

Memorandum of Understanding
Between The State Board of Community and Technical Colleges
And
The Office of Administrative Hearings

Memorandum of Understanding 1
Exhibit A – Statement of Work 5
Exhibit B – Timeliness Standards10
Exhibit C – Case Age Calculation Methodology 11
Exhibit D – Reports..... 14
Exhibit E – Data Sharing and Security15

Parties and Purpose

This Memorandum of Understanding (Agreement) is made between the State Board of Community and Technical Colleges (SBCTC), on behalf of Washington State Community and Technical Colleges (CTCs), and the Office of Administrative Hearings (OAH), under RCW 39.34, for the purpose of providing adjudicative proceedings under RCW 34.05. OAH and SBCTC are independent agencies entering into this agreement to promote effective communication and establish mutual expectations as to how each agency will conduct its work relating to the adjudicative proceedings for CTCs which are the subject of this agreement. OAH and CTCs subject to this agreement will execute a separate Addendum incorporating by reference the terms of this agreement, and setting out additional CTC-specific program requirements.

Period of Performance

This Agreement will become effective April 1, 2021 and will expire on June 30, 2023, unless terminated sooner or extended as provided herein.

Statement of Work

OAH shall furnish the necessary personnel, equipment, material and/or services and otherwise do all things reasonably necessary for or incidental to the performance of work described in Exhibit A, Statement of Work.

Payment for OAH Services

CTCs will pay OAH under the billing methodology approved by the Office of Financial Management (OFM). The OAH billing methodology is available upon request.

CTCs shall not pay any claims for payment submitted more than twelve (12) months after the calendar month in which the services were performed, or for a closed state fiscal year. OAH shall not bill and CTCs shall not pay for services performed under this

Agreement if OAH has charged or will charge another agency of the State of Washington or any other party for the same services.

OAH agrees to submit a final invoice to any CTC receiving OAH services within forty-five (45) calendar days after OAH has completed the services or after this Agreement is terminated, whichever comes first.

CTC agrees to pay for services completed by OAH within thirty (30) calendar days from the date the invoice is sent to CTC. ALJ billable time includes time ALJs spend: at SBCTC or CTC-required trainings; preparing for, traveling to, and presiding at, Hearings; supervising legal assistant work; preparing initial orders, if applicable; and conducting other activities that support the processing of Hearings.

Agreement Amendments

This Agreement may be amended by written agreement executed by both parties.

Notification and Agreement Administration

SBCTC will ensure that each CTC is provided a copy of this Agreement in order to acquire OAH services, pursuant to terms and conditions herein, should they choose. The Agreement Manager for each of the parties shall be the contact person for all communication and billing regarding the performance of this Agreement. Agency contacts listed in the CTC addenda shall be the Agreement Managers for the individual CTCs. From time to time, Agreement Managers may change. Any change to a party's Agreement Manager identified shall be provided to the other party in writing or by electronic mail notification.

The parties' Agreement Managers are as follows:

State Board of Community and Technical Colleges OAH (Fiscal/Billing Questions)

Julie Huss
Director of Human Resources
WA State Board of Community & Technical Colleges
P.O. Box 42495
Olympia, WA 98504-2495
jhuss@sbctc.edu
360-704-4350

Deborah M. Feinstein
Finance & Facilities Manager
Office of Administrative Hearings
P.O. Box 42488
Olympia, WA 98504-2488
Deborah.Feinstein@oah.wa.gov
(360) 407-2717

OAH (Adjudications Questions)

Don Capp
Deputy Chief Administrative Law Judge
Office of Administrative Hearings
P.O. Box 42488
Olympia, WA 98504-2488
donald.capp@oah.wa.gov
(360) 407-2713

Termination

This Agreement may be terminated by either party upon sixty (60) days' written notice.

Entire Agreement

This Agreement consists of the following:

Document	Exhibit
Memorandum of Understanding	N/A
Statement of Work	A
Timeliness Standards	B
Case Age Calculation Methodology Reports	C
	D
Data Sharing and Security	E

Governance

If there is inconsistency between the terms of this Agreement, or between this Agreement and any applicable statute or rule, the inconsistency shall be resolved by giving precedence in the following order:

- Applicable state and federal law;
- Statement of Work (Exhibit A); and
- Any provision of this Agreement, including any other exhibits.

