

**TRAFFIC AND CRIMINAL SOFTWARE
DATA SHARING AGREEMENT
BETWEEN
WASHINGTON STATE PATROL
AND
Snoqualmie Police Department**

This Agreement is made and entered into by and between the Washington State Patrol, hereinafter referred to as WSP, and the Snoqualmie Police Department hereinafter referred to as the Agency (collectively referred to as "Party or Parties"). This Agreement is entered into under authority of the Revised Code of Washington 39.34 Interagency Agreements.

PURPOSE

The purpose of this Agreement is to provide the Agency listed above access to the WSP's Traffic and Criminal Software (TraCS). This Agreement defines roles and expectations regarding the Traffic and Criminal Software (TraCS) processes data sharing and use practices, and the method for resolving technical issues.

- ☒ A general authority Washington law enforcement agency as defined in Section 10.93.020 of the Revised Code of Washington
- ☐ A limited authority Washington law enforcement agency as defined in **Click or tap here to enter text.**
- ☐ An Office of a Prosecuting Attorney as defined in Chapter 36.27 of the Revised Code of Washington
- ☐ An "Animal care and control agency" as defined in Chapter 16.52.011(c) of the Revised Code of Washington

THEREFORE, IT IS MUTUALLY AGREED THAT:

1. DEFINITIONS

As used throughout this Agreement, the following terms shall have the meanings set forth below:

"AOC" means the Administrative Office of the Courts.

"Confidential Information" shall mean information that may be exempt from disclosure to the public or other unauthorized persons under either [Chapter 42.56 RCW \(Public Records Act\)](#) or other state or federal statutes. Confidential Information includes, but is not limited to, Personal Information, agency source code or object code, and agency security data.

"DOL" means the Department of Licensing.

"DUI" means Driving Under the Influence.

"eTRIP Committee" means the group comprised of the WTSC, WASPC, WSP, AOC, WSDOT and DOL traffic records governing entities.

"Individually Identifiable Health Information" is a subset of health information, including demographic information collected from an individual and relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual, as set forth in [45 CFR 164.501](#) as currently enacted and subsequently amended or revised.

"JINDEX" means Justice Information Network Data Exchange, an application managed by WaTech.

"LASA" means Local Agency System Administrator.

"NOCC" means Notice of Criminal Citation.

"NOI" means Notice of Infraction.

"Personal Information" means information or set of linked 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 license numbers, e-mail addresses, credit card information, law

enforcement records or other identifying numbers or Protected Health Information, any financial identifiers, and other information that may be exempt from disclosure to the public or other unauthorized persons under either [Chapter 42.56 RCW \(Public Records Act\)](#) or other state and federal statutes.

“PTCR” means Police Traffic Collision Reports.

“Protected Health Information” means Individually Identifiable Health Information that is transmitted by electronic media or transmitted or maintained in any other form or medium, as set forth in [45 CFR 164.501](#), as currently enacted and subsequently amended or revised.

“TraCS Client” means Traffic and Criminal Software.

“WASPC” means the Washington Association of Sheriffs and Police Chiefs.

“WaTech” means Washington Technology Solutions.

“WSDOT” means the Washington State Department of Transportation.

“WSP” means the Washington State Patrol.

“WTSC” means the Washington Traffic Safety Commission.

2. Statement of Work

The Parties to this Agreement shall furnish the necessary personnel, equipment, material, or service(s) and otherwise do all things necessary for or incidental to the exchange of data as set forth in *Attachment A, Statement of Work and Data Security Requirements*.

3. Period of Performance

The period of performance shall commence on the date of the last signature and continue in full force and effect until terminated as provided herein.

4. Payment

This is a non-financial Agreement. In no event shall either Party seek compensation from the other Party for work performed under this Agreement.

