SPRINGFIELD TOWNSHIP POLICE DEPARTMENT
Wyndmoor, Pennsylvania

Policy 5-06

Policy Title: CLEAN and NCIC

Date of Issue: December 1, 2022 **Rescinds:** None

By Authority of: Chief of Police

I. Purpose

The purpose of this policy is to establish procedures for this department to maintain compliance with rules and regulations developed by the State and Federal Agencies which regulate the Commonwealth Law Enforcement Assistance Network (CLEAN), and the National Crime Information Center (NCIC) terminal. This order is meant to provide basic in-house operation procedures for the Springfield Township Police Department. CLEAN and NCIC have operating standards which by reference are included as part of this order and shall be complied with by all department personnel. Any additional information on these standards can be found in the NCIC manual, online help, or other related material on file in the department.

II. Policy

A. It shall be the policy of the Springfield Township Police Department to comply with the State and Federal laws, rules and regulations, as well as the requirements established in this order concerning CLEAN and NCIC. Additionally, this agency shall comply with all record keeping requirements for the terminal and shall maintain such records for the required periods of time. Nothing contained in this order shall supersede the rules and regulations of CLEAN or NCIC. Any part of this order found to be contrary shall be null and void.

B. Employees of the Springfield Township Police Department are prohibited at all times from using the law enforcement databases available to the department to query themselves or their immediate family. No exception exists. This includes but is not limited to driver's license information, registration information, and criminal history information.

III. Definitions

A. CLEAN

1. CLEAN is used by the Commonwealth's criminal justice agencies to access driver license and motor vehicle information, state criminal history record information maintained in the Pennsylvania State Police Central Repository, the Commonwealth's central registry for Protection from Abuse orders, "hot" (stolen and wanted) files, law enforcement messaging capabilities, and a host of other services. CLEAN is Pennsylvania's conduit to NCIC, the FBI's National Crime Information Center, and to NLETS, the National Law Enforcement Telecommunications System.

2. CLEAN maintains connections to over forty other networks, including the Pennsylvania Justice Network (JNET). JNET interfaces with CLEAN to access criminal history information, arrest data, protection from abuse information, and "hot" files.

3. CLEAN access and the use of criminal justice systems and information is restricted to criminal justice agencies. The CLEAN Administrative Section in PSP's Bureau of Technology Services is responsible to the FBI's Criminal Justice Information Services (CJIS) Division to ensure that NCIC regulations are enforced among Pennsylvania NCIC users. In addition, the CLEAN Administrative Section prescribes regulations for CLEAN system use, conducts user training, audits transactions to maintain system security and discipline, and investigates allegations of misuse of information systems.

4. CLEAN is capable of sending law enforcement messages such as Be On the Look Outs (BOLOs), requests for motor vehicle registration data, notification of robberies, requests for information, legal bulletins, and road and weather reports. Messages can be sent from 10 to 99 miles, statewide, or by regions. There are eight (8) different regions which consist of groups of states and agencies.

B. NCIC

1. NCIC is a computerized index of criminal justice information (i.e. criminal record history information, fugitives, stolen properties, missing persons). It is available to Federal, state, and local law enforcement and other criminal justice agencies and is operational 24 hours a day, 365 days a year.

2. The purpose for maintaining the NCIC system is to provide a computerized database for ready access by a criminal justice agency making an inquiry, and for prompt disclosure of information in the system from other criminal justice agencies about crimes and criminals. This information assists authorized agencies in criminal justice and related law enforcement objectives, such as apprehending fugitives, locating missing persons, locating and returning stolen property, as well as in the protection of the law enforcement officers encountering the individuals described in the system.

3. There are two types of NCIC information:

   a. "HOT" Files – consisting of the Vehicle, License Plate, Boat, Gun, Article, Securities, Wanted Person, Foreign Fugitive, United States Secret Service Protective, Missing Person, Unidentified Person, and the Bureau of Alcohol, Tobacco and Firearms Violent Felon File.

b. Interstate Identification Index (III) – contains extremely sensitive records for offenders of serious and or significant violations that are:

   i. Known to the FBI

   ii. With a date of birth of 1956 or later

   iii. Arrested for the first time and reported to the FBI Identification Division since July 1, 1974 (regardless of date of birth).

