INTERAGENCY AGREEMENT
BETWEEN
DEPARTMENT OF CHILDREN, YOUTH, AND FAMILIES
AND
WASHINGTON STATE OFFICE OF CIVIL LEGAL AID

THIS **INTERAGENCY AGREEMENT (IAA)** is made and entered into between the Department of Children, Youth, and Families (DCYF) and the Office of Civil Legal Aid (OCLA).

I. Purpose

The purpose of this IAA is to establish the basis of a relationship between the Department of Children, Youth, and Families and the Office of Civil Legal Aid whereby OCLA may receive partial reimbursement for payment for services incurred by OCLA for the legal representation of DCYF Client children who remain in foster care six (6) months following the termination of their parents' legal rights.

II. Background

The Office of Civil Legal Aid (OCLA) manages the Children's Representation Program (CRP), which provides legal representation to children who remain in foster care six (6) months following the termination of their parents' legal rights. The program is set forth in RCW 13.34.100(6)(c)(i) and (ii), which provide in relevant part that the court must appoint an attorney for a child in a dependency proceeding six months after granting a petition to terminate the parent and child relationship and when there is no remaining parent with parental rights. When an attorney is appointed under this authority, the state must pay the costs of legal services if those services are in accordance with the standards of practice, voluntary training, and caseload limits developed and recommended by the children's representation work group pursuant to section 5, chapter 180, Laws of 2010. Under RCW 2.53.145, OCLA is responsible for contracting with attorneys or agencies that provide legal representation to children under this authority. Title IV-E reimbursement of expenses for legal representation for children in these dependency cases shall be in accordance with the Children's Bureau Child Welfare Policy Manual's stated objectives of ensuring reasonable efforts to prevent removal, finalizing children's permanency plans, ensuring that parents and youth are engaged in and complying with case plans, and the Manual's requirement that attorneys for children's representation be independent of and not overseen by the IV-E agency. As a matter of constitutional separation of powers, responsibility to regulate the practice of law is assigned to the judicial branch and operationalized through rules adopted by the Washington Supreme Court. The duties owed by attorneys representing children in dependency cases are governed by the Washington Supreme Court's Rules of Professional Conduct.

III. Definitions

A. "Case" means a dependency proceeding brought under ch. 13.34 RCW in which a client is represented by an attorney and also means any substantially associated court or administrative proceeding(s) in which Attorney's client is a party, including but not limited to guardianships, reinstatement proceedings, authorized family law proceedings that finalize the child's permanent plan.

B. "Children's Representation Program Manager" means the employee assigned by OCLA to manage and oversee the Children's Representation Program.

C. "Confidential Information" or "Data" means information that is exempt from disclosure to the public or other unauthorized persons under RCW 42.56 or other federal or state laws. Confidential Information includes, but is not limited to, Personal Information.

D. "Legally Free Child or Children" means a child/ren who remain(s) dependent six months following termination of legal rights as to all persons with parental rights to that child/ren.

E. "Personal Information" means information identifiable to any person, including, but not limited to, information that relates to a person's name, health, finances, education, business, use or receipt of governmental services or other activities, addresses, telephone numbers, Social Security Numbers, driver license numbers, other identifying numbers, and any financial identifiers.

IV. Data Security Requirements – Exhibit A.

OCLA shall protect, segregate, and dispose of DCYF data as described in Exhibit A.

V. Assignment

The OCLA shall not assign its rights and responsibilities under this Agreement to a third party without the prior written consent of DCYF. Nothing in this Agreement shall limit the role of OCLA in contracting for the services of attorneys for children as provided by law.

VI. Audit

A. If OCLA is required to have an audit or if an audit is performed, OCLA shall forward a copy of the audit report to DCYF.

B. If federal or state audit exceptions are made relating to this agreement, OCLA must reimburse the amount of the audit exception, and any other costs including, but not limited to, audit fees, court costs, and penalty assessments.

C. OCLA shall be financially responsible for any overpayments by DCYF associated with activities undertaken by attorneys and agencies with which OCLA contracts. OCLA shall be financially responsible for any audit disallowances resulting from a federal or state audit which resulted from an action, omission or failure to act on the part of the attorneys and agencies with which OCLA contracts for representation of legally free children.

D. OCLA shall require the attorneys and agencies providing legal representation to retain administrative records, such as fiscal records that shall substantiate costs invoiced to DCYF under this Agreement.

VII. Confidentiality

DCYF and OCLA agree that confidential information will be kept confidential on all data and communications systems and will be treated confidentially in accordance with applicable state and federal law, including Title IV-E confidentiality requirements, and DCYF data requirements as described in Exhibit A.