Definitions

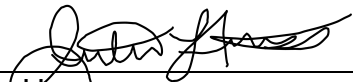
“Agreement” means this Memorandum of Understanding and all Exhibits.

“Case File” means the same thing as “Official Record”.

“CTC” means a Washington State Community or Technical College as defined in RCW 28B.50.030. Contact information for each CTC participating in this Agreement is identified in each respective CTC Addendum.

“Official Record” means the complete record of a case, as defined in RCW 34.05.476. The official record may be either paper or electronic. The official record does not include any additional copies or drafts of documents, or notes.

**STATE OF WASHINGTON
STATE BOARD OF COMMUNITY &
TECHNICAL COLLEGES**




Julie Huss
Contracts Administrator

3/19/2021

Date

**STATE OF WASHINGTON
OFFICE OF ADMINISTRATIVE
HEARINGS**

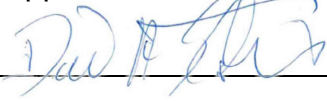
 for

Lorraine Lee
Chief Administrative Law Judge

3/31/2021

Date

Approved as to form:



3/25/2021

Date

Exhibit A – Statement of Work

Context:

Pursuant to Title IX of the Higher Education Act, formal complaints of sexual harassment at a CTC must be investigated and subject to a grievance process, which must include a live hearing prior to any determination of responsibility for conduct constituting sexual harassment. CTCs require an ALJ from OAH to preside over such hearings. In addition, certain decisions of a CTC (such as non-Title IX student conduct or faculty tenure dismissals) may be appealed when an affected person disagrees with the decision. Those appeals are heard at OAH by administrative law judges appointed by the Chief Administrative Law Judge.

Duties of OAH:

1. *Receiving an Hearing Request.* After receiving a hearing or appeal request from a CTC, OAH will assign an OAH docket number, open a case file, assign an ALJ, coordinate with the CTC in scheduling a hearing or prehearing conference, issue a notice of hearing or prehearing conference, and preside over prehearing conferences and hearing events in person, by telephone, by videoconference or other means under chapter 34.05 RCW (Administrative Procedure Act). OAH will retain the CTC's case number parallel to its own. For each case, unless presiding only, OAH shall issue an initial administrative decision, and/or other orders that comply with chapter 34.05 RCW.
2. *Programs.* OAH will receive appeal requests for the programs listed in each CTC Addendum.
3. *Orders.* Unless presiding only, the administrative law judge (ALJ) will issue an initial order after the evidentiary hearing. See the CTC addenda for which programs receive initial orders and which do not. These orders will be served on the parties. The orders will include language setting forth the applicable administrative appeal rights.
4. *Timeliness Standards.* OAH shall take steps to ensure that it issues decisions and other orders within the timeframes required by chapter 34.05 RCW, chapter 10-08 WAC (Washington Administrative Code), and applicable CTC regulations. OAH shall also take steps to ensure it meets the timeliness standards set forth in Exhibit B—Timeliness Standards. Meeting the timeliness standards is a cooperative effort which is in part dependent on the availability and preparedness of agency representatives, which is outside the control of OAH. OAH's ability to meet timeliness standards may also be affected when due process requires the ALJ to grant one or more continuances of the hearing based on the request of a party and a showing of good cause.

