WASHINGTON STATE PATROL (WSP)

LIVESCAN TO WIN ABIS USER AGREEMENT

This Agreement, entered into between the Washington State Patrol (hereinafter referred to as "***WSP***"), an agency of the State of Washington; and Yakima Police Department, (hereinafter referred to as "***the User***"), witnesses that:

The WSP is an agency of the State of Washington authorized by law to establish and operate an Automated Biometric Identification System (ABIS) capable of, but not limited to, reading, classifying, matching, and storing fingerprints, and maintaining information based on fingerprint identification. ABIS forwards the criminal history record information to the Washington State Identification System (WASIS) where it is stored and maintained by the WSP.

The WSP has entered into agreement with the Western Identification Network (WIN) for ABIS services. The WIN supports ABIS processing for the following eight states: Alaska, Idaho, Montana, Nevada, Oregon, Utah, Washington, and Wyoming.

The User may utilize Livescan equipment to capture biometric fingerprint images and record related personal identifiable information and submit to ABIS for authorized purposes as allowed by state and federal statutes.

NOW THEREFORE, in light of the foregoing representations and the promises, conditions, and other valuable considerations more fully set out or incorporated herein by reference, the parties, by their duly authorized officials, do mutually agree as follows:

I. PERIOD OF PERFORMANCE

This agreement replaces any previous Livescan to WIN ABIS User Agreement between the WSP and the User. This agreement is effective on the date of the last signature and continues until status of services or the User signatory changes.

II. DEFINITIONS

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

"Confidential Information" means information that may be exempt from disclosure to the public or other unauthorized persons under either chapter 42.56 RCW or other state or federal statutes. Confidential Information includes, but is not limited to, Personal Identifiable Information (PII), agency source code or object code, and agency security data, including Livescan data as described herein.

"*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.

III. SECURITY REQUIREMENTS

This section will outline security requirements in reference to Livescan devices defined as devices that collect, process, store, communicate, retrieve, display, or print Livescan information.

WSP recognizes that the FBI CJIS Security Policy is a minimum standard and that circumstances are encountered that create a need for additional security measures.

These standards are in addition to the current CJIS Security Policy.

a. Livescan devices will comply with the following security requirements:
    i. Unauthorized unescorted physical and logical access to Livescan devices will be restricted. In some environments, it might not be realistic to expect absolute control over a Livescan device 100% of the time. In these environments, acceptable risk mitigations will be provided in lieu of 100% control through escorted access. The WSP reserves the right to object to equipment security measures and to suspend or withhold service until such matters are corrected to the reasonable satisfaction of WSP.
    ii. Livescan devices will be single purpose workstations. That is, applications used on the workstation will be used only for functions involving Livescans.
    iii. Livescan devices will have restricted internet access (i.e. authorized vendor support).
    iv. Livescan devices will not host email clients that can receive email from the internet.
    v. Livescan devices will not be used to display or edit documents except for reports produced by the Livescan device (word processing, spreadsheets, PDF's, etc.),
    vi. Livescan devices will not be connected to any external media, except for the purpose of performing software and application upgrades. The media should be used only on Livescan devices. If the media is used on a non-Livescan device, it will be erased and a new image will be placed on the media before it is used with a Livescan device.
    vii. Livescan devices will be protected from workstations that do have general workstation functions by firewalls that prohibit external access to Livescan devices.
    viii. The Livescan will be located in an area that is physically restricted to the public or other unauthorized users. When the Livescan is not in use and left unattended, it must be logged off and password protected. In the cases of portable Livescans, the Livescan will not be left unattended in a non-secure area.

b. All security exceptions must be documented in writing and approved by WSP and WIN.

c. The threat vectors currently addressed are:
    i. Physical access issues
    ii. Multiple/shared function (due to security issues raised by co-resident applications)
    iii. Unrestricted internet access
    iv. Email access
    v. Accessing documents that could have been maliciously crafted
    vi. External media
    vii. Contact with other workstations over the local network segment that are at higher risk for infection/compromise
    viii. Lack of firewall separation/overly permissive firewall configuration

