NEW SMYRNA BEACH POLICE DEPARTMENT
NEW SMYRNA BEACH, FLORIDA

POLICY & PROCEDURE

TITLE:	**CJIS NETWORK & INFORMATION SECURITY**
NUMBER:	**26-5**
EFFECTIVE:	**6/14**
REFERENCE:	**CJIS SECURITY POLICY**
RESCINDS/ AMENDS:	**34-5**
REVISED:	**8/22**
ATTACHMENTS:	**CFR-2014-title28-vol1-sec20-3.pdf** **FSS 943.045.pdf** **FSS 119.071.pdf**

A. PURPOSE

This policy establishes guidelines for adhering to Federal Bureau of Investigation (FBI) Criminal Justice information Services (CJIS) Security Policy and provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of Criminal Justice Information (CJI) date, to protect the CJI from unauthorized disclosure, alteration or misuse. Florida Department of Law Enforcement (FDLE) has adopted the CJIS Security Policy as the standard for protecting Florida's Criminal Justice Information (CJI). The FDLE User Agreement mandates that agencies with FCIC and/or CJNET access comply with the CJIS Security Policy

B. POLICY

It is the policy of the New Smyrna Beach Police Department that information received or transmitted via computer shall conform to law and regulations governing FCIC/NCIC, CJIS, and DHSMV files. Information obtained via FCIC/NCIC is for official law enforcement purposes only, and shall not be released to non-law enforcement personnel, except as provided for by law. Unauthorized access or dissemination of such information may result in disciplinary or criminal sanctions against the offending employee.

C. DEFINITIONS

ADVANCED AUTHENTICATION - The verification of a user's identity utilizing two (2) or more authentication methods (e.g. username/password, biometrics, proximity card, hardware tokens, paper tokens, etc.)

CRIMINAL JUSTICE INFORMATION SERVICES (CJIS) - Programs within both the FDLE and the FBI responsible for the collection, warehousing, and timely dissemination of relevant Criminal Justice Information to qualified law enforcement, criminal justice, civilian, academic, employment, and licensing agencies.

FLORIDA CRIME INFORMATION CENTER (FCIC) - The State of Florida's centralized database for tracking crime-related information, which can be queried by appropriate federal, state and local law enforcement and other criminal justice agencies.

NATIONAL CRIME INFORMATION CENTER (NCIC) - The national centralized database for tracking crime-related information, which can be queried by appropriate federal, state and local law enforcement and other criminal

justice agencies.

CRIMINAL JUSTICE NETWORK (CJNET) - A secure, private, statewide intranet system managed and maintained by the FDLE to connect Florida criminal justice agencies to various data sources provided by the criminal justice community, such as secure email accounts, training manuals and announcements, memos, policy and procedure manuals, links to intelligence databases, links to state and local information systems, etc.

FALCON (ICHS) - ICHS is used to perform tasks related to the management of applicant type fingerprints retained by FDLE when organizations submit criminal history background check requests. FALCON improves and expands biometric identification by utilizing available livescan technology to obtain and store an applicant and/or licensee's fingerprints. The prints are compared and subsequently retained within the FALCON system making the individual more readily identified.

CRIMINAL JUSTICE INFORMATION (CJI) - The term used to refer to all CJIS-provided data, either from the FBI or FDLE, necessary for law enforcement agencies to perform their missions and enforce the laws, including, but not limited to, biometric, identity history, biographic, property, and case/incident history data. CJIS FCIC/NCIC data is provided to criminal justice agencies and statutorily defined agencies for official criminal justice purposes. The term "criminal justice purpose" is defined in section **FSS 943.045(2)**, Florida Statutes, and **28 Code of Federal Regulations (CFR) Part 20.3** as follows: "Administration of criminal justice means performing functions of detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision, or rehabilitation of accused persons or criminal offenders by governmental agencies. The administration of criminal justice includes criminal identification activities and the collection, processing, storage, and dissemination of criminal justice information by governmental agencies." FDLE has adopted the FBI CJIS Security Policy as the foundation for FCIC, CJNet, Interstate Identification Index (III) and Computerized Criminal History (CCH) records related to information security. FCIC/NCIC data is any data obtained through a query to the FCIC message switch or other systems accessed via the CJNet (excluding DAVID), containing FCIC/NCIC Hot Files, Florida CCH and/or III/CCH information from other states and/or the FBI. Any information from an FBI system (NCIC, III, N-DEX) or FCIC or Florida criminal history record shall be considered CJI.

