WORKFIRST STUDENT SUPPORT FUNDS

2021-22 GRANT GUIDELINES

Student Services 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**

<table>
<thead>
<tr>
<th>Milestone</th>
<th>Dates (subject to change)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application available in OGMS</td>
<td>July 26, 2021</td>
</tr>
<tr>
<td>Applications due in OGMS</td>
<td>August 23, 2021</td>
</tr>
<tr>
<td>Grant start date</td>
<td>October 1, 2021</td>
</tr>
</tbody>
</table>

**Grant Contacts**

**Program Administration Questions**

Deana Rader  
Program Administrator, Student Services  
drader@sbctc.edu  
360-704-1837

**Fiscal Policy Questions**

Denise Costello  
Policy Associate, Fiscal Management  
dcostello@sbctc.edu  
360-704-4344

**eJAS Password Resets & Technical Assistance**

Katelynn Orellana  
Integrations Coordinator, Student Services  
korellana@sbctc.edu  
360-704-1027

**Budget, Invoicing, & OBIS Questions**

Dylan Jilek  
Contracts Specialist  
djilek@sbctc.edu  
360-704-4343

**Program Policy Questions**

Jennifer Dellinger  
Policy Associate, Student Services  
jdellinger@sbctc.edu  
360-704-3449

**OGMS, OBIS, & Invoicing Questions**

Kari Kauffman  
Program Assistant  
kkauffman@sbctc.edu  
360-704-1021
# Table of Contents

Deadlines and Milestones ....................................................................................................................... 2
Grant Contacts ......................................................................................................................................... 2
Table of Contents ..................................................................................................................................... 3
Overview ................................................................................................................................................... 5
Application Information ........................................................................................................................... 6
  Who May Apply ..................................................................................................................................... 6
  How Does the Provider Apply ............................................................................................................... 6
  Application Process .............................................................................................................................. 6
Student Support Funding ........................................................................................................................ 7
  Funding Policies ................................................................................................................................... 7
  Redistribution Policy ............................................................................................................................. 7
Student Support Funds for Participants ................................................................................................. 8
WorkFirst Student Eligibility .................................................................................................................... 9
  WorkFirst Student Support Funds Eligibility ...................................................................................... 9
  WorkFirst Policy and Procedure Manual ............................................................................................ 12
  Student Support Funding Documentation and Reporting .................................................................. 12
  Disclaimer ........................................................................................................................................... 13
Compliance with Applicable Laws ......................................................................................................... 13
Confidentiality and Records ................................................................................................................... 13
  Maintaining Confidentiality ................................................................................................................ 13
  Maintenance of Records ...................................................................................................................... 13
  Securing Confidential Information ..................................................................................................... 14
  Notification of Compromise or Potential Compromise ..................................................................... 14
  Fraud Reporting .................................................................................................................................. 14
Appendix A: Data Security Requirements ............................................................................................... 15
  Definitions ........................................................................................................................................... 15
  Authority ............................................................................................................................................ 16
  Administrative Controls ...................................................................................................................... 17
  Authorization, Authentication, and Access .......................................................................................... 17
  Protection of Data .............................................................................................................................. 19
  System Protection ............................................................................................................................... 21
  Data Segregation ............................................................................................................................... 22
Data Disposition ................................................................................................................................. 22
Notification of Compromise or Potential Compromise..................................................................... 23
Data shared with Subcontractors ...................................................................................................... 23
Overview

Washington State began WorkFirst, the state’s Temporary Assistance for Needy Families (TANF) program, in August 1997. The program provides cash grants, medical assistance, welfare-to-work services, and work supports (including subsidized childcare through the Working Connections Child Care program) to eligible TANF families. The goal of WorkFirst is to help TANF families build a pathway that can lead them out of poverty and toward economic security.

With the signing of Engrossed Second Substitute House Bill 3141 on April 1, 2010, Governor Christine Gregoire directed the WorkFirst Subcabinet to “examine how to best meet the challenges for WorkFirst families to obtain employment and achieve family self-sufficiency,” and provide a report and plan to implement evidence-based best practices that are sustainable within a block grant program. The Governor challenged the WorkFirst Subcabinet to think anew and to ‘reboot’ WorkFirst for the 21st century.

