provide Child Development Services (CDS) to infants and toddlers determined eligible by DSHS/DDA in accordance with the following policies, laws, and regulations and will comply with all applicable federal state and local laws, rules, and regulations in implementing this contract.

3.1 Federal Law

Americans with Disabilities Act (ADA) (http://www.usdoj.gov/crt/ada/adahom1.htm)
Individuals with Disabilities Education Act (IDEA), Part C (http://idea.ed.gov/)
Fair Labor Standards Act (FLSA) (http://www.dol.gov/esa/whd/flsa/)
Rehabilitation Act of 1973 (http://www.ed.gov/policy/speced/reg/narrative.html)

3.2 Revised Code of Washington (RCW)

26.44	Abuse of Children
49.46	Minimum Wage Act
42.56	Public Records Act
43.43.830 - 845	Background Checks
49.17	Washington Industrial Safety & Health Act
71A.14.070	Confidentiality of Information, Oath
74.15.30	Background Checks, health and safety
71A.12	Developmental Disabilities

3.3 Washington Administrative Code (WAC)

296-24	General Safety & Health
296-62	General Occupational Health Standards
388-823	Developmental Disabilities Administration Service Rules
388-825	Developmental Disabilities Administration Services
170-400	Early Supports for Infants and Toddlers

3.4 DDA Policies https://www.dshs.wa.gov/dda/policies-and-rules/policy-manual

5.01	Background Authorizations
5.06	Client Rights
5.19	Positive Behavior Support for Children & Youth
6.08	Mandatory Reporting
6.13	Day Program Provider Qualifications
9.07	HIV/AIDS

3.5 DDA Guiding Values

www.dshs.wa.gov/sites/default/files/DDA/dda/documents/DDA%20Guiding%20Values%20Booklet.pdf

3.6 County Criteria for Evaluation

Please see https://www.dshs.wa.gov/dda/county-best-practices

3.7 DSHS Contract requirements

- DSHS General Terms and Conditions
- DSHS/DDA County contract for the current biennium
- Exhibit A-Data Security Requirements

3.8 Order of Precedence

In the event of any inconsistency in this Agreement, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order to:

- Applicable federal, state, and local law, regulations, rules, and ordinances
- This Agreement
- Any document incorporated in the Agreement by reference

4.0 HEALTH, SAFETY, AND INDIVIDUAL RIGHT

4.1 Background Checks

Each employee has a current (within three years), satisfactory background check which has been completed by the DSHS Background Check Central Unit (BCCU) in accordance with RCW 43.43.830-845, RCW 74.15.030 and WAC 388-825. Child Development service providers may submit their background checks directly to the BCCU at DSHS, or they may submit the background checks to the Department oof Children, Youth and Families, for processing by the DSHS BCCU.

Background checks are conducted in line with DSHS/DDA policy 5.01.

4.2 Mandatory Reporting of Abuse, Neglect and other incidents

The contractor's staff providing services to individuals with developmental disabilities are deemed mandatory reporters, and are responsible for reporting incidents of suspected abandonment, abuse, exploitation, financial exploitation, mistreatment and neglect of clients of in line with DDA Policy 6.08.

- Reporting to the County and DDA must comply with the requirements, definitions and timelines outlined in the policy.
- Contractor must have policies and procedures in place consistent with Policy 6.08
- The contractor must use an approved incident reporting form, when providing written report of incidents to the County and DDA.
- Completion of DSHS Form 27-081 by each administrator, employee contractor or volunteer upon hire and annually thereafter, and kept in the employees file.

4.3 Access to Disability Rights Washington (DRW)

Disability Rights Washington (DRW) has the authority and responsibility to investigate all reports of alleged abuse, neglect, and violation of civil rights of individuals with developmental disabilities pursuant to the Developmental Disabilities Assistance and Bill of Rights Act of 1975 (42 USC, sec. 6000, *et seq.)*. If DRW is investigating an allegation of abuse, neglect, or rights violation, the Contractor will cooperate fully, allowing access by DRW to clients and to client records as outlined in the DSHS/DRW Access Agreement.

