

<p align="center"><b>“Cross the Board” Contract Revision</b></p>	<p align="center"><b>Reason for Revision</b></p>
<p><b>Budget Exhibit – Exhibit __.</b> Contractor’s Budget for providing services under this Contract is attached as Exhibit __. Funds may be transferred between budget line items of the Contractor’s Budget subject to the following conditions:</p> <p>a. Transfer of funds up to 10% of the budget line item must be requested in writing by the Contractor and may be made without amending this Contract;</p> <p>b. Transfer of funds that exceeds 10% of the budget line item shall require a written amendment to this Contract prior to the transfer of funds between budget line items.</p>	<p>Allows Contractor’s some flexibility within approved budget maximum; reduces CA workload by eliminating need for amendment of small transfers between line items.</p>
<p><b>Transportation clause –</b> Revision to subsection “g” to clarify necessity of appropriate insurance and addition of new subsection h. to allow DSHS discretion in disallowing someone from transporting clients.</p> <p><b>g. The Contractor shall ensure that no transportation of DSHS clients occurs unless an auto insurance policy that covers the transportation of DSHS clients is in effect</b></p> <p><b>h. DSHS shall have discretion to disallow any employee, subcontractor, or volunteer of the Contractor from providing transportation to DSHS clients.</b></p>	<p>Current subsection g. could be construed that the Contractor is not responsible for auto coverage if services are subcontracted out.</p> <p>Current clause does not address situations where the background check is approved to allow unsupervised access to CA clients, but the driving record is such that CA does not wish to allow the applicant to transport clients.</p>
<p><b>Electronic submission of written reports by encrypted email</b></p> <p><b>Reports -</b> Add a new subsection to boilerplate section, <i>Reports</i>, in Program Requirements Exhibit</p> <p>b. Written reports must be submitted by secure email to the DSHS contact identified on page one of this document. The DSHS Secure E-mail User Guide is available at <a href="http://www.dshs.wa.gov/ca/partners/intro.asp">http://www.dshs.wa.gov/ca/partners/intro.asp</a>.</p>	<p>This is a requirement of CA’s Policy/Workload Reduction Implementation plan. Electronic Reporting provisions have already been created and inserted into templates 2042 and 2358, effective 10/1/12; needs to be in the other templates.</p>
<p><b>Secure Management of Confidential Information</b></p> <p><b>See attachment</b></p>	<p>In response to Contractors’ requests to electronically store data.</p> <p>Also, to meet DSHS/Information Support System Division’s security concerns and to address DSHS/ Operations Review &amp; Consultation’s audit recommendations.</p>

## Revisions related to secure management of confidential information

2. **Definitions Specific to Special Terms.** The words and phrases listed below, as used in this Contract, shall each have the following definitions: **We will add the following definitions to our standard list:**

- a. "Authorized User(s)" means an individual or individuals with an authorized business requirement to access DSHS Confidential Information.
- b. "Hardened Password" means 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.
- b. "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.

3. **Purpose.** The purpose of this Contract is to:

4. **Data Security Requirements – Exhibit A.** The Contractor shall protect, segregate, and dispose of data from Children's Administration as described in Exhibit A, as required in Section 7 **Secure Management of Confidential Information.**

5. **Statement of Work – Exhibit B.** The Contractor shall provide services and staff as described in the Statement of Work attached as Exhibit B.

6. **Program Requirements – Exhibit C.** The Contractor shall comply with all program and other requirements for providing services under this Contract, as stated in the Program Requirements attached as Exhibit C.

7. **Budget Exhibit – Exhibit D.** Contractor's Budget for providing services under this Contract is attached as Exhibit D.

## 8. **Secure Management of Confidential Information**

The Contractor shall ensure that all **Confidential Information** (also referred to as **Personal Information**) as defined in the General Terms and Conditions Section 1, acquired under this contract is used only for the provision of services under this contract and is handled with the utmost confidentiality as described in the General Terms and Conditions, Section 6, *Confidentiality*. In addition:

- a. Sole Proprietor Contractors shall ensure that mobile devices and data are accessed, and protected as described in the Special Terms and Condition Section below entitled **Data Security – Sole Proprietors.**
- b. All other Contractors shall ensure that mobile devices and data are accessed and protected as described in **Exhibit A- Data Security Requirements.**
- c. **Failure to comply with applicable requirements may result in termination of this contract.**

9. **Consideration**
10. **Billing and Payment**
11. **Services Authorized as Needed**
12. **Payment Only for Authorized Services**
13. **Funding Stipulations**
14. **Recovery of Fees for Noncompliance**
15. **Business/Financial Assessment**
16. **Investigations of Contractor or Related Personnel**
17. **Removal of Individuals from Performing Services**
18. **Compliance with Corrective Action Plan**
19. **Insurance**
20. **Resolution of Differences**
21. **Disputes**
22. **Addressing Diversity**
23. **Data Security – Sole Proprietors.** Sole Proprietors shall comply with the following requirements:
  - a. The Contractor shall instruct all staff, subcontractors and volunteers that confidential information may not be shared in any form except to provide services as required under this contract. This restriction applies to voice conversations, data in any electronic format, data in any paper format, and all other forms of communication.
  - b. The Contractor shall ensure that all staff, subcontractors and volunteers understand and agree that:
    - (1) Confidential information in any form must not be left unattended; and
    - (2) Any loss or misplacement of confidential information must be promptly reported to the Contractor, who must report it to DSHS within one day, in accordance with General Terms and Conditions, Section 6.
  - c. **Data Transport.** When transporting DSHS Confidential Information electronically the Data will be encrypted. This includes any transmission of the Data over the Internet in any manner including, but not limited to, email outside of their own network.
  - d. **Protection of Data.** If the Contractor stores DSHS Data on any of the following media, the data will be protected as described. Storage of the data on any other medium is not allowed unless specifically allowed within the Special Terms and Conditions.