5. Records Maintenance

Records and other documents, in any medium, furnished by one party to this agreement to the other party, will remain the property of the furnishing party, unless otherwise agreed. Except as outlined in this agreement or otherwise required by law, the receiving party will not disclose or make available this material to any third party without first giving notice to the furnishing party at least fifteen days in advance of the disclosure. Each party will utilize reasonable security procedures and protections to assure that records and documents provided by the other party are not erroneously disclosed to third parties.

6. Confidentiality

Except as set forth herein or otherwise required by law, the use or disclosure by either Party of any information concerning the other Party for purposes not directly connected with the administration of responsibilities for the services provided under this agreement is prohibited. Each Party shall maintain all information which the other Party specifies in writing as Confidential Information to the extent consistent with Washington State or federal law. The Agency shall have an appropriate agreement with its employees and all others with access to the system to this effect.

6.1 Safeguarding of Confidential Information:

Each Party shall not use or disclose Confidential Information in any manner that would constitute a violation of federal or Washington State law. Each Party agrees to comply with all applicable federal and state laws and regulations, as currently enacted or revised, regarding data security, personal information, and electronic data interchange of Confidential Information.

Each Party shall protect Confidential Information collected, used, or acquired in connection with this Agreement, against unauthorized use, disclosure, modification, or loss. Except as otherwise required by law, each Party shall ensure their directors, officers, employees, subcontractors, or agents use it only for the purposes of accomplishing the services set forth in this Agreement. Each Party and all other

authorized users with access to the system agree not to release, divulge, publish, transfer, sell, or otherwise make it known to unauthorized persons. Additional authorized users may be added to the system or may receive data upon execution of a data sharing agreement between the Parties, the execution of which shall require WSP advanced approval. Each Party agrees to implement physical, electronic, and managerial policies, procedures, and safeguards to prevent unauthorized access, use, or disclosure. The Contractor shall make corrections or amendments to the Personal Information as directed by WSP and incorporate those changes into all the copies maintained by the Contractor or their Subcontractors.

Each Party reserves the right to monitor, audit, or investigate the use of Confidential Information collected, used, or acquired by the other party through this Agreement. The monitoring, auditing, or investigating may include, but is not limited to, Salting. “*Salting*” is the act of introducing data containing unique but false information that can be used later to identify inappropriate disclosure of data.

Each Party shall notify the other Party in writing within 24 hours upon becoming aware of any unauthorized access, use, or disclosure. Each Party shall take necessary steps to mitigate the harmful effects of such use or disclosure. The Party whose data has been subject to any unauthorized access, use, or disclosure, is financially responsible for notification of the unauthorized access, use, or disclosure. The details of the notification must be approved by the other Party. Each Party agrees to defend, protect, and hold harmless the other party for any damages related to unauthorized use or disclosure by their officers, directors, employees, Subcontractors, or agents.

Any breach of this clause may result in termination of the Agreement, suspension of on-line access accounts, or the demand for return of all confidential information.

6.2 Release of Records to State Agencies

The WSP may release records to the WTSC for carrying out the purpose, powers, and duties of the WTSC as defined in RCW 43.59. The WSP may release records to other state agencies with an authorized purpose for receiving records upon request. The WSP will maintain data sharing agreements with external agencies receiving records governed by this agreement.

6.3 Release of Records for Human Subjects Research

“Research” means a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge. Release of confidential records for research shall comply with state and federal human research review processes, as implemented by the Washington State Institutional Review Board.

7. Keep Washington Working / Immigration Law

Under Washington law, the WSP and its personnel are generally prohibited from enforcing federal immigration law. See RCW 10.93.160. Neither WSP nor any of its employees may contract in any way to provide civil immigration enforcement assistance. The purpose of this addendum is to make clear that the parties interpret the attached agreement as consistent with the Washington law, including RCW 10.93.160, in that WSP and its personnel shall not engage in any acts proscribed by Washington law.

Consistent with RCW 10.93.160 and Washington Executive Order 17-01, the parties to this agree not to use or share any information obtained from the WSP, its systems, or its personnel, with any third parties to support or engage in civil immigration enforcement activities.