4.4 Client Rights

The Contractor will provide each parent/guardian with an infant or child who is receiving services with information explaining their rights as a consumer of contracted services. Communication of client rights, grievance procedures, and services expectations, should be in line with ESIT policy and procedure and DDA policy 5.06, *Client Rights*

Client Rights and Grievance procedures should be provided to the client upon entry into the program, and as required by ESIT procedural safeguard requirements thereafter. The Contractor will confirm that the information was provided through documentation of a parent or guardian's signature and date or as otherwise required by ESIT

4.5 Health and Safety Regulations

All services for persons with developmental disabilities must be provided with attention to their health and safety. The Contractor will comply with all state regulations and all local ordinances related to fire, health, and safety standards whenever services are delivered. This applies to the environment itself (e.g., a facility-based employment site or pre-school), a part of the environment (e.g., machinery present), or program components (e.g., community travel or mobility training).

Contractors will comply with all applicable federal, state, and local fire, health, and safety regulations, which include, but are not limited to:

a. Federal: Occupational Safety and Health Act of 1970, P.L. 91-596, 84 USC 1590
b. State: Washington Industrial Safety and Health Act, RCW 49.17, WAC 296-24 and 296-62; State Building Code Act/Uniform Fire Code, RCW 19.27

4.6 Staff Intervention

The Contractor will provide for staff intervention in the most dignified, age-appropriate manner necessary in all situations, including instances when a client's behavior jeopardizes the safety of him/herself or others, or the behavior significantly disrupts program operations. All training interventions developed to assist the child and family enrolled in program services shall meet requirements under DSHS/DDA Policy 5.19, Positive Behavior Support for Children & Youth

4.7 Updated Medical Information

The Contractor will maintain a file for each client containing current medical information (e.g., medications, dietary restrictions, allergies, etc.) needed for the safe provision of County-funded services by the Contractor. Medical information will be updated as needed and at minimum annually.

4.8 Confidentiality

A. The contractor shall not use, publish, transfer, sell or otherwise disclose any confidential information for any purpose that is not directly connected with the performance of County funded services, except:

   1. As provided by law
   2. In the case of personal information, as provided by law or with written consent of the person or personal representative of the person who is the subject of personal information.

B. The Contractor's employees with access to confidential information are required to sign an oath of confidentiality, pursuant to RCW 71A.14.070. In order to share confidential information with other agencies, individuals, or entities, the Contractor will require Release of Information Forms (ROIF) signed by the client or guardian and indicating the type of information released, the agency to whom the information will be released, and for how long or for what purpose(s) the ROIF is valid.

C. The contractor shall protect and maintain all confidential information gained by reason of contracted County services against unauthorized use, access, disclosure, modification or loss. This duty requires the contractor to employ reasonable security measures, which includes restricting access to the Confidential information by:

   1. Allowing access only to staff that have an authorized business requirement to view the confidential information.
   2. Physically securing any computers, documents, or other media containing the confidential information.

D. In the event that the contractor ends its contractual relationship with the County, all client files and related confidential materials shall be returned to the County. Alternately, with approval from the County, the Contractor may certify in writing the destruction of confidential materials. Certification must include the method used, entity contracted to carry out file destruction.

E. The Contractor shall comply with the data security requirements outlined in Exhibit A, and have policies and procedures which address these requirements.

4.9 Non-Discrimination

The Contractor will not discriminate against any person on the basis of race, creed, political ideology, color, national origin, sex, marital status, sexual orientation, age, or the presence of any sensory, mental, or physical handicap. The Contractor will have written policies prohibiting discrimination, in compliance with state law and Section 504 of the Federal Rehabilitation Act and the Americans with Disabilities Act.

4.10 Culturally-Appropriate Services

The Contractor will respect and support the linguistic and cultural ties of the client and his/her family in the delivery of services.

5.0 SERVICES ACCORDING TO INDIVIDUAL NEED

5.1 Eligibility

Client eligibility and service referral is the responsibility of DSHS/DDA, pursuant to WAC 388-823. Children are not eligible for services on or after their third birthday.

All children must have evidence of a multi-disciplinary evaluation for eligibility available within the child's file, in line with ESIT requirements.