IV. SYSTEMS MANAGEMENT

(User Agency) shall ensure all Livescan systems, including portable systems are maintained with the best security practices including but not limited to:

a. updating antivirus
b. maintaining current levels of security patches on operating systems
c. utilize firewalls
d. maintain physically secure areas for information systems
e. report any breaches to the WSP Criminal Records Division

V. OTHER TERMS AND CONDITIONS

By signing this agreement, the WSP and the User will mutually agree to the following:

a. The WSP will provide the User, as allowed, with information available in WASIS, ABIS and WIN ABIS files. The WSP will serve as the means of exchange of computerized criminal history information and biometric data.

b. The network connection will be made via an approved method identified by WSP.

c. The User will submit Livescan data (fingerprints, palm prints, mug shots, etc.) and related demographic information electronically to the WSP for the purpose of identification and when applicable, inclusion to the WIN ABIS and WASIS.

d. For applicant submissions requiring a fee, the User will establish a billing account with the WSP. By establishing a billing account, the User agrees to collect, hold, and reconcile fees charged by WSP. If a submission is sent in error, the User is responsible for all fees associated with that submission.

e. The User agrees that WSP will provide authorization to connect to the ABIS and WIN ABIS databases with certain restrictions as follows:
    i. The User will submit Livescan data and related demographic information for identification search and possible inclusion in ABIS, WASIS, and WIN ABIS databases as allowed by statute.
    ii. The User agrees to comply with statutory mandates concerning the submission of criminal and civil fingerprint submissions to WSP.

f. The User is responsible for all personnel, operating, maintenance and data transmission costs to submit Livescan data and related demographic information as required under state statutes and/or local ordinances.

g. The User agrees to assign a Livescan point of contact to serve as the primary contact person for any Livescan to ABIS connection related issues. The User must notify WSP as soon as possible if the Livescan point of contact changes.

h. The WSP will schedule and provide Livescan training to User personnel at locations and times specified by WSP. Livescan training may also be provided by the Livescan vendor.

VI. COMPLIANCE

a. The User will operate Livescan equipment and maintain strict compliance with applicable policies and procedures as identified in this Agreement.

b. Fingerprint identification and/or criminal history record information will not be further disseminated by the User to any other person (private or public) or entity, except as required in criminal proceedings pursuant to state and/or federal laws.

c. Users submitting Livescan data and related demographic information via Livescan to the WSP are subject to audit per FBI CJIS Security Policy standards.

VII. SUSPENSION AND TERMINATION

a. The WSP may suspend services hereunder when, in its reasonable estimation, the User has breached any material term of the Agreement. For the purposes of this Agreement, the violation of any specific term of this Agreement or of any substantive requirement or limitation imposed by the federal or state statutes, regulations, or rules incorporated into this Agreement will be deemed a breach of material term of the Agreement.

b. The WSP may terminate this Agreement if the User commits any material breach of any term of this Agreement, which breach is not corrected within thirty (30) business days after receipt of notice from WSP. Both parties may, by mutual agreement, terminate this Agreement on terms acceptable to them.

c. Neither the WSP nor the User will be liable for any indirect, incidental, consequential or special damage under this agreement arising solely from the termination of this Agreement in accordance with its terms.

VIII. HOLD HARMLESS

To the extend allowed by law, the User agrees to hold harmless the WIN and its employees and the State of Washington, the WSP and its employees from and against any and all claims, demands, actions, suits, including but not limited to, any liability for damages by reason of or arising out of any misuse of the ABIS, WASIS and WIN ABIS databases, erroneous identifications, or any cause of action whatsoever, against any loss, cost, expense, and damage resulting therefrom, including attorney fees.

IX. RECORDS MAINTENANCE AND INSPECTION

The parties to this Agreement shall each maintain books, records, documents, and other evidence which sufficiently and properly reflect all direct and indirect delivery, receipt, safeguarding, and uses of the Data shared under this Agreement. These records shall be subject to inspection, review, or audit by personnel of each party, or other personnel authorized by either party, the Office of the State Auditor, and federal officials authorized by law. Each party shall retain all books, records, documents, and other material relevant to this Agreement in accordance with the state retention schedules applicable to their agency. The Office of the State Auditor, federal auditors, and any persons authorized by either party shall have full access and the right to examine any of these materials during this period.

