



WASHINGTON STATE PATROL (WSP)

A Central Computerized Enforcement Service System (ACCESS)

2023 USER ACKNOWLEDGMENT

I. Introduction

Since its inception, the National Crime Information Center (NCIC) has operated under a shared management concept between the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Division and state users. The NCIC Advisory Policy Board established a single state agency in each state to assume responsibility as the NCIC CJIS Systems Agency (CSA) for all agencies within the state. The CSA is responsible for the planning of necessary hardware, software, funding, security, auditing, and training of all authorized agencies within the state for complete access to FBI CJIS systems. The CJIS Systems include, but are not limited to: the Interstate Identification Index (III); NCIC; Uniform Crime Reporting (UCR); summary or incident-based reporting to the National Incident- Based Reporting System (NIBRS); Fingerprint Identification Record System; National Data Exchange (N-DEX); Law Enforcement Enterprise Portal (LEEP); and the National Instant Criminal Background Check System (NICS). The WSP Criminal Records Division (CRD) Administrator is designated as the NCIC CJIS Systems Officer (CSO). The FBI CJIS Division requires the CSO to manage the following:

1. Operational, technical, and investigative assistance.
2. Telecommunications lines to state, federal and regulatory interfaces.
3. Legal and legislative review of matters pertaining to all CJIS systems.
4. Timely information regarding all aspects of CJIS systems and other related programs by means of the ACCESS Operations Manual, NCIC Operating Manual, NCIC Code Manual, CJIS Security Policy, Technical and Operational Updates (TOU), and related documents.
5. Training and training materials to all participating agencies.
6. System security to include physical security, personnel, and all technical aspects of security as required in the CJIS Security Policy.

The following documents are incorporated by reference and made part of this user acknowledgment:

1. ACCESS Operations Manual: <http://www.wsp.wa.gov/secured/access/manuals.htm>
2. CJIS Security Policy: <https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center/view>
3. U.S. Code of Federal Regulations, Title 28, Part 20
4. Applicable federal and state laws and regulations; ACCESS/WACIC rules, regulations, and policies as recommended by the ACCESS Section

II. Primary Connection and Originating Agency Identifier (ORI) Issuance

All agencies that inquire on or enter data into ACCESS must have a primary connection to ACCESS and a signed WSP ACCESS User Acknowledgment on file prior to adding secondary connections such as regional management systems. Agencies must ensure that all system use, through both the primary or secondary connections, remain in compliance with ACCESS and FBI CJIS rules.

The CSO will coordinate the assignment of new ORI numbers, the change in ORI location or address, and any other changes, cancellations, or retirements of ORIs accessing WACIC/NCIC. The assignment of an ORI to an agency is not a guarantee of access to the state and federal systems. The CSA makes the final determination of who may access WACIC/NCIC based on the standards provided by the CJIS Security Policy and determination of an agency's administration of criminal justice. Any requests for additional ORIs by an agency will be forwarded to the ACCESS Section, who will conduct a short audit of the agency to verify compliance standards are being met. See the ACCESS Operations Manual Introduction for more information.

III. Indemnification

The parties acknowledge that each party is liable for the negligent or wrongful acts or omissions of its agents and employees while acting within the scope of their employment as permitted by applicable law, including, but not limited to, the Federal Tort Claims Act, 28 U.S.C. Section 1346(b), 2401-2416.

IV. Administrative Responsibilities

The agency shall respond to requests for information by the FBI CJIS Division or ACCESS in the form of questionnaires, surveys, or similar methods, to the maximum extent possible, consistent with any fiscal, time, or personnel constraints of that agency.

All agencies are required to have formalized written procedures for the following, if applicable: validations, hit confirmation, criminal history use and dissemination, ACCESS misuse, record entry (for all record types entered into WACIC and NCIC), background re-investigations, password management, disposal of media, physical protection, NICS appeal process, and a network drawing.

The CSO provides system training to agencies accessing WACIC/NCIC through the state computer system. If employees are using inquiry only functions, they must attend Level 1 certification training. Employees entering information into the WACIC/NCIC system must attend Level 2 certification training. All certifications must be acquired within six months of hire date and renewed biennially.

Security awareness training is required within six months of initial assignment, and biennially thereafter, for all personnel (who are not ACCESS certified) that have unescorted access to Criminal Justice Information (CJI), or to the secure area where CJI is stored. This includes agency employees, custodial staff, Information Technology (IT) staff, upper management, etc. Records of individual basic security awareness training shall be documented, kept current, and maintained by each agency for review during the triennial ACCESS or Technical Security audit.

