2022

Skagit County Developmental Disabilities Program

Child Development Services Implementation Guide

1.0	PURPOSE	2
2.0	MODIFICATION	2
3.0	DEFINITION OF TERMS	2
4.0	APPLICABLE POLICIES, LAWS & REGULATIONS	8
5.0	ORDER OF PRECEDENCE	9
6.0	HEALTH, SAFETY & INDIVIDUAL RIGHTS	10
	6.1 Background Checks	10
	6.2 Mandatory Reporting of Abuse, Neglect & other Incidences	10
	6.3 Access to Disability Rights WA (DRW)	11
	6.4 Family Rights	11
	6.5 Health & Safety Regulations	12
	6.6 Staff Intervention	12
	6.7 Confidentiality	13
	6.8 Non-Discrimination	14
	6.9 Culturally-Appropriate Services	14
7.0	SERVICES ACCORDING TO INDIVIDUAL NEED	14
	7.1 Eligibility	14
	7.2 Admission & Termination Criteria	15
	7.3 Individualized Family Service Plan (IFSP)	16
	7.4 Content of IFSP	16
	7.5 Other Services	17
	7.6 Transition Steps and Services	18
8.0	EMPLOYMENT & DAY SERVICES QUALIFIED PROVIDER INFORMATION	18
	8.1 Qualifications	18
	8.2 Staff Qualifications & Training	19
	8.3 Training Reimbursement	20
9.0	OUTCOMES	21
10.0	MONITORING & EVALUATION	21
	10.1 Access to Records	21
	10.2 Corrective Action	21
11.0	NON-COMPLIANCE	21
12.0	NO ACTIVE DEBARMENT	21

1.0 PURPOSE

The Skagit County Public Health Developmental Disabilities Program currently contracts to provide Child Development Services to clients of 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 policies, procedures, and requirements related to the implementation of County-funded child development services.

The requirements outlined in this guide, and 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

2.0 MODIFICATION

This guide provides a summary of State and County policy, procedures, and references applicable to 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.

3.0 DEFINITION OF TERMS

Acuity Level:	The level of an individual's abilities and needs as determined through the DDA assessment
American Indian/ Alaska Native; Indian tribe:	1. Mean a person having origins in any of the original people of North and South America (Including Central America) and who maintain tribal affiliation or community attachment. 2. Indian tribe means any federally or state recognizes Indian tribe, band rancheria, pueblo, colony, or community, including any Alaska native village or regional village corporation (as defined in or established under the Alaska Native Claims Settlement Act, 43 U.S.C. 1601 et seq.) 3. Nothing in this definition is intended to indicate that the United State Secretary of the Interior is required to provide services or funding to a state Indian tribe that is not listed in the Federal Register list of Indian entities recognized as eligible to receive services from the United State, published pursuant to section 104 of the Federally Recognized Indian Tribe List Act of 1994, 25 U.S.C. 479a-1.
AWA:	ALTSA Web Access
Additional	

Consumer Services: Refers to indirect client service types as follows:

1. "Community Information and Education": Activities to inform and/or educate the general public about developmental disabilities and related services. These may include information and referral services; activities aimed to promoting public awareness and involvement; and community consultation, capacity building and organization activities.

2. "Training": To increase the job-related skills and knowledge of staff, providers, volunteers, or interning students in the provision of services to people with developmental disabilities. Also, to enhance program related skills to board or advisory board members.

3. "Other Activities": reserved for special project and demonstrations categorized into the following types:

    a. Infrastructure projects: Projects in support of Clients (services not easily tracked back to a specific working age Client) or that directly benefit a Client(s) but the client in not of working age. Examples include planning services like benefits planning or generic job development e.g. "Project Search".

    b. Start-up Projects: Projects that support an agency or directly benefit the agency. Examples include equipment purchases and agency administrative support.

    c. Partnership Project: Collaborative partnerships with school districts, employment providers, DVR, families, employers, and other community collaborators needed to provide the employment supports and services young adults with developmental disabilities require to become employed during the school year they turn twenty-one (21).

Appropriate early intervention services: Determined through the IFSP process. The IFSP must include a statement of the specific early intervention services necessary to meet the unique needs of the child and the family to achieve

