ACCESS

812.1 PURPOSE AND SCOPE

This policy clarifies ACCESS requirements to include but not limited to, physical security of ACCESS/CJIS systems, CJIS information and the requirements for the use and dissemination of criminal history record information.

812.2 POLICY

Use of the ACCESS system is restricted to authorized criminal justice agencies, and criminal justice information obtained through the system may only be used for official law enforcement business in the administration of criminal justice such as to facilitate the apprehension of fugitives, the location of missing persons, the location and/or return of stolen property or similar criminal justice objectives. All users will conform to the requirements outlined in this policy to ensure proper and efficient use of the ACCESS system.

812.3 DEFINITIONS

ACCESS - A Central Computerized Enforcement Service System (ACCESS) is a computer controlled communications system located at the Washington State Patrol Information Technology Division in Tumwater. Through the use of special interfacing equipment, ACCESS extracts data from multiple repositories including the Washington State Patrol’s Criminal Information Center (WACIC), Washington State Identification System (WASIS), the National Crime Information Center (NCIC), the Department of Licensing (DOL), the Department of Corrections Offender file (DOC), the International Justice & Public Safety Network (NLETS), and numerous regional systems. ACCESS provides direct contact with NCIC when WACIC is non-operational.

Criminal Justice Information (CJI) - Information contained in records collected by criminal justice agencies that provide individual identification of a person along with the individual’s record of involvement in the criminal justice system as an alleged or convicted offender including but not limited to arrests, detentions, indictments, acquittals, and sentences.

Criminal Justice Agency - A government agency which performs the administration of criminal justice pursuant to a statute or executive order and which allocates a substantial part of its annual budget to the administration of criminal justice. Criminal justice agencies include police departments, courts, the prosecuting attorney’s office and sheriff’s offices. Criminal justice agencies do not include code enforcement, the medical examiner, animal control, fire departments, defense attorneys, or security companies. (RCW10.97.030)

NCIC - The National Crime Information Center (NCIC) is a computerized system of criminal justice records. The Interstate Identification Index (III) is part of the NCIC network. The NCIC database allows a law enforcement agency automated access to all information regarding an individual's criminal history that is within the records of any law enforcement agency in the NCIC network. The system can be accessed 24 hours a day by any local, state or federal law enforcement agency to obtain criminal history information in eleven specific categories, including records of convicted sex offenders, foreign fugitives, identity theft, missing persons, gang and terrorist organizations, fingerprint data, unidentified persons, and wanted persons.

Copyright Lexipol, LLC 2022/06/16, All Rights Reserved.
Published with permission by Vancouver Police Department

WACIC – The Washington Crime Information Center (WACIC) is a statewide computerized repository for multiple types of entries including wanted persons, persons of interest and others. All entries are completed and managed by contributing agencies. WACIC stores criminal justice information that can be instantly retrieved and furnished to an authorized criminal justice agency. For WACIC, criminal justice information is information collected by criminal justice agencies that is needed in the performance of legally authorized, required function.

812.3.1 ACRONYM / ABBREVIATION LIST FOR CRIMINAL HISTORIES

http://cvsharepoint/departments/PoliceDept/VPDNet/Documents/Abbreviation%20List.docx

812.4 SECURITY MEASURES

The Vancouver Police D epartment has adopted the following security measures to comply with applicable laws and regulations and to prevent unauthorized access to the system data and/or unauthorized use of data obtained from the computerized file.

Members accessing or receiving protected information shall ensure the information is not accessed or received by persons who are not authorized to access or receive it. This includes leaving protected information, such as documents or computer databases, accessible to others when it is reasonably foreseeable that unauthorized access may occur (e.g., on an unattended table or desk; in or on an unattended vehicle; in an unlocked desk drawer or file cabinet; on an unattended computer terminal).

