
	<b>LEXINGTON POLICE DEPARTMENT</b>  POLICY AND PROCEDURE GENERAL ORDER	Distribution	General Order Number
		ALL PERSONNEL	<b>10.12</b>
		Original Issue Date	Reissue/Effective Date
		01/06/2024	04/20/2026
Order Title:  <b>NCIC and VCIN MAINTENANCE AND SECURITY PROCEDURES</b>		Accreditation Standard:	Section
		CALEA 81.2.8	10
		Rescinds:	
Section Title SUPPORT AND TECHNICAL SERVICES		 <b>Justin T. Doll, Chief of Police</b>	

*This General Order is for departmental use only and does not apply in any criminal or civil proceeding. This General Order should not be construed as creation of a higher legal standard of safety or care in an evidentiary sense with respect to third party claims. Violations of this General Order will only form the basis for departmental administrative sanctions. Violations of law will form the basis for civil and criminal sanctions in a recognized judicial setting.*

## I. PURPOSE

The purpose of this general order is to establish a written directive that outlines the policies, procedures, and guidelines required by state and federal authorities to ensure the Lexington Police Department is compliant concerning access and maintenance of VCIN and NCIC information systems.

## II. POLICY

The Lexington Police Department (“Department”) will ensure that all Department personnel access and maintain VCIN and NCIC information systems in a manner that meets all Department, state and federal guidelines. The Chief of Police, or designee, is responsible for overseeing Department activities related to these criminal justice systems and will designate Department personnel to act as the Department’s Terminal Agency Control Officer (TAC) and the Local Agency Security Officer (LASO). The person(s) designated as the TAC and LASO shall report directly to the Chief of Police, or designee, in carrying out their duties and responsibilities of those positions as outlined below. The Lexington Police Department will have a signed agreement with the Virginia State Police authorizing CJIS access. This document will be titled “VA Criminal Information Network User Agreement” and will be signed by the current agency head and the Virginia State Police.

This Department directive is meant to complement the VCIN and FBI Security Policy and is not meant to provide less-stringent requirements than the FBI Security Policy. Violations of this directive may result in disciplinary action up to, and including, dismissal.

## DEFINITIONS

**CJI (Criminal Justice Information):** Refers to all information disseminated by the State and Federal Criminal Justice Information Systems and VCIN.

Electronic Media: Includes memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, backup medium, optical disk, flash drives, external hard drives, or digital memory card.

Local Agency Security Officer (LASO): A security point of contact for local agencies that have access to criminal justice information.

NCIC (National Crime Information Center): A computer system controlled and operated by the Federal Bureau of Investigation in Washington DC, that gives law enforcement agencies access to information on warrants, criminal histories, stolen property, and missing persons statewide and nationwide.

Physical Media: Includes printed documents and imagery that contain CJI.

Terminal Agency Coordinator (TAC): The point of contact at an agency for matters relating to access to VCIN and NCIC information. The TAC administers systems programs within the agency and oversees the agency's compliance with systems policies.

Visitor: A visitor is defined as a person who visits the Department facility on a temporary basis, who is not an employee and has no unescorted access to the physically secure locations where CJI and associated information systems are located.

### **III. PROCEDURE**

#### **A. Terminal Agency Coordinator (TAC) Duties and Responsibilities**

1. The TAC is responsible for overseeing all Department activities related to the access and maintenance of VCIN and NCIC information in accordance with the these directives, and VCIN/NCIC/CJIS directives.
2. The TAC will maintain contact with Virginia State Police NCIC Unit personnel to remain aware of changes to state and federal requirements, and will make recommendations for amendments to this directive in accordance with those changes.
3. Additional duties and responsibilities include, but are not limited to, the following:
  - a. Complete TAC Training available on NexTest.
  - b. Complete all forms and reports required by NCIC, CJIS and VCIN;
  - c. Assure that agency employees receive training in compliance with this directive;
  - d. Maintain a roster of authorized employees and review this roster at least annually to make appropriate notifications when employees are terminated or transferred to a position that does not require access;

- e. Conduct background checks and provide security clearance for non- employees who are contracted to service equipment and assure they complete a non-disclosure agreement;
- f. The TAC and the IT Director will coordinate agency practices with the LASO to assure security of the system and system information and maintain validation procedures in accordance with these guidelines;
- g. If a Management Control Agreement is in place, the TAC will have a copy of the current, signed agreement;
- h. Maintain VCIN/NCIC holder or record agreement; and
- i. Maintain a copy of the current, approved VCIN network diagram and update as needed.

