COMMUNITY AND TECHNICAL COLLEGES
Washington State Board

ABLE-BODIED ADULTS WITHOUT DEPENDENTS NAVIGATION FUNDS

2020-21 GRANT GUIDELINES

Workforce Education Department

Washington State Board for Community and Technical Colleges

PO Box 42495

Olympia, WA 98504

SBCTC.edu

The Washington State Board for Community and Technical Colleges reserves the right to make changes to this document due to, but not limited to, federal, state, or local legislation or policy changes.

Deadlines and Milestones

Milestone	Dates (subject to change)
Applications released	July 23, 2020
Applications due in OGMS	August 20, 2020
Applicants notified of approval status	Prior to October 1, 2020
Grants expected to begin	October 1, 2020

Grant Contacts

Program Administration Questions

Kathi Medcalf
Program Administrator, Workforce Education
kmedcalf@sbctc.edu
360-704-1838

Dylan Jilek
Program Coordinator, Workforce Education
djilek@sbctc.edu
360-704-1021

Policy Oversight Questions

Erin Frasier
Policy Associate, Workforce Education
efrasier@sbctc.edu
360-704-4339

Budget, Invoicing & OBIS Questions

Vacant
Contracts Specialist
360-704-4343

OGMS, OBIS, & Invoicing Questions

Kari Kauffman
Program Assistant
kkauffman@sbctc.edu
360-704-1021

Fiscal Policy Questions

Karl Ludeman
Policy Associate, Fiscal Management
kludeman@sbctce.edu
360-704-4344

Table of Contents

Overview

Federal regulations require Basic Food Assistance recipients identified as Able-Bodied Adults without Dependents (ABAWD) to meet work requirements to remain eligible for benefits.

Beginning April 1, 2020 many counties lost their exemption status. As a result, Washington State is expanding ABAWD services to ensure ABAWDs are supported and connected to activities to meet work requirements. The Basic Food Employment and Training (BFET) program is one of these options, but they can also participate at a Workfare site, complete job search or find employment. To support statewide efforts, the SBCTC negotiated an umbrella contract with DSHS to provide funding for each college to participate in an ABAWD Navigation system.

The ABAWD Navigator Funds provide resources to implement a statewide cohort of ABAWD Navigators located at each community and technical college. This will create a single point of contact for immediate engagement of ABAWDs in activities that meet work requirements to maintain their Basic Food eligibility and are appropriate for the individual. This includes providing intake and assessment and access to open entry activities at community colleges or community-based organizations. ABAWD Navigators will also work to enhance collaborations with community partners and increase resources for colleges to support low-income students.

Applicant Guidelines

Who May Apply

All Washington State Community and Technical Colleges who received ABAWD Navigation Design Funds are eligible for ABAWD Navigation Funds and are encouraged to continue to be a part of this statewide effort to support individuals receiving basic food assistance, enhance college collaboration with community partners and increase resources for colleges to support students.

How Does the Provider Apply

Access the 2020-21 ABAWD Navigation Funds application through the Online Grant Management System (OGMS). -

If you do not have an account, contact your organization's Security Contact for access. If you already have an account, you will need your Security Contact to give your permission to access the grant.

Submit completed applications to SBCTC through OGMS no later than August 20, 2020 at 11:55 p.m. SBCTC staff are available for assistance until 4:00 p.m. on August 20, 2020.

Disclaimer

The SBCTC reserves the right to refrain from granting to any or all applicants. Additionally, SBCTC reserves the right to add additional grant requirements to applicants meeting minimum criteria to receive funds but that are deemed to be higher risk grantees. Additional requirements may include, but are not limited to, additional reporting requirements or additional monitoring to assess the applicant's ability to adhere to grant requirements. Any additional requirements will be outlined for individual applicants prior to applicants accepting any resulting grant funding.