CRIMINAL HISTORY RECORD INFORMATION (CHRI) - CHRI is a subset of CJI and includes any notations or other written or electronic evidence of an arrest, detention, complaint, indictment, information or other formal criminal charge relating to an identifiable person that includes identifying information regarding the individual as well as the disposition of any charges. This includes Computerized Criminal Histories (CCH). Criminal History information is sensitive and should be treated as such. These records are disseminated only as a part of the user's criminal justice duties on a need to know, right to know basis. Voice transmission of a criminal history should be limited, and details of a criminal history should be given over a radio or cell phone only when an officer's safety is in danger or the officer determines that there is a danger to the public.
The following files shall be protected as CHRI:

1. Gang File
2. Known or Appropriately Suspected Terrorist File
3. Convicted Persons on Supervised Release File
4. Immigration Violator File (formerly the Deported Felon File)
5. National Sex Offender Registry File
6. Historical Protection Order File of the NCIC
7. Identity Theft File

The remaining NCIC files are considered "hot files." Improper access, use or dissemination of CHRI and Hot File information is serious and may result in administrative sanctions including, but not limited to, termination of services and state and federal criminal penalties.

PERSONALLY IDENTIFIABLE INFORMATION (PII) - PII is information that can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name. Any CJIS-provided data maintained by an agency, including but not limited

to, education, financial transactions, medical history, and criminal or employment history may include PII. A criminal history record, for example, inherently contains PII as would an N-DEx case file. PII shall be extracted from CJI for the purpose of official business only. PII must be protected as required by current state and local statutes. There is no requirement associated with PII and secondary dissemination. PII derived from CJI should be used only for official purposes.

PHYSICALLY SECURE LOCATION - For the purpose of this Directive, is a facility, a law enforcement vehicle, or an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect criminal justice information and associated information systems from unauthorized access.

TERMINAL AGENCY COORDINATOR (TAC) - The TAC is responsible for ensuring agency and user compliance with CJIS policies and procedures as they relate to FCIC and NCIC. The TAC is designated by the Chief of Police and serves as the point-of-contact for matters relating to CJIS information access.

LOCAL AGENCY SECURITY OFFICER (LASO) - The LASO ensures compliance with the FBI-CJIS Security Policy and any other applicable security requirements. LASOs should have technical knowledge of the department's network or be able to confirm information through local technical support. The LASO actively represents their agency in all matters pertaining to Information Security, disseminates Information Security alerts and other material to his or her constituents, and maintains Information Security documentation, including system and network configuration. The City's Technology Management Security Officer shall serve as the LASO.

D. USER AGREEMENT(S)

The User Agreement between an agency and FDLE/FBI is a legally-binding document that covers liability issues and outlines what is expected of the agency regarding proper use of FCIC/NCIC systems from that day forward. Whenever the agency head changes, the agency shall prepare and submit an updated User Agreement to FDLE. The Chief's Office shall be the central repository for these user agreements.

The agency TAC/LASO should be familiar with the contents of the agency's CJIS-related User Agreements. The TAC is responsible for notifying and ensuring that all agency users implement new CJIS procedures and capabilities when they are made available.

To be in compliance with the CJSI Security Policy the New Smyrna Beach Police Department (NSBPD) has User Agreements with FDLE, VSO and the New Smyrna Beach IT Department.

E. RELATED POLICIES

The following policies contain more information on CJI:

7-1 Disciplinary Protocol
32-4 Automated License Plate Readers

F. NETWORK & BUILDING SECURITY

26.5.1 The City of New Smyrna Beach Information Technology Department is responsible for maintaining the secure architecture. The FBI CJIS Security policy requires that FCIC/NCIC be encrypted to 128 bits when transmitted over a public network segment. FDLE encrypts FCIC/NCIC from the message switch to the edge routers at each

agency. The City of New Smyrna Beach Information Technology Department maintains a secure network architecture ensuring that all CJIS information is encrypted in transit over segments of the internal network not exclusively dedicated to the NSBPD purposes. The LASO shall maintain an up-to-date network diagram for review and audit purposes. All computers accessing FCIC/NCIC or the CJNet must have virus protection software installed and be regularly updated.