C. National Law Enforcement Telecommunication System (NLETS) - NLETS was created by the principal law enforcement agencies of the states. Since its founding, NLETS' role has evolved from being primarily an interstate telecommunications service for law enforcement to a more broad-based network servicing the justice community at the local, state, and Federal levels. It is now the pre-eminent interstate law enforcement network in the nation for the exchange of law enforcement and related justice information.

IV. Background

A. The CLEAN and NCIC terminal allows this agency access to online records held within the files of the Pennsylvania State Police, Pennsylvania Department of Transportation and the FBI which operates NCIC. Access is granted to out of state records as well, via the NLETS.

B. The CLEAN / NCIC terminals has been placed into all desktop computers in the Springfield Township Police Department under an agreement with the Pennsylvania State Police that this agency will comply with all regulations as promulgated by the State and Federal agencies who control the access to the records provided through the terminals. This agency will comply with all regulations and shall not misuse the information gathered via the terminals contrary to any of these regulations.

C. The administration of CLEAN / NCIC access by this department is under the authority of the Chief of Police. The Chief of Police may delegate administrative and operational responsibilities for managing and maintaining the integrity of the department's CLEAN / NCIC access to sworn and / or civilian members of this department. Any such delegation shall be consistent with the policies of the department and the rules and regulations of CLEAN / NCIC.

V. Procedures

A. CLEAN / NCIC requests from outside criminal justice agencies shall not be honored. Doing so could result in this department losing CLEAN / NCIC access. Printouts of CLEAN / NCIC information contain this department's ORI number. If we give this printout to an outside agency and they discard it or lose it, and it is later found by another party, we will be held

liable, not the agency given the printout. Failure to abide by this provision shall result in disciplinary action in accordance with department policy.

B. If a CLEAN terminal operator is requested to perform a function on the CLEAN terminal that may be in violation of law or CLEAN / NCIC policy, the operator shall immediately contact the TAC Officer if working, or if not available, any supervisor, or the Chief of Police, for resolution.

C. Department Information Security Officer (ISO)

1. The department ISO is the department liaison to CLEAN security officers. The CLEAN security officer is the liaison to FBI CJIS Division on all technical security issues related to our CLEAN equipment.

2. All new network connections to CLEAN must be approved by the department's ISO through the County and CLEAN ISOs.

3. All intrusions into an agency network must be reported to the department ISO for reporting to the County and CLEAN ISOs for reporting to FBI CJIS Division.

D. Terminal Agency Coordinator (TAC) Officer

1. System's management for CLEAN / NCIC access, and integration into the department's computerized information system, is the responsibility of the TAC Officer.

2. CLEAN / NCIC auditing of the terminal's use and function, daily filing and review of information is the responsibility and is controlled by the TAC Officer. The TAC Officer shall be designated by the Chief of Police and shall have attended the Administrator training conducted by the Pennsylvania State Police.

3. The TAC Officer is responsible to ensure:

a. The storage and filing of records generated by the use of the terminal.

b. The administering of the terminal testing for operators as required by PSP.

c. Completion of monthly validations.

d. Attendance at CLEAN user group meetings.

e. Submission of a list of authorized CLEAN users to the CLEAN Administrative Unit.

f. Receipt of NCIC matters and NCIC memorandums and corrections of problems associated with such messages.

E. CLEAN Stationary Terminal Operators

1. Only authorized employees of this department may access information by use of the CLEAN / NCIC terminal. All operators must be currently certified by completion of the mandatory background investigation and testing requirements of the Pennsylvania State Police. The only exception to this would be an employee in training and under the immediate supervision of the certified operator conducting training.

2. Prior to being authorized CLEAN / NCIC access, employees shall undergo a background investigation which shall include submission of a completed FBI applicant fingerprint card. The card shall be submitted to the FBI Identification Bureau, through the Pennsylvania State Police, Records and Identification Division.

3. All operators shall undergo a Criminal History check for convictions of misdemeanor or felony crimes. The Criminal History check shall include a state and national fingerprint search for a criminal history.

    a. Should a conviction be found, authority for use of the CLEAN / NCIC terminal shall immediately be suspended.

    b. Convictions for any of the following shall show cause for the aforementioned suspension of access privileges:

        i. Conviction or under indictment for any felony.

        ii. Conviction for any misdemeanor where the person was incarcerated within the last ten years.

        iii. Conviction for two or more misdemeanors within the last ten years.

        iv. Misdemeanors and felonies under the laws of Pennsylvania, and the laws of any other State, or Federal Law.

    c. A computerized Criminal History check shall be repeated each time that an operator is due to recertify.

