	Norwich Police Department Standard Operating Procedure

Subject:	VCIC CJIS
Distribution:	All Officers & H.Q.
Reevaluation date:	October 2030
Approved / By order of:	Jennifer Frank, Chief of Police

I. PURPOSE:	The purpose of this Standard Operating Procedure is to provide direction and guidelines to assist the Norwich Police Department in ensuring compliance with FBI Criminal Justice Information Services (CJIS) security policy. Any agency maintaining or utilizing an access point for National Crime Information Center (NCIC) data is required to adhere to strict security guidelines to ensure the integrity and confidentiality of the data is protected. This SOP defines the policy adopted by the CSA and clarifies and puts into perspective the minimum responsibilities and requirements for various agencies, that are set forth in the CJIS Security Policy by the CJIS Division of the FBI and approved by the National CJIS Advisory Policy Board. Failure to comply exposes the Norwich Police Department to risk, including virus attacks, compromises to the network systems and services, and legal issues. The consequences of non-compliance can be expensive legal battles as well as termination from the information services that are critical to accomplishing the law enforcement mission. This Standard Operating Procedure becomes effective October 1, 2020, and rescinds all previous rules and regulations pertaining to the subject.
II. POLICY:	This policy and guidelines are applicable to and mandated for the Norwich Police Department and for any Criminal Justice Agency in the State of Vermont that accesses and utilizes the state switching services for obtaining CJIS data, such as NCIC, Interstate Identification Index (III aka Triple-I).

III. DEFINITIONS:	A. Advanced Authentication: This is a higher level of authentication (identification of the end-user) that is required for systems generally outside the secure environment. This is achieved when a user presents, verified across the network, any combination of at least two of the following credentials: 1. Something the user knows (e.g., password or pin) 2. Something the user has (e.g., token, smart card or challenge card) 3. Something the user is (e.g., a biometric such as a fingerprint or iris scan) B. CJIS Systems Agency (CSA): The Vermont Crime Information Center (a division of the Vermont Department of Public Safety Criminal Justice Services Division) is the CSA for the State of Vermont. This is the agency responsible for establishing and administering an IT security program throughout the CSA's user community, to include the local levels. C. CJIS Systems Agency Information Security Officer (ISO): This person documents technical compliance with the CJIS Security Policy with the goal to assure the confidentiality, integrity, and availability of criminal justice information to the user community through the CSA's user community, to include the local level. This person documents and provides assistance for implementing security-related controls for the Interface Agency and its users. The ISO also serves as the security point of contact for the FBI CJIS Division ISO. This responsibility currently lies with the Deputy Director of the Vermont Crime Information Center. D. CJIS Systems Officer (CSO): The person responsible for enforcing system discipline, ensuring appropriate use and that FBI CJIS Division operating procedures are followed by all users of the respective telecommunications links. This person also ensures state and federal agency compliance with policies approved by the National CJIS Advisory Policy Board and adopted by the FBI, and approves FBI CJIS systems access. This role also assumes ultimate responsibility for managing the security of CJIS systems within the state. This responsibility currently lies with the Director of the Vermont Crime Information Center. E. Interface Agency (IA): Any authorized law enforcement, criminal justice agency, governmental agency or private entity which performs criminal justice functions, which has access to or which is the authorized recipient of information derived from the FBI CJIS Division's systems. F. Interstate Identification Index (III): The III Program provides for the decentralized interstate exchanges of Identity History