26.5.2 Access to the NCIC/FCIC terminal for a criminal history is possible from secure locations within the Police Department. Such access is controlled by secure access control badges and electronic locks. Access to secured locations is logged by access control server software and monitored by video surveillance.

26.5.3 Personally Owned Information Systems –BYOD (Bring Your Own Device) devices are prohibited from accessing the NSBPD CJIS network or the VSO CJIS network through internal and external network connections.

26.5.4 Remote access of any kind is prohibited on the NSBPD CJIS network, except for FDLE remote access that complies with CJIS Security Policy.

26.5.5 Wireless access is prohibited on the NSBPD CJIS network.

1. Wireless technology includes, but is not limited to, cellular networks, Bluetooth, satellite, and microwave.

26.5.6 Patch Management will be in compliance with the CJIS Security Policy.

1. NSBPD CJIS network patch management shall be done using Windows Server Update Services (WSUS) by authorized personnel from the City of New Smyrna Beach IT Department, on a monthly basis.
2. All MCT/laptops used to access the Volusia Sheriff's Office secure network are updated automatically through the use of Windows Update.

G. RESPONSIBILITIES OF THE INFORMATION TECHNOLOGY UNIT

26.5.7 The Information Technology Department shall be tasked with the planning, economics, and management of the agency's information technology security program and establishing related procedures. The Information Technology Department shall:

1. Provide for the development, coordination, dissemination, and maintenance of agency objectives, concepts, policies, procedures, and standards for managing information technology security; and
2. Provide for, or assist with, the development, coordination, maintenance, and implementation of information technology security documents related to:

    - Administrative procedures and members;
    - Physical and virtual environments;
    - Network and other communications mediums;
    - Hardware and software; and
    - Special testing/evaluation.

26.5.8 The internal security is the responsibility of the Information Technology Department, who shall serve as the CJIS Information Technology Security Officer and shall be the designated Local Agency Security Officer. The Information Technology Security Officer shall be required to:

1. Establish and document specific information technology security requirements;
2. Create new and improved policies, techniques, and procedures to fulfill information technology security requirements;
3. Develop practical guidelines that can be easily understood and used to economically protect sensitive information at the level required;
4. Establish an information technology security test and evaluation policy, procedures, and techniques, including a test and evaluation program;
5. Investigate any reported security incidents;
6. Identify who is using the Criminal Justice Information Services Systems Agency approved hardware, software, and firmware, and ensure no unauthorized individuals or processes have access to the same;
7. Identify and document how the equipment is connected to the state system;
8. Ensure that personnel security screening procedures are being followed as stated in this policy;

9. Ensure the approved and appropriate security measures are in place and working as expected; and
10. Support policy compliance.

26.5.9 The Information Technology Department shall be responsible for carrying out these information technology security policies and procedures including:

1. Safeguarding sensitive information in their custody;
2. Making sure members who receive sensitive information are authorized members who have proper need and access; and
3. Informing Information Technology customers and users of published security policies and procedures.

26.5.10 The Information Technology Department shall be responsible for the development of a comprehensive information security plan to protect the secure Department network and all information systems that access the secure Department network and its information. The information security plan shall be considered confidential and exempt from disclosure pursuant to **FSS 119.071(3)(a).**

26.5.11 Security Alerts & Advisories – The Information Technology Department shall:

1. Receive Information system security alerts/advisories on a regular basis.
2. Issue alerts/advisories to appropriate members.
3. Document the types of actions taken in response to security alerts/advisories.
4. Take appropriate actions in response to security alerts/advisories for all devices on the NSBPD CJIS network & all MCTs access the Volusia Sheriff's Office secure network.

