12.050 – Criminal Justice Information Systems

Original Effective Date: 08/27/2020
Revised Effective Date: 11/01/2022

12.050-POL

Criminal Justice Information Services Security Policy

WSP ACCESS/WACIC/NCIC/User Acknowledgement

1. Definitions

Criminal History Record Information: Information contained in records collected by criminal justice agencies, other than courts, on individuals, consisting of identifiable descriptions and notations of arrests, detentions, indictments, information, or other formal criminal charges, and any disposition including sentences, correctional supervision, and release. The term includes information contained in records maintained by or obtained from criminal justice agencies, other than courts, which records provide individual identification of a person together with any portion of the individual's record of involvement in the criminal justice system as an alleged or convicted offender, except:

- Posters, announcements, or lists for identifying or apprehending fugitives or wanted persons,

- Original records of entry maintained by criminal justice agencies to the extent that such records are compiled and maintained chronologically and are accessible only on a chronological basis,

- Court indices and records of public judicial proceedings, court decisions, and opinions, and information disclosed during public judicial proceedings, and

- Records of traffic violations that are not punishable by a maximum term of imprisonment of more than ninety days.

Dissemination: Disclosing criminal history record information, or the absence of criminal history record information, to any person or agency outside the agency possessing the information, subject to the following exceptions:

- Agencies participating in a single (joint) record-keeping department,

- Furnishing information to process a matter through the criminal justice system (information to a prosecutor), and

- Reporting events to a record-keeping agency.

NCIC III: The National Crime Information Center Interstate Identification Index, managed by the FBI and state law enforcement agencies. The NCIC Advisory Policy Board has established a set of standards and goals that the FBI and state agencies enforce. The information contained in the NCIC includes all records collected by criminal justice agencies on individuals including identifiable descriptions, notations of arrests, detentions, indictments, formal criminal charges, dispositions, sentences, correctional supervision, and release. Federal, state, and local laws and regulations dictate that this information is to be accessed and used only by authorized individuals within a criminal justice agency, that this information is to be used for criminal justice reasons, that this information is to be kept confidential, and that this information is to be stored in a secure location.

- Employees must be working for the Seattle Police Department in an on-duty or extra-duty capacity and investigating a criminal offense.

- Employees shall not run names or make inquiries through NCIC III, or any other criminal record system while working for an off-duty employer or on behalf of an off-duty employer.

2. Inquiries Through ACCESS, or Any Other Criminal Justice Record System, Are Only to Be Made for Legitimate Law Enforcement Purposes

This includes, but is not limited to, inquiries made to DOL, DOC, WACIC, WASIS, NCIC III, LInX, and any inquiries processed through NLETS to other states. Inquiries made for personal use, or inappropriate use or dissemination of the information, can result in internal discipline, as well as penalties under federal and state law.

3. All Employees Who Use Terminals That Have Access to Information in WACIC/NCIC Files Must Be Certified

After initial certification, employees shall take a recertification test every year.

- For inquiries only, employees shall attain Level I certification.

- If employees make data entries into the system, they shall attain Level II certification.

4. SPD Must Remain in Compliance With the ACCESS/WACIC/NCIC User Acknowledgement or Risk Termination of One or More of the Services Provided

The ACCESS/WACIC/NCIC User Acknowledgement is the formal agreement between WSP and SPD. This document acknowledges the standards established in the FBI's Criminal Justice Information (CJI) Service Security Policy. The standards require accuracy, completeness, timeliness, and security in the dissemination and recording of information.

5. Data Center Manager is the Technical Agency Coordinator

The department must designate a Technical Agency Coordinator (TAC) to act as the point of contact for the WSP and the Federal Bureau of Investigation (FBI). The individual designated to function as a TAC will be responsible to ensure compliance with state and National Crime Information Center (NCIC) policies and regulations. The TAC must maintain a Level II training certification and attend TAC training once every three years.

Additionally, the TAC shall participate in and ensure that all appropriate records be available during the triennial audit conducted by the ACCESS audit staff. Responsibility for proper operator performance, strict adherence to regulations, prompt notification of CJIS violations to the ACCESS Section, and subsequent training rests with the TAC. The SPD TAC is the Data Center Manager.

6. All Employees Shall Adhere to WASIS and NCIC Policies

Use of WASIS (Washington State Identification System and Criminal History Section) and NCIC Interstate Identification Index (NCIC III) is regulated by the FBI and WSP in accordance with the 28 CFR Part 20, WAC 446-20-260, and RCW Chapter 10.97. Improper use of the system may result in severe penalties to the department and the individual user.

All employees shall adhere to the following WASIS and NCIC policies:

1. Any information obtained through these systems shall not be disseminated to anyone outside the department, except to a prosecutor. If necessary, sworn employees may confirm to a criminal justice agency the WASIS or FBI number, if it is known.

    a. Examples of agencies and/or organizations to whom we cannot release criminal history information include, DSHS, Passport Agencies, Child Protective Services, Adult Protective Services, Crime Stoppers, victims, and witnesses.

    b. Inquiries for criminal history information from outside agencies, organizations, and individuals should be referred to Washington State Patrol.