5. *Reports.* OAH has developed a series of standard reports to assist referring agencies in monitoring and analyzing appeals data. The reports currently available are listed on Exhibit D below. These are available upon request to OAH. Some reports are also available on-demand through OAH's referring agency portal. OAH will provide SBCTC with copies of any of the reports selected on Exhibit D, upon request. When requested, the reports will be provided by the end of the month following the final month of the applicable reporting period. For example, requests for monthly reports covering August data will be completed by September 30.
6. *Case Age Calculation Methodology.* Case age and days in hearing status will be calculated according to the case age calculation methodology set forth in Exhibit C. Days during which a case is stayed will not be included in the case age or days in hearing status total. For purposes this calculation, stays are appropriate in the following situations:
 - a. When there is a related case pending in another court or forum;
 - b. When there is a stay order entered in another tribunal, that stays the OAH action pending the outcome in that tribunal;
 - c. Where there is an interlocutory petition for review of an OAH ruling or decision; or
 - d. When the Servicemembers Civil Relief Act requires that the OAH action be continued or stayed.
7. *Language Access and ADA Accommodations.* OAH is committed to providing equal access to the administrative hearing process. OAH will provide for interpreters as required by RCW 2.42-43, RCW 34.05, and WAC 10-08. OAH will provide reasonable accommodations to all participants who need accommodations due to a disability, in compliance with Title II of the Americans with Disabilities Act of 1990, Title VI of the Civil Rights Act of 1964, Section 504 of the Rehabilitation Act of 1973, the Age Discrimination Act of 1975, and the Washington Law Against Discrimination.
8. *Audio Recording.* An OAH Administrative Law Judge (ALJ) will make a complete and clear audio recording of the proceedings, even when a court reporter is also used to record the proceedings.
9. *Transmittal of Case File.* OAH will provide CTC with the case file when the case closes, or after the appropriate retention period. The file may be in electronic or paper format and will include a complete record of the proceedings. The case file is the official record of the proceedings, as defined in RCW 34.05.476, and will not include notes or other draft materials used by the ALJ. The case file shall identify the case name, docket number, and applicable program. Each case file will meet the requirements of chapter 34.05 RCW and any other applicable statutes and rules, and will include the following if applicable:

//

- a. Notices of all proceedings;
 - b. Any prehearing order;
 - c. Any motions, pleadings, briefs, petitions, requests, and intermediate rulings;
 - d. Evidence received or considered, including any list of exhibits or witnesses submitted by a party;
 - e. A statement of matters officially noticed;
 - f. A complete and clear audio recording of the proceedings;
 - g. Any transcript of all or part of the hearing considered before final disposition of the proceeding;
 - h. Proffers of proof and objections and rulings thereon;
 - i. Proposed findings, requested orders, and exceptions;
 - j. Any initial order or other order closing the case;
 - k. Staff memoranda or data submitted to the presiding officer, unless prepared and submitted by personal assistants and not inconsistent with RCW [34.05.455](#); and
 - l. Matters placed on the record after an ex parte communication.
10. *Transmittal of Paper File*. For cases in which the case file is transmitted to CTC in paper format, OAH will transmit the file to CTC as soon as possible after the case closes.
11. *Transmittal of Electronic File*. For cases in which the case file is transmitted to the CTC electronically, OAH will transmit the file at the time the case closes.
12. *Custodian of the Official Record*. While a case is pending before OAH, OAH serves as a temporary custodian of the official record. As soon as OAH transmits the closed file to the CTC, OAH is no longer the custodian of the official record and no longer has any obligation to retain the records related to the closed file.
13. *Adequate Staffing*. OAH agrees to provide an adequate number of ALJs and support staff to cover the expected volume of work to assure timely scheduling, conduct of hearings, and issuance of decisions in accordance with the terms of this Agreement.
14. *Training Standards*. OAH will ensure ALJs assigned to the SBCTC caseload are properly trained and qualified, and have the expertise needed for proper handling of the cases.
15. *Specific Training Requirements*. TBD

Duties of SBCTC and CTCs:

16. *Transmittal of Hearing Request to OAH*. Upon receiving a hearing request, CTC will transmit the hearing request to OAH electronically, using the participant portal, referring agency portal or other agreed-upon means. CTC will take steps

to ensure the hearing request is transmitted within the timeliness standards listed on Exhibit B. CTC will ensure the date the hearing request was received is clearly marked on the hearing request or an accompanying document.