A Terminal Agency Coordinator (TAC) must be assigned for each terminal agency. This person is the Point of Contact (POC) for the agency. A TAC must maintain a Level 2 ACCESS certification. The TAC retains the responsibility of ensuring his/her agency is in compliance with state and FBI CJIS Division policies and regulations. A TAC must attend TAC training within six months of being assigned the TAC duties and then at least once every three years thereafter. The TAC may attend multiple classes, if desired.

For those agencies providing ACCESS services through regional computer systems to outside agencies, the TAC shall be responsible for the dissemination of all administrative messages received on the 24 hour printer to those agencies.

The CSO provides the criminal justice community with the current ACCESS Operations Manual, NCIC Operating Manual, NCIC Code Manual, and CJIS Security Policy. The TAC will be notified immediately of any updates. The agency shall incorporate such changes when notified. Information is provided via email and can be found on the ACCESS website at the following link: http://www.wsp.wa.gov/_secured/access/access.htm.

V. Fees

Every criminal justice agency that has a connection to the ACCESS switch is responsible for fees associated with the amount of transactions processed. All fees are transaction based. See the Fee Explanation for the current rates. http://www.wsp.wa.gov/_secured/access/access.htm

VI. Criminal Justice Information (CJI) Responsibilities

Each agency shall conform to system policies, as established by the FBI CJIS Division and ACCESS, before access to CJI is permitted. This will allow for control over the data and give assurance of system security.

1. The rules and procedures governing terminal access to CJI shall apply equally to all participants in the system.
2. All criminal justice agencies with ACCESS terminals and access to computerized CJI data from the system shall permit an FBI CJIS Division and an ACCESS audit team to conduct appropriate audits. Agencies must cooperate with these audits and respond promptly.
3. All terminals interfaced directly with the ACCESS/WACIC/NCIC systems for the exchange of CJI must be under the management control of a criminal justice agency, as defined by the CJIS Security Policy.
4. All agencies must ensure they provide all required information when running criminal justice information.
5. WSP retains access to all agency criminal history logs through the ACCESS System. Secondary dissemination of criminal history must be logged by the agency

VII. Prohibition on Use

Immigration Enforcement Activities

Under Washington's Keep Washington Working (KWW) law, RCW 10.93.160, state and local law enforcement agencies are generally prohibited from enforcing federal immigration law. This prohibition is in recognition of the fact that, standing alone, an individual's unauthorized presence in the United States is not a violation of state or local law.

Therefore, to comply with KWW, no criminal justice agency shall use or share ACCESS, or any information obtained through ACCESS, to support or engage in immigration enforcement activities. The prohibition on information sharing includes place of birth, present location, release date from detention, if applicable, and family members' names, absent a court order, judicial warrant, or 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.

Out-of-State Abortion and Other Reproductive Health Care Enforcement Activities

Pursuant to the provisions of RCW 9.02.110, RCW 9.02.120, and the Governor's Directive 22-12.1 dated February 1, 2023, the WSP is generally prohibited from knowingly cooperating with or providing assistance to out-of-state abortion and other reproductive health care investigations, prosecutions, or other legal actions, unless necessary to comply with Washington or federal law.

Neither WSP nor any of its employees, contractors, or agents 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, unless necessary to comply with Washington or federal law. 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 knowingly support or engage in abortion or other reproductive health care investigations, prosecutions or other legal actions, unless necessary to comply with Washington or federal law.

Therefore, to comply with Governor's directive 22-12.1 and applicable statutes, no criminal justice agency shall 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 knowingly support or engage abortion or other reproductive health care investigations, prosecutions, or other legal actions, unless necessary to comply with Washington or federal law.

The prohibition on information sharing includes, but is not limited to, place of birth, present location, release date from detention, if applicable, reproductive health care history, and family members' names, unless necessary to comply with Washington or federal law to include the Public Records act, 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.

VIII. Record Entry Responsibilities Record Quality

Criminal justice agencies have a specific duty to maintain records that are accurate, complete, and current. ACCESS recommends agencies conduct self-audits as a means of verifying the completeness and accuracy of the information in the system. These self-assessments should be on a continual basis to ensure both quality assurance and compliance with standards. Errors discovered in NCIC records are classified as serious errors or non-serious errors.

Serious errors: FBI CJIS will cancel the record and notify the entering agency via administrative message. The message provides the entire canceled record and a detailed explanation of the reason for cancellation.

Non-serious errors: The CSA notifies the ORI by email of the corrective action to be taken. No further notification or action will be taken by the CSA, unless the CSA deems it appropriate.

Timeliness

WACIC/NCIC records must be entered promptly to ensure maximum system effectiveness. Records must be entered according to standards defined in the ACCESS Operations Manual.

