Data Security Requirements

1. **Data Transport.** When transporting DSHS/ADS 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.

2. **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 users by requiring logon to the local workstation using a unique user ID and complex 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 complex 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/ADS confidential data stored on these disks, deleting unneeded data is sufficient as long as the disks remain in a secured area and otherwise meets the requirements listed in the above paragraph. Destruction of the data as outlined in Section 4. Data Disposition may be deferred until the disks are retired, replaced, or otherwise taken out of the secure environment.
   c. **Optical discs (CDs or DVDs) in local workstation optical disc drives.** Data provided by DSHS/ADS 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 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/ADS 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/ADS 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 complex 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 locked container, such as a file cabinet, locking drawer, or safe, to which only authorized persons have access.

f. **Access via remote terminal/workstation over the State Governmental Network (SGN).** Data accessed and used interactively over the SGN. Access to the data will be controlled by DSHS/ADS staff who will issue authentication credentials (e.g. a unique user ID and complex password) to authorized contractor staff. Contractor will notify DSHS/ADS staff immediately whenever an authorized person in possession of such credentials is terminated or otherwise leaves the employ of the contractor, and whenever a user's duties change such that the user no longer requires access to perform work for this contract.

g. **Access via remote terminal/workstation over the Internet through Secure Access Washington.** Data accessed and used interactively over the SGN. Access to the data will be controlled by DSHS/ADS staff who will issue authentication credentials (e.g. a unique user ID and complex password) to authorized contractor staff. Contractor will notify DSHS/ADS staff immediately whenever an authorized person in possession of such credentials is terminated or otherwise leaves the employ of the contractor and whenever a user's duties change such that the user no longer requires access to perform work for this contract.

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

(1) DSHS/ADS data shall not be stored by the Contractor on portable devices or media unless specifically authorized within the Special 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 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 protect 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 secure area, portable devices and media with confidential DSHS/ADS data must be under the physical control of contractor staff with authorization to access the data.

(3) Portable devices include, but are not limited to; handhelds/PDAs, Ultramobile PCs, flash memory devices (e.g. USB flash drives, personal media players), portable hard disks, and laptop/notebook computers if those computers may be transported outside of a secure area.

(4) Portable media includes, but is not limited to; optical media (e.g. CDs, DVDs), magnetic media (e.g. floppy disks, tape, Zip or Jaz disks), or flash media (e.g. CompactFlash, SD, MMC).

3. **Data Segregation.**

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

b. DSHS/ADS data will be kept on media (e.g. hard disk, optical disc, tape, etc.) which will contain no non-DSHS/ADS data. Or,

c. DSHS/ADS data will be stored in a logical container on electronic media, such as a partition or folder dedicated to DSHS/ADS data. Or,

d. DSHS/ADS data will be stored in a database which will contain no non-DSHS/ADS data. Or,

e. DSHS/ADS data will be stored within a database and will be distinguishable from non-DSHS/ADS data by the value of a specific field or fields within database records. Or,

f. When stored as physical paper documents, DSHS/ADS data will be physically segregated from non-DSHS/ADS data in a drawer, folder, or other container.

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

4. **Data Disposition.** When the contracted work has been completed or when no longer needed, except as noted in 2.b, data shall be returned to DSHS/ADS or destroyed in accordance with DSHS/ADS IT Security Policy. 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	Using a “wipe” utility which will overwrite the data at least three (3) times using either random or single character data Degaussing sufficiently to ensure that the data cannot be reconstructed, or Physically destroying the disk
Paper documents with sensitive or confidential data	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
Removable media (e.g. floppies, USB flash drives, portable hard disks, Zip or similar disks)	Using a “wipe” utility which will overwrite the data at least three (3) times using either random or single character data Physically destroying the disk Degaussing magnetic media sufficiently to ensure that the data cannot be reconstructed

5. **Notification of Compromise or Potential Compromise.** The compromise or potential compromise of DSHS/ADS shared data must be reported to the DSHS/ADS Contact designated on the contract within one (1) business day of discovery.

6. **Data shared with Sub-contractors.** If DSHS/ADS data provided under this contract is to be shared with a sub-contractor, the contract with the sub-contractor 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/ADS Contact specified for this contract for review and approval.