5.2 Admission and Termination Criteria

The Contractor retains the right to deny new referrals for service. The Contractor also retains the right to terminate services to individuals for cause.

a. The Contractor shall have written policies and procedures in place detailing admission and termination criteria that are provided to the client/guardian upon request for or entry into services.
b. The policies shall describe the reasons that may lead to non-acceptance of a referral or termination of current service to an individual child/family.

5.3 Individual Family Service Plan (IFSP)

The IFSP is the driver for all Child Development Services provided by the Contractor.

The Contractor is responsible, in collaboration with ESIT, for ensuring each child authorized for County services has an IFSP which is developed and implemented in line with ESIT policy and procedures.

The IFSP will be reviewed at least every 6 months, or more often if conditions warrant , or by family request, in collaboration with ESIT and the child's Family Resources Coordinator.

5.4 Implementing Services in Natural Environments

Natural environments mean settings that are natural or normal for the child's age peers who have no disabilities. Services should be provided in home, neighborhood, or community settings in which children without disabilities participate.

Methods and strategies used to promote family-centered services in natural environments should include, but are not limited to, the following:

a. Identifying and documenting everyday family and community activity settings.
b. Identifying and documenting child interests and family assets for learning.
c. Selecting everyday activities as contexts for interest-based child learning.
d. Increasing the child's learning opportunities in everyday family and community learning environments.
e. Using responsive teaching strategies which support the parent to identify and engage their child in everyday learning opportunities.
f. Creating new learning opportunities within family and community activities.

5.5 Services in Other than Natural Environments

Settings that are not *"natural settings"* include clinics, hospitals, therapists' offices, rehabilitation centers, and segregated group settings. This includes any settings designed to serve children based on categories or disabilities.

Justification for services which occur in settings other than natural environments will include the following:

- Sufficient documentation to support the IFSP team's decision that the child's outcome(s) could not be met in natural settings, even with supplementary supports.
- How the services provided in a specialized setting will be generalized into the child's daily activities and routines.
- A plan with timelines and the supports necessary to return to early intervention within daily activities and routines, as soon as possible.

5.6 Service Documentation

a. The Contractor will ensure that all services provided under this contract will have clear, dated documentation showing services provided relative to the billed unit, available to the County for review upon request. All documentation, including staff case notes, must be legible and must relate to the IFSP. The Contractor will ensure that a supervisor or other responsible agency staff reviews these items.

b. The Contractor will document each child's progress towards the goals and objectives established in the IFSP. This information will be documented in collaboration with the Child's FRC as established by ESIT.

6.0 ORGANIZATIONAL REQUIREMENTS

6.1 Board of Directors

a. The Contractor, if it has a board of directors, will include members who are knowledgeable about developmental disabilities, who understand their responsibilities as board members, and who are able to give guidance and direction to the legal, fiscal, and programmatic aspects of program activities.

b. The Board's membership roster, copies of the by-laws, and minutes of meetings will be available for review.

c. The Board will approve the agency's annual budget, and there will be Board oversight of fiscal operations.

6.2 Administration

The Contractor will:

a. Maintain current organizational charts describing administrative lines of authority and containing the position titles of program staff.
b. Maintain a job description for each position within the organization detailing duties, responsibilities, and necessary qualifications.
c. Have a written statement describing the mission of the organization.
d. Provide a Contractor representative to participate in meetings scheduled by the County concerning County, State, and Federal requirements.
e. The contractor will written policy manuals for information systems, personnel and accounting/finance in sufficient detail such that operations can continue should staffing change or absences occur.
f. Have on file all appropriate certificates and licenses in order for the contracting agency to operate as required by Federal, State, or local law, rule, or regulation.

6.3 Performance Plan

The Contractor will develop a written performance plan that describes its mission, program objectives, goal outcomes, and strategies relevant to the County Guidelines and the provision of services under contract with the County. The plan shall be evaluated at least biennially and revised based on actual performance.

6.4 Client Involvement

The Contractor will identify meaningful ways to involve family/guardians of children with developmental disabilities in program and policy development and document the impact this has on the program.