812.4.1 SYSTEM SECURITY

1. ACCESS terminal locations have adequate physical security to protect against any unauthorized personnel gaining access to the computer equipment or to any stored data.
2. VPD will establish usage restrictions and implementation guidelines for wireless technologies; and authorize, monitor, and control wireless access to the information system. Wireless technologies will maintain at least the minimum security applied to wired technology.
3. VPD personnel can only utilize ACCESS and CJIS information from secure terminals. A secure terminal is any Department owned or approved electronic device, mobile data computer (MDC), desk top computer, laptop, or wireless device used inside a VPD building or police vehicle.
4. If a VPD employee utilizes one of these devices to obtain ACCESS or CJIS information in a non-secure location, then Advanced Authentication is mandatory.
5. If a police vehicle is left in a non-secure location and no Advanced Authentication is on the MDT, personnel must adhere to one of the following:
    A. The MDT must be removed from the vehicle and secured in a VPD building.
    B. A fingerprinted criminal justice employee must remain with the MDT at all times.
    C. The staff/personnel servicing the vehicle must be fingerprinted and background checked and review the Security Awareness training available on CJIS Online.
6. A secure location is considered to be inside the secured area in any VPD police building or police vehicle.
7. Any VPD employee utilizing ACCESS or CJIS information outside of a VPD police building or police vehicle is considered to be in a non-secure location and requires Advanced Authentication.

Copyright Lexipol, LLC 2022/06/16, All Rights Reserved.
Published with permission by Vancouver Police Department

To access this information in a non-secure location, without Advanced Authentication, violates state and federal regulations.

A. *Example*: Any VPD owned or approved electronic device, as noted above, which is removed from a VPD police building or police vehicle and is carried into and utilized for ACCESS or CJIS information in any location, private or public, subject to the viewing of any non-ACCESS approved person, such as a restaurant, private residence (whether their own or not), City Hall, etc., without Advance Authentication, is a violation.

B. *Example*: Any VPD employee who removes a MDT from a VPD police vehicle and utilizes it within a VPD police building does not require Advanced Authentication and is not a violation.

812.4.2 PHYSICAL PROTECTION

The purpose of this policy is to provide guidance for agency personnel, support personnel, and private contractors/vendors for physical, logical, and electronic protection of Criminal Justice Information (CJI). all physical, logical, and electronic access must be properly documented, authorized and controlled on devices that store, process, or transmit unencrypted CJI. This Physical Protection Policy focuses on the appropriate access control methods needed to protect the full lifecycle of CJI from inside and outside threats.

(a) **Physically Secure Location**: 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 the physically secure location shall be prominently posted and separated from non-secure locations by physical controls. Security perimeters shall be defined, controlled, and secured.

(b) **Visitor Access**: A visitor is defined as a person who visits th agency on a temporary basis who is not employed by the Vancouver Police Department and has no unescorted access to the physically secure location within the agency where CJI and associated information systems are located. Visitors must:

A. Be accompanied by agency personnel at all times to include delivery or service personnel. An escort is defined as authorized personnel who accompany a visitor at all times while within a physically secure location to ensure the protection and integrity of the physically secure location and any CJI therein.

B. Follow policy for unescorted access:

i. City of Vancouver IT and vendors which are Noncriminal Justice Agency (NCJA) who require unescorted access to restricted area(s) have an established Management Control Agreement between the Vancouver Police Department and City of Vancouver IT. Each employee with CJI access will appropriately have state and national fingerprint-based record background checks and CJIS certification prior to this restricted area access being granted.

ii. Private contractors/vendors who have unescorted access to restricted area(s) will be required to establish a Security Addendum with each private contractor personnel.

C. Not be allowed to view screen information, mitigating shoulder surfing.

D. Be escorted to a public area of the facility when they do not have any legitimate business in a restricted area. Strangers in physically secure areas without an escort should be challenged.

Copyright Lexipol, LLC 2022/06/16, All Rights Reserved.
Published with permission by Vancouver Police Department

E. Not be allowed to sponsor another visitor.

F. Photographs within a secure area are not allowed without permission of the Vancouver Police Department assigned personnel.