17. *Hearing representatives.* CTC agrees to provide an adequate number of hearing representatives and support staff to cover the expected volume of work to allow timely completion of work by OAH.
18. *Docket and Case Schedule Information.* CTC will obtain any needed docket or case scheduling information from the referring agency portal, participant portal, or the provided reports.
19. *Redaction of exhibits—Generally.* OAH applies the Public Records Act (Chapter 42.56 RCW) and other applicable law in responding to requests for records. In response to a public records request, OAH will only withhold or redact information if such withholding or redaction is supported by an exemption in the Public Records Act or other legal basis. OAH generally does not redact the exhibits or other documents filed in a case unless and until information is redacted in response to a public records request. Therefore, any exhibits or other case documents filed with OAH will generally be viewable as filed by all parties and representatives to a case. Prior to filing exhibits with OAH, the CTC should redact any information it believes is not appropriate for release to all other parties in the case.
20. *Filing.* CTC will file exhibits, pleadings, motions, and other documents through the participant portal or referring agency portal unless another filing method is agreed upon.
21. *Marking of Exhibits.* When filing exhibits, CTC will number each exhibit in a consistent manner in the lower right-hand corner.
22. *Access to Case Information and Documents for Agency Representatives.* OAH uses the referring agency portal, and/or the participant portal to provide case information and serve notices and orders on agency representatives and program contacts. The representatives of the CTC shall use one or more of these methods to obtain case information and to receive service of notices and orders from OAH.
23. *Transmittal of Closed File.* OAH uses the referring agency portal to transmit closed files. CTC agrees to accept one or both of these methods as the exclusive means to receive the official record of the adjudication back from OAH.

Duties of OAH and SBCTC:

24. *Operational Meetings.* Representatives from SBCTC and OAH will meet as necessary to discuss common issues and concerns, such as workload

forecasts, financial and budget projections, changes in the law, hearing procedures, performance measures, review of program protocols.

25. *Notice of Significant Changes.* Each agency will inform the other of policy, program and procedural changes that would significantly affect the hearing process or the volume of work.

26. *Collaboration on Process Improvement.* Both agencies will work together collaboratively to continually improve the quality and timeliness of the adjudicative process, including the efficiency and security of the information exchange between the two agencies.

Exhibit B – Timeliness Standards

Program	Event	Timeliness Standard
All programs	Transmit hearing request	CTC will transmit hearing request to OAH as soon as possible following its investigation.
All programs	Issue notice of prehearing conference	OAH will issue the notice of prehearing conference within five business days of receiving the request for hearing.
All programs	Schedule hearing	Schedule the hearing to occur within 1-2 weeks after the prehearing conference.
All programs	Issue decision	Issue the initial order within thirty days after the hearing record closes.
All programs	Issue dismissal order	If an order of default or dismissal will be issued based on a party's failure to appear or withdrawal of a hearing request, issue the default or dismissal order within three business days after the receipt of the withdrawal request or the failure to appear.
All programs	Close case	Issue the initial decision or other dispositive order within the case closure timeline specified in the applicable CTC Addendum.

Exhibit C – Case Age Calculation Methodology

Case Definition

An adjudicative proceeding received by OAH, either from a referring agency or directly from a non-agency party, where OAH has delegated or other authority to receive the appeal request.

Case Initiation

For purposes of calculating case age and days in hearing status, a case is initiated by one of the following, as applicable:

- Filing of an appeal of a referring agency's determination
- Filing of a petition to vacate an OAH order
- Issuance of a remand by a higher authority review body to OAH for further proceedings
- Filing of a petition for review of an OAH initial order, for caseloads where the referring agency has delegated the administrative review authority to OAH
- Issuance of a request from a higher authority review body for OAH to conduct a hearing only

The following types of requests are not counted for purposes of calculating case age or days in hearing status:

- Request for correction of an OAH order

Case Age

The time period from case initiation until the corresponding closing order is published, minus the following:

- Any period of time during which the case is stayed
- Any periods of time excepted by interagency agreement

For purposes of calculating case age, the first day is the first calendar day following the date of the event that initiated the case. For pending cases, the last day is the current day. For closed cases, the last day is the date the applicable dispositive order was published.

Days in Hearing Status

The time period from the date OAH received the appeal, petition or request that initiated the case until the corresponding closing order is published, minus the following:

- Any period of time during which the case stayed
- Any periods of time excepted by interagency agreement

For purposes of counting days in hearing status, the first day is the calendar day following the date OAH received the document or communication that initiated the case. For pending cases, the last day is the current day. For closed cases, the last day is the date the applicable dispositive order was published.