6.5 Independent Financial Review or Audit Requirements

Contractors receiving in excess of $100,000 annually shall obtain a periodic independent review of financial statements or independent audit of financial records. The review or audit shall be performed biennially based upon the fiscal year of the Contractor. This requirement will be included in all subcontractor contracts.

The purpose of the independent review or audit is to reasonably ensure the financial stability of County contractors and that adequate internal control exists to ensure the efficient, proper processing and use of contract funds.

For agencies receiving less than $100,000 annually, the county may request to review agency financial statements.

If the Contractor is subject to OMB Circular A-133, it or its subcontractors shall comply with the single audit requirement of OMB Circular A-133. In the event of audit findings,

the Contractor will take appropriate corrective action, per OMB Circular A-133 requirements.

6.6 Continued Qualification

The contractor must maintain their status as a qualified provider in line with the requirements set forth in DSHS/DDA policy 6.13.
https://www.dshs.wa.gov/sites/default/files/DDA/dda/documents/policy/policy6.13.pdf

7.0 STAFF TRAINING AND QUALIFICATIONS

7.1 Staff Qualifications

The Contractor must ensure that its staff meets provider qualifications and employs hiring and training procedures as outlined in DSHS/DDA Policy 6.13, "Day Program Provider Qualifications" as presently adopted or subsequently amended.

7.2 Staff Training and Certification

All staff providing CDS services must meet the personnel standards established for their discipline under ESIT guidelines. Documentation of current certification is required.

Employees providing direct services to children and toddlers must be 18 years or older and will receive basic orientation to and training in client services to ensure that employees meet the qualifications specified in DSHS/DDA Policy 6.13.

Staff orientation and training in line with Policy 6.13 must be documented in the personnel file. A summary of the training requirements and timelines within Policy 6.13 is outlined below. Any future amendments or modifications to the policy take precedent.

a. Prior to working with clients unsupervised, staff must have knowledge of and receive training in the following areas:

1) Client confidentiality;
2) Current Individual Family Service plans for each client with whom the employee works;
3) DDA Policy 5.06, *Client Rights*;
4) DDA Policy 6.08, Mandatory reporting Requirements for Employment and Day Program Service Providers. (DDA Policy 6.08 verification statement must be signed and kept in the employee file.)
5) DDA Policy 9.07 HIV and AIDS
6) First Aid and CPR (current certification is required)

b. **Within three (3) months of employment** employees must have received training in the following:
1) DDA Policy 5.19 Positive Behavior Supports for Children and Youth

c. **Continuing Education and Staff Evaluation:** In addition to the above DDA requirements, it is the County's expectation that each contractor have an established procedure for orienting, training, mentoring and providing on-going evaluation to staff including:

1) Values that support family centered practice and learning as outlined in the County Guidelines and within IDEA part C
2) Effective communication skills (i.e., the ability to listen carefully and to make one's self understood;
3) Planning methods; and
4) Continuing education to support staff in the performance of their work to better serve children and families.

7.3 Training Reimbursement

Requests for training reimbursement related to County-recommended training events, or other training designed to improve the quality of services to individuals under the County contract, may be made in writing to the County at least ten (10) business days prior to the training event. Costs for which the Contractor may request a training reimbursement include registration and related travel costs. Requests should clearly outline the training requested, dates, the number of staff attending, the destination, and travel reimbursement requested.

Mileage reimbursement may not exceed the County's established reimbursement rate. Acceptance of training reimbursement requests is at the discretion of the County and is dependent upon funding availability. Reimbursement for training requests will require back-up documentation and receipts.

8.0 DSHS/DDA COUNTY SERVICE AUTHORIZATION

8.1 Necessary Pre-Authorization

A DSHS/DDA County Service Authorization (CSA) is required for each client for whom the Contractor intends to submit a billing to the County. The County Service Authorization form must be finalized by the DDA Case/Resource Manager, and the County before it is deemed valid.

The County will not reimburse for services provided prior to authorization. In the event that the contractor does not accept a child for services, the contractor must note the reason within the comments section of the CSA and return to the County within 10 business days.

8.2 Termination

The Contractor must notify the County when a child has terminated from service prior to the child's third birthday. The effective date of the termination and the reason for termination will be documented

8.3 Coordination with ESIT

Family Resource Coordinators (FRC) are an important part of CDS services. The Contractor is required to keep the client's FRC informed of any major changes in the client's program, including funding or support changes.