	the outcomes identified in the IFSP. Federal Part C regulations define early intervention services as services that "are designed to meet the developmental needs of each child eligible under Part C and the needs of the family related to enhancing the child's development."
Authorized User:	An individual with an authorized business requirement to access DSHS Confidential Information
BARS:	Budget and Accounting Reporting System
CMIS:	Case Management Information System
Client:	A person with a developmental disability as defined in chapter 388-823 WAC who is currently eligible and active with the Developmental Disabilities Administration or is an identified Child: An individual under the age of six (6) and may include an infant or toddler with a disability, as that term is defined in this section.
Consent:	1. The parent has been fully informed of all information relevant to the activity for which consent is sought, in the parent's native language, as defined in this section; 2. The parent understands and agrees in writing to the carrying out of the activity for which the parent's consent is sought, and the consent form describes that activity and lists the early intervention records (if any) that will be released and to whom they will be released and a. The parent understands that the granting of consent is voluntary on the part of the parent and may be revoked at any time; and b. If a parent revokes consent, that revocation is not retroactive to an action that occurred before the consent was revoked.
Consumer Support:	Refers to direct Client service types: Community Inclusion (CI), Child Development Services (CDS), Individual Supported Employment (IE), Individualized Technical Assistance (ITA), Group Supported Employment (GSE)
Confidential Information:	Information that is exempt from disclosure to the public or other unauthorized persons under Chapter 42.56 RCW or other federal or state laws. Confidential information includes but is not limited to personal information.

Contractor:	A Provider that delivers specified services under contract with the Skagit County Public Health and Community Services, Developmental Disabilities Program
CRM:	DDA Case Resource Manager
CSA:	County Service Authorization
County:	The political subdivision of the state of Washington and the county or counties entering into this Program Agreement.
County Lead Agency:	(CLA) The four (4) designated county organizations, under contract with DCYF's ESIT program, to ensure through subcontracts with EIPA's and EIS Providers, that EIS are provided countywide in accordance with the CLA's contract with ESIT, Part C of IDEA, and Washington's Federally Approved State Plan.
DCYF:	Department of Children, Youth and Families of the State of Washington
DD:	developmental disabilities
DDA:	Department of Social and Health Services, Developmental Disabilities Administration.
DDA Region:	DDA Regional office
Developmental delay:	used with respect to a child residing in Washington State , has the following meaning: 1. A child has a developmental delay if she/he is experiencing a 1.5 standard deviation or 25 % of chronological age delay in one or more developmental areas: or 2. Has a diagnosed physical or mental condition that has a high probability of resulting in developmental delay.
DSHS:	Washington State Department of Social and Health Services
DVR:	Division of Vocational Rehabilitation
Early Intervention Provider Agency (EIPA):	An organization and its subcontractors that are under contract with DCYF's ESIT program or the four (4) CLA's to provide EIS in a designated school district catchment area of the state.
Early Intervention Service Provider:	An entity (whether public, or private, or nonprofit, including school districts) or an individual that is either an employee or

	subcontractor, who provides EIS in accordance with the CLA or EIPA's contract with ESIT, Part C of IDEA, and Washington Federally Approved
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.
Family Resources Coordinators (FRCs):	Work with families, can suggest additional materials to help families understand their procedural safeguards under Part C. They can also suggest ways that you and other family members can be partners with professional to help meet the developmental needs of child.
General Terms and Conditions:	The Contractual provisions contained within that agreement, which govern the contractual relationship between DSHS and the county.
HCBS:	Medicaid Home and Community Based Services.
Hardened Password:	A string of at least eight characters containing at least one alphabetic character, at least one number and at least one special character such as an asterisk, ampersand or exclamation point.
IDEA:	Individuals with Disabilities Education Act
Natural environments:	The statewide system includes policies and procedure to ensure, consistent with 34 CFR §§303.13(a)(8) (EIS), 303.26 (natural environments), and 303.344(d)(1)(ii) (content of an IFSP), that EIS for infants and toddlers with disabilities are provided: 1. To the maximum extent appropriate, in natural environments; and 2. In settings other than the natural environment that are most appropriate, as determined by the parent and the IFSP team, only when EIS cannot be achieved satisfactorily in a natural environment.
Native Language:	The language normally used by family, child or the mode of communication that is normally used by the person (sign language, braille, or oral communication).
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.
Personal Identifiable Information:	Includes: 1. the name of your child, your name, or the names of other family members; 2. the address of your child or family; 3. a personal identifier such as your child's or your social security number; 4. other indirect identifiers, such as your child's date of birth, place of birth, and mother's maiden name; 5. a list of personal characteristics or other information that would make it possible to identify your child with reasonable certainty; or 6. information requested by a person who the early intervention program reasonable believes knows the identity of your child.
Physically Secure:	Access is restricted through physical means to authorized individuals only.
Quality Assurance:	Adherence to all Program Agreement requirements, including DDA Policy 6.13, Employment/Day Program Provider Qualifications, County Guidelines, and the Criteria for Evaluation, as well as a focus on reasonably expected levels of performance, quality, and practice.
Quality Improvement:	A focus on activities to improve performance above minimum standards and reasonably expected levels of performance, quality, and practice.
RCW:	Revised Code of Washington
Secured Area:	An area to which only authorized representatives of the entity possessing the Confidential Information have access. Secured Areas may include buildings, rooms, or locked storage containers (such as a filing cabinet) within a room, as long as access to the Confidential Information is not available to unauthorized personnel.
Service Provider:	A qualified Client service vendor who is contracted to provide Employment and Day Program Services.
Subcontractor:	The Service Provider contracted by the County to provide services.