	Summary (IdHS) records and functions as a part of the FBI Criminal Justice Information Services (CJIS) Division. The III provides a means of conducting national record searches for criminal justice and other purposes as specified by existing local, state, and/or federal laws. G. Local Agency Security Officer (LASO) or Security Point of Contact: Each LASO shall: 1. Identify who is using the CSA approved hardware, software, and firmware and ensure no unauthorized individuals or processes have access to the same. 2. Identify and document how the equipment is connected to the state system. 3. Ensure that personnel security screening procedures are being followed as stated in the CJIS Security Policy. 4. Ensure the approved and appropriate security measures are in place and working as expected. 5. Support policy compliance and ensure the CSA ISO is promptly informed of security incidents. H. NCIC Auditor: The individual appointed by the CSO to provide training to and routinely audit agencies accessing, using and disseminating CJIS data to ensure compliance with agency and FBI NCIC and CJIS policy and regulations. I. NCIC Hot Files: There are a total of 21 NCIC files, comprised of seven article files and 14 person files, all of which are considered "hot files", except for the following: 1. Violent Gang and Terrorist Organization file 2. Convicted Persons on Supervised Release file 3. Immigration Violator file 4. Convicted Sex Offender Registry file 5. Historical Protection Order file J. Physically Secure Location: A criminal justice facility, an area, a room, a group of rooms, or a police vehicle that is/are subject to criminal justice agency management control/security addendum and which contain hardware, software and/or firmware that provide access to the CJIS network. K. Terminal Agency Coordinator (TAC): The TAC serves as the point-of-contact at the local agency for matters relating to CJIS information access. The TAC administers CJIS systems programs within the local agency and oversees the agency's compliance with CJIS systems policies.
IV. PROCEDURES:	A. Restricted Files v. Non-Restricted Files: The NCIC hosts restricted files and non-restricted files. NCIC restricted files are distinguished from NCIC non-restricted files by the policies governing their access and use. Proper access to, use, and dissemination of data from

	restricted files shall be consistent with the access, use, and dissemination policies concerning the III described in Title 28, Part 20 CFR and the NCIC Operating Manual. The restricted files, which shall be protected as CHRI, are as follows: 1. Gang Files 2. Known or Appropriately Suspected Terrorist Files 3. Supervised Release Files 4. National Sex Offender Registry Files 5. Historical Protection Order Files of the NCIC 6. Identity Theft Files 7. Protective Interest Files 8. Person with Information (PWI) data in the Missing Person Files 9. Violent Person File 10. NICS Denied Transactions File *The remaining NCIC files are considered non-restricted files. B. <u>General Statements:</u> Below, you will find some general statements referred to in the CJIS Security Policy which sets the basis for this document and its requirements. 1. The FBI CJIS Division maintains a central database of nationwide criminal history information to which they allow access for criminal justice agencies conditioned upon that have been established for the protection of systems and data. 2. The FBI conducts routine audits (currently, every three years) to ensure state and local agencies are in compliance with the minimum-security requirements as outlined in the FBI CJIS Security Policy. 3. Failure to comply can result in loss of access to CJIS data and services, notwithstanding additional training and alternate corrective actions may be applied. 4. Only agencies with an FBI authorized ORI shall have access to the CJIS system confidential data. 5. Any criminal justice agency that receives access to the FBI CJIS data shall enter a signed written agreement with the CSA providing access. 6. The CSO or Designee has the authority to approve FBI CJIS system access and has the authority to set, maintain and enforce policy governing the operation of computers, access devices, hubs, routers, firewalls and other components that comprise and support a telecommunications network used to process, store, or transmit criminal justice information.

	7. The CSA or Designee is responsible for the management control of network security to include setting and enforcing policy governing the operation of circuits and network equipment used to transmit CJIS data. 8. Each Interface Agency shall have a criminal justice employee designated as a security POC (Point of Contact) for their network or points of access. 9. The computer site and related infrastructure used to access the CJIS networks must have adequate physical security as specified in the CJIS Security Policy. 10. Each CJIS Systems Agency and Interface Agency shall administer an IT security program throughout their user community. C. <u>Usage and Dissemination:</u> Proper access to, use and dissemination of FBI CJIS system information is governed by policy and subject to audit. Guidelines vary depending on the information required. The III is considered criminal history record information (CHRI) and numerous files contain CHRI, and are to be treated consistent with the use and dissemination policies governing the III. These include: Violent Gang and Terrorist Organization file, Convicted Persons on Supervised Release file, Immigration Violator file, Convicted Sex Offender Registry file, and the Historical Protection Order file. All remaining NCIC files are considered "hot files." The following guidelines apply to the use and dissemination of CHRI and NCIC "hot file" information: 1. The III may only be accessed for an authorized purpose and used for a purpose consistent with the purpose the FBI CJIS system was accessed. 2. Dissemination to another Criminal Justice agency is authorized if the other agency is an authorized recipient and is being serviced by the accessing agency or is consistent with the "related agency doctrine." 3. NCIC hot files may be accessed for any purpose consistent with the inquiring agency's responsibility. 4. Hot file information may be disseminated to other government agencies or private agencies authorized by law to receive such information. 5. Bulk information requests and commercial distribution of hot file information is prohibited. 6. Logging, purpose codes and reason for inquires shall be recorded for all III inquiries. 7. Logs shall be maintained for a minimum of three (3) years on all NCIC and III transactions. The III portion of