The Contractor will participate as appropriate in on-going assessments, IFSPs, and staffing related to the provision of services as requested by ESIT.

9.0 OUTCOMES

The following are the expected outcomes associated with the provision of Child Development Services under the County contract.

a. An increase in the child's developmental performance, as defined by established state and federal functional outcome guidelines and assessment practices. These include assessing the child relative to same-aged peers in the following areas:
b. Positive social-emotional skills (including social relationships).
c. Acquisition and use of knowledge and skills (including early language/communication).
d. Use of appropriate behaviors to meet their needs.
e. Increased ability of parents, guardians, and caregivers, including child care providers, to enhance the developmental progress of their children and promote quality parent-child interactions and relationships.
f. The integration of children with developmental disabilities in natural environments and/or typical settings with children without developmental disabilities.

10.0 MONITORING AND EVALUATION

The County will develop a quality assurance and evaluation process to monitor contract compliance. The review will incorporate:

- DSHS/DDA criteria for evaluation
- DSHS/DDA Policy 6.13
- DSHS/DDA County Guidelines
- The DSHS/DDA Program Agreement with the County for the current biennium
- Provider agreement with Whatcom County Health Department
- This implementation guide

The County shall conduct at least one formal on–site visit review during each DSHS/DDA biennium. A formal written report will be sent to the agency summarizing the review findings, recommendations and corrective action. The contractor is required to file a written response within 30 days. The review process must be successfully completed in order to maintain qualified provider status with Whatcom County.

10.1 Access to Records

The County may request reasonable access to the Contractor's records and place of business for the purpose of monitoring, auditing, and evaluating the Contractor's compliance with the Agreement and applicable laws and regulations. The Contractor will, upon receiving reasonable written notice, provide the County with access to its place of business and to its records that are relevant to its compliance with the Agreement and applicable laws and regulations.

10.2 Corrective Action

The Contractor will be responsible for addressing in writing all County findings and recommendations by the due date specified in the County contract compliance report.

10.3 Extended Records Retention Timeframe

During the term of the Agreement and for six (6) years after termination of the Agreement, the parties shall maintain records sufficient to:

- Document performance under this contract.
- Demonstrate accounting procedures, practices, and records that sufficiently and properly document all invoices, expenditures, and payments.

In the event of litigation, unresolved audits, and/or unresolved claims, the Contractor agrees to retain all records, reports, and other documentation until such claims are resolved.

11.0 NON-COMPLIANCE

In the event the Contractor fails to comply with any of the terms and conditions of this contract and that failure results in a contract overpayment, the County shall recover the amount due to the County. In the case of overpayments, the Contractor shall cooperate in the recoupment process and return to the County the amount due.

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. "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. For purposes of this contract, data classified as Category 4 refers to data protected by: the Health Insurance Portability and Accountability Act (HIPAA).

d. "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 iCloud, Dropbox, Box.com, and many other entities. Enterprise cloud vendors include Microsoft Azure, Amazon Web Services, O365, and Rackspace.

e. "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 128 bits (256 preferred and required to be implemented by 6/30/2020) 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.

f. "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.

g. "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.

h. "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.

i. "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.

j. "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.

k. "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.

l. "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.

m. "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/fsa/central-contract-services/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 data, 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 data, 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.

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 do not allow end-user modification. Examples would include but not be limited to installing key loggers, malicious software, or any software that will compromise DSHS data.

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

(3) Using industry standard protocols and solutions for remote access. Examples include, but are not limited to RADIUS Microsoft Remote Desktop (RDP) 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. All Contractors must be in compliance by 6/30/2020.

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 attest to the contact listed in the contract and keep a copy of that attestation for your records 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.

(f) The Data will not be downloaded to non-authorized systems, meaning systems that are not on the contractor network.

(g) The Data will not be decrypted until downloaded onto a computer within the control of an Authorized User and within the 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 HIPAA compliant.

(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 category 4 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.

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

(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 DSHS Data is no longer needed, except as noted above in Section 5.b, DSHS 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, incineration, or contractor
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.