B. Duties and Responsibilities of the Local Agency Security Officer (LASO)

1. The LASO will coordinate his/her activities with the TAC to assure that all required security requirements are maintained and the TAC and the IT Director are made aware of any discovered security issues.
2. The LASO will conduct unannounced audits of inquiries and make written reports concerning the audit findings. In addition, security audits will be conducted once every three years, as required by state and federal guidelines, and reports filed with the TAC utilizing the forms provided by the Virginia State Police and VCIN.
3. Other duties and responsibilities of the LASO include, but are not limited to, the following:
  - a. Coordinate with the IT Director to identify individuals authorized to use the - approved hardware, software, and firmware, and ensure no unauthorized individuals or processes have access to the same.
  - b. Coordinate with the IT Director to identify and document how the equipment is connected to the systems;
  - c. Ensure that all personnel security screening procedures are being followed as stated in this policy. This will include ensuring that all personnel have signed necessary security agreements with Human Resources prior to assigning a unique identifier in coordinator with IT staff;
  - d. Maintain documentation to verify that all individuals with access to CJI systems have passed a fingerprint-based background and submitted applicant cards per the VCIN Operating Manual;
  - e. Coordinate with the IT Director to ensure the approved and appropriate security measures are in place and working as expected;
  - f. Support policy compliance and ensure the TAC is promptly informed of security incidents;
  - g. Complete the required training available on CJIS online upon initial hire and annually thereafter;
  - h. Ensure all personnel with direct or indirect access to CJI, including those with unescorted access, have completed CJIS Security Training prior to accessing CJI and annually thereafter prior to issuing authorization credentials.

C. Accessing NCIC/CJIS/VCIN Information on Personal or Public Devices

1. Department personnel may only access NCIC/CJIS/VCIN information on authorized Department computer terminals. Department personnel are prohibited from accessing NCIC/CJIS/VCIN information on personally-owned devices, and doing so may result in disciplinary action.
2. Department personnel will not utilize publicly accessible computers to access, process, store, or transmit CJI. Publicly accessible computers include, but are not limited to: hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.

D. Protection of /VCIN Media

1. Authorized Department personnel shall protect and control electronic and physical CJI while at rest and in transit. Department staff will take appropriate safeguards for protecting CJI to limit potential mishandling or loss while being stored, accessed, or transported. Any inadvertent or inappropriate CJI disclosure and/or use will be reported to the Local Agency Security Officer (LASO).
2. To protect CJI, Department personnel shall:
  - a. Securely store electronic and physical media within a physically secure or controlled area. A secured area includes a locked drawer, cabinet, or room. Secure areas also include any office that contains a CJI system (patrol office, sergeants office, etc.). Department personnel will keep these areas secure and the door locked when not in use;
  - b. Restrict access to electronic and physical media to authorized individuals only;
  - c. Ensure that only authorized users remove printed form or digital media from the CJI;
  - d. Physically protect CJI until media end of life. End of life CJI is destroyed or sanitized using LASO and IT Director-approved equipment, techniques, and procedures;
  - e. Store all hardcopy CJI printouts in secure areas, as designated by the LASO or TAC, and assure that such documents are only accessible to those employees whose job function requires them to handle such documents.
  - f. Take appropriate action when in possession of CJI while not in a secure area, to include not leaving the CJI outside of the employee's immediate control, and taking precautions to obscure CJI from public view by means of an opaque file folder or envelope for hard copy printouts and session lock for electronic devices like laptops, use session lock use, and/or privacy screens;
  - g. CJI shall not be left in plain public view. When CJI is electronically transmitted outside the boundary of the physically secure location, the data shall be immediately protected using encryption;
  - h. When CJI is at rest (i.e. stored electronically) outside the boundary of the physically secure location, the data shall be protected using encryption. Storage devices

include external hard drives from computers, printers and copiers used with CJI. In addition, storage devices include thumb drives, flash drives, back-up tapes, mobile devices, laptops, etc.;