(c) **Authorized Physical Access**: Only authorized personnel will have access to physically secure non-public locations. All physical access points into the agency's secure areas will be authorized before granting access. The agency will implement access controls for protecting all transmission and display mediums of CJI. Authorized personnel will take necessary steps to prevent and protect the agency from physical, logical and electronic breaches. All personnel who are not escorted with CJI physical and logical access must:

A. Met the minimum personnel screening requirements prior to CJI access.

i. Agencies must conduct a state of residency and national fingerprint-based background checks for all agency personnel and IT personnel who have direct access to CJI and those who have direct responsibility to configure and maintain computer systems and networks with direct access to CJI prior to employment or assignment.

ii. Support personnel, private contractors/vendors, and custodial workers with access to physically secure locations or controlled areas (during CJI processing) shall be subject to a state and national fingerprint-based records check unless these individuals are escorted by authorized personnel at all times.

B. Complete Security Awareness Training: All authorized Vancouver Police Department and NCJA personnel, like city or county IT and private contractor/vendor, will receive Security Awareness Training within sex months of being granted duties that require CJI access and every two years thereafter.

C. Be aware of who is in their secure area before accessing confidential data.

i. Take appropriate action to protect all confidential data.

ii. Protect all terminal monitors with viewable CJI displayed on the monitor and not allow viewing by the public or escorted visitors.

D. Properly protect and not share any individually issued keys, proximity cards, computer account passwords, etc.

i. Report loss of issued keys, proximity cards, etc. to authorized agency personnel.

ii. If loss occurs after normal business hours, weekends or holidays, personnel are to call the Vancouver Police Department POC to have authorized credentials like a proximity card de-activated and/or door locks possibly re-keyed.

iii. Safeguard and do not share passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), and all other facility and computer systems security access procedures.

E. Properly protect from viruses, worms, trojan horses, and other malicious code.

F. Web usage - monitoring of user activity.

G. Use of electronic media is allowed only by authorized personnel. Controls shall be in place to protect electronic media and printouts containing CJI while in transport. When CJI is

Copyright Lexipol, LLC 2022/06/16, All Rights Reserved.
Published with permission by Vancouver Police Department

physically moved from a secure location to a non-secure location, appropriate controls will prevent data compromise and/or unauthorized access.

H. If CJI is transmitted by email, the email must be encrypted and email recipient must be authorized to receive and view CJI.

I. Report any physical security incidents to the City of Vancouver's IT POC, to include facility access violations, loss of CJI, loss of laptops, thumb drives, CDs/DVDs and printouts containing CJI.

J. Properly release hard copy printouts of CJI only authorized personnel in a secure envelope and shred and burn hard copy printouts when no longer needed. Information should be shared on a "need to know" basis.

K. Ensure data centers with CJI are physically and logically secure.

L. Keep appropriate agency security personnel informed when CJI access is no longer needed. In the event of ended employment, the individual must surrender all property and access managed by the local agency, state and/or federal agencies.

M. Ensure the perimeter security door securely locks after entry or departure. Do not leave any perimeter door propped open and take measures to prevent piggybacking entries.

(d) **Penalties**: Violation of any of the requirements in this policy by any authorized personnel could result in disciplinary action, up to and including loss of ACCESS privileges, civil and criminal prosecution and/or termination. Violation by any visitor can result in similar disciplinary action against the sponsoring employee and can also result in termination of services with any associated consulting organization or prosecution in the case of criminal activity.

812.4.3 SECURITY BACKGROUND FOR PERSONNEL

VPD adheres to strict security standards for personnel who use or have access to the ACCESS system including:

(a) Conducting national fingerprint-based background checks shall be conducted 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. The record checks shall be conducted prior to employee accessing any systems.

(b) All personnel, contractors, volunteers, and custodial workers with access to computer centers, terminal areas and/or areas where CJIS information is housed shall be escorted by authorized personnel or receive a fingerprint-based criminal background check. Authorized personnel are those persons who have passed a state and national fingerprint-based record check and have been granted access.

(c) VPD shall use the following procedures when reviewing the results of the fingerprint-based background check:

A. If the background check reveals a felony conviction, the individual shall be denied use, certification and/or the ability to work on connection to ACCESS.

