SBHO Data Security Checklist

	ITEM	SCORE	COMMENTS
Data Security Requirements – Agency			
1	IS/ IT Disaster Recovery Plan, present and meets requirements of contact. Examples of evidence- Disaster Plan checklist		
2	Electronic data protected by transporting data within contractor's internal network or encrypting any data in transit outside the contractor's internal network. This includes transit over public internet.		
3	Data stored on local workstations hard disks have restricted access to authorized users by requiring unique user IDs and hardened passwords.		
4	Data stored on network servers and made available through shared folders have restricted access to authorized users through access control lists which will grant access only after authorized user has authenticated to the network using a unique user ID and hardened password. Data on disks mounted to such servers must be located in an area which is accessible only to authorized personnel and access controlled with use of a key, card key, combination lock or comparable mechanism.		
5	Paper documents protected by storing records in a secured area only accessible to authorized personal. Such records must be stored in a locked container to which only authorized persons have access. Data stored on optical disks will not be transported out of a secured area and must be kept in secure storage.		

6	Access to State data will be controlled by State staff who will issue authentication credentials. Contractor will notify State staff immediately whenever an authorized user in possession of such credentials is terminated or otherwise leaves the employ of the contractor or the authorized user no longer requires access to perform work for the contractor.		
7	Storage of data on portable media or devices is given special protection, if being transported outside of an secure area, by: (check all that apply) __ Encrypting the data and devices to 128 bits __ Controlling access to devices with a password or stronger authentication methods, forced password changes every 90 days __ Manually locking devices whenever they are left unattended and setting devices to lock automatically after a period of inactivity (maximum period is 20 minutes) __ Physically protect portable devices an media by: keeping them in locked storage when not in use, using check-in procedures, and frequent inventories		
8	Transporting portable devices: Devices and media with State data must be under the physical control of agency staff with authorization to access data.		
9	Portable devices: State data shall not be stored on portable devices or media unless specifically authorized. Portable devices include Handhelds/PDAs, Ultra mobile PCs, Flash memory devices, portable hard disks, and laptop/ notebook computers (if transported outside of secure area).		
10	State data may be stored on portable media as part of a contractor's existing documented backup processes for business continuity or disaster recovery purposes. If backup media retired while still containing State information such media will be destroyed.		
11	State data may be stored on non-portable media as part of a contractor's existing documented backup processes for business continuity or disaster recovery purposes. If backup media retired while still containing State information such media will be destroyed.		
12	State data is segregated or otherwise distinguishable from non-State data. This includes procedures for storage of data on media, in a logical container, within a shared database, and paper documents.		
13	Disposal of media stored on server or workstation hard disks or on removable media: - using a wipe utility - degaussing - physical destruction		

14	Disposal of paper documents with sensitive or confidential information - recycling through a contracting firm - onsite shredding, pulping, or incineration		
15	Disposal of optical discs: -incineration, shredding, defacing readable surface with a coarse abrasive		
16	Disposal of magnetic tape: - degaussing, incinerating, or crosscut shredding		