Accuracy and Completeness

The accuracy of WACIC/NCIC data must be double checked and documented, including the initials and date by a second party. This must be done within seven days of the initial entry. The verification should include assuring the data in the WACIC/NCIC record matches the data in the investigative report and that other checks were made. Agencies lacking support staff for second party checks should require the case officer to check the record.

Complete records of any kind include all information available on the person or property at the time of entry, otherwise known as “packing the record”. Complete inquiries on persons include numbers that could be indexed in the record (i.e. Social Security Number (SSN), Vehicle Identification Number (VIN), Operator’s License Number (OLN), etc.). Inquiries should be made on all names/aliases used by the suspect. Complete vehicle inquiries include VIN and license plate numbers.

Record Validations

WACIC/NCIC validation listings are prepared pursuant to a schedule, as published in the ACCESS Operations Manual. These listings are distributed to the originating agency via CJIS Validations.

Validation requires the originating agency to confirm the record is complete, accurate, and active. Validation is accomplished by reviewing the original entry and current supporting documents and correspondence with any appropriate complainant, victim, prosecutor, court, motor vehicle registry files, or other appropriate source or individual. Validation efforts must be well documented. Validation efforts include what was done to complete the validation of the individual record. Documentation of phone calls, letters, dates and dispositions need to be included with each record that was validated. Many agencies document this information in the case file. In the event the agency is unsuccessful in its attempts to contact the victim, complainant, etc., the entering agency must make a determination based on the best information and knowledge available whether or not to retain the original entry in the file.

The agency must review the validation list found within CJIS Validations. Once all of the records have been processed the system will advise ACCESS once they are complete. If the CSA is notified the records have not been validated within the specified period of time, the CSA will purge all records which are the subject of that agency’s validation listings from WACIC and NCIC.

IX. Security Responsibilities

Technical Roles and Responsibilities

All agencies participating in ACCESS must comply with and enforce system security. Each interface agency (city, county, or other agency) having access to a criminal justice network must have someone designated as the technical security POC. A criminal justice network is a telecommunications infrastructure dedicated to the use by criminal justice entities exchanging criminal justice information. The technical security POCs shall be responsible for the following:

1. Identifying the user of the hardware/software and ensuring that nonauthorized users have access to the same.
2. Identifying and documenting how the equipment is connected to the state system.
3. Ensuring that personnel security screening procedures are being followed as stated in the CJIS Security Policy.
4. Ensuring that appropriate hardware security measures are in place.
5. Supporting policy compliance and keeping the WSP Information Security Officer (ISO) informed of security incidents.

Security Enforcement

Each interface agency is responsible for enforcing system security standards for their agency, in addition to all of the other agencies and entities to which the interface agency provides CJIS and Washington State Department of Licensing (DOL) records information. Authorized users shall access CJIS and DOL systems and disseminate the data only for the purpose for which they are authorized. Each criminal justice and non-criminal justice agency authorized to access FBI CJIS systems and DOL shall have a written policy for the discipline of policy violators.

Physical Security

A physically secure location is a facility, a criminal justice conveyance, or an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect CJI and associated information systems. The physically secure location is subject to criminal justice agency management control.

The perimeter of a physically secure location shall be prominently posted and separated from non-secure locations by physical controls.

All personnel with access to computer centers, terminal areas, and/or areas where unencrypted CJIS information is housed shall either be escorted by authorized personnel at all times or receive a fingerprint-based background check and view security awareness training prior to being granted access to the area.

Personnel Security

To verify identification, a state of residency and national fingerprint-based record checks shall be conducted prior to employment or assignment for all personnel who have authorized access to FBI CJIS systems and those who have direct responsibility to configure and maintain computer systems and networks with access to FBI CJIS systems. All requests for system access shall be made as specified by the CSO. The CSO or their official designee is authorized to approve CJIS systems access. All official designees to the CSO shall be from an authorized criminal justice agency. If a record of any kind exists, access to CJI shall not be granted until the CSO or his/her designee reviews the matter to determine if access is appropriate. The agency is required to request a variance from the CSO.

Support personnel, contractors, and custodial workers who access computer terminal areas shall be subject to a Washington state and national fingerprint-based background check and view the security awareness training, unless these individuals are escorted by authorized personnel at all times. Authorized personnel are those persons who have passed a Washington state and national fingerprint-based background check and have been granted access. These personnel must be employed by the criminal justice agency or part of the IT Department that provides a criminal justice function for the criminal justice agency.