VIII. Disputes

A. Both DCYF and OCLA agree to work in good faith to resolve all conflicts at the lowest level possible. However, if unable to promptly and efficiently resolve, through direct informal contact, any dispute concerning the interpretation, application, or implementation of any section of this Agreement, either party may reduce its description of the dispute in writing, and deliver it to the other Party for consideration. Once received, the assigned managers or designees of each Party will work to informally and amicably resolve the issue within five (5) business days. If managers or designees are unable to come to a mutually acceptable decision within five (5) business days, they may agree to issue an extension to allow for more time.

B. If the dispute cannot be resolved by the managers or designees, the issue will be referred through each Agency's respective operational protocols, to the Secretary of DCYF ("Secretary") and OCLA's designated delegate(s). Both Parties will be responsible for submitting all relevant documentation, along with a short statement as to how they believe the dispute should be settled, to the Secretary and OCLA's designated delegate(s).

C. Upon receipt of the referral and relevant documentation, the Secretary and OCLA's designated delegate(s) will confer to consider the potential options of resolution, and to arrive at a decision within fifteen (15) business days. The Secretary and OCLA's designated delegate(s) may appoint a review team, a facilitator, or both, to assist in the resolution of the dispute. If the Secretary and OCLA are unable to come to a mutually acceptable decision within fifteen (15) business days, they may agree to issue an extension to allow for more time.

D. If the Secretary and OCLA are unable to come to a mutually acceptable decision after following the above procedures, the final decision shall be determined by a Dispute Board. Each Party to this Agreement shall appoint one member to the Dispute Board. The members so appointed shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall review the facts, Agreement terms, and applicable

statutes and rules and make a determination of the dispute. Participation in the dispute process shall precede any judicial or quasi-judicial action and shall be the final administrative remedy available to the Parties.

IX. Insurance

The parties certify that they are self-insured under the State's self-insurance liability program, as provided by RCW 4.92.130, and shall pay for losses for which it is found liable.

X. Provision of Legal Representation

A. OCLA's CRP underwrites and oversees the delivery of high quality, standards-based legal representation to children who are entitled to representation pursuant to RCW 13.34.100 (6).

B. OCLA will contract with individual attorneys and agencies to provide legal presentation under a case-by-case or % FTE basis.

C. Attorneys with limited numbers of cases are paid on a case-by-case basis at $75 per hour up to $1500 per case per year in the instance of an individual child and, as required by RCW 13.34.100(6)(c)(ii), up to $750 per year in the instance of second and subsequent siblings.

D. The contracted rate of pay for a full time contract attorney (100% FTE) carrying 80 cases is $120,000 per year.

E. Attorneys contracted on a %FTE basis are required to provide a list of cases (using non-identifying case numbers) with their invoices, showing the date they were appointed to the case, whether the case is still open and whether the child is in a group care setting.

F. For attorneys contracted on a case-by-case basis, each case is individually tracked to ensure billings do not exceed the contracted maximum amount per case.

G. Consistent with caseload standards referenced in statute, attorneys are limited to a caseload of no more than 80 cases total in their practice, even when child representation occupies only a portion of their practice.

H. OCLA will contract with qualified third-party training providers to deliver high quality training for CRP attorneys that focus on skills and substantive areas relevant to child welfare practice, to include mandatory training under the Quality Improvement Center on the Representation of Children in the Child Welfare System (QIC-ChildRep) model.

I. CRP attorneys will advocate for the legal and stated interests of their clients.

J. In addition to direct attorney-client communication and in-court representation, standards-based representation requires:

1. Attorneys to observe their clients in placement settings;

2. Attorneys to regularly communicate with collateral contacts such as:

a) Teachers;

       b) Foster Parents; and

       c) Service Providers.

    3. Attorneys to visit their clients at their placement regardless of where they are placed.

K. CRP attorneys are required to enter their time and case activity into the online Case Activity Reporting and Oversight System (CAROS).

XI.   Operating Budget and Reimbursement

DCYF will reimburse OCLA for OCLA's Title IV-E allowable expenses for legal representation of children in dependency cases and appeals. Allowable expenditures will be determined by applying the combined foster care/relative care penetration rate averaged for the quarter to the allowable costs for the child representation program. The combined foster care/relative care penetration rate is the rate derived by dividing the number of Title IV-E eligible children in out-of-home care by the total number of children in out of home care. OCLA expenditures shall be submitted and reimbursed as indicated below. OCLA shall not submit a request for reimbursement, and DCYF shall not pay for, services performed under this IAA if OCLA has charged or will charge another agency of the state of Washington or any other party for the same services.

