# Memorandum of Understanding

Between the Washington State Criminal Justice Training Commission

And

The Office of Administrative Hearings

[Memorandum of Understanding 1](#_Toc95466488)

[Exhibit A – Statement of Work 5](#_Toc95466489)

[Exhibit B – Programs List 10](#_Toc95466490)

[Exhibit C – Timeliness Standards 11](#_Toc95466491)

[Exhibit D – Case Age Calculation Methodology 12](#_Toc95466492)

[Exhibit E – Agency Contacts 13](#_Toc95466493)

[Exhibit F – Reports 14](#_Toc95466494)

[Exhibit G – Data Sharing and Security 15](#_Toc95466495)

**Parties and Purpose**

This Memorandum of Understanding (Agreement) is made between the Washington State Criminal Justice Training Commission (WSCJTC) and the Office of Administrative Hearings (OAH), under chapter 39.34 RCW, for the purpose of providing adjudicative proceedings under chapter 34.05 RCW. OAH and WSCJTC 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 which are the subject of this agreement.

**Period of Performance**

This Agreement will become effective May 1, 2022, and will expire on June 30, 2027, 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**

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

WSCJTC 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 WSCJTC 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 WSCJTC within forty-five (45) calendar days after OAH has completed the services or after this Agreement is terminated, whichever comes first.

WSCJTC agrees to pay for services completed by OAH within thirty (30) calendar days from the date the invoice is sent to WSCJTC.

**Agreement Amendments**

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

**Notification and Agreement Administration**

The Agreement Manager for each of the parties shall be the contact person for communication regarding the performance of this Agreement, or any amendment or update. 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:

|  |  |
| --- | --- |
| **WSCJTC (Fiscal/Billing Matters)** | **OAH (Fiscal/Billing Matters)** |
| Brian ElliottFiscal Services ManagerWSCJTC3060 Willamette DriveLacey, WA 98516-6267BElliott@cjtc.wa.gov (360) 281-9346 | Deborah M. FeinsteinFinance & Facilities ManagerOffice of Administrative HearingsP.O. Box 42488Olympia, WA 98504-2488Deborah.Feinstein@oah.wa.gov(360) 407-2717 |
|  |  |
| **OAH** (**Other Matters)**Kevin Zeller Assistant DirectorWSCJTC19010 1ST Avenue SBurien, WA 98418KZeller@cjtc.wa.gov(360) 835-7337 | **OAH** (**Other Matters)**Josh SundtDeputy Chief Administrative Law JudgeOffice of Administrative HearingsP.O. Box 42488Olympia, WA 98504-2488joshua.sundt@oah.wa.gov(360) 968-9509 |

**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 |
| Programs List | B |
| Timeliness Standards | C |
| Case Age Calculation Methodology | D |
| Agency Contacts | E |
| Reports | F |
| Data Sharing and Security | G |

**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”

“Official Record” means the complete record of a case, as defined in RCW [34.05.476](http://app.leg.wa.gov/RCW/default.aspx?cite=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 CRIMINAL JUSTICE TRAINING COMMISSION** |  | **STATE OF WASHINGTON OFFICE OF ADMINISTRATIVE HEARINGS** |
|  |  |  |
|  |  |  |
| Monica Alexander  |  | Lorraine Lee |
| Executive Director  |  | Chief Administrative Law Judge |
|  |  |  |
| 4/6/2022 |  | 4/7/2022 |
| Date |  | Date |
|  |  |  |
|  |  |  |
|  |  |  |
| Approved as to form: |  |  |
|  |  |  |
|  |  |  |
| Date |  |  |

# Exhibit A – Statement of Work

**Context:**

Under RCW 43.101.155, a peace officer or corrections officer who disagrees with a statement of charges denying, suspending, or revoking the officer’s certification may request a hearing before the hearings panel appointed under RCW 43.101.380. An OAH administrative law judge appointed under chapter 34.12 RCW shall be the presiding officer at the hearing, shall make all necessary rulings in the course of the hearing, and shall issue a proposed recommendation, but is not entitled to vote. The WSCJTC’s final administrative decision is subject to judicial review under RCW 34.05.510 through 34.05.598.