Examples:

Docket No. 1

Event	Date	Case Age	Days in Hearing Status	Case Tracking
Appeal filed with referring agency	Jan 1	0 - start	n/a	Start of case #1
OAH receives appeal	Jan 4	3	0 - start	
OAH publishes default order	Jan 31	30 – end	27 – end	End of case #1
PTV filed with OAH	Feb 6	0 – start	0 – start	Start of case #2
OAH publishes order granting PTV	Feb 16	10	10	
OAH issues initial order	Feb 28	22 – end	22 – end	End of case #2
Higher Authority issues remand order	Mar 31	0 – start	n/a	Start of case #3
OAH receives remand order	Apr 3	3	0 – start	
OAH issues new initial order	Apr 30	30 - end	27 – end	End of case #3
OAH receives request for corrected order	May 4	30	27	
OAH issues corrected order	May 5	30	27	

Docket No. 2

Event	Date	Case Age	Days in Hearing Status	Case Tracking
Appeal filed with referring agency	Jan 1	0 – start	n/a	Start of Case #1
OAH receives appeal	Jan 4	3	0 – start	
OAH puts case in “stay” status due to criminal matter pending in another forum	Jan 31	30 – stop	27 – stop	
OAH lifts stay upon resolution of criminal case	Mar 31	30 – start	27 – start	
OAH issues initial order	Apr 30	60 – stop	57 – stop	End of Case #1

Exhibit D – Reports

Report No.	Report Name	Frequency
2001	Hearings	Upon request
2005	Pending Appeals	Upon request
2008	Interpreter Language	Upon request
2101	Intake	Upon request
2203	Continuance	Upon request
2205	Notice Timeliness	Upon request
2205a	Notice Timeliness Detail	Upon request
2205b	Notice Timeliness Detail – Late Notices	Upon request
2301	Orders Pending	Upon request
2302	Hearing Calendar	Upon request
2401	Closed Appeals	Upon request
2402	Default Rate	Upon request
2404	Case Disposition Summary	Upon request

Exhibit E – Data Sharing and Security

1. Purpose of the Data Sharing

The purpose of these data sharing and security provisions is to identify, describe and protect the data to be exchanged between CTC and OAH for the cooperative partnership between OAH, SBCTC, and CTC. The requirements in these provisions are designed to reduce the risk associated with the unauthorized access, disclosure or destruction of the agency data, as well as to ensure compliance with applicable law, including the OCIO Public Records Privacy Protection Policy.

2. Justification and Authority for Data Sharing

The Data to be shared under this Agreement is necessary to comply with Chapter 34.12 RCW and 34.05 RCW, which authorize OAH to conduct administrative adjudications for other state and local government agencies. Specifically, CTC student conduct rules and employment policies governing Title IX grievance proceedings, consistent with 34 C.F.R 106.45(b)(6), provide that a respondent accused of conduct in violation of Title IX is entitled to a live hearing prior to a determination of responsibility.

3. Description of Data to be Shared

OAH and CTCs will share data related to administrative appeals. The data to be shared includes case numbers and other unique identifiers; appeal dates; case dispositions; case record of events; case timelines; judge identification; review and judgment status; case participants; participant identification and contact information; hearings list and outcomes; hearing type; hearing participants; case issue type; orders; notices; exhibits and other case documents.

4. Methods of Data Sharing and Access

Data will be transferred from CTC to OAH, as well from OAH to CTC via:

- a. For new cases, an agreed upon method; and
- b. For existing cases, via the OAH referring agency portal.

5. Location and Retention of Electronic Data

OAH and CTCs each have a data storage system that houses the electronic data to be shared. The individual CTC is the official custodian of the appeal record, and has sole responsibility for any retention and archiving of the official record. After transmitting data to CTC, OAH no longer has an obligation to retain the data. Currently, OAH's practice is to retain the case documents for two years after case closure, then delete.