Trusted Systems:	Includes only the following methods of physical delivery (1) hand-delivery by a person authorized to have access to the Confidential Information with written acknowledgement of receipt; (2) United States Postal Service ("USPS") first class mail, or USPS delivery services that include Tracking, such as Certified Mail, Express Mail or Registered Mail; (3) commercial delivery services (e.g. FedEx, UPS, DHL) which offer tracking and receipt confirmation. For electronic transmission, the Washington State Governmental Network (SGN) is a Trusted System for communications within that Network.
Unique User ID:	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.
WAC:	Washington Administrative Code

4.0 APPLICABLE POLICIES, LAWS & REGULATIONS

The Contractor will provide employment and community inclusion services to persons 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.

A. Federal Law

- Americans with Disabilities Act (ADA) Americans with Disabilities Act | U.S. Department of Labor (dol.gov)
- Individuals with Disabilities Education Act (IDEA) http://idea.ed.gov/
- Individuals with Disabilities Education Act (IDEA) Part 303 (Part C) – Early Intervention Program for Infants and Toddlers with Disabilities Part 303 (Part C)— Early Intervention Program For Infants And Toddlers With Disabilities - Individuals with Disabilities Education Act
- Home and Community-based Settings Home & Community Based Settings Requirements Compliance Toolkit | Medicaid
- The Child Abuse Prevention and Treatment Act (CAPTA) The Child Abuse Prevention and Treatment Act (CAPTA) | The Administration for Children and Families (hhs.gov)
-

B. Revised Code of Washington

26.44	Abuse of Children
42.56	Public Records Act
43.216	Department of Children, Youth and Families
43.43.830 - 845	Background Checks
71A.14.070	Confidentiality of Information, Oath

74.15.030	Background Checks
74.34	Abuse of Vulnerable Adults

C. Washington Administrative Code

Title 110	Department of Children, Youth and Families
296-24	General Safety & Health
388-823	Developmental Disabilities Administration Eligibility
388-825	Developmental Disabilities Administration Service Rules
388-845	Home and Community Based Waivers
388-850:	Program Operations, General provisions
388-06	Background Checks
388-845	HCBS Waiver definitions

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

a. Policy 5.03 Client Complaints
b. Policy 5.05 Limited English Proficient Clients
c. Policy 5.06 Client Rights
d. Policy 5.13 Protection from Abuse: Mandatory Reporting
e. Policy 5.19 Positive Behavior Support for Children and Youth
f. Policy 5.20 Restrictive Procedures and Physical Interventions with Children and Youth
g. Policy 6.08 Incident Management and Reporting Requirements for County and County-Contracted Providers

E. County Guidelines

Please see:
https://www.dshs.wa.gov/sites/default/files/DDA/dda/documents/c_guidelines.pdf

F. County Criteria for Evaluation

Please see Counties Best Practices website, Administrative Reference Section:
https://www.dshs.wa.gov/dda/county-best-practices

5.0 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:

1. Applicable federal, state, and local law, regulations, rules, and ordinances
2. This agreement
3. Any document incorporated in the Agreement by reference

6.0 HEALTH, SAFETY, & INDIVIDUAL RIGHTS

6.1 Background Checks

A background/criminal history clearance is required every three years for all employees, subcontractors, and/or volunteer who may have unsupervised access to vulnerable DSHS Clients, in accordance with RCW 43.43.830-845, RCW 74.15.030 and chapter 388 WAC.

The Contractor will ensure that:

- The criminal background clearance is completed in line with timelines and requirements outlined in DSHS/DDA policy 5.01 *Background Authorizations*
- Individuals who have resided less than three (3) consecutive years in Washington State must be fingerprinted so that an FBI criminal history may be completed.
- Initial background checks are completed before hiring.
- Applicant's information provided on the form is verified through photo identification such as driver's license, passport, tribal ID, etc.

The Contractor will make available upon request by the County proof of satisfactory background check clearance, free of disqualifying convictions from the DSHS Background Check Unit (BCCU), for each employee, subcontractor, intern, and/or volunteer involved with the provision of services specified in this Agreement. If the entity reviewing the application elects to hire or retain an individual after receiving notice that the applicant has a conviction for an office that would disqualify the applicant from having unsupervised access to vulnerable adults as defined in Chapter 73.34 RCW, then payment shall be denied for any subsequent services rendered by the disqualified individual provider. The DSHS Background Check Central Unit (BCCU) must be utilized to obtain background clearance.