Private Contractors/Vendors

Private contractors shall be permitted access to CJIS record information systems pursuant to an agreement which specifically identifies the contractor's purpose and scope of providing services for the administration of criminal justice. The agreement between the criminal justice government agency and the private contractor shall incorporate the CJIS Security Addendum approved by the Director of the FBI, found at <https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center/view>. User shall download the latest Addendum at least annually and conform to its requirements. Private contractors who perform the administration of criminal justice shall meet the same training and certification criteria required by governmental agencies performing a similar function, and shall be subject to the same extent of audit review as are local user agencies.

Hit Confirmation

Any agency that enters a record into WACIC/NCIC has the duty to promptly respond with the necessary confirmation of the hit and other details. They must furnish a response within a specific time period. Valid hit confirmation is based on two levels of priority:

Priority 1: Urgent

The hit must be confirmed within ten minutes. In those instances where the hit is the only basis for detaining a suspect or the nature of a case requires urgent confirmation of a hit, priority 1 should be specified.

Priority 2: Routine

The hit must be confirmed within one hour. Generally, this priority will be used when the person is being held on local charges, property has been located under circumstances where immediate action is not necessary, or an urgent confirmation is not required.

X. Compliance Audits

The FBI CJIS Division requires triennial audits be conducted by the CSA to review CJIS standards of compliance and provide recommendations for best business practices. WSP audit staff provide three types of

reviews:

1. **Agency Compliance Review:** WSP Auditors conduct an administrative interview with the TAC. The interview includes questions to determine adherence to WACIC/NCIC policy requirements including:
 - a. System Administration
 - b. System Integrity
 - c. Hit Confirmation
 - d. Record Integrity
 - e. Criminal History
 - f. NICS
 - g. N-DEx
 - h. Written Procedures
 - i. Validations
2. **Data Quality Review:** WSP Auditors conduct an on-site data quality review. Auditors compare WACIC/NCIC records against agency case files. Auditors check for accuracy, completeness, and verify entry and removal practices. The auditors document records with errors for the agency to update.
3. **Auditor Recommendations for Best Practices:** WSP Auditors provide a compliance report of information received during the interview and data quality review. They provide recommendations for best business practices.

XI. Technical Security Audits

The agency is responsible for compliance to technical standards set forth by ACCESS and the CJIS Security Policy. Technical Security Audits will follow the WACIC/NCIC triennial audit schedule.

1. **Agency Compliance Review:** The WSP performs security audits addressing the following compliance areas:
 - a. Personnel security
 - b. CJIS data breach reporting
 - c. Configuration management
 - d. Media protection (physical and electronic)
 - e. Physical protection
 - f. Session lock
 - g. System and communications protection and information integrity
 - h. Boundary protection
 - i. Malicious code protection
 - j. Event logging
 - k. System use notification
 - l. Patch management
 - m. Identification and authentication
 - n. Wireless devices – mobile / bluetooth / cellular
 - o. Handheld mobile devices



WSP ACCESS USER ACKNOWLEDGMENT

As an agency head/director, I hereby acknowledge the duties and responsibilities as set forth in this WSP ACCESS User Acknowledgment, as well as those documents incorporated by reference. I acknowledge that these duties and responsibilities have been developed to ensure the reliability, confidentiality, completeness, and accuracy of all records contained in or obtained by means of the WACIC/NCIC system. I also acknowledge that a failure to comply with these duties and responsibilities will subject my agency to various sanctions. These sanctions may include the termination of ACCESS/WACIC/NCIC services to my agency.

I further understand Department of Licensing (DOL) may review activities of any person who receives driver, vehicle, vessel, and firearm record information to ensure compliance with limitations imposed on the use of the information. The DOL may suspend or revoke for up to five years the privilege of obtaining information of a person found to be in violation of Revised Code of Washington (RCW) 42.56, RCW 46.52, RCW 46.22, RCW 46.12, or the user agreement with DOL. I understand misuse of this information is subject to civil and criminal penalties punishable by fines or imprisonment under the Federal Driver Privacy Protection act and RCW 46.12, RCW 46.22, and RCW 46.52.

Agency Name:	Everett Police Department	
ORI:	WA0310300	
Agency Head Name (printed):	John DeRousse	
Agency Head Email:	jderousse@everettwa.gov	
Agency Head Telephone Number:	425-257-8460	
Agency Head Signature:	<i>John DeRousse</i>	Date: 11/14/2024

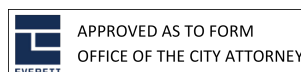
Please return a copy of this signature page to the WSP ACCESS Section.