26.5.12 The agency shall follow the secure password attributes listed to authenticate a member's unique identification. A member's password shall:

1. Be a minimum length of eight (8) characters on all systems;
2. Not be a dictionary word or proper name;
3. Not be the same as the user identification;
4. Expire within a maximum of ninety (90) calendar days;
5. Not be identical to the previous ten (10) passwords;
6. Not be transmitted in the clear (unencrypted) outside the secure location; and
7. Not be displayed when entered.

26.5.13 If an agency member forgets their password, they shall go to the Information Technology Department to have their password reset.

26.5.14 The information system shall prevent further access to the system by initiating a session lock after a maximum of thirty (30) minutes of inactivity. The session lock shall remain in effect until the user reestablishes access to the system using appropriate identification and authentication sign-on procedures.

H. VOICE OVER INTERNET PROTOCOL

26.5.15 The usage of department phone systems, including VOIP, digital or analog is strictly limited to police department employees and those contractors or vendors as authorized by the TAC and IT. The following additional controls shall be implemented:

1. The default administrative password on the IP phones and VOIP switches.
2. Virtual Local Area Network (VLAN) technology to segment VOIP traffic from data traffic shall be utilized.

I. CERTIFICATION REQUIREMENTS

26.5.16 Personnel who have written, computerized or audible access to CJI data will require either Full or Limited Access CJIS certification or CJIS Online Security certification within six months of initial assignment, and biennially (every two years) thereafter.

26.5.17 CJIS Online Security Certification is obtained by personnel reviewing online instruction offered by FDLE. This instruction will conclude with personnel taking a test administered by the software program. Users must pass the test and upon completion users can print a certificate. CJIS Online Security does not allow users to make queries, but does provide the user the knowledge to understand how to properly handle CJIS-related information.

26.5.18 Limited Access CJIS Certification is obtained by personnel reviewing online instruction offered by FDLE. This instruction will conclude with personnel taking a test using the nexTest online testing system. Users must pass the test and upon completion users can print a certificate. Limited Access Users will be granted query access only to CJIS related data.

26.5.19 Full CJIS Certification is obtained by personnel attending classroom training offered by a Limited Access Instructor (LAI). During the course the LAI will review from the CJIS Certification Training Manual. After attending the course, personnel are required to take test using the nexTest online testing system. Users must successfully pass the test and upon completion users can print a certificate and will be granted query, entry, modify, clear, cancel and locate access to CJIS related data.

26.5.20 All NSBPD employees, Information Technology employees, volunteers, vendors or contract services employees who work in or visit areas where CJI is accessible must complete CJIS Online Security Certification and maintain Security Certification. This group of individuals does not have the capability to query FCIC/NCIC transactions.

26.5.21 All NSBPD sworn personnel who have physical and logical access (as defined in CJIS Security Policy) to NSBPD computer networks with the ability to query FCIC/NCIC transactions must maintain Limited Access CJIS certification at all times.

26.5.22 If a user lets their certification lapse, regardless of assignment, they shall not access or view CJIS data nor contact Teletype or another certified user to query CJIS information for them, as the user with the expired certificate would not be authorized to receive CJIS information. Users will receive reminders from FCIC about their certification expiring beginning 90 days prior to their expiration date. When a user sees this expiration notice, the certification exam should be taken as soon as possible. Users who allow their certification to remain expired for two years or more will be required to complete the Online Limited Access User certification program.

26.5.23 FDLE will notify the agency TAC of expiring CJIS certifications. The TAC shall disseminate this list to sworn and civilian employees, their supervisors and the agency LASO, of upcoming expirations to the individuals with expiring certificates.

26.5.24 All users requiring certification shall contact the agency TAC to arrange for the proper training.

J. eAGENT

26.5.25 The FCIC eAGENT system is a browser-based application provided and maintained by FDLE that allows CJIS certified users to query, enter, modify, locate, clear and cancel records that are in the Florida Crime Information Center (FCIC II)/National Crime Information Center (NCIC2000) systems based upon their user authority. The purpose of this software for most users is to run criminal histories.

26.5.26 This software will be loaded onto the CJIS Network desktop computers. It shall not be loaded onto any MCT/Laptop designed for deployment in a vehicle or any desktop computer connected to the City Network. Users with Limited Access CJIS certification may access the designated CJIS Network desktop computer to fulfill the law enforcement functions required on CJNET and NCIC/FCIC.