Application Guidelines

The SBCTC will review your application and provide feedback, if changes are required. After your application is approved by SBCTC ABAWD program staff, your ABAWD budget approved by the SBCTC fiscal staff and DSHS, and the state plan is approved by FNS, the SBCTC will approve your application in OGMS.

Assurances

A completed and signed Assurances document must be uploaded to the Attachment section of your grant application in the OGMS. Agreeing to all requirements identified in the Assurances document replaces the need for a grant narrative. Please ensure a thorough review of the listed requirements.

Budget

Funding is being provided for one ABAWD Navigator's salary and benefits, goods and services, travel and associated indirects. The ABAWD Navigator must be funded entirely with ABAWD Grant funds.

Please ensure you have identified how your funds will be expended in the budget in OGMS. Budget revisions can be made during the year. Refer to the 2020-21 ABAWD Navigation Funds Fiscal Guidelines and Grant Terms for the budget revision process.

Narrative

Provide a clear description of how funds will be expended for each budget category. The SBCTC staff will provide a template for budget narratives since the scope of work for these funds is predefined.

Grant and Fiscal Accountability Questions

Fiscal accountability questions are a required part of the SBCTC granting process and must be completed in the OGMS. These answers, along with other factors such as monitoring and audits, will help SBCTC determine the grant and fiscal accountability of each grantee.

Funding

Funding in the amount of $75,000 will be granted to each college that has met the application requirements. Funds will be available October 1, 2020 and must be expended by September 30, 2021. See Fiscal Guidelines for allowable expenditures.

These federal program funds for E&T Programs are contingent upon approval of a State E&T Plan by FNS and the availability of Federal funds.

Scope of Work

The 2020-21 ABAWD Navigation Funds support the ABAWD Navigator’s work in collaborating with SBCTC, their ABAWD Navigation Cohort, and DSHS to continue this new support system beginning October 1, 2020. Navigators will be supporting ABAWDs, enhancing community collaborations and expanding resources. These elements of the position’s scope of work are further outlined below:

ABAWD Support

The ABAWD Navigator will provide the following direct services to ABAWDS to ensure they are supported toward meeting work requirements in a meaningful way for the individual in order to advance career opportunities and maintain basic food assistance:

- Orientation
- SNAP/BFET Eligibility
- Tracking and Reporting of referrals
- Issuance of Support Services
- Work Participation Verification Assistance

- Immediate Engagement in Basic Ed, Voc Ed, or approved activities
- Regular support meetings with ABAWDs

ABAWD Navigators will be contacted directly by ABAWDS after they receive notice from DSHS of their work requirements. ABAWDs may be referred to college or other community partner activities.

Collaboration Enhancement

The ABAWD Navigator will work to increase and enhance collaboration between organizations, businesses and agencies in order to strengthen supports for ABAWDs and the college ability to support all students. Targeted areas for enhanced collaboration include, but are not limited to:

- BFET Providers
- Community Resources
- TANF
- College Student Supports
- Guided Pathways

The ABAWD Navigator will collaborate with SBCTC and other ABAWD Navigators to establish and maintain a record management system (likely Excel Workbooks) to track ABAWD interactions, activities and outcomes and implements local program preparations.

The ABAWD Navigator will collaborate with SBCTC and other ABAWD Navigators to establish and maintain orientation, assessment, and referral procedures and implement local preparations.

Resource Expansion

The ABAWD Navigator will work to increase access to resources for ABAWDs and all students. They will give focus to resource expansion in these critical areas:

- Non-federal resources for all BFET Providers
- Additional Community resources for participants
- Apprenticeship Pathways
- Leveraging College Resources

In addition to focusing locally, Navigators will collaborate with other Navigator cohort members to advance regional and statewide efforts to secure resources with the support of SBCTC.

Placement of administrative oversight of the ABAWD Navigator must be within the BFET program to ensure the ABAWD Navigator is able to work closely with BFET direct services staff.