The WorkFirst Subcabinet was comprised of the leaders of six state agencies that collaborate to administer the program:

- Department of Commerce (COMMERCE)
- Department of Early Learning (DEL)
- Department of Social and Health Services (DSHS)
- Employment Security Department (ESD)
- Office of Financial Management (OFM)
- State Board for Community and Technical Colleges (SBCTC)

Since this time, there has been an evolution of changes to the WorkFirst Subcabinet. The Subcabinet leadership has transitioned to the Legislative Executive WorkFirst Poverty Reduction Oversight Task Force (LEWPRO). WorkFirst legislation has resulted in the creation of the LEWPRO to help determine program outcomes, accountability measures, and to make program design recommendations to the Governor and Legislature. The WorkFirst Chartbook, compiled by the Office of Financial Management, highlights program outcomes and guides program redesign.

DSHS contracts with the State Board for Community and Technical Colleges to provide services to prepare WorkFirst (TANF) adults for entry into employment. From fiscal year 2002 through fiscal year 2008, the SBCTC subsequently awarded block grants to 34 community and technical colleges to deliver these education and job skills training services. From fiscal year 2009 to the present the SBCTC has administered a WorkFirst Delivery Agreement (WFDA) which continues to incorporate a strong emphasis on local planning and prioritization of services and leveraging resources to create efficiency and meet the needs of the current caseload.

In 2018 through a directive from Governor Inslee, the Poverty Reduction Work Group, (PWRG) was formed. The group was charged with developing a 10-year plan to address poverty and racism in Washington State. To best address the ongoing poverty and inequality in our state, the PWRG membership represented different systems and sectors. Additionally, a Steering Committee was created to lead PWRG work comprised of community voices representing communities in poverty.
The Steering Committee led the PRWG in decision making focused on two key principles:

1) reduce poverty by addressing racism as the epicenter of impoverished communities and
2) incorporate and elevate community voices who experience poverty in decision making and the development of the 10-year plan.

These two groups along with many stakeholders worked together to develop Washington State's 10-year plan now known as Blueprint For A Just and Equitable Future. The plan calls for 8 strategies and 60 recommendations as a guide to addressing poverty and inequality in Washington State.

**Application Information**

**Who May Apply**

Applications for WorkFirst Student Support Funds will be accepted in addition to the 2021-22 WorkFirst Delivery Agreement applications from Washington’s community and technical colleges as defined under RCW 28B.50.030. While the funds for student supports are part of the 2021-22 WorkFirst Delivery Agreement contract the State Board holds with the Department of Social and Health Services (DSHS), the application process will be separate for FY22.

**How Does the Provider Apply**

Access the 2021-22 WorkFirst Student Support Funds Grant Application through the Online Grant Management System (OGMS).

If you do not have an account, contact your organization’s Security Contact for access; you will also need your Security Contact to give you permission for FY22.

Submit completed grant applications for consideration of funding to the SBCTC through OGMS no later than August 23, 2021 at 11:55 p.m. SBCTC staff is available for assistance until 4:00 p.m. on August 23, 2021.

An OGMS user manual can be found in the How To section of OGMS.

**Application Process**

**Student Support Funds Participation Design Requirements**

The development and implementation of effective policies and procedures to capture and report students’ actual hours of participation remains a state and federal requirement. WorkFirst Programs are designed to enhance a student’s ability to meet participation requirements and positively contribute to the WorkFirst partnerships’ statewide participation rate as outlined in the FY22 WorkFirst Delivery Agreement Grant Guidelines.

Student Support Funds are transitional by nature and not an intended to be an ongoing supplement to other funding sources. These funds are not an entitlement and are designed to meet the needs of

---

parents to support ongoing participation and engagement in required WorkFirst activities

Student Support Funds available to the system total $1,100,000 for state fiscal year 2022. Accordingly, grant applications for these funds are capped at $33,300 per college.

**Assurances**

A completed and signed Assurances document must be uploaded to the attachment of your grant application in the OGMS. Ensure a thorough review of the listed requirements as these are necessary to ensure the proper administration of these funds.

**Budget Matrix and Narrative**

Describe the level of funding for each eligible WorkFirst Student Support Funds category in which you intend to expend grant funds. Provide enough detail to give a clear picture of where and how your funds will be used. Budget revisions can be made during the year. Refer to the FY22 WorkFirst Student Support Funds Fiscal Guidelines and Grant Terms for the budget revision process.

Describe the processes and procedures you will use to develop and manage your WorkFirst Student Support Funds grant and the practices you will use to help your students be successful academically and become self-sufficient and resilient. Enough detail should be included to allow a reviewer to be able to understand what you intend to do and how you intend to direct your program during the grant year. It should be a tool you can use as a reference to guide you during the grant year.

**Student Support Funding**

WorkFirst Student Support Funds will not be part of the WorkFirst Funding Formula and not subject to take back, however, the following funding and redistribution policies will apply.