26.5.27 The Attention (ATN) field must contain the employee identification number of the person requesting the CJIS data.

26.5.28 The Control (CTL) field must contain the employee identification number of the operator or employee submitting the CJIS data query.

K. EMAIL,FAXING, OR COPY/PASTE

26.5.29 Emailing or Faxing CJIS-related material is prohibited as the City's email system does not currently meet CJIS Encryption standards.

26.5.30 An agency must meet the requirements of the FBI CJIS Security Policy prior to cutting and/or copying and pasting from an FCIC/NCIC response (this would include any transaction received from the FCIC message switch) into a local system. Local systems include email, record management systems, jail management systems and any type of electronic storage media that is accessed via a network connection. Members shall not cut and/or copy and paste FCIC/NCIC and CHI responses into any application on the City Network.

L. DATA STORAGE

26.5.31 CJIS Data is prohibited from being stored on either City or personal Electronic Media. Electronic media includes, but is not limited to, diskettes, tape cartridges, ribbons, CDs, DVDs, hard drives from computers and USB flash drives.

26.5.32 Printers

A printer is defined as an electronic device capable of buffering the information only long enough to print. Information is not stored long term on this machine. CJIS data is prohibited from being printed on devices outside the secure area of the NSBPD.

26.5.33 Multi-Functional Devices

A multi-functional device is a copier, printer, scanner and/or fax machine capable of storing information long term. The disposal process for this machine should be treated the same as if it were a computer. CJIS data is prohibited from being printed on multi-functional devices outside the secure area of the New Smyrna Beach Police Department.

26.5.34 Cloud CJIS FCIC/NCIC

Employees are prohibited from transmitting or storing data on any Cloud solution without the approval of the City Local Agency Security Officer (LASO). Cloud solutions include Google apps (email, Google Docs, Google Sites), Facebook, etc., as those solutions do not currently meet CJIS encryption standards.

M. USER DISSEMINATION OF CRIMINAL JUSTICE INFORMATION

26.5.35 A criminal history is confidential information that can **only** be used for law enforcement purposes. Any other use is strictly forbidden by this directive and FDLE regulations.

26.5.36 Under no circumstances will members of the agency disseminate criminal history information outside the agency, including to other law enforcement personnel, verbally or in writing. NSBPD does not maintain secondary dissemination logs, as dissemination is not authorized. Criminal history information will not be given to outside

agencies such as the jail, State Attorney's Office (SAO), Clerk of the Court, or other police departments as those agencies have access to FCIC/NCIC information and systems.

26.5.37 Any release of criminal history information to another agency, physically or verbally, shall be a violation of department policy and any violations of this directive will be handled according to **Directive 7-1 Discipline Protocol.**

N. DISPOSAL

26.5.38 Disposal of Hardcopy Criminal Histories

Criminal history data is constantly changing and should be kept only until a case file is closed or the record is superseded, obsolete, or the administrative value is lost. Criminal histories should not be retained in case files stored in the Records Section. If a history is needed at a later time, a new history should be obtained. When destroying a criminal history record, the NSBPD will dispose of it in the appropriate bin labeled for shredding. Do not discard CJI in the trash. The destruction will be carried out internally at the direction of the TAC and will be carried out by authorized personnel, with CJIS Security Online Certification or better. Documents that have not lost their value and are still being kept for investigative purposes must be kept in a manner to prevent unauthorized or unintended access.

26.5.39 Disposal/Destruction of Electronic Media

Electronic media used to store FCIC/NCIC must be properly erased/sanitized/wiped prior to disposal (disposal includes reuse by or transfer to a non-criminal justice entity). Electronic media includes, but is not limited to, diskettes, tape cartridges, ribbons, CDs, DVDs, hard drives from computers and USB flash drives. It will be the policy of the NSBPD to physically destroy all computer and printer hard drives prior to disposing of any computer or printer that is used to access, view, retrieve, or print CJI.