DSHS/DDA background check forms and information may be found at:
http://www.dshs.wa.gov/BCCU/bccuforms.shtml

Current definitions and listing of disqualifying convictions are available online at:
Disqualifying List of Crimes and Negative Actions | DSHS (wa.gov)

6.2 Mandatory Reporting of Abuse, Neglect & other Incidents

Contractor staff members providing services to individuals with developmental disabilities are deemed mandatory reporters, and are responsible for reporting incidents of suspected abuse, improper use of restraint, neglect, self-neglect, personal or financial exploitation, abandonment, and mistreatment of clients of the DDA as well as other types of incidents. Reporting of incidents involving DDA clients shall be in line with the requirements and definitions listed within 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.
- Attachment A provides a summary of the reporting timelines in Policy 6.08.
- Attachment B provides a copy of the form required for signature by all contractor's staff upon initial hire and then annually thereafter (effective 7.1.11). This assurance form

verifies that contractors' staff members have read and will abide by Policy 6.08. Another format may substitute if it contains all the elements required.

- DSHS form 10-331 DDA Mortality Review referenced in the policy can be found at the following link: https://www.dshs.wa.gov/sites/default/files/FSA/forms/pdf/10-331.pdf
- Incident reports are tracked and analyzed for potential trends and patterns.

6.3 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 WPAS to clients and to client records as outlined in the DSHS/DRW Access Agreement.

https://www.dshs.wa.gov/sites/default/files/DDA/dda/documents/policy/policy13.04.pdf

6.4 Family Rights

The Contractor will provide each family who is receiving services with information explaining the client's rights as a consumer of contracted services. This information will include the following:

A. The right to multidisciplinary evaluation and assessment followed by the development of an Individualized Family Service Plan (IFSP) at the initial IFSP meeting, within 45 calendar days from referral. "Multidisciplinary" means the involvement of two or more different disciplines or specialties such as an educator and physical therapist.

B. The right to receive evaluation, assessment, IFSP development, service coordination, and procedural safeguards at no cost to families.

C. The right to receive evaluation, if you request and provide consent for it, at any time during the screening process (if used).

D. If eligible under Part C, the right to receive appropriate early intervention services for your child and family as addressed in IFSP.

E. The right to refuse screening, evaluations, assessments, and services.

F. The right to be invited to and participate in all meetings in which a decision is expected to be made regarding a proposal to change the identification, evaluation, or placement of your child, or the provision of appropriate early intervention services to your child or family.

G. The right to receive timely written notice before a change is proposed or refused in the identification, evaluation, or placement of your child, or in the provision of appropriate early intervention services to your child or family.

H. The right to receive each early intervention service in natural environments to the extent appropriate to meet your child's developmental needs.

I. The right to maintenance of the confidentiality of personally identifiable information.

J. The right to obtain an initial copy of your child's early intervention record at no cost.

K. The right to a copy of each evaluation, assessment and IFSP which must be provided to you as soon as possible after each IFSP meeting.

L. The right to inspect and review and, if appropriate, amend your child's records.

M. The right to request mediation and/or an impartial due process hearing to resolve parent/provider disagreements.

N. The right to file an administrative complaint.

6.5 Health & 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). The Contractor will develop and update an annual Health and Safety Plan for each participant.

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

Federal: Occupational Safety and Health Act of 1970, P.L. 91-596, 84 USC 1590

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

6.6 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 interventions shall meet requirements under DSHS/DDA Policy 5.19: *Positive Behavior Supports for Children and Youth.* Policy 5.20: *Restrictive Procedures* and Physical Interventions with Children and Youth.

Restrictive procedures implemented under emergency guidelines as described in DDA Policy 5.22 *Restrictive Procedures and Restraints* and Policy 5.17 *Physical Intervention Techniques* must be reported in writing to DDA within one (1) business day as outlined in Policy 6.08 Incident Management and Reporting Requirements for County and County-Contracted Providers.

6.7 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, RCW 42.56, Public Records Act
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/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.
3. Ensuring the security of confidential information transmitted via fax (Facsimile) by verifying the recipient phone number to prevent accidental transmittal of confidential information to an unauthorized provider.
4. Use of State of Washington secure email server when communicating confidential information through email.

D. When transporting six (6) to one hundred and forty nine (149) records containing Confidential Information, outside of a secure area, do one or more of the following as appropriate:

1. Use a Trusted System
2. Encrypt the confidential information, including:
   - Email and/or email attachments
   - Confidential information when it is stored on portable devices or media, including but not limited to laptop computers and flash memory devices.

E. When transporting one hundred fifty (150) records or more containing confidential information outside a secure area, refer to the requirement in Attachment C – Data Security Requirements.