**Funding Policies**

Funds that are not projected to be used must be returned to SBCTC on a quarterly basis for reallocation based on system need. In order to facilitate this:

- SBCTC will conduct funding surveys during the fiscal year as a means to move undedicated funds to those colleges demonstrating need. Grant recipients are required to complete each funding survey by the designated due date and return any unspent funds.

**Redistribution Policy**

Grant recipients are expected to expend their awarded funds by the following timeline and corresponding percentages. Any unspent funds outside of the allowable range will be recalled by SBCTC for distribution to meet system needs.

- Through December - 40% (Additional funds received from funding survey requests will not be taken into consideration when reviewing percent expended.)
- Through March - 65%
- Through June – 100%
Student Support Funds for Participants

These services are transitional by nature and are not an ongoing supplement to the student’s grant. Supports are not an entitlement and must be carefully managed. There is a maximum of $3,000 per student per program year that can be awarded.

Take note of suggested limits for each category. The suggested amounts are the average cost of these supports, however, vendors and other factors may increase or decrease the cost for your area.

Costs per support cannot exceed what would be reasonable and necessary for a non-WorkFirst student. All other sources of payment should be considered first before expending WorkFirst Student Support Funds.

<table>
<thead>
<tr>
<th>College Provided</th>
<th>Description</th>
<th>Suggested Funding Limits Per Student</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tools</td>
<td>WorkFirst can provide assistance tools/kits and supplies required for a student’s program and or activity.</td>
<td>$300 per request</td>
</tr>
<tr>
<td>Clothing</td>
<td>WorkFirst can provide assistance for the cost of required uniforms/specialized clothing, PPE. Also, to include clothing to seek and maintain employment or participate in a work-like activity.</td>
<td>$300 per request for required clothing and $75-$150 for employment clothing</td>
</tr>
<tr>
<td>Transportation</td>
<td>WorkFirst can provide assistance for the cost of a bus pass, van pool, train, ferry, and gas cards to help the student get to and from their required activity. Included in this category is car repair and license and fees, such as vehicle licensing plates/tabs, fees for establishment/reestablishment of driver’s license, emissions testing and title transfer. Repairs must have at minimum two estimates from a licensed automobile mechanic. Estimates must itemize all repairs and costs necessary. Please see the WorkFirst Student Support Fiscal Guidelines for requirements for each.</td>
<td>$200 per program year for licensing and fees, $250-$500 per program year for car repair, $150 per month for transportation</td>
</tr>
<tr>
<td>Testing</td>
<td>WorkFirst can provide assistance for the cost of literacy, aptitude, skills proficiency, credential testing and certifications.</td>
<td>$250-$300 per request</td>
</tr>
<tr>
<td>College Provided</td>
<td>Description</td>
<td>Suggested Funding Limits Per Student</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------</td>
<td>-------------------------------------</td>
</tr>
<tr>
<td><strong>Medical</strong></td>
<td>WorkFirst can provide assistance for the cost of medical exams/services necessary to accept employment or participate in WorkFirst activities that are not covered by Apple Health. May include (but not limited to): doctors’ visits, counseling, and exams. *note that counseling does not count towards the annual limit.</td>
<td>$150 per exam</td>
</tr>
<tr>
<td><strong>Personal Hygiene</strong></td>
<td>WorkFirst can provide assistance for the cost of items reasonably needed by the student to maintain personal appearance and grooming. Such items include: haircuts, soap, shampoo, toothpaste, mouthwash, deodorant, shaving supplies, feminine hygiene products, makeup, laundry supplies, hair color, and cleaning supplies.</td>
<td>$50 per request for haircuts and $100 per request for other items</td>
</tr>
<tr>
<td><strong>Emergency Costs</strong></td>
<td>WorkFirst can provide assistance for the cost of internet services (fees for set up and or maintenance of internet), computer equipment (mouse, cords, USB drives, etc. If no other resources exist computers and laptops may be purchased for the student), and diapers/pull-ups, wipes, creams and ointments for a child to attend daycare so the parent can participate in required activities.</td>
<td>$75 per month/per child, $500 per program year for computer equipment, and $300 per program year for internet services</td>
</tr>
</tbody>
</table>

**WorkFirst Student Eligibility**

A WorkFirst student is a parent who is receiving a Temporary Assistance for Needy Families (TANF) grant from DSHS and has been referred to a college by DSHS for education and training. Students must be open on TANF and currently enrolled in classes.

**WorkFirst Student Support Funds Eligibility**

Review the parent’s Individual Responsibility Plan (IRP) to verify eligibility for WorkFirst (TANF). Current IRP status must be identified in the students’ files.