8. Directive 22-12 Reproductive Health Care Rights

Prohibiting cooperation or assistance with out-of-state abortion and other reproductive health care investigations, prosecutions, or other legal actions

Pursuant to the provisions of RCW 9.02.110, RCW 9.02.120, and the Governor’s Directive 22-12 dated June 30, 2022, the WSP is generally prohibited from cooperating with or providing assistance to out-of-state abortion and other reproductive health care investigations, prosecutions, or other legal actions.

Neither WSP nor any of its employees or subdivisions may contract in any way to provide civil or criminal cooperation or assistance with abortion and other reproductive health care investigations,

prosecutions or other legal actions, including through agreements for task force participation, mutual aid, data sharing, communications dispatch, or any other agreement that shares resources and/or provides data as described herein. WSP shall not use or share WSP resources and/or data, including any individuals' personal information ascertained by the WSP or its personnel, with any third parties to support or engage in abortion or other reproductive health care investigations, prosecutions, or other legal actions.

Therefore, to comply with Governor's directive 22-12 and applicable statutes, the Agency shall not use or share WSP resources and/or data, including any individuals' personal information ascertained by the WSP or its personnel, with any third parties or to support or engage abortion or other reproductive health care investigations, prosecutions, or other legal actions.

The prohibition on information sharing includes place of birth, present location, release date from detention, if applicable, reproductive health care history, and family members' names, absent a court order, judicial warrant, except as may be required by the Public Records Act (PRA), chapter 42.56 RCW. Incidents of disclosure of such personal information shall be considered a breach of this agreement and shall be reported to a designated WSP official.

9. Data Retention Notification

WSP will notify Agency when data sets have met the WSP requirements for destruction and provide Agency 14 (fourteen) days to export any data that they own before WSP submits a destruction request.

10. Independent Capacity

The employees or agents of each party who are engaged in the performance of this Agreement shall continue to be employees or agents of that party and shall not be considered for any purpose to be employees or agents of the other party. WSP staff providing services under the terms of this Agreement shall be under the direct command and control of the Chief of WSP or designee and shall perform the duties required by this Agreement in a manner consistent with WSP policy and regulations, applicable state and local laws, and the Constitutions of the State of Washington and the United States. The assignment of personnel to accomplish the purpose of this Agreement shall be at the discretion of the Chief of WSP or designee.

11. Agreement Alterations and Amendments

This agreement may be amended or altered upon execution of a written mutual agreement of the Parties. Such amendments shall not be binding unless they are in writing and signed by personnel authorized to bind each of the parties.

- 11.2 Changes to the points of contact information may be provided in writing by email to the other Party within 10 days of any such change and enter into a written amendment to memorialize such change.
- 11.3 Without need for written amendment, in its sole discretion, the WSP may require changes in data formats, report forms and other business rules. The Agency will be notified when any changes or updates to these requirements occur, and the Agency shall comply with any such changes.
- 11.4 WSP shall advise the Agency of any changes to *Attachment C, eTRIP Committee Training* within five (5) business days of the change taking affect, without need for written amendment.

12. Termination

Either party may terminate this Agreement upon 30 days' prior written notification to the other party. If this Agreement is so terminated, the parties shall be liable only for performance rendered or costs incurred in accordance with the terms of this Agreement before the effective date of termination.

13. Disputes

If a dispute arises under this Agreement, it shall be determined by a Dispute Board in the following manner: Each party to this Agreement shall appoint one member to the Dispute Board. The members so appointed shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall review the facts,

agreement terms and applicable statutes and rules and make a determination of the dispute. The determination of the Dispute Board shall be final and binding on the parties hereto. As an alternative to this process, either party may request intervention by the Governor, as provided by [RCW 43.17.330](#), in which event the Governor's process will control.

14. Governance

This Agreement is entered into pursuant to and under the authority granted by the laws of the state of Washington, and any applicable federal laws and WSP policy. The provisions of this Agreement shall be construed to conform to those laws and policy.