Trainings, Meetings, and Cohort Activities

ABAWD Navigator participation in the statewide ABAWD Navigator cohort activities is required, including phone and web meetings, training, and regional and statewide efforts to advance support for individuals experiencing food insecurity. The ABAWD Navigator must also meet with community partners to further local efforts to support individuals.

ABAWD Program Compliance

Compliance with Applicable Laws

See grant fiscal guidelines for a list of applicable laws.

ABAWD Policy & Work Registration Guide

In addition to requirements identified in the ABAWD Guidelines and Fiscal Guidelines documents; compliance with all DSHS policies and procedures as outlined in the ABAWD Policy & Work Guide is also required.

ABAWD Local Policy and Procedure Manual

ABAWD Navigators will be responsible in the development and maintenance of a local policy and procedure manual for their job duties and processes to ensure services are maintained and grant requirements are met in the absence of, or change in, staffing. This manual should include policies and procedures for both administrative functions and for student services functions.

Time and Effort

All ABAWD Navigators must be funded in whole with ABAWD Navigation Funds, which are federal funds, and not split the position's time and effort with other funding sources. The college must have up-to-date time and effort records.

Additional time and effort reporting information can be found in these online Time and Effort Guidelines.

Mandatory Training

All ABAWD staff must complete training in the following areas on an annual basis, and verifying documentation of the completions submitted to the SBCTC no later than -30-days after hire and retained at the college:

- Understanding and Abiding by the Civil Rights Act of 1964*
- Abuse Reporting*
- Fraud Reporting*
    i. *Videos are linked in this document. Both Abuse Reporting and Fraud Reporting are addressed in the same video.

Mandatory Reporting

All ABAWD staff are mandatory reporters for welfare fraud and abuse reporting. Any knowledge of welfare fraud must be reported to DSHS by calling 1-800-562-6906. Any knowledge of suspected abuse to children or vulnerable adults must be immediately reported by call 1-800-END-HARM (1-800-363-4276).

Records, Data Security, and Confidentiality

Maintenance of Records

All records and other materials relevant to this grant shall be retained for six (6) years after the grant year ends, or six (6) years after any audit.

Maintaining Confidentiality

Confidential information must not be used, published, transferred, sold or otherwise disclosed.

Notification of Compromise or Potential Compromise

A compromise or potential compromise of confidential information must be reported to the SBCTC within one (1) business day of discovery.

Notice of Non-disclosure

All employees with access to confidential client information must have an up-to-date DSHS Confidential Information, Fraud and Abuse form (DSHS 03-374E – Rev. 11/2014). These forms must be renewed for all employees at the start of each Federal Fiscal Year in October and submitted to SBCTC.

Securing Confidential Information

- Only authorized staff are allowed access to confidential information
- Computers, documents, or other media containing confidential information are secured
- Ensure security of faxed confidential information (confirm #, communicate with recipient, verify receipt)
- Paper documents containing confidential information are transported using a Trusted System
- Electronic confidential information is either encrypted or shared through a Trusted System (refer to the Data Security section for further details)

Appendix A: Data Security Requirements

ABAWD Contract – Attachment A: requirements for SBCTC Subcontractors and Sub grantees

Definitions

The words and phrases listed below, as used in this Exhibit, shall each have the following definitions:

1. "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.

2. "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.

3. "Business Associate Agreement" means an agreement between DSHS and a contractor who is 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.

4. "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; 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.

5. "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 iTunes, Dropbox, Box.com, and many other entities. Enterprise cloud vendors include Microsoft Azure, Amazon Web Services, and Rackspace.

6. "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.

7. "FedRAMP" means the Federal Risk and Authorization Management Program, 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.

8. "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.

9. “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.

10. “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.

11. “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.

12. “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.

13. “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.

14. “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.

15. “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.

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, which is a site developed by the DSHS Information Security Office and hosted by DSHS Central Contracts and Legal Services.

Administrative Controls

The Contractor must have the following controls in place:

1. 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.