- i. When encryption is employed, the cryptographic module used shall be certified to meet current Federal Information Processing Standards (FIPS).;
  - j. Log off the computer when not in immediate vicinity of the work area to protect CJI. Not all personnel have the same CJI access permissions and need to keep CJI protected on a need-to-know basis.
3. Dissemination of CJI to another agency is authorized if the other agency is an “Authorized Recipient” of such information and is being serviced by the accessing agency, or the other agency is performing personnel and appointment functions for criminal justice employment applicants.
  4. Department personnel shall protect and control electronic and physical media during transport outside of controlled areas and restrict the pickup, receipt, transfer and delivery of such media to only authorized personnel.
  5. Department personnel shall document activities associated with the transport of CJI media.
  6. Department personnel will not take CJI home, or when traveling, unless authorized by the LASO. When disposing of CJI documents, such documents will be shredded.

E. Physical Protection of CJI and Hardware

1. All physical, logical, and electronic access must be properly documented, authorized and controlled on devices that store, process, or transmit unencrypted CJI.
2. A physically secure location is a facility 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 perimeter of the physically secure location shall be prominently posted and separated from non-secure locations by physical controls. Security perimeters shall be defined and approved by the LASO, controlled, and secured. Restricted non-public areas in the Lexington Police Department shall be identified with a sign.
  - a. The following procedures are required for any visitors allowed into a restricted area where CJI or associated systems are located: Be accompanied by an authorized escort at all times to include delivery or service personnel. An escort is defined as an authorized personnel who accompanies 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. The use of cameras or other electronic means used to monitor a physically secure location does not constitute an escort.
  - b. The LASO will establish a Security Agreement with any private

contractors/vendors who require frequent unescorted access to restricted areas. Each staff member of the private contractor will submit to a state and national fingerprint-based record background check and complete CJIS Security and Awareness Training prior to being granted access to a restricted area; and this training will be completed annually thereafter.

- c. Visitors will not be allowed to view screen information, mitigating shoulder surfing;
  - d. Individuals not having any legitimate business in a restricted area shall be courteously escorted to a public area of the facility. Strangers in physically secure areas without an escort should be challenged. If resistance or behavior of a threatening or suspicious nature is encountered, sworn personnel shall be notified or call 911;
  - e. A visitor may not sponsor another visitor;
  - f. Visitors may not enter into a secure area with electronic devices unless approved by the LASO to include cameras and mobile devices. Photographs are not allowed without permission of the LASO.
3. The LASO will maintain a list of authorized individuals with access to physically secure non-public locations that contain CJI systems and review this list at least annually or as needed based on changes to an individual's status with the Department and/or need for access. The agency will implement access controls and monitor physically secure areas for the protection of all CJI transmissions and display mediums. Authorized personnel will take necessary steps to prevent and protect the agency from physical, logical and electronic breaches.
  4. All personnel with CJI physical and logical access must meet the minimum personnel screening requirements prior to CJI access. These requirements include the following:
    - a. To verify identification, a state of residency and national fingerprint-based records check shall be conducted within 30 days of assignment for all 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;
    - b. Receive CJIS security awareness training within 6 months of hire and annually thereafter
  5. Personnel shall properly protect and not share any individually issued keys or proximity cards to the facility or secured area(s), controlling ingress and egress to the facility. Personnel shall properly protect and not share any computer account passwords, combinations, etc., and shall report loss of issued keys, proximity cards, etc. to authorized agency personnel. If the loss occurs after normal business hours, or on weekends or holidays, personnel are to call the the Chief of Police or designee to have authorized credentials, like a proximity card, de-activated and/or door locks possibly rekeyed.
  6. The Chief of Police or designee will maintain a list of issued physical access devices to the facility and/or secured areas (i.e. keys, proximity cards, etc.) and at minimum review this inventory annually. The Chief of Police and/or his designee will ensure that in the

event of a personnel change all access devices to the facility and/or secure areas are returned to the Department.