**Duties of OAH:**

1. *Receiving a Hearing Request*. A hearing request must be filed directly with WSCJTC. WSCJTC then forwards the hearing request to OAH. After receiving a hearing request from WSCJTC, OAH will assign an OAH docket number, open a case file, assign an administrative law judge to serve as the presiding officer, schedule a hearing or prehearing conference, issue a notice of hearing or prehearing conference, and conduct hearing events in person, by telephone, by videoconference or other means under chapter 34.05 RCW (Administrative Procedure Act). For each case, OAH shall issue an initial order (proposed recommendation), and/or other orders that comply with chapter 34.05 RCW.
2. *Programs*. OAH will receive hearing requests for the programs listed in Exhibit B – Programs List.
3. *Hearings Panel Appointment, Scheduling, and Communication*. WSCJTC will appoint the members of the hearings panel and will manage the coordination and scheduling of panel members. In scheduling prehearing conferences, hearings and other hearing events, OAH will coordinate with the WSCJTC hearings coordinator, who will communicate with members of the hearings panel.
4. *Orders*. The administrative law judge (ALJ) will issue an initial order, which shall serve as the proposed recommendation referenced in RCW 43.101.380(2). OAH will serve all prehearing, interim, and initial orders on the parties. The proposed recommendation will be reviewed by the hearings panel. The hearings panel will then meet to deliberate and will make the decision to accept, reject or modify the proposed recommendation. The WSCJTC will issue the final administrative order within forty-five (45) days after the date of the proposed recommendation. If the Respondent disagrees with the final administrative order, they may file an appeal with the superior court. Each order will include a description of the applicable rights of further review.
5. *Timeliness Standards*. OAH shall take steps to ensure it issues decisions and other orders within the timeframes required by chapter 34.05 RCW, chapter 10-08 WAC (Washington Administrative Code), and chapter 139 WAC. OAH shall also take steps to ensure it meets the timeliness standards set forth in Exhibit C - Timeliness Standards. Meeting the timeliness standards is a cooperative effort which is in part dependent on the availability and preparedness of agency representatives and hearing panel members, and 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.
6. *Reports*. OAH has developed a series of standard reports to assist referring agencies in monitoring and analyzing case management data. The reports currently available are listed in Exhibit F below. Some reports are also available on-demand through OAH’s Referring Agency Portal. For more detailed data and analysis referring agencies may wish to access OAH’s case management data through OAH’s Border Services, if applicable. OAH will provide WSCJTC with copies of the reports selected in Exhibit F. The selected reports will be provided by the end of the month following the final month of the applicable reporting period. For example, monthly reports covering August data will be provided by September 30.
7. *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 D. 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:
	1. When there is a related case pending in another court or forum;
	2. When there is a stay order entered in another tribunal, that stays the OAH action pending the outcome in that tribunal;
	3. Where there is an interlocutory petition for review of an OAH ruling or decision; or
	4. When the Servicemembers Civil Relief Act requires the OAH action be continued or stayed.
8. *Special Case Age Calculation Terms*. N/A
9. *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 chapters 2.42, 2.43, and 34.05 RCW, and chapter 10-08 WAC. 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.
10. *Transmittal of Case File*. OAH will make the case file available to WSCJTC in electronic format through the Referring Agency Portal and/or Border Services. Once the case is closed, the case file 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:
	1. Notices of all proceedings;
	2. Any prehearing order;
	3. Any motions, pleadings, briefs, petitions, requests, and intermediate rulings;
	4. Evidence received or considered, including any list of exhibits or witnesses submitted by a party;
	5. A statement of matters officially noticed;
	6. A complete and clear audio recording of the proceedings;
	7. Any transcript of all or part of the hearing considered before final disposition of the proceeding;
	8. Proffers of proof and objections and rulings thereon;
	9. Proposed findings, requested orders, and exceptions;
	10. Any initial order, final order, order on reconsideration or other order closing the case;
	11. Staff memoranda or data submitted to the presiding officer, unless prepared and submitted by personal assistants and not inconsistent with RCW [34.05.455](http://app.leg.wa.gov/RCW/default.aspx?cite=34.05.455); and
	12. Matters placed on the record after an ex parte communication.
11. *Custodian of the Official Record*. While a case is pending before OAH, OAH serves as a temporary custodian of the official record. Once OAH closes the case, 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. WSCJTC is the official custodian of the agency record of each administrative proceeding and has sole responsibility for any retention and archiving of the official record. OAH’s current practice is to retain case documents for two years after case closure, then delete.
12. *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.
13. *Training Standards*. OAH will ensure ALJs assigned to the WSCJTC caseload are properly trained and qualified, and have the expertise needed for proper handling of the cases. WSCJTC will provide OAH with the necessary training to be completed by the ALJ’s.
14. *Payment for Specific Required Training*. ALJ time spent attending training required or provided by WSCJTC will be billed at the normal hourly rate.