In the event of an inconsistency in the terms of this Agreement, or between its terms and any applicable statute, rule, or policy, the inconsistency shall be resolved by giving precedence in the following order:

1. The terms of this Agreement
2. Applicable state and federal statutes, rules, and WSP policy;
3. Statement of work; and
4. Any other provisions of the agreement, including materials incorporated by reference.

15. Assignment

The work to be provided under this Agreement, and any claim arising thereunder, is not assignable or delegable by either party in whole or in part.

16. Waiver

A failure by either party to exercise its rights under this Agreement shall not preclude that party from subsequent exercise of such rights and shall not constitute a waiver of any other rights under this Agreement unless stated to be such in a written amendment executed between the parties.

17. Hold Harmless

To the extent allowable by law, each Party shall defend, protect, and hold harmless the other Party from and against all claims, suits and/or actions arising from any negligent or intentional act or omission of that Party's employees, agents, and/or authorized subcontractor(s) while performing under this Agreement.

18. **Rights of Inspection** Each party shall provide right of access to the other party, its officers, or any other authorized agent or official of the state or federal government at all reasonable times, in order to monitor and evaluate the following: Performance, compliance, or quality assurance of internal policies and procedures, or records relating to the safeguarding, use, and disclosure of Confidential Information obtained or used as a result of this Agreement. Each party shall make available information necessary for the other party to comply with a client's right to access, amend, or receive an accounting of disclosures of their Confidential Information.

19. Subcontracting

Subcontractors are not anticipated under this Agreement. However, if Agency desires to subcontract any of the services herein, it must first obtain approval from the WSP. Consent shall not be unreasonably withheld. This clause does not include contracts of employment between a party and their personnel who have been assigned to work under this Agreement. Each party is responsible for ensuring that all terms, conditions, assurances, and certifications set forth in this Agreement are carried forward to any subcontracts.

"Subcontractor" means one not in the employment of a party to this Agreement, who is performing all or part of those services under this contract under a separate contract with a party to this Agreement. The terms "subcontractor" and "subcontractors" mean subcontractor(s) in any tier.

20. Severability

If any provision of this Agreement or any provision of any document incorporated by reference shall be held invalid, such invalidity shall not affect the other provisions of this Agreement which can be given effect without the invalid provision, if such remainder conforms to the requirements of applicable law and the fundamental purpose of this agreement, and to this end the provisions of this Agreement are declared to be severable.

21. Termination of Access

Each party may at its discretion disqualify an individual authorized by the other party from gaining access to data. Termination of access of one individual by either party does not affect other individuals authorized under this Agreement.

22. Filing Requirements

This Contract may be required to be filed with the Department of Enterprise Services pursuant to Chapter 39.26 RCW. No contract so filed is effective nor shall work commence under it until the tenth (10th) working day following the date of filing subject to DES approval.

23. Governing Law

This Contract shall be governed in all respects by the laws of the State of Washington. The jurisdiction for any action hereunder shall be the Superior Court for the State of Washington. The venue of any action hereunder shall be in the Superior Court for Thurston County, State of Washington

24. Antidiscrimination - SB 5186

- 25.1 **Nondiscrimination Requirement.** During the term of this Agreement, Agency shall not discriminate on the bases enumerated at RCW 49.60.530(3). In addition, Agency shall give written notice of this nondiscrimination requirement to any labor organizations with which Agency has a collective bargaining or other agreement.
- 25.2 **Obligation to Cooperate.** Agency shall cooperate and comply with any Washington state agency investigation regarding any allegation that Agency has engaged in discrimination prohibited by this Agreement pursuant to RCW 49.60.530(3).
- 25.3 **Default.** Notwithstanding any provision to the contrary, WSP may suspend Agency may upon notice of a failure to participate and cooperate with any state agency investigation into alleged discrimination prohibited by this Agreement pursuant to RCW 49.60.530(3). Any such suspension will remain in place until WSP receives notification that Agency is cooperating with the investigating state agency. In the event Agency is determined to have engaged in discrimination identified at RCW 49.60.530(3), WSP may terminate this Agreement in whole or in part, and Agency may be referred for debarment as provided in RCW 39.26.200. Agency may be given a reasonable time in which to cure this noncompliance, including implementing conditions consistent with any court-ordered injunctive relief or settlement agreement.

