TRAFFIC AND CRIMINAL SOFTWARE (TraCS)

RECORD SHARING AGREEMENT
BETWEEN
WASHINGTON STATE PATROL
AND
CITY OF OLYMPIA

This Agreement is made and entered into by and between the Washington State Patrol, hereinafter referred to as the WSP, and the City of Olympia 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.

The Agency acknowledges that this document is provided in a secured PDF format and is not to be converted to other formats (including but not limited to Microsoft Word) for editing. Any changes made outside of the WSP review process will render the document null and void.

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 record sharing and use practices, and the method for resolving technical issues. Agency is:

- ☒ A general authority Washington law enforcement agency as defined in Section 10.93.020 of the Revised Code of Washington.
- ☐ A Washington Tribal Authority as defined in Section 10.92 of the Revised Code of Washington.
- ☐ A limited authority Washington law enforcement agency as defined in
- ☐ An Office of a Prosecuting Attorney as defined in Chapter 36.27 or Chapter 35A.11 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**"* means Records as defined herein, or information specifically protected from release or disclosure by law under either Chapter 42.56 RCW (Public Records Act) or other state or federal statutes. Confidential Information includes, but is not limited to, information about public employees, lists of individuals for commercial purposes, information about the infrastructure and security of computer and telecommunication networks, and/or personally identifiable information as described herein.

*"**Record Steward**"*: A Record Steward is a guardian of an organization's records, responsible for ensuring its quality, usability, security, and compliance with policies, acting as a bridge between user teams and business users to make Records trustworthy for decision-making.

*"**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.

*"**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.

*"**Personally Identifiable Information (PII**)" means information, Records, or a set of linked information that is identifiable to a specific person, including, but not limited to, information that relates to the person's name, health, finances, education, business, use or receipt of governmental services or other activities such as addresses, telephone numbers, social security numbers, driver's license numbers, email addresses, credit card information, law enforcement records, or other identifying information or Protected Health Information (PHI).

*"**PTCR**"* means Police Traffic Collision Reports.

*"**Records**"* means any paper, correspondence, completed form, bound record book, photograph, film, sound, or video recording, map drawing, machine-readable materials, electronic data (including email), compact disc, or other document, regardless of physical form or characteristics, and including copies thereof, that have been made by or received by any agency, company, or the State of Washington in connection with the transaction of public business, or the work of the department or its employees. For purposes of this Agreement, Records includes, without limitation source code, NOIs, NOCCs, PTCRs, DUI Arrest Reports, and other forms that are created, collected, or transmitted into the TraCS system and stored, and used by the Parties specific to the TraCS application as described herein.

*"**Research**"* means a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.

*"**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.

*"**TraCS**"* means Traffic and Criminal Software.

*"**User**"* means any Agency Personnel that have TraCS User Accounts.

*"**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 Records as set forth in *Attachment A (Statement of Work for 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 superseded by a new agreement or 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 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 these Records 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 ensure that the Records 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 ensure that its employees and all others with access to the system adhere to this requirement.

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 Records security, PII, and electronic 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 Records 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.

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 Records containing unique but false information that can be used later to identify inappropriate disclosure of Records.

Each Party shall notify the other Party in writing within 24 hours upon becoming aware of any unauthorized access, use, or disclosure of Confidential Information. Each Party shall take necessary steps to mitigate the harmful effects of such use or disclosure. The Party, whose Records have 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 both Parties. The reviewing Party shall approve or provide specific, actionable objections to the proposed notification within 48 hours of receipt, or approval shall be deemed granted. Each party shall be responsible for the acts, errors, and omissions of itself and its own officers, employees, and agents acting within the scope of their authority and within the scope of the performance of this Agreement.

Any unauthorized release of Confidential Information may result in termination of the Agreement, suspension of on-line access accounts, or the demand for return of all Confidential Information. Each Party warrants that its agents, employees, Authorized Users, or subcontractors are bound to all confidentiality and security obligations of this Agreement.

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 Records sharing agreements with external agencies receiving records governed by this Agreement.

6.3 Release of Records for Human Subjects Research

Release of Confidential Information for human subject 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 provision is to make clear that the Parties interpret this Agreement as consistent with Washington law, including RCW 10.93.160, and that the WSP and its personnel shall not engage in any acts prohibited by Washington law.

The Parties to this Agreement agree not to use or share any information obtained from the TraCS system, the WSP, its systems, or its personnel, with any third parties to support or engage in civil immigration enforcement activities prohibited by RCW 10.93.160 and/or WA Executive Order 17-01.

8. Directive 22-12 Reproductive Health Care Rights

This Directive prohibits 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 the 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 (Record) sharing, communications dispatch, or any other agreement that shares resources and/or provides Records as described herein. the WSP shall not use or share WSP resources, Records, or Confidential Information or other 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 any Confidential Information and/or Records, with any third parties or to support or engage in 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 or 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. Records Retention Notification

WSP will notify Agency when Records owned by the Agency have met the WSP requirements for destruction. WSP will provide Agency 14 (fourteen) days to export any Records owned by the Agency 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 for all purposes 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. Personnel of either Party providing services under the terms of this Agreement shall be under the direct command and control of that Party's Chief or appropriate authority or designee and shall perform the duties required by this Agreement in a manner consistent with respective Party's 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 respective Party's Chief or appropriate authority 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.