4. Obtaining an account

    a. A CLEAN account is created by the TAC in the CLEAN portal via remote administrator.

    b. The new user will then complete the training and testing in the CLEAN system.

    c. The department will then create a mobile data terminal access account for the new user.

5. User Transfer or Termination

a. When a user is transferred or terminated, the TAC Officer shall submit a request to CLEAN Administration for the user's account be deactivated.

F. CLEAN Stationary Terminal Operators and CLEAN / Mobile Data Terminals

1. All operators shall be required to acknowledge and accept CLEAN's "Statement of Liability" when signing onto the portal. Any violations of the requirements contained in this "Statement of Liability" are viewed as serious violations since they may affect this department's ability to continue to use CLEAN and NCIC. Failure to abide by this provision shall result in disciplinary action in accordance with department policy.

2. All operators shall use their own sign-on when operating any terminal for the purposes of querying or inputting CLEAN / NCIC records.

3. Operators shall ensure that any protected information obtained from the terminal usage is protected and not made available to the public in any way.

4. All operator information screens or any other screens wherein the requestor's name can be entered in compliance with CLEAN regulations shall have the name of the requestor entered.

5. Terminal operators shall sign-off when not in control of the terminal even when relieved for a few minutes for personal reasons.

6. If a criminal justice official with access to CLEAN / NCIC is arrested or indicted for a felony or misdemeanor, that official shall lose access to CLEAN / NCIC until the charges are disposed in court. The official shall permanently lose current CLEAN / NCIC access if convicted, as defined below:

   a. Conviction for any felony

   b. Conviction and incarceration for any misdemeanor

7. The Bureau of Records and Information Services, CLEAN Administrative Section Supervisor, must be notified within five (5) days of receipt of a positive criminal history response meeting the aforementioned criteria. The final decision as to whether the individual will be granted CLEAN / NCIC access will be made by the Control Terminal Officer (CTO).

8. Training

   a. The testing is administered by the TAC Officer and must be completed independently.

   b. All terminal users, shall be required to maintain proficiency in the use of any terminal which they are authorized to use for CLEAN / NCIC access.

c. All new employees who will be using CLEAN / NCIC access computers shall receive training in the use of such terminal. This training shall be limited to the functions related to their level of certification by the TAC Officer. The trainee will be monitored while using any access computer.

   i. Primary terminal training can be conducted by the TAC officer.

   ii. Mobile data software training may be conducted by the TAC Officer or Field Training Officers (after initial training by TAC Officer).

d. After completion of the training and demonstration to the TAC Officer of their ability to perform the functions of the terminal the trainee will be administered a test from CLEAN / NCIC and must pass the test prior to using the terminal. They must also demonstrate their knowledge and ability to use the online help screens provided by CLEAN / NCIC.

e. There are four (4) levels of CJIS Security Training as follows:

   i. Level 1 CJIS Security Training – Personnel with unescorted access to a physically secure location (This level is designated for people who have access to a secure area, but are not authorized to us CJI). This level will include cleaning personnel, vendors other than IT vendors, and other Township employees.

      a. Required

         1. Fingerprinted (one time only).

         2. RAP Sheet (every two years).

         3. Security Awareness Training (every two years).

   ii. Level 2 CJIS Security Training – All personnel with access to CJI (This level is designated for people who do not have physical and logical access to CJI but may encounter it in their duties). This level will include the civilian employees of this agency.

      a. Required

         1. Fingerprinted (one time only).

         2. RAP Sheet (every two years).

         3. Security Awareness Training (every two years).

iii. Level 3 CJIS Security Training – All personnel with access to both physical and logical CJI. This level includes all sworn personnel, Terminal Operators, and TAC Officers.

a. Required

1. Fingerprinted (one time only).

2. RAP Sheet (every two years).

3. CLEAN nexTEST (every two years).

iv. Level 4 CJIS Security Training – Personnel with Information Technology Roles (This level is designed for all information technology personnel including system administrators, security administrators, network administrators, etc.). This level includes County IT, and IT vendors.

a. Required

1. Fingerprinted (one time only).

2. RAP Sheet (every two years).

3. Security Awareness Training (every two years).

G. Stationary Terminal Functions

1. While CLEAN terminals assigned to this department are capable of entries, removals, and queries, MCEDS is the only source to be used for CLEAN / NCIC entries and removals.