	the log shall clearly identify the operator and the authorized receiving agency, as well as the requestor and any secondary recipients. 8. Transfer of FBI CJIS CHRI via the internet and associated electronic media may be permitted if all technical security requirements are met. 9. CHRI records shall be stored in a secure records environment. Specifically, this refers to an area under the control of the requesting agency and is accessible only by authorized individuals with a right to access or review the data. 10. Voice transmission (over wireless or radio technology) of CHRI information is generally not allowed, but permitted if an officer determines there is an immediate, imminent, or exigent need to further an investigation or there is a situation involving the safety of an officer of the public. 11. Facsimile transmission is allowed as long as both agencies involved have an authorized ORI number and the sending agency has verified the receiving agency's authenticity, and that receipt of the transmission is monitored by an authorized person. D. <u>Security:</u> A secure network is one that minimizes the risk for the integrity of the system or its data being compromised. Security is the responsibility of all users, and the *FBI CJIS Security Policy* sets the minimum standards. Physical security perimeters are defined by the CSO. These perimeters are specified below: 1. Law enforcement sensitive facilities and restricted/controlled areas shall be separated from non-restricted areas by physical barriers that restrict unauthorized access. 2. Every physical access point to sensitive facilities or restricted areas that house systems accessing, processing or displaying CJIS data, during working or non-working hours shall be secured in a manner that is acceptable to the CSO. 3. Visitors to computer centers and terminal areas shall be escorted at all times. 4. Individuals (such as vendors, maintenance personnel, etc.) who access computer terminal areas, unescorted by authorized personnel, shall have a national fingerprint-based record check. Times of access should be documented per access agency policy.

	5. Fingerprint supported record checks will be done within thirty (30) days from anyone with authorized access to CJIS systems. 6. Any third-party contractor or vendor responsible for system maintenance, repair or data support can be granted access in accordance with CJIS logon and authentication policy. If this access gives them the actual or potential capability of accessing FBI CJIS systems data, they will be provided a copy of and required to sign the CJIS Security Addendum prior to such access. This is in addition to the national fingerprint-record check. E. <u>Auditing:</u> Auditing plays an important role in tracking activity on the network and provides a tool for identifying and rectifying security issues and potential breaches or security violations. FBI CJIS Security Policy requires adherence to several auditing requirements: 1. All Interface Agencies shall establish an audit trail capable of monitoring successful and unsuccessful log-on attempts, file access, type of transaction, and password changes. • For some agencies, without an internal network, this may already be maintained by the CSA on the switch. If in doubt, the IA should verify. 2. All audit trail files shall be protected to prevent unauthorized changes or destruction. 3. The CSA should ensure that security audits for operational systems are conducted at least once every three (3) years. 4. The CSA reserves the right to conduct an audit of any IA's policy compliance at any time to ensure the agency has operational policy in place. F. <u>Training:</u> 1. The CSO or Designee shall ensure that security awareness training is provided at least once every three years, or as otherwise mandated. 2. New employees and appropriate IT personnel shall receive security awareness training within six (6) months of their appointment or assignment. This training is to be provided by the CSA. 3. Documentation of materials used and those employees who receive security awareness training shall be maintained by all agencies. 4. This does not preclude an Interface Agency from establishing and maintaining an internal security training program in addition to that established by the CSA. G. <u>Network Configuration Documentation:</u>