B. If there are charges pending a disposition, the TAC will notify the ACCESS manager.

C. If the background check reveals a misdemeanor conviction, the TAC will notify the ACCESS section where the severity of offense and the time that has passed would support a possible

Copyright Lexipol, LLC 2022/06/16, All Rights Reserved.
Published with permission by Vancouver Police Department

variance. VPD will have discretion whether to limit use of the ACCESS system even if a variance approval is granted by the Access section manager.

(d) Assuring that all personnel within six months of employment or assignment with direct use of ACCESS systems are ACCESS certified at the appropriate level. ACCESS certification requires biennial recertification.

A. Level 1 – All users who use ACCESS for inquiries, locates or administrative messages.

B. Level 2 – Includes all abilities of Level 1 and includes entry, clearing, canceling of records within the databases.

(e) CJIS Security Awareness Training is required for all other personnel, volunteers, and contractors who have unescorted access to a physically secure location. An appropriate level of Security Awareness Training is required within six months of initial assignment, and biennially thereafter.

812.4.4 RE-BACKGROUND INVESTIGATIONS

ACCESS requires all personnel who use or work on the connections to ACCESS to have a re-background investigation conducted every five years.

Documentation of re-background dates is maintained within nexTEST and CJIS Online systems.

812.5 TECHINCAL AGENCY COORDINATOR (TAC)

VPD has a designated Technical Agency Coordinator (TAC) to act as the point of contact for matters relating to ACCESS and CJIS information.

(a) The TAC must maintain a Level 2 certification and attend TAC training at least once every three years.

(b) The TAC will send recertification email to staff with a deadline to re-certify and copy personnel's chain of command to ensure its compliance

(c) The TAC assures that re-background checks are performed as required.

(d) The TAC retains the state identification number of each employee who uses ACCESS or maintains the application or network connection.

(e) The TAC shall participate in and ensure that all appropriate records are available during audits conducted by ACCESS.

(f) The TAC is responsible for proper operator performance, strict adherence to state and FBI CJIS policies and regulations, and prompt notification of policy violations to ACCESS.

812.6 VALIDATIONS

VPD acknowledges that it is necessary to confirm all records are complete, accurate and valid and that validation efforts must be well documented. Validation requirements are outlined within Records procedures.

812.7 QUERIES AND CRIMINAL HISTORY LOG

All criminal history logs are maintained in an automated format by the Washington State Patrol (WSP).

The criminal history inquiry must contain the following information:

1. The Attention (ATN) Field must contain:

Copyright Lexipol, LLC 2022/06/16, All Rights Reserved.
Published with permission by Vancouver Police Department

A. Requestor's first initial and last name or PSN

B. Specific criminal justice reason for the request or a case number

i. A specific criminal justice reason may include the agency case number or the crime being investigated, i.e., assault, robbery, etc.

ii. If an acronym is used for the purpose, it must be on the Department approved acronym list found on Sharepoint - VPDnet. Person running the inquiry, if different from the requestor, should enter their PSN.

C. EXAMPLES:

ATN/J SMITH / 19-1234

ATN/J SMITH / BURGLARY / 9999

ATN/J SMITH / BURGLARY

ATN/ 1234 / BURGLARY

2. The correct purpose code:

A. **C** - Use this purpose code for the official duties in connection with the administration of criminal justice and investigation of crimes.

B. **F** - Use this purpose code for the issuance of silencers/suppressors and Federal Firearm Licenses.

C. **J** - Use this purpose code when conducting initial background checks and five year re-background checks of criminal justice agency personnel, including IT.

3. Prohibited actions:

A. VPD personnel will not provide criminal history information to another party or outside agency representatives.

B. Personnel shall not use any information obtained through the ACCESS system, including all Department of Licensing (DOL) and Department of Corrections (DOC) information for private business/personal reasons, or further any information so obtained to any other person for such use other than for the official law enforcement purposes.

C. NCIC III information shall not be placed or copied into the investigative case file.

812.8 HIT CONFIRMATION

A WACIC or NCIC hit alone is not probable cause to arrest a subject, but indicates a stolen property report, missing person report, or warrant, etc., may have been filed.