CITY OF EVERETT

Cassie Franklin, Mayor

ATTEST

Office of the City Clerk



Attachment A 24x7 Hit Confirmation Agreement

24x7 Hit Confirmation Agreement Must be completed by agencies who:

- A. Provide 24x7 teletype printer coverage for another agency.**
- B. Receive 24x7 teletype printer coverage from another agency.**

Every terminal agency that enters records destined for WACIC/NCIC must ensure hit confirmation is available for all records, except criminal history, 24 hours per day either at the agency or through a written agreement with another agency. The terminal agency printer must be monitored 24 hours per day. In the event that 24 hour hit confirmation coverage is not available, the terminal agency printer must be capable of being forwarded to a 24 hour facility. A 24 hour telephone number of the agency responsible for confirming hits must be placed in the Miscellaneous Field of every entry.

Parties who enter into this agreement must adhere to the response times and regulations set forth in the ACCESS Operations Manual and the CJIS Security Policy. This interagency agreement must be current and approved by the CJIS Systems Agency (CSA), the Washington State Patrol (WSP), before agencies adopt the policies and procedures set forth by the agreement.

Termination of Agreement

This agreement shall remain in effect unless terminated by either agency upon thirty (30) days written notice. The agency terminating the agreement must also formally notify the WSP ACCESS Section within the thirty (30) days. Termination of this agreement requires the agency printer to be forwarded to another 24 hour authorized criminal justice facility.

I hereby acknowledge the responsibility and duty to perform teletype hit confirmation to the terminal agency 24 hours per day within the requirements defined by WACIC/NCIC and the CJIS Security Policy.

Agency Providing 24x7 Coverage:	Snohomish County 911	
ORI:	WA031W93N	
Agency Head Name (printed):	Kurt Mills	
Agency Head Signature:	<i>KD Mills</i>	Date: 11/13/2024

Agency Receiving 24x7 Coverage:	Everett Police Department	
ORI:	WA0310300	
Agency Head Name (printed):	John DeRousse, Chief	
Agency Head Signature:	<i>John DeRousse</i>	Date: 11/14/2024

Holder of the Record Agreement Must be completed by agencies who:

A. Use their ORI to enter another agency's records.

B. Have their records entered under another agency's ORI.

A Holder of the Record Agreement (HORA) is required when an agency uses their ORI to enter another agency's records. The holder of the record is defined as an agency that is using their ORI to enter another agency's records. The owner of the record is defined as the agency where the record originated.

The purpose of this agreement is to establish responsibility for records entered in WACIC/NCIC by the holder of the record under its NCIC assigned ORI on behalf of the owner of the record. As they relate to records entered for the owner of the record, the holder of the record assumes the following responsibilities: data entry; documentation; cancellation and modification of entries; timeliness of entries, clears, cancellations and modifications; hit confirmation; second party checks; and validation of entries. The owner of the record is also responsible for providing the HORA with information for entry in a timely manner.

The holder of record must adhere to the regulations set forth in the ACCESS Operations Manual and the CJIS Security Policy. This HORA must be current and approved by the CJIS Systems Agency (CSA), the Washington State Patrol (WSP), before agencies adopt the policies set forth by the agreement.

Entries provided under the HORA (check all that apply):

- | | | | |
|---|---|--|---|
| <input type="checkbox"/> All Entries | <input type="checkbox"/> Articles | <input type="checkbox"/> Boats | <input type="checkbox"/> Gangs |
| <input type="checkbox"/> Guns | <input type="checkbox"/> Identity Theft | <input type="checkbox"/> Images | <input type="checkbox"/> License Plates |
| <input type="checkbox"/> Missing Persons | <input type="checkbox"/> Person of Interest | <input type="checkbox"/> Protection Orders | <input type="checkbox"/> Securities |
| <input type="checkbox"/> Supervised Persons | <input type="checkbox"/> Unidentified Persons | <input type="checkbox"/> Vehicles | <input type="checkbox"/> Vehicle/Boat Parts |
| <input type="checkbox"/> Wanted Persons | <input type="checkbox"/> Violent Persons | | |

Termination of Agreement

This agreement shall remain in effect unless terminated by either agency upon thirty (30) days written notice. The agency terminating the agreement must also formally notify the WSP ACCESS Section within the thirty (30) days. Termination of this agreement shall not negate the obligation of either party to maintain records entered under this agreement to ensure their accuracy, completeness and timeliness.

Agency Acting as the Holder of the Record:		
ORI:		
Agency Head Name (printed):		
Agency Head Signature:		Date:

Agency Acting as the Owner of the Record:		
ORI:		
Agency Head Name (printed):		
Agency Head Signature:		Date:

Inter-Agency Agreement Must be completed by agencies who:

- A. Provide criminal justice services to another agency.**
B. Receive criminal justice services from another agency.

