ELIZABETH POLICE DEPARTMENT
GENERAL ORDERS

VOLUME: 5	CHAPTER: 16	# OF PAGES: 7

SUBJECT: CRIMINAL JUSTICE INFORMATION SYSTEM (CJIS)

EFFECTIVE DATE: **February 1,2016**	ACCREDITATION STANDARDS: **N/A**
BY THE ORDER OF: **Chief Patrick Shannon**	
BY AUTHORITY OF: **Police Director James Cosgrove**	

SUPERSEDES ORDER #: G.O. 154 (12/04/03), G.O. 140 (01/14/00)

PURPOSE The purpose of this general order is to codify this agency's procedures regarding the use of the criminal justice information system commonly referred to as CJIS.

POLICY It is the policy of the Elizabeth Police Department to conform to the requirements set forth in the *CJIS User Agreement* with the New Jersey State Police and to any applicable policies and procedures established by the Federal Bureau of Investigation, New Jersey Attorney General and/or Union County Prosecutor.

PROCEDURES

I. GENERAL PROVISIONS

A. For purposes of this general order, the following applications are considered part of CJIS:

1. NCIC – National Crime Information Center

2. NLETS – National Law Enforcement Telecommunication System

3. NJLETS – New Jersey Law Enforcement Telecommunication System

B. This general order also installs a mechanism to:

1. Provide for continuing education and certification in the use of the CJIS equipment and applications;

2. Adequately document required CJIS transactions in accordance with FBI, NJSP, and Union County Prosecutor's Office requirements;

3. Identify potential abuses.

C. The Chief of Police shall appoint the terminal agency coordinator (TAC) and assistant terminal agency coordinators (ATACs).

1. The TAC and ATACs are primarily responsible for ensuring the integrity of the equipment and various applications.

2. The TAC and ATACs have full staff and functional authority over all matters pertaining to CJIS related matters.

3. The TAC and ATACs shall ensure that terminal users are familiar with the various applications and shall provide the necessary training where indicated, including regular competency tests. Terminal operators shall receive a minimum biennial recertification that includes an affirmation of proficiency.

4. Upon recommendation by the TAC and ATACs, The Chief of Police shall determine what personnel have access to the CJIS terminals and applications.

D. The Chief of Police shall also appoint a local area security officer (LASO) to oversee the security of the CJIS network equipment. The LASO can be a person different from the TAC and ATACs.

E. All terminal operators must pass a background investigation as described within the NJCJIS Security Policy.

F. All terminal operators must successfully complete a basic CJIS training course that minimally includes NCIC, NJLETS, NLETS, NJDMV and NJCJIS policies and procedures, hit confirmations and terminal security.

G. Terminal operators are responsible for checking the CJIS Manual website (*http://172.25.15.10/index.html*) for access to all manuals, technical updates, and training notes distributed by the NJSP and the FBI.

H. Terminal operator shall not utilize other operator's access codes.

I. Terminal operator users shall be assigned a unique user ID. The unique user ID, including password, shall not be shared with any other person, nor shall anyone utilize another user's ID or password. Passwords are selected by the individual user and 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 ID.

4. Expire within a maximum of 90 calendar days;

5. Not be identical to the previous ten (10) passwords;

6. Not be displayed when entered.

J. All personnel who operate NJCJIS must adhere to the FBI's Criminal Justice Information Services Security Policy and NJCJIS Security Policy, as amended.

K. The FBI's Criminal Justice Information Services Security Policy, CJIS User Agreement, Non-Compliance Sanction Plan, and the CJIS Security Policy can be viewed via Internet (*http://172.25.15.10/index.html*).

L. All CJIS network equipment, including switches, patch panels, servers, desktop workstations, communications center workstations and mobile data computer workstations shall be secured at all times to retard unauthorized access or viewing.

1. The LASO is responsible for maintaining a complete network diagram depicting the interconnectivity of this agency's CJIS network. This topological drawing shall be kept current at all times with revisions forwarded to the Chief of Police.

2. The LASO is responsible for maintaining the security of all network equipment and associated physical media (e.g., manuals, hard drives (internal and external), memory boards, data disks, CDs, DVDs, flash drives, etc.).