2. Messages via CLEAN / NCIC

a. The TAC officer shall review all received messages which specifically list this police agency's ORI (PA0462300), to include entries, modifications, cancellations, hits, locates, and general messages (to include BOLOs, trainings, alerts, and notifications). Message do not need to be printed, except for those pertaining to persons wanted by outside agencies requiring local detention.

b. Messages shall only be posted with a supervisor's approval.

H. It is the responsibility of every member of this agency to provide concise information for entry or query of information into CLEAN / NCIC.

1. The entry of information into the CLEAN / NCIC system is controlled and reviewed by the State Police computer center. This information is checked against standards that allow for consistent entry into the system.

2. All information to be entered into the system shall be done at the direction of the officer requesting such entry. A report number shall be included. It shall be the responsibility of the officer to furnish, review, and approve the information for entry. The officer shall verify the accuracy of the entry.

3. Requests for entry should be made to MCEDS on the appropriate electronic form.

I. Verifying Vehicle VIN, License Plate, and Firearms Serial Numbers

1. This department has various means of verifying VINs and registration plate numbers for vehicles and checking firearm records. Prior to the entry of these items the officer shall:

   a. For vehicles, run a search through PennDOT files either by VIN, registration, or owner information.

   b. For firearms, make an inquiry of the firearms owned by the crime victim in the PSP files.

J. Entry of Stolen Articles and Securities

1. Items that may be entered in the articles file include, but are not limited to, the following:

   a. Office equipment.

   b. Stereo equipment.

   c. Cellular phones.

   d. Bicycles.

   e. Jewelry.

   f. Serialized lottery tickets.

   g. Television sets.

2. Items that may be entered in the securities file include, but are not limited to, currency, money orders, traveler's checks, and savings certificates (see CLEAN on-line manual for complete listing).

K. Missing Person Entry

1. Adults

a. The officer responsible for the initial investigation of a missing person report shall ensure that the information is provided to MCEDS / CLEAN for entry into the CLEAN / NCIC system.

b. The officer responsible for follow-up investigation of a missing person report shall ensure that additionally obtained information is provided for entry into the NCIC system.

c. Copies of the data entry shall be processed in accordance with established NCIC and this order.

d. Any police officer or detective who completes a supplemental investigation report involving the locating of a missing person entered by this department in the NCIC system shall promptly have the file entry removed from the system.

2. Juveniles

a. Information entered into CLEAN / NCIC on a missing child should include, but is not limited to; full name, nickname, date and place of birth, age, social security number, operator's license number, height, weight, color of hair and eyes, use of eyeglasses or contacts, physical or mental handicaps, special medical conditions or needs, scars and marks, or any other distinguishing characteristics. Information should also be entered regarding any vehicle the missing child might be using or traveling within, as well as any persons that the missing child might be with.

b. In all cases, the missing child shall be entered into CLEAN / NCIC as soon as possible after the information is obtained. There shall be no waiting period before entry is made.

L. Entry of a Wanted Person(s) for Criminal Warrants

1. Warrant procedures shall be followed per department policy.

2. Warrants are entered into the AOPC (Administrative Office of the Pennsylvania Courts) system by the issuing Magisterial District Justice's office. Misdemeanor and felony warrants are automatically entered into NCIC and CLEAN through AOPC.

3. The information used for the warrant is obtained directly from the criminal complaint; therefore, it is the responsibility of the officer completing a criminal complaint to ensure that the information on the complaint is accurate.

4. If a warrant is obtained by an officer who considers a CLEAN / NCIC entry urgent, and it is outside of the normal MDJ business hours, the officer may have the warrant entered immediately. The Wanted Persons Information form shall be completed to assist personnel with the entry. The officer shall include the NCIC reference number into their incident / CFS report.

5. If a warrant received has not been entered into CLEAN / NCIC, and it is later determined that the warrant should be entered, the entering officer shall either notify the MDJ or following the instructions in Section V (L) (4) above.