7. All entry and exit points to the facility and secure areas will be continuously monitored by video surveillance to prevent unauthorized access. A physical access log will be maintained for all visitors accessing the secure facility and will be reviewed quarterly.
8. Personnel will safeguard and not share passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), and all other facility and computer systems security access procedures. Personnel will protect from viruses, worms, Trojan horses, and other malicious code that access CJI.
9. Personnel will report any physical security incidents to the LASO to include facility access violations, loss of CJI, loss of laptops, electronic devices, thumb drives, CDs/DVDs and printouts containing CJI.
10. All properly vetted IT staff assigned to support CJI-associated systems will protect CJI from compromise by performing the following:
  - a. Protect information subject to confidentiality concerns—in systems, archived, on backup media, and until destroyed. IT staff will know where CJI is stored, printed, copied, transmitted and planned for end of life. CJI is stored on laptops, mobile data terminals (MDTs), computers, servers, tape backups, CDs, DVDs, thumb drives, RISC devices and internet connections as authorized by the agency. This includes Live Scan terminals that receive CJI back to the Live Scan terminal;
  - b. Be knowledgeable of technical requirements and policies, taking appropriate preventative measures and corrective actions to protect CJI at rest, in transit, and at the end of life;
  - c. Take appropriate action to ensure maximum uptime of CJI and expedited backup restores by using approved best practices for power backup and data backup means such as generators, backup universal power supplies on CJI-based terminals, servers, switches, etc.
  - d. Properly protect the system(s) from viruses, worms, Trojan horses, and other malicious code to include real-time scanning and ensuring updated definitions.
  - e. Install and update antivirus programs on computers, laptops, MDTs, servers, etc.
11. The LASO will coordinate with authorized IT staff to ensure that the following actions are completed:
  - a. Conduct appropriate data backups and take appropriate measures to protect all stored CJI.
  - b. Ensure only authorized vetted personnel transport off-site tape backups or any other media that store CJI and is removed from a physically secured location.
  - c. Perform timely application of system patches. As part of the configuration management function, only authorized IT staff will be permitted to access and/or make changes to CJI systems.
  - d. Identify applications, services, and information systems containing software or

components affected by recently announced software flaws and potential vulnerabilities resulting from those flaws.

12. The LASO shall establish Access Control measures that include the following:
  - a. Address privileges and separation of duties;
  - b. Coordinate with IT staff to employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with the mission and functions of the Department.
  - c. Prevent authorized users from utilizing publicly accessible computers to access, process, store, or transmit CJI. Publicly accessible computers include, but are not limited to: hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.
  
13. The LASO shall maintain an Account Management program in coordination with the TAC, to include the following:
  - a. Ensure that all personnel authorized to store, process, and transmit information on the CJI system are individually authenticated and associated with processes on behalf of that user through a unique user name and password;
  - b. Ensure that all user IDs belong to currently authorized users;
  - c. Keep login access current, updated and monitored. Remove or disable any account that is terminated or transferred;
  - d. Not use shared generic or default administrative user accounts or passwords for any device used with CJI.
  - e. Review the access rights of all users at least annually to validate their continued need for access and their privileges within the system.
  
14. The LASO will coordinate with IT staff to ensure that passwords will include the following standards:
  - a. Be a minimum length of eight (8) characters on all systems;
  - b. Not be the same as the User ID;
  - c. Expire within a maximum of 120 calendar days;
  - d. Not be identical to the previous twelve (12) passwords;
  - e. Not be transmitted in clear or plaintext outside the secure location;
  - f. Not be displayed when entered; and
  - g. Ensure passwords are only reset for authorized user.
  