X. CONFIDENTIALITY

Data provided pursuant to this Agreement includes Confidential, Personal identifiable information (jointly “Confidential Information”). Each Party acknowledges and agrees that it has a continuing obligation to comply with all federal and state laws, regulations, and security standards as enacted or revised over time, regarding Data Security, electronic data interchange and restricted Permissible Uses of such information. As agencies of the state of Washington, these standards must minimally meet all regulations set forth by the Office of the Chief Information Officer (OCIO) under OCIO policy 141.10.

XI. SAFEGUARDING OF CONFIDENTIAL INFORMATION

Each Party shall protect and safeguard all Confidential Information provided under this Agreement against any and all unauthorized disclosure, use, or loss because each party is regulated by OCIO standards for the safeguarding of Confidential Information, each party must conform to its own standards.

Each party shall notify the other party in writing within 24 hours upon becoming aware of any unauthorized access, use, or disclosure of Confidential Data. Each party shall take necessary steps to mitigate any and all harmful effects of such use or disclosure.

XII. AUDIT

Both parties are obligated to maintain current standing with all OCIO audit requirements. Additionally, WSP reserves the right to monitor, audit, or investigate the use of Confidential Information collected, used, or acquired by the User through this Agreement.

XIII. DISPUTES

In the event that 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.

XIV. 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:

a. Applicable state and federal statutes;
b. OCIO policy 141.10 and rules and WSP policy;
c. Terms and Conditions of this Contract

XV. 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, without the express prior written consent of the other party. Consent shall not be unreasonably withheld.

XVI. 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 writing signed by an authorized representative of the party and attached to the original Agreement.

XVII. 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.

XVIII. SUBCONTRACTING

A party may only enter into subcontracts for any of the work or services under this contract if it first receives written approval from the other party. 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 all subcontracts.

If the User grants any subcontractor access to any confidential information, it must first carry forward all terms, conditions, and restrictions of this agreement to the subcontractor. The User remains responsible for any violation committed by a subcontractor.

XIX. 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.

XX. 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.

XXI. CONTRACT MANAGEMENT

The contract manager 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.

Contract Manager for Yakima Police Department:	Contract Manager for WASHINGTON STATE PATROL:
Ms. Jeannett Mora Yakima Police Department 200 S 3rd St Yakima WA 98902 Phone: (509) 575-6201 E-Mail: jeannett.mora@yakimawa.gov	Deborah Collinsworth Identification and Background Check Section Manager Criminal Records Division PO Box 42619 Olympia WA 98504-2619 Phone: (360) 534-2102 E-Mail: deborah.collinsworth@wsp.wa.gov

XXII. The following documents are incorporated by reference and made part of this agreement:

1. FBI CJIS Security Policy - The FBI CJIS Security Policy can be found at https://www.fbi.gov/file-repository/cjis-security-policy-v5_6_20170605.pdf/view. WSP will provide a copy of the manual upon request.
2. Applicable federal and state laws and regulations

As an agency head/director, I hereby acknowledge the duties and responsibilities set forth in this Livescan to WIN ABIS User Agreement, as well as those documents incorporated by reference. I acknowledge that these duties and responsibilities have been developed to ensure system integrity and security. I also acknowledge that failure to comply with these duties and responsibilities will subject my agency to various sanctions. These sanctions may include the termination of services to submit fingerprint information to the WSP.

The parties signing below warrant that they have read and understand this Contract and have the authority to enter into this Contract.

Livescan User Agency Name	Yakima Police Department	
Agency ORI	WA0390500	
Agency Head Name	Cliff Moore, City Manager	
Agency Head Email	cliff.moore@yakimawa.gov	
Agency Head Telephone Number	(509) 575-6040	
Agency Head or Designee Signature		Date

WSP Agency Head or Designee Name	Ms. Deborah Collinsworth	
Title	Identification and Background Check Section	
WSP Agency Head or Designee Signature		Date