1. Destruction shall be witnessed by a member who has been through the CJI background check process and who has successfully completed the security awareness training.
2. Media destruction may be accomplished by:

    - Digital tapes may be shredded or burned;
    - CD's and DVD's may be destroyed by shredding;
    - Flash drives may be destroyed by using a hammer or similar device;
    - Hard-drives (to include copier hard-drives, if equipped, that were used to produce CJIS information) may be destroyed by drilling multiple holes in the device.

3. The destruction shall be documented and will include the name(s) of the person(s) completing the destruct, and the CJIS qualified person witnessing the procedure.

O. AUDITS

26.5.40 FDLE Audits - FDLE Auditors conduct triennial (every three years) audits in compliance with ***FSS 943*** on every agency with access to the CJNet and FCIC/NCIC. Audits consist of an on-site visit by the audit staff. At the discretion of the auditors, an on-site visit can be performed at an agency regardless of the entry/non-entry status of that agency. The objective of the audit is to verify adherence to CJIS policies and procedures.

26.5.41 During an on-site visit, FDLE auditors will use a questionnaire to evaluate entries in the system and a sample of these entries will be checked for accuracy and proper validation procedures. The auditor will also need to review any Interagency User Agreements currently in use by the agency, perform a technical audit and review a network diagram. An out-briefing will be conducted, and any violations, potential problems, or recommendations will be identified, followed by a written report sent to the agency head. If an agency is cited with a violation, the agency must respond, in writing, within thirty (30) days identifying corrective measures taken to ensure compliance.

26.5.42 FBI Audits

The FBI CJIS Division is authorized to conduct a triennial audit (once every three years) as a minimum, to assess agency compliance with applicable statutes, regulations and policies. Audits may be conducted on a more frequent basis if the audit reveals that an agency is not in compliance. The FBI CJIS Division shall also have the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.

P. PHYSICAL SECURITY

26.5.43 Physical security measures for computers and network workstations are the responsibility of the office or unit where those systems are installed and located. The individual unit or office supervisor is responsible for providing physical safeguards for the hardware, software and data to the same extent as is provided for other agency property in the unit. All computers and workstations shall use both logical and physical security as preventative measures.

26.5.44 Computer equipment will be kept in areas not easily accessible to the public or unauthorized personnel. Agency personnel will control access to computers, servers, or attached hardware.

1. Access can also be considered the unintentional viewing of information on a computer screen. All computers must be placed in such a manner as to prevent viewing by unauthorized personnel.

26.5.45 Members shall log off any computer that contains or has access to the agency computer network, mail system, files, FCIC/NCIC, or software whenever they are no longer in physical control of the computer for an extended period of time.

26.5.46 Pursuant to the FBI CJIS Security Policy, any device outside of a Physically Secure Location that has access to criminal justice information shall require Advanced Authentication methods to verify the identity of a user. Such authentication shall be accomplished through the use of a USB Token or Grid Card.

1. Members shall immediately report lost or stolen authentication devices such as USB tokens to Information Technology so the device can be disabled from accessing agency systems.

26.5.47 Members are prohibited from opening multiple concurrent active sessions or logons for one user identification in applications accessing criminal justice information.

Q. DEVICE SECURITY

26.5.48 Access to desktop or mobile computers is governed by assignment. User Identification and Passwords control access to the network and programming.

26.5.49 MCT users shall close the lid or blank the screen of their computer when exiting the vehicle IF any CJI or NCIC/FCIC application/screen is open and able to be seen from outside the vehicle, to prevent non-CJIS-certified members or citizens from viewing data on their screen.

R. NCIC/FCIC RECORDS VALIDATION

26.5.50 The Volusia Sheriff's Office Records Section will complete all Validations for the NSBPD based on the VSO FCIC High Speed Interface User's Agreement.

S. NCIC/FCIC "HIT" CONFIRMATION PROCEDURE

26.5.51 The following procedures will be used to verify the status of property or persons that have been entered

into the NCIC/FCIC computer database:

26.5.52 Normal Business Hours (Monday through Fridays 0800/1800) – Requests will be forwarded to the Police Department Records Section.

26.5.53 After-hours including holidays – for records entered after 04/30/12-Verification will be handled by the Volusia Sheriff's Department Records Section;

26.5.54 After Hours including holidays – for records entered before 05/01/12—Verification will be handled by a police supervisor. To confirm a record, access the report, check the case status (i.e. Open, closed, etc.) and check the property section for stolen/recovered items and review supplements as appropriate.