15. The LASO will coordinate with IT to maintain Network Infrastructure protection measures that include the following:
  - a. Take action to protect CJI-related data from unauthorized public access;
  - b. Ensure all terminals with access to CJI display a "System Use Notification" message before granting access to the system;

- c. Ensure all terminals automatically terminate the user session when a user has logged out;
- d. Control access to monitor and monitor network infrastructure, enabling and updating configurations of boundary protection firewalls to provide continuous monitoring at an organizational level;
- e. Ensure confidential electronic data is only transmitted on secure network channels using encryption and advanced authentication when leaving a physically secure location. No confidential data should be transmitted in clear text;
- f. Ensure any media that is removed from a physically secured location is encrypted in transit by a person or network;
- g. Not use default accounts on network equipment that passes CJI like switches, routers, firewalls;
- h. Make sure law enforcement networks with CJI shall be on their own network, accessible by authorized personnel who have been properly vetted;
- i. Utilize Virtual Local Area Network (VLAN) technology to segment CJI traffic from other noncriminal justice agency traffic to include other city and/or county agencies using same wide area network; and
- j. Communicate and keep agency personnel informed of all scheduled and unscheduled network and computer downtimes and all security incidents and misuse. The ultimate information technology management control belongs to the Lexington Police Department.

#### F. Electronic Media Sanitization and Disposal

1. When no longer usable, hard drives, diskettes, tape cartridges, CD's, ribbons, and other similar items used to process, store and or transmit VCIN/NCIC data shall be properly disposed of in accordance with measures established by the Lexington Police Department. An authorized employee of the Lexington Police Department will complete the sanitation process.
2. Physical media (printouts) shall be disposed of by shredding. Electronic media (hard-drives, tape cartridges, 3D printer ribbons, flash drives, printer, and copier hard drives, etc.) shall be disposed of by one of the following methods:
  - a. Overriding (at least three times) - an effective method of clearing data from magnetic media, using a program to write (1s, 0s, or a combination of both) onto the location of the media where the file to be sanitized is located.
  - b. Degaussing - a method used to magnetically erase data from magnetic media.
  - c. Destruction- a method of destroying magnetic media by physically dismantling it. Such methods may include crushing, disassembling, etc., ensuring that the platters have been physically destroyed so that no data can be retrieved.
3. Systems that have been used to process, store, or transmit VCIN/NCIC data shall not be released until the equipment has been sanitized and all stored information has been cleared using one of the above methods.

#### G. Breach Notification and Incident Reporting

1. The agency shall promptly report incident information to appropriate authorities. Information security events and weaknesses associated with information systems shall be

communicated in a manner allowing timely corrective action to be taken. Incident-related information can be obtained from a variety of sources including, but not limited to, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports. Examples of such incidents include:

- a. Loss, theft, or missing data, equipment of IT resources
  - b. Denial of Services (DoS) intentional or unintentional
  - c. Compromise of computer security (includes virus and malware threats)
  - d. Phishing attempts to acquire sensitive information such as usernames or passwords for malicious reasons, by masquerading as trustworthy in an electronic communication, or,
  - e. Unauthorized access to the VCIN/NCIC system or data.
2. If CJI is improperly disclosed, lost, or reported as not received, the agency personnel notified of the incident shall immediately (but not to exceed one hour) notify their direct supervisor, the LASO, and the IT Director. The LASO will complete and submit an incident-report form within eight (8) hours of discovery of the incident. The submitted report is to contain a detailed account of the incident, to include:
- a. What happened
  - b. Where it happened (Console ID)
  - c. When did it happen (date and time)
  - d. Possible cause of the incident, if known
  - e. Immediate action taken, and
  - f. Additional information.
3. The supervisor will take immediate corrective action when a breach is discovered and will communicate the situation with the LASO and the IT Director to notify of the loss or disclosure of CJI records.
4. The LASO will ensure the IT Director is promptly informed of security incidents and provided the incident report. The IT Director will take necessary remedial actions to mitigate the potential harm of the security incident.
5. IT staff in coordination with the LASO will employ automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.
6. All CJI system users with direct or indirect access to CJI will be trained in the incident response plan as outlined in this policy prior to accessing the CJI system and annually thereafter.
7. The Chief of Police or his or her designee will, in coordination with the LASO, review and update incident response training at least annually or following a security incident.