All Student Support Funds must be awarded through the financial aid system. Colleges will establish Financial Aid Program Codes (FAPC) to uniquely identify those awards funded from the DSHS/WorkFirst program.
The following global item type numbers have been reserved for WorkFirst Student Support funding. Item types with “ND” in the description are placeholders for FA tracking outside student supports – these item types do not disburse to the customer account and are used when the award needs to be reflected on a financial aid award for a student, but the method of payment is not through the Financial Aid office (i.e. AP Check or PCard). This way the award can be reflected on the students Financial Aid award without paying to the student account.

To request these item types be created for your college, please open a Ticket under the following SolarWinds request type: ctcLink Support • Campus Solutions • Student Financials • Item Types.

**NOTE:** For those colleges using Dual Processing, these item types will be used for 21-22 forward only.

<table>
<thead>
<tr>
<th>Item Type Number Reserved</th>
<th>Category</th>
<th>Description</th>
<th>Short Desc</th>
<th>Refund-able Indicator</th>
<th>Account Types</th>
<th>CPL (may vary by local CPL options)</th>
</tr>
</thead>
<tbody>
<tr>
<td>9120000002060</td>
<td>Clothing</td>
<td>WorkFirst Clothing</td>
<td>WkFrstClth</td>
<td>Y</td>
<td>FEE, MIS</td>
<td>FMISCFEE</td>
</tr>
<tr>
<td>9120000002070</td>
<td>Clothing Non Disb</td>
<td>WorkFirst Clothing ND</td>
<td>Wrk1ClthND</td>
<td>N</td>
<td>TUT</td>
<td></td>
</tr>
<tr>
<td>9120000002080</td>
<td>Emergency Costs</td>
<td>WorkFirst Emergency</td>
<td>WkFrstEmrg</td>
<td>Y</td>
<td>FEE</td>
<td>FMISCFEE</td>
</tr>
<tr>
<td>9120000002090</td>
<td>Emergency Costs Non Disb</td>
<td>WorkFirst Emergency ND</td>
<td>W1stEmrgND</td>
<td>N</td>
<td>TUT</td>
<td></td>
</tr>
<tr>
<td>9120000002100</td>
<td>Medical</td>
<td>WorkFirst Medical</td>
<td>WrkFrstMed</td>
<td>Y</td>
<td>FEE</td>
<td>HLTHCARE</td>
</tr>
<tr>
<td>9120000002110</td>
<td>Medical Non Disb</td>
<td>WorkFirst Medical ND</td>
<td>Wk1stMedND</td>
<td>N</td>
<td>TUT</td>
<td></td>
</tr>
<tr>
<td>Code</td>
<td>Description</td>
<td>Category</td>
<td>Code</td>
<td>Type</td>
<td>Code</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------------</td>
<td>------------------------------</td>
<td>----------</td>
<td>----------</td>
<td>----------</td>
<td>-------------------</td>
</tr>
<tr>
<td>912000002120</td>
<td>Personal Hygiene</td>
<td>WorkFirst Personal</td>
<td>Wrk1stPers</td>
<td>Y</td>
<td>FEE</td>
<td>FMISCFEE</td>
</tr>
<tr>
<td>912000002130</td>
<td>Personal Hygiene</td>
<td>WorkFirst Personal ND</td>
<td>W1stPersND</td>
<td>N</td>
<td>TUT</td>
<td></td>
</tr>
<tr>
<td>912000002140</td>
<td>Testing</td>
<td>WorkFirst Testing</td>
<td>Wrk1stTest</td>
<td>Y</td>
<td>FEE</td>
<td>FMISCFEE</td>
</tr>
<tr>
<td>912000002150</td>
<td>Testing Non Disb</td>
<td>WorkFirst Testing ND</td>
<td>W1stTestND</td>
<td>N</td>
<td>TUT</td>
<td></td>
</tr>
<tr>
<td>912000002160</td>
<td>Tools &amp; Supplies</td>
<td>WorkFirst Tools</td>
<td>Wrk1stTool</td>
<td>Y</td>
<td>FEE</td>
<td>FMISCFEE</td>
</tr>
<tr>
<td>912000002170</td>
<td>Tools &amp; Supplies</td>
<td>WorkFirst Tools ND</td>
<td>W1stTooLN</td>
<td>N</td>
<td>TUT</td>
<td></td>
</tr>
<tr>
<td>912000002180</td>
<td>Transportation</td>
<td>WorkFirst Transportation</td>
<td>Wrk1stTran</td>
<td>Y</td>
<td>FEE, MIS</td>
<td>TRNSPORT</td>
</tr>
<tr>
<td>912000002190</td>
<td>Transportation</td>
<td>WorkFirst Transportation ND</td>
<td>W1TransND</td>
<td>N</td>
<td>TUT</td>
<td></td>
</tr>
</tbody>
</table>
International students and students interested in academic transfer degree programs are not eligible for student support funds. Please also refer to the WFDA Fiscal Guidelines for student eligibility.