3. The LASO shall keep the CJIS server room/area secured at all times and deny access to all persons without a legitimate need.

a. The LASO must create a record when an authorized visitor enters the CJIS server room/area. The record shall document the identity of the escorting officer, the visitor, and the timeframe.

b. Visitors shall be under escort at all times.

4. Personnel are prohibited from installing any program to a computer workstation or terminal on the CJIS network without the expressed written permission of the LASO.

M. All data received from any NJCJIS workstation or mobile data computer/terminal is confidential information for use by authorized criminal justice personnel, for criminal justice purposes only. Unauthorized disclosure could result not only in departmental discipline, but also subject to civil liabilities and criminal penalties.

1. All data received from or stored in any workstation, mobile data computer, server or related physical media shall be securely maintained and disposed of in accordance with New Jersey Division of Revenue and Enterprise Services, Bureau of Records Management (BRM) records retention schedules and N.J.A.C. 15:3-1 et seq.

2. Data that has exceeded the retention requirements of BRM shall be destroyed or sanitized.

3. Physical media shall be destroyed or sanitized in any of the following methods:

a. Shredding (paper records, data disks, CDs. DVDs)

b. Erasure by deleting and reformatting (data disks, CDs. DVDs, hard drives, flash drives, etc.)

c. Physical destruction.

4. The LASO shall maintain a log of all media that is destroyed or sanitized including the type of media, reason for disposal/destruction, and date of disposal/destruction.

II. CJIS TRANSACTIONS

A. CJIS terminal operators duties include, but are not limited to:

1. The prompt entry of appropriate time sensitive Elizabeth Police data (e.g., stolen and recovered motor vehicle investigations, missing persons investigations, etc.)

2. Response to and proper dissemination of messages directed to the Elizabeth Police Department.

3. Proper dissemination of bulletins directed to all organizational subcomponents.

4. Checking for active warrants on all individuals arrested by the Elizabeth Police Department.

5. Messages to other organizational subcomponents or law enforcement agencies as directed by appropriate supervisory personnel.

B. The various manuals dealing with NCIC/CJIS transactions need not be repeated within this policy, but a short synopsis of important points is provided.

C. CJIS Manuals, policies, newsletters, agreements and forms are accessible at all CJIS terminals via the Internet (*http://172.25.15.10/index.html*).

D. Each entry should be 'packed' with as many identifiers as possible. This serves to reduce the chance of false hits and unnecessary CJIS transactions. Operators are required to modify entries when required.

E. When making any entry or removal of a NCIC record the NIC number will be memorialized in CAD and in investigation report.

F. Stolen MV entries: As much information as possible must be entered into the appropriate fields. Note that each state's DMV identifiers may not conform to standard NCIC codes. Therefore, it is incumbent upon terminal operators to verify the information provided by each state's DMV record and the information provided by the investigator prior to entry.

G. NCIC wanted person: The Union County Prosecutor's Office must preauthorize any entry requiring extradition outside of New Jersey.

H. Missing persons: Refer to *General Order V3C22*, *Missing and Unidentified Person Investigations*. Again, pack the record as much as possible to facilitate identification and to minimize the chance of false hits. Update and modify records, when appropriate

I. Hit confirmations: Upon receipt of a hit confirmation request, the operator shall ensure that a substantive response is furnished. Urgent hit requests require a ten-minute response. Routine hit requests require a one-hour response. A substantive response is a positive or negative confirmation or notice of a specific amount of time necessary to confirm or reject.

J. Guns: All surrendered and recovered guns that come into the possession of this agency will be queried in NCIC and if they meet the requirements will be entered into NCIC as a recovered gun.

1. eTrace: When entering a recovered gun, the '*Enter Recovered Gun Screen*' must be utilized. Upon completing the first page, click on the eTrace tab and complete all pertinent fields. When entering the NCIC Crime Code utilize '0098' for '*Found/Abandoned*' if the gun has been surrendered. Additionally, click on the '*Misc. Info*' tab and type in "*surrendered weapon, no criminal charges at this time*." Additional information and codes can be found in the *How to Submit Gun Traces NJ Trace Manual*.