11.1 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.

11.2 Without need for written amendment, in its sole discretion, the WSP may require changes in Records 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.

11.3 WSP shall advise the Agency of any changes to *Attachment C (eTRIP Committee Training)* within five (5) business days of the change taking effect, 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. Applicable federal and state statutes and rules;
2. The terms of this Agreement;
3. Statement of Work for Data Security Requirements (Attachment A);
4. WSP Policy; and
5. Any other provisions of the Agreement, including material 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. Subcontracting

Subcontractors are not allowed under this Agreement.

19. 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.

20. Termination of Access

Each Party may at its discretion disqualify an individual authorized by the other Party from gaining access to Records or Confidential Information. Termination of access of one individual by either Party does not affect other individuals authorized under this Agreement. The Party requiring disqualification shall notify the other Party of the disqualification within 48 business hours of the event.

21. Filing Requirements

This Agreement may be required to be filed with the Department of Enterprise Services pursuant to Chapter 39.26, 39.34.040, and 34.080 RCW. No contract so filed is effective nor shall work commence under it until the tenth (10th) working day following the date of filing.

22. Governing Law

This Agreement 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

23. Antidiscrimination - SB 5186

23.1 ***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.

23.2 ***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).

23.3 ***Default***. Notwithstanding any provision to the contrary, WSP may suspend Agency 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.

24. Supplier Diversity

This Agreement is not subject to Subcontractor Payment Reporting.

25. 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:
Steven J. Burney *(Signing Authority Name)* *(Record Sharing Agreement Issues)* City of Olympia 601 4th Ave E Olympia WA 98501 Phone: 360-753-8300 Email: jburney@ci.olympia.wa.us	Debra Peterman, TraCS Program Manager Washington State Patrol PO Box 42622 Olympia WA 98504-2622 Phone: 253-753-8285 Email: debbie.peterman@wsp.wa.gov Jamie Ralkey, TraCS Support Specialist *(Technical Issues and Change Requests)* Phone: 360-705-5999 Email: TraCS@wsp.wa.gov

26. Public Disclosure

The Parties acknowledge that both Parties are subject to Chapter 42.56 RCW and that this Agreement shall be a public record as defined in the Public Records Act. Any specific information claimed by either Party to be proprietary information must be clearly identified as such. To the extent consistent with Chapter 42.56 RCW, the Parties shall maintain the confidentiality of all such information marked as proprietary information. If a public records request for a copy of this Agreement is received pursuant to Chapter 42.56 RCW, or if a public records request is received for Confidential Information, or other documentation related to the TraCS system, the receiving Party will give the furnishing Party ten days' written notice at the furnishing Party's last known address before releasing any documents that Party has marked as proprietary information. It is furnishing Party's responsibility to take legal action to obtain an injunction prior to the expiration of the ten days' notice. To the extent allowable by law, the furnishing Party will indemnify, defend, and hold harmless the receiving Party 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 either Party's obligation to disclose public records under Chapter 42.56 RCW or other applicable law.

If either Party receives a public records request under Chapter 42.56 RCW for any records containing information subject to this Agreement, the receiving Party agrees to notify the other Party's 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 Section can be contacted at pubrecs@wsp.wa.gov.

The receiving Party must provide a copy of the records with proposed redactions to the furnishing Party within the time frame required by WSP Public Records Section. The furnishing Party 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 receiving Party's redactions, or request more time if needed. If the receiving Party disagrees with any of the furnishing Party's concerns or proposed changes, the receiving Party must notify the furnishing Party of that disagreement and provide them with a minimum of fifteen (15) business days to obtain a restraining order or injunction under RCW 42.56.540 before disclosing any records.

27. 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 reasonable 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: Either Party reserves the right to cancel the Agreement during the time of force majeure, and the other Party Agency shall have no recourse against the cancelling Party.

28. 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.

29. 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 Agreement.

Each party to this document, and each individual signing on behalf of each party, hereby represents and warrants to the other that it has full power and authority to enter into this document and that its execution, delivery, and performance of this document has been fully authorized and approved, and no further approvals or consents are required to bind each party.

IN WITNESS WHEREOF, the Parties have executed this Agreement.

STATE OF WASHINGTON City of Olympia	STATE OF WASHINGTON WASHINGTON STATE PATROL
Signature Date Name: Steven J. Burney Title: City Manager	Signature Date Name: Christopher Anderson Title: Information Technology Division Commander

Attachment A:
Statement of Work for
Data Security Requirements

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 A documents the security requirements for transferring, accessing, and protecting WSP's network, Records, or Confidential Information shared under the terms of this Agreement**.**

1. Description of Records

TraCS Records consist of three primary parts:

Part One: The TraCS Forms Manager 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 TraCS Configuration Manager is used by Local Agency System Administrators (LASA) to manage Agency User Accounts