**Duties of WSCJTC:**

1. *Transmittal of Hearing Request to OAH*. Upon receiving a hearing request WSCJTC will transmit the hearing request to OAH electronically, using the Participant Portal, Referring Agency Portal, Border Services or other agreed-upon means. The WSCJTC will take steps to ensure the hearing request is transmitted within the timeliness standards listed in Exhibit C. The WSCJTC will ensure the date the hearing request was received is clearly marked on the hearing request or an accompanying document.
2. *Hearing Representatives and Panel Members*. WSCJTC agrees to provide an adequate number of hearing representatives, hearings panel members, and support staff to cover the expected volume of work to allow timely completion of work by OAH.
3. *Docket and Case Schedule Information*. WSCJTC will obtain any needed docket or case scheduling information from the Referring Agency Portal, Border Services, Participant Portal, or the provided reports.
4. *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 WSCJTC should redact any information it believes is not appropriate for release to all other parties in the case.
5. *Redaction of Exhibits—Special Terms*. [e.g. DCS caseload, for after-filed exhibits.] N/A
6. *Filing*. WSCJTC will file exhibits, pleadings, motions, and other documents through the Participant Portal or Referring Agency Portal unless another filing method is agreed upon.
7. *Format and Order of Exhibits*. When filing exhibits with OAH, the WSCJTC will provide the documents electronically in a format that supports automatic indexing, to allow OAH staff to efficiently order and mark the exhibits. Alternatively, if WSCJTC is not able to provide the exhibits in such a format, it will provide the documents electronically in a logical, consistent sequence.
8. *Marking of Exhibits*. When filing exhibits, the WSCJTC will number each exhibit in a consistent manner in the lower right-hand corner.
9. *Access to Case Information and Documents for Agency Representatives*. OAH uses Border Services, 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 WSCJTC shall use one or more of these methods to obtain case information and to receive service of notices and orders from OAH.
10. *Transmittal of Closed File*. OAH uses Border Services and/or the Referring Agency Portal to transmit closed files. The WSCJTC agrees to accept one or both methods as the exclusive means to receive the official record of the adjudication back from OAH.

**Duties of OAH and WSCJTC:**

1. *Operational Meetings*. Representatives from WSCJTC 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, and review of program protocols.
2. *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.
3. *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 – Programs List

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Program Name** | **Reference** | **Request for Hearing Filed with** | **OAH****Order Type**  | **Case Closure Timeline****(from receipt by OAH)** |
| Certification Denial | RCW 43.101.155,43.101.115 | WSCJTC | Initial (proposed recommendation) | N/A |
| Certification Suspension | RCW 43.101.155 | WSCJTC | Initial (proposed recommendation) | N/A |
| Certification Revocation | RCW 43.101.155 | WSCJTC | Initial (proposed recommendation) | N/A |