2. Inquiries into these systems shall not be made in response to a request by another criminal justice agency or by any retired employees, including those

holding any extended authority, special police commission, or similar police commission.

3. The Department of Justice Criminal Justice Information System (CJIS) restricts the use of all criminal-related data bases to official investigations when conducted while working for a criminal justice organization. As a result, no employee shall run names or make inquiries through ACCESS, WACIC, WASIS, NCIC III, LInX, or any other criminal record system while working for an off-duty employer or on behalf of an off-duty employer.

4. All NCIC III queries are stored in the system. A program has been developed to create an automated user log from that data.

5. This log is audited by the Washington State Patrol, the FBI, and the Audit Unit and shall be available for inspection by any of the agencies at any time. The following procedures must be followed when accessing the Criminal History Database:

   a. All NCIC III queries should be made using Transaction Code CQCH – Common Query Criminal History

   b. The Purpose Code box must be filled in with 1 of the 2 authorized Purpose Codes that appear in the pull-down. The query will not go through if the box is left blank. The only authorized Purpose Codes are:

      C - Criminal Justice purposes as well as authorized uses in relation to the security of the criminal justice facility including, vendors/contractors who are not involved with administration of criminal justice (e.g., janitors, maintenance personnel, visitors, etc.).

      J – Criminal Justice employment/applicants and re-background requirement for criminal justice agency personnel as well as vendors, contractors, volunteers, and interns, who are involved with the administration of criminal justice for the agency.

   c. The Reason field must be filled in with a specific criminal justice reason. The report number should always be listed in the reason field if available. If a report number has not been generated the specific criminal justice reason must be listed in the reason field such as theft, narcotics, homicide, missing person, or criminal justice applicant. Listing terms such as investigation, arrest, criminal history, or employment in the reason field are not valid. Listing abbreviations of any kind in the reason field is not authorized unless the abbreviation has been approved and is on file with the department TAC.

6. An automated user log for all queries made using the Omnixx system is maintained by the Washington State Patrol. Data Center and Public Request Unit Personnel may request access to this log via the "Request for Off-Line

Search." The following information must be included in the Attention Field (ATN) when making a criminal history inquiry using Omnixx:

a. Requestor's SPD serial number.

b. Specific criminal justice reason such as theft, narcotics, homicide, or the report number. Use of abbreviations is acceptable but must be on the list approved by the department TAC found here.

Examples for the ATN field:

(Serial # / Reason)

4545 / Assault

4545 / ASLT (approved abbreviation)

4545 / 2019-16735

7. The NCIC III system is only to be used by personnel involved in criminal investigations, and background investigations. As of 2/11/15, a NICS check will be required for firearms returns. The Public Request Unit is the only unit authorized to complete NICS checks.

8. MDCs and PDTs (mobile and portable data computers/terminals) are not authorized to access NCIC III information because the terminals are unable to comply with NCIC audit requirements.

9. It is important to enter inquiries to the Criminal History Records system properly. The following information must be accurate and complete on the inquiry mask:

a. The "Purpose Code" must be entered correctly, "C", for criminal investigation, or another appropriate code. See NCIC manual for details.

b. The "Requestor Full Name/Serial" must contain the name and SPD serial number of the person making the inquiry. It is not acceptable to use "Det", "Off", or the "unit title" in this field.

7. Employees Are Prohibited from Accessing or Sharing Criminal Justice Information on Public Devices

Employees will not access or share CJI from a publicly accessible device (library, personal phone, etc.) The Mark 43 records management system will not be accessed from a publicly accessible device.

8. Employees Will Not Cut and Paste Information from ACCESS Sources

Employees will not directly cut and paste information from ACCESS sources (WACIC, NCIC, DOL, DOC, etc.). Details should be written out in narratives when needed.

9. Employees Will Not Discuss or Provide Information to Any Person or Entity Who Is Not a Member of the Criminal Justice System Without the Permission of the Chief of Police, or By Due Process of Law

The Washington State Criminal Records Privacy Act (RCW 10.97) provides for the completeness, accuracy, confidentiality, and security of criminal history record information, as well as victim, witness, and complainant record information. Employees shall not discuss or provide information to any person or entity who is not a member of the criminal justice system (prosecuting attorney, court, etc.) without the permission of the Chief of Police, or by due process of law. Violations may lead to criminal sanctions.

10. Criminal Records Releases Are Restricted

Requests for information shall be referred to the appropriate section.

- Criminal history record information dissemination to individuals, agencies, or groups outside the department shall be administered by the Records File Unit and Data Center Unit.

- Juvenile record information dissemination to individuals, agencies, or groups outside the department shall be administered by the Records File Unit.

Printouts of criminal history record information from the department's computerized and manual files are prohibited except when:

- Required for a detective investigative file.

- Required by a prosecuting attorney.

- Required by agencies or individuals authorized by the Records, Evidence, and Identification Section access procedures.