- (1) **Hard disk drives, CDs, DVDs, USB Flash (thumb) drives, or any form of portable electronic media.** Data stored on hard disks, CDs, DVDs, or USB flash drives, or any form of portable electronic media must be encrypted and stored in an area or place to which only the Contractor or authorized Contractor staff has access. Only authorized Contractor staff may access the data, and a Unique User ID and Hardened Password, or other authentication mechanism which provides equal or greater security, such as biometrics or smart cards, must be used to control access to the data.

At the end of the contract period, or when no longer needed, the Data must be deleted. The Data must be destroyed in accordance with sub section f. if the hard disk is removed from service.

Any system containing DSHS data, including PCs, laptops, or servers, must:

- (a) Be encrypted
  - (b) Be manually locked to prevent unauthorized access. Such system must be set to lock automatically after no more than 20 minutes of inactivity.
  - (c) Be physically inaccessible to unauthorized individuals.
- (2) **Paper documents.** Any paper records must be protected by storing the records in a Secured Area which is only accessible to authorized personnel. When not in use, such records must be stored in a locked container, such as a file cabinet, locking drawer, or safe, to which only authorized persons have access.
  - (3) **Cloud storage.** DSHS data may not be stored on any medium not controlled by the Contractor. Storage on any Internet service such as DropBox, iCloud, Amazon Web Services, or any other Internet based storage system is not allowed.
  - (4) **Data stored for backup purposes.**
    - (a) DSHS data 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. Such media will be protected as otherwise described in this exhibit. 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 in subsection f. Data Disposition
    - (b) DSHS 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 in subsection f. Data Disposition.

**e. Data Segregation.**

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

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

(3) 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.

f. **Data Disposition.** When the contracted work has been completed or when no longer needed, except as noted in subsections d (1) and d (4) (b) above, Data shall be returned to DSHS or destroyed. Media on which Data may be stored and associated acceptable methods of destruction are as follows:

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

g. **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.

h. **If the Contractor cannot protect the Data as articulated within this Contract, including Data shared with a subcontractor, then the Contractor must immediately contact the DSHS Contact prior to signing this contract.**

### Exhibit A – Data Security Requirements

1. **Definitions.** The words and phrases listed below, as used in this Exhibit, shall each have the following definitions:
  - a. “Authorized User(s)” means an individual or individuals with an authorized business requirement to access DSHS Confidential Information.
  - b. “Hardened Password” means 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.
  - c. “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. **Data Transport.** When transporting DSHS Confidential Information electronically, including via email, the Data will be protected by:
  - a. Transporting the Data within the (State Governmental Network) SGN or Contractor’s internal network, or;
  - b. Encrypting any Data that will be in transit outside the SGN or Contractor’s internal network. This includes transit over the public Internet.
3. **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.** 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.** 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 Secured Area and otherwise meet the requirements listed in the above paragraph. Destruction of the Data as outlined in Section 5. Data Disposition may be deferred until the disks are retired, replaced, or otherwise taken out of the Secured 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 Secured Area. When not in use for the contracted purpose, such discs must be locked in a drawer, cabinet or other container to which only Authorized Users have the key, combination or mechanism required to access the contents of the container. 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 Secured 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 Secured Area which is only accessible to authorized personnel. When not in use, such records must be stored in a locked container, such as a file cabinet, locking drawer, or safe, to which only authorized persons have access.
- 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 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 with a key length of at least 128 bits
    - (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.

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

  - (d) Keeping them in locked storage when not in use
  - (e) Using check-in/check-out procedures when they are shared, and
  - (f) 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.
- (3) Portable devices include, but are not limited to; smart phones, tablets, flash memory devices (e.g. USB flash drives, personal media players), portable hard disks, and laptop/notebook/netbook computers if those computers may be transported outside of a Secured Area.
- (4) Portable media includes, but is not limited to; optical media (e.g. CDs, DVDs), magnetic media (e.g. floppy disks, tape), or flash media (e.g. CompactFlash, SD, MMC).

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

- (1) DSHS data 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 in Section 5. Data Disposition
- (2) DSHS 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 in Section 5. Data Disposition.

**4. Data Segregation.**

- a. DSHS Data must be segregated or otherwise distinguishable from non-DSHS data. This is to ensure that when no longer needed by the Contractor, all DSHS Data can be identified for return or destruction. It also aids in determining whether DSHS Data has or may have been compromised in the event of a security breach. As such, one or more of the following methods will be used for data segregation.
- b. DSHS Data will be kept on media (e.g. hard disk, optical disc, tape, etc.) which will contain no non-DSHS Data. And/or,
- c. DSHS Data will be stored in a logical container on electronic media, such as a partition or folder dedicated to DSHS Data. And/or,
- d. DSHS Data will be stored in a database which will contain no non-DSHS data. And/or,
- e. 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.
- f. When stored as physical paper documents, DSHS Data will be physically segregated from non-DSHS data in a drawer, folder, or other container.
- g. 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.

5. **Data Disposition.** When the contracted work has been completed or when no longer needed, except as noted in 4.b above, Data shall be returned to DSHS or destroyed. Media on which Data may be stored and associated acceptable methods of destruction are as follows:

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

6. **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](mailto: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.

7. **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.