2. If the Data shared under this agreement is classified as Category 4, the Contractor must be aware of

and compliant with the applicable legal or regulatory requirements for that Category 4 Data.

3. If Confidential Information shared under this agreement is classified as Category 4, the Contractor must have a documented risk assessment for the system(s) housing the Category 4 Data.

Authorization, Authentication, and Access

In order to ensure that access to the Data is limited to authorized staff, the Contractor must:

1. Have documented policies and procedures governing access to systems with the shared Data.
2. Restrict access through administrative, physical, and technical controls to authorized staff.
3. 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.
4. Ensure that only authorized users are capable of accessing the Data.
5. Ensure that an employee's access to the Data is removed immediately:
    a. Upon suspected compromise of the user credentials.
    b. When their employment, or the contract under which the Data is made available to them, is terminated.
    c. When they no longer need access to the Data to fulfill the requirements of the contract.
6. Have a process to periodically review and verify that only authorized users have access to systems containing DSHS Confidential Information.
7. 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:
    a. 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.
    b. That a password does not contain a user's name, logon ID, or any form of their full name.
    c. 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.
    d. That passwords are significantly different from the previous four passwords. Passwords that increment by simply adding a number are not considered significantly different.
8. 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:
    a. Ensuring mitigations applied to the system don't allow end-user modification.
    b. Not allowing the use of dial-up connections.
    c. Using industry standard protocols and solutions for remote access. Examples would include RADIUS and Citrix.

d. 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.

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

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

9. 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:

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

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

   c. Must not contain a “run” of three or more consecutive numbers (12398, 98743 would not be acceptable)

10. If the contract specifically allows for the storage of Confidential Information on a Mobile Device, passcodes used on the device must:

    a. Be a minimum of six alphanumeric characters.

    b. Contain at least three unique character classes (upper case, lower case, letter, number).

    c. Not contain more than a three consecutive character run. Passcodes consisting of 12345, or abcd12 would not be acceptable.

11. Render the device unusable after a maximum of 10 failed logon attempts.

Protection of Data

The Contractor agrees to store Data on one or more of the following media and protect the Data as described:

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.

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.

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.

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.

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.

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.

Data storage on portable devices or media

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:

1. Encrypt the Data.
2. Control access to devices with a Unique User ID and Hardened Password or stronger authentication method such as a physical token or biometrics.
3. 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.
4. Apply administrative and physical security controls to Portable Devices and Portable Media by:
    a. Keeping them in a Secure Area when not in use,
    b. Using check-in/check-out procedures when they are shared, and
    c. Taking frequent inventories.

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.

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.

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 attests 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 and/or DSHS.

   f. The Data will not be downloaded to non-authorized systems, meaning systems that are not on either the DSHS or Contractor networks.

   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 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.

System Protection

To prevent compromise of systems which contain DSHS Data or through which that Data passes:

1. Systems containing DSHS Data must have all security patches or hotfixes applied within 3 months of being made available.
2. The Contractor will have a method of ensuring that the requisite patches and hotfixes have been applied within the required timeframes.
3. Systems containing DSHS Data shall have an Anti-Malware application, if available, installed.
4. 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.

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. As such, one or more of the following methods will be used for data segregation.

   a. DSHS Data will be kept on media (e.g. hard disk, optical disc, tape, etc.) which will contain no non-DSHS Data. And/or,

   b. DSHS Data will be stored in a logical container on electronic media, such as a partition or folder dedicated to DSHS Data. And/or,

   c. DSHS Data will be stored in a database which will contain no non-DSHS data. And/or,

   d. 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.

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

2. 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.

Data Disposition

When the contracted 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 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, portal 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

Data stored on:	Will be destroyed by:
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

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. Contractor must also take actions to mitigate the risk of loss and comply with any notification or other requirements imposed by law or DSHS.

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.

Washington State Board for Community and Technical Colleges