An Inter-Agency Agreement describing the criminal justice services provided and/or received by an agency must be in place.

Services provided (check all that apply):

- ✓
- | | |
|--|---|
| <input checked="" type="checkbox"/> Hit Confirmation | <input type="checkbox"/> Gun transfers/Concealed Pistol Licenses (CPLs) |
| <input checked="" type="checkbox"/> Dispatch | <input checked="" type="checkbox"/> Use of regional management system |
| <input checked="" type="checkbox"/> Record Entry | <input checked="" type="checkbox"/> Terminal connection to ACCESS |
| <input type="checkbox"/> Record Validations | <input type="checkbox"/> Other Services (Describe) |

Parties who enter into this agreement must adhere to the regulations set forth in the ACCESS Operations Manual and the CJIS Security Policy. This Inter-Agency Agreement must be current and approved by the CJIS Systems Agency (CSA), the Washington State Patrol (WSP), before agencies adopt the policies and procedures set forth by the agreement.

Termination of Agreement

This agreement shall remain in effect unless terminated by either agency upon thirty (30) days written notice. The agency terminating the agreement must also formally notify the WSP ACCESS Section within the thirty (30) days.

Agency Providing Criminal Justice Service(s):	Snohomish County 911	
ORI:	WA031W93N	
Agency Head Name (printed):	Kurt Mills	
Agency Head Signature:	<i>KDMills</i>	Date: 11/13/2024

Agency Receiving Criminal Justice Service(s):	Everett Police Department	
ORI:	WA0310300	
Agency Head Name (printed):	John DeRousse, Chief	
Agency Head Signature:	<i>John DeRousse</i>	Date: 11/14/2024

Management Control Agreement

Must be completed by a criminal justice agency receiving services from a non-criminal justice agency (such as city, county or tribal information technology or record archive facility) and updated whenever either signatory changes.

Pursuant to the CJIS Security Policy, it is agreed that with respect to administration of that portion of computer systems and network infrastructure interfacing directly or indirectly with A Central Computerized Enforcement Service System (ACCESS) for the interstate exchange of criminal history/criminal justice information, the Criminal Justice Agency shall have the authority, via managed control, to set and enforce:

- (1) Priorities.
- (2) Standards for the selection, supervision, and elimination of access to criminal history/criminal justice information by personnel who may be tasked with working on or interfacing with any of the telecommunication systems or criminal justice systems/computers enumerated in paragraph three below.
- (3) Policy governing operation of justice systems, computers, access devices, circuits, hubs, routers, firewalls, and any other components, including encryption, that comprise and support a telecommunications network and related criminal justice systems to include but not limited to criminal history record/criminal justice information, insofar as the equipment is used to process or transmit criminal justice systems information guaranteeing the priority, integrity, and availability of service needed by the criminal justice community.
- (4) Restriction of unauthorized personnel from access or use of equipment accessing the State network.
- (5) Compliance with all rules and regulations of the criminal justice agency policies and CJIS Security Policy in the operation of all information received.

Responsibility for management control of the criminal justice function remains solely with the criminal justice agency, as required by the CJIS Security Policy.

This agreement covers the overall supervision of all criminal justice agency systems, applications, equipment, systems design, programming, and operational procedures associated with the development, implementation, and maintenance of any criminal justice agency system to include NCIC Programs that may be subsequently designed and/or implemented within the criminal justice agency.

Non-Criminal Justice Agency Providing Service(s):	City of Everett IT Department	
Agency Head Name (printed):	Chris Fadden, City of Everett IT Director	
Agency Head Signature:	<i>Chris Fadden</i>	Date: 11/15/2024

Criminal Justice Agency Receiving Service(s):	Everett Police Department	
ORI:	WA0310300	
Agency Head Name (printed):	John DeRousse, Chief	
Agency Head Signature:	<i>John DeRousse</i>	Date: 11/14/2024

Attachment D.2 Management Control Agreement For Combined 911 Centers Only

Management Control Agreement for Personnel Determinations

Must be completed between a combined 911/dispatch center (ORI ends in "N") with at least one of the Criminal Justice Agencies (CJA) to which they provide service and updated whenever either signatory changes.

Agencies issued an ORI ending in "N" are by NCIC definition, non-criminal justice agencies providing dispatch functions for CJA.

Therefore, pursuant to the CJIS Security Policy, it is agreed that with respect to personnel determinations for employees/contractors of the 911 center interfacing directly or indirectly with A Central Computerized Enforcement Service System (ACCESS) for the interstate exchange of criminal history/criminal justice information, the CJA shall have the authority, via managed control, to set and enforce:

- (1) Standards for the selection, supervision, and elimination of access to criminal history/criminal justice information by personnel who may be tasked with working on or interfacing with any of the telecommunication systems or criminal justice systems/computers
- (2) Restriction of unauthorized personnel from access or use of equipment accessing the State network

Responsibility for management control of the criminal justice functions above remain solely with the CJA, as required by the CJIS Security Policy.