6. Data Classification

The State classifies data into categories based on the sensitivity of the data pursuant to the Security policy and standards promulgated by the Office of the State of Washington Chief Information Officer. (See Section 4, *Data Security*, of *Securing IT Assets*

Standards No. 141.10 in the *State Technology Manual* at <https://ocio.wa.gov/policies/141-securing-information-technology-assets/14110-securing-information-technology-assets>. Section 4 is hereby incorporated by reference into this Agreement.)

The Data that is the subject of this DSA is classified as indicated below:

[Check a category]

Category 1 – Public Information

Public information is information that can be or currently is released to the public. It does not need protection from unauthorized disclosure, but does need integrity and availability protection controls.

Category 2 – Sensitive Information

Sensitive information may not be specifically protected from disclosure by law and is for official use only. Sensitive information is generally not released to the public unless specifically requested.

Category 3 – Confidential Information

Confidential information is information that is specifically protected from disclosure by law. It may include but is not limited to:

- a. Personal Information about individuals, regardless of how that information is obtained;
- b. Information concerning employee personnel records;
- c. Information regarding IT infrastructure and security of computer and telecommunications systems;

Category 4 – Confidential Information Requiring Special Handling

Confidential information requiring special handling is information that is specifically protected from disclosure by law and for which:

- a. Especially strict handling requirements are dictated, such as by statutes, regulations, or agreements;
- b. Serious consequences could arise from unauthorized disclosure, such as threats to health and safety, or legal sanctions.

7. Constraints on Use of Data

The Data being shared/accessed is owned and belongs to the State of Washington.

This Agreement does not constitute a release of the Data for the Receiving Party's discretionary use. Receiving Party must use the Data received or accessed under this Data Sharing Agreement only to carry out the purpose and justification of this agreement as set out in sections 1, *Purpose of the Data Sharing*, and 2, *Justification and Authority for Data Sharing*.

Any disclosure of Data contrary to this Agreement is unauthorized and is subject to penalties identified in law.

8. Security of Data

OAH shall protect and maintain all Confidential Information gained by reason of this Agreement against unauthorized use, access, disclosure, modification or loss. OAH will not use, publish, transfer, sell or otherwise disclose any Confidential Information gained by reason of this Agreement for any purpose that is not directly connected with the purpose and justification of this Agreement, except that disclosure shall be authorized as follows:

- As provided by law;
- To parties, party representatives and other case participants (for example, interpreters) who are authorized or entitled to receive the Confidential Information because of their role in the proceeding;
- With the prior written consent of the person or personal representative of the person who is the subject of the Confidential Information;
- To OAH personnel or contractors who have an authorized business requirement to view the Confidential Information and who have been instructed on the use restrictions on the Confidential Information; or
- In response to public records requests, when the responsive information is not exempt from disclosure under chapter 42.56 RCW or other federal or state laws.

OAH shall physically secure any computers, documents, or other media containing Confidential Information.

9. Data Security Standards

Receiving Party must comply with the Data Security Requirements set out in section 13 below and the Washington OCIO Security Standard, 141.10

(<https://ocio.wa.gov/policies/141-securing-information-technology-assets/14110-securing-information-technology-assets>.) The Security Standard 141.10 is hereby incorporated by reference into this Agreement.

10. Data Retention and Disposition

At the end of the Agreement's term, or when no longer needed, Confidential Information/Data must be disposed of as set out in section 13.6 *Data Disposition*, except as required to be maintained for compliance or accounting purposes. OAH may retain appeal data, including exhibits, recordings, notices and orders to conduct its core business activities, including but not limited to training, responding to legislative inquiry, public records requests, fiscal note responses, caseload management, agency reporting, supporting a decision library, and secure electronic communication of docket related data/information with authorized case participants.

11. Public Disclosure

The party that receives a public records request for records containing Data subject to this Agreement will be responsible for responding to it.

12. Breach Reporting

OAH will report any Breach of Data shared under this Agreement to CTC's Privacy Officer within five (5) business days of discovery. Upon discovering a breach, OAH will take actions to mitigate the risk of loss and comply with any notification or other requirements imposed by applicable law or reasonably requested by CTC in order to meet its regulatory obligations. After discovering a Breach, OAH will perform a root cause analysis and mitigation plan, so as to systematically identify and reduce any data insecurity factors within OAH's control.