25. Supplier Diversity

This contract is not subject to Subcontractor Payment Reporting.

26. Agency Contacts

The below-listed Contacts for each of the parties shall be responsible for and shall be the contact person for all communications and billings regarding the performance of this Agreement.

The Contacts for the Agency are:	The Contacts for the WSP are:
<i>Gary Horejsi, Interim Chief of Police</i> <i>(Data Sharing Agreement Issues)</i> Snoqualmie Police Department 34825 SE Douglas St Snoqualmie, WA 98065-9220 Phone: 425 888-3333 Email: ghorejsi@snoqualmiewa.gov	<u>Debra Peterman, TraCS Program Manager</u> Washington State Patrol PO Box 42622 Olympia WA 98504-2622 Phone: 253-753-8285 E-Mail: debbie.peterman@wsp.wa.gov <u>Jamie Ralkey, TraCS Support Specialist</u> <i>(Technical Issues and Change Requests)</i> Phone: 360-705-5999 E-Mail: TraCS@wsp.wa.gov

27. Public Disclosure

The Agency acknowledges that WSP is subject to Chapter 42.56 RCW and that this contract shall be a public record as defined in the Public Records Act. Any specific information claimed by the Agency to be proprietary information must be clearly identified as such. To the extent consistent with Chapter 42.56 RCW, the WSP shall maintain the confidentiality of all such information marked as proprietary information. If a public records request is received pursuant to Chapter 42.56 RCW for documents related to this agreement, the WSP will give the contractor ten days' written notice at the Agency's last known address before releasing any documents the Agency has marked as proprietary information. It is the Agency's responsibility to take legal action to obtain an injunction prior to the expiration of the ten days' notice. The Agency will indemnify, defend, and hold harmless the WSP for release of documents related to this contract as required by law. Nothing contained in this Section or any other portion of this agreement affects or modifies the WSP's obligation to disclose public records under Chapter 42.56 RCW or other applicable law.

If the Agency receives a public records request under Chapter 42.56 RCW for any records containing Data subject to this Agreement, Agency agrees to notify the WSP RMD Public Records Officer within five (5) business days and to follow the procedure set out in this section before disclosing any records. The WSP Public Records Officer can be contacted at pubrecs@wsp.wa.gov.

The Agency must provide a copy of the records with proposed redactions to WSP within the time frame required by WSP. WSP will respond within ten (10) business days of receipt of the redacted records to identify concerns with disclosure of the records, propose any changes to the Agency's redactions, or request more time if needed. If the Agency disagrees with any of WSP's concerns or proposed changes, the Agency must notify WSP of that disagreement and provide WSP with a minimum of fifteen (15) business days to obtain a restraining order or injunction under RCW 42.56.540 before disclosing any records.

28. Force Majeure

Neither Party shall be liable to the other or deemed in default under this Agreement if and to the extent that such Party's performance of this contract is prevented by reason of force majeure. The term "force majeure" means an occurrence that is beyond the control of the Party affected and could not have been avoided by exercising reasonable diligence. Force majeure shall include acts of God, war, riots, floods, epidemics, or other similar occurrences. Notification: If either Party is delayed by force majeure, said Party shall provide written notification within forty-eight (48) hours. The notification shall provide evidence of the force majeure to the satisfaction of the other Party. Such delay shall cease as soon as practicable and written notification of same shall be provided. The time of completion shall be extended by contract modification for a period of time equal to the time that the results or effects of such delay prevented the Party from performing in accordance with this contract. Rights Reserved: The state reserves the right to cancel the Agreement during the time of force majeure, and Agency shall have no recourse against WSP.