F. 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 and the entity contracted to carry out file destruction.

G. Paper documents with confidential information may be recycled through a contracted firm, provided the contract with the recycler specifies that the confidentiality of information will be protected, and the information destroyed through the recycling process. Paper documents containing confidential information requiring special handling (e.g. protected health information) must be destroyed through shredding, pulping or incineration.

H. The compromise or potential compromise of confidential information must be reported to the County DD Coordinator and DDA Regional Administrator within one (1) business day of discovery. The Contractor must also take actions to mitigate the risk of loss and comply with any notification or other requirements imposed by law.

6.8 Non-Discrimination

The Contractor will not discriminate against any person on the basis of race, age, creed, political ideology, color, national origin, citizenship or immigration status, sex, military status, marital status, sexual orientation including gender Identity, age, HIV/AIDS status or the presence of any sensory, mental, or physical disability or the use of a trained dog guide or service animal by a person with a disability. 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.

Families have access to culturally competent services within appropriately and adequately trained personnel.

Contractor ensures that traditionally underserved groups, including minority, low-income, homeless and rural families and children with disabilities who are wards of the state, are meaningfully involved in the planning and implementation of all the requirements of Part C of IDEA; and their local geographical areas.

6.9 Culturally Appropriate Services

The Contractor will respect and support the linguistic and cultural background of the participant and his/her family in the delivery of services. The Contractor shall ensure equal access of services and programs to those persons who do not speak, have a limited ability to speak, read or write English well enough to understand and communicate effectively pursuant to DDA Policy 5.05, Limited English Proficient (LEP) clients.

7.0 SERVICES ACCORDING TO INDIVIDUAL NEED

7.1 Eligibility

Children, birth to three, shall be eligible for Early Intervention Services (EIC) Under Part C of IDEA, if the multidisciplinary team finds any one of the following criteria exists:

A. Developmental delay:

1. A child shall be eligible if he or she demonstrates a delay of 1.5 standard deviation or 25 % of chronological age delay in one or more of the following

developmental areas, as measured by appropriate diagnostic instruments and procedures, and administered by qualified personnel;

I. Cognitive
II. Physical (fine or gross motor)
III. Communication (receptive or expressive language
IV. Social or Emotional
V. Adaptive

2. Informed Clinical Opinion
   I. The state lead agency (SLA) shall ensure that informed clinical opinion given by qualified personnel may be used as an independent basis to establish a child's eligibility even when instruments do not establish eligibility; and
   II. In no even may informed clinical opinion be used to negate the results of evaluation instruments used to establish eligibility.

B. Diagnosed physical or mental condition: A child shall be eligible if he or she has a diagnosed physical or mental condition that has a high probability of of resulting in developmental delay. Such conditions include but are not limited to:

1. Chromosomal abnormalities
2. Genetic or congenital disorders
3. Sensory impairments
4. Inborn errors of metabolism
5. Disorders reflecting disturbance of the development of the nervous system
6. Congenital infections
7. Severe attachment disorders
8. Toxic substances – disorders secondary to exposure to toxic substances, including fetal alcohol syndrome.

7.2 Admission & 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.

1. The Contractor shall have written policies and procedures in place detailing admission and termination criteria that are provided to the client upon request for or entry into services.

2. The policies shall describe the reasons that may lead to non-acceptance of a referral or termination of current service to an individual.

7.3. Individual Family Service Plan

1. For the purpose of adopting requirements for Individual Family Service Plans (IFSP) under Part C of the IDEA, the following definitions apply:
   a. *Individualized family service plan (IFSP)* means a written plan for providing EIS to an infant or toddler with a disability under Part C of IDEA and the infant's or toddler's family that:

i. Is based on the evaluation and assessment described in ESIT policies and procedures;
ii. Includes the content specified in ESIT policies and procedures;
iii. Is implemented as soon as possible once parental consent for the EIS in the IFSP is obtained, consistent with ESIT policies;
iv. Is developed in accordance with the IFSP procedures according to ESIT policy
v. Provides a consistent level of frequency and intensity for a continuous twelve-month period based on child and family need, and not availability of providers.

b. *Frequency and intensity* means the number of days or sessions that a service will be provided, and whether the service is provided on an individual or group basis.
c. *Method* means how a service is provided
d. *Natural environments* mean settings that are natural and typical for same-aged infant and toddler without a disability, may include the home or community settings
e. *Location* means the actual setting, place or places, where a service will be provided.
f. *Length* means the length of time the service is provided during each session of that service, such as an hour or other specified time period.
g. *Duration* means projecting when a given service will no longer be provided, such as when the child is expected to achieve the results or outcomes in her or her IFSP.