13. Data Security Requirements

13.1 Data Transmitting

When transmitting Confidential Information electronically, including via email, the Data must be protected by:

- a. transmitting the Data within the State Governmental Network (SGN) or Receiving Party's internal network; or
- b. Encrypting any Data that will be transmitted outside the SGN or Receiving Party's internal network with 256-bit Advanced Encryption Standard (AES) encryption or better. This includes transit over the public Internet.

Confidential Information will not be transmitted via facsimile (fax). When transmitting Confidential Information via paper documents, the Receiving Party must use a Trusted System.

13.2 Protection of Data

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

- a. **Hard disk drives.** Data stored on local workstation hard disks. Access to the Data will be restricted to Authorized User(s) by requiring logon to the local workstation using a Unique User ID and Hardened Password or other authentication mechanisms which provide equal or greater security, such as biometrics or smart cards.
- b. **Network server disks.** Data stored on hard disks mounted on network servers and made available through shared folders. Access to the Data will be restricted to Authorized Users through the use of access control lists which will grant access only after the Authorized User has authenticated to the network using a Unique User ID and Hardened Password or other authentication mechanisms which provide equal or greater security, such as biometrics or smart cards. Data on disks mounted to such servers must be located in an area that is accessible only to authorized personnel, with access controlled through use of a key, card key, combination lock, or comparable mechanism.

13.3 Data Destruction

For Confidential Information stored on network disks, deleting unneeded Data is sufficient as long as the disks remain in a Secured Area and otherwise meet the requirements listed in the above paragraph. Destruction of the Data as outlined in section 13.6 *Data Disposition* of this Exhibit may be deferred until the disks are retired, replaced, or otherwise taken out of the Secured Area.

- a. **Removable Media, including Optical discs (CDs or DVDs) in local workstation optical disc drives and which *will be maintained in a secure area when not in use*.** When not in use for the contracted purpose, Confidential Information provided by Disclosing Party on removable media, such as optical discs or USB drives, which will be used in local workstation optical disc drives or USB connections 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 that access Confidential Information 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.
- b. **Optical discs (CDs or DVDs) in drives or jukeboxes attached to servers and which *will be maintained in a secure area when not in use*.** Confidential Information provided by Disclosing Party on optical discs which will be attached to network servers will be encrypted with 128-bit AES encryption or better. 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 been 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.

- c. **Paper documents.** Any paper records containing Confidential Information must be protected by storing the records in a secure area that is accessible only 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.

13.4 Protection of Data Stored on Portable Devices or Media

Data must **not** be stored by the Receiving Party on portable devices or media unless specifically authorized within the Data Share Agreement. If so authorized, the Receiving Party must protect the Data as provided in this section 4.

Portable devices are any small computing device that can be transported, including but are not limited to: handhelds/PDAs/phones; Ultramobile PCs, flash memory devices (e.g. USB flash drives, personal media players); and laptop/notebook/tablet computers.

Portable media means any Data storage device that can be detached or removed from a computer and transported, including but not limited to: optical media (e.g. CDs, DVDs); magnetic media (e.g. floppy disks, tape, Zip or Jaz disks); USB drives; or flash media (e.g., CompactFlash, SD, MMC).

For Data stored on Portable devices or media, Receiving Party must:

- a. Encrypt the Data with a key length of at least 128 bits using an industry standard algorithm, such as AES;
- b. Ensure that portable devices such as flash drives are Federal Information Processing Standards (FIPS) Level 2 compliant;
- c. Control access to the devices with a unique user ID and password or stronger authentication method such as a physical token or biometrics;
- d. Manually lock devices whenever they are left unattended and set devices to lock automatically after a period of inactivity, if this feature is available. The maximum period of inactivity is 20 minutes.
- e. Physically protect the portable device(s) and/or media by:

- i. Keeping them in locked storage when not in use;
- ii. Using check-in/check-out procedures when they are shared;
- iii. Maintaining an inventory; and
- iv. Ensuring that when being transported outside of a Secured Area, portable devices and media with Data are under the physical control of an Authorized User.