6. CLEAN / NCIC warrant entries handled by an officer require a supplement to the original report.

M. Record Modifications

1. Occasionally information may be entered and accepted initially and after checking may be found to be incorrect. In the event this occurs, MCEDS / SCOPE is to be contacted to make the modification / correction. The information contained in the modified records shall be compared to the original information obtained by the officer for accuracy.

   a. Should the information in the incident report be found to be incorrect, the incident report shall be modified by submission of a supplement report along with the record of modification. The record modification shall be an attachment to the supplement in the incident / CFS.

   b. If the incident report is accurate and an entry error occurred, the record modification only shall be submitted and attached in the incident / CFS.

N. Hit Confirmation

1. In the event of a location of a wanted person, stolen vehicle, or other property MCEDS will coordinate with the shift supervisor on duty to handle the incident in accordance with CLEAN rules and regulations.

2. If the department receives a positive "hit" on a wanted person, property, or vehicle, the MCEDS dispatcher will radio the officer and state "Unit 28-XX, 10-99." This alerts the officer to a positive hit on the want requested and they should determine if they should distance themselves from the person or situation. MCEDS will not give the information until told to do so by the officer.

3. Enforcement action shall not be taken based solely on the results of a "hit" on an inquiry. Officers also have to follow up with the hit confirmation request.

O. Cancellation of Entries

1. At any time there is a need to cancel a CLEAN / NCIC entry for whatever reason the entry shall be canceled without delay. Copies of the cancellation shall be forwarded to the TAC Officer.

2. The only exception to an immediate cancellation will be with wanted person(s).

a. The entry will remain until the preliminary arraignment before a Magisterial District Judge or other appropriate official on our charges, and at that time the entry will be cancelled.

P. Criminal History Records

1. The only personnel of this agency authorized to request a criminal history check on an individual is a CLEAN Criminal History user.

2. When requesting a criminal history, it can be done for two reasons only;

   a. Investigation involving suspected criminal activity. This requires a "C" code. A reason (RSN) must be completed with the OCA and or report number.

   b. Employee background checks. This requires a "J" code and may be conducted by a CLEAN Criminal History user as chosen by the Chief of Police.

3. Upon receipt of a criminal history record, the printed copy of the record shall be reviewed, and the information contained within shall be noted in the case folder. Once noted and recorded, the printed copy shall then be disposed of in accordance with CLEAN rules and regulations.

Q. Validations

1. Validation is the process by which the entering agency confirms, on an annual basis, that each NCIC entry is accurate, complete, and still outstanding or active. Records must be validated within 90 days from the date that they are first entered into NCIC. Thereafter, validations are completed annually.

2. Each month the entering agency receives a printout of their records from CLEAN and NCIC from the following files:

   a. Wanted Person.

   b. Missing Person.

   c. Unidentified Person.

   d. Boat.

   e. License Plate.

   f. Vehicle.

   g. Vehicle Parts.

   h. Gun.

i. Securities.

3. Each record in the printout must be compared to the supporting documents, such as:

   a. Case Files.

   b. Incident Reports.

   c. Warrants.

4. Comparisons include:

   a. Examining the record to ensure accuracy.

   b. Examining the documents (report, warrants, etc.) to ensure all the information contained in them is included in the record.

   c. Ensuring all information in the record can be verified by the supporting documents.

5. A second validation step is necessary for validation of:

   a. Wanted Persons File.

   b. Missing Persons File.

   c. Note: Consultation must be made with any appropriate complainant, victim, prosecutor, court, motor vehicle registry files, or to other appropriate source or individuals to ensure that the entry is still valid and should remain in the NCIC system.

6. Receipt of Validation Sheets

   a. CLEAN admin emails validation sheets directly to TAC officers. On receipt of the validation sheets the following shall be verified:

      i. Wanted person(s) entry verifications shall be done by checking that the original warrant is on file. In the case of a Wanted Person file, a "sealed" warrant must be available for confirmation and validation. Since all missing person investigations are assigned to an officer or investigator they shall also be contacted for the verification.

      ii. Stolen vehicle records shall be verified by forwarding a letter to the victim(s) last known address stating that we will be holding the record open unless notified that the vehicle has been recovered.

iii. Stolen vehicle registration plates shall be verified by forwarding a letter to the victim(s) last known address stating that we will be holding the record open unless notified that the vehicle registration plate has been recovered.

iv. Stolen gun records shall be verified by forwarding a letter to the victim(s) last known address stating that we will be holding the record open unless notified that the gun has been recovered.

v. Stolen articles shall be verified and since they are removed from CLEAN / NCIC on a scheduled purge they will be verified by examination of the case status.