2. For each infant or toddler with a disability, the state lead agency shall ensure the development, review and implementation of an IFSP is developed by a multidisciplinary team, which includes the parent.
3. The SLA ensures, if there is a dispute between agencies, as to who has responsibility for developing or implementing an IFSP, the SLA shall resolve the dispute and assign responsibility.
4. Ensure to the maximum extent appropriate to the needs of the child, EIS are provided in natural environments.

7.4 Content of IFSP

The IFSP shall include:

1. Based on the information from the child's evaluation and assessments conducted under ESIT policy and procedures, a statement of the infant and toddler with a disability's present levels of:
    a. Physical development, including fine motor, gross motor, vision, hearing and health status
    b. Cognitive development
    c. Communication development
    d. Social or emotional development and
    e. Adaptive development; and
2. With the concurrence of the family, a statement of the family's resources, priorities, and concerns related to enhancing the development of the child as identified through the assessment of the family under ESIT policies and procedures;

3. A statement of the measurable results for measurable outcomes expected to be achieved for the child, including pre-literacy and language skills, as developmentally appropriate for the child and family and the criteria, procedures, and timelines used to determine:
    a. The degree to which progress toward achieving the results or outcomes, identified in the IFSP, is being made: and
    b. Whether modifications or revisions of the expected results or outcomes or EIS identified in the IFSP are necessary; and

4. A statement of the specific EIS based on peer-reviewed research, to the extent practicable, that are necessary to meet the unique needs of the child and the family, to achieve the results or outcomes identified above including:
    a. Length, duration, frequency, intensity, and method of delivering the EIS;
    b. A statement that each early intervention service is provided in the natural environment for that child or service to the maximum extent appropriate, consistent with ESIT policies and procedures, or subject to Part C of IDEA, a justification as to why an early intervention service will not be provided in the natural environment;
    c. The determination of the appropriate setting for providing EIS to an infant or toddler with a disability, including any justification for not providing a particular early intervention service in the natural environment for the infant or toddler with a disability and service, shall be:
        i. Made by the IFSP team, which included the parent and other team members;
        ii. Consistent with the provisions in the ESIT policies and procedures; and
        iii. Based on the child's outcomes that are identified by the IFSP team; and
            1. The location of the EIS; and
            2. The payment arrangements, if any; and
    d. EIS providers may not interrupt, modify, or otherwise change the delivery of EIS for reasons unrelated to the child's individual needs, including service availability, changes in EIS providers' schedules, or availability or staff including, during summer months;

7.5 Other Services:

1. The IFSP shall identify medical and other services that the child or family needs or is receiving through other sources, but that are neither required by team agreement or funded under Part C of IDEA; and
    a. If those services are not currently being provided, include a description of the steps the FRC or family may take to assist the child and family in securing those other services; and
2. The projected date for the initiation of each early intervention service in the IFSP, which date shall be as soon as possible after the parent consents to the service, as required in the policies and procedures and the anticipated duration of each service;
3. The name of the FRC from the profession most relevant to the child's or family's needs, or who is otherwise qualified to carry out all applicable responsibilities under this Part C of IDEA, who will be responsible for implementing the EIS identified in a child's IFSP, including transition services, and coordination with other agencies and persons. In

meeting the requirements of this section, the term profession included service coordination.

7.6 Transition Steps and Services:

1. Steps and services to be taken to support the smooth transition of the child accordance with these policies and procedures from Part C of IDEA to:
    a. Preschool services under Part B of IDEA, to the extent that those services are appropriate; or
    b. Other appropriate services; and
2. The steps required in this section include:
    a. Discussions with and training of parents, as appropriate, regarding future placements and other matters related to the child's transition;
    b. Procedures to prepare the child for changes in service delivery, including steps to help the child adjust to, and function in, a new setting;
    c. Confirmation that child find information about the child has been transmitted to the local educational agency (LEA) or other relevant agency, in accordance with ESIT policies and procedures and, with parental consent if required, transmission of additional information needed by the LEA to ensure continuity of services from the Part C of IDEA program to the Part B of IDEA program, including a copy of the most recent evaluation and assessments of the child and family and most recent IFSP development in accordance with ESIT policy; and
3. Ensure a seamless transition between services under Part C of IDEA and under Part B of IDEA through the development and implementation of an interagency agreement that meets the requirement of ESIT policy, chapter 392-172A WAC, rules for special education.
4. Ensure transition notification, conference and plan occurs.

8.0 EMPLOYMENT AND DAY SERVICES QUALIFIED PROVIDER INFORMATION

To be a qualified provider of Child Development Services, an agency employee must have a valid Washington State credential prior to employment in the position requires the employee to be registered certified or licensed under Washington State law of administrative rule for any service the agency intends to provide.