This agreement requires personnel determinations be made by the CJA, but does not allow the CJA to direct hiring or termination of 911 center personnel; only to approve/reject personnel from working on CJIS systems.

Combined 911 Center ORI:	Snohomish County 911	
Agency Head Name (printed):	Kurt Mills	
Agency Head Signature:	<i>KDMills</i>	Date: 11/13/2024

Criminal Justice Agency ORI:	WA0310300	
Agency Head Name (printed):	John DeRousse, Chief	
Agency Head Signature:	<i>John DeRousse</i>	Date: 11/14/2024

Information Exchange Agreement Must be completed by agencies who:

A. Provide criminal justice information to contracted prosecutors.

An Information Exchange Agreement describing the Criminal Justice Information (CJI) provided and/or received by an agency must be in place between the agency providing the information and the contracted prosecutor receiving the information.

1. Security Control: Each person receiving the information will maintain the information in a physically secure location and only authorized individuals will have access to the CJI. The information will not be left in the open for unauthorized individuals to view.
2. Misuse: Each person receiving the information will use the information for criminal justice purposes only. The information received is not to be used in any civil cases or disseminated to non-criminal justice personnel.
3. Training: Each person receiving the information will be responsible for viewing the Basic Security Awareness Training once every two years. The training log will be provided by and maintained at the criminal justice agency providing the CJI for review at the audit.
4. Destruction: CJI shall be securely disposed of when no longer required and destroyed by shredding or incineration.

Services Provided: (Check all that apply):

☐ Criminal History

☐ Other CJI (Describe):

Parties who enter into this agreement must adhere to the regulations set forth in the WSP ACCESS NCIC Operating Manuals and the CJIS Security Policy. This Information Exchange Agreement must be current and approved by the CJIS Systems Agency (CSA), the Washington State Patrol (WSP), before agencies adopt the policies and procedures set forth by the agreement.

Termination of Agreement

This agreement shall remain in effect unless terminated by either party upon thirty (30) days written notice.

Agency Providing Criminal Justice Information:		
ORI:		
Agency Head Name (printed):		
Agency Head Signature:		Date:

Contracted Prosecutor Receiving Criminal Justice Information:		
Contractor Name (printed):		
Contractor Signature:		Date:

City Named in the Contract:		
Authorizing Name (printed):		
Authorizing Signature:		Date:

Addendum for Criminal Justice Agency (CJA) using a Non-Criminal Justice (NCJA) ORI Must be completed by agencies who:

- A. Have been issued an NCJA ORI to conduct fingerprint submissions for licensing, non-criminal justice employment, CASA/GAL and/or purpose code X/emergency placement of children.**

This addendum is added to the ACCESS User Acknowledgement for a criminal justice agency that has statutory authority under Public Law 92-544 and/or 101-630 to request fingerprint based Criminal History Record Information (CHRI) checks to perform a non-criminal justice function such as licensing, Guardian Ad Litem (GAL), Court Appointed Special Advocate (CASA) and other non-criminal justice employment purposes under the Public Laws listed.

Because the CJA must adhere to the CJIS Security Policy, the following CJA policies and procedures cover the requirements normally provided by an NCJA, and do not need to be duplicated:

- Management Control Agreement and/or CJIS Security Addendums for contractor personnel
- Physical protection
- Password management
- Disposal of media
- Data breach reporting

The CJA is still required to create, maintain and provide the following NCJA specific policies and procedures:

- NCJA Misuse
- Fingerprint Process

All fingerprint based applicant submissions must include in the 'reason fingerprinted' field an accurate representation of the purpose and/or authority for which the CHRI is to be used.

The CJA must notify the applicant fingerprinted that the fingerprints will be used to check the criminal history records of the FBI. The agency making the determination of suitability for licensing or non-criminal justice employment shall:

- Provide the applicants the opportunity to complete, or challenge the accuracy of, the information contained in the FBI identification record.
- Advise the applicants that procedures for obtaining a change, correction, or updating of an FBI identification record are set forth in Title 28, C.F.R. 16.34.

The agency should not deny the license or non-criminal justice employment based on information in the record until the applicant has been afforded a reasonable time to correct or complete the record, or has declined to do so.