vi. Missing person(s) entry verifications shall be done by checking the original incident report and verified with the reporting party. Since all missing person investigations are assigned to an officer or investigator they shall also be contacted for the verification.

b. Verification letters sent by this agency shall include the following information.

i. Victim's name and last known address.

ii. Date of entry and of incident.

iii. Incident number.

iv. Description of missing item to include serial number or VIN.

c. The verification letter will require response, especially if the items have been recovered. The letter will also state that their failure to notify us of the recovery may place the person(s) in possession of the property in jeopardy of being detained by police.

d. Should a verification letter be returned undeliverable, attempts to find a new address shall be made. No records shall be cancelled until approved by the TAC Officer after their review of the attempts to locate the victim.

7. The CLEAN validation process is outlined in Attachment A.

VI. Personal Sanctions Policy and Accountability

A. Disciplinary Policy

1. The Springfield Township Police Department provides its personnel with the needed technological resources to access FBI CJIS systems and information in support of the agency's mission. All agency personnel, with access to FBI Criminal Justice Information

(CJI) or any system with stored FBI CJI, have a duty to protect the system and related systems from physical and environmental damage and are responsible for correct use, operation, care and maintenance of the information. All technology equipment: computers, laptops, software, copiers, printers, terminals, MDTs, mobile devices, live scan devices, fingerprint scanners, software to include RMS / CAD, operating systems, etc., used to process, store, and/or transmit FBI CJIS is a privilege allowed by the Springfield Township Police Department, state CSO, and the FBI. To maintain the integrity and security of the Springfield Township Police Department's and FBI's CJIS systems and data, this computer use privilege requires adherence of relevant federal, state and local laws, regulations and contractual obligations. All existing laws and Springfield Township Police Department regulations and policies apply, including not only those laws and regulations that are specific to computers and networks, but also those that may apply to personal conduct.

2. 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 for 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 for evidence laid down in the relevant jurisdiction(s). Complaints alleging misuse of the Springfield Township Police Department computing and network resources and FBI CJIS systems and/or data will be directed to those responsible for taking appropriate disciplinary action.

B. Examples of Misuse with Access to FBI CJI

1. Using someone else's login that you are not the owner.

2. Leaving computer logged in with your login credentials unlocked in a physically unsecure location allowing anyone to access Springfield Township Police Department systems and / or FBI CJIS systems and data in your name.

3. Allowing unauthorized person to access FBI CJI at any time for any reason. Note: Unauthorized use of the FBI CJIS systems is prohibited and may be subject to criminal and / or civil penalties.

4. Allowing remote access of Springfield Township Police Department issued computer equipment to FBI CJIS systems and / or data without prior authorization by the Springfield Township Police Department.

5. Obtaining a computer account that you are not authorized to use.

6. Obtaining a password for a computer account of another account owner.

7. Using the Springfield Township Police Department network to gain unauthorized access to FBI CJI.

8. Knowingly performing an act which will interfere with the normal operation of FBI CJIS systems.

9. Knowingly propagating a computer virus, Trojan horse, worm and malware to circumvent data protection or compromising existing security holes to FBI CJIS systems.

10. Violating terms of software and / or operating system licensing agreements or copyright laws.

11. Duplication of licensed software, except for backup and archival purposes that circumvent copyright laws for use by the Springfield Township Police Department, for home use or for any customer or contractor.

12. Deliberately wasting computing resources to include streaming audio, videos for personal use that interferes with Springfield Township Police Department network performance.

13. Using electronic mail or instant messaging to harass others.

14. Masking the identity of an account or machine.

15. Posting materials publicly that violate existing laws or Springfield Township Police Department codes of conduct.

16. 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.

17. Using Springfield Township Police Department technology resources to advance unwelcome solicitation of a personal or sexual relationship while on duty or through the use of official capacity.

18. Unauthorized possession of, loss of, or damage to Springfield Township Police Department technology equipment with access to FBI CJI through unreasonable carelessness or maliciousness.

19. Maintaining FBI CJI or duplicate copies of official Springfield Township Police Department files in either manual or electronic formats at his or her place of residence or in other physically non-secure locations without express permission.

20. Using Springfield Township Police Department technology resources and / or FBI CJIS systems for personal or financial gain.

21. Deliberately failing to report promptly any known technology-related misuse by another employee that may result in criminal prosecution or discipline under this policy.