8.1 Qualifications

To be a qualified employment and day services provider, an agency must:

1. Develop and implement a plan for each client based on their individual needs. The plan must include all information required by the Criteria for Evaluation.
2. Provide services in accordance with the County Guide to Achieve DDA Guiding Values.
3. Develop and implement internal control policies.
4. Develop and implement an employee training plan for all applicable service categories approved by the county.
5. Manage public funds in compliance with Generally Accepted Accounting Principles (GAAP).

6. Submit Certified Public Accountant reviewed or audited financial statements and federal audits according to the DSHS General terms and Conditions. Refer to Criteria for Evaluation for more information.
7. Maintain a management system that provides for systematic filing, and retention of timely records and reports related to:
    a. Clients
    b. Staff
    c. The agency's tax status; and
    d. The agency's structure, capabilities, and performance as described in the Criteria for Evaluation.

8. Develop a plan to address potential conflicts of interest including, but not limited to, if the agency or an agency employee is also the client's:
    a. Guardian or legal representative
    b. Residential provider
    c. Family member or decision maker

9. Develop a plan to address potential conflicts of interest if the county and service provider are the same.
10. Develop a performance plan that describes objectives, expected outcomes, and how and when objectives will be accomplished. The performance plan must include performance indicators that address diversity, equity and inclusion efforts.

The SLA ensures the establishment and maintenance of qualification standards for personnel necessary to carry out Part C of IDEA.

Personnel shall be appropriately and adequately training, including the use of paraprofessionals and assistance who are appropriately trained and supervised in accordance with state law, regulations, or written policy, to assist in the provision of EIS to infants and toddlers with disabilities and their families.

The personnel qualification standards are consistent with any state approved or recognized certification, licensing, registration, or other comparable requirements that apply to the profession, discipline, or area in which the individual is conducting evaluations, assessment or providing EIS.

An adopted policy should be in place that includes making good-faith efforts to recruit and hire appropriately and adequately training personnel to provider EIS to infants and toddlers with disabilities and their families.

Consult with the Washington Department of Health and OSPI for the most current licensure and/or certification requirements.

8.2 Staff Qualifications and Training

All employees must:

1. Be age 18 or older;
2. Clear a criminal history background check under chapter 388-825 WAC; and
3. Complete training on the following:

a. **Before working unsupervised with any clients:**
    i. Client confidentiality;
    ii. Current work and support plans for each client with whom the employee works;
    iii. DDA Policy 5.06, Client Rights
    iv. DDA Policy 6.08, Incident Management and Reporting Requirements for County and County-Contracted Providers;
    v. First Aid, Blood Borne Pathogens, and CPR (current);
b. **Within one month of employment**
    i. DDA Policy 5.13 Protection from Abuse: Mandatory Reporting
    ii. DDA Policy 5.17 Physical Intervention Techniques
    iii. DDA Policy 5.19 Positive Behavior Support for Children and Youth
    iv. DDA Policy 5.20, Restrictive Procedures and Physical Interventions with Children and Youth
    v. DDA Policy 5.23 Functional Assessments and Positive Behavior Support Plans: Employment and Day Program Services
c. DDA Policies listed in section C must be reviewed at least annually and when updated.

Documentation of staff orientation and training including all training requirements outlined in Policy 6.13 must be documented in the personnel file. The Contractor should maintain an up-to-date record of training for all employees. 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.

Policy and procedure manuals providing sufficient guidance when, and if, staffing changes or absences occur are present and readily available.

To be a qualified provider of Child Development services, an agency employee must have a valid Washington State credential prior to employment if the position requires the employee to be registered, certified, or licensed under Washington state law or administrative rule for any service the agency intends to provide.

8.3 Training Reimbursement

All training reimbursement is at the discretion of the County and is dependent upon funding availability. In accordance with annual budget changes, County may give each agency a flat amount if County finds this more equitable for all contracted providers.

Requests for training reimbursement related to County-recommended trainings or other trainings designed to improve the quality of services to individuals, may be made in writing to the County at least ten (10) business days prior to the training event. Requests should clearly outline the training requested, dates of training and travel, and the number of staff attending. Mileage, food purchases, and lodging may not exceed the Federal per diem/rate allowance. Reimbursement for training requests will require back-up documentation and receipts.

9.0 OUTCOMES

The Contractor will track and make measurable progress related to the key quality indicators as outlined below:

10.0 MONITORING & EVALUATION

The County will develop a contract monitoring and evaluation system incorporating the most recent Criteria for Evaluation System provided by DDA, which may be found on the DSHS/DDA website listed below:
https://www.dshs.wa.gov/dda/county-best-practices

ESIT Monitoring and Enforcement Procedures can be found at: Policies and Procedures (wa.gov)

The County shall conduct at least one on-site audit to each Contractor during each State DSHS/DDA biennium and will prepare a contract compliance report to respond to strengths and potential need for corrective action.

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.