	To maintain the overall security of the CSA network, it is critical to have a thorough understanding of how the Interface Agencies are configured and how they access the network. To this end, the CJIS Security Policy requires certain documentation: 1. Every Interface Agency shall ensure that the ISO has a complete and current topological drawing depicting the interconnectivity of the Interface Agency's network configuration. This drawing shall include: a. All communication paths, circuits and other components use for interconnection, beginning with the organization-owned system(s) and traversing through all interconnected systems to the organization endpoint. b. The logical location of all components (e.g. firewalls, routers, switches, hubs, servers, encryption devices, and computer workstations, etc.). Individual workstations (clients) do not have to be shown – an annotation of the number of clients and their ORI designations is sufficient. c. The words "FOR OFFICIAL USE ONLY" shall appear near the bottom of the page containing the drawing. 2. Records of wireless devices ID numbers and contact numbers of commercial wireless providers shall also be maintained to allow for deactivation of lost or stolen devices. H. <u>Required Policy and Procedures:</u> FBI CJIS Security Policy requires certain polices & procedures be in place at all CSA and Interface Agency locations. The following is a list of required Polices & procedures with apply to both CSA and IAs unless otherwise noted: 1. Each CJIS Systems Agency and each Interface Agency shall administer an IT Security Program throughout their user community. The mission of the program shall be to fully and properly implement the requirement of the FBI CJIS Security Policy to ensure the confidentiality, integrity and availability of the CJIS data and systems throughout the user community. 2. Documented procedures shall be in place to monitor all security policies. 3. Authorized access agencies for FBI CJIS systems shall have a written policy for discipline of CJIS policy violators. Discipline is specific to each department and action for violations should be already covered in existing

	agency policy, but enforcement should be reflected in all security policy with the underlying concept that, at any time, the CSO/CSA have the authority to terminate an individual's or Interface Agency's connectivity to CJIS systems, depending on the severity of the infraction and its potential impact on the network. 4. An acceptable use policy shall be established regarding the use of computer systems, internet, email, etc. This policy may differ considerably from agency-to-agency, but must be in place to ensure security and network integrity. 5. Media disposal policy is required. The Interface Agency whose computers and media, etc., are under the control of the CSA, simply need a policy statement reflecting the same. 6. Computer Incident response policy is required. 7. CSA shall oversee establishment of policy for mobile or remote devices. The Interface Agency should have an individual policy in place regarding the use of such equipment specific to their agency. 8. User logon policy is required 9. CSA needs to establish policy for advanced authentication The Interface Agency needs a separate policy when applicable (internal networks allowing outside access to systems that can access CJIS systems data). 10. Password policy is required. 11. CSA is authorized to grant internet access, including internet dial-up access to support CJIS processing when a minimum set of requirements have been met. The Interface Agency with their own internet access is required to have this policy in place. 12. Dial-In access policy is required, if applicable. 13. Firewall devices and firewall policy are required for physically secured location that house equipment that allows access to the CJIS networks. Police vehicles are not subject to these requirements. 14. Anti-virus protection policy is required. The interface Agency that uses the CSA-managed antivirus do not need a separate antivirus policy, as they are governed by the CSA policy. I. <u>Enforcement:</u> Failure of a CSA agency to comply with or ensure compliance with the CJIS Security Policy can result in being denied access to CJIS systems and mission-critical data. At the discretion of the CSO and/or ISO, non-compliance on

	either a CSA or Interface Agency level can result in a denial of service for the entire state. Based on the facts of the case, the following may occur for non-compliance: 1. Immediate disconnection from the network, pending investigation. If any agency action, intentional or unintentional, poses an immediate threat to the integrity of the network or the security of sensitive information has been or will be compromised. 2. In the event of less immediate issues, the following will occur: a. The pertinent information will be brought to the attention of the appropriate agency authority, to include potential options or solutions, if available. b. A reasonable opportunity will be granted to remedy the situation. c. Failure to rectify the issue in a reasonable fashion will result in a review of the situation for potential disconnection or other punitive actions (i.e. remedial training, increased audit frequency, etc.).

	Norwich Police Department **Paperwork Service Record**
Date Received:	
Receiving Officer:	
Sending Party:	
Targeted Recipient:	
Known location / Contact information:	

SERVICE ATEMPTS				
	Date:	**Time:**	**Serving officer:**	**Outcome:**
Attempt 1				☐ Successful ☐ Unsuccessful
Attempt 2				☐ Successful ☐ Unsuccessful
Attempt 3				☐ Successful ☐ Unsuccessful
After the 3rd unsuccessful attempt, service paperwork will be returned to the sending party and marked as undeliverable.				

Returned to:	
Date / Time:	
Returning officer:	