An inquiring agency must contact the originating agency of the hit for confirmation of data. To confirm a hit means to contact the agency that entered the record to:

(a) Ensure that the person or property inquired upon is identical to the person or property identified in the record.

(b) Ensure the warrant, missing person report, protection order, or theft report is still outstanding.

Copyright Lexipol, LLC 2022/06/16, All Rights Reserved.
Published with permission by Vancouver Police Department

(c) Obtain a decision regarding:

A. The extradition of a wanted person when applicable.

B. The return of the missing person to the appropriate authorities.

C. The return of stolen property to its rightful owner.

D. The terms and conditions of a protection order.

The source documents used for hit confirmation may be electronic if the agency has implemented the proper controls for electronic documents supporting WACIC/NCIC records.

A confirmed hit can be adequate grounds to arrest the wanted person, detain the missing person, seize the stolen property, or charge the subject with violating a protection order, etc.

When an agency receives a record(s) in response to an inquiry, and no enforcement action is contemplated or possible because of extenuating circumstances, the hit should not be confirmed, and the record must not be located.

812.9 DISPOSAL OF CRIMINAL JUSTICE INFORMATION

VPD personnel must dispose of criminal history information by observing the actual shredding of the documents.

(a) Criminal history information run for purposes of a criminal investigation cannot be included in a case file. Detectives and officers may quote specific information reviewed into their case report and shred the referenced criminal history information.

(b) Criminal history information will not be scanned, and should not be attached as a supporting document into the Records Management System.

(c) All CJIS (Criminal Justice Information Systems) information to include Criminal History, all wants and protection order queries, DOL Checks, etc. should be disposed in secured shredding bins.

812.9.1 DISPOSAL OF MEDIA

Any media shall be disposed of as follows:

(a) Electronic media shall be sanitized prior to disposal or release for reuse by unauthorized individuals. Inoperable electronic media shall be destroyed (cut up, shredded, etc.).

(b) Physical media shall be destroyed by shredding or incineration when no longer required, using formal procedures.

(c) The disposal process will be observed by a fingerprinted criminal justice employee. Or, the disposal process does not need to be observed if the contracted company has all been fingerprinted and they have signed a CJIS Security Addendum. A copy of the Addendum must be provided to the ACCESS Section.

812.10 MISUSE OF THE ACCESS SYSTEM

The ACCESS System shall only be used for official law enforcement business. The Vancouver Police Department will investigate allegations of ACCESS misuse. Examples of misuse include:

- Running criminal history for yourself, family or friends.
- Running information for a civilian or non-criminal justice employee for non-law enforcement use.

Copyright Lexipol, LLC 2022/06/16, All Rights Reserved.
Published with permission by Vancouver Police Department

- Using the system for any personal reasons.
- “Visiting” or sending inappropriate administrative messages across a mobile data terminal (MDT) ACCESS connection

Users do not have to disseminate information in order to be in violation. Accessing CJIS data for personal reasons is prohibited by state and federal law.

Violations of the rules, regulations, policies, or procedures developed by NCIC and adopted by the Washington State Patrol or any other misuse or abuse of the ACCESS system may result in agency disciplinary measures and/or criminal prosecution.

812.10.1 REPORTING ACCESS/NCIC VIOLATIONS

(a) If the Department initiates an internal investigation for ACCESS misuse, the PSU Lieutenant or designee must immediately notify the Department’s TAC. The TAC then must submit an ACCESS Violation Incident Report to the ACCESS Manager at the Washington State Patrol.

(b) Whether the allegations are sustained or unfounded, the TAC must again be advised in order to notify the ACCESS manager of the investigation’s outcome.

(c) If the allegations are sustained, the Vancouver Police Department will choose the level of internal discipline. The Washington State Patrol may work in conjunction with the Department to impose additional sanctions if warranted. This may include, but not limited to, additional training, revocation of individual certification, or termination of system access to the Department.

(d) Even if the allegations are unfounded, the Washington State Patrol will then determine if there was indeed any violation of the ACCESS/NCIC system.

Copyright Lexipol, LLC 2022/06/16, All Rights Reserved.
Published with permission by Vancouver Police Department