The Contractor must also have documentation that they are able to account for and manage public funds in compliance with Generally Accepted Accounting Principles (GAAP).

10.2 Corrective Action

If agency in out of compliance with their contract, the agency must correct each issue by a date agreed upon by both parties.

If an agency fails to correct identified issues, or is out of compliance with their contract or subcontract, DDA or the county may:

1. Switch the agency to a provisional contract; or
2. Terminate the agency's contract.

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 the amount due to the County.

12.0 NO ACTIVE DEBARMENT

Agency must have no active debarment certification.

COUNTY IMPLEMENTATION GUIDE, Attachment A
INCIDENT REPORTING TIMELINES

One Hour Protocol Phone call to regional office within one hour followed by written notification within one business day	**One Day Protocol** Written notification within one business day
1. **Alleged or suspected sexual abuse of a client.** 2. **Missing client** 3. **Choking – Client chokes on food, liquid, or object during county or county contracted services** and required intervention regardless of outcome. Refer to your CPR and first aid training. 4. **Client arrested** 5. **Death of a client during county or county-contracted services** 6. **Injuries requiring hospital admission** **7. Life threatening, medically emergent condition** 8. **Natural disaster or** environmental condition threatening client safety or program operation 9. **Suicide** 10. **Suicide Attempt**	1. **Alleged or suspected abuse, improper use of restraint, neglect, self-neglect, personal or financial exploitation, or abandonment of a client** 2. **Alleged or suspected criminal activity by a client** 3. **Alleged or suspected criminal activity perpetrated against a client** 4. **Awareness that a client or the client's legal representative is contemplating permanent sterilization procedures** 5. **Client to client abuse** 6. **Hospital or nursing facility admission** 7. **Injuries to a client:** resulting from the use of restrictive procedures or physical intervention techniques; when there is reason to suspect abuse or neglect; that are serious and require professional medical attention; or that are of an unknown origin and cause suspicion of abuse or neglect 8. **Medication or nurse delegation errors** 9. **Mental health crisis** resulting in inpatient admission to a state or local community hospital or psychiatric hospital or evaluation and treatment center. 10. **Property Damage** of $250 or more 11. **Restrictive Procedure** implemented under emergency guidelines 12. **Serious treatment or court order violations**

COUNTY IMPLEMENTATION GUIDE ATTACHMENT B
CHAPTER 6 DDA Policy 6.08

Incident Management and Reporting Requirements for County and County-Contracted Provider

This policy establishes uniform reporting requirements and procedures for county and county contracted providers regarding incidents that involve clients enrolled with the Developmental Disabilities Administration (DDA). This policy also addresses reporting allegations of suspected abuse, improper use of restraint, neglect, self-neglect, personal or financial exploitation, abandonment, and mistreatment.

Clients must be treated with kindness, respect, care, and consideration at all times. Abandonment, abuse, neglect, improper use of restraint, personal and financial exploitation are not permitted under any circumstances.

I have read DDA Policy 6.08, Incident Management and reporting Requirements for County and County-Contracted, in its entirety and understand:

- ☐ The definitions found in Attachment A of Policy 6.08;
- ☐ My legal requirement as a mandatory reporter to report abuse, improper use of restraint, neglect, personal or financial exploitation, or abandonment of a client;
- ☐ How to report abuse, improper use of restraint, neglect, personal or financial exploitation, or abandonment of a client, including incident reporting procedures;
- ☐ Failure to report can result in disciplinary action and may result in termination of the provider's contract. Furthermore, failure to report is a gross misdemeanor under RCW 74.34.053. Any provider employee, contractor, or volunteer found to have knowingly failed to fulfill their mandatory reporting obligation will be reported to the appropriate law enforcement agency and may be prosecuted.; and
- ☐ My responsibilities to protect clients and other vulnerable adults and children from abuse, improper use of restraint, neglect, personal or financial exploitation, or abandonment.

I also acknowledge that I have had an opportunity to ask questions of my supervisor regarding this policy and have had those questions answered.

_____	_____	
PRINT EMPLOYEE LEGAL NAME	EMPLOYEE SIGNATURE	DATE
_____	_____	
PRINT WITNESS LEGAL NAME	WITNESS SIGNATURE	DATE

COUNTY IMPLEMENTATION GUIDE ATTACHMENT C
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

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

3. (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. 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.

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.

Physically Secure the portable device(s) and/or media by

a. Keeping them in locked storage when not in use

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

c. Taking frequent inventories

2. When being transported outside of a Secured Area, portable devices and media with DSHS Confidential Information must be under the physical control of Contractor staff with authorization to access the Data.

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 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 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. 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.

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. Dat

8. Data Disposition. When the contracted work has been completed or when the Data is no longer needed, except as noted above in 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 course 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.