**WorkFirst Policy and Procedure Manual**

WorkFirst providers must develop and maintain a local policy and procedure manual for their program to ensure services are maintained and grant requirements are met in the absence of, or change in, staffing.

Processes for administering the Student Support Funds should be outlined in your local policy and procedure manual.

Please refer to Appendix B for SBCTC Table of Contents Guide in the WFDA Grant Guidelines.

**Student Support Funding Documentation and Reporting**

In order to qualify for WorkFirst Student Support funding, each institution receiving WorkFirst Delivery Agreement funding must comply with the federal requirements for supervising, documenting, reporting, and verifying participation by WorkFirst (TANF) students in WorkFirst activities using the eJAS system.

Colleges administering the Student Support Funds are required to manage these funds carefully to ensure duplication of supports doesn’t occur. All other funding sources must be exhausted before using WorkFirst Student Support Funds.

Before awarding Student Support Funds, you must:

- Verify student’s eligibility and IRP status
- Check eJAS to ensure the student as not already received the same support they are requesting from another provider

**Documentation in eJAS**

In effort to ensure we are not duplicating services you will need to document in eJAS when a student receives Student Support Funds from your WorkFirst program. To document Student Support Funds received on behalf of a student in eJAS, you will need to create a case note that identifies: the type of support received, date received, amount and reason needed. Please use the case note type – “support services”.

All student support services requested, issued, or denied must be documented with justification in the eJAS case notes for the student.

Example: Jason requested and received $100 for a gas card on 9/15/2021 for winter quarter. This support will help Jason get to and from his classes on campus.

Example: Claire requested and was denied tools for her educational program as WorkFirst does not have the funding to support this request.
Disclaimer
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.

Compliance with Applicable Laws

- Omnibus Crime Control and Safe Streets Act of 1968
- Title VI of the Civil Rights Act of 1964
- Section 504 of the Rehabilitation Act of 1973
- Title II of the Americans with Disabilities Act of 1975
- Title IX of the Education Amendments of 1972
- The Age Discrimination Act of 1975

The Department of Justice Non-Discrimination Regulation:

- 28 C.F. R. Part 42, Subparts C.D.E. and G
- 28 C.F.R. Part 35
- 28 C.F.R. Part 39

Confidentiality and Records

Maintaining Confidentiality
Confidential information must not be used, published, transferred, sold or otherwise disclosed. When transmitting any confidential information secure email MUST be used.

Notice of Non-Disclosure
All employees with access to client information must have an up-to-date Confidential Information, Fraud and Abuse form (DSHS 03-374E - Rev. 11/2014). Employees that require access to eJAS must also complete the request for access at the bottom of this form. This form must be updated for each employee in September of each grant year and sent to the SBCTC.

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

Notification of Compromise or Potential Compromise

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

Fraud Reporting

Any knowledge of welfare fraud must be reported to DSHS by calling 1-800-562-6906 or online here.

The DSHS fraud reporting number must be posted in staff offices for ease of access by staff and employees.
Appendix A: Data Security Requirements

The following are requirements for SBCTC Subcontractors & Subgrantees as determined in Special Terms and Conditions Exhibit A- Data Security Requirements of the contract between the Department of Social and Health Services and the State Board for Community and Technical Colleges.

Definitions

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


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.
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:

<table>
<thead>
<tr>
<th>Data stored on:</th>
<th>Will be destroyed by:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server or workstation hard disks, or Removable media (e.g. floppies, USB flash drives, portal hard disks) excluding optical discs</td>
<td>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</td>
</tr>
<tr>
<td>Paper documents with sensitive or Confidential Information</td>
<td>Recycling through a contracted firm, provided the contract with the recycler assures that the confidentiality of Data will be protected.</td>
</tr>
<tr>
<td>Paper documents containing Confidential Information requiring special handling (e.g. protected health information)</td>
<td>On-site shredding, pulping, or incineration</td>
</tr>
<tr>
<td>Optical discs (e.g. CDs or DVDS)</td>
<td>Incineration, shredding, or completely defacing the readable surface with a coarse abrasive</td>
</tr>
</tbody>
</table>
### 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.