Child Dependency Representation FY20	
Salaries & Benefits	$179,771.00
Office Supplies	$500.00
Communications	$3,500.00
Staff Development	$1,500.00
Subscriptions	$50.00
Rental & Leases	$4,000.00
Attorney Services	$1,344,000.00
Training	$30,000.00
Staff Travel	$7,500.00
Contractor Travel	$17,500.00
Indirect @ 10%	$21,432.10
Totals	$1,609,753.10

XII.   Governance

A. In the event of an inconsistency in the terms of this IAA, or between its terms and any applicable statute or rule, the inconsistency shall be resolved by giving precedence in the following order:

1. Applicable state and federal statutes and rules;

2. Terms and Conditions contained in this IAA and any and all Exhibits or Attachments;

3. Any other provisions of this IAA incorporated by reference or otherwise.

B. A failure by either party to exercise its rights under this IAA shall not preclude that party from subsequent exercise of such rights and shall not constitute a waiver of any other rights under this IAA unless stated to be such in a writing signed by an authorized representative of the party and attached to the original IAA.

XIII. Term of Agreement

This IAA becomes effective July 1, 2019 and shall remain in effect until June 30, 2020, unless terminated.

XIV. Termination

This IAA may be terminated by either party with a minimum of thirty (30) days advanced notice.
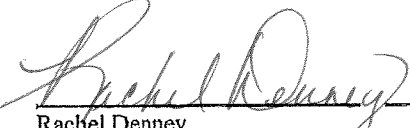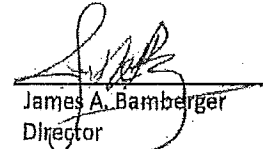
XV. Termination Due to Change in Funding

If the funds DCYF relied upon to establish this Agreement are withdrawn, reduced or limited, or if additional or modified conditions are placed on such funding, DCYF may immediately terminate this Agreement by providing written notice to the attorneys and agencies providing representation under this Agreement. The termination shall be effective on the date specified in the termination notice.
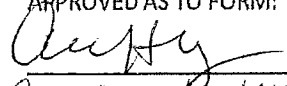
XVI. Amendments

This IAA may be amended by mutual agreement of the parties. Such amendments shall not be binding unless they are in writing and signed by personnel authorized to bind each of the parties.

XVII. Signatures

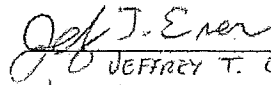In witness whereof, the parties have executed this IAA:

Rachel Denney,
DCYF HQ Contract Manager   Date

July 17, 2019

James A. Bamberger
Director   Date

APPROVED AS TO FORM:

Carrie Hoanleayno
AAG   Date

APPROVED AS TO FORM:

JEFFREY T. EVEN
July 17, 2019   Date

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 DCYF Confidential Information, and who has or have been authorized to do so.

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

   d. "Category 4 Data" is data that is confidential and requires special handling due to statutes or regulations that require especially strict protection of the data and from which especially serious consequences may arise in the event of any compromise of such data. Data classified as Category 4 includes but is not limited to data protected by: the Health Insurance Portability and Accountability Act (HIPAA), Pub. L. 104-191 as amended by the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH), 45 CFR Parts 160 and 164; the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. §1232g; 34 CFR Part 99; Internal Revenue Service Publication 1075 (https://www.irs.gov/pub/irs-pdf/p1075.pdf); Substance Abuse and Mental Health Services Administration regulations on Confidentiality of Alcohol and Drug Abuse Patient Records, 42 CFR Part 2; and/or Criminal Justice Information Services, 28 CFR Part 20. "Data" used without modification refers to Category 4 Data.

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

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

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

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

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

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

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

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

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

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

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

2. **Authority.** The security requirements described in this document reflect the applicable requirements of Standard 141.10 (https://ocio.wa.gov/policies) of the Office of the Chief Information Officer for the state of Washington, and of the DCYF Information Security Policy

and Standards Manual. Reference material related to these requirements can be found here: https://www.dcyf.wa.gov/services/child-welfare-providers which is a site developed by the DSHS Information Security Office and hosted by DCYF.

3. **Administrative Controls.** The attorneys and agencies that provide legal representation 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 staff for violating that policy.

    b. Security awareness training for all employees, presented at least annually, which informs staff of their responsibilities under the attorneys and agencies that provide legal representation's security policy. If the attorneys and agencies do not have an appropriate security awareness course, any of their staff who will work with the Data or systems housing the Data, must successfully complete the DSHS Information Security Awareness Training, which can be taken on this web page: https://www.dshs.wa.gov/fsa/central-contract-services/it-security-awareness-training, or a replacement later identified by DCYF.

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

    d. If Confidential Information shared under this agreement is classified as Category 4, the attorneys and agencies that provide legal representation 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 attorneys and agencies that provide legal representation 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 agreement 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 agreement.