# Exhibit C – Timeliness Standards

|  |  |  |
| --- | --- | --- |
| Program | Event | Timeliness Standard |
| All programs | Transmit hearing request | WSCJTC will transmit hearing request to OAH within \_14\_ days after receiving hearing request. |
| All programs | Hold prehearing conferenceSet hearing date | Under RCW 43.101.155, within 14 days after WSCJTC receives the hearing request, OAH will hold a prehearing conference and set the date for hearing. This timeline may be changed by mutual agreement of the parties or for good cause.The ALJ shall issue the prehearing order within one week of the conclusion of the first prehearing conference. The ALJ shall issue orders on non-dispositive motions within eight business days of the conclusion of the non-dispositive motion hearing. The ALJ shall issue orders on dispositive motions within 30 calendar days of the dispositive motion hearing, or if no such hearing takes place, within 30 calendar days of the end of the briefing period.  |
| All programs | Hold hearing | Under RCW 43.101.155(2) the hearing will be held within 90 days after the first prehearing conference (where the hearing date is set) unless another date is set by mutual agreement of the parties or for good cause.The hearings may be held in person or virtually. If hearings are held in person, they will be conducted at the commission’s training facility located at 19010 1ST Avenue S. Burien, WA 98148, unless another location is set by mutual agreement of the parties or for good cause. |
| All programs | Issue decision | OAH will issue the initial order (proposed recommendation) within 45 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, OAH will issue the default or dismissal order within three business days after the receipt of the withdrawal request or the failure to appear.  |

# Exhibit D – Case Age Calculation Methodology

**Case Definition**

An adjudicative proceeding received by OAH, from WSCJTC where OAH has been delegated the authority to receive the case. All appeals of the Commission’s decision will be submitted to the Washington State Superior Court.

**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 request for hearing from WSCJTC until the corresponding closing order is published by OAH, 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.

# Exhibit E – Agency Contacts

|  |  |  |
| --- | --- | --- |
| **Program** | **WSCJTC Contact Person/Contact Information** | **OAH Contact Person/Contact Information** |
| Adjudication Operations – Operational Manager | Kevin ZellerAssistant Directorkzeller@cjtc.wa.gov (206) 835-7337 | Lisa DublinDivision Chief ALJLisa.dublin@oah.wa.gov(253) 548-4130 |
| Billing/Invoices Questions | Brian ElliotFiscal Managerbelliott@cjtc.wa.gov (360) 281-9346 | Deborah FeinsteinFinance ManagerDeborah.feinstein@oah.wa.gov(360) 407-2717 |
| Privacy/Breach Reporting  | Jeff WilcoxIT Managerjwilcox@cjtc.wa.gov (206) 835-7297 | Tiffany ScogginPrivacy OfficerPublicRecords@oah.wa.gov(360) 407-2756 |
| Public Records  | Derek ZableRecords Managementdzable@cjtc.wa.gov(206) 835-7350 | Tiffany ScogginPublic Records OfficerPublicRecords@oah.wa.gov(360) 407-2756 |
| WSCJTC Hearing CoordinatorOAH Legal Administrative Manager | Kayla WoldHearing Coordinatorkwold@cjtc.wa.gov(206) 835-7306 | Hailey MilesLegal Administrative ManagerHailey.miles@oah.wa.gov(253) 476-6881 |

# Exhibit F – Reports

|  |  |  |  |
| --- | --- | --- | --- |
| Applicable? | Report No.  | Report Name | Frequency |
|  | 2001 | Hearings |  |
|  | 2008 | Interpreter Language |  |
|  | 2101 | Intake |  |
|  | 2203 | Continuance |  |
|  | 2205 | Notice Timeliness |  |
|  | 2205a | Notice Timeliness Detail |  |
|  | 2205b | Notice Timeliness Detail – Late Notices |  |
|  | 2301 | Orders Pending |  |
|  | 2302 | Hearing Calendar |  |
|  | 2402 | Default Rate |  |
|  | 2404 | Case Disposition Summary |  |

# Exhibit G – 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 WSCJTC and OAH for the cooperative partnership between OAH and WSCJTC. 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.