Statutory Authority (check all that apply):

☐ PL 92-544

☐ PL 101-630

Description of what fingerprint submissions are used for (CASA/GAL, City Ordinance #, non-criminal justice employment, etc.):

Criminal Justice Agency and ORI		
NCJA ORI:		
Agency Head Name (printed):		
Agency Head Signature:		Date:











WSP ACCESS User Acknowledgment Everett 2024_SD


Final Audit Report

2024-11-15


Created:	2024-11-12
By:	Marista Jorve (mjorve@everettwa.gov)
Status:	Signed
Transaction ID:	CBJCHBCAABAA2UHpJ9k7eifcft0YtO3UA-5nWEtAVPfZ

"WSP ACCESS User Acknowledgment Everett 2024_SD" History

-  Document created by Marista Jorve (mjorve@everettwa.gov)
2024-11-12 - 9:24:22 PM GMT
-  Document emailed to Alicia Gill (AGill@everettwa.gov) for approval
2024-11-12 - 9:28:09 PM GMT
-  Email viewed by Alicia Gill (AGill@everettwa.gov)
2024-11-12 - 9:40:45 PM GMT
-  Document approved by Alicia Gill (AGill@everettwa.gov)
Approval Date: 2024-11-12 - 9:41:33 PM GMT - Time Source: server
-  Document emailed to Sandra Albertson (SAlbertson@everettwa.gov) for approval
2024-11-12 - 9:41:35 PM GMT
-  Email viewed by Sandra Albertson (SAlbertson@everettwa.gov)
2024-11-12 - 9:44:55 PM GMT
-  Document approved by Sandra Albertson (SAlbertson@everettwa.gov)
Approval Date: 2024-11-12 - 9:45:11 PM GMT - Time Source: server
-  Document emailed to Tim Benedict (TBenedict@everettwa.gov) for approval
2024-11-12 - 9:45:14 PM GMT
-  Email viewed by Tim Benedict (TBenedict@everettwa.gov)
2024-11-12 - 10:12:06 PM GMT
-  Document approved by Tim Benedict (TBenedict@everettwa.gov)
Approval Date: 2024-11-12 - 10:12:19 PM GMT - Time Source: server

 Document emailed to Kurt Mills (kmills@sno911.org) for signature


2024-11-12 - 10:12:21 PM GMT

 Email viewed by Kurt Mills (kmills@sno911.org)

2024-11-12 - 10:26:47 PM GMT

 Document e-signed by Kurt Mills (kmills@sno911.org)

Signature Date: 2024-11-13 - 11:43:53 PM GMT - Time Source: server

 Document emailed to jderousse@everettwa.gov for signature

2024-11-13 - 11:43:56 PM GMT

 Email viewed by jderousse@everettwa.gov


2024-11-14 - 3:40:56 AM GMT

 Signer jderousse@everettwa.gov entered name at signing as John DeRousse


2024-11-14 - 9:14:21 PM GMT

 Document e-signed by John DeRousse (jderousse@everettwa.gov)


Signature Date: 2024-11-14 - 9:14:23 PM GMT - Time Source: server

 Document emailed to Chris Fadden (cfadden@everettwa.gov) for signature

2024-11-14 - 9:14:25 PM GMT

 Email viewed by Chris Fadden (cfadden@everettwa.gov)

2024-11-15 - 5:28:07 PM GMT

 Document e-signed by Chris Fadden (cfadden@everettwa.gov)

Signature Date: 2024-11-15 - 5:29:02 PM GMT - Time Source: server

 Document emailed to Cassie Franklin (cfranklin@everettwa.gov) for signature

2024-11-15 - 5:29:04 PM GMT

 Email viewed by Cassie Franklin (cfranklin@everettwa.gov)

2024-11-15 - 5:46:16 PM GMT

 Document e-signed by Cassie Franklin (cfranklin@everettwa.gov)

Signature Date: 2024-11-15 - 5:46:32 PM GMT - Time Source: server

 Document signing automatically delegated to Ashleigh Scott (ascott@everettwa.gov) by Marista Jorve (mjorve@everettwa.gov)

2024-11-15 - 5:46:33 PM GMT

 Document emailed to Ashleigh Scott (ascott@everettwa.gov) for signature

2024-11-15 - 5:46:34 PM GMT



Document emailed to Marista Jorve (mjorve@everettwa.gov) for signature

2024-11-15 - 5:46:34 PM GMT



Email viewed by Ashleigh Scott (ascott@everettwa.gov)

2024-11-15 - 11:47:56 PM GMT



Document e-signed by Ashleigh Scott (ascott@everettwa.gov)

Signature Date: 2024-11-15 - 11:48:41 PM GMT - Time Source: server



Agreement completed.

2024-11-15 - 11:48:41 PM GMT