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

g. When accessing the Data from within the attorneys and agencies that provide legal representation's network (the Data stays within the attorneys and agencies' network at all times), enforce password and logon requirements for users within the attorneys and agencies' 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 attorneys and agencies' network), mitigate risk and enforce password and logon requirements for users by employing measures including:

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

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

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

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

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

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

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

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

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

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

j. If the agreement 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 attorneys and agencies that provide legal representation agree 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 DCYF 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 DCYF on optical discs which will be used in local workstation optical disc drives and which will not be transported out of a Secure Area. When not in use for the agreed upon purpose, such discs must be Stored in a Secure Area. Workstations which access DCYF Data on optical discs must be located in an area which is accessible only to authorized personnel, with access controlled through use of a key, card key, combination lock, or comparable mechanism.

d. **Optical discs (CDs or DVDs) in drives or jukeboxes attached to servers.** Data provided by DCYF on optical discs which will be attached to network servers and which will not be transported out of a Secure Area. Access to Data on these discs will be restricted to Authorized Users through the use of access control lists which will grant access only after the Authorized User has authenticated to the network using a Unique User ID and Hardened

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

e. **Paper documents.** 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 DCYF staff who will issue authentication credentials (e.g. a Unique User ID and Hardened Password) to Authorized Users on staff of the attorneys and agencies that provide legal representation. Those attorneys and agencies will notify DCYF staff immediately whenever an Authorized User in possession of such credentials is terminated or otherwise leaves the employ of the attorneys and agencies that provide legal representation and whenever an Authorized User's duties change such that the Authorized User no longer requires access to perform work for this Agreement.

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

    (1) Except where otherwise specified herein, DCYF Data shall not be stored by the attorneys and agencies that provide legal representation on portable devices or media unless specifically authorized within the terms and conditions of the Agreement. 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 DCYF Confidential Information must be under the physical control of the staff of the attorneys and agencies that provide legal representation with authorization to access the Data, even if the Data is encrypted.

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

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

i. **Cloud storage.** DCYF Confidential Information requires protections equal to or greater than those specified elsewhere within this exhibit. Cloud storage of Data is problematic as neither DCYF nor the attorneys and agencies that provide legal representation has control of the environment in which the Data is stored. For this reason:

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

(a) Attorneys and agencies that provide legal representation has written procedures in place governing use of the Cloud storage and attorneys and agencies that provide legal representation attests in writing that all such procedures will be uniformly followed.

(b) The Data will be Encrypted while within the attorneys and agencies that provide legal representation's 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 attorneys and agencies that provide legal representation will possess a decryption key for the Data, and the decryption key will be possessed only by the attorneys and agencies that provide legal representation and/or DCYF.

(f) The Data will not be downloaded to non-authorized systems, meaning systems that are not on either the DCYF or attorneys and agencies that provide legal representation's networks.

(g) The Data will not be decrypted until downloaded onto a computer within the control of an Authorized User and within either the DCYF or attorneys and agencies that provide legal representation's network.

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

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

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

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

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

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

b. The attorneys and agencies that provide legal representation will have a method of ensuring that the requisite patches and hotfixes have been applied within the required timeframes.

c. Systems containing DCYF 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. DCYF Data must be segregated or otherwise distinguishable from non-DCYF data. This is to ensure that when no longer needed by the attorneys and agencies that provide legal representation, all DCYF Data can be identified for return or destruction. It also aids in determining whether DCYF 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) DCYF Data will be kept on media (e.g. hard disk, optical disc, tape, etc.) which will contain no non-DCYF Data. And/or,

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

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

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

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

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

8. **Data Disposition.** When the agreed work has been completed or when the Data is no longer needed, except as noted above in Section 5.b, Data shall be returned to DCYF 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 agreement with the recycler assures that the confidentiality of Data will be protected.
Paper documents containing Confidential Information requiring special handling (e.g. protected health information)	On-site shredding, pulping, or incineration
Optical discs (e.g. CDs or DVDs)	Incineration, shredding, or completely defacing the readable surface with a coarse abrasive
Magnetic tape	Degaussing, incinerating or crosscut shredding

9. **Notification of Compromise or Potential Compromise.** The compromise or potential compromise of DCYF shared Data must be reported to the DCYF Contact designated in the Agreement within one (1) business day of discovery. If no DCYF Contact is designated in the Agreement, then the notification must be reported to the DCYF Privacy Officer at: dcyfprivacyofficer@dcyf.wa.gov. Attorneys and agencies that provide legal representation must also take actions to mitigate the risk of loss and comply with any notification or other requirements imposed by law or DCYF.

10. **Data shared with attorneys and agencies that provide legal representation.** If DCYF Data provided under this Agreement is to be shared with attorneys and agencies that provide legal representation, the Agreement with the attorneys and agencies that provide legal representation must include all of the data security provisions within this Agreement and within any amendments, attachments, or exhibits within this Agreement. If the attorneys and agencies that provide legal representation cannot protect the Data as articulated within this Agreement, then the agreements with other attorneys and agencies that provide legal representation must be submitted to the DCYF Contact specified for this Agreement for review and approval.