1. **Justification and Authority for Data Sharing**

The Data to be shared under this Agreement is necessary to comply with chapter 34.12 and 34.05 RCW, which authorize OAH to conduct administrative adjudications for other state and local government agencies.

1. **Description of Data to be Shared**

OAH and WSCJTC will share data related to administrative hearings. The Data to be shared includes case numbers and other unique identifiers; request for hearing 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.

1. **Methods of Data Sharing and Access**

Data will be transferred from WSCJTC to OAH, as well from OAH to WSCJTC using the OAH Border Services data transfer system.

1. **Location and Retention of Electronic Data**

OAH and WSCJTC each have a data storage system that houses the electronic data to be shared. WSCJTC is the official custodian of the agency record of adjudicative proceeding and has sole responsibility for any retention and archiving of the official record. After transmitting data to WSCJTC, OAH no longer has an obligation to retain the data. OAH’s current practice is to retain case documents for two years after case closure, then delete.

1. **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:

[ ]  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.

[x]  Category 3 – Confidential Information

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

1. Personal Information about individuals, regardless of how that information is obtained;
2. Information concerning employee personnel records;
3. 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:

1. Especially strict handling requirements are dictated, such as by statutes, regulations, or agreements;
2. Serious consequences could arise from unauthorized disclosure, such as threats to health and safety, or legal sanctions.
3. **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.

1. **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.

1. **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.

1. **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 case 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.

1. **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.

1. **Breach Reporting**

OAH will report any Breach of Data shared under this Agreement to WSCJTC’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 WSCJTC 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. The agencies’ contacts for privacy and public records purposes are listed in Exhibit E – Agency Contacts.

1. **Data Security Requirements**

**13.1 Data Transmitting**

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

1. Transmitting the Data within the State Governmental Network (SGN) or receiving party’s internal network; or
2. 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:

* 1. **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.
	2. **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.

* 1. **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.
	2. **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.
	3. **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.

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:

* 1. Encrypt the Data with a key length of at least 128 bits using an industry standard algorithm, such as AES;
	2. Ensure that portable devices such as flash drives are Federal Information Processing Standards (FIPS) Level 2 compliant;
	3. Control access to the devices with a Unique User ID and password or stronger authentication method such as a physical token or biometrics;
	4. 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.
	5. Physically protect the portable device(s) and/or media by:
		1. Keeping them in locked storage when not in use;
		2. Using check-in/check-out procedures when they are shared;
		3. Maintaining an inventory; and
		4. 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 the 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.

* 1. Data must be kept in one of the following ways:
		1. On media (e.g. hard disk, optical disc, tape, etc.) which will contain no non-disclosing party Data; or
		2. In a logical container on electronic media, such as a partition or folder dedicated to disclosing party’s Data; or
		3. In a database that will contain no non-disclosing party Data; or
		4. 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
		5. When stored as physical paper documents, physically segregated from non-disclosing party Data in a drawer, folder, or other container.
	2. 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 1.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, orRemovable media (e.g. floppies, USB flash drives, portable hard disks, Zip or similar disks) | Using a “wipe” utility which will overwrite the Data at least three (3) times using either random or single character Data, orDegaussing sufficiently to ensure that the Data cannot be reconstructed, orPhysically destroying the disk. |
| 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. |

1. **Definitions—Data Sharing and Security**
	1. “Authorized User”means an individual or individuals with an authorized business need to access Confidential Information under this Agreement.
	2. “Border Services” means a type of Windows Communication Foundation (WCF) data services. Border Services links the data storage systems via the State Governmental Network (SGN) and acts as a security barrier to the Data using a secure Partner ID. The Partner ID authenticates and verifies the agency seeking access to the Data.
	3. “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.
	4. “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.
	5. **“**Data” means the case-related information that is transmitted, disclosed or exchanged between OAH and WSCJTC to carry out the purpose of this Agreement. The Data may include paper records as well as electronic records.
	6. “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.
	7. “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.
	8. “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.
	9. “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).
	10. “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.
	11. "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.
	12. “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.