22. Using personally owned devices on Springfield Township Police Department network to include personally-owned thumb drives, CDs, mobile devices, tablets on wifi, etc. Personally-owned devices should not store Springfield Township Police Department data, state data, or FBI CJI.

23. The above listing is not all-inclusive and any suspected technology resource or FBI CJIS system or FBI CJI misuse will be handled by the Springfield Township Police Department on a case by case basis. Activities will not be considered misuse when authorized by appropriate Springfield Township Police Department officials for security or performance testing.

C. Privacy Policy – All agency personnel utilizing agency-issued technology resources funded by the Springfield Township Police Department expressly acknowledges and agrees that such service, whether for business or personal use, shall remove any expectation of privacy. Use of Springfield Township Police Department systems indicates consent to monitoring and recording. The Springfield Township Police Department reserves the right to access and audit any and all communications including electronic and physical media at rest, in transit and at end of life. Springfield Township Police Department personnel shall not store personal information with an expectation of personal privacy that are under the control and management of the Springfield Township Police Department.

D. Personal Use of Agency Technology – The computers, electronic media and services provided by the Springfield Township Police Department are primarily for business use to assist personnel in the performance of their jobs. Limited, occasional, or incidental use of electronic media (sending or receiving) for personal, non-business purposes is understandable and acceptable, and all such use should be done in a manner that does not negatively affect the systems' use for their business purposes. However, employees are expected to demonstrate a sense of responsibility and not abuse this privilege

E. Misuse Notification

1. Due to the increase in the number of accidental or malicious computer attacks against both government and private agencies, the Springfield Township Police Department shall:

    a. Establish an operational incident handling capability for all information systems with access to FBI CJIS systems and data. This includes adequate preparation, detection, analysis, containment, recovery, and user response activities;

    b. Track, document, and report incidents to appropriate agency officials and/or authorities.

2. The Information Security Officer (ISO) is the point of contact on security-related issues for this department, who shall ensure proper incident response reporting procedures at the local level.

3. All Springfield Township Police personnel are responsible to report misuse of Springfield Township Police Department technology resources to appropriate Springfield Township Police Department officials.

4. See Attachment A for the Department's Information Security Officer (ISO).

VII. Miscellaneous

CLEAN users can find the most recent and up-to-date information regarding CLEAN rules, regulations, documents, and training using the CLEAN PortalXL under Links / CJIS Launch Pad.

VIII. Attachments

A. CJIS Validations Monthly Process Training Document

B. Terminal Operators List

ATTACHMENT A

CJIS Validations Monthly Process

PEAK PERFORMANCE SOLUTIONS

This document is designed to help you through each step using the CJIS Validations application. For additional help with individual operations, please refer to the help files in the application.

**** The first time you login to the CJIS Validations system, you will be presented with the option to take the online tutorial. We highly recommend that you spend a few minutes to go through the course. It will guide you through all of the screens that you will need to accomplish your validations using this application. You can return to this tutorial any time by going to the online help section within the application.

Step 1

You will receive a validation notification via email or admin message that will inform you that your records are ready to be validated. Simply login and proceed to the "Reports" screen. This is where you will work with your records. First, you can view or print your records in the "Print Validations" section. You could also use our "Checklist Report" to mark your validation actions as you work with them, and easily process them when you are finished.

Step 2

Once you have validated the record information and are ready to send the validation transactions or mark them as completed, you can use either the "Batch Validations" or "Interactive Validations" screen. The "Batch Validations" screen allows you to send up to 50 transactions at a time. The "Interactive Validations" screen allows you to validate one at a time. Make sure to select the appropriate action when using these screens. If you select the "Cancel" option it will remove these records from NCIC or your state files.

Step 3

After you have completed the validation process it is ***Very Important*** that you check the "Summary Reports" section and make sure all of the transactions processed correctly. If you have any records in the "Pending Ack" column, you will need to determine why they did not process and correct them. We have a "Pending Records Help" document to help you with this process.

Congratulations! Now that you have marked all your records as complete and have verified there are no pending records, you have completed your validations for the month.

ATTACHMENT B

Terminal Operators List

TAC OFFICERS: Detective Corporal Robert Chiarlanza
Detective Robert Baiada

INFORMATION SECURITY OFFICER: Detective Corporal Robert Chiarlanza