K. Articles: Refer to the NCIC Operator's Manual for entry criteria. Be sure to use the article names as defined in the NCIC Code Manual.

III. CCH/III

A. CCH refers to computerized criminal history, a State of New Jersey database. III refers to interstate identification index. Both of these applications are strictly monitored and controlled. Authorized personnel may access CCH/III files as follows:

1. A *CCH Detailed Record Request* should be conducted for all criminal arrests (1st, 2nd, 3rd, and 4th degree crimes), including domestic violence and CDS related offenses, but not for municipal ordinance violations. Once the *Detailed Record Request* has served its use in the criminal investigation, it will be destroyed.

2. A *CCH Detained Record Request* should be conducted prior to NCIC and/or missing person entries. If an arrest record is present, the pedigree on the first page can be utilized to pack the record. If used, the pedigree shall be attached to the appropriate incident report and files. The remainder of the record must be destroyed after it has served its investigative purpose.

3. Only personnel authorized to run CCH/III queries can conduct such queries.

4. Authorized CCH personnel may request and receive criminal history information in either of two circumstances, specifically:

   a. To further a criminal investigation; or

   b. Where the officer determines that the encounter constitutes a situation affecting the safety of an officer. This determination is left to the discretion of the officer.

   c. Note: criminal history information showing that a detainee had been previously convicted of armed offenses does not, by itself, justify a protective frisk (*State v. Valentine*). Furthermore, criminal history information may provide the articulable facts warranting heightened caution that in appropriate cases might justify order a passenger out of a lawfully detained vehicle. (*State v. Smith*)

5. All requests for CCH are electronically logged and shall be periodically checked by the TAC officer for compliance.

   a. Requests by the Elizabeth Municipal Court for a CCH record shall be logged as NJ020011J on the automated log.

   b. Requests for a CCH record for all persons arrested on a domestic violence restraining order violation shall be attached to the domestic violence package prepared for the Union County Family Court and shall be logged on the automated log as U.C. Family Court NJ020013A.

6. The term '*destroy the record*' shall be narrowly construed to mean rendering the record useless through shredding or similar destruction. Records containing criminal histories shall not be discarded in the trash without shredding.

IV. ADMINISTRATIVE OFFICE OF THE COURTS (AOC) APPLICATIONS

A. The Administrative Office of the Courts is a subsidiary of the New Jersey judicial branch and is not governed by the New Jersey State Police or any subdivision of the executive branch.

B. The following applications are governed in this section:

1. Automated Complaint System (ACS);

2. Automated Traffic System (ATS);

3. Domestic Violence Central Registry (DVCR);

4. PROMIS/GAVEL (Prosecution Management).

C. All personnel who operate AOC applications must adhere to the AOC Security Policy.

D. Data received from any AOC application is confidential information for use by authorized criminal justice personnel, for criminal justice purposes only. Unauthorized disclosure could result in criminal, civil and administrative penalties.

E. The TAC and/or ATACs are responsible for ensuring the integrity of the AOC applications. The TAC and ATACs shall have full staff and functional authority over all matters pertaining to AOC related matters.

F. The TAC and ATACs shall be responsible for distributing all manuals, technical updates and training notes distributed by the AOC. When this occurs the TAC and ATACs will document this in the CJIS training log for each terminal operator.

G. The TAC and ATACs shall ensure that terminal users are familiar with the various applications and shall provide the necessary training where indicated, including regular competency tests. Terminal operators shall receive a minimum biennial recertification that includes an affirmation of proficiency.

H. Terminal operators shall not utilize other operator's access codes for other transactions, such as generating criminal complaints on-line.

I. Record checks for wants and warrants shall also include a check of the person through ACS and ATS. Positive responses, including a copy of the warrant and warrant history must be printed and attached to the arrest reports. A computer record printout is considered a valid detainer. The computer record printout shall become part of the permanent record and shall ultimately be filed in the file jacket of the precipitating the event, when applicable.

J. The domestic violence central registry shall be utilized to its fullest extent when investigating and/or prosecuting domestic violence related cases.