29. Electronic Signatures

A signed copy of this document or any other ancillary document transmitted by facsimile, email, or other means of electronic transmission shall be deemed to have the same legal effect as delivery of an original executed copy of this document or such an ancillary document for all purposes. Approved signatures shall include wet ink scanned signatures, or certified electronic signatures. Uncertified electronic signatures are not considered valid signatures and shall not be accepted by the WSP.

30. All Writings Contained Herein

This Agreement contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this Agreement shall be deemed to exist or to bind any of the parties hereto. Notwithstanding any provision to the contrary, in no event shall any unilateral documents such as 'click-through agreements,' software or web-based application terms and conditions, or any other unilateral agreement not specifically incorporated herein modify the terms and conditions of this Contract.

IN WITNESS WHEREOF, the parties have executed this Agreement.

STATE OF WASHINGTON
City of Snoqualmie

STATE OF WASHINGTON
WASHINGTON STATE PATROL

Signature
Name: Katherine Ross
Title: Mayor

Date

Signature
Name: Heather Anderson
Title: IT Division Commander

Date

The Agency shall furnish the necessary personnel, equipment, material, or services and otherwise do all things necessary incidental to the performance of work as set forth below.

This Attachment documents the security requirements for transferring, accessing, and protecting WSP's network or data shared under the terms of this Agreement.

1. Description of Data

TraCS has two primary parts:

Part One: The TraCS Client application is used by law enforcement officers and prosecutors across the state of Washington to collect data and to create, print, and file electronically NOI/NOCC, PTCR, DUI Arrest Reports, Warnings/Correction Notices, Tow/Impound Forms, and Marine Law Enforcement Vessel Inspection and Warning forms.

Part Two: The second part is all the eTRIP Committee partner agency applications that receive and process the data collected on the NOI/NOCC, PTCR, DUI Arrest Reports, Warnings/Correction Notices, Tow/Impound Forms, and Marine Law Enforcement Vessel Inspection and Warning forms either through TraCS (or on paper forms).

2. Agency Responsibilities

The Agency certifies that it operates computers to create or review NOI/NOCC, PTCR, DUI Arrest Reports, Warnings/Correction Notices, Tow/Impound Forms, and Marine Law Enforcement Vessel Inspection and Warning forms pursuant to federal, state, and local requirements using TraCS Client. Under this Agreement the responsibilities of the Agency are:

- A) The Agency shall designate LASA as the primary contact for TraCS and who will receive TraCS Administrator training. The LASA shall:
 - Accept modifications to the TraCS Client;
 - Document and submit recommendations for modification of TraCS via the change request process;
 - Manage the connection(s) needed to move data between the TraCS Client to the TraCS database;
 - Provide support for Agency users and reviewers;
 - Update required Agency processes with the parameters of TraCS.
 - Contact WSP Information Technology Division Customer Services to initiate a work order for problem resolution and tracking.
- B) Agency support staff will install TraCS Client software on Agency-owned equipment. The Agency will not share the TraCS Client with others.
- C) The Agency will adhere to the TraCS application standards for the computing environment as published by WSP. The Agency will make its electronic reporting equipment and system secure and prevent unauthorized use. The Agency will ensure Agency equipment maintains current virus checking software. If the Agency equipment becomes infected, the Agency will take all necessary steps to remove the virus and ensure the virus is not transmitted to the TraCS server located at and maintained by WSP.
- D) Agency users and reviewers will transfer PTCRs, NOIs, and NOCCs electronic records regularly and promptly. All Agency users and reviewers will adhere to the training program.
- E) The Agency will be responsible for all required hardware and software purchased for the Agency use of the TraCS Client application and the transmittal of electronic records to WSP, including Agency personnel, operating, maintenance, and data transmission costs. Any costs associated with the Agency interfacing with the TraCS database through JINDEX will be the responsibility of the Agency.