Part Three: All eTRIP Committee partner agency applications that receive and process Records collected on the NOI/NOCC, PTCR, DUI Arrest Reports, Warnings/Correction Notices, Tow/Impound Forms, and Marine Law Enforcement Vessel Inspection and Warning forms and all other TraCS Forms, current or future, 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. 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:
   - Document and submit recommendations for modification of TraCS via the change request process;
   - Manage the connection(s) needed to move Records between the TraCS application to the TraCS database;
   - Provide support for Agency Users and reviewers;
   - Update required Agency processes with the parameters of TraCS; and
   - Contact the WSP Information Technology Division Customer Services to initiate a work order for problem resolution and tracking.

b. Agency support staff will install TraCS software on Agency-owned equipment. The Agency will not share the TraCS installation package with any third party not specifically bound by the confidentiality obligations of this Agreement.

c. The Agency will adhere to the TraCS application standards for the computing environment as published by WSP and documented in the Agency application for use of the TraCS system. 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 the WSP.

d. Agency Users and reviewers will send/transmit 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 application and the transmittal of electronic records to the WSP, including Agency personnel, operating, maintenance, and Records 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. The WSP will provide TraCS software to the Agency at no charge. Maintenance of the TraCS Client application is provided by a third-party vendor Technology Enterprise Group, Inc. (TEG) and the WSP, including maintaining TraCS baseline code, compliance with the business rules, Records formats, and standardized forms. the WSP will provide a secure environment for electronic Records, and retain these Records according to federal and state laws and regulations. the WSP will also provide the Agency with any evasive action required to protect the TraCS computing environment from significant risk.

b. The WSP will create LASA accounts, train the LASA, and assist the LASA in administration of agency accounts.

c. The 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 at least 30 days in advance of implementation, unless the change is required for immediate security or compliance purposes.

d. The WSP will transmit NOIs and NOCCs to AOC, and transmit PTCRs to WSDOT and DOL via the JINDEX application.

e. The WSP reserves the right to review and approve Agency equipment security measures and to suspend or withhold service if a security risk to the TraCS exists or if the Agency fails to correct a known security deficiency with a reasonable time. The WSP shall provide the Agency with written notice of the required correction and the reason for the suspension. Service will be restored upon correction of the security issue to the reasonable satisfaction of the WSP. This includes validation of current virus checking software packages.

f. The WSP will provide system requirements to Agency during the application process and will answer questions when asked by the Agency regarding security and system requirements.

g. The WSP will support eTRIP Committee sanctioned training.

h. The 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 system. Agencies may call (360) 705-5999 to request support. This support is limited to resolutions for routine questions on the TraCS application and processes, including troubleshooting and password resets, and using pre-defined policies and procedures. Items not immediately resolved by the 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.

4. Use of Records

Except as otherwise outlined in this Agreement or required by law, the Records 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 Records 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 Records provided for any purpose not specifically authorized under this Agreement.

Attachment A:
Statement of Work for
Data Security Requirements

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. Copyrights

For all purposes under Title 17 U.S.C., the State of Washington shall be the copyright owner of all copyrightable material which originates from this Agreement, including but not 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. Notwithstanding the foregoing, Agency shall retain copyrights on all Agency owned copyrightable materials.

6. Security of Records

Each Party shall take due care to protect the shared Records 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. Records Handling Requirements

The handling requirements and protective measures for (Restricted) Confidential Information or Records while in motion and at rest are as follows:

a. *GENERAL ACCESS:*
Access to the TraCS application is based on business need-to-know. It is explicitly authorized by the WSP Record owner to specific individuals.

b. *Transmission of Records:*
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/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 and lockable enclosure.

d. *Copying:*
Photocopying equipment use electronic storage devices to process the photocopied/ scanned images. 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 (Records):*
Access to areas containing the Data (Records) must be physically restricted. Records must be locked when left unattended.

g. Electronic Records at Rest:

If there is a need for Records 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. Records stored on non-WSP equipment must be encrypted utilizing FIPS 140-2 certified encryption software as required by Section J(iv) below.

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.).

i. Records Recovery:

If either Party experiences loss of the Records or equipment obtained or maintained pursuant to this Agreement, that Party shall promptly provide written notification to the other Party's Contract Manager.

j. Systems Management:

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

i. Install and maintain commercially available antivirus program
ii. Maintain current levels of security patches on operating systems
iii. Utilize firewalls
iv. Utilize FIPS 140-2 certified encryption software with proper configurations
v. Maintain physically secure areas for information systems
vi. Monitor logs
vii. Utilize an established incident plan
viii. Report incidents involving WSP Data

Attachment B:
Data Classification and Method of Data Access

RECORDS CLASSIFICATION DECLARATION

Records described in this Data Sharing Agreement are assessed to be in the following 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 RECORDS 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:

Frequency of Records Exchange

☐ One time: Records shall be delivered by (date)
☐ Repetitive: frequency or dates
☒ As available

AUTHORIZED ACCESS TO RECORDS

Access to the TraCS Records 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 Records available, the Agency shall notify all staff with access to the Records of the use and disclosure requirements.

Attachment C:
eTRIP Committee Training

1. TRAINING REQUIREMENTS

a. Training courses conducted 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 list to the WSP for User account creation.