## H. Misuse and Unauthorized Use of CJI Systems

1. Misuse of computing, networking, or information resources may result in temporary or permanent restriction of computing privileges up to employment termination. In some misuse situations, account privileges will be suspended to prevent ongoing misuse while under investigation. Additionally, misuse can be prosecuted under applicable statutes. All files are subject to search. Where follow-up actions against a person or agency after an information security incident involves legal action (either civil or criminal), the evidence shall be collected, retained, and presented to conform to the rules of evidence laid down in the relevant jurisdiction(s). Complaints alleging misuse of Department computing and network resources and CJI systems and/or data will be directed to the Chief of Police, or designee, for appropriate disciplinary action.
2. The following are examples of misuse or unauthorized conduct:
  - a. Using someone else's login;
  - b. Leaving computer logged in with your login credentials unlocked in a physically unsecure location, allowing anyone to access agency systems and/or CJI systems and data in your name;
  - c. Allowing an unauthorized person to access CJI at any time for any reason;
  - d. Allowing remote access of issued computer equipment to CJI systems and/or data without prior authorization by the LASO;
  - e. Obtaining a computer account that you are not authorized to use;
  - f. Obtaining a password for a computer account of another account owner;
  - g. Using the agency network to gain unauthorized access to CJI;
  - h. Knowingly performing an act that interferes with the normal operation of CJI systems;
  - i. Knowingly propagating a computer virus, Trojan horse, worm and malware to circumvent data protection, or compromising existing security holes to CJI systems;
  - j. Violating terms of software and/or operating system licensing agreements or copyright laws;
  - k. Duplicating licensed software, except for backup and archival purposes, that circumvent copyright laws for use in agency systems, for home use or for any customer or contractor;
  - l. Using electronic mail or instant messaging to harass others;
  - m. Masking the identity of an account or machine;
  - n. Posting materials publicly that violate existing laws or the agency's codes of conduct;
  - o. Attempting to monitor or tamper with another user's electronic mail or files by reading, copying, changing, or deleting without explicit agreement of the owner;
  - p. Using Department technology resources to advance unwelcome solicitation of a personal or sexual relationship while on duty or through the use of official capacity;
  - q. Unauthorized possession of, loss of, or damage to the agency's technology equipment with access to CJI through unreasonable carelessness or maliciousness;
  - r. Maintaining CJI or duplicate copies of official files in either manual or electronic formats at his or her place of residence or in other physically non-secure locations without express permission.

- s. Using agency technology resources and/or CJI systems for personal or financial gain.
- t. Deliberately failing to report promptly any known technology-related misuse by another employee that may result in criminal prosecution or discipline under this policy;
- u. Using personally owned devices on the Department network to include personally-owned thumb drives, CDs, mobile devices, tablets on wifi, etc. Personally owned devices should not store Department or CJI data.

The above listing is not all-inclusive, and any suspected technology resource or CJI system or CJI misuse will be handled by the Chief of Police or designee and the TAC on a case by case basis. Activities will not be considered misuse when authorized by the LASO or TAC for security or performance testing.

#### G. Review of Policy and Procedures

1. The LASO and TAC will work in conjunction with the IT Director and other authorized Department personnel as needed to review and update the Department's CJIS policies and procedures, including required trainings, annually or in the event of the following:
  - a. Any changes to the CJIS Security Policy and/or Department policy pertaining to the security of the CJI systems.
  - b. Any changes in the CJI systems.
  - c. Any security incident involving unauthorized access to CJI systems or CJI media.
  - d. Any assessment or audit findings which indicate remedial action must be taken to address deficiencies.