3. WSP Responsibilities

- a. WSP will provide TraCS Client software to the Agency at no charge. Maintenance of the TraCS Client application is provided by a 3rd party vendor Technology Enterprise Group, Inc. (TEG) and the WSP, including maintaining TraCS baseline code, compliance with the business rules, data formats, and standardized forms. WSP will provide a secure environment for electronic data; and retain this data according to federal and state laws and regulations. WSP will also provide the Agency with any evasive action required to protect the TraCS computing environment from significant risk.
- b. WSP will create LASA Accounts; train the LASA; and assist the LASA in administration of agency accounts.
- c. WSP will provide a change request/control process via the ServiceNow application; coordinate change requests describing issues or enhancements through the eTRIP Committee; and provide notification of application modifications.
- d. WSP will transmit NOIs and NOCCs to AOC; and transmit PTCRs to WSDOT and DOL via the JINDEX application.
- e. WSP reserves the right to review and approve Agency equipment security measures; and to suspend or withhold service until such matters are corrected to the reasonable satisfaction of WSP. This includes validation of current virus checking software packages.
- f. WSP will support eTRIP Committee sanctioned training.
- g. WSP Information Technology Division Customer Services will provide first level telephone support twenty-four (24) hours-a-day, seven (7) days-a-week to assist the Agency in resolving problems with the TraCS application. This support is limited to resolutions for routine questions on the TraCS Client application and processes, including troubleshooting and password resets, and using pre-defined policies and procedures. Items not immediately resolved by WSP/ITD/CSU will be escalated to the WSP/ITD/TraCS Support; this higher level of support is provided during regular business hours, Monday through Friday.

Data provided within the context of this Agreement may be confidential, private or may contain sensitive details about PTCRs, notice of infractions (NOI), and notice of criminal citations (NOCC).

4. Use of Data

Except as otherwise outlined in this agreement or required by law, the data provided by either party shall be used and accessed only for the limited purposes of carrying out activities pursuant to this Agreement as described herein. The data shall not be duplicated or disclosed to any third except as authorized in Section 6.1 of the Agreement. Each party shall not use the data provided for any purpose not specifically authorized under this Agreement.

The party to this Agreement that receives personal information from another state agency must protect it in the same manner as the original agency that collected the information pursuant to [Executive Order 00-03](#).

5. Rights in Data

The State of Washington shall be the copyright owner, for all purposes under Title 17 U.S.C., of all data which originates from this Agreement. Data shall include, but not be limited to reports, documents, pamphlets, advertisements, books, magazines, surveys, studies, computer programs, films, tapes, or sound reproductions. Ownership includes the right to use, copyright, patent, register, and transfer these rights.

6. Security of Data

Each party shall take due care to protect the shared data from unauthorized physical and electronic access, as described in this Agreement, to ensure the parties are in compliance with all appropriate federal laws, Criminal Justice Information Services (CJIS) Security Policy as appropriate, and

applicable provisions of the State of Washington Office of the Chief Information Officer (OCIO) security standards.

7. Data Handling Requirements

The handling requirements and protective measures for (Restricted) Confidential data while it is in motion and at rest are as follows:

a. GENERAL ACCESS:

Access to the TraCS System is based on business need-to-know. It is explicitly authorized by the WSP data owner to specific individuals.

b. Transmission of Data:

- i. Electronic file transfer— Secure file transfer (encrypted) required.
- ii. Transmission by mail—Traceable delivery required (e.g., messenger, federal or commercial carrier, certified, return receipt mail).
- iii. Transmission by facsimile to a facility that is not secure is prohibited
- iv. Electronic Mail – Encrypted files/data attached to email required
- v. Portable Storage Media, e.g., CDs, DVDs, USB flash drives, tapes, etc. – Encryption Required

c. Print:

Store in a secured, lockable enclosure.

d. Copying:

Photocopying, equipment use, electronic storage devices to process the photocopied/scanned image. Any electronic storage devices in the photocopying equipment must be either wiped or destroyed upon termination of this agreement

e. Media Disposal:

- i. Printed materials (reports and documents): Destruction is required (recycling is prohibited). Crosscut shredding of printed material is approved. The use of certified, marked, and locked bins to hold printed material until it is shredded is appropriate.
- ii. Removable magnetic or optical storage media (tape, diskettes, CDs): Media must be destroyed or deposited in certified bins specifically designated for magnetic media or "cleaned" using a U.S. Department of Defense-standard data cleaning program and then may be reused. Note: Inoperable electronic media must be destroyed. For example, failed hard disks are not returned to the manufacturer, but are destroyed.

f. Physical Security of Data:

Access to areas containing the data must be physically restricted. Data must be locked when left unattended.

g. Electronic Data at Rest:

If there is a need for data to be stored on any of the Recipient's devices, the Agency must assure unauthorized access cannot take place, including but not limited to session locks with password protection when the computer is on and left unattended. Data stored on non-WSP equipment must be encrypted.

h. Authentication of User Identity:

- i. Authentication from inside a WSP facility for the Agency staff to access internal LAN and computer systems requires user ID and password.
- ii. Authentication for the Agency staff from a location outside of a WSP facility requires strong authentication (e.g., digital certificates, hardware, tokens, biometrics, etc.) is required.

i. Data Recovery:

Loss of the data or equipment. Legal notification to WSP's contract manager is required.

j. Data/Media Disposal:

Upon completion of work, the data collected must be destroyed or returned to WSP. Certification of Data Disposition form (*Attachment D*) is required.

k. Systems Management:

Contractor shall ensure all systems, including portable systems are maintained with all best security practices equal to WSP's including but not limited to:

- Install and maintain commercially available antivirus program
- maintain current levels of security patches on operating systems
- utilize firewalls
- utilize FIPS 140-2 certified encryption software with proper configurations
- maintain physically secure areas for information systems
- monitor logs
- utilize an established incident plan
- report incidents involving WSP data

DATA CLASSIFICATION DECLARATION

Data described in this data sharing agreement is assessed to be in the following data (confidentiality) classification:

☒ **CONFIDENTIAL**

A data classification for data that, due to its sensitive or private nature, requires limited and authorized access. Its unauthorized access could adversely impact the agency legally, financially or damage its public integrity.

☐ **RESTRICTED CONFIDENTIAL**

A data classification for the most sensitive medical and business data within the agency. It is confidential (as defined above); however, with a need for added protection. Its unauthorized access would seriously and adversely impact the organization, its customers, employees, or business partners.

METHOD OF DATA ACCESS

Method of Access/Transfer

The data shall be provided by the WSP in the following format:

- ☐ Encrypted data on CD-ROM
- ☐ Encrypted electronic mail
- ☐ Encrypted files/data attached to electronic mail
- ☐ US or CMS mail
- ☐ Secure file transfer
- ☐ On-line application
- ☐ Network assessment
- ☒ Direct connection to the network –and security information to assure Client connectivity.
- ☐ Other: **Click or tap here to enter text.**

Frequency of Data Exchange

- ☐ One time: data shall be delivered by **Click or tap here to enter text.** (date)
- ☐ Repetitive: frequency or dates **Click or tap here to enter text.**
- ☒ As available

AUTHORIZED ACCESS TO DATA

Access to the data is limited to individual agency staff and business partners who are specifically authorized and who have a business need-to-know. In accordance with the terms contained herein and prior to making the data available, the Agency shall notify all staff with access to the data of the use and disclosure requirements.

1. TRAINING REQUIREMENTS

- a. Training courses conducted within an Agency must be coordinated with the Washington Association of Sheriffs and Police Chiefs (WASPC) TraCS Training Coordinator.
- b. Each agency user must attend a WASPC sponsored training course.
- c. WASPC will provide a course attendee to the WSP for user account creation.