T. DAVID

26.5.55 Employees of the NSBPD are NOT allowed to access DAVID from any personally own device/computer. Device includes but is not limited to smartphones, tablets and any other similar device.

26.5.56 If a MCT/Laptop is removed from the patrol vehicle the user is prohibited from accessing the DAVID database.

U. INCIDENT RESPONSE

26.5.57 It will be the policy of the NSBPD to notify FDLE of any Security Incident. Any actual or suspected Security Incident should be reported to the NSBPD TAC and/or LASO. The TAC/LASO will notify FDLE using the procedures in the FCIC Full Access Certification Manual (see below).

26.5.58 Security Incidents

A security incident is a violation or possible violation of the technical aspects of the CJIS Security Policy that threatens the confidentiality, integrity or availability of FCIC/NCIC. Users may only see indicators of a security incident. The following is a partial list of incident indicators that deserve special attention from users and/or system administrators:

1. The system unexpectedly crashes without clear reasons
2. New user accounts are mysteriously created which bypass standard procedures
3. Sudden high activity on an account that has had little or no activity for months
4. New files with novel or strange names appear
5. Accounting discrepancies
6. Changes in file lengths or modification dates
7. Attempts to write to system files
8. Data modification or deletion
9. Denial of service
10. Unexplained poor system performance
11. Anomalies
12. Suspicious probes
13. Suspicious browsing

26.5.59 Members noting any of the above or any other activity that is suspicious shall report their concern to the Department's Local Agency Security Officer (LASO), TAC (Terminal Agency Coordinator) or any available IT Specialists. The incident should be reported to the FDLE ISO via email at: CJISCSO@fdle.state.fl.us and the message subject line should say "possible security incident". The email should include the following information: date of the incident, locations of incident, systems affected, method of detection, nature of the incident, description of the incident, actions taken/resolution and contact information for the agency.

26.5.60 Currently, the NSBPD does not allow CJIS access via smartphones, tablets, or similar devices. The use of this technology requires the minimum security precautions as applied to wired technology and, based upon the specific technology, may require additional security controls. The required enhanced response policy for mobile devices shall be promulgated if/ when mobile devices are deployed.

V. VIOLATIONS

26.5.61 Any member of the NSBPD who violates the provisions of this Policy or any laws or regulations pertaining to the dissemination of criminal history records information, or any other information obtained through the F.C.I.C/ N.C.I.C computer terminal is subject to discipline, to include possible termination, and possible prosecution under State and/ or Federal Law, and civil liability. The New Smyrna Beach Police Department will assist in any State and/ or Federal investigation of misuse of any information obtained from the F.C.I.C/ N.C.I.C terminal or any violation of Criminal History Information.

W. FALCON NATIONAL RAP BACK

26.5.62 The FBI Next Generation Identification (NGI) Noncriminal Justice (NCJ) Rap Back Service will provide national notifications when the following triggering events occur:

- Criminal arrests
- Want Additions and Deletions (new warrant entry which includes the individual's FBI/UCN number)
- Sexual Offender Registry Additions and Deletions
- Death Notice with Fingerprints

26.5.63 It will be the policy of the NSBPD to notify potential applicants of their rights prior to being fingerprinted and/or prior to an applicant's resubmission to establish a National Rap Back subscription along with a sample of the notification. The notification must address the retention of fingerprints, privacy policy, and the right to challenge an incorrect criminal history record.

26.5.64 The department will retain the signed applicant notification and acknowledgment document in the agency file for audit purposes. Authorized personnel will also make sure those that have separated from the agency are deleted from the system to ensure CJI for them is not received.

X. PERSONALLY IDENTIFIABLE INFORMATION

26.5.65 Personally Identifiable Information (PII)-Any information pertaining to an individual that can be used to distinguish or trace a person's identity.

- New Smyrna Beach Police Department will ensure the appropriate access, use, handling, storage and dissemination of Personally Identifiable Information in accordance with **FSS817.568** and **FSS 943.125**.

Revised: BSS 8/22

Approved: Signature on File
Chief Mike Coffin