13.5 Data Segregation

Data received under this DSA must be segregated or otherwise distinguishable from all other Data. This is to ensure that when no longer needed by the Receiving Party, all of Disclosing Party’s Data can be identified for return or destruction. It also aids in determining whether Disclosing Party’s Data has or may have been compromised in the event of a security breach.

- a. Data must be kept in one of the following ways:
 - i. On media (e.g. hard disk, optical disc, tape, etc.) which will contain no non-Disclosing Party Data; or
 - ii. In a logical container on electronic media, such as a partition or folder dedicated to Disclosing Party’s Data; or
 - iii. In a database that will contain no non-Disclosing Party Data; or
 - iv. Within a database and will be distinguishable from non-Disclosing Party Data by the value of a specific field or fields within database records; or
 - v. When stored as physical paper documents, physically segregated from non-Disclosing Party Data in a drawer, folder, or other container.
- b. When it is not feasible or practical to segregate Data from all other data, then all data which is commingled with the Data provided under this Agreement must be protected as described in this exhibit.

13.6 Data Disposition

When the Confidential Information is no longer needed, except as noted in 3.b above, the Data must be returned to Disclosing Party 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	Using a “wipe” utility which will overwrite the Data at least three (3)

Removable media (e.g. floppies, USB flash drives, portable hard disks, Zip or similar disks)	<p>times using either random or single character Data, or</p> <p>Degaussing sufficiently to ensure that the Data cannot be reconstructed, or</p> <p>Physically destroying the disk</p>
Paper documents with Category 3 and higher 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 by a method that renders the Data unreadable, pulping, or incineration
Optical discs (e.g. CDs or DVDs)	Incineration, shredding, or cutting/breaking into small pieces.
Magnetic tape	Degaussing, incinerating or crosscut shredding

14. Definitions—Data Sharing and Security

- a. “Authorized User” means an individual or individuals with an authorized business need to access Confidential Information under this Agreement.
- b. “Breach” means the unauthorized acquisition, access, use, or disclosure of Data shared under this Agreement that compromises the security, confidentiality or integrity of the Data.
- c. “Confidential Information” means information that is exempt from disclosure to the public or other unauthorized persons under chapter 42.56 RCW or other federal or state laws. Confidential Information includes, but is not limited to,

Personal Information.

- d. "Data" means the case-related information that is transmitted, disclosed or exchanged between OAH, SBCTC, and/or CTC to carry out the purpose of this Agreement. The Data may include paper records as well as electronic records.
- e. "Hardened Password" means a string of at least eight characters containing at least three of the following character classes: upper case letters; lower case letters; numerals; and special characters, such as an asterisk, ampersand or exclamation point.
- f. "Participant Portal" means a secured web application specific to authorized OAH case participants allowing access to their case related records and data. This portal allows the participants to file documents electronically for existing cases.
- g. "Personal Information" means information identifiable to any person, including, but not limited to, information that relates to a person's name, health, finances, education, business, use or receipt of governmental services or other activities, addresses, telephone numbers, social security numbers, driver's license numbers, credit card numbers, any other identifying numbers, and any financial identifiers.
- h. "Referring Agency Portal" means a web application view specific to an individual agency's caseloads and associated programs. Referring agencies have access to their entire caseload and are not limited to an individual case view. Authentication varies depending on the referring agencies participation in the state enterprise active directory services (State Forest).
- i. "Secured Area" means an area to which only Authorized Users have access. Secured Areas may include buildings, rooms or locked storage containers (such as a filing cabinet) within a room, as long as access to the Confidential Information is not available to unauthorized personnel.
- j. "Trusted System" includes only the following methods of delivery: (1) electronic transmission within the Washington State Governmental Network; (2) secure email; (3) WaTech managed security layer (OAH Portals); (4) hand-delivery by a person authorized to have access to the Confidential Information with written acknowledgement of receipt; (5) United States Postal Service ("USPS") first class mail, or USPS delivery services that include Tracking, such as Certified Mail, Express Mail or Registered Mail; (6) commercial delivery services (e.g. FedEx, UPS) which offer tracking and receipt confirmation; and (7) the Washington State campus mail system.
- k. "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.