- Required in a mutual criminal investigation with a court or government agency authorized by the Washington State Patrol to receive criminal history record information.

- The Records File Unit and Data Center Unit shall maintain a current list of agencies so authorized.

- Authorized by a watch, section, or unit supervisor as required for an investigation or in an emergency.

When releasing criminal history information to a prosecutor the release tracking should always be used to indicate release to either King County Prosecutor's Office or the City Law Department. The release tracking serves as the automated secondary dissemination log.

In authorized instances when criminal history is secondarily disseminated to any agency or person the following information relating to secondary dissemination of criminal history record information shall be maintained by the appropriate section in the form of a manual log and will include the following:

- To whom (agency or person) criminal history information was released,

- The date of release, and

- A brief description of the information released.

The disposal of printouts from computer terminals shall be by destruction.

11. Individuals Have the Right to Inspect and Review Their Criminal History Record Information Maintained by the Department

A copy of the department operating instructions titled, "Inspection and Review of Criminal History Record Information" and "Challenge and Deletion of Criminal History Record Information" shall be maintained at locations where the public can make inquiries concerning department procedures.

An individual's right to access and review their criminal history record information shall not extend to data contained in intelligence, investigative, or other related files and shall not be construed to include any information other than that defined as Criminal History Record Information by RCW 10.97.030.

In order to inspect, review, or challenge and have deleted criminal history record information, the individual must appear in person at the 1st floor of the Police Headquarters Building 610 Fifth Avenue, Tuesday through Thursday (excluding holidays) between the hours of 8:00 a.m. and 4:30 p.m. and make a request in writing on the forms provided.

Employees are responsible for directing individuals to the Records File Unit in order to facilitate review of their criminal history record information.

An individual will be provided an opportunity, following review of the criminal history record information collected, stored, and maintained by the department, to challenge the accuracy and completeness of the data and request deletion of certain non-conviction arrests.

If the challenge is rejected, the individual has a right to appeal the decision to the Office of the Chief of Police.

It shall be the duty of the Records File Unit manager and supervisors to administer the rules pertaining to an individual's right to review their criminal history record information, concurrent with the aforementioned laws, regulations, and ordinances.

12. All SPD Personnel Must Have a Background Re-Investigation Every Five Years

To complete this compliance measure, the department must:

- Run a criminal history inquiry using purpose code "J". Use "Criminal Justice Re-background" as a reason. Log the date and SID# of the employee. Do not retain rap sheet information.

- If there are felony findings within the employee's rap sheet, they will be denied continued use and certification with ACCESS. The TAC must notify the WSP Information Security Officer of any findings.

- If there are charges pending a disposition, the TAC must notify the WSP Information Security Officer (ISO).

- If there are misdemeanor findings the TAC shall notify the WSP Information Security Officer. The Seattle Police Department will ultimately decide whether to limit ACCESS usage.

- Keep a log of all personnel SID numbers and the date of the background re-investigation for future ACCESS audits.

13. SPD Must Comply With ACCESS/NCIC Security Requirements

All employees must complete the Security Awareness Training within six months of initial hire. Any employee not Level I or Level II-certified must review the Security Awareness Training every year.

Maintaining security of the terminal sites and information received is the responsibility of agency personnel operating the terminal, the TAC, and the agency head. Terminal locations must be secure from authorized access, and all employees authorized to use the system shall be instructed on the proper use of equipment and the dissemination of information received. Federal and state laws protect the information provided by ACCESS.

Violations of the rules, regulations, policies, or procedures developed by FBI and adopted by the WSP, or any other misuse or abuse of the ACCESS system may result in agency disciplinary measures and/or criminal prosecution. Disciplinary measures imposed by the WSP may include revocation of individual certification, discontinuance of system access to the department, or purging the department's records.

Any misuse of the NCIC III system must be reported to the TAC (Data Center Manager) immediately. The TAC shall report the misuse to the Washington State Patrol

and the FBI via the "ACCESS Violation Incident Report" form. The violator's chain of command will be notified of the misuse.

14. The Lieutenant of the Audit Unit Will Assign Personnel to Conduct Regular Audits of the Department's Criminal History Records Inquiries

The department audits will be completed biannually, and the results of these audits will be reported to the Chief Operating Officer.

The audit will look for any violations of the CJIS Security Policy, The WSP User Acknowledgement, and department policy. Violations include but are not limited to:

- Queries made for personal reasons.

- Reason Field errors, such as using general terms such as investigation, arrest, warrant, criminal history.

- The Reason Field must contain a specific crime such as homicide, assault, burglary.

Any users who are in violation of any or all of the above will have their access to the Criminal History system shut off. Access will be denied until they have attended a remedial class for making Criminal History inquiries.

- An e-mail will be sent to the employee and their immediate supervisor from the Audit Unit lieutenant that their access to the Criminal History system has been denied.

- The e-mail will contain information about the remedial classes that they must take to regain access.

- A copy of the e-mail will be